발 간 등 록 번 호

전자금융 및 개인정보 관련 법규

2017.3.8

법제처 국가법령정보센터
Korea Law Service Center

목 차

정보통신망법

1. 정보통신망 이용촉진 및 정보보호 등에 관한 법률
2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령
3. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙
4. 정보보호관리체계 인증
5. 정보보호관리체계 인증
6. 정보보호 관리체계 인증 등에 관한 고시
7. 정보보호 관리체계 인증 등에 관한 고시
8. 정보보호 관리체계 인증 등에 관한 고시
9. 정보보호관리체계 인증 등에 관한 고시
10. 정보보호관리체계 인증 등에 관한 고시
11. 정보보호조치에 관한 지침
12. 정보보호 사전점검에 관한 고시
13. 집적정보 통신시설 보호지침
14. 정보보호 관리체계 인증 등에 관한 고시
15. 정보보호 관리체계 인증 등에 관한 고시

개인정보법

1. 개인정보 보호법 시행규칙
2. 표준 개인정보 보호지침
3. 개인정보의 안전성 확보조치 기준
4. 개인정보 보호법
5. 개인정보 보호법 시행령

기반보호법

1. 주요정보통신기반시설 취약점 분석 · 평가 기준
2. 미래창조과학부 소관 주요정보통신기반시설 보호지침
3. 정보통신기반 보호법
4. 정보통신기반 보호법 시행령
5. 정보통신기반 보호법 시행규칙

신용정보법

1. 신용정보업감독규정
2. 신용정보업감독규정
3. 신용정보업감독업무시행세칙
4. 신용정보업감독업무시행세칙
5. 신용정보의 이용 및 보호에 관한 법률
6. 신용정보의 이용 및 보호에 관한 법률 시행령
7. 신용정보의 이용 및 보호에 관한 법률 시행규칙

전자금융거래법

1. 전자금융감독규정
2. 전자금융감독규정시행세칙
3. 전자금융거래 기본약관
4. 전자금융거래법
5. 전자금융거래법 시행령

IT위탁

1. 금융기관의 업무위탁 등에 관한 규정
2. 금융회사의 정보처리 업무 위탁에 관한 규정

정보통신망법

1. 정보통신망 이용촉진 및 정보보호 등에 관한 법률
2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령
3. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙
4. 정보보호관리체계 인증
5. 정보보호관리체계 인증
6. 정보보호 관리체계 인증 등에 관한 고시
7. 정보보호 관리체계 인증 등에 관한 고시
8. 정보보호 관리체계 인증 등에 관한 고시
9. 정보보호관리체계 인증 등에 관한 고시
10. 정보보호관리체계 인증 등에 관한 고시
11. 정보보호조치에 관한 지침
12. 정보보호 사전점검에 관한 고시
13. 집적정보 통신시설 보호지침
14. 정보보호 관리체계 인증 등에 관한 고시
15. 정보보호 관리체계 인증 등에 관한 고시

정보통신망 이용촉진 및 정보보호 등에 관한 법률

[시행 2016.9.23] [법률 제14080호, 2016.3.22, 일부개정]

제1장 총칙

제1조(목적) 이 법은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다.

[전문개정 2008.6.13]

제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2004.1.29, 2007.1.26, 2007.12.21, 2008.6.13, 2010.3.22, 2014.5.28>

1. "정보통신망"이란 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.
2. "정보통신서비스"란 「전기통신사업법」 제2조제6호에 따른 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다.
3. "정보통신서비스 제공자"란 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.
4. "이용자"란 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
5. "전자문서"란 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 저장된 문서형식의 자료로서 표준화된 것을 말한다.
6. "개인정보"란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.
7. "침해사고"란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다.
8. 삭제 <2015.6.22>
9. "게시판"이란 그 명칭과 관계없이 정보통신망을 이용하여 일반에게 공개할 목적으로 부호·문자·음성·음향·화상·동영상 등의 정보를 이용자가 게재할 수 있는 컴퓨터 프로그램

이나 기술적 장치를 말한다.

10. "통신과금서비스"란 정보통신서비스로서 다음 각 목의 업무를 말한다.

가. 타인이 판매·제공하는 재화 또는 용역(이하 "재화등"이라 한다)의 대가를 자신이 제공하는 전기통신역무의 요금과 함께 청구·징수하는 업무

나. 타인이 판매·제공하는 재화등의 대가가 가목의 업무를 제공하는 자의 전기통신역무의 요금과 함께 청구·징수되도록 거래정보를 전자적으로 송수신하는 것 또는 그 대가의 정산을 대행하거나 매개하는 업무

11. "통신과금서비스제공자"란 제53조에 따라 등록을 하고 통신과금서비스를 제공하는 자를 말한다.

12. "통신과금서비스이용자"란 통신과금서비스제공자로부터 통신과금서비스를 이용하여 재화등을 구입·이용하는 자를 말한다.

13. "전자적 전송매체"란 정보통신망을 통하여 부호·문자·음성·화상 또는 영상 등을 수신자에게 전자문서 등의 전자적 형태로 전송하는 매체를 말한다.

② 이 법에서 사용하는 용어의 뜻은 제1항에서 정하는 것 외에는 「국가정보화 기본법」에서 정하는 바에 따른다.<개정 2008.6.13, 2013.3.23>

제3조(정보통신서비스 제공자 및 이용자의 책무) ① 정보통신서비스 제공자는 이용자의 개인정보를 보호하고 건전하고 안전한 정보통신서비스를 제공하여 이용자의 권익보호와 정보이용능력의 향상에 이바지하여야 한다.

② 이용자는 건전한 정보사회가 정착되도록 노력하여야 한다.

③ 정부는 정보통신서비스 제공자단체 또는 이용자단체의 개인정보보호 및 정보통신망에서의 청소년 보호 등을 위한 활동을 지원할 수 있다.

[전문개정 2008.6.13]

제4조(정보통신망 이용촉진 및 정보보호등에 관한 시책의 마련) ① 미래창조과학부장관 또는 방송통신위원회는 정보통신망의 이용촉진 및 안정적 관리·운영과 이용자의 개인정보보호 등(이하 "정보통신망 이용촉진 및 정보보호등"이라 한다)을 통하여 정보사회의 기반을 조성하기 위한 시책을 마련하여야 한다. <개정 2011.3.29, 2013.3.23>

② 제1항에 따른 시책에는 다음 각 호의 사항이 포함되어야 한다.

1. 정보통신망에 관련된 기술의 개발·보급
2. 정보통신망의 표준화
3. 정보내용물 및 제11조에 따른 정보통신망 응용서비스의 개발 등 정보통신망의 이용 활성화
4. 정보통신망을 이용한 정보의 공동활용 촉진
5. 인터넷 이용의 활성화
6. 정보통신망을 통하여 수집·처리·보관·이용되는 개인정보의 보호 및 그와 관련된 기술의 개발·보급

7. 정보통신망에서의 청소년 보호
8. 정보통신망의 안전성 및 신뢰성 제고
9. 그 밖에 정보통신망 이용촉진 및 정보보호등을 위하여 필요한 사항

③ 미래창조과학부장관 또는 방송통신위원회는 제1항에 따른 시책을 마련할 때에는 「국가정보화 기본법」 제6조에 따른 국가정보화 기본계획과 연계되도록 하여야 한다.<개정 2011.3.29, 2013.3.23>

[전문개정 2008.6.13]

제5조(다른 법률과의 관계) 정보통신망 이용촉진 및 정보보호등에 관하여는 다른 법률에서 특별히 규정된 경우 외에는 이 법으로 정하는 바에 따른다. 다만, 제7장의 통신과금서비스에 관하여 이 법과 「전자금융거래법」의 적용이 경합하는 때에는 이 법을 우선 적용한다.

[전문개정 2008.6.13]

제2장 정보통신망의 이용촉진

제6조(기술개발의 추진 등) ① 미래창조과학부장관은 정보통신망과 관련된 기술 및 기기의 개발을 효율적으로 추진하기 위하여 대통령령으로 정하는 바에 따라 관련 연구기관으로 하여금 연구개발ㆍ기술협력ㆍ기술이전 또는 기술지도 등의 사업을 하게 할 수 있다. <개정 2013.3.23>

② 정부는 제1항에 따라 연구개발 등의 사업을 하는 연구기관에는 그 사업에 드는 비용의 전부 또는 일부를 지원할 수 있다.

③ 제2항에 따른 비용의 지급 및 관리 등에 필요한 사항은 대통령령으로 정한다.

[전문개정 2008.6.13]

제7조(기술관련 정보의 관리 및 보급) ① 미래창조과학부장관은 정보통신망과 관련된 기술 및 기기에 관한 정보(이하 이 조에서 "기술관련 정보"라 한다)를 체계적이고 종합적으로 관리하여야 한다. <개정 2013.3.23>

② 미래창조과학부장관은 기술관련 정보를 체계적이고 종합적으로 관리하기 위하여 필요하면 관계 행정기관 및 국공립 연구기관 등에 대하여 기술관련 정보와 관련된 자료를 요구할 수 있다. 이 경우 요구를 받은 기관의 장은 특별한 사유가 없으면 그 요구에 따라야 한다.<개정 2013.3.23>

③ 미래창조과학부장관은 기술관련 정보를 신속하고 편리하게 이용할 수 있도록 그 보급을 위한 사업을 하여야 한다.<개정 2013.3.23>

④ 제3항에 따라 보급하려는 정보통신망과 관련된 기술 및 기기의 범위에 관하여 필요한 사항은 대통령령으로 정한다.

[전문개정 2008.6.13]

제8조(정보통신망의 표준화 및 인증) ① 미래창조과학부장관은 정보통신망의 이용을 촉진하기 위하여 정보통신망에 관한 표준을 정하여 고시하고, 정보통신서비스 제공자 또는 정보통신망

과 관련된 제품을 제조하거나 공급하는 자에게 그 표준을 사용하도록 권고할 수 있다. 다만, 「산업표준화법」 제12조에 따른 한국산업표준이 제정되어 있는 사항에 대하여는 그 표준에 따른다. <개정 2013.3.23>

② 제1항에 따라 고시된 표준에 적합한 정보통신과 관련된 제품을 제조하거나 공급하는 자는 제9조제1항에 따른 인증기관의 인증을 받아 그 제품이 표준에 적합한 것임을 나타내는 표시를 할 수 있다.

③ 제1항 단서에 해당하는 경우로서 「산업표준화법」 제15조에 따라 인증을 받은 경우에는 제2항에 따른 인증을 받은 것으로 본다.

④ 제2항에 따른 인증을 받은 자가 아니면 그 제품이 표준에 적합한 것임을 나타내는 표시를 하거나 이와 비슷한 표시를 하여서는 아니 되며, 이와 비슷한 표시를 한 제품을 판매하거나 판매할 목적으로 진열하여서는 아니 된다.

⑤ 미래창조과학부장관은 제4항을 위반하여 제품을 판매하거나 판매할 목적으로 진열한 자에게 그 제품을 수거·반품하도록 하거나 인증을 받아 그 표시를 하도록 하는 등 필요한 시정조치를 명할 수 있다.<개정 2013.3.23>

⑥ 제1항부터 제3항까지의 규정에 따른 표준화의 대상·방법·절차 및 인증표시, 제5항에 따른 수거·반품·시정 등에 필요한 사항은 미래창조과학부령으로 정한다.<개정 2013.3.23>

[전문개정 2008.6.13]

제9조(인증기관의 지정 등) ① 미래창조과학부장관은 정보통신망과 관련된 제품을 제조하거나 공급하는 자의 제품이 제8조제1항 본문에 따라 고시된 표준에 적합한 제품임을 인증하는 기관(이하 "인증기관"이라 한다)을 지정할 수 있다. <개정 2013.3.23>

② 미래창조과학부장관은 인증기관이 다음 각 호의 어느 하나에 해당하면 그 지정을 취소하거나 6개월 이내의 기간을 정하여 업무의 정지를 명할 수 있다. 다만, 제1호에 해당하는 경우에는 그 지정을 취소하여야 한다.<개정 2013.3.23>

1. 속임수나 그 밖의 부정한 방법으로 지정을 받은 경우
2. 정당한 사유 없이 1년 이상 계속하여 인증업무를 하지 아니한 경우
3. 제3항에 따른 지정기준에 미달한 경우

③ 제1항 및 제2항에 따른 인증기관의 지정기준·지정절차, 지정취소·업무정지의 기준 등에 필요한 사항은 미래창조과학부령으로 정한다.<개정 2013.3.23>

[전문개정 2008.6.13]

제10조(정보내용물의 개발 지원) 정부는 국가경쟁력을 확보하거나 공익을 증진하기 위하여 정보통신망을 통하여 유통되는 정보내용물을 개발하는 자에게 재정 및 기술 등 필요한 지원을 할 수 있다.

[전문개정 2008.6.13]

제11조(정보통신망 응용서비스의 개발 촉진 등) ① 정부는 국가기관·지방자치단체 및 공공기관이 정보통신망을 활용하여 업무를 효율화·자동화·고도화하는 응용서비스(이하 "정보통신

망 응용서비스"라 한다)를 개발·운영하는 경우 그 기관에 재정 및 기술 등 필요한 지원을 할 수 있다.

② 정부는 민간부문에 의한 정보통신망 응용서비스의 개발을 촉진하기 위하여 재정 및 기술 등 필요한 지원을 할 수 있으며, 정보통신망 응용서비스의 개발에 필요한 기술인력을 양성하기 위하여 다음 각 호의 시책을 마련하여야 한다.

1. 각급 학교나 그 밖의 교육기관에서 시행하는 인터넷 교육에 대한 지원
2. 국민에 대한 인터넷 교육의 확대
3. 정보통신망 기술인력 양성사업에 대한 지원
4. 정보통신망 전문기술인력 양성기관의 설립·지원
5. 정보통신망 이용 교육프로그램의 개발 및 보급 지원
6. 정보통신망 관련 기술자격제도의 정착 및 전문기술인력 수급 지원
7. 그 밖에 정보통신망 관련 기술인력의 양성에 필요한 사항

[전문개정 2008.6.13]

제12조(정보의 공동활용체제 구축) ① 정부는 정보통신망을 효율적으로 활용하기 위하여 정보통신망 상호 간의 연계 운영 및 표준화 등 정보의 공동활용체제 구축을 권장할 수 있다.

② 정부는 제1항에 따른 정보의 공동활용체제를 구축하는 자에게 재정 및 기술 등 필요한 지원을 할 수 있다.

③ 제1항과 제2항에 따른 권장 및 지원에 필요한 사항은 대통령령으로 정한다.

[전문개정 2008.6.13]

제13조(정보통신망의 이용촉진 등에 관한 사업) ① 미래창조과학부장관은 공공, 지역, 산업, 생활 및 사회적 복지 등 각 분야의 정보통신망의 이용촉진과 정보격차의 해소를 위하여 관련 기술·기기 및 응용서비스의 효율적인 활용·보급을 촉진하기 위한 사업을 대통령령으로 정하는 바에 따라 실시할 수 있다. <개정 2013.3.23>

② 정부는 제1항에 따른 사업에 참여하는 자에게 재정 및 기술 등 필요한 지원을 할 수 있다.

[전문개정 2008.6.13]

제14조(인터넷 이용의 확산) 정부는 인터넷 이용이 확산될 수 있도록 공공 및 민간의 인터넷 이용시설의 효율적 활용을 유도하고 인터넷 관련 교육 및 홍보 등의 인터넷 이용기반을 확충하며, 지역별·성별·연령별 인터넷 이용격차를 해소하기 위한 시책을 마련하고 추진하여야 한다.

[전문개정 2008.6.13]

제15조(인터넷 서비스의 품질 개선) ① 미래창조과학부장관은 인터넷 서비스 이용자의 권익을 보호하고 인터넷 서비스의 품질 향상 및 안정적 제공을 보장하기 위한 시책을 마련하여야 한다. <개정 2013.3.23>

② 미래창조과학부장관은 제1항에 따른 시책을 추진하기 위하여 필요하면 정보통신서비스 제공자단체 및 이용자단체 등의 의견을 들어 인터넷 서비스 품질의 측정·평가에 관한 기준을 정하여 고시할 수 있다.<개정 2013.3.23>

③ 정보통신서비스 제공자는 제2항에 따른 기준에 따라 자율적으로 인터넷 서비스의 품질 현황을 평가하여 그 결과를 이용자에게 알려줄 수 있다.

[전문개정 2008.6.13]

제16조 삭제 <2004.1.29>

제17조 삭제 <2004.1.29>

제3장 삭제 <2015.6.22>

제18조 삭제 <2015.6.22>

제19조 삭제 <2015.6.22>

제20조 삭제 <2015.6.22>

제21조 삭제 <2015.6.22>

제4장 개인정보의 보호

제1절 개인정보의 수집·이용 및 제공 등

제22조(개인정보의 수집·이용 동의 등) ① 정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항을 변경하려는 경우에도 또한 같다.

1. 개인정보의 수집·이용 목적
2. 수집하는 개인정보의 항목
3. 개인정보의 보유·이용 기간

② 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 제1항에 따른 동의 없이 이용자의 개인정보를 수집·이용할 수 있다.

1. 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우
2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
3. 이 법 또는 다른 법률에 특별한 규정이 있는 경우

[전문개정 2008.6.13]

제23조(개인정보의 수집 제한 등) ① 정보통신서비스 제공자는 사상, 신념, 가족 및 친인척관계, 학력(學歷)·병력(病歷), 기타 사회활동 경력 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 제22조제1항에 따른 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 필요한 범위에서 최소한으로 그 개인정보를 수집할 수 있다. <개정 2014.5.28>

② 정보통신서비스 제공자는 이용자의 개인정보를 수집하는 경우에는 정보통신서비스의 제공을 위하여 필요한 범위에서 최소한의 개인정보만 수집하여야 한다.<개정 2014.5.28>

③ 정보통신서비스 제공자는 이용자가 필요한 최소한의 개인정보 이외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 아니 된다. 이 경우 필요한 최소한의 개인정보는 해당 서비스의 본질적 기능을 수행하기 위하여 반드시 필요한 정보를 말한다.<신설 2014.5.28>

[전문개정 2008.6.13]

제23조의2(주민등록번호의 사용 제한) ① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다.

1. 제23조의3에 따라 본인확인기관으로 지정받은 경우
2. 법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우
3. 영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는 경우

② 제1항제2호 또는 제3호에 따라 주민등록번호를 수집·이용할 수 있는 경우에도 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하 "대체수단"이라 한다)을 제공하여야 한다.

[전문개정 2012.2.17]

제23조의3(본인확인기관의 지정 등) ① 방송통신위원회는 다음 각 호의 사항을 심사하여 대체수단의 개발·제공·관리 업무(이하 "본인확인업무"라 한다)를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 본인확인기관으로 지정할 수 있다.

1. 본인확인업무의 안전성 확보를 위한 물리적·기술적·관리적 조치계획
2. 본인확인업무의 수행을 위한 기술적·재정적 능력
3. 본인확인업무 관련 설비규모의 적정성

② 본인확인기관이 본인확인업무의 전부 또는 일부를 휴지하고자 하는 때에는 휴지기간을 정하여 휴지하고자 하는 날의 30일 전까지 이를 이용자에게 통보하고 방송통신위원회에 신고하여야 한다. 이 경우 휴지기간은 6개월을 초과할 수 없다.

③ 본인확인기관이 본인확인업무를 폐지하고자 하는 때에는 폐지하고자 하는 날의 60일 전까지 이를 이용자에게 통보하고 방송통신위원회에 신고하여야 한다.

④ 제1항부터 제3항까지의 규정에 따른 심사사항별 세부 심사기준·지정절차 및 휴지·폐지 등에 관하여 필요한 사항은 대통령령으로 정한다.

[본조신설 2011.4.5]

제23조의4(본인확인업무의 정지 및 지정취소) ① 방송통신위원회는 본인확인기관이 다음 각 호의 어느 하나에 해당하는 때에는 6개월 이내의 기간을 정하여 본인확인업무의 전부 또는 일부의 정지를 명하거나 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 때에는 그 지정을 취소하여야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 본인확인기관의 지정을 받은 경우
2. 본인확인업무의 정지명령을 받은 자가 그 명령을 위반하여 업무를 정지하지 아니한 경우
3. 지정받은 날부터 6개월 이내에 본인확인업무를 개시하지 아니하거나 6개월 이상 계속하여 본인확인업무를 휴지한 경우
4. 제23조의3제4항에 따른 지정기준에 적합하지 아니하게 된 경우

② 제1항에 따른 처분의 기준, 절차 및 그 밖에 필요한 사항은 대통령령으로 정한다.

[본조신설 2011.4.5]

제2절 삭제 <2007.1.26>

제24조(개인정보의 이용 제한) 정보통신서비스 제공자는 제22조 및 제23조제1항 단서에 따라 수집한 개인정보를 이용자로부터 동의받은 목적이나 제22조제2항 각 호에서 정한 목적과 다른 목적으로 이용하여서는 아니 된다.

[전문개정 2008.6.13]

제24조의2(개인정보의 제공 동의 등) ① 정보통신서비스 제공자는 이용자의 개인정보를 제3자에게 제공하려면 제22조제2항제2호 및 제3호에 해당하는 경우 외에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간

② 제1항에 따라 정보통신서비스 제공자로부터 이용자의 개인정보를 제공받은 자는 그 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우 외에는 개인정보를 제3자에게 제공하거나 제공받은 목적 외의 용도로 이용하여서는 아니 된다.

③ 제25조제1항에 따른 정보통신서비스 제공자등은 제1항에 따른 제공에 대한 동의와 제25조제1항에 따른 개인정보 처리위탁에 대한 동의를 받을 때에는 제22조에 따른 개인정보의 수집·이용에 대한 동의와 구분하여 받아야 하고, 이에 동의하지 아니한다는 이유로 서비스 제공을 거부하여서는 아니 된다.<신설 2011.4.5, 2016.3.22>

[전문개정 2008.6.13]

제25조(개인정보의 처리위탁) ① 정보통신서비스 제공자와 그로부터 제24조의2제1항에 따라 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)는 제3자에게 이용자의 개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위(이하 "처리"라 한다)를 할 수 있도록 업무를 위탁(이하 "개인정보 처리위탁"이라 한다)하는 경우에는 다음 각 호의 사항 모두를 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다. <개정 2016.3.22>

1. 개인정보 처리위탁을 받는 자(이하 "수탁자"라 한다)
2. 개인정보 처리위탁을 하는 업무의 내용

② 정보통신서비스 제공자등은 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 제1항 각 호의 사항 모두를 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 처리위탁에 따른 제1항의 고지절차와 동의절차를 거치지 아니할 수 있다. 제1항 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.<개정 2014.5.28, 2016.3.22>

③ 정보통신서비스 제공자등은 개인정보 처리위탁을 하는 경우에는 수탁자가 이용자의 개인정보를 처리할 수 있는 목적을 미리 정하여야 하며, 수탁자는 이 목적을 벗어나서 이용자의 개인정보를 처리하여서는 아니 된다.<개정 2016.3.22>

④ 정보통신서비스 제공자등은 수탁자가 이 장의 규정을 위반하지 아니하도록 관리·감독 및 교육하여야 한다.<개정 2016.3.22>

⑤ 수탁자가 개인정보 처리위탁을 받은 업무와 관련하여 이 장의 규정을 위반하여 이용자에게 손해를 발생시키면 그 수탁자를 손해배상책임에 있어서 정보통신서비스 제공자등의 소속 직원으로 본다.<개정 2016.3.22>

⑥ 정보통신서비스 제공자등이 수탁자에게 개인정보 처리위탁을 할 때에는 문서에 의하여야 한다.<신설 2016.3.22>

⑦ 수탁자는 개인정보 처리위탁을 한 정보통신서비스 제공자등의 동의를 받은 경우에 한하여 제1항에 따라 위탁받은 업무를 제3자에게 재위탁할 수 있다.<신설 2016.3.22>

[전문개정 2008.6.13]

[제목개정 2016.3.22]

제26조(영업의 양수 등에 따른 개인정보의 이전) ① 정보통신서비스 제공자등이 영업의 전부 또는 일부의 양도·합병 등으로 그 이용자의 개인정보를 타인에게 이전하는 경우에는 미리 다음 각 호의 사항 모두를 인터넷 홈페이지 게시, 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알려야 한다.

1. 개인정보를 이전하려는 사실

2. 개인정보를 이전받는 자(이하 "영업양수자등"이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다. 이하 이 조에서 같다)·주소·전화번호 및 그 밖의 연락처
3. 이용자가 개인정보의 이전을 원하지 아니하는 경우 그 동의를 철회할 수 있는 방법과 절차

② 영업양수자등은 개인정보를 이전받으면 지체 없이 그 사실 및 영업양수자등의 성명·주소·전화번호 및 그 밖의 연락처를 인터넷 홈페이지 게시, 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알려야 한다.<개정 2014.5.28>

③ 영업양수자등은 정보통신서비스 제공자등이 이용자의 개인정보를 이용하거나 제공할 수 있는 당초 목적의 범위에서만 개인정보를 이용하거나 제공할 수 있다. 다만, 이용자로부터 별도의 동의를 받은 경우에는 그러하지 아니하다.

[전문개정 2008.6.13]

제26조의2(동의를 받는 방법) 제22조제1항, 제23조제1항 단서, 제24조의2제1항·제2항, 제25조제1항, 제26조제3항 단서 또는 제63조제2항에 따른 동의(이하 "개인정보 수집·이용·제공 등의 동의"라 한다)를 받는 방법은 개인정보의 수집매체, 업종의 특성 및 이용자의 수 등을 고려하여 대통령령으로 정한다.

[전문개정 2008.6.13]

제2절 개인정보의 관리 및 파기 등 <신설 2007.1.26>

제27조(개인정보 보호책임자의 지정) ① 정보통신서비스 제공자등은 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보 보호책임자를 지정하여야 한다. 다만, 종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자등의 경우에는 지정하지 아니할 수 있다. <개정 2016.3.22>

② 제1항 단서에 따른 정보통신서비스 제공자등이 개인정보 보호책임자를 지정하지 아니하는 경우에는 그 사업주 또는 대표자가 개인정보 보호책임자가 된다.<개정 2016.3.22>

③ 개인정보 보호책임자의 자격요건과 그 밖의 지정에 필요한 사항은 대통령령으로 정한다. <개정 2016.3.22>

④ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 정보통신서비스 제공자등의 사업주 또는 대표자에게 개선조치를 보고하여야 한다. 다만, 제2항에 따라 사업주 또는 대표자가 개인정보 보호책임자가 되는 경우에는 개선조치 보고에 대한 사항을 적용하지 아니한다. <신설 2016.3.22>

[전문개정 2008.6.13]

[제목개정 2016.3.22]

제27조의2(개인정보 처리방침의 공개) ① 정보통신서비스 제공자등은 이용자의 개인정보를 처리하는 경우에는 개인정보 처리방침을 정하여 이용자가 언제든지 쉽게 확인할 수 있도록 대통

령령으로 정하는 방법에 따라 공개하여야 한다. <개정 2016.3.22>

② 제1항에 따른 개인정보 처리방침에는 다음 각 호의 사항이 모두 포함되어야 한다.<개정 2012.2.17, 2016.3.22>

1. 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집방법
2. 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법인인 경우에는 법인의 명칭을 말한다), 제공받는 자의 이용 목적과 제공하는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 파기방법(제29조제1항 각 호 외의 부분 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
4. 개인정보 처리위탁을 하는 업무의 내용 및 수탁자(해당되는 경우에만 처리방침에 포함한다)
5. 이용자 및 법정대리인의 권리와 그 행사방법
6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항
7. 개인정보 보호책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처

③ 정보통신서비스 제공자등은 제1항에 따른 개인정보 처리방침을 변경하는 경우에는 그 이유 및 변경내용을 대통령령으로 정하는 방법에 따라 지체 없이 공지하고, 이용자가 언제든지 변경된 사항을 쉽게 알아 볼 수 있도록 조치하여야 한다.<개정 2016.3.22>

[전문개정 2008.6.13]

[제목개정 2016.3.22]

제27조의3(개인정보 유출등의 통지·신고) ① 정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 "유출등"이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다. <개정 2014.5.28, 2016.3.22>

1. 유출등이 된 개인정보 항목
2. 유출등이 발생한 시점
3. 이용자가 취할 수 있는 조치
4. 정보통신서비스 제공자등의 대응 조치
5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처

② 제1항의 신고를 받은 한국인터넷진흥원은 지체 없이 그 사실을 방송통신위원회에 알려야 한다.<신설 2014.5.28>

③ 정보통신서비스 제공자등은 제1항 본문 및 단서에 따른 정당한 사유를 방송통신위원회에 소명하여야 한다.<신설 2014.5.28>

④ 제1항에 따른 통지 및 신고의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다. <개정 2014.5.28>

⑤ 정보통신서비스 제공자등은 개인정보의 유출등에 대한 대책을 마련하고 그 피해를 최소화할 수 있는 조치를 강구하여야 한다.<개정 2014.5.28, 2016.3.22>

[본조신설 2012.2.17]

[제목개정 2016.3.22]

제28조(개인정보의 보호조치) ① 정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다. <개정 2016.3.22>

1. 개인정보를 안전하게 처리하기 위한 내부관리계획의 수립·시행
2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영
3. 접속기록의 위조·변조 방지를 위한 조치
4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치
5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치
6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치

② 정보통신서비스 제공자등은 이용자의 개인정보를 처리하는 자를 최소한으로 제한하여야 한다.<개정 2016.3.22>

[전문개정 2008.6.13]

제28조의2(개인정보의 누설금지) ① 이용자의 개인정보를 처리하고 있거나 처리하였던 자는 직무상 알게 된 개인정보를 훼손·침해 또는 누설하여서는 아니 된다. <개정 2016.3.22>

② 누구든지 그 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받아서는 아니 된다.

[전문개정 2008.6.13]

제29조(개인정보의 파기) ①정보통신서비스 제공자등은 다음 각 호의 어느 하나에 해당하는 경우에는 지체 없이 해당 개인정보를 복구·재생할 수 없도록 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다. <개정 2012.2.17, 2014.5.28>

1. 제22조제1항, 제23조제1항 단서 또는 제24조의2제1항·제2항에 따라 동의를 받은 개인정보의 수집·이용 목적이나 제22조제2항 각 호에서 정한 해당 목적을 달성한 경우
2. 제22조제1항, 제23조제1항 단서 또는 제24조의2제1항·제2항에 따라 동의를 받은 개인정보의 보유 및 이용 기간이 끝난 경우
3. 제22조제2항에 따라 이용자의 동의를 받지 아니하고 수집·이용한 경우에는 제27조의2제2항제3호에 따른 개인정보의 보유 및 이용 기간이 끝난 경우

4. 사업을 폐업하는 경우

② 정보통신서비스 제공자등은 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다. 다만, 그 기간에 대하여 다른 법령 또는 이용자의 요청에 따라 달리 정한 경우에는 그에 따른다.<신설 2012.2.17, 2015.12.1>

③ 정보통신서비스 제공자등은 제2항의 기간 만료 30일 전까지 개인정보가 파기되는 사실, 기간 만료일 및 파기되는 개인정보의 항목 등 대통령령으로 정하는 사항을 전자우편 등 대통령령으로 정하는 방법으로 이용자에게 알려야 한다.<신설 2015.12.1>

[전문개정 2008.6.13]

제3절 이용자의 권리

제30조(이용자의 권리 등) ① 이용자는 정보통신서비스 제공자등에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회할 수 있다.

② 이용자는 정보통신서비스 제공자등에 대하여 본인에 관한 다음 각 호의 어느 하나의 사항에 대한 열람이나 제공을 요구할 수 있고 오류가 있는 경우에는 그 정정을 요구할 수 있다.

1. 정보통신서비스 제공자등이 가지고 있는 이용자의 개인정보
2. 정보통신서비스 제공자등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황
3. 정보통신서비스 제공자등에게 개인정보 수집·이용·제공 등의 동의를 한 현황

③ 정보통신서비스 제공자등은 이용자가 제1항에 따라 동의를 철회하면 지체 없이 수집된 개인정보를 복구·재생할 수 없도록 파기하는 등 필요한 조치를 하여야 한다.<개정 2014.5.28>

④ 정보통신서비스 제공자등은 제2항에 따라 열람 또는 제공을 요구받으면 지체 없이 필요한 조치를 하여야 한다.

⑤ 정보통신서비스 제공자등은 제2항에 따라 오류의 정정을 요구받으면 지체 없이 그 오류를 정정하거나 정정하지 못하는 사유를 이용자에게 알리는 등 필요한 조치를 하여야 하고, 필요한 조치를 할 때까지는 해당 개인정보를 이용하거나 제공하여서는 아니 된다. 다만, 다른 법률에 따라 개인정보의 제공을 요청받은 경우에는 그 개인정보를 제공하거나 이용할 수 있다.

⑥ 정보통신서비스 제공자등은 제1항에 따른 동의의 철회 또는 제2항에 따른 개인정보의 열람·제공 또는 오류의 정정을 요구하는 방법을 개인정보의 수집방법보다 쉽게 하여야 한다.

⑦ 영업양수자등에 대하여는 제1항부터 제6항까지의 규정을 준용한다. 이 경우 "정보통신서비스 제공자등"은 "영업양수자등"으로 본다.

[전문개정 2008.6.13]

제30조의2(개인정보 이용내역의 통지) ① 정보통신서비스 제공자등으로서 대통령령으로 정하는 기준에 해당하는 자는 제22조 및 제23조제1항 단서에 따라 수집한 이용자 개인정보의 이용내역(제24조의2에 따른 제공 및 제25조에 따른 개인정보 처리위탁을 포함한다)을 주기적으로 이용자에게 통지하여야 한다. 다만, 연락처 등 이용자에게 통지할 수 있는 개인정보를 수

집하지 아니한 경우에는 그러하지 아니하다. <개정 2016.3.22>

② 제1항에 따라 이용자에게 통지하여야 하는 정보의 종류, 통지 주기 및 방법, 그 밖에 이용내역 통지에 필요한 사항은 대통령령으로 정한다.

[본조신설 2012.2.17]

제31조(법정대리인의 권리) ① 정보통신서비스 제공자등이 만 14세 미만의 아동으로부터 개인정보 수집、이용、제공 등의 동의를 받으려면 그 법정대리인의 동의를 받아야 한다. 이 경우 정보통신서비스 제공자는 그 아동에게 법정대리인의 동의를 받기 위하여 필요한 법정대리인의 성명 등 최소한의 정보를 요구할 수 있다.

② 법정대리인은 해당 아동의 개인정보에 대하여 제30조제1항 및 제2항에 따른 이용자의 권리를 행사할 수 있다.

③ 제2항에 따른 법정대리인의 동의 철회, 열람 또는 오류정정의 요구에 관하여는 제30조제3항부터 제5항까지의 규정을 준용한다.

[전문개정 2008.6.13]

제32조(손해배상) ①이용자는 정보통신서비스 제공자등이 이 장의 규정을 위반한 행위로 손해를 입으면 그 정보통신서비스 제공자등에게 손해배상을 청구할 수 있다. 이 경우 해당 정보통신서비스 제공자등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다. <개정 2016.3.22>

② 정보통신서비스 제공자등의 고의 또는 중대한 과실로 인하여 개인정보가 분실、도난、유출、위조、변조 또는 훼손된 경우로서 이용자에게 손해가 발생한 때에는 법원은 그 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다. 다만, 정보통신서비스 제공자등이 고의 또는 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다.<신설 2016.3.22>

③ 법원은 제2항의 손해배상액을 정할 때에는 다음 각 호의 사항을 고려하여야 한다.<신설 2016.3.22>

1. 고의 또는 손해 발생의 우려를 인식한 정도
2. 위반행위로 인하여 입은 피해 규모
3. 위반행위로 인하여 정보통신서비스 제공자등이 취득한 경제적 이익
4. 위반행위에 따른 벌금 및 과징금
5. 위반행위의 기간、횟수 등
6. 정보통신서비스 제공자등의 재산상태
7. 정보통신서비스 제공자등이 이용자의 개인정보 분실、도난、유출 후 해당 개인정보를 회수하기 위하여 노력한 정도
8. 정보통신서비스 제공자등이 이용자의 피해구제를 위하여 노력한 정도

[전문개정 2008.6.13]

제32조의2(법정손해배상의 청구) ① 이용자는 다음 각 호의 모두에 해당하는 경우에는 대통령령으로 정하는 기간 내에 정보통신서비스 제공자등에게 제32조에 따른 손해배상을 청구하는

대신 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 정보통신서비스 제공자등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다. <개정 2016.3.22>

1. 정보통신서비스 제공자등이 고의 또는 과실로 이 장의 규정을 위반한 경우
2. 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우

② 법원은 제1항에 따른 청구가 있는 경우에 변론 전체의 취지와 증거조사의 결과를 고려하여 제1항의 범위에서 상당한 손해액을 인정할 수 있다.

③ 제32조에 따라 손해배상을 청구한 이용자는 사실심의 변론이 종결되기 전까지 그 청구를 제1항에 따른 청구로 변경할 수 있다.<신설 2016.3.22>

[본조신설 2014.5.28]

제32조의3(노출된 개인정보의 삭제·차단) ① 정보통신서비스 제공자등은 주민등록번호, 계좌정보, 신용카드정보 등 이용자의 개인정보가 정보통신망을 통하여 공중에 노출되지 아니하도록 하여야 한다.

② 정보통신서비스 제공자등은 방송통신위원회 또는 한국인터넷진흥원의 요청이 있는 경우 제1항의 노출된 개인정보에 대한 삭제·차단 등 필요한 조치를 취하여야 한다.

[본조신설 2016.3.22]

제4절 삭제 <2011.3.29>

제33조 삭제 <2011.3.29>

제33조의2 삭제 <2011.3.29>

제34조 삭제 <2011.3.29>

제35조 삭제 <2011.3.29>

제36조 삭제 <2011.3.29>

제37조 삭제 <2011.3.29>

제38조 삭제 <2011.3.29>

제39조 삭제 <2011.3.29>

제40조 삭제 <2011.3.29>

제5장 정보통신망에서의 이용자 보호 등 <개정 2007.1.26>

제41조(청소년 보호를 위한 시책의 마련 등) ① 방송통신위원회는 정보통신망을 통하여 유통되는 음란·폭력정보 등 청소년에게 해로운 정보(이하 "청소년유해정보"라 한다)로부터 청소년을 보호하기 위하여 다음 각 호의 시책을 마련하여야 한다.

1. 내용 선별 소프트웨어의 개발 및 보급
2. 청소년 보호를 위한 기술의 개발 및 보급
3. 청소년 보호를 위한 교육 및 홍보
4. 그 밖에 청소년 보호를 위하여 대통령령으로 정하는 사항

② 방송통신위원회는 제1항에 따른 시책을 추진할 때에는 「방송통신위원회의 설치 및 운영에 관한 법률」 제18조에 따른 방송통신심의위원회(이하 "심의위원회"라 한다), 정보통신서비스 제공자단체·이용자단체, 그 밖의 관련 전문기관이 실시하는 청소년 보호를 위한 활동을 지원할 수 있다.

[전문개정 2008.6.13]

제42조(청소년유해매체물의 표시) 전기통신사업자의 전기통신역무를 이용하여 일반에게 공개를 목적으로 정보를 제공하는 자(이하 "정보제공자"라 한다) 중 「청소년 보호법」 제2조제2호마목에 따른 매체물로서 같은 법 제2조제3호에 따른 청소년유해매체물을 제공하려는 자는 대통령령으로 정하는 표시방법에 따라 그 정보가 청소년유해매체물임을 표시하여야 한다. <개정 2011.9.15>

[전문개정 2008.6.13]

제42조의2(청소년유해매체물의 광고금지) 누구든지 「청소년 보호법」 제2조제2호마목에 따른 매체물로서 같은 법 제2조제3호에 따른 청소년유해매체물을 광고하는 내용의 정보를 정보통신망을 이용하여 부호·문자·음성·음향·화상 또는 영상 등의 형태로 같은 법 제2조제1호에 따른 청소년에게 전송하거나 청소년 접근을 제한하는 조치 없이 공개적으로 전시하여서는 아니 된다. <개정 2011.9.15>

[전문개정 2008.6.13]

제42조의3(청소년 보호 책임자의 지정 등) ① 정보통신서비스 제공자 중 일일 평균 이용자의 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 자는 정보통신망의 청소년유해정보로부터 청소년을 보호하기 위하여 청소년 보호 책임자를 지정하여야 한다.

② 청소년 보호 책임자는 해당 사업자의 임원 또는 청소년 보호와 관련된 업무를 담당하는 부서의 장에 해당하는 지위에 있는 자 중에서 지정한다.

③ 청소년 보호 책임자는 정보통신망의 청소년유해정보를 차단·관리하고, 청소년유해정보로부터의 청소년 보호계획을 수립하는 등 청소년 보호업무를 하여야 한다.

④ 제1항에 따른 청소년 보호 책임자의 지정에 필요한 사항은 대통령령으로 정한다.

[전문개정 2008.6.13]

제43조(영상 또는 음향정보 제공사업자의 보관의무) ① 「청소년 보호법」 제2조제2호마목에 따른 매체물로서 같은 법 제2조제3호에 따른 청소년유해매체물을 이용자의 컴퓨터에 저장 또는 기록되지 아니하는 방식으로 제공하는 것을 영업으로 하는 정보제공자 중 대통령령으로 정하는 자는 해당 정보를 보관하여야 한다. <개정 2011.9.15>

② 제1항에 따른 정보제공자가 해당 정보를 보관하여야 할 기간은 대통령령으로 정한다.

[전문개정 2008.6.13]

제44조(정보통신망에서의 권리보호) ① 이용자는 사생활 침해 또는 명예훼손 등 타인의 권리를 침해하는 정보를 정보통신망에 유통시켜서는 아니 된다.

② 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 제1항에 따른 정보가 유통되지 아니하도록 노력하여야 한다.

③ 방송통신위원회는 정보통신망에 유통되는 정보로 인한 사생활 침해 또는 명예훼손 등 타인에 대한 권리침해를 방지하기 위하여 기술개발·교육·홍보 등에 대한 시책을 마련하고 이를 정보통신서비스 제공자에게 권고할 수 있다.<개정 2013.3.23, 2014.5.28>

[전문개정 2008.6.13]

제44조의2(정보의 삭제요청 등) ① 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 처리한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 "삭제등"이라 한다)를 요청할 수 있다. <개정 2016.3.22>

② 정보통신서비스 제공자는 제1항에 따른 해당 정보의 삭제등을 요청받으면 지체 없이 삭제·임시조치 등의 필요한 조치를 하고 즉시 신청인 및 정보게재자에게 알려야 한다. 이 경우 정보통신서비스 제공자는 필요한 조치를 한 사실을 해당 게시판에 공시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다.

③ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 제42조에 따른 표시방법을 지키지 아니하는 청소년유해매체물이 게재되어 있거나 제42조의2에 따른 청소년 접근을 제한하는 조치 없이 청소년유해매체물을 광고하는 내용이 전시되어 있는 경우에는 지체 없이 그 내용을 삭제하여야 한다.

④ 정보통신서비스 제공자는 제1항에 따른 정보의 삭제요청에도 불구하고 권리의 침해 여부를 판단하기 어렵거나 이해당사자 간에 다툼이 예상되는 경우에는 해당 정보에 대한 접근을 임시적으로 차단하는 조치(이하 "임시조치"라 한다)를 할 수 있다. 이 경우 임시조치의 기간은 30일 이내로 한다.

⑤ 정보통신서비스 제공자는 필요한 조치에 관한 내용·절차 등을 미리 약관에 구체적으로 밝혀야 한다.

⑥ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보에 대하여 제2항에 따른 필요한 조치를 하면 이로 인한 배상책임을 줄이거나 면제받을 수 있다.

[전문개정 2008.6.13]

제44조의3(임의의 임시조치) ① 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보가 사생활 침해 또는 명예훼손 등 타인의 권리를 침해한다고 인정되면 임의로 임시조치를 할 수 있다.

② 제1항에 따른 임시조치에 관하여는 제44조의2제2항 후단, 제4항 후단 및 제5항을 준용한다.

[전문개정 2008.6.13]

제44조의4(자율규제) 정보통신서비스 제공자단체는 이용자를 보호하고 안전하며 신뢰할 수 있는 정보통신서비스를 제공하기 위하여 정보통신서비스 제공자 행동강령을 정하여 시행할 수 있다.

[전문개정 2008.6.13]

제44조의5(게시판 이용자의 본인 확인) ① 다음 각 호의 어느 하나에 해당하는 자가 게시판을 설치·운영하려면 그 게시판 이용자의 본인 확인을 위한 방법 및 절차의 마련 등 대통령령으로 정하는 필요한 조치(이하 "본인확인조치"라 한다)를 하여야 한다.

1. 국가기관, 지방자치단체, 「공공기관의 운영에 관한 법률」 제5조제3항에 따른 공기업·준정부기관 및 「지방공기업법」에 따른 지방공사·지방공단(이하 "공공기관등"이라 한다)
2. 삭제 <2014.5.28>

② 삭제 <2014.5.28>

③ 정부는 제1항에 따른 본인 확인을 위하여 안전하고 신뢰할 수 있는 시스템을 개발하기 위한 시책을 마련하여야 한다.

④ 공공기관등이 선량한 관리자의 주의로써 제1항에 따른 본인확인조치를 한 경우에는 이용자의 명의가 제3자에 의하여 부정사용됨에 따라 발생한 손해에 대한 배상책임을 줄이거나 면제받을 수 있다.<개정 2014.5.28>

[전문개정 2008.6.13]

[2014.5.28 법률 제12681호에 의하여 2012.8.23 헌법재판소에서 위헌 결정된 이 조 제1항 제2호를 삭제함.]

제44조의6(이용자 정보의 제공청구) ① 특정한 이용자에 의한 정보의 게재나 유통으로 사생활 침해 또는 명예훼손 등 권리를 침해당하였다고 주장하는 자는 민·형사상의 소를 제기하기 위하여 침해사실을 소명하여 제44조의10에 따른 명예훼손 분쟁조정부에 해당 정보통신서비스 제공자가 보유하고 있는 해당 이용자의 정보(민·형사상의 소를 제기하기 위한 성명·주소 등 대통령령으로 정하는 최소한의 정보를 말한다)를 제공하도록 청구할 수 있다.

② 명예훼손 분쟁조정부는 제1항에 따른 청구를 받으면 해당 이용자와 연락할 수 없는 등의 특별한 사정이 있는 경우 외에는 그 이용자의 의견을 들어 정보제공 여부를 결정하여야 한다.

③ 제1항에 따라 해당 이용자의 정보를 제공받은 자는 해당 이용자의 정보를 민·형사상의 소를 제기하기 위한 목적 외의 목적으로 사용하여서는 아니 된다.

④ 그 밖의 이용자 정보 제공청구의 내용과 절차에 필요한 사항은 대통령령으로 정한다.

[전문개정 2008.6.13]

제44조의7(불법정보의 유통금지 등) ① 누구든지 정보통신망을 통하여 다음 각 호의 어느 하나에 해당하는 정보를 유통하여서는 아니 된다. <개정 2011.9.15, 2016.3.22>

1. 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보
2. 사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인의 명예를 훼손하는 내용의 정보
3. 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 내용의 정보
4. 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해하는 내용의 정보
5. 「청소년 보호법」에 따른 청소년유해매체물로서 상대방의 연령 확인, 표시의무 등 법령에 따른 의무를 이행하지 아니하고 영리를 목적으로 제공하는 내용의 정보
6. 법령에 따라 금지되는 사행행위에 해당하는 내용의 정보

6의2. 이 법 또는 개인정보 보호에 관한 법령을 위반하여 개인정보를 거래하는 내용의 정보

7. 법령에 따라 분류된 비밀 등 국가기밀을 누설하는 내용의 정보
8. 「국가보안법」에서 금지하는 행위를 수행하는 내용의 정보
9. 그 밖에 범죄를 목적으로 하거나 교사(敎唆) 또는 방조하는 내용의 정보

② 방송통신위원회는 제1항제1호부터 제6호까지 및 제6호의2의 정보에 대하여는 심의위원회의 심의를 거쳐 정보통신서비스 제공자 또는 게시판 관리·운영자로 하여금 그 처리를 거부·정지 또는 제한하도록 명할 수 있다. 다만, 제1항제2호 및 제3호에 따른 정보의 경우에는 해당 정보로 인하여 피해를 받은 자가 구체적으로 밝힌 의사에 반하여 그 처리의 거부·정지 또는 제한을 명할 수 없다.<개정 2016.3.22>

③ 방송통신위원회는 제1항제7호부터 제9호까지의 정보가 다음 각 호의 모두에 해당하는 경우에는 정보통신서비스 제공자 또는 게시판 관리·운영자에게 해당 정보의 처리를 거부·정지 또는 제한하도록 명하여야 한다.<개정 2016.3.22>

1. 관계 중앙행정기관의 장의 요청이 있었을 것
2. 제1호의 요청을 받은 날부터 7일 이내에 심의위원회의 심의를 거친 후 「방송통신위원회의 설치 및 운영에 관한 법률」제21조제4호에 따른 시정 요구를 하였을 것
3. 정보통신서비스 제공자나 게시판 관리·운영자가 시정 요구에 따르지 아니하였을 것

④ 방송통신위원회는 제2항 및 제3항에 따른 명령의 대상이 되는 정보통신서비스 제공자, 게시판 관리·운영자 또는 해당 이용자에게 미리 의견제출의 기회를 주어야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 의견제출의 기회를 주지 아니할 수 있다.

1. 공공의 안전 또는 복리를 위하여 긴급히 처분을 할 필요가 있는 경우
2. 의견청취가 뚜렷이 곤란하거나 명백히 불필요한 경우로서 대통령령으로 정하는 경우
3. 의견제출의 기회를 포기한다는 뜻을 명백히 표시한 경우

[전문개정 2008.6.13]

제44조의8 삭제 <2008.2.29>

제44조의9 삭제 <2008.2.29>

제44조의10(명예훼손 분쟁조정부) ① 심의위원회는 정보통신망을 통하여 유통되는 정보 중 사생활의 침해 또는 명예훼손 등 타인의 권리를 침해하는 정보와 관련된 분쟁의 조정업무를 효율적으로 수행하기 위하여 5명 이하의 위원으로 구성된 명예훼손 분쟁조정부를 두되, 그중 1명 이상은 변호사의 자격이 있는 자로 한다.

② 명예훼손 분쟁조정부의 위원은 심의위원회의 위원장이 심의위원회의 동의를 받아 위촉한다.

③ 명예훼손 분쟁조정부의 분쟁조정절차 등에 관하여는 제33조의2제2항, 제35조부터 제39조까지의 규정을 준용한다. 이 경우 "분쟁조정위원회"는 "심의위원회"로, "개인정보와 관련한 분쟁"은 "정보통신망을 통하여 유통되는 정보 중 사생활의 침해 또는 명예훼손 등 타인의 권리를 침해하는 정보와 관련된 분쟁"으로 본다.

④ 명예훼손 분쟁조정부의 설치·운영 및 분쟁조정 등에 관하여 그 밖의 필요한 사항은 대통령령으로 정한다.

[전문개정 2008.6.13]

제6장 정보통신망의 안정성 확보 등

제45조(정보통신망의 안정성 확보 등) ① 정보통신서비스 제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다.

② 미래창조과학부장관은 제1항에 따른 보호조치의 구체적 내용을 정한 정보보호조치에 관한 지침(이하 "정보보호지침"이라 한다)을 정하여 고시하고 정보통신서비스 제공자에게 이를 지키도록 권고할 수 있다.<개정 2012.2.17, 2013.3.23>

③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다.<개정 2016.3.22>

1. 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치
2. 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치
3. 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치
4. 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치

[전문개정 2008.6.13]

제45조의2(정보보호 사전점검) ① 정보통신서비스 제공자는 새로이 정보통신망을 구축하거나 정보통신서비스를 제공하고자 하는 때에는 그 계획 또는 설계에 정보보호에 관한 사항을 고려하여야 한다.

② 미래창조과학부장관은 다음 각 호의 어느 하나에 해당하는 정보통신서비스 또는 전기통신사업을 시행하고자 하는 자에게 대통령령으로 정하는 정보보호 사전점검기준에 따라 보호조치를 하도록 권고할 수 있다.<개정 2013.3.23>

1. 이 법 또는 다른 법령에 따라 미래창조과학부장관의 인가·허가를 받거나 등록·신고를 하도록 되어 있는 사업으로서 대통령령으로 정하는 정보통신서비스 또는 전기통신사업
2. 미래창조과학부장관이 사업비의 전부 또는 일부를 지원하는 사업으로서 대통령령으로 정하는 정보통신서비스 또는 전기통신사업

③ 제2항에 따른 정보보호 사전점검의 기준·방법·절차·수수료 등 필요한 사항은 대통령령으로 정한다.

[본조신설 2012.2.17]

제45조의3(정보보호 최고책임자의 지정 등) ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정할 수 있다. 다만, 종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하고 미래창조과학부장관에게 신고하여야 한다.<개정 2014.5.28>

② 제1항에 따른 신고의 방법 및 절차 등에 대해서는 대통령령으로 정한다.<신설 2014.5.28>

③ 정보보호 최고책임자는 다음 각 호의 업무를 총괄한다.<개정 2014.5.28>

1. 정보보호관리체계의 수립 및 관리·운영
2. 정보보호 취약점 분석·평가 및 개선
3. 침해사고의 예방 및 대응
4. 사전 정보보호대책 마련 및 보안조치 설계·구현 등
5. 정보보호 사전 보안성 검토
6. 중요 정보의 암호화 및 보안서버 적합성 검토
7. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

④ 정보통신서비스 제공자는 침해사고에 대한 공동 예방 및 대응, 필요한 정보의 교류, 그 밖에 대통령령으로 정하는 공동의 사업을 수행하기 위하여 제1항에 따른 정보보호 최고책임자를 구성원으로 하는 정보보호 최고책임자 협의회를 구성·운영할 수 있다.<개정 2014.5.28>

⑤ 정부는 제4항에 따른 정보보호 최고책임자 협의회의 활동에 필요한 경비의 전부 또는 일부를 지원할 수 있다.<개정 2014.5.28, 2015.6.22>

[본조신설 2012.2.17]

제46조(집적된 정보통신시설의 보호) ① 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자(이하 "집적정보통신시설 사업자"라 한다)는 정보통신시설을 안정적으로 운영하기 위하여 대통령령으로 정하는 바에 따른 보호조치를 하여야 한다.

② 집적정보통신시설 사업자는 집적된 정보통신시설의 멸실, 훼손, 그 밖의 운영장애로 발생한 피해를 보상하기 위하여 대통령령으로 정하는 바에 따라 보험에 가입하여야 한다.

[전문개정 2008.6.13]

제46조의2(집적정보통신시설 사업자의 긴급대응) ① 집적정보통신시설 사업자는 다음 각 호의 어느 하나에 해당하는 경우에는 이용약관으로 정하는 바에 따라 해당 서비스의 전부 또는 일부의 제공을 중단할 수 있다. <개정 2009.4.22, 2013.3.23>

1. 집적정보통신시설을 이용하는 자(이하 "시설이용자"라 한다)의 정보시스템에서 발생한 이상현상으로 다른 시설이용자의 정보통신망 또는 집적된 정보통신시설의 정보통신망에 심각한 장애를 발생시킬 우려가 있다고 판단되는 경우
2. 외부에서 발생한 침해사고로 집적된 정보통신시설에 심각한 장애가 발생할 우려가 있다고 판단되는 경우
3. 중대한 침해사고가 발생하여 미래창조과학부장관이나 한국인터넷진흥원이 요청하는 경우

② 집적정보통신시설 사업자는 제1항에 따라 해당 서비스의 제공을 중단하는 경우에는 중단사유, 발생일시, 기간 및 내용 등을 구체적으로 밝혀 시설이용자에게 즉시 알려야 한다.

③ 집적정보통신시설 사업자는 중단사유가 없어지면 즉시 해당 서비스의 제공을 재개하여야 한다.

[전문개정 2008.6.13]

제46조의3 삭제 <2012.2.17>

제47조(정보보호 관리체계의 인증) ① 미래창조과학부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립·운영하고 있는 자에 대하여 제4항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다. <개정 2012.2.17, 2013.3.23, 2015.12.1>

② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.<신설 2012.2.17, 2015.12.1>

1. 「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자
2. 집적정보통신시설 사업자
3. 연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 3개월간의 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

③ 미래창조과학부장관은 제2항에 따라 인증을 받아야 하는 자가 미래창조과학부령으로 정하는 바에 따라 국제표준 정보보호 인증을 받거나 정보보호 조치를 취한 경우에는 제1항에 따른 인증 심사의 일부를 생략할 수 있다. 이 경우 인증 심사의 세부 생략 범위에 대해서는 미래창조과학부장관이 정하여 고시한다.<신설 2015.12.1>

④ 미래창조과학부장관은 제1항에 따른 정보보호 관리체계 인증을 위하여 관리적·기술적·물리적 보호대책을 포함한 인증기준 등 그 밖에 필요한 사항을 정하여 고시할 수 있다.<개정 2012.2.17, 2013.3.23, 2015.12.1>

⑤ 제1항에 따른 정보보호 관리체계 인증의 유효기간은 3년으로 한다. 다만, 제47조의5제1항에 따라 정보보호 관리등급을 받은 경우 그 유효기간 동안 제1항의 인증을 받은 것으로 본다.<신설 2012.2.17, 2015.12.1>

⑥ 미래창조과학부장관은 한국인터넷진흥원 또는 미래창조과학부장관이 지정한 기관(이하 "정보보호 관리체계 인증기관"이라 한다)으로 하여금 제1항 및 제2항에 따른 인증에 관한 업무로서 다음 각 호의 업무를 수행하게 할 수 있다.<신설 2012.2.17, 2013.3.23, 2015.12.1>

1. 인증 신청인이 수립한 정보보호 관리체계가 제4항에 따른 인증기준에 적합한지 여부를 확인하기 위한 심사(이하 "인증심사"라 한다)
2. 인증심사 결과의 심의
3. 인증서 발급·관리
4. 인증의 사후관리
5. 정보보호 관리체계 인증심사원의 양성 및 자격관리
6. 그 밖에 정보보호 관리체계 인증에 관한 업무

⑦ 미래창조과학부장관은 인증에 관한 업무를 효율적으로 수행하기 위하여 필요한 경우 인증심사 업무를 수행하는 기관(이하 "정보보호 관리체계 심사기관"이라 한다)을 지정할 수 있다.<신설 2015.12.1>

⑧ 한국인터넷진흥원, 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관은 정보보호 관리체계의 실효성 제고를 위하여 연 1회 이상 사후관리를 실시하고 그 결과를 미래창조과학부장관에게 통보하여야 한다.<신설 2012.2.17, 2013.3.23, 2015.12.1>

⑨ 제1항 및 제2항에 따라 정보보호 관리체계의 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다.<개정 2012.2.17, 2015.12.1>

⑩ 미래창조과학부장관은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 경우에는 인증을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 인증을 취소하여야 한다.<신설 2012.2.17, 2013.3.23, 2015.12.1>

1. 거짓이나 그 밖의 부정한 방법으로 정보보호 관리체계 인증을 받은 경우
2. 제4항에 따른 인증기준에 미달하게 된 경우
3. 제8항에 따른 사후관리를 거부 또는 방해한 경우

⑪ 제1항 및 제2항에 따른 인증의 방법·절차·범위·수수료, 제8항에 따른 사후관리의 방법·절차, 제10항에 따른 인증취소의 방법·절차, 그 밖에 필요한 사항은 대통령령으로 정한다.

<개정 2012.2.17, 2015.12.1>

⑫ 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관 지정의 기준、절차、유효기간 등에 필요한 사항은 대통령령으로 정한다.<개정 2012.2.17, 2015.12.1>

[전문개정 2008.6.13]

제47조의2(정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관의 지정취소 등) ① 미래창조과학부장관은 제47조에 따라 정보보호 관리체계 인증기관 또는 정보보호 관리체계 심사기관으로 지정받은 법인 또는 단체가 다음 각 호의 어느 하나에 해당하면 그 지정을 취소하거나 1년 이내의 기간을 정하여 해당 업무의 전부 또는 일부의 정지를 명할 수 있다. 다만, 제1호나 제2호에 해당하는 경우에는 그 지정을 취소하여야 한다. <개정 2012.2.17, 2013.3.23, 2015.12.1>

1. 거짓이나 그 밖의 부정한 방법으로 정보보호 관리체계 인증기관 또는 정보보호 관리체계 심사기관의 지정을 받은 경우
2. 업무정지기간 중에 인증 또는 인증심사를 한 경우
3. 정당한 사유 없이 인증 또는 인증심사를 하지 아니한 경우
4. 제47조제11항을 위반하여 인증 또는 인증심사를 한 경우
5. 제47조제12항에 따른 지정기준에 적합하지 아니하게 된 경우

② 제1항에 따른 지정취소 및 업무정지 등에 필요한 사항은 대통령령으로 정한다.

[전문개정 2008.6.13]

[제목개정 2015.12.1]

제47조의3(개인정보보호 관리체계의 인증) ① 방송통신위원회는 정보통신망에서 개인정보보호 활동을 체계적이고 지속적으로 수행하기 위하여 필요한 관리적、기술적、물리적 보호조치를 포함한 종합적 관리체계(이하 "개인정보보호 관리체계"라 한다)를 수립、운영하고 있는 자에 대하여 제2항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.

② 방송통신위원회는 제1항에 따른 개인정보보호 관리체계 인증을 위하여 관리적、기술적、물리적 보호대책을 포함한 인증기준 등 그 밖에 필요한 사항을 정하여 고시할 수 있다.

③ 개인정보보호 관리체계의 수행기관, 사후관리 등에 대하여는 제47조제6항부터 제12항까지의 규정을 준용한다. 이 경우 "제1항 및 제2항"은 "제1항"으로 본다.<개정 2015.12.1>

④ 개인정보보호 관리체계 인증기관의 지정취소 등에 대하여는 제47조의2를 준용한다.

[본조신설 2012.2.17]

[종전 제47조의3은 제47조의4로 이동 <2012.2.17>]

제47조의4(이용자의 정보보호) ① 정부는 이용자의 정보보호에 필요한 기준을 정하여 이용자에게 권고하고, 침해사고의 예방 및 확산 방지를 위하여 취약점 점검, 기술 지원 등 필요한 조치를 할 수 있다.

② 주요정보통신서비스 제공자는 정보통신망에 중대한 침해사고가 발생하여 자신의 서비스를 이용하는 이용자의 정보시스템 또는 정보통신망 등에 심각한 장애가 발생할 가능성이 있으면

이용약관으로 정하는 바에 따라 그 이용자에게 보호조치를 취하도록 요청하고, 이를 이행하지 아니하는 경우에는 해당 정보통신망으로의 접속을 일시적으로 제한할 수 있다.

③ 「소프트웨어산업 진흥법」 제2조에 따른 소프트웨어사업자는 보안에 관한 취약점을 보완하는 프로그램을 제작하였을 때에는 한국인터넷진흥원에 알려야 하고, 그 소프트웨어 사용자에게는 제작한 날부터 1개월 이내에 2회 이상 알려야 한다.<개정 2009.4.22>

④ 제2항에 따른 보호조치의 요청 등에 관하여 이용약관으로 정하여야 하는 구체적인 사항은 대통령령으로 정한다.

[전문개정 2008.6.13]

[제47조의3에서 이동 <2012.2.17>]

제47조의5(정보보호 관리등급 부여) ① 제47조에 따라 정보보호 관리체계 인증을 받은 자는 기업의 통합적 정보보호 관리수준을 제고하고 이용자로부터 정보보호 서비스에 대한 신뢰를 확보하기 위하여 미래창조과학부장관으로부터 정보보호 관리등급을 받을 수 있다. <개정 2013.3.23>

② 미래창조과학부장관은 한국인터넷진흥원으로 하여금 제1항에 따른 등급 부여에 관한 업무를 수행하게 할 수 있다.<개정 2013.3.23>

③ 제1항에 따라 정보보호 관리등급을 받은 자는 대통령령으로 정하는 바에 따라 해당 등급의 내용을 표시하거나 홍보에 활용할 수 있다.

④ 미래창조과학부장관은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 경우에는 부여한 등급을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 부여한 등급을 취소하여야 한다.<개정 2013.3.23, 2015.12.1>

1. 거짓이나 그 밖의 부정한 방법으로 정보보호 관리등급을 받은 경우
2. 제5항에 따른 등급기준에 미달하게 된 경우

⑤ 제1항에 따른 등급 부여의 심사기준 및 등급 부여의 방법·절차·수수료, 등급의 유효기간, 제4항에 따른 등급취소의 방법·절차, 그 밖에 필요한 사항은 대통령령으로 정한다.

[본조신설 2012.2.17]

제48조(정보통신망 침해행위 등의 금지) ① 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다.

② 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램(이하 "악성프로그램"이라 한다)을 전달 또는 유포하여서는 아니 된다.

③ 누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게 하여서는 아니 된다.

[전문개정 2008.6.13]

제48조의2(침해사고의 대응 등) ① 미래창조과학부장관은 침해사고에 적절히 대응하기 위하여 다음 각 호의 업무를 수행하고, 필요하면 업무의 전부 또는 일부를 한국인터넷진흥원이 수행하도록 할 수 있다. <개정 2009.4.22, 2013.3.23>

1. 침해사고에 관한 정보의 수집·전파
2. 침해사고의 예보·경보
3. 침해사고에 대한 긴급조치
4. 그 밖에 대통령령으로 정하는 침해사고 대응조치

② 다음 각 호의 어느 하나에 해당하는 자는 대통령령으로 정하는 바에 따라 침해사고의 유형별 통계, 해당 정보통신망의 소통량 통계 및 접속경로별 이용 통계 등 침해사고 관련 정보를 미래창조과학부장관이나 한국인터넷진흥원에 제공하여야 한다.<개정 2009.4.22, 2013.3.23>

1. 주요정보통신서비스 제공자
2. 집적정보통신시설 사업자
3. 그 밖에 정보통신망을 운영하는 자로서 대통령령으로 정하는 자

③ 한국인터넷진흥원은 제2항에 따른 정보를 분석하여 미래창조과학부장관에게 보고하여야 한다.<개정 2009.4.22, 2013.3.23>

④ 미래창조과학부장관은 제2항에 따라 정보를 제공하여야 하는 사업자가 정당한 사유 없이 정보의 제공을 거부하거나 거짓 정보를 제공하면 상당한 기간을 정하여 그 사업자에게 시정을 명할 수 있다.<개정 2013.3.23>

⑤ 미래창조과학부장관이나 한국인터넷진흥원은 제2항에 따라 제공받은 정보를 침해사고의 대응을 위하여 필요한 범위에서만 정당하게 사용하여야 한다.<개정 2009.4.22, 2013.3.23>

⑥ 미래창조과학부장관이나 한국인터넷진흥원은 침해사고의 대응을 위하여 필요하면 제2항 각 호의 어느 하나에 해당하는 자에게 인력지원을 요청할 수 있다.<개정 2009.4.22, 2013.3.23>

[전문개정 2008.6.13]

제48조의3(침해사고의 신고 등) ① 다음 각 호의 어느 하나에 해당하는 자는 침해사고가 발생하면 즉시 그 사실을 미래창조과학부장관이나 한국인터넷진흥원에 신고하여야 한다. 이 경우 「정보통신기반 보호법」 제13조제1항에 따른 통지가 있으면 전단에 따른 신고를 한 것으로 본다. <개정 2009.4.22, 2013.3.23>

1. 정보통신서비스 제공자
2. 집적정보통신시설 사업자

② 미래창조과학부장관이나 한국인터넷진흥원은 제1항에 따라 침해사고의 신고를 받거나 침해사고를 알게 되면 제48조의2제1항 각 호에 따른 필요한 조치를 하여야 한다.<개정 2009.4.22, 2013.3.23>

[전문개정 2008.6.13]

제48조의4(침해사고의 원인 분석 등) ① 정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하면 침해사고의 원인을 분석하고 피해의 확산을 방지하여야 한다.

② 미래창조과학부장관은 정보통신서비스 제공자의 정보통신망에 중대한 침해사고가 발생하면 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위하여 정보보호에 전문성을 갖춘 민·관합동조사단을 구성하여 그 침해사고의 원인 분석을 할 수 있다.<개정 2013.3.23>
③ 미래창조과학부장관은 제2항에 따른 침해사고의 원인을 분석하기 위하여 필요하다고 인정하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 정보통신망의 접속기록 등 관련 자료의 보전을 명할 수 있다.<개정 2013.3.23>
④ 미래창조과학부장관은 침해사고의 원인을 분석하기 위하여 필요하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 침해사고 관련 자료의 제출을 요구할 수 있으며, 제2항에 따른 민·관합동조사단에게 관계인의 사업장에 출입하여 침해사고 원인을 조사하도록 할 수 있다. 다만, 「통신비밀보호법」 제2조제11호에 따른 통신사실확인자료에 해당하는 자료의 제출은 같은 법으로 정하는 바에 따른다.<개정 2013.3.23>
⑤ 미래창조과학부장관이나 민·관합동조사단은 제4항에 따라 제출받은 자료와 조사를 통하여 알게 된 정보를 침해사고의 원인 분석 및 대책 마련 외의 목적으로는 사용하지 못하며, 원인 분석이 끝난 후에는 즉시 파기하여야 한다.<개정 2013.3.23>
⑥ 제2항에 따른 민·관합동조사단의 구성과 제4항에 따라 제출된 침해사고 관련 자료의 보호 등에 필요한 사항은 대통령령으로 정한다.
[전문개정 2008.6.13]

제49조(비밀 등의 보호) 누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다.
[전문개정 2008.6.13]

제49조의2(속이는 행위에 의한 개인정보의 수집금지 등) ① 누구든지 정보통신망을 통하여 속이는 행위로 다른 사람의 정보를 수집하거나 다른 사람이 정보를 제공하도록 유인하여서는 아니 된다.
② 정보통신서비스 제공자는 제1항을 위반한 사실을 발견하면 즉시 미래창조과학부장관, 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다.<개정 2009.4.22, 2016.3.22>
③ 미래창조과학부장관, 방송통신위원회 또는 한국인터넷진흥원은 제2항에 따른 신고를 받거나 제1항을 위반한 사실을 알게 되면 다음 각 호의 필요한 조치를 하여야 한다.<개정 2009.4.22, 2016.3.22>
1. 위반 사실에 관한 정보의 수집·전파
2. 유사 피해에 대한 예보·경보
3. 정보통신서비스 제공자에게 접속경로의 차단을 요청하거나 이용자에게 제1항의 위반행위에 노출되었다는 사실을 알리도록 요청하는 등 피해 예방 및 피해 확산을 방지하기 위한 긴급조치
④ 미래창조과학부장관 또는 방송통신위원회는 제3항제3호의 조치를 취하기 위하여 정보통신서비스 제공자에게 정보통신서비스 제공자 간 정보통신망을 통하여 속이는 행위에 대한 정보

공유 등 필요한 조치를 취하도록 명할 수 있다.<신설 2016.3.22>

[전문개정 2008.6.13]

제50조(영리목적의 광고성 정보 전송 제한) ① 누구든지 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하려면 그 수신자의 명시적인 사전 동의를 받아야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 사전 동의를 받지 아니한다. <개정 2016.3.22>

1. 재화등의 거래관계를 통하여 수신자로부터 직접 연락처를 수집한 자가 대통령령으로 정한 기간 이내에 자신이 처리하고 수신자와 거래한 것과 동종의 재화등에 대한 영리목적의 광고성 정보를 전송하려는 경우
2. 「방문판매 등에 관한 법률」에 따른 전화권유판매자가 육성으로 수신자에게 개인정보의 수집출처를 고지하고 전화권유를 하는 경우

② 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하려는 자는 제1항에도 불구하고 수신자가 수신거부의사를 표시하거나 사전 동의를 철회한 경우에는 영리목적의 광고성 정보를 전송하여서는 아니 된다.

③ 오후 9시부터 그 다음 날 오전 8시까지의 시간에 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하려는 자는 제1항에도 불구하고 그 수신자로부터 별도의 사전 동의를 받아야 한다. 다만, 대통령령으로 정하는 매체의 경우에는 그러하지 아니하다.

④ 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 자는 대통령령으로 정하는 바에 따라 다음 각 호의 사항 등을 광고성 정보에 구체적으로 밝혀야 한다.

1. 전송자의 명칭 및 연락처
2. 수신의 거부 또는 수신동의의 철회 의사표시를 쉽게 할 수 있는 조치 및 방법에 관한 사항

⑤ 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 자는 다음 각 호의 어느 하나에 해당하는 조치를 하여서는 아니 된다.

1. 광고성 정보 수신자의 수신거부 또는 수신동의의 철회를 회피·방해하는 조치
2. 숫자·부호 또는 문자를 조합하여 전화번호·전자우편주소 등 수신자의 연락처를 자동으로 만들어 내는 조치
3. 영리목적의 광고성 정보를 전송할 목적으로 전화번호 또는 전자우편주소를 자동으로 등록하는 조치
4. 광고성 정보 전송자의 신원이나 광고 전송 출처를 감추기 위한 각종 조치
5. 영리목적의 광고성 정보를 전송할 목적으로 수신자를 기망하여 회신을 유도하는 각종 조치

⑥ 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 자는 수신자가 수신거부나 수신동의의 철회를 할 때 발생하는 전화요금 등의 금전적 비용을 수신자가 부담하지 아니하도록 대통령령으로 정하는 바에 따라 필요한 조치를 하여야 한다.

⑦ 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하려는 자는 수신자가 제1항에 따른 사전 동의, 제2항에 따른 수신거부의사 또는 수신동의 철회 의사를 표시할 때에는 해당 수신자에게 대통령령으로 정하는 바에 따라 수신동의, 수신거부 또는 수신동의 철회에 대한 처리 결과를 알려야 한다.

⑧ 제1항 또는 제3항에 따라 수신동의를 받은 자는 대통령령으로 정하는 바에 따라 정기적으로 광고성 정보 수신자의 수신동의 여부를 확인하여야 한다.

[전문개정 2014.5.28]

제50조의2 삭제 <2014.5.28>

제50조의3(영리목적의 광고성 정보 전송의 위탁 등) ① 영리목적의 광고성 정보의 전송을 타인에게 위탁한 자는 그 업무를 위탁받은 자가 제50조를 위반하지 아니하도록 관리·감독하여야 한다. <개정 2014.5.28>

② 제1항에 따라 영리목적의 광고성 정보의 전송을 위탁받은 자는 그 업무와 관련한 법을 위반하여 발생한 손해의 배상책임에 있어 정보 전송을 위탁한 자의 소속 직원으로 본다.

[전문개정 2008.6.13]

제50조의4(정보 전송 역무 제공 등의 제한) ① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우에 해당 역무의 제공을 거부하는 조치를 할 수 있다.

1. 광고성 정보의 전송 또는 수신으로 역무의 제공에 장애가 일어나거나 일어날 우려가 있는 경우
2. 이용자가 광고성 정보의 수신을 원하지 아니하는 경우
3. 삭제 <2014.5.28>

② 정보통신서비스 제공자는 제1항 또는 제4항에 따른 거부조치를 하려면 해당 역무 제공의 거부에 관한 사항을 그 역무의 이용자와 체결하는 정보통신서비스 이용계약의 내용에 포함하여야 한다.<개정 2014.5.28>

③ 정보통신서비스 제공자는 제1항 또는 제4항에 따른 거부조치 사실을 그 역무를 제공받는 이용자 등 이해관계인에게 알려야 한다. 다만, 미리 알리는 것이 곤란한 경우에는 거부조치를 한 후 지체 없이 알려야 한다.<개정 2014.5.28>

④ 정보통신서비스 제공자는 이용계약을 통하여 해당 정보통신서비스 제공자가 이용자에게 제공하는 서비스가 제50조 또는 제50조의8을 위반하여 영리목적의 광고성 정보전송에 이용되고 있는 경우 해당 역무의 제공을 거부하거나 정보통신망이나 서비스의 취약점을 개선하는 등 필요한 조치를 강구하여야 한다.<신설 2014.5.28>

[전문개정 2008.6.13]

제50조의5(영리목적의 광고성 프로그램 등의 설치) 정보통신서비스 제공자는 영리목적의 광고성 정보가 보이도록 하거나 개인정보를 수집하는 프로그램을 이용자의 컴퓨터나 그 밖에 대통령령으로 정하는 정보처리장치에 설치하려면 이용자의 동의를 받아야 한다. 이 경우 해당 프로그램의 용도와 삭제방법을 고지하여야 한다.

[전문개정 2008.6.13]

제50조의6(영리목적의 광고성 정보 전송차단 소프트웨어의 보급 등) ① 방송통신위원회는 수신자가 제50조를 위반하여 전송되는 영리목적의 광고성 정보를 편리하게 차단하거나 신고할 수

있는 소프트웨어나 컴퓨터프로그램을 개발하여 보급할 수 있다.
② 방송통신위원회는 제1항에 따른 전송차단, 신고 소프트웨어 또는 컴퓨터프로그램의 개발과 보급을 촉진하기 위하여 관련 공공기관、법인、단체 등에 필요한 지원을 할 수 있다.
③ 방송통신위원회는 정보통신서비스 제공자의 전기통신역무가 제50조를 위반하여 발송되는 영리목적의 광고성 정보 전송에 이용되면 수신자 보호를 위하여 기술개발、교육、홍보 등 필요한 조치를 할 것을 정보통신서비스 제공자에게 권고할 수 있다.
④ 제1항에 따른 개발、보급의 방법과 제2항에 따른 지원에 필요한 사항은 대통령령으로 정한다.
[전문개정 2008.6.13]

제50조의7(영리목적의 광고성 정보 게시의 제한) ① 누구든지 영리목적의 광고성 정보를 인터넷 홈페이지에 게시하려면 인터넷 홈페이지 운영자 또는 관리자의 사전 동의를 받아야 한다. 다만, 별도의 권한 없이 누구든지 쉽게 접근하여 글을 게시할 수 있는 게시판의 경우에는 사전 동의를 받지 아니한다.
② 영리목적의 광고성 정보를 게시하려는 자는 제1항에도 불구하고 인터넷 홈페이지 운영자 또는 관리자가 명시적으로 게시 거부의사를 표시하거나 사전 동의를 철회한 경우에는 영리목적의 광고성 정보를 게시하여서는 아니 된다.
③ 인터넷 홈페이지 운영자 또는 관리자는 제1항 또는 제2항을 위반하여 게시된 영리목적의 광고성 정보를 삭제하는 등의 조치를 할 수 있다.
[전문개정 2014.5.28]

제50조의8(불법행위를 위한 광고성 정보 전송금지) 누구든지 정보통신망을 이용하여 이 법 또는 다른 법률에서 금지하는 재화 또는 서비스에 대한 광고성 정보를 전송하여서는 아니 된다.
[전문개정 2008.6.13]

제51조(중요 정보의 국외유출 제한 등) ① 정부는 국내의 산업、경제 및 과학기술 등에 관한 중요 정보가 정보통신망을 통하여 국외로 유출되는 것을 방지하기 위하여 정보통신서비스 제공자 또는 이용자에게 필요한 조치를 하도록 할 수 있다.
② 제1항에 따른 중요 정보의 범위는 다음 각 호와 같다.
1. 국가안전보장과 관련된 보안정보 및 주요 정책에 관한 정보
2. 국내에서 개발된 첨단과학 기술 또는 기기의 내용에 관한 정보
③ 정부는 제2항 각 호에 따른 정보를 처리하는 정보통신서비스 제공자에게 다음 각 호의 조치를 하도록 할 수 있다.<개정 2016.3.22>
1. 정보통신망의 부당한 이용을 방지할 수 있는 제도적、기술적 장치의 설정
2. 정보의 불법파괴 또는 불법조작을 방지할 수 있는 제도적、기술적 조치
3. 정보통신서비스 제공자가 처리 중 알게 된 중요 정보의 유출을 방지할 수 있는 조치
[전문개정 2008.6.13]

제52조(한국인터넷진흥원) ① 정부는 정보통신망의 고도화(정보통신망의 구축·개선 및 관리에 관한 사항을 제외한다)와 안전한 이용 촉진 및 방송통신과 관련한 국제협력·국외진출 지원을 효율적으로 추진하기 위하여 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다)을 설립한다. <개정 2009.4.22>

② 인터넷진흥원은 법인으로 한다.<개정 2009.4.22>

③ 인터넷진흥원은 다음 각 호의 사업을 한다.<개정 2009.4.22, 2012.2.17, 2013.3.23, 2014.11.19, 2015.6.22>

1. 정보통신망의 이용 및 보호, 방송통신과 관련한 국제협력·국외진출 등을 위한 법·정책 및 제도의 조사·연구
2. 정보통신망의 이용 및 보호와 관련한 통계의 조사·분석
3. 정보통신망의 이용에 따른 역기능 분석 및 대책 연구
4. 정보통신망의 이용 및 보호를 위한 홍보 및 교육·훈련
5. 정보통신망의 정보보호 및 인터넷주소자원 관련 기술 개발 및 표준화
6. 정보보호산업 정책 지원 및 관련 기술 개발과 인력양성
7. 정보보호 관리체계의 인증, 정보보호시스템 평가·인증 등 정보보호 인증·평가 등의 실시 및 지원
8. 개인정보보호를 위한 대책의 연구 및 보호기술의 개발·보급 지원
9. 분쟁조정위원회의 운영 지원과 개인정보침해 신고센터의 운영
10. 광고성 정보 전송 및 인터넷광고와 관련한 고충의 상담·처리
11. 정보통신망 침해사고의 처리·원인분석 및 대응체계 운영
12. 「전자서명법」 제25조제1항에 따른 전자서명인증관리
13. 인터넷의 효율적 운영과 이용활성화를 위한 지원
14. 인터넷 이용자의 저장 정보 보호 지원
15. 인터넷 관련 서비스정책 지원
16. 인터넷상에서의 이용자 보호 및 건전 정보 유통 확산 지원
17. 「인터넷주소자원에 관한 법률」에 따른 인터넷주소자원의 관리에 관한 업무
18. 「인터넷주소자원에 관한 법률」 제16조에 따른 인터넷주소분쟁조정위원회의 운영 지원
19. 「정보보호산업의 진흥에 관한 법률」 제25조제7항에 따른 조정위원회의 운영지원
20. 방송통신과 관련한 국제협력·국외진출 및 국외홍보 지원
21. 제1호부터 제20호까지의 사업에 부수되는 사업
22. 그 밖에 이 법 또는 다른 법령에 따라 인터넷진흥원의 업무로 정하거나 위탁한 사업이나 미래창조과학부장관·행정자치부장관·방송통신위원회 또는 다른 행정기관의 장으로부터 위탁받은 사업

④ 인터넷진흥원이 사업을 수행하는 데 필요한 경비는 다음 각 호의 재원으로 충당한다.<개정 2016.3.22>

1. 정부의 출연금
2. 제3항 각 호의 사업수행에 따른 수입금
3. 그 밖에 인터넷진흥원의 운영에 따른 수입금

⑤ 인터넷진흥원에 관하여 이 법에서 정하지 아니한 사항에 대하여는 「민법」의 재단법인에 관한 규정을 준용한다.<개정 2009.4.22>

⑥ 인터넷진흥원이 아닌 자는 한국인터넷진흥원의 명칭을 사용하지 못한다.<개정 2009.4.22>

⑦ 인터넷진흥원의 운영 및 업무수행에 필요한 사항은 대통령령으로 정한다.<개정 2009.4.22>

[전문개정 2008.6.13]

[제목개정 2009.4.22]

제7장 통신과금서비스 <신설 2007.12.21>

제53조(통신과금서비스제공자의 등록 등) ① 통신과금서비스를 제공하려는 자는 대통령령으로 정하는 바에 따라 다음 각 호의 사항을 갖추어 미래창조과학부장관에게 등록하여야 한다. <개정 2008.2.29, 2013.3.23>

1. 재무건전성
2. 통신과금서비스이용자보호계획
3. 업무를 수행할 수 있는 인력과 물적 설비
4. 사업계획서

② 제1항에 따라 등록할 수 있는 자는 「상법」 제170조에 따른 회사 또는 「민법」 제32조에 따른 법인으로서 자본금·출자총액 또는 기본재산이 5억원 이상의 범위에서 대통령령으로 정하는 금액 이상이어야 한다.

③ 통신과금서비스제공자는 「전기통신사업법」 제22조에도 불구하고 부가통신사업자의 신고를 하지 아니할 수 있다.<개정 2010.3.22>

④ 「전기통신사업법」 제23조부터 제26조까지의 규정은 통신과금서비스제공자의 등록사항의 변경, 사업의 양도·양수 또는 합병·상속, 사업의 승계, 사업의 휴지·폐지·해산 등에 준용한다. 이 경우 "별정통신사업자"는 "통신과금서비스제공자"로 보고, "별정통신사업"은 "통신과금서비스제공업"으로 본다.<개정 2010.3.22>

⑤ 제1항에 따른 등록의 세부요건, 절차, 그 밖에 필요한 사항은 대통령령으로 정한다.

[본조신설 2007.12.21]

[종전 제53조는 제62조로 이동 <2007.12.21>]

제54조(등록의 결격사유) 다음 각 호의 어느 하나에 해당하는 자는 제53조에 따른 등록을 할 수 없다. <개정 2008.2.29, 2013.3.23>

1. 제53조제4항에 따라 사업을 폐지한 날부터 1년이 지나지 아니한 법인 및 그 사업이 폐지될 당시 그 법인의 대주주(대통령령으로 정하는 출자자를 말한다. 이하 같다)이었던 자로서 그 폐지일부터 1년이 지나지 아니한 자

2. 제55조제1항에 따라 등록이 취소된 날부터 3년이 지나지 아니한 법인 및 그 취소 당시 그 법인의 대주주이었던 자로서 그 취소가 된 날부터 3년이 지나지 아니한 자
3. 「채무자 회생 및 파산에 관한 법률」에 따른 회생절차 중에 있는 법인 및 그 법인의 대주주
4. 금융거래 등 상거래에 있어서 약정한 기일 내에 채무를 변제하지 아니한 자로서 미래창조과학부장관이 정하는 자
5. 제1호부터 제4호까지의 규정에 해당하는 자가 대주주인 법인

[본조신설 2007.12.21]

[종전 제54조는 제63조로 이동 <2007.12.21>]

제55조(등록의 취소명령) ① 미래창조과학부장관은 통신과금서비스제공자가 거짓이나 그 밖의 부정한 방법으로 등록을 한 때에는 등록을 취소하여야 한다. <개정 2015.6.22>

② 제1항에 따른 처분의 절차, 그 밖에 필요한 사항은 대통령령으로 정한다.<개정 2015.6.22>

[본조신설 2007.12.21]

[제목개정 2015.6.22]

[종전 제55조는 제64조로 이동 <2007.12.21>]

제56조(약관의 신고 등) ① 통신과금서비스제공자는 통신과금서비스에 관한 약관을 정하여 미래창조과학부장관에게 신고(변경신고를 포함한다)하여야 한다. <개정 2008.2.29, 2013.3.23>

② 미래창조과학부장관은 제1항에 따른 약관이 통신과금서비스이용자의 이익을 침해할 우려가 있다고 판단되는 경우에는 통신과금서비스제공자에게 약관의 변경을 권고할 수 있다.<개정 2008.2.29, 2013.3.23>

[본조신설 2007.12.21]

[종전 제56조는 제65조로 이동 <2007.12.21>]

제57조(통신과금서비스의 안전성 확보 등) ① 통신과금서비스제공자는 통신과금서비스가 안전하게 제공될 수 있도록 선량한 관리자로서의 주의의무를 다하여야 한다. <개정 2014.5.28>

② 통신과금서비스제공자는 통신과금서비스를 통한 거래의 안전성과 신뢰성을 확보하기 위하여 대통령령으로 정하는 바에 따라 업무처리지침의 제정 및 회계처리 구분 등의 관리적 조치와 정보보호시스템 구축 등의 기술적 조치를 하여야 한다.

[본조신설 2007.12.21]

[종전 제57조는 제66조로 이동 <2007.12.21>]

제58조(통신과금서비스이용자의 권리 등) ① 통신과금서비스제공자는 재화등의 판매·제공의 대가가 발생한 때 및 대가를 청구할 때에 통신과금서비스이용자에게 다음 각 호의 사항을 고지하여야 한다. <개정 2011.4.5, 2014.5.28>

1. 통신과금서비스 이용일시
2. 통신과금서비스를 통한 구매·이용의 거래 상대방(통신과금서비스를 이용하여 그 대가를 받고 재화 또는 용역을 판매·제공하는 자를 말한다. 이하 "거래 상대방"이라 한다)의 상호

와 연락처

3. 통신과금서비스를 통한 구매·이용 금액과 그 명세

4. 이의신청 방법 및 연락처

② 통신과금서비스제공자는 통신과금서비스이용자가 구매·이용 내역을 확인할 수 있는 방법을 제공하여야 하며, 통신과금서비스이용자가 구매·이용 내역에 관한 서면(전자문서를 포함한다. 이하 같다)을 요청하는 경우에는 그 요청을 받은 날부터 2주 이내에 이를 제공하여야 한다.

③ 통신과금서비스이용자는 통신과금서비스가 자신의 의사에 반하여 제공되었음을 안 때에는 통신과금서비스제공자에게 이에 대한 정정을 요구할 수 있으며(통신과금서비스이용자의 고의 또는 중과실이 있는 경우는 제외한다), 통신과금서비스제공자는 이용자의 정정요구가 이유 있을 경우 판매자에 대한 이용 대금의 지급을 유보하고 그 정정 요구를 받은 날부터 2주 이내에 처리 결과를 알려 주어야 한다.<개정 2014.5.28>

④ 통신과금서비스제공자는 통신과금서비스에 관한 기록을 5년 이내의 범위에서 대통령령으로 정하는 기간 동안 보존하여야 한다.

⑤ 통신과금서비스제공자(제2조제1항제10호가목의 업무를 제공하는 자)는 통신과금서비스를 제공하거나 이용한도액을 증액할 경우에는 미리 해당 통신과금서비스이용자의 동의를 받아야 한다.<신설 2014.5.28>

⑥ 통신과금서비스제공자(제2조제1항제10호가목의 업무를 제공하는 자)는 약관을 변경하는 때에는 변경되는 약관의 시행일 1개월 전에 이용자에게 통지하여야 한다. 이 경우 변경되는 약관에 대하여 이의가 있는 이용자는 통신과금서비스에 관한 계약을 해지할 수 있다.<신설 2014.5.28>

⑦ 제2항에 따라 통신과금서비스제공자가 제공하여야 하는 구매·이용내역의 대상기간, 종류 및 범위, 제4항에 따라 통신과금서비스제공자가 보존하여야 하는 기록의 종류 및 보존방법, 제6항에 따른 약관변경에 관한 통지의 방법 및 이의기간·절차 등 계약해지에 필요한 사항은 대통령령으로 정한다.<개정 2014.5.28>

⑧ 제5항에 따른 동의의 방법 등에 필요한 사항은 미래창조과학부장관이 정하여 고시한다.<신설 2014.5.28>

⑨ 미래창조과학부장관은 통신과금서비스가 통신과금서비스이용자의 의사에 반하여 제공되지 아니하도록 결제방식 등에 관한 세부적인 사항을 정하여 고시할 수 있다.<신설 2014.5.28>

[본조신설 2007.12.21]

[종전 제58조는 제67조로 이동 <2007.12.21>]

제59조(분쟁해결 등) ① 통신과금서비스제공자는 통신과금서비스에 있어서 이용자의 권익을 보호하기 위하여 자율적인 분쟁해결 등을 시행하는 기관 또는 단체를 설치·운영할 수 있다.

② 통신과금서비스제공자는 대통령령으로 정하는 바에 따라 통신과금서비스와 관련한 통신과금서비스이용자의 이의신청 및 권리구제를 위한 절차를 마련하여야 하고, 통신과금서비스 계약을 체결하는 경우 이를 이용약관에 명시하여야 한다.<개정 2014.5.28>

[본조신설 2007.12.21]

[종전 제59조는 제68조로 이동 <2007.12.21>]

제60조(손해배상 등) ① 통신과금서비스제공자는 통신과금서비스를 제공함에 있어서 통신과금서비스이용자에게 손해가 발생한 경우에 그 손해를 배상하여야 한다. 다만, 그 손해의 발생이 통신과금서비스이용자의 고의 또는 중과실로 인한 경우에는 그러하지 아니하다.

② 제1항에 따른 손해배상을 함에 있어서는 손해배상을 받을 자와 협의하여야 한다.

③ 제2항에 따른 손해배상에 관한 협의가 성립되지 아니하거나 협의를 할 수 없는 경우에는 당사자는 방송통신위원회에 재정을 신청할 수 있다.<개정 2008.2.29>

[본조신설 2007.12.21]

[종전 제60조는 제69조로 이동 <2007.12.21>]

제61조(통신과금서비스의 이용제한) 미래창조과학부장관은 통신과금서비스제공자에게 다음 각 호의 어느 하나에 해당하는 자에 대한 서비스의 제공을 거부, 정지 또는 제한하도록 명할 수 있다. <개정 2008.2.29, 2011.9.15, 2013.3.23>

1. 「청소년 보호법」 제16조를 위반하여 청소년유해매체물을 청소년에게 판매·대여·제공하는 자
2. 다음 각 목의 어느 하나에 해당하는 수단을 이용하여 통신과금서비스이용자로 하여금 재화 등을 구매·이용하게 함으로써 통신과금서비스이용자의 이익을 현저하게 저해하는 자
   가. 제50조를 위반한 영리목적의 광고성 정보 전송
   나. 통신과금서비스이용자에 대한 기망 또는 부당한 유인
3. 이 법 또는 다른 법률에서 금지하는 재화등을 판매·제공하는 자

[본조신설 2007.12.21]

[종전 제61조는 제70조로 이동 <2007.12.21>]

제8장 국제협력 <신설 2007.12.21>

제62조(국제협력) 정부는 다음 각 호의 사항을 추진할 때 다른 국가 또는 국제기구와 상호 협력하여야 한다.

1. 개인정보의 국가간 이전 및 개인정보의 보호에 관련된 업무
2. 정보통신망에서의 청소년 보호를 위한 업무
3. 정보통신망의 안전성을 침해하는 행위를 방지하기 위한 업무
4. 그 밖에 정보통신서비스의 건전하고 안전한 이용에 관한 업무

[전문개정 2008.6.13]

제63조(국외 이전 개인정보의 보호) ① 정보통신서비스 제공자등은 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결하여서는 아니 된다.

② 정보통신서비스 제공자등은 이용자의 개인정보를 국외에 제공(조회되는 경우를 포함한다)·처리위탁·보관(이하 이 조에서 "이전"이라 한다)하려면 이용자의 동의를 받아야 한다. 다만, 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 제3항 각 호의 사항 모두를 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 처리위탁·보관에 따른 동의절차를 거치지 아니할 수 있다.<개정 2016.3.22>

③ 정보통신서비스 제공자등은 제2항에 따른 동의를 받으려면 미리 다음 각 호의 사항 모두를 이용자에게 고지하여야 한다.

1. 이전되는 개인정보 항목
2. 개인정보가 이전되는 국가, 이전일시 및 이전방법
3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다)
4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간

④ 정보통신서비스 제공자등은 제2항에 따른 동의를 받아 개인정보를 국외로 이전하는 경우 대통령령으로 정하는 바에 따라 보호조치를 하여야 한다.

[전문개정 2008.6.13]

제9장 보칙 <신설 2007.12.21>

제64조(자료의 제출 등) ① 미래창조과학부장관 또는 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 정보통신서비스 제공자등(제67조에 따라 준용되는 자를 포함한다. 이하 이 조에서 같다)에게 관계 물품·서류 등을 제출하게 할 수 있다. <개정 2011.3.29, 2012.2.17, 2013.3.23>

1. 이 법에 위반되는 사항을 발견하거나 혐의가 있음을 알게 된 경우
2. 이 법의 위반에 대한 신고를 받거나 민원이 접수된 경우

2의2. 이용자 정보의 안전성과 신뢰성 확보를 현저히 해치는 사건·사고 등이 발생하였거나 발생할 가능성이 있는 경우

3. 그 밖에 이용자 보호를 위하여 필요한 경우로서 대통령령으로 정하는 경우

② 방송통신위원회는 이 법을 위반하여 영리목적 광고성 정보를 전송한 자에게 다음 각 호의 조치를 하기 위하여 정보통신서비스 제공자등에게 해당 광고성 정보 전송자의 성명·주소·주민등록번호·이용기간 등에 대한 자료의 열람이나 제출을 요청할 수 있다.

1. 제4항에 따른 시정조치
2. 제76조에 따른 과태료 부과
3. 그 밖에 이에 준하는 조치

③ 미래창조과학부장관 또는 방송통신위원회는 정보통신서비스 제공자등이 제1항 및 제2항에 따른 자료를 제출하지 아니하거나 이 법을 위반한 사실이 있다고 인정되면 소속 공무원에게

정보통신서비스 제공자등, 해당 법 위반 사실과 관련한 관계인의 사업장에 출입하여 업무상황, 장부 또는 서류 등을 검사하도록 할 수 있다.<개정 2011.3.29, 2013.3.23, 2016.3.22>

④ 미래창조과학부장관 또는 방송통신위원회는 이 법을 위반한 정보통신서비스 제공자등에게 해당 위반행위의 중지나 시정을 위하여 필요한 시정조치를 명할 수 있고, 시정조치의 명령을 받은 정보통신서비스 제공자등에게 시정조치의 명령을 받은 사실을 공표하도록 할 수 있다. 이 경우 공표의 방법·기준 및 절차 등에 필요한 사항은 대통령령으로 정한다.<개정 2011.3.29, 2013.3.23>

⑤ 미래창조과학부장관 또는 방송통신위원회는 제4항에 따라 필요한 시정조치를 명한 경우에는 시정조치를 명한 사실을 공개할 수 있다. 이 경우 공개의 방법·기준 및 절차 등에 필요한 사항은 대통령령으로 정한다.<개정 2011.3.29, 2013.3.23>

⑥ 미래창조과학부장관 또는 방송통신위원회가 제1항 및 제2항에 따라 자료 등의 제출 또는 열람을 요구할 때에는 요구사유, 법적 근거, 제출시한 또는 열람일시, 제출·열람할 자료의 내용 등을 구체적으로 밝혀 서면(전자문서를 포함한다)으로 알려야 한다.<개정 2011.3.29, 2013.3.23>

⑦ 제3항에 따른 검사를 하는 경우에는 검사 시작 7일 전까지 검사일시, 검사이유 및 검사내용 등에 대한 검사계획을 해당 정보통신서비스 제공자등에게 알려야 한다. 다만, 긴급한 경우나 사전통지를 하면 증거인멸 등으로 검사목적을 달성할 수 없다고 인정하는 경우에는 그 검사계획을 알리지 아니한다.

⑧ 제3항에 따라 검사를 하는 공무원은 그 권한을 표시하는 증표를 지니고 이를 관계인에게 내보여야 하며, 출입할 때 성명·출입시간·출입목적 등이 표시된 문서를 관계인에게 내주어야 한다.

⑨ 미래창조과학부장관 또는 방송통신위원회는 제1항부터 제3항까지의 규정에 따라 자료 등을 제출받거나 열람 또는 검사한 경우에는 그 결과(조사 결과 시정조치명령 등의 처분을 하려는 경우에는 그 처분의 내용을 포함한다)를 해당 정보통신서비스 제공자등에게 서면으로 알려야 한다.<개정 2011.3.29, 2013.3.23>

⑩ 미래창조과학부장관 또는 방송통신위원회는 제1항부터 제4항까지의 규정에 따른 자료의 제출 요구 및 검사 등을 위하여 인터넷진흥원의 장에게 기술적 자문을 하거나 그 밖에 필요한 지원을 요청할 수 있다.<개정 2009.4.22, 2011.3.29, 2013.3.23>

⑪ 제1항부터 제3항까지의 규정에 따른 자료 등의 제출 요구, 열람 및 검사 등은 이 법의 시행을 위하여 필요한 최소한의 범위에서 하여야 하며 다른 목적을 위하여 남용하여서는 아니 된다.

[전문개정 2008.6.13]

제64조의2(자료 등의 보호 및 폐기) ① 미래창조과학부장관 또는 방송통신위원회는 정보통신서비스 제공자등으로부터 제64조에 따라 제출되거나 수집된 서류·자료 등에 대한 보호 요구를 받으면 이를 제3자에게 제공하거나 일반에게 공개하여서는 아니 된다. <개정 2011.3.29, 2013.3.23>

② 미래창조과학부장관 또는 방송통신위원회는 정보통신망을 통하여 자료의 제출 등을 받은 경우나 수집한 자료 등을 전자화한 경우에는 개인정보·영업비밀 등이 유출되지 아니하도록 제도적·기술적 보안조치를 하여야 한다.<개정 2011.3.29, 2013.3.23>

③ 미래창조과학부장관 또는 방송통신위원회는 다른 법률에 특별한 규정이 있는 경우 외에 다음 각 호의 어느 하나에 해당하는 사유가 발생하면 제64조에 따라 제출되거나 수집된 서류·자료 등을 즉시 폐기하여야 한다. 제65조에 따라 미래창조과학부장관 또는 방송통신위원회의 권한의 전부 또는 일부를 위임 또는 위탁받은 자도 또한 같다.<개정 2011.3.29, 2013.3.23>

1. 제64조에 따른 자료제출 요구, 출입검사, 시정명령 등의 목적이 달성된 경우
2. 제64조제4항에 따른 시정조치명령에 불복하여 행정심판이 청구되거나 행정소송이 제기된 경우에는 해당 행정쟁송절차가 끝난 경우
3. 제76조제4항에 따른 과태료 처분이 있고 이에 대한 이의제기가 없는 경우에는 같은 조 제5항에 따른 이의제기기간이 끝난 경우
4. 제76조제4항에 따른 과태료 처분에 대하여 이의제기가 있는 경우에는 해당 관할 법원에 의한 비송사건절차가 끝난 경우

[전문개정 2008.6.13]

제64조의3(과징금의 부과 등) ① 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다. <개정 2012.2.17, 2014.5.28, 2016.3.22>

1. 제22조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 경우
2. 제23조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집한 경우
3. 제24조(제67조에 따라 준용되는 경우를 포함한다)를 위반하여 개인정보를 이용한 경우
4. 제24조의2(제67조에 따라 준용되는 경우를 포함한다)를 위반하여 개인정보를 제3자에게 제공한 경우
5. 제25조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보 처리위탁을 한 경우

5의2. 제25조제4항(제67조에 따라 준용되는 경우를 포함한다)에 따른 관리·감독 또는 교육을 소홀히 하여 수탁자가 제4장의 규정을 위반한 경우

6. 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우로서 제28조제1항 제2호부터 제5호까지(제67조에 따라 준용되는 경우를 포함한다)의 조치를 하지 아니한 경우
7. 제31조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 경우

8. 제63조제2항 본문을 위반하여 이용자의 동의를 받지 아니하고 이용자의 개인정보를 국외에 제공한 경우

② 제1항에 따른 과징금을 부과하는 경우 정보통신서비스 제공자등이 매출액 산정자료의 제출을 거부하거나 거짓의 자료를 제출한 경우에는 해당 정보통신서비스 제공자등과 비슷한 규모의 정보통신서비스 제공자등의 재무제표 등 회계자료와 가입자 수 및 이용요금 등 영업현황 자료에 근거하여 매출액을 추정할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 4억원 이하의 과징금을 부과할 수 있다.<개정 2012.2.17>

③ 방송통신위원회는 제1항에 따른 과징금을 부과하려면 다음 각 호의 사항을 고려하여야 한다.

1. 위반행위의 내용 및 정도
2. 위반행위의 기간 및 횟수
3. 위반행위로 인하여 취득한 이익의 규모

④ 제1항에 따른 과징금은 제3항을 고려하여 산정하되, 구체적인 산정기준과 산정절차는 대통령령으로 정한다.

⑤ 방송통신위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 이를 내지 아니하면 납부기한의 다음 날부터 내지 아니한 과징금의 연 100분의 6에 해당하는 가산금을 징수한다.

⑥ 방송통신위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 이를 내지 아니한 경우에는 기간을 정하여 독촉을 하고, 그 지정된 기간에 과징금과 제5항에 따른 가산금을 내지 아니하면 국세 체납처분의 예에 따라 징수한다.

⑦ 법원의 판결 등의 사유로 제1항에 따라 부과된 과징금을 환급하는 경우에는 과징금을 낸 날부터 환급하는 날까지 연 100분의 6에 해당하는 환급가산금을 지급하여야 한다.

[본조신설 2008.6.13]

제64조의4(청문) 미래창조과학부장관 또는 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 청문을 하여야 한다.

1. 제9조제2항에 따라 인증기관의 지정을 취소하려는 경우
2. 제23조의4제1항에 따라 본인확인기관의 지정을 취소하려는 경우
3. 제47조제10항(제47조의3제3항에서 준용하는 경우를 포함한다)에 따라 정보보호 관리체계 인증을 취소하려는 경우
4. 제47조의2제1항(제47조의3제4항에서 준용하는 경우를 포함한다)에 따라 정보보호 관리체계 인증기관의 지정을 취소하려는 경우
5. 제47조의5제4항에 따라 정보보호 관리등급을 취소하려는 경우
6. 제55조제1항에 따라 등록을 취소하려는 경우

[본조신설 2015.12.1]

제65조(권한의 위임·위탁) ① 이 법에 따른 미래창조과학부장관 또는 방송통신위원회의 권한은 대통령령으로 정하는 바에 따라 그 일부를 미래창조과학부 소속 기관의 장 또는 지방우정청장에게 위임·위탁할 수 있다. <개정 2011.3.29, 2013.3.23>

② 미래창조과학부장관은 제13조에 따른 정보통신망의 이용촉진 등에 관한 사업을 대통령령으로 정하는 바에 따라 「국가정보화 기본법」 제14조에 따른 한국정보화진흥원에 위탁할 수 있다.<개정 2013.3.23>

③ 미래창조과학부장관 또는 방송통신위원회는 제64조제1항 및 제2항에 따른 자료의 제출 요구 및 검사에 관한 업무를 대통령령으로 정하는 바에 따라 인터넷진흥원에 위탁할 수 있다.<개정 2009.4.22, 2011.3.29, 2013.3.23>

④ 제3항에 따른 인터넷진흥원의 직원에게는 제64조제8항을 준용한다.<개정 2009.4.22>

[전문개정 2008.6.13]

제65조의2 삭제 <2005.12.30>

제66조(비밀유지 등) 다음 각 호의 어느 하나에 해당하는 업무에 종사하는 자 또는 종사하였던 자는 그 직무상 알게 된 비밀을 타인에게 누설하거나 직무 외의 목적으로 사용하여서는 아니 된다. 다만, 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다. <개정 2012.2.17>

1. 삭제 <2011.3.29>
2. 제47조에 따른 정보보호 관리체계 인증 업무

2의2. 제47조의3에 따른 개인정보보호 관리체계 인증 업무

3. 제52조제3항제4호에 따른 정보보호시스템의 평가 업무
4. 삭제 <2012.2.17>
5. 제44조의10에 따른 명예훼손 분쟁조정부의 분쟁조정 업무

[전문개정 2008.6.13]

제67조(방송사업자에 대한 준용) ① 「방송법」 제2조제3호가목부터 마목까지와 같은 조 제6호·제9호·제12호 및 제14호에 해당하는 자가 시청자의 개인정보를 수집·이용 또는 제공하는 경우에는 제4장을 준용한다. 이 경우 "정보통신서비스 제공자" 또는 "정보통신서비스 제공자등"은 "「방송법」 제2조제3호가목부터 마목까지와 같은 조 제6호·제9호·제12호 및 제14호에 해당하는 자"로, "이용자"는 "시청자"로 본다.

② 제25조제1항에 따른 수탁자에 관하여는 제22조, 제23조, 제23조의2부터 제23조의4까지, 제24조, 제24조의2, 제26조, 제26조의2, 제27조, 제27조의2, 제27조의3, 제28조, 제28조의2, 제29조, 제30조, 제30조의2 및 제31조를 준용한다.

[본조신설 2012.2.17]

제68조 삭제 <2010.3.22>

제68조의2 삭제 <2015.6.22>

제69조(벌칙 적용 시의 공무원 의제) 미래창조과학부장관 또는 방송통신위원회가 제65조제2항 및 제3항에 따라 위탁한 업무에 종사하는 한국정보화진흥원과 인터넷진흥원의 임직원은 「형법」 제129조부터 제132조까지의 규정에 따른 벌칙을 적용할 때에는 공무원으로 본다. <개정 2009.4.22, 2011.3.29, 2013.3.23>

[전문개정 2008.6.13]

제69조의2(고발) ①방송통신위원회는 제64조의3제1항 각 호의 어느 하나에 해당하는 행위가 있다고 인정하는 경우에는 해당 정보통신서비스 제공자등을 검찰 등 수사기관에 고발할 수 있다. <개정 2016.3.22>

② 방송통신위원회는 개인정보 보호와 관련하여 이 법을 위반한 정보통신서비스 제공자등에게 책임이 있는 자(대표자 및 책임있는 임원을 포함한다)를 징계할 것을 권고할 수 있다. 이 경우 권고를 받은 사람은 이를 존중하여야 하며 그 결과를 방송통신위원회에 통보하여야 한다.<신설 2016.3.22>

[본조신설 2012.2.17]

제10장 벌칙 <신설 2007.12.21>

제70조(벌칙) ① 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다. <개정 2014.5.28>

② 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 다른 사람의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.

③ 제1항과 제2항의 죄는 피해자가 구체적으로 밝힌 의사에 반하여 공소를 제기할 수 없다.

[전문개정 2008.6.13]

제70조의2(벌칙) 제48조제2항을 위반하여 악성프로그램을 전달 또는 유포하는 자는 7년 이하의 징역 또는 7천만원 이하의 벌금에 처한다.

[본조신설 2016.3.22]

제71조(벌칙) ①다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. <개정 2016.3.22>

1. 제22조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 자
2. 제23조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인의 권리ㆍ이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집한 자

3. 제24조, 제24조의2제1항 및 제2항 또는 제26조제3항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
4. 제25조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보 처리위탁을 한 자
5. 제28조의2제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 개인정보를 훼손·침해 또는 누설한 자
6. 제28조의2제2항을 위반하여 그 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
7. 제30조제5항(제30조제7항, 제31조제3항 및 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 필요한 조치를 하지 아니하고 개인정보를 제공하거나 이용한 자
8. 제31조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 자
9. 제48조제1항을 위반하여 정보통신망에 침입한 자
10. 제48조제3항을 위반하여 정보통신망에 장애가 발생하게 한 자
11. 제49조를 위반하여 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설한 자

② 제1항제9호의 미수범은 처벌한다.<신설 2016.3.22>

[전문개정 2008.6.13]

제72조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다. <개정 2015.1.20, 2015.3.27>

1. 삭제 <2016.3.22>
2. 제49조의2제1항을 위반하여 다른 사람의 개인정보를 수집한 자

2의2. 「재난 및 안전관리 기본법」 제14조제1항에 따른 대규모 재난 상황을 이용하여 제50조의8을 위반하여 광고성 정보를 전송한 자

3. 제53조제1항에 따른 등록을 하지 아니하고 그 업무를 수행한 자
4. 다음 각 목의 어느 하나에 해당하는 행위를 통하여 자금을 융통하여 준 자 또는 이를 알선·중개·권유·광고한 자
   가. 재화등의 판매·제공을 가장하거나 실제 매출금액을 초과하여 통신과금서비스에 의한 거래를 하거나 이를 대행하게 하는 행위
   나. 통신과금서비스이용자로 하여금 통신과금서비스에 의하여 재화등을 구매·이용하도록 한 후 통신과금서비스이용자가 구매·이용한 재화등을 할인하여 매입하는 행위
5. 제66조를 위반하여 직무상 알게 된 비밀을 타인에게 누설하거나 직무 외의 목적으로 사용한 자

② 삭제 <2016.3.22>

[전문개정 2008.6.13]

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. <개정 2014.5.28, 2016.3.22>

1. 제28조제1항제2호부터 제5호까지(제67조에 따라 준용되는 경우를 포함한다)의 규정에 따른 기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 자

1의2. 제29조제1항을 위반하여 개인정보를 파기하지 아니한 자(제67조에 따라 준용되는 경우를 포함한다)

2. 제42조를 위반하여 청소년유해매체물임을 표시하지 아니하고 영리를 목적으로 제공한 자

3. 제42조의2를 위반하여 청소년유해매체물을 광고하는 내용의 정보를 청소년에게 전송하거나 청소년 접근을 제한하는 조치 없이 공개적으로 전시한 자

4. 제44조의6제3항을 위반하여 이용자의 정보를 민·형사상의 소를 제기하는 것 외의 목적으로 사용한 자

5. 제44조의7제2항 및 제3항에 따른 방송통신위원회의 명령을 이행하지 아니한 자

6. 제48조의4제3항에 따른 명령을 위반하여 관련 자료를 보전하지 아니한 자

7. 제49조의2제1항을 위반하여 개인정보의 제공을 유인한 자

8. 제61조에 따른 명령을 이행하지 아니한 자

[전문개정 2008.6.13]

제74조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다. <개정 2012.2.17, 2014.5.28>

1. 제8조제4항을 위반하여 비슷한 표시를 한 제품을 표시·판매 또는 판매할 목적으로 진열한 자

2. 제44조의7제1항제1호를 위반하여 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시한 자

3. 제44조의7제1항제3호를 위반하여 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하게 한 자

4. 제50조제5항을 위반하여 조치를 한 자

5. 삭제 <2014.5.28>

6. 제50조의8을 위반하여 광고성 정보를 전송한 자

7. 제53조제4항을 위반하여 등록사항의 변경등록 또는 사업의 양도·양수 또는 합병·상속의 신고를 하지 아니한 자

② 제1항제3호의 죄는 피해자가 구체적으로 밝힌 의사에 반하여 공소를 제기할 수 없다.

[전문개정 2008.6.13]

제75조(양벌규정) 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제71조부터 제73조까지 또는 제74조제1항의 어느 하나에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형을

과(科)한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.

[전문개정 2010.3.17]

제75조의2(몰수·추징) 제71조제1항제1호부터 제8호까지, 제72조제1항제2호 및 제73조제1호·제1호의2·제7호의 어느 하나에 해당하는 죄를 지은 자가 해당 위반행위와 관련하여 취득한 금품이나 그 밖의 이익은 몰수할 수 있으며, 이를 몰수할 수 없을 때에는 그 가액을 추징할 수 있다. 이 경우 몰수 또는 추징은 다른 벌칙에 부가하여 과할 수 있다.

[본조신설 2016.3.22]

제76조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다. <개정 2011.3.29, 2012.2.17, 2013.3.23, 2014.5.28, 2015.6.22, 2015.12.1, 2016.3.22>

1. 제23조제3항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 서비스의 제공을 거부한 자
2. 제23조의2제1항을 위반하여 주민등록번호를 수집·이용하거나 같은 조 제2항에 따른 필요한 조치를 하지 아니한 자(제67조에 따라 준용되는 경우를 포함한다)

2의2. 제24조의2제3항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 제공 또는 처리위탁에 대한 동의를 받을 때 개인정보의 수집·이용에 대한 동의와 구분하여 받지 아니하거나 이에 동의하지 아니한 이유로 서비스 제공을 거부한 자

2의3. 제27조의3제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자·방송통신위원회 및 한국인터넷진흥원에 통지 또는 신고하지 아니하거나 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 자

2의4. 제27조의3제3항에 따른 소명을 하지 아니하거나 거짓으로 한 자

3. 제28조제1항(제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 아니한 자
4. 제29조제2항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 파기 등의 조치를 취하지 아니한 자
5. 제30조제3항·제4항 및 제6항(제30조제7항, 제31조제3항 및 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 필요한 조치를 하지 아니한 자

5의2. 제30조의2제1항 본문을 위반하여 개인정보의 이용내역을 통지하지 아니한 자(제67조에 따라 준용되는 경우를 포함한다)

6. 삭제 <2014.5.28>

6의2. 제45조의3제1항을 위반하여 정보보호 최고책임자의 지정을 신고하지 아니한 자

6의3. 제47조제2항을 위반하여 정보보호 관리체계 인증을 받지 아니한 자

7. 제50조제1항부터 제3항까지의 규정을 위반하여 영리 목적의 광고성 정보를 전송한 자

8. 제50조제4항을 위반하여 광고성 정보를 전송할 때 밝혀야 하는 사항을 밝히지 아니하거나 거짓으로 밝힌 자
9. 제50조제6항을 위반하여 비용을 수신자에게 부담하도록 한 자
9의2. 제50조제8항을 위반하여 수신동의 여부를 확인하지 아니한 자
10. 제50조의5를 위반하여 이용자의 동의를 받지 아니하고 프로그램을 설치한 자
11. 제50조의7제1항 또는 제2항을 위반하여 인터넷 홈페이지에 영리목적의 광고성 정보를 게시한 자
12. 이 법을 위반하여 제64조제4항에 따라 미래창조과학부장관 또는 방송통신위원회로부터 받은 시정조치 명령을 이행하지 아니한 자

② 다음 각 호의 어느 하나에 해당하는 자에게는 2천만원 이하의 과태료를 부과한다.<개정 2016.3.22>

1. 제25조제2항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자에게 개인정보 처리위탁에 관한 사항을 공개하지 아니하거나 알리지 아니한 자
1의2. 제25조제7항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 처리위탁을 한 정보통신서비스 제공자등의 동의를 받지 아니하고 제3자에게 재위탁한 자
2. 제26조제1항 및 제2항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자에게 개인정보의 이전사실을 알리지 아니한 자
3. 제27조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 보호책임자를 지정하지 아니한 자
4. 제27조의2제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 처리방침을 공개하지 아니한 자
5. 제63조제2항 단서를 위반하여 제63조제3항 각 호의 사항 모두를 공개하거나 이용자에게 알리지 아니하고 이용자의 개인정보를 국외에 처리위탁·보관한 자

③ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.<개정 2009.4.22, 2011.4.5, 2012.2.17, 2014.5.28, 2015.6.22, 2015.12.1, 2016.3.22>

1. 삭제 <2015.6.22>
2. 삭제 <2015.6.22>
2의2. 제23조의3제1항을 위반하여 본인확인기관의 지정을 받지 아니하고 본인확인업무를 한 자
2의3. 제23조의3제2항에 따른 본인확인업무의 휴지 또는 같은 조 제3항에 따른 본인확인업무의 폐지 사실을 이용자에게 통보하지 아니하거나 방송통신위원회에 신고하지 아니한 자
2의4. 제23조의4제1항에 따른 본인확인업무의 정지 및 지정취소 처분에도 불구하고 본인확인업무를 계속한 자
2의5. 제25조제6항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 처리위탁을 할 때에 문서에 의하지 아니한 자

3. 제42조의3제1항을 위반하여 청소년 보호 책임자를 지정하지 아니한 자
4. 제43조를 위반하여 정보를 보관하지 아니한 자
5. 제46조제2항을 위반하여 보험에 가입하지 아니한 자
6. 삭제 <2015.12.1>
7. 제47조제9항 및 제47조의3제3항을 위반하여 인증받은 내용을 거짓으로 홍보한 자
8. 삭제 <2012.2.17>
9. 삭제 <2012.2.17>
10. 제47조의4제3항을 위반하여 소프트웨어 사용자에게 알리지 아니한 자
11. 제48조의2제4항에 따른 시정명령을 이행하지 아니한 자
11의2. 제48조의3제1항을 위반하여 침해사고의 신고를 하지 아니한 자
12. 제48조의4제4항에 따른 사업장 출입 및 조사를 방해하거나 거부 또는 기피한 자
12의2. 제49조의2제4항을 위반하여 미래창조과학부장관 또는 방송통신위원회의 명령을 이행하지 아니한 자
12의3. 제50조제7항을 위반하여 수신동의, 수신거부 또는 수신동의 철회에 대한 처리 결과를 알리지 아니한 자
12의4. 제50조의4제4항을 위반하여 필요한 조치를 하지 아니한 자
13. 제52조제6항을 위반하여 한국인터넷진흥원의 명칭을 사용한 자
14. 제53조제4항을 위반하여 사업의 휴지·폐지·해산의 신고를 아니한 자
15. 제56조제1항을 위반하여 약관을 신고하지 아니한 자
16. 제57조제2항을 위반하여 관리적 조치 또는 기술적 조치를 하지 아니한 자
17. 제58조제1항을 위반하여 통신과금서비스 이용일시 등을 통신과금서비스이용자에게 고지하지 아니한 자
18. 제58조제2항을 위반하여 통신과금서비스이용자가 구매·이용 내역을 확인할 수 있는 방법을 제공하지 아니하거나 통신과금서비스이용자의 제공 요청에 응하지 아니한 자
19. 제58조제3항을 위반하여 통신과금서비스이용자로부터 받은 통신과금에 대한 정정요구가 이유 있음에도 결제대금의 지급을 유보하지 아니하거나 통신과금서비스이용자의 요청에 대한 처리 결과를 통신과금서비스이용자에게 알려 주지 아니한 자
20. 제58조제4항을 위반하여 통신과금서비스에 관한 기록을 보존하지 아니한 자
20의2. 제58조제5항을 위반하여 통신과금서비스이용자의 동의를 받지 아니하고 통신과금서비스를 제공하거나 이용한도액을 증액한 자
20의3. 제58조제6항을 위반하여 통신과금서비스 약관의 변경에 관한 통지를 하지 아니한 자
21. 제59조제2항을 위반하여 통신과금서비스이용자의 이의신청 및 권리구제를 위한 절차를 마련하지 아니하거나 통신과금서비스 계약 시 이를 명시하지 아니한 자
22. 제64조제1항에 따른 관계 물품·서류 등을 제출하지 아니하거나 거짓으로 제출한 자
23. 제64조제2항에 따른 자료의 열람·제출요청에 따르지 아니한 자

24. 제64조제3항에 따른 출입·검사를 거부·방해 또는 기피한 자

④ 제1항부터 제3항까지의 과태료는 대통령령으로 정하는 바에 따라 미래창조과학부장관 또는 방송통신위원회가 부과·징수한다.<개정 2011.3.29, 2013.3.23>

⑤ 제4항에 따른 과태료 처분에 불복하는 자는 그 처분을 고지받은 날부터 30일 이내에 미래창조과학부장관 또는 방송통신위원회에 이의를 제기할 수 있다.<개정 2011.3.29, 2013.3.23>

⑥ 제4항에 따라 과태료 처분을 받은 자가 제5항에 따라 이의를 제기하면 미래창조과학부장관 또는 방송통신위원회는 지체 없이 관할 법원에 그 사실을 통보하여야 하며, 그 통보를 받은 관할 법원은 「비송사건절차법」에 따른 과태료 재판을 한다.<개정 2011.3.29, 2013.3.23>

⑦ 제5항에 따른 기간에 이의를 제기하지 아니하고 과태료를 내지 아니하면 국세 체납처분의 예에 따라 징수한다.

[전문개정 2008.6.13]

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

[시행 2017.1.1] [대통령령 제27751호, 2016.12.30, 타법개정]

제1장 총칙

제1조(목적) 이 영은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 위임된 사항과 그 시행에 필요한 사항을 규정함을 목적으로 한다.

제2조(윤리강령) ① 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) 제2조제1항제3호에 따른 정보통신서비스 제공자 및 그 단체는 이용자의 개인정보를 보호하고 건전하고 안전한 정보통신서비스 제공을 위하여 정보통신서비스 제공자 윤리강령을 정하여 시행할 수 있다. <개정 2009.1.28>

② 법 제2조제1항제4호에 따른 이용자의 단체는 건전한 정보사회가 정착되도록 이용자 윤리강령을 정하여 시행할 수 있다.

③ 정부는 제1항 및 제2항에 따른 윤리강령의 제정 및 시행을 위한 활동을 지원할 수 있다.

제3조(개인정보보호지침) ① 방송통신위원회는 법 제4조에 따라 이용자의 개인정보를 보호하기 위한 개인정보보호지침을 정하여 고시하고, 정보통신서비스 제공자에게 이를 준수할 것을 권장할 수 있다. <개정 2009.1.28, 2011.9.29>

② 방송통신위원회는 제1항에 따른 개인정보보호지침을 정하여 고시하려면 관련 업계 및 이용자단체 등의 의견을 수렴하고 관계 중앙행정기관의 장과의 협의를 거쳐야 한다.<개정 2011.9.29>

제2장 정보통신망의 이용촉진

제4조 삭제 <2009.8.18>

제5조 삭제 <2009.8.18>

제6조(정보의 공동 활용체제 구축 시책 등) ① 중앙행정기관의 장은 법 제12조에 따라 소관 분야의 정보의 공동 활용을 위한 계획을 수립하여 고시할 수 있다. <개정 2010.5.4>

② 중앙행정기관의 장은 제1항에 따른 정보의 공동 활용을 위한 계획을 효율적으로 추진하기 위하여 필요한 경우에는 다음 각 호의 사업 등을 하는 자에 대하여 지원할 수 있다.

1. 보유·관리하는 정보 중 공동 활용 대상 정보의 선정
2. 정보통신망 상호간 연계 시스템의 구축 및 운영
3. 정보통신망의 연계에 따른 각 기관 간 비용부담의 조정
4. 그 밖에 정보의 공동 활용체제 구축을 위하여 필요한 사항

제7조(정보통신망의 이용촉진 등에 관한 사업의 실시) 미래창조과학부장관이 법 제13조제1항에 따라 실시할 수 있는 사업은 다음 각 호와 같다. <개정 2013.3.23>

1. 정보통신망의 구성·운영을 위한 시험적 사업
2. 새로운 매체의 실용화를 위한 시험적 사업
3. 정보화산업 육성을 위한 선도 응용사업 및 관련 연구 지원 사업
4. 전자거래에 관한 기술개발 등 전자거래의 활성화를 위한 기반 조성 사업
5. 정보통신망 이용촉진을 위한 법·제도 개선 등 지원 사업
6. 그 밖에 정보사회의 기반조성을 위한 관련 기술·기기 및 응용서비스의 효율적인 활용과 보급을 위한 시범사업

제3장 삭제 <2015.12.22>

제8조 삭제 <2015.12.22>

제9조 삭제 <2015.12.22>

제4장 개인정보의 보호

제9조의2 삭제 <2012.8.17>

제9조의3(심사사항별 세부 심사기준) ① 법 제23조의3제1항에 따른 심사사항별 세부 심사기준은 다음 각 호와 같다. <개정 2012.8.17>

1. 물리적·기술적·관리적 조치계획: 다음 각 목의 사항에 대한 조치계획을 마련할 것
   가. 법 제23조의3제1항에 따른 본인확인업무(이하 "본인확인업무"라 한다) 관련 설비의 관리 및 운영에 관한 사항
   나. 정보통신망 침해행위의 방지에 관한 사항
   다. 시스템 및 네트워크의 운영·보안 및 관리에 관한 사항
   라. 이용자 보호 및 불만처리에 관한 사항
   마. 긴급상황 및 비상상태의 대응에 관한 사항
   바. 본인확인업무를 위한 내부 규정의 수립 및 시행에 관한 사항
   사. 법 제23조의2제2항에 따른 대체수단(이하 "대체수단"이라 한다)의 안전성 확보에 관한 사항

아. 접속정보의 위조·변조 방지에 관한 사항

자. 그 밖에 본인확인업무를 위하여 방송통신위원회가 정하여 고시하는 사항

2. 기술적 능력: 다음 각 목의 어느 하나에 해당하는 요건을 갖춘 자를 8명 이상 보유할 것

가. 정보통신기사·정보처리기사 및 전자계산기조직응용기사 이상의 국가기술자격 또는 이와 동등 이상의 자격이 있다고 방송통신위원회가 인정하는 자격을 갖출 것

나. 방송통신위원회가 정하여 고시하는 정보보호 또는 정보통신운영·관리 분야에서 2년 이상 근무한 경력이 있을 것

3. 재정적 능력: 자본금이 80억원 이상일 것(국가기관 및 지방자치단체는 제외한다)

4. 설비규모의 적정성: 다음 각 목의 설비를 본인확인업무의 적절한 수행에 필요한 규모 이상 보유할 것

가. 이용자의 개인정보를 검증·관리 및 보호하기 위한 설비

나. 대체수단을 생성·발급 및 관리하기 위한 설비

다. 출입통제 및 접근제한을 위한 보안설비

라. 시스템 및 네트워크의 보호설비

마. 화재·수해 및 정전 등 재난 방지를 위한 설비

② 제1항에 따른 심사사항별 세부 심사기준의 평가기준 및 평가방법 등에 관하여 필요한 사항은 방송통신위원회가 정하여 고시한다.

[본조신설 2011.8.29]

제9조의4(본인확인기관의 지정절차) ① 법 제23조의3제1항에 따라 본인확인기관으로 지정을 받으려는 자는 본인확인기관지정신청서(전자문서로 된 신청서를 포함한다)에 다음 각 호의 서류(전자문서를 포함한다)를 첨부하여 방송통신위원회에 제출하여야 한다.

1. 조직·인력 및 설비 등의 현황을 기재한 사업계획서

2. 제9조의3에 따른 심사사항별 세부 심사기준이 충족됨을 증명할 수 있는 서류

3. 법인의 정관 또는 단체의 규약(법인 또는 단체인 경우에만 해당한다)

4. 그 밖에 본인확인업무 수행의 전문성과 재무구조의 건전성 등을 확인하기 위하여 필요한 서류로서 방송통신위원회가 정하여 고시하는 서류

② 제1항에 따라 본인확인기관지정신청서를 제출받은 방송통신위원회는 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 법인 등기사항증명서(법인인 경우에만 해당한다)를 확인하여야 한다.

③ 방송통신위원회는 제1항에 따른 신청을 심사하는 데 필요하다고 인정하는 경우에는 그 신청인에게 자료의 제출을 요청하거나 그 의견을 들을 수 있다.

④ 방송통신위원회는 제1항에 따른 신청을 받은 경우에는 신청을 받은 날부터 90일 이내에 제9조의3에 따른 심사사항별 세부 심사기준의 충족 여부를 심사하여 그 심사결과를 신청인에게 통지하여야 한다. 다만, 부득이한 사유가 있는 경우에는 그 사유를 알리고 30일의 범위에서 그 기간을 연장할 수 있다.

⑤ 방송통신위원회는 제4항의 심사결과에 따라 본인확인기관을 지정한 경우에는 그 신청인에게 본인확인기관지정서를 발급하고, 본인확인기관의 명칭·소재지 및 지정일 등 지정내용을 관보에 고시하여야 한다.
⑥ 제1항부터 제5항까지의 규정에 따른 지정신청, 지정심사 등의 절차 및 방법 등에 관하여 필요한 사항은 방송통신위원회가 정하여 고시한다.
[본조신설 2011.8.29]

제9조의5(본인확인업무의 휴지·폐지) ① 본인확인기관이 법 제23조의3제2항 또는 제3항에 따라 업무를 휴지 또는 폐지하려면 다음 각 호의 사항을 이용자에게 통보하여야 한다.
1. 휴지 또는 폐지의 사유
2. 휴지 또는 폐지의 일시(휴지의 경우에는 사업의 개시일시를 포함한다)
3. 대체수단 및 개인정보의 이용 제한에 관한 사항(휴지의 경우에만 해당한다)
4. 대체수단 및 개인정보의 파기에 관한 사항(폐지의 경우에만 해당한다)
② 본인확인기관은 법 제23조의3제2항 또는 제3항에 따라 본인확인업무의 휴지 또는 폐지를 신고할 때에는 본인확인업무 휴지·폐지 신고서에 다음 각 호의 서류를 첨부하여 방송통신위원회에 제출하여야 한다.
1. 제1항 각 호의 사항을 기재한 통보 서류
2. 대체수단 및 개인정보의 이용 제한 또는 파기 계획에 관한 서류
3. 이용자의 보호조치 계획에 관한 서류
4. 본인확인기관지정서(폐지의 경우에만 해당한다)
③ 제1항 또는 제2항에 따른 휴지 또는 폐지의 통보 및 신고의 절차, 기준 및 방법 등에 관하여 필요한 세부사항은 방송통신위원회가 정하여 고시한다.
[본조신설 2011.8.29]

제9조의6(본인확인업무의 정지 및 지정취소) ① 법 제23조의4제1항에 따른 본인확인업무의 정지 또는 지정취소의 기준은 별표 1과 같다.
② 방송통신위원회는 제1항에 따라 본인확인업무를 정지하거나 지정을 취소한 경우에는 그 사실을 관보에 고시하여야 한다.
[본조신설 2011.8.29]

제10조(개인정보 처리위탁의 통지) 법 제25조제2항 전단에서 "대통령령으로 정하는 방법"이란 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법을 말한다. <개정 2011.8.29>
[제목개정 2016.9.22]

제11조(영업의 양도 등에 따른 개인정보 이전 시의 통지) ① 법 제26조제1항 각 호 외의 부분 및 제2항 본문에서 "대통령령으로 정하는 방법"이란 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법을 말한다. <개정 2011.8.29>

② 정보통신서비스 제공자 등 또는 영업양수자 등이 과실 없이 이용자의 연락처를 알 수 없는 경우에 해당되어 제1항의 방법에 따라 통지할 수 없는 경우에는 인터넷 홈페이지에 최소 30일 이상 게시하여야 한다.<개정 2009.1.28>

③ 천재·지변이나 그 밖에 정당한 사유로 제2항에 따른 홈페이지 게시가 곤란한 경우에는 「신문 등의 진흥에 관한 법률」에 따라 전국을 보급지역으로 하는 둘 이상의 일반일간신문(이용자의 대부분이 특정지역에 거주하는 경우에는 그 지역을 보급구역으로 하는 일반일간신문)에 1회 이상 공고하는 것으로 갈음할 수 있다.<개정 2010.1.27>

제12조(동의획득방법) ① 정보통신서비스 제공자 등이 법 제26조의2에 따라 동의를 얻는 방법은 다음 각 호의 어느 하나와 같다. 이 경우 정보통신서비스 제공자 등은 동의를 얻어야 할 사항(이하 "동의 내용"이라 한다)을 이용자가 명확하게 인지하고 확인할 수 있도록 표시하여야 한다. <개정 2009.1.28>

1. 인터넷 사이트에 동의 내용을 게재하고 이용자가 동의 여부를 표시하도록 하는 방법
2. 동의 내용이 기재된 서면을 이용자에게 직접 교부하거나, 우편 또는 모사전송을 통하여 전달하고 이용자가 동의 내용에 대하여 서명날인 후 제출하도록 하는 방법
3. 동의 내용이 적힌 전자우편을 발송하여 이용자로부터 동의의 의사표시가 적힌 전자우편을 전송받는 방법
4. 전화를 통하여 동의 내용을 이용자에게 알리고 동의를 얻거나 인터넷주소 등 동의 내용을 확인할 수 있는 방법을 안내하고 재차 전화 통화를 통하여 동의를 얻는 방법

② 정보통신서비스 제공자 등은 개인정보 수집 매체의 특성상 동의 내용을 전부 표시하기 어려운 경우 이용자에게 동의 내용을 확인할 수 있는 방법(인터넷주소·사업장 전화번호 등)을 안내하고 동의를 얻을 수 있다.<개정 2009.1.28>

제13조(개인정보 보호책임자의 자격요건 등) ① 정보통신서비스 제공자와 그로부터 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)가 법 제27조제1항 본문에 따라 지정하는 개인정보 보호책임자는 다음 각 호의 어느 하나에 해당하는 지위에 있는 자로 하여야 한다. <개정 2009.1.28, 2016.9.22>

1. 임원
2. 개인정보와 관련하여 이용자의 고충처리를 담당하는 부서의 장

② 법 제27조제1항 단서에서 "대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자등"이란 상시 종업원 수가 5명 미만인 정보통신서비스 제공자등을 말한다. 다만, 인터넷으로 정보통신서비스를 제공하는 것을 주된 업으로 하는 정보통신서비스 제공자등의 경우에는 상시 종업원 수가 5명 미만으로서 전년도 말 기준으로 직전 3개월간의 일일평균이용자가 1천명 이하인 자를 말한다.<개정 2009.1.28>

[제목개정 2016.9.22]

제14조(개인정보 처리방침의 공개 방법 등) ① 법 제27조의2제1항에 따라 정보통신서비스 제공자등은 개인정보를 처리(개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집,

검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다. 이하 이 조, 제15조, 제17조 및 제34조에서 같다)하는 경우에는 개인정보의 수집 장소와 매체 등을 고려하여 다음 각 호 중 어느 하나 이상의 방법으로 개인정보 처리방침을 공개하되, 그 명칭을 '개인정보 처리방침'이라고 표시하여야 한다. <개정 2009.1.28, 2016.9.22>

1. 인터넷 홈페이지의 첫 화면 또는 첫 화면과의 연결화면을 통하여 법 제27조의2제2항 각 호의 사항을 이용자가 볼 수 있도록 하는 방법. 이 경우 정보통신서비스 제공자등은 글자 크기, 색상 등을 활용하여 이용자가 개인정보 처리방침을 쉽게 확인할 수 있도록 표시하여야 한다.
2. 점포·사무소 안의 보기 쉬운 장소에 써 붙이거나 비치하여 열람하도록 하는 방법
3. 동일한 제호로 연 2회 이상 계속적으로 발행하여 이용자에게 배포하는 간행물·소식지·홍보지·청구서 등에 지속적으로 게재하는 방법

② 법 제27조의2제3항에 따른 개인정보 처리방침의 변경 이유 및 내용은 다음 각 호의 방법 중 어느 하나 이상의 방법으로 공지한다.<개정 2009.1.28, 2016.9.22>

1. 정보통신서비스 제공자등이 운영하는 인터넷 홈페이지의 첫 화면의 공지사항란 또는 별도의 창을 통하여 공지하는 방법
2. 서면·모사전송·전자우편 또는 이와 비슷한 방법으로 이용자에게 공지하는 방법
3. 점포·사무소 안의 보기 쉬운 장소에 써 붙이거나 비치하는 방법

③ 삭제 <2014.11.28>

[제목개정 2016.9.22]

제14조의2(개인정보 유출 등의 통지·신고) ① 정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제27조의3제1항 각 호의 모든 사항을 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다. <개정 2014.11.28, 2016.9.22>

② 정보통신서비스 제공자등은 제1항에 따른 통지·신고를 하려는 경우 법 제27조의3제1항 제1호 또는 제2호의 사항에 관한 구체적인 내용이 확인되지 아니하였으면 그때까지 확인된 내용과 같은 항 제3호부터 제5호까지의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고하여야 한다.

③ 정보통신서비스 제공자등은 법 제27조의3제1항 각 호 외의 부분 단서에 따른 정당한 사유가 있는 경우에는 법 제27조의3제1항 각 호의 사항을 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제1항의 통지를 갈음할 수 있다.

④ 천재지변이나 그 밖의 정당한 사유로 제3항에 따른 홈페이지 게시가 곤란한 경우에는 「신문 등의 진흥에 관한 법률」에 따른 전국을 보급지역으로 하는 둘 이상의 일반일간신문에 1회 이상 공고하는 것으로 제3항에 따른 홈페이지 게시를 갈음할 수 있다.

⑤ 정보통신서비스 제공자등은 법 제27조의3제1항 각 호 외의 부분 본문 및 단서에 따른 정당한 사유를 지체 없이 서면(전자문서를 포함한다)으로 방송통신위원회에 소명하여야 한다.<신설 2014.11.28>

[본조신설 2012.8.17]

[제목개정 2016.9.22]

제15조(개인정보의 보호조치) ① 법 제28조제1항제1호에 따라 정보통신서비스 제공자등은 개인정보의 안전한 처리를 위하여 다음 각 호의 내용을 포함하는 내부관리계획을 수립·시행하여야 한다. <개정 2016.9.22>

1. 개인정보 보호책임자의 지정 등 개인정보보호 조직의 구성·운영에 관한 사항
2. 정보통신서비스 제공자의 지휘·감독을 받아 이용자의 개인정보를 처리하는 자(이하 이 조에서 "개인정보취급자"라 한다)의 교육에 관한 사항
3. 제2항부터 제5항까지의 규정에 따른 보호조치를 이행하기 위하여 필요한 세부 사항

② 법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 다음 각 호의 조치를 하여야 한다. 다만, 제3호의 조치는 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등만 해당한다.<개정 2012.8.17>

1. 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 "개인정보처리시스템"이라 한다)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행
2. 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영
3. 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단
4. 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영
5. 그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치

③ 법 제28조제1항제3호에 따라 정보통신서비스 제공자등은 접속기록의 위조·변조 방지를 위하여 다음 각 호의 조치를 하여야 한다.

1. 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독
2. 개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관

④ 법 제28조제1항제4호에 따라 정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 다음 각 호의 보안조치를 하여야 한다.<개정 2014.11.28>

1. 비밀번호의 일방향 암호화 저장
2. 주민등록번호, 계좌정보 및 바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다) 등 방송통신위원회가 정하여 고시하는 정보의 암호화 저장
3. 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안서버 구축 등의 조치
4. 그 밖에 암호화 기술을 이용한 보안조치

⑤ 법 제28조제1항제5호에 따라 정보통신서비스 제공자등은 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로

그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치하여야 하며, 이를 주기적으로 갱신·점검하여야 한다.

⑥ 방송통신위원회는 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다.

[전문개정 2009.1.28]

제16조(개인정보의 파기 등) ① 삭제 <2016.5.31>

② 정보통신서비스 제공자등은 이용자가 정보통신서비스를 법 제29조제2항의 기간 동안 이용하지 아니하는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다.<개정 2016.5.31>

③ 정보통신서비스 제공자등은 제2항에 따라 개인정보를 별도로 저장·관리하는 경우에는 법 또는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 해당 개인정보를 이용하거나 제공하여서는 아니 된다.

④ 법 제29조제3항에서 "개인정보가 파기되는 사실, 기간 만료일 및 파기되는 개인정보의 항목 등 대통령령으로 정하는 사항"이란 다음 각 호의 사항을 말한다.<개정 2016.5.31>

1. 개인정보를 파기하는 경우: 개인정보가 파기되는 사실, 기간 만료일 및 파기되는 개인정보의 항목
2. 다른 이용자의 개인정보와 분리하여 개인정보를 저장·관리하는 경우: 개인정보가 분리되어 저장·관리되는 사실, 기간 만료일 및 분리·저장되어 관리되는 개인정보의 항목

⑤ 법 제29조제3항에서 "전자우편 등 대통령령으로 정하는 방법"이란 전자우편·서면·모사전송·전화 또는 이와 유사한 방법을 말한다.<신설 2016.5.31>

[본조신설 2012.8.17]

제17조(개인정보 이용내역의 통지) ① 법 제30조의2제1항 본문에서 "대통령령으로 정하는 기준에 해당하는 자"란 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등을 말한다.

② 법 제30조의2제1항에 따라 이용자에게 통지하여야 하는 정보의 종류는 다음 각 호와 같다.<개정 2016.9.22>

1. 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목
2. 개인정보를 제공받은 자와 그 제공 목적 및 제공한 개인정보의 항목. 다만, 「통신비밀보호법」 제13조, 제13조의2, 제13조의4 및 「전기통신사업법」 제83조제3항에 따라 제공한 정보는 제외한다.
3. 법 제25조에 따른 개인정보 처리위탁을 받은 자 및 그 처리위탁을 하는 업무의 내용

③ 법 제30조의2제1항에 따른 통지는 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 연 1회 이상 하여야 한다.

[본조신설 2012.8.17]

제18조(법정손해배상의 청구기간) ① 법 제32조의2제1항에 따른 배상은 이용자가 개인정보의 분실·도난·유출·위조·변조 또는 훼손의 사실을 안 날부터 3년 이내에 청구하여야 한다. <개정 2016.9.22>

② 법 제32조의2제1항에 따른 배상은 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 날부터 10년이 지나면 청구하지 못한다.<개정 2016.9.22>

[본조신설 2014.11.28]

제19조 삭제 <2011.9.29>

제20조 삭제 <2011.9.29>

제21조 삭제 <2011.9.29>

제22조 삭제 <2011.9.29>

제5장 정보통신망에서의 이용자 보호 등

제23조(청소년보호시책) 법 제41조제1항제4호에서 "대통령령으로 정하는 사항"이란 다음 각 호와 같다. <개정 2009.1.28, 2011.8.29>

1. 청소년에게 유익한 정보의 개발 및 보급 촉진
2. 정보통신망을 통하여 유통되는 음란·폭력정보 등의 유해한 정보로부터 청소년을 보호하기 위한 청소년의 자발적 참여활동의 촉진 및 지원
3. 청소년 보호를 위한 학부모·교사 또는 민간단체 등의 자율적인 감시·상담·피해구제활동의 촉진 및 지원
4. 청소년보호활동을 위한 정보통신서비스 제공자 간의 협력체계 구축 지원
5. 그 밖에 법 제41조제1항 각 호에 따른 시책을 추진하는 데 부수되는 사항

제24조(청소년유해매체물의 표시방법) ① 법 제42조에 따른 청소년유해매체물을 제공하는 자는 그 매체물에 19세 미만의 자는 이용할 수 없다는 취지의 내용을 누구나 쉽게 확인할 수 있도록 음성·문자 또는 영상으로 표시하여야 한다.

② 제1항에 따른 표시를 하여야 하는 자 중 인터넷을 이용하여 정보를 제공하는 자의 경우에는 기호·부호·문자 또는 숫자를 사용하여 청소년유해매체물임을 나타낼 수 있는 전자적 표시도 함께 하여야 한다.

③ 방송통신위원회는 정보의 유형 등을 고려하여 제1항 및 제2항에 따른 표시의 구체적 방법을 정하여 관보에 고시하여야 한다.

제25조(청소년보호책임자 지정의무자의 범위) 법 제42조의3제1항에서 "일일평균이용자의 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 요건에 모두 해당하는

자를 말한다. <개정 2011.8.29, 2012.9.14>

1. 다음 각 목의 어느 하나에 해당하는 자
   가. 전년도말 기준 직전 3개월간의 일일평균이용자가 10만 명 이상인 자
   나. 정보통신서비스부문 전년도(법인의 경우에는 전 사업연도) 매출액이 10억원 이상인 자
2. 「청소년 보호법」 제2조제3호에 따른 청소년유해매체물을 제공하거나 매개하는 자

제26조(청소년보호책임자의 업무) 법 제42조의3제1항에 따른 청소년보호책임자는 정보통신망상의 청소년유해정보(이하 "유해정보"라 한다)로부터 청소년을 보호하기 위하여 다음의 업무를 수행한다.

1. 유해정보로부터의 청소년보호계획의 수립
2. 유해정보에 대한 청소년접근제한 및 관리조치
3. 정보통신업무 종사자에 대한 유해정보로부터의 청소년보호를 위한 교육
4. 유해정보로 인한 피해상담 및 고충처리
5. 그 밖에 유해정보로부터 청소년을 보호하기 위하여 필요한 사항

제27조(청소년보호책임자의 지정기한) 법 제42조의3제1항에 따른 청소년보호책임자의 지정은 매년 4월말까지 하여야 한다.

제28조(영상 또는 음향정보의 보관 등) ① 법 제43조제1항에서 "대통령령으로 정하는 자"란 전기통신회선을 통하여 정보를 유통시키는 자를 말한다. 다만, "방송", "텔레비전" 또는 "라디오"의 명칭을 사용하면서 일정한 편성계획에 따라 정보를 유통시키는 자 중 「방송법」 제2조제3호·제6호 및 제12호에 따른 방송사업자·중계유선방송사업자 및 전광판방송사업자는 제외한다. <개정 2011.8.29>

② 법 제43조에 따른 정보제공자는 해당 정보를 이용에 제공한 때부터 6개월간 이를 보관하여야 한다.

제29조 삭제 <2014.11.28>

제30조 삭제 <2014.11.28>

제31조(청구할 수 있는 이용자 정보의 범위) 법 제44조의6제1항에서 "대통령령으로 정하는 최소한의 정보"란 다음 각 호의 정보를 말한다. <개정 2011.8.29>

1. 성명
2. 주소
3. 그 밖에 민·형사상의 소제기를 위하여 법 제44조의10에 따른 명예훼손분쟁조정부(이하 "명예훼손분쟁조정부"라 한다)가 필요하다고 인정하는 해당 이용자의 연락처 등의 정보

제32조(정보제공청구의 절차) ① 법 제44조의6제1항에 따라 해당 이용자의 정보제공을 청구하려는 자(이하 "청구인"이라 한다)는 다음 각 호의 사항을 기재한 정보제공청구서를 소명자료와 함께 명예훼손분쟁조정부에 제출하여야 한다.

1. 청구인의 성명、주소、연락처(전화번호、전자우편주소 등을 말한다)
2. 제기하려는 소의 종류 및 소로써 구하는 취지
3. 침해된 권리의 유형 및 해당 이용자의 구체적인 권리침해사실

② 명예훼손분쟁조정부는 법 제44조의6제2항에 따라 정보제공 여부를 결정할 때 필요하다고 인정하는 경우 청구인에게 의견을 진술하게 할 수 있다.

제33조(정보제공의 절차) ① 명예훼손분쟁조정부는 청구인으로부터 정보제공 요청을 받은 경우 해당 이용자의 정보제공 여부를 결정하여 그 결과를 청구인에게 통지하여야 한다.

② 명예훼손분쟁조정부는 정보제공을 결정한 경우 해당 정보통신서비스 제공자에게 제31조에 따른 정보를 제공해 주도록 요청하여야 한다. 이 경우 해당 정보통신서비스 제공자는 정당한 사유가 없으면 이에 따라야 한다.<개정 2009.1.28>

③ 정보통신서비스 제공자는 제2항에 따른 정보를 제공한 사실을 해당 이용자에게 알려야 한다.<개정 2009.1.28>

④ 명예훼손분쟁조정부는 이용자정보제공사실 등 관련 자료를 5년간 보관하여야 한다.

제34조(불법정보의 처리제한명령 등의 요청) ① 관계 중앙행정기관의 장이 법 제44조의7제3항에 따라 방송통신위원회에 정보통신서비스 제공자 또는 게시판 관리、운영자에게 같은 조 제1항제7호부터 제9호까지의 정보의 처리를 거부、정지 또는 제한하도록 하는 명령을 하여 줄 것을 요청하려는 때에는 다음 각 호의 사항을 적은 요청서를 증빙자료와 함께 방송통신위원회에 제출하여야 한다. <개정 2009.1.28, 2016.9.22>

1. 요청의 취지와 그 이유
2. 관련 법령 및 위반내용
3. 해당 정보의 목록 및 제공처
4. 정보통신서비스 제공자 또는 게시판 관리、운영자 및 해당 이용자의 명칭 또는 성명과 주소、전화번호、전자우편주소 등의 연락처

② 방송통신위원회는 제1항에 따라 제출된 서류 등에 흠이 있음을 발견한 때에는 즉시 관계 중앙행정기관의 장에게 보완을 요구할 수 있다. 이 경우 5일 이상의 보완기간을 부여하여야 한다.

③ 방송통신위원회는 제2항에 따른 보완요구에도 불구하고 보완기간이 끝나는 날까지 보완이 이루어지지 아니한 때에는 제1항에 따라 제출받은 요청서와 증빙자료를 관계 중앙행정기관의 장에게 반려할 수 있다.

[제목개정 2016.9.22]

제35조(의견제출의 예외사유) 법 제44조의7제4항제2호에서 "대통령령으로 정하는 경우"란 다음 각 호의 경우를 말한다. <개정 2011.8.29>

1. 해당 이용자를 알 수 없는 경우(이용자의 의견제출의 경우에만 해당한다)
2. 법원의 확정판결 등에 따라 명령의 전제가 되는 사실이 객관적으로 증명되어 명령에 따른 의견청취가 불필요하다고 판단되는 경우

제36조(명예훼손분쟁조정부의 설치·운영 및 분쟁조정 등) ① 명예훼손분쟁조정부의 회의는 명예훼손분쟁조정부의 장이 소집한다.

② 명예훼손분쟁조정부의 장이 명예훼손분쟁조정부의 회의를 개최하려는 때에는 회의일시·장소 및 안건을 정하여 부득이한 사유가 있는 경우를 제외하고는 회의개시 7일 전까지 위원에게 통지하여야 한다.

③ 명예훼손분쟁조정부의 회의는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.

④ 명예훼손분쟁조정부의 장은 위원 중에서 「방송통신위원회의 설치 및 운영에 관한 법률」 제18조에 따른 방송통신심의위원회(이하 "방송통신심의위원회"라 한다) 위원장이 지명한다.

⑤ 명예훼손분쟁조정부의 회의는 공개하지 아니한다. 다만, 필요하다고 인정될 때에는 명예훼손분쟁조정부의 의결로 당사자 또는 이해관계인에게 방청을 하게 할 수 있다.

⑥ 삭제 <2011.9.29>

⑦ 이 영에서 규정한 것 외에 명예훼손분쟁조정부의 설치·구성 및 운영 그 밖에 분쟁조정에 필요한 사항은 방송통신심의위원회의 의결을 거쳐 정한다.

제6장 정보통신망의 안정성 확보 등

제36조의2(정보보호 사전점검기준) 법 제45조의2제2항에 따른 정보보호 사전점검기준은 다음 각 호의 사항을 고려하여 미래창조과학부장관이 정하여 고시한다. <개정 2013.3.23>

1. 정보통신망을 구축하거나 정보통신서비스를 제공하기 위한 시스템의 구조 및 운영환경
2. 제1호에 따른 시스템의 운영을 위한 하드웨어, 프로그램, 콘텐츠 등 자산 중 보호해야 할 대상의 식별 및 위험성
3. 보호대책의 도출 및 구현현황

[본조신설 2012.8.17]

제36조의3(정보보호 사전점검 권고 대상) ① 법 제45조의2제2항제1호에서 "대통령령으로 정하는 정보통신서비스 또는 전기통신사업"이란 정보시스템 구축에 필요한 투자금액이 5억원 이상(하드웨어·소프트웨어의 단순한 구입비용은 제외한 금액을 말한다)인 정보통신서비스 또는 전기통신사업을 말한다.

② 법 제45조의2제2항제2호에서 "대통령령으로 정하는 정보통신서비스 또는 전기통신사업"이란 미래창조과학부장관이 신규 정보통신서비스 또는 전기통신사업의 발굴·육성을 위하여 사업비의 전부 또는 일부를 지원하는 정보통신서비스 또는 전기통신사업을 말한다.<개정 2013.3.23>

[본조신설 2012.8.17]

제36조의4(정보보호 사전점검의 방법 및 절차 등) ① 법 제45조의2제2항에 따른 정보보호 사전점검은 서면점검, 현장점검 또는 원격점검(외부에서 정보통신망을 통하여 제36조의2제1호에

따른 시스템에 접속하여 보안 관련 사항을 점검하는 것을 말한다)의 방법으로 실시한다.

② 법 제45조의2제2항에 따른 정보보호 사전점검은 다음 각 호의 순서로 진행한다.

1. 사전점검 준비
2. 설계 검토
3. 보호대책 적용
4. 보호대책 구현현황 점검
5. 사전점검 결과 정리

③ 법 제45조의2제2항에 따른 미래창조과학부장관의 권고를 받은 자는 정보보호 사전점검을 직접 실시하거나 법 제52조에 따른 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다) 또는 외부 전문기관으로 하여금 실시하게 할 수 있다. 이 경우 정보보호 사전점검은 별표 2에 따른 정보보호 기술인력의 자격기준을 갖춘 사람만 수행할 수 있다.<개정 2013.3.23>

④ 제1항부터 제3항까지에서 규정한 사항 외에 정보보호 사전점검의 방법 및 절차에 관하여 필요한 세부사항은 미래창조과학부장관이 정하여 고시한다.<개정 2013.3.23>

[본조신설 2012.8.17]

제36조의5(정보보호 사전점검 수수료) ① 법 제45조의2제2항에 따른 미래창조과학부장관의 권고를 받은 자가 정보보호 사전점검을 인터넷진흥원이나 외부 전문기관으로 하여금 실시하게 한 경우에는 인터넷진흥원이나 외부 전문기관에 수수료를 납부하여야 한다. <개정 2013.3.23>

② 미래창조과학부장관은 다음 각 호의 사항을 고려하여 정보보호 사전점검 수수료의 산정기준을 정하여 고시한다.<개정 2013.3.23>

1. 정보보호 사전점검을 받는 정보통신서비스 또는 전기통신사업의 규모
2. 정보보호 사전점검에 참가하는 자의 전문성
3. 정보보호 사전점검에 필요한 기간

[본조신설 2012.8.17]

제36조의6(정보보호 최고책임자 지정ㆍ신고 대상자의 범위) 법 제45조의3제1항 단서에서 "종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자"란 정보통신서비스 제공자로서 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 법 제41조제1항제1호에 따른 내용 선별 소프트웨어를 개발 및 보급하는 사업자
2. 법 제47조제2항에 따라 정보보호 관리체계 인증을 받아야 하는 자
3. 「저작권법」 제104조제1항에 따른 특수한 유형의 온라인서비스제공자로서 상시 종업원 수가 5명 이상이거나 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 1천명 이상인 자
4. 「전자상거래 등에서의 소비자보호에 관한 법률」 제2조제3호에 따른 통신판매업자(통신판매중개업자를 포함한다)로서 상시 종업원 수가 5명 이상인 자
5. 「게임산업진흥에 관한 법률」 제2조제7호에 따른 인터넷컴퓨터게임시설제공업을 영위하는 자에게 같은 법 제28조제6호에 따라 고시된 음란물 및 사행성게임물 차단 프로그램을 제

공하는 사업자

6. 상시 종업원 수가 1천명 이상인 자

[본조신설 2014.11.28]

[종전 제36조의6은 제36조의8로 이동 <2014.11.28>]

제36조의7(정보보호 최고책임자의 신고 방법 및 절차) 법 제45조의3제1항 단서에 따라 정보보호 최고책임자를 지정하고 신고하려는 정보통신서비스 제공자는 제36조의6 각 호의 어느 하나에 해당하게 된 날부터 90일 이내에 미래창조과학부령으로 정하는 정보보호 최고책임자 지정신고서를 미래창조과학부장관에게 제출하여야 한다.

[본조신설 2014.11.28]

제36조의8(정보보호 최고책임자 협의회의 사업 범위) 법 제45조의3제4항에서 "대통령령으로 정하는 공동의 사업"이란 다음 각 호의 사업을 말한다. <개정 2014.11.28>

1. 정보통신서비스 제공자의 정보보호 강화를 위한 정책의 조사, 연구 및 수립 지원
2. 정보통신서비스 이용에 따른 침해사고 분석 및 대책 연구
3. 정보보호 최고책임자 교육 등 정보통신서비스 제공자의 정보보호 능력 및 전문성 향상
4. 정보통신서비스 보안 관련 국제교류 및 협력
5. 그 밖에 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 필요한 사업

[본조신설 2012.8.17]

[제36조의6에서 이동 <2014.11.28>]

제37조(집적정보통신시설사업자의 보호조치) ① 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자(이하 "집적정보통신시설사업자"라 한다)가 법 제46조제1항에 따라 정보통신시설의 안정적 운영을 위한 보호조치는 다음 각 호와 같다. <개정 2009.1.28>

1. 정보통신시설에 대한 접근 권한이 없는 자의 접근 통제 및 감시를 위한 기술적·관리적 조치
2. 정보통신시설의 지속적·안정적 운영을 확보하고 화재·지진·수해 등의 각종 재해와 테러 등의 각종 위협으로부터 정보통신시설을 보호하기 위한 물리적·기술적 조치
3. 정보통신시설의 안정적 관리를 위한 관리인원 선발·배치 등의 조치
4. 정보통신시설의 안정적 운영을 위한 내부관리계획(비상시 계획을 포함한다)의 수립 및 시행
5. 침해사고의 확산을 차단하기 위한 기술적·관리적 조치의 마련 및 시행

② 미래창조과학부장관은 관련 사업자의 의견을 수렴하여 제1항에 따른 보호조치의 구체적인 기준을 정하여 고시한다.<개정 2013.3.23>

③ 미래창조과학부장관은 제1항에 따른 보호조치의 이행확인을 하는 과정에서 다른 기관이 수행하는 업무와 관계되는 때에는 해당 기관과 미리 협의하여야 한다.<개정 2013.3.23>

제38조(보험가입) ① 집적정보통신시설사업자는 법 제46조제2항에 따라 사업 개시와 동시에 책임보험에 가입하여야 한다.

② 제1항에 따라 사업자가 가입하여야 하는 책임보험의 최저보험금액은 별표 1의2와 같다. <개정 2011.8.29>

제39조 삭제 <2012.8.17>

제40조 삭제 <2012.8.17>

제41조 삭제 <2012.8.17>

제42조 삭제 <2012.8.17>

제43조 삭제 <2012.8.17>

제44조 삭제 <2012.8.17>

제45조 삭제 <2012.8.17>

제46조 삭제 <2012.8.17>

제47조(정보보호 관리체계 인증의 방법·절차·범위 등) ① 법 제47조제1항 또는 제2항에 따라 정보보호 관리체계의 인증을 받으려는 자는 정보보호 관리체계 인증신청서(전자문서로 된 신청서를 포함한다)에 다음 각 호의 사항에 대한 설명이 포함된 정보보호 관리체계 명세서(전자문서를 포함한다)를 첨부하여 인터넷진흥원, 법 제47조제6항에 따라 지정된 기관(이하 "정보보호 관리체계 인증기관"이라 한다) 또는 법 제47조제7항에 따라 지정된 기관(이하 "정보보호 관리체계 심사기관"이라 한다)에 제출하여야 한다. <개정 2013.3.23, 2016.5.31>

1. 정보보호 관리체계의 범위
2. 정보보호 관리체계의 범위에 포함되어 있는 주요 정보통신설비의 목록과 시스템 구성도
3. 정보보호 관리체계를 수립·운영하는 방법과 절차
4. 정보보호 관리체계와 관련된 주요 문서의 목록
5. 정보보호 관리체계와 관련된 국내외 품질경영체제의 인증을 취득한 경우에는 그 명세

② 제1항에 따른 신청을 받은 인터넷진흥원, 정보보호 관리체계 인증기관 또는 정보보호 관리체계 심사기관은 법 제47조제6항제1호에 따른 인증심사(이하 "인증심사"라 한다)를 하는 경우 같은 조 제4항에 따라 미래창조과학부장관이 정하여 고시하는 정보보호 관리체계 인증을 위한 관리적·기술적·물리적 보호대책을 포함한 인증기준 등(이하 "관리체계인증고시"라 한다)에 따라 신청인과 인증의 범위 및 일정 등에 관한 협의를 하여야 한다.<개정 2013.3.23, 2016.5.31>

③ 인터넷진흥원, 정보보호 관리체계 인증기관 또는 정보보호 관리체계 심사기관은 인증심사를 하는 경우 인증 신청인이 수립한 정보보호 관리체계가 관리체계인증고시에 적합한지 여부를 심사하여야 한다. 이 경우 인증심사는 서면심사 또는 현장심사의 방법으로 실시한다.<개정

2016.5.31>

④ 인증심사는 제53조제1항제1호에 따른 인증심사원만 수행할 수 있다.<개정 2016.5.31>

⑤ 정보보호 관리체계 심사기관은 인증심사의 결과를 인터넷진흥원 또는 정보보호 관리체계 인증기관에 제출하여야 한다.<신설 2016.5.31>

⑥ 인터넷진흥원 또는 정보보호 관리체계 인증기관은 인증심사의 결과를 심의하기 위하여 정보보호에 관한 학식과 경험이 풍부한 자를 위원으로 하는 인증위원회를 설치·운영하여야 한다.<개정 2016.5.31>

⑦ 인터넷진흥원 또는 정보보호 관리체계 인증기관은 제6항에 따른 인증위원회의 심의 결과 관리체계인증고시에 적합한 때에는 그 인증신청을 한 자에게 정보보호 관리체계 인증서를 발급하여야 한다.<개정 2016.5.31>

⑧ 제1항부터 제7항까지에서 규정한 사항 외에 인증신청, 인증심사, 인증위원회의 설치·운영 및 인증서의 발급 등에 필요한 세부사항은 미래창조과학부장관이 정하여 고시한다.<개정 2013.3.23, 2016.5.31>

[전문개정 2012.8.17]

[제50조에서 이동, 종전 제47조는 제53조로 이동 <2012.8.17>]

제48조(정보보호 관리체계 인증의 수수료) ① 제47조제1항에 따라 인증을 신청하는 자는 인터넷진흥원, 정보보호 관리체계 인증기관 또는 정보보호 관리체계 심사기관에 수수료를 납부하여야 한다. <개정 2016.5.31>

② 미래창조과학부장관은 인증심사에 투입되는 인증심사원의 수, 인증심사에 필요한 일수 등을 고려하여 정보보호 관리체계 인증 수수료 산정을 위한 구체적인 기준을 정하여 고시한다. <개정 2013.3.23>

[본조신설 2012.8.17]

[종전 제48조는 제53조의2로 이동 <2012.8.17>]

제49조(정보보호 관리체계 인증 대상자의 범위) ① 법 제47조제2항제1호에서 "대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자"란 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자를 말한다.

② 법 제47조제2항제3호에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.<개정 2016.5.31>

1. 연간 매출액 또는 세입이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자
   가. 「의료법」 제3조의4에 따른 상급종합병원
   나. 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교
2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.

3. 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 100만명 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.

[본조신설 2012.8.17]

[종전 제49조는 제53조의3으로 이동 <2012.8.17>]

제50조

[제47조로 이동 <2012.8.17>]

제51조(인증의 사후관리) ① 법 제47조제8항에 따른 사후관리는 서면심사 또는 현장심사의 방법으로 실시한다. <개정 2016.5.31>

② 정보보호 관리체계 심사기관은 법 제47조제8항에 따라 사후관리를 실시한 결과 같은 조 제10항 각 호의 사유가 있는 경우에는 인터넷진흥원 또는 정보보호 관리체계 인증기관에 그 사후관리 실시결과를 즉시 제출하여야 한다.<신설 2016.5.31>

③ 인터넷진흥원 또는 정보보호 관리체계 인증기관은 다음 각 호의 어느 하나에 해당하는 경우에는 제47조제6항에 따른 인증위원회의 심의를 거쳐 그 결과를 미래창조과학부장관에게 통보하여야 한다.<개정 2016.5.31>

1. 법 제47조제8항에 따른 사후관리를 실시한 결과 같은 조 제10항 각 호의 사유가 있는 경우
2. 제2항에 따라 정보보호 관리체계 심사기관으로부터 그 사후관리 실시결과를 제출받은 경우

[전문개정 2012.8.17]

[제52조에서 이동, 종전 제51조는 삭제 <2012.8.17>]

제52조(인증표시 및 홍보) 법 제47조제1항 및 제2항에 따라 정보보호 관리체계 인증을 받은 자는 같은 조 제9항에 따라 인증받은 내용을 문서·송장·광고 등에 표시·홍보하는 경우 미래창조과학부장관이 정하여 고시하는 정보보호 관리체계 인증표시를 사용할 수 있다. 이 경우 인증의 범위와 유효기간을 함께 표시하여야 한다. <개정 2013.3.23, 2016.5.31>

[전문개정 2012.8.17]

[제53조에서 이동, 종전 제52조는 제51조로 이동 <2012.8.17>]

제53조(정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관의 지정기준) ① 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관의 지정기준은 다음 각 호와 같다. <개정 2013.3.23, 2016.5.31>

1. 미래창조과학부장관이 정하여 고시하는 자격 요건을 갖춘 자(이하 "인증심사원"이라 한다)를 5명 이상 보유할 것
2. 미래창조과학부장관이 실시하는 업무수행 요건·능력 심사에서 적합하다고 인정받을 것

② 미래창조과학부장관은 인증심사원의 교육·자격관리에 관한 사항 및 제1항제2호에 따른 업무수행 요건·능력 심사에 관한 세부기준을 정하여 고시한다.<개정 2013.3.23>

[전문개정 2012.8.17]

[제목개정 2016.5.31]

[제47조에서 이동, 종전 제53조는 제52조로 이동 <2012.8.17>]

제53조의2(정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관의 지정절차 등) ① 법 제47조제6항 또는 제7항에 따라 정보보호 관리체계 인증기관 또는 정보보호 관리체계 심사기관으로 지정을 받으려는 자는 정보보호 관리체계 인증기관 지정신청서 또는 정보보호 관리체계 심사기관 지정신청서(전자문서로 된 신청서를 포함한다)에 다음 각 호의 서류(전자문서를 포함한다)를 첨부하여 미래창조과학부장관에게 제출하여야 한다. <개정 2012.8.17, 2013.3.23, 2016.5.31>

1. 법인의 정관 또는 단체의 규약
2. 인증심사원의 보유현황과 이를 증명할 수 있는 서류
3. 정보보호 업무를 수행한 경력이나 전문화 정도 등 업무수행 요건·능력 심사를 위하여 필요한 서류로서 미래창조과학부장관이 정하여 고시하는 서류

② 제1항에 따른 지정신청을 받은 미래창조과학부장관은 신청인이 법인인 경우에는 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 법인 등기사항증명서를 확인하여야 한다.<개정 2010.5.4, 2010.11.2, 2013.3.23>

③ 미래창조과학부장관은 제1항에 따른 지정신청을 받은 경우에는 제53조제1항에 따른 지정기준 충족 여부를 심사하여 신청을 받은 날부터 3개월 이내에 그 결과를 신청인에게 통지하고, 정보보호 관리체계 인증기관 또는 정보보호 관리체계 심사기관으로 지정되는 신청인에게 정보보호 관리체계 인증기관 지정서 또는 정보보호 관리체계 심사기관 지정서를 발급하여야 한다.<개정 2012.8.17, 2013.3.23, 2016.5.31>

④ 미래창조과학부장관은 제3항에 따라 지정기준의 충족여부를 심사하는 때에는 필요한 범위에서 신청인에게 자료의 제출을 요구하거나 현장실사를 할 수 있다. 이 경우 현장실사를 수행하는 자는 자신의 자격을 증명하는 증표를 신청인에게 내보여야 한다.<개정 2012.8.17, 2013.3.23>

⑤ 삭제 <2012.6.25>

[제목개정 2016.5.31]

[제48조에서 이동 <2012.8.17>]

제53조의3(정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관 지정의 유효기간) ① 제53조의2에 따른 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관 지정의 유효기간은 3년으로 한다. <개정 2012.8.17, 2016.5.31>

② 제1항에 따른 유효기간이 끝나기 전 6개월부터 끝나는 날까지 재지정의 신청을 할 수 있다. 이 경우 재지정의 신청에 대한 처리결과를 통지받을 때까지는 그 지정이 계속 유효한 것으로 본다.

③ 제2항에 따른 재지정에 관하여는 제53조, 제53조의2 및 제1항을 준용한다.<개정 2012.8.17>

[제목개정 2016.5.31]

[제49조에서 이동 <2012.8.17>]

제53조의4(정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관의 사후관리) ① 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관은 다음 각 호의 구분에 따른 보고서를 매년 1월 31일까지 미래창조과학부장관에게 제출하여야 한다. <개정 2016.5.31>

1. 정보보호 관리체계 인증기관: 전년도 인증실적 보고서
2. 정보보호 관리체계 심사기관: 전년도 인증심사실적 보고서

② 미래창조과학부장관은 법 제47조의2제1항 각 호에 해당하는지를 확인하기 위하여 필요한 경우 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관에 대하여 자료의 제출을 요구하거나 현장실사를 할 수 있다.<개정 2013.3.23, 2016.5.31>

[본조신설 2012.8.17]

[제목개정 2016.5.31]

제54조(지정취소 등의 기준) 법 제47조의2에 따른 지정취소 및 업무정지에 관한 행정처분의 기준은 별표 4와 같다.

제54조의2(개인정보보호 관리체계의 인증) 법 제47조의3에 따른 개인정보보호 관리체계 인증의 방법·절차·범위·수수료·사후관리 및 인증기관 지정의 기준·절차·유효기간·취소 등에 관하여는 제47조, 제48조, 제51조부터 제53조까지, 제53조의2부터 제53조의4까지 및 제54조를 준용한다.

[본조신설 2012.8.17]

제55조(이용자 보호조치의 요청에 관한 약관사항) 법 제47조의4제4항에 따라 이용자에 대한 보호조치의 요청에 관하여 이용약관으로 정하여야 하는 사항은 다음 각 호와 같다. <개정 2012.8.17>

1. 이용자에게 보호조치를 요청할 수 있는 사유 및 요청하는 방법
2. 이용자가 하여야 할 보호조치의 내용
3. 이용자가 보호조치를 이행하지 아니할 경우 정보통신망으로의 접속 제한 기간
4. 이용자의 보호조치 불이행에 대하여 부당한 접속 제한을 한 경우 이용자의 이의제기 및 배상 절차

제55조의2(정보보호 관리등급 부여의 심사기준) ① 법 제47조의5제1항에 따른 정보보호 관리등급 부여의 심사기준은 다음 각 호와 같다.

1. 정보보호 관리체계의 구축 범위 및 운영기간
2. 정보보호를 위한 전담조직 및 예산
3. 정보보호 관리 활동 및 보호조치 수준

② 제1항에 따른 심사기준별 세부 평가기준 및 평가방법 등에 관하여 필요한 사항은 미래창조과학부장관이 정하여 고시한다.<개정 2013.3.23>

[본조신설 2012.8.17]

제55조의3(정보보호 관리등급 부여의 방법 및 절차) ① 법 제47조의5제1항에 따라 정보보호 관리등급을 부여받으려는 자는 정보보호 관리등급 신청서(전자문서로 된 신청서를 포함한다)에 정보보호 관리체계 인증서 사본을 첨부하여 인터넷진흥원에 제출하여야 한다.

② 정보보호 관리등급 부여를 위한 심사는 서면심사 또는 현장심사의 방법으로 실시한다.

③ 제2항에 따른 심사는 인증심사원만 수행할 수 있다.

④ 인터넷진흥원은 제2항에 따른 심사 결과가 제55조의2에 따른 심사기준에 적합한 때에는 그 관리등급 부여를 신청한 자에게 정보보호 관리등급 증명서를 발급하여야 한다.

⑤ 제1항부터 제4항까지에서 규정한 사항 외에 정보보호 관리등급 부여의 신청·심사 및 정보보호 관리등급 증명서의 발급 등에 필요한 세부사항은 미래창조과학부장관이 정하여 고시한다.<개정 2013.3.23>

[본조신설 2012.8.17]

제55조의4(정보보호 관리등급 부여의 수수료 등) 정보보호 관리등급 부여의 수수료, 등급표시 및 홍보에 관하여는 제48조 및 제52조를 준용한다.

[본조신설 2012.8.17]

제55조의5(정보보호 관리등급의 유효기간) 제55조의3에 따른 정보보호 관리등급의 유효기간은 1년으로 한다.

[본조신설 2012.8.17]

제56조(침해사고 대응조치) 법 제48조의2제1항제4호에서 "그 밖에 대통령령으로 정한 침해사고 대응조치"란 다음 각 호의 조치를 말한다. <개정 2009.1.28>

1. 주요정보통신서비스 제공자 및 법 제46조제1항에 따른 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자에 대한 접속경로(침해사고 확산에 이용되고 있거나 이용될 가능성이 있는 접속경로만 해당한다)의 차단 요청
2. 「소프트웨어산업 진흥법」 제2조제4호에 따른 소프트웨어사업자 중 침해사고와 관련이 있는 소프트웨어를 제작 또는 배포한 자에 대한 해당 소프트웨어의 보안상 취약점을 수정·보완한 프로그램(이하 "보안취약점보완프로그램"이라 한다)의 제작·배포 요청 및 정보통신서비스 제공자에 대한 보안취약점보완프로그램의 정보통신망 게재 요청
3. 언론기관 및 정보통신서비스 제공자에 대한 법 제48조의2제1항제2호에 따른 침해사고 예보·경보의 전파
4. 국가 정보통신망 안전에 필요한 경우 관계 기관의 장에 대한 침해사고 관련정보의 제공

제57조(침해사고 관련정보 제공자) 법 제48조의2제2항제3호에서 "정보통신망을 운영하는 자로서 대통령령으로 정하는 자"란 정보통신망을 운영하는 자 중 다음 각 호의 어느 하나에 해당하는 자를 말한다. <개정 2008.3.28, 2009.1.28, 2010.10.1, 2011.8.29, 2013.3.23>

1. 「정보통신기반 보호법」 제6조 및 제10조에 따라 미래창조과학부장관이 수립 및 제정하는 주요정보통신기반시설보호계획 및 보호지침의 적용을 받는 기관
2. 정보통신서비스 제공자의 정보통신망운영현황을 주기적으로 관찰하고 침해사고 관련정보를 제공하는 서비스를 제공하는 자
3. 인터넷진흥원으로부터 「인터넷주소자원에 관한 법률」 제2조제1호가목에 따른 인터넷 프로토콜 주소를 할당받아 독자적으로 정보통신망을 운영하는 민간사업자 중 미래창조과학부장관이 정하여 고시하는 자
4. 정보보호산업에 종사하는 자 중 컴퓨터바이러스 백신소프트웨어 제조자

제58조(침해사고 관련정보의 제공방법) 법 제48조의2제2항에 따라 침해사고 관련정보를 제공하는 자는 다음 각 호의 방법에 따라 침해사고 관련정보를 제공하여야 한다. <개정 2013.3.23>

1. 미래창조과학부장관이 정보통신망의 특성, 침해사고 동향 등을 고려하여 정하는 제공방식에 적합할 것
2. 침해사고 관련정보의 훼손·멸실 및 변경 등을 방지할 수 있는 조치를 취할 것
3. 필요할 때에는 미래창조과학부장관이 정하는 암호기술을 적용할 것
4. 그 밖에 미래창조과학부장관이 정하여 고시하는 방법 및 절차에 적합할 것

제59조(민·관 합동조사단의 구성 등) ① 미래창조과학부장관이 법 제48조의4제2항에 따라 민·관 합동조사단(이하 "조사단"이라 한다)을 구성할 때에는 다음 각 호의 자로 조사단을 구성하여야 한다. <개정 2010.10.1, 2013.3.23>

1. 침해사고를 담당하는 공무원
2. 침해사고에 관한 전문지식과 경험이 있는 자
3. 인터넷진흥원의 직원
4. 그 밖에 침해사고의 원인 분석에 필요하다고 인정되는 자

② 제1항에 따른 조사단의 구성은 침해사고의 규모 및 유형에 따라 조정할 수 있다.

제60조(조사단의 사업장 출입) ① 조사단이 법 제48조의4제4항에 따라 관계인의 사업장에 출입하는 때에는 그 권한을 나타내는 증표를 관계인에게 내보여야 한다.

② 제1항에 따른 증표는 별표 5와 같다.

제61조(영리목적의 광고성 정보 전송기준) ① 법 제50조제1항제1호에서 "대통령령으로 정한 기간"이란 해당 재화등의 거래가 종료된 날부터 6개월을 말한다. <개정 2014.11.28>

② 법 제50조제3항 단서에서 "대통령령으로 정하는 매체"란 전자우편을 말한다.<신설 2014.11.28>

③ 법 제50조제4항에 따라 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 자가 해당 정보에 명시하여야 할 사항과 그 방법은 별표 6과 같다.<개정 2014.11.28>

제62조(수신거부 또는 수신동의 철회용 무료전화서비스 등의 제공) 법 제50조제6항에 따라 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 자는 별표 6에서 정하는 바에

따라 수신거부 및 수신동의 철회용 무료전화서비스 등을 해당 정보에 명시하여 수신자에게 이를 제공하여야 한다. <개정 2011.3.29, 2014.11.28>

제62조의2(수신동의 등 처리 결과의 통지) 법 제50조제7항에 따라 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하려는 자는 수신자가 수신동의, 수신거부 또는 수신동의 철회 의사를 표시한 날부터 14일 이내에 다음 각 호의 사항을 해당 수신자에게 알려야 한다.

1. 전송자의 명칭
2. 수신자의 수신동의, 수신거부 또는 수신동의 철회 사실과 해당 의사를 표시한 날짜
3. 처리 결과

[본조신설 2014.11.28]

제62조의3(수신동의 여부의 확인) ① 법 제50조제1항 또는 제3항에 따라 수신자의 사전 동의를 받은 자는 같은 조 제8항에 따라 그 수신동의를 받은 날부터 2년마다(매 2년이 되는 해의 수신동의를 받은 날과 같은 날 전까지를 말한다) 해당 수신자의 수신동의 여부를 확인하여야 한다.

② 제1항에 따라 수신동의 여부를 확인하려는 자는 수신자에게 다음 각 호의 사항을 밝혀야 한다.

1. 전송자의 명칭
2. 수신자의 수신동의 사실과 수신에 동의한 날짜
3. 수신동의에 대한 유지 또는 철회의 의사를 표시하는 방법

[본조신설 2014.11.28]

제63조(영리목적의 광고성 프로그램 등의 설치 제한 장치) 법 제50조의5 전단에서 "대통령령으로 정하는 정보처리장치"란 휴대인터넷ㆍ휴대전화 등과 같이 정보통신망에 연결되어 정보를 송수신 할 수 있는 정보처리장치를 말한다. <개정 2011.8.29>

제64조(영리목적의 광고성 정보전송차단 소프트웨어 등 개발 지원) ① 방송통신위원회는 법 제50조의6에 따라 법 제50조를 위반하여 전송되는 영리목적의 광고성 정보를 편리하게 차단하거나 신고할 수 있는 소프트웨어나 컴퓨터프로그램(이하 "광고차단ㆍ신고 소프트웨어등"이라 한다)을 개발ㆍ보급하는 공공기관ㆍ법인ㆍ단체 등에 대하여 예산의 범위에서 해당 사업비의 전부 또는 일부를 지원할 수 있다.

② 방송통신위원회는 정보통신서비스 제공자등 및 이용자에게 제1항에 따라 개발된 광고차단ㆍ신고 소프트웨어등을 사용하도록 권고할 수 있다.<개정 2009.1.28>

제65조(인터넷진흥원의 운영 등) ① 미래창조과학부장관, 행정자치부장관 또는 방송통신위원회는 법 제52조제3항 각 호에 따른 인터넷진흥원의 업무와 관련 있는 공무원의 파견근무를 관계 기관의 장에게 요청할 수 있다. <개정 2010.10.1, 2013.3.23, 2014.11.19>

② 제1항에 따라 공무원을 파견한 관계 기관의 장이 파견된 자에 대하여 파견근무기간 중 복귀시켜야 할 경우에는 미리 파견을 요청한 기관의 장과 협의하여야 한다.

③ 인터넷진흥원의 장은 미래창조과학부장관, 행정자치부장관 또는 방송통신위원회의 승인을 받아 법 제52조제3항제4호에 따른 업무 중 일부를 정보통신 관련 연구기관이 수행하도록 할 수 있다.<개정 2010.10.1, 2013.3.23, 2014.11.19>

④ 인터넷진흥원의 장은 법 제52조제3항에 따른 업무를 수행할 때 해당 업무가 공공기관의 정보보호와 관련되는 경우에는 관계기관의 장의 승인을 받아야 한다.<개정 2010.10.1>

[제목개정 2010.10.1]

제66조(개인정보침해신고센터의 운영) ① 법 제52조제3항제9호에 따른 개인정보침해 신고센터(이하 "개인정보침해신고센터"라 한다)는 다음 각 호의 업무를 수행한다. <개정 2009.1.28>

1. 개인정보 침해방지 및 보호와 관련한 법 제64조제10항에 따른 기술적 자문과 그 밖에 필요한 지원
2. 개인정보 침해 및 광고성 정보전송과 관련한 고충처리 및 상담
3. 개인정보 침해 관련 대책 연구
4. 개인정보 침해방지를 위한 교육 및 홍보
5. 제1호부터 제4호까지에 따른 업무와 관련되는 사업

② 방송통신위원회는 개인정보의 보호와 관련하여 법 제64조제1항 및 제3항에 따른 정보통신서비스 제공자등에 대한 관계 물품·서류 등의 제출요구 및 검사업무를 효율적으로 수행하기 위하여 필요한 경우에는 「국가공무원법」 제32조의4에 따라 소속 공무원을 인터넷진흥원에 파견할 수 있다.<개정 2008.3.28, 2009.1.28, 2010.10.1, 2011.9.29>

제6장의2 통신과금서비스 <신설 2008.3.28>

제66조의2(등록요건) ① 법 제53조에 따라 통신과금서비스제공자로 등록하려는 자는 다음 각 호의 요건을 모두 갖추어야 한다. <개정 2013.3.23>

1. 자기자본, 출자총액 또는 기본재산에 대한 부채총액의 비율이 100분의 200 이내의 범위에서 미래창조과학부장관이 정하여 고시하는 비율 이하일 것. 이 경우 대주주가 「독점규제 및 공정거래에 관한 법률」 제2조제2호에 따른 기업집단(같은 법 시행령 제17조제1항제1호 및 제2호에 해당하는 기업집단은 제외한다)에 속하는 회사이면 그 기업집단을 기준으로 계산하되, 그 기업집단에 속하는 회사 중 금융업 또는 보험업을 영위하는 회사는 제외하고 계산한다.
2. 업무를 수행할 수 있는 다음 각 목의 인력과 물적 설비를 모두 갖출 것
   가. 전산업무 종사경력이 2년 이상인 5명 이상의 임직원
   나. 통신과금서비스를 원활하게 제공하는 데 필요한 전산설비와 각종 컴퓨터프로그램
   다. 법 제57조제2항에 따른 정보보호시스템
3. 자본금, 출자총액 또는 기본재산이 제2항에 따른 금액 이상일 것

② 법 제53조제2항에서 "대통령령으로 정하는 금액"이란 10억원을 말한다.

[본조신설 2008.3.28]

제66조의3(등록절차) ① 법 제53조에 따라 통신과금서비스제공자로 등록하려는 자는 다음 각 호의 사항이 포함된 등록신청서를 미래창조과학부장관에게 제출하여야 한다. <개정 2013.3.23>

1. 상호 및 주된 사무소의 소재지
2. 대표자의 성명
3. 자본금, 출자총액 또는 기본재산
4. 출자자(미래창조과학부장관이 정하여 고시하는 소액출자자는 제외한다)의 성명 또는 명칭과 그 지분율

② 제1항의 등록신청서에는 다음 각 호의 서류를 첨부하여야 한다.

1. 정관
2. 제66조의2에 따른 등록요건을 갖추었음을 증명할 수 있는 서류
3. 업무개시 후 3년간의 사업계획서(추정 재무제표와 예상수지계산서를 포함한다)
4. 통신과금서비스이용자보호계획서(제66조의7부터 제66조의9까지의 사항을 포함하여야 한다)

③ 제1항에 따라 등록신청서를 제출받은 미래창조과학부장관은 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 법인 등기사항증명서를 확인하여야 한다.<개정 2010.5.4, 2010.11.2, 2013.3.23>

④ 미래창조과학부장관은 제1항 및 제2항에 따라 제출받은 서류에 흠결이 있으면 신청인에게 서류를 제출받은 날부터 10일 이내에 보완하여 제출할 것을 요청할 수 있다.<개정 2013.3.23>

⑤ 미래창조과학부장관은 통신과금서비스제공자의 등록을 한 때에는 그 내용을 관보에 공고하고 인터넷 등을 통하여 일반인에게 알려야 한다.<개정 2013.3.23>

[본조신설 2008.3.28]

제66조의4(등록의 결격사유) 법 제54조제1호에서 "대통령령으로 정하는 출자자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다. <개정 2008.7.29>

1. 해당 법인의 의결권 있는 발행주식 또는 출자지분(이하 이 조에서 "주식등"이라 한다)을 기준으로 본인과 「자본시장과 금융투자업에 관한 법률 시행령」 제8조 각 호의 어느 하나에 해당하는 특수관계인이 누구의 명의로 하든지 자기의 계산으로 소유하는 주식등을 합하여 그 수가 가장 많은 경우의 그 본인
2. 누구의 명의로 하든지 자기의 계산으로 해당 법인의 주식등의 100분의 10 이상을 소유하는 자 또는 임원의 임면 등의 방법으로 그 법인의 주요 경영사항에 대하여 사실상의 영향력을 행사하는 주주로서 「자본시장과 금융투자업에 관한 법률 시행령」 제8조 각 호의 어느 하나에 해당하는 특수관계인

[본조신설 2008.3.28]

제66조의5(행정처분) ① 삭제 <2015.12.22>

② 미래창조과학부장관은 법 제55조에 따라 통신과금서비스제공자의 등록을 취소하려는 경우에는 청문을 실시하여야 한다.<개정 2013.3.23>

③ 미래창조과학부장관은 법 제55조에 따라 통신과금서비스제공자의 등록을 취소한 경우에는 그 내용을 관보에 공고하고 인터넷 등을 통하여 일반인에게 알려야 한다.<개정 2013.3.23>

[본조신설 2008.3.28]

제66조의6(통신과금서비스의 안정성·신뢰성 확보를 위한 필요 조치) 통신과금서비스를 통한 거래의 안정성과 신뢰성을 확보하기 위하여 통신과금서비스제공자가 법 제57조제2항에 따라 하여야 하는 관리적 조치와 기술적 조치는 별표 7과 같다.

[본조신설 2008.3.28]

제66조의7 삭제 <2011.8.29>

제66조의8(거래기록의 보존기간 및 약관 변경 방법) ① 통신과금서비스제공자는 법 제58조제4항 및 제7항에 따라 다음 각 호의 사항에 관한 기록을 해당 거래를 한 날부터 1년간 보존하여야 한다. 다만, 건당 거래 금액이 1만원을 초과하는 거래인 경우에는 5년간 보존하여야 한다.<개정 2011.8.29, 2013.3.23, 2014.11.28>

1. 통신과금서비스를 이용한 거래의 종류
2. 거래금액
3. 통신과금서비스를 통한 구매·이용의 거래 상대방(통신과금서비스를 이용하여 그 대가를 받고 재화 또는 용역을 판매·제공하는 자를 말한다)
4. 거래일시
5. 대금을 청구·징수하는 전기통신역무의 가입자번호
6. 해당 거래와 관련한 전기통신역무의 접속에 관한 사항
7. 거래의 신청 및 조건의 변경에 관한 사항
8. 거래의 승인에 관한 사항
9. 그 밖에 미래창조과학부장관이 정하여 고시하는 사항

② 제1항에 따른 거래기록은 서면, 마이크로필름, 디스크, 자기테이프, 그 밖의 전산정보처리조직에 의하여 보존하여야 한다. 다만, 디스크, 자기테이프, 그 밖의 전산정보처리조직에 의하여 보존하는 경우에는 「전자문서 및 전자거래 기본법」 제5조제1항 각 호의 요건을 모두 갖추어야 한다.<개정 2012.8.31>

③ 통신과금서비스제공자(법 제2조제1항제10호가목의 업무를 제공하는 자로 한정한다)는 법 제58조제6항에 따라 약관을 변경하는 때에는 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 통신과금서비스이용자에게 통지하여야 한다.<신설 2014.11.28>

④ 통신과금서비스이용자는 변경되는 약관에 대하여 제3항에 따른 통지를 받은 날부터 변경되는 약관의 시행일 전의 영업일까지 이의를 제기할 수 있다.<신설 2014.11.28>

[본조신설 2008.3.28]

[제목개정 2014.11.28]

제66조의9(이의신청 및 권리구제를 위한 절차) ① 통신과금서비스제공자는 법 제59조제2항에 따른 이의신청 및 권리구제를 위하여 통신과금서비스이용자 보호책임자 및 담당자를 지정하고, 그 연락처(전화번호, 모사전송번호, 전자우편주소 등을 말한다)를 인터넷 등을 통하여 통신과금서비스이용자에게 알려야 한다.

② 통신과금서비스이용자는 서면(전자문서를 포함한다), 전화, 모사전송 등을 통하여 통신과금서비스제공자에게 통신과금서비스와 관련된 이의신청을 할 수 있다.

③ 통신과금서비스제공자는 제2항에 따른 이의신청을 받은 날부터 2주일 이내에 그 조사 또는 처리 결과를 통신과금서비스이용자에게 알려야 한다.

[본조신설 2008.3.28]

제6장의3 국제협력 <신설 2008.3.28>

제67조(개인정보 국외 이전시 보호조치) ① 법 제63조제2항 단서에서 "전자우편 등 대통령령으로 정하는 방법"이란 전자우편、서면、모사전송、전화 또는 이와 유사한 방법 중 어느 하나의 방법을 말한다. <신설 2016.9.22>

② 법 제63조제4항에 따라 개인정보를 국외로 이전하는 경우에 하여야 하는 보호조치는 다음 각 호와 같다.<개정 2008.3.28, 2016.9.22>

1. 제15조에 따른 개인정보보호를 위한 기술적、관리적 조치
2. 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 사항
3. 그 밖에 이용자의 개인정보 보호를 위하여 필요한 조치

③ 정보통신서비스 제공자등은 제2항 각 호의 사항을 개인정보를 국외에서 이전받는 자와 미리 협의하고, 이를 계약내용 등에 반영하여야 한다.<개정 2009.1.28, 2016.9.22>

제7장 보칙

제68조(자료제출 등) 법 제64조제1항제3호에서 "이용자 보호를 위하여 필요한 경우로서 대통령령으로 정하는 경우"란 다음 각 호의 어느 하나에 해당하는 경우를 말한다. <개정 2008.3.28, 2011.8.29>

1. 법 제41조제1항 각 호의 청소년보호를 위한 시책의 마련을 위하여 필요한 경우
2. 법 제42조의3제3항의 청소년보호책임자의 청소년보호업무 수행 여부를 확인하기 위하여 필요한 경우
3. 삭제 <2012.8.17>

제68조의2(시정조치의 명령의 공표방법 등) ① 미래창조과학부장관 또는 방송통신위원회는 법 제64조제4항에 따라 정보통신서비스 제공자등에게 시정조치의 명령을 받은 사실의 공표를 명하는 때에는 다음 각 호의 사항을 고려하여 공표의 내용·횟수·매체 및 지면의 크기 등을 정하여 이를 명하여야 한다. <개정 2011.9.29, 2013.3.23>

1. 위반행위의 내용 및 정도
2. 위반행위의 기간 및 횟수

② 미래창조과학부장관 또는 방송통신위원회는 제1항에 따라 시정조치의 명령을 받은 사실의 공표를 명할 때에는 해당 정보통신서비스 제공자등과 공표 문안 등에 관하여 협의할 수 있다. <개정 2011.9.29, 2013.3.23>

[본조신설 2009.1.28]

제69조(시정명령의 공개) ① 법 제64조에 따른 시정조치를 명한 사실의 공개는 다음 각 호의 어느 하나에 해당하는 경우에 할 수 있다. 이 경우 미래창조과학부장관 또는 방송통신위원회는 해당 정보통신서비스 제공자등에게 그 사실을 미리 알려야 한다. <개정 2008.3.28, 2009.1.28, 2011.9.29, 2013.3.23>

1. 법 제71조부터 제74조까지의 규정에 해당하는 행위로 시정명령을 받은 경우
2. 연 2회 이상 시정명령을 받은 경우

② 제1항에 따른 시정명령의 공개는 인터넷 홈페이지 또는 「신문 등의 진흥에 관한 법률」에 따라 전국을 보급지역으로 하는 일반일간신문 등에 게재하는 방법으로 한다.<개정 2010.1.27>

제69조의2(과징금의 산정기준 등) ① 법 제64조의3제1항 각 호 외의 부분 본문에서 "위반행위와 관련한 매출액"이란 해당 정보통신서비스 제공자등의 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도의 연평균 매출액을 말한다. 다만, 해당 사업연도 초일 현재 사업을 개시한지 3년이 되지 아니하는 경우에는 그 사업개시 후 직전 사업연도 말일까지의 매출액을 연평균 매출액으로 환산한 금액을 말하며, 해당 사업연도에 사업을 개시한 경우에는 사업개시일부터 위반행위일까지의 매출액을 연매출액으로 환산한 금액을 말한다. <개정 2012.8.17>

② 법 제64조의3제2항 단서에서 "대통령령으로 정하는 경우"란 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 영업을 개시하지 아니하거나 영업을 중단하는 등의 사유로 영업실적이 없는 경우
2. 재해 등으로 인하여 매출액 산정자료가 소멸되거나 훼손되는 등 객관적인 매출액의 산정이 곤란한 경우

③ 방송통신위원회는 제1항에 따른 매출액 산정을 위하여 재무제표 등 자료가 필요한 경우 20일 이내의 기간을 정하여 해당 정보통신서비스 제공자등에게 관련 자료의 제출을 요청할 수 있다.<개정 2012.8.17>

④ 법 제64조의3제4항에 따른 과징금의 산정기준과 산정절차는 별표 8과 같다.<신설 2010.10.1, 2014.11.28>

[본조신설 2009.1.28]

제69조의3(과징금의 부과 및 납부) ① 방송통신위원회가 법 제64조의3에 따라 과징금을 부과하려는 경우에는 해당 위반행위를 조사·확인한 후 위반사실·부과금액·이의제기방법 및 이의제기기간 등을 서면으로 명시하여 이를 납부할 것을 과징금 부과대상자에게 통지하여야 한다.

② 제1항에 따라 통지를 받은 자는 통지를 받은 날부터 20일 이내에 방송통신위원회가 지정하는 금융기관에 과징금을 납부하여야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 그 기간 내에 과징금을 납부할 수 없는 경우에는 그 사유가 없어진 날부터 7일 이내에 납부하여야 한다.

③ 제2항에 따라 과징금의 납부를 받은 금융기관은 과징금을 납부한 자에게 영수증을 발급하여야 한다.

[본조신설 2009.1.28]

제70조(권한의 위임·위탁) ① 미래창조과학부장관 또는 방송통신위원회는 법 제65조제1항에 따라 다음 각 호에 해당하는 자에 대한 법 제76조에 따른 과태료 부과·징수의 권한을 중앙전파관리소장에게 위임·위탁한다. <개정 2008.3.28, 2008.7.3, 2010.10.1, 2013.3.23, 2014.11.28>

1. 「전기통신사업법」 제21조제1항에 따른 별정통신사업의 등록을 한 자(이하 "별정통신사업자"라 한다)
2. 법 제45조의3제1항 단서에 따라 정보보호 최고책임자를 지정하고 신고하여야 하는 자
3. 법 제53조제1항에 따라 통신과금서비스제공자로 등록을 한 자

② 방송통신위원회는 법 제65조제1항에 따라 법 제22조부터 제32조까지의 규정을 위반한 사실을 확인하기 위한 법 제64조제1항 및 제3항에 따른 자료제출 요구 및 검사에 관한 권한(개인정보 침해와 관련하여 중앙전파관리소장에게 접수된 사항만 해당한다)을 중앙전파관리소장에게 위탁한다.<신설 2012.8.17, 2013.3.23>

③ 방송통신위원회는 법 제65조제1항에 따라 별정통신사업자 외의 자(제2호의 경우에는 제1항 각 호 외의 자)에 대한 다음 각 호의 권한(법 제50조, 제50조의3부터 제50조의5까지 및 제50조의7에 관한 사항만 해당한다)을 중앙전파관리소장에게 위탁한다.<개정 2008.3.28, 2008.7.3, 2011.9.29, 2012.8.17, 2013.3.23, 2014.11.28>

1. 법 제64조제4항에 따른 시정조치의 명령
2. 법 제76조에 따른 과태료 부과·징수

④ 방송통신위원회는 법 제65조제3항에 따라 다음 각 호의 업무를 인터넷진흥원의 장에게 위탁한다.<개정 2008.3.28, 2010.10.1, 2011.9.29, 2012.8.17, 2014.11.28>

1. 법 제22조부터 제32조까지의 규정을 위반한 사실을 확인하기 위한 법 제64조제1항 및 제3항에 따른 자료제출 요구 및 검사에 관한 업무(개인정보 침해와 관련하여 인터넷진흥원에 접수된 고충처리 및 상담사항만 해당한다)

2. 법 제50조, 제50조의3부터 제50조의5까지, 제50조의7 및 제50조의8을 위반한 사실을 확인하기 위한 법 제64조제1항부터 제3항까지의 규정에 따른 자료제출 요구 및 검사에 관한 업무(광고성 정보 전송행위와 관련하여 인터넷진흥원에 접수된 고충처리 및 상담사항만 해당한다)

⑤ 미래창조과학부장관은 법 제65조제1항에 따라 다음 각 호의 권한을 중앙전파관리소장에게 위임한다.<신설 2014.11.28, 2015.12.22>

1. 법 제45조의3에 따른 정보보호 최고책임자 지정의 신고
2. 법 제53조제1항에 따른 통신과금서비스제공자 등록
3. 법 제53조제4항에 따른 통신과금서비스제공자의 변경등록, 사업의 양도·양수 또는 합병·상속, 사업의 승계 및 사업의 휴지·폐지·해산의 신고
4. 법 제55조제1항에 따른 통신과금서비스제공자에 대한 등록취소
5. 법 제56조제1항에 따른 통신과금서비스에 관한 약관의 신고(변경신고를 포함한다)
6. 법 제56조제2항에 따른 통신과금서비스제공자에 대한 약관변경의 권고
7. 법 제61조에 따른 통신과금서비스 제공 거부, 정지 또는 제한의 명령
8. 법 제53조부터 제61조까지의 규정을 위반한 사실을 확인하기 위한 법 제64조제1항 및 제3항에 따른 자료제출 요구와 검사
9. 법 제53조제1항에 따라 통신과금서비스제공자로 등록을 한 자에 대한 법 제64조제4항에 따른 시정조치의 명령

제70조의2(고유식별정보의 처리) 미래창조과학부장관 또는 방송통신위원회(제70조에 따라 방송통신위원회의 권한을 위탁받은 자를 포함한다)는 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제19조제1호 또는 제4호에 따른 주민등록번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

1. 법 제64조제1항부터 제3항까지의 규정에 따른 자료 등의 제출 요구, 열람, 검사 등에 관한 사무
2. 법 제64조의3에 따른 과징금 부과·징수에 관한 사무

[본조신설 2014.8.6]

제71조(규제의 재검토) ① 미래창조과학부장관 또는 방송통신위원회는 제74조에 따른 과태료의 부과기준에 대하여 2017년 1월 1일을 기준으로 3년마다(매 3년이 되는 해의 기준일과 같은 날 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 하여야 한다. <개정 2016.12.30>

② 미래창조과학부장관은 다음 각 호의 사항에 대하여 다음 각 호의 기준일을 기준으로 3년마다(매 3년이 되는 해의 기준일과 같은 날 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.<개정 2016.12.30>

1. 제37조에 따른 집적정보통신시설사업자의 보호조치: 2017년 1월 1일

2. 제38조에 따른 보험가입 의무와 최저보험금액: 2017년 1월 1일
3. 제49조에 따른 정보보호 관리체계 인증 대상자의 범위: 2014년 1월 1일
4. 제51조에 따른 인증의 사후관리: 2017년 1월 1일
5. 제53조에 따른 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관의 지정기준: 2017년 1월 1일
6. 제53조의2에 따른 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관의 지정절차: 2017년 1월 1일
7. 제66조의2에 따른 통신과금서비스제공자 등록요건: 2014년 1월 1일
8. 제66조의8에 따른 거래기록의 보존기간 및 방법: 2014년 1월 1일

③ 삭제 <2016.12.30>

④ 방송통신위원회는 다음 각 호의 사항에 대하여 다음 각 호의 기준일을 기준으로 3년마다(매 3년이 되는 해의 기준일과 같은 날 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.<개정 2014.11.28>

1. 제12조에 따른 동의를 얻는 방법: 2015년 1월 1일
2. 제17조에 따른 개인정보 이용내역을 통지하여야 하는 자의 범위, 통지하여야 하는 정보의 종류 및 통지 주기와 방법: 2015년 1월 1일
3. 제25조에 따른 청소년보호책임자 지정의무자의 범위: 2015년 1월 1일
4. 제27조에 따른 청소년보호책임자의 지정기한: 2015년 1월 1일
5. 삭제 <2016.12.30>

[본조신설 2013.12.30]

제72조 삭제 <2010.12.27>

제73조 삭제 <2009.8.18>

제74조(과태료의 부과기준) 법 제76조제1항부터 제3항까지의 규정에 따른 과태료의 부과기준은 별표 9와 같다.

[전문개정 2010.10.1]

부칙 <제20668호,2008.2.29>

제1조(시행일) 이 영은 공포한 날부터 시행한다.

제2조(다른 법령과의 관계) 이 영 시행 당시 다른 법령에서 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙」 또는 그 규정을 인용하고 있는 경우 이 영 중 그에 해당하는 규정이 있는 경우에는 종전의 규정에 갈음하여 이 영 또는 이 영의 해당 규정을 인용한 것으로 본다.

부칙 <제20756호,2008.3.28>

이 영은 공포한 날부터 시행한다.

부칙 <제20896호,2008.7.3>(방송통신위원회와 그 소속기관 직제)

제1조(시행일) 이 영은 공포한 날부터 시행한다.

제2조(다른 법령의 개정) ① 및 ② 생략

③ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제70조제1항 중 "행정안전부장관 또는 방송통신위원회"를 "방송통신위원회"로, "체신청장에게 위탁"을 "중앙전파관리소장에게 위임"으로 하고, 같은 조 제2항 각 호 외의 부분 중 "체신청장에게 위탁"을 "중앙전파관리소장에게 위임"으로 한다.

④ 부터 ⑥ 까지 생략

부칙 <제20947호,2008.7.29>(자본시장과 금융투자업에 관한 법률 시행령)

제1조(시행일) 이 영은 2009년 2월 4일부터 시행한다. <단서 생략>

제2조부터 제25조까지 생략

제26조(다른 법령의 개정) ① 부터 <89> 까지 생략

<90> 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제66조의4제1호 및 같은 조 제2호 중 "「증권거래법 시행령」 제2조의8"을 "「자본시장과 금융투자업에 관한 법률 시행령」 제8조"로 한다.

<91> 부터 <113> 까지 생략

제27조 및 제28조 생략

부칙 <제21278호,2009.1.28>

제1조(시행일) 이 영은 공포한 날부터 시행한다. 다만, 제15조제4항제2호 및 제4호의 개정규정은 공포 후 1년이 경과한 날부터 시행한다.

제2조(고시에 대한 준비행위) 부칙 제1조 단서에도 불구하고 제15조제6항의 개정규정에 따른 고시에는 제15조제4항제2호 및 제4호의 개정규정에 따른 기준을 포함하여 고시할 수 있다.

부칙 <제21692호,2009.8.18>

제1조(시행일) 이 영은 2009년 8월 23일부터 시행한다.

제2조부터 제4조까지 생략

제5조(다른 법령의 개정) ① 부터 <23> 까지 생략

<24> 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제4조, 제5조 및 제73조를 각각 삭제한다.

<25> 부터 <28> 까지 생략

제6조 생략

부칙 <제21719호,2009.9.9>

제1조(시행일) 이 영은 2009년 9월 10일부터 시행한다.

제2조 생략

제3조(다른 법령의 개정) ① 부터 ⑬ 까지 생략

⑭ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제71조제2호 중 "「항공법」 제2조제26호"를 "「항공법」 제2조제31호"로 한다.

⑮ 부터 <17> 까지 생략

부칙 <제22003호,2010.1.27>

제1조(시행일) 이 영은 2010년 2월 1일부터 시행한다.

제2조 및 제3조 생략

제4조(다른 법령의 개정) ① 부터 <37> 까지 생략

<38> 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제11조제3항 및 제69조제2항 중 "「신문 등의 자유와 기능보장에 관한 법률」"을 각각 "「신문 등의 진흥에 관한 법률」로 한다.

<39> 부터 <45> 까지 생략

제5조 생략

부칙 <제22151호,2010.5.4>

제1조(시행일) 이 영은 2010년 5월 5일부터 시행한다.

제2조 및 제3조 생략

제4조(다른 법령의 개정) ① 부터 <150> 까지 생략

<151> 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제6조제1항 후단을 삭제한다.

제46조제2항 본문, 제48조제2항 본문 및 제66조의3제3항 본문 중 "「전자정부법」 제21조제1항"을 각각 "「전자정부법」 제36조제1항"으로 한다.

<152> 부터 <192> 까지 생략

부칙 <제22423호,2010.10.1>

제1조(시행일) 이 영은 공포한 날부터 시행한다.

제2조(행정처분기준에 관한 경과조치) ① 이 영 시행 전의 위반행위에 대하여 행정처분기준(과징금 부과기준을 포함한다)을 적용할 때에는 별표 4 및 별표 8의 개정규정에도 불구하고 종전의 규정에 따른다.

② 이 영 시행 전의 위반행위로 받은 행정처분은 별표 4의 개정규정에 따른 위반행위의 횟수 산정에 포함한다.

제3조(과태료에 관한 경과조치) ① 이 영 시행 전의 위반행위에 대하여 과태료를 적용할 때에는 별표 9의 개정규정에도 불구하고 종전의 예에 따른다.

② 이 영 시행 전의 위반행위로 받은 과태료 부과처분은 별표 9의 개정규정에 따른 위반행위의 횟수 산정에 포함한다.

부칙 <제22424호,2010.10.1>

제1조(시행일) 이 영은 공포한 날부터 시행한다.

제2조부터 제9조까지 생략

제10조(다른 법령의 개정) ①부터 ⑮까지 생략

<16> 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제9조제1항제3호 중 "「전기통신사업법」 제2조제1항제2호"를 "「전기통신사업법」 제2조제8호"로 한다.

제70조제1항 중 "「전기통신사업법」 제19조제1항"을 "「전기통신사업법」 제21조제1항"으로 한다.

<17>부터 <20>까지 생략

부칙 <제22467호,2010.11.2>

이 영은 공포한 날부터 시행한다.

부칙 <제22550호,2010.12.27>

제1조(시행일) 이 영은 공포한 날부터 시행한다. <단서 생략>

제2조부터 제5조까지 생략

제6조(다른 법령의 개정) ①부터 ③까지 생략

④ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제72조를 삭제한다.

⑤부터 ⑧까지 생략

부칙 <제22773호,2011.3.29>

이 영은 공포한 날부터 시행한다.

부칙 <제23104호,2011.8.29>

이 영은 공포한 날부터 시행한다.

부칙 <제23169호,2011.9.29>

제1조(시행일) 이 영은 2011년 9월 30일부터 시행한다. <단서 생략>

제2조부터 제6조까지 생략

제7조(다른 법령의 개정) ①부터 ⑤까지 생략

⑥ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제3조제1항 중 "정보통신서비스 제공자 및 제71조에 따른 정보통신서비스 제공자 외의 자"를 "정보통신서비스 제공자"로 한다.

제16조부터 제22조까지를 각각 삭제한다.

제36조제6항을 삭제한다.

제66조제2항 중 "정보통신서비스 제공자등(법 제67조에 따라 준용되는 경우에 해당되는 자를 포함한다)"을 "정보통신서비스 제공자등"으로 한다.

제71조를 삭제한다.

제3조제1항ㆍ제2항, 제66조제2항, 제68조의2제1항 각 호 외의 부분, 같은 조 제2항, 제69조제1항 각 호 외의 부분 후단, 제70조제2항 각 호 외의 부분, 같은 조 제3항 각 호 외의 부분 및 별표 9 위반행위란의 제12호 각 목 외의 부분 중 "행정안전부장관 또는 방송통신위원회"를 각각 "방송통신위원회"로 한다.

제8조 생략

부칙 <제23876호,2012.6.25>

이 영은 공포한 날부터 시행한다.

부칙 <제24047호,2012.8.17>

제1조(시행일) 이 영은 2012년 8월 18일부터 시행한다. 다만, 제15조제2항, 제36조의2부터 제36조의6까지, 제39조부터 제49조까지, 제51조부터 제53조까지, 제53조의2부터 제53조의4까지, 제54조의2, 제55조의2부터 제55조의5까지, 별표 2, 별표 3, 별표 9 중 제2호어목·저목 및 부칙 제3조의 개정규정은 2013년 2월 18일부터 시행한다.

제2조(미이용 기간의 기산에 관한 적용례) 제16조제1항의 개정규정에 따른 기간은 2012년 8월 18일 이후 정보통신서비스를 이용하지 아니하는 경우부터 기산한다.

제3조(다른 법령의 개정) 지능형전력망의 구축 및 이용촉진에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제16조제1호를 삭제한다.

부칙 <제24076호,2012.8.31>

제1조(시행일) 이 영은 2012년 9월 2일부터 시행한다. <단서 생략>

제2조 생략

제3조(다른 법령의 개정) ①부터 ⑪까지 생략

⑫ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제66조의8제2항 단서 중 "「전자거래기본법」"을 "「전자문서 및 전자거래 기본법」"으로 한다.

⑬부터 <16>까지 생략

제4조 생략

부칙 <제24102호,2012.9.14>

제1조(시행일) 이 영은 2012년 9월 16일부터 시행한다. <단서 생략>

제2조 생략

제3조(다른 법령의 개정) ①부터 ④까지 생략

⑤ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제25조제2호 중 "「청소년보호법」"을 "「청소년 보호법」"으로 한다.

⑥부터 ⑧까지 생략

제4조 생략

부칙 <제24445호,2013.3.23>

제1조(시행일) 이 영은 공포한 날로부터 시행한다.

제2조 및 제3조 생략

제4조(다른 법령의 개정) ①부터 ⑨까지 생략

⑩ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제7조 각 호 외의 부분 및 제9조제3항 중 "지식경제부장관"을 각각 "미래창조과학부장관"으로 한다.

제9조제2항 중 "지식경제부령"을 "미래창조과학부령"으로 한다.

제36조의2 각 호 외의 부분, 제36조의3제2항, 제36조의4제4항, 제47조제1항 각 호 외의 부분, 같은 조 제2항·제7항, 제52조 전단, 제53조제1항제1호·제2호, 제53조의2제1항제3호, 제55조의2제2항, 제55조의3제5항, 제57조제1호·제3호, 제58조제1호·제3호·제4호, 제59조제1항 각 호 외의 부분, 제66조의2제1항제1호 전단, 제66조의3제1항제4호 및 제66조의8제1항제9호 중 "방송통신위원회가"를 각각 "미래창조과학부장관이"로 한다.

제36조의4제3항 전단 및 제36조의5제1항 중 "방송통신위원회"를 각각 "미래창조과학부장관"으로 한다.

제36조의5제2항 각 호 외의 부분, 제37조제2항·제3항, 제48조제2항, 제53조제2항, 제53조의2제2항·제3항, 같은 조 제4항 전단, 제53조의4제2항, 제66조의3제3항부터 제5항까지 및 제66조의5제2항·제3항 중 "방송통신위원회는"을 각각 "미래창조과학부장관은"으로 한다.

제51조제2항, 제53조의2제1항 각 호 외의 부분, 제53조의4제1항 및 제66조의3제1항 각 호 외의 부분 중 "방송통신위원회에"를 각각 "미래창조과학부장관에게"로 한다.

제65조제1항 중 "방송통신위원회"를 "미래창조과학부장관, 안전행정부장관 또는 방송통신위원회"로 하고, 같은 조 제3항 중 "행정안전부장관 또는 방송통신위원회"를 "미래창조과학부장관, 안전행정부장관 또는 방송통신위원회"로 한다.

제68조의2제1항 각 호 외의 부분, 같은 조 제2항, 제69조제1항 각 호 외의 부분 후단 중 "방송통신위원회"를 각각 "미래창조과학부장관 또는 방송통신위원회"로 한다.

제70조제1항 중 "방송통신위원회"를 "미래창조과학부장관 또는 방송통신위원회"로, "위임"을 "위임·위탁"으로 하고, 같은 조 제2항 중 "위임"을 "위탁"으로 하며, 같은 조 제3항 각 호 외의 부분 중 "위임"을 "위탁"으로 한다.

별표 2 비고 제1호 중 "지식경제부장관 또는 방송통신위원회"를 "미래창조과학부장관 또는 산업통상자원부장관"으로 한다.

별표 5 중 "방송통신위원회"를 "미래창조과학부장관"으로 한다.

별표 7 제3호 중 "방송통신위원회가"를 "미래창조과학부장관이"로 한다.

별표 9 제2호두목1)부터 6)까지의 규정 외의 부분 중 "방송통신위원회"를 "미래창조과학부장관 또는 방송통신위원회"로 한다.

⑪ 및 ⑫ 생략

부칙 <제25050호,2013.12.30>

이 영은 2014년 1월 1일부터 시행한다. <단서 생략>

부칙 <제25532호,2014.8.6>

이 영은 2014년 8월 7일부터 시행한다.

부칙 <제25751호,2014.11.19>

제1조(시행일) 이 영은 공포한 날부터 시행한다. 다만, 부칙 제5조에 따라 개정되는 대통령령 중 이 영 시행 전에 공포되었으나 시행일이 도래하지 아니한 대통령령을 개정한 부분은 각각 해당 대통령령의 시행일부터 시행한다.

제2조부터 제4조까지 생략

제5조(다른 법령의 개정) ①부터 <42>까지 생략

<43> 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제65조제1항 및 제3항 중 "안전행정부장관"을 각각 "행정자치부장관"으로 한다.

<44>부터 <418>까지 생략

부칙 <제25789호,2014.11.28>

제1조(시행일) 이 영은 2014년 11월 29일부터 시행한다. 다만, 제16조제1항 각 호 외의 부분 본문의 개정규정은 2015년 8월 18일부터 시행한다.

제2조(개인정보의 파기 등에 관한 적용례) 제16조제1항 각 호 외의 부분 본문의 개정규정은 2015년 8월 18일 전에 수집하거나 제공받은 개인정보에 대해서도 적용한다.

제3조(수신동의 등 처리 결과의 통지에 관한 적용례) 제62조의2의 개정규정은 이 영 시행 이후 수신자가 수신동의, 수신거부 또는 수신동의 철회 의사를 표시하는 경우부터 적용한다.

제4조(정보보호 최고책임자의 신고에 관한 특례) 이 영 시행 당시 제36조의6의 개정규정의 각 호의 어느 하나에 해당하는 정보통신서비스 제공자는 제36조의7의 개정규정에도 불구하고 이 영 시행일부터 90일 이내에 정보보호 최고책임자 지정신고서를 미래창조과학부장관에게 제출하여야 한다.

제5조(영리목적의 광고성 정보 전송기준에 관한 특례) 이 영 시행 전에 재화등의 거래가 종료된 경우에 대해서 제61조제1항의 개정규정을 적용하는 경우에는 이 영 시행일을 해당 재화등의 거래가 종료된 날로 본다.

제6조(수신동의 여부의 확인에 관한 특례) 이 영 시행 전에 수신동의를 받은 경우에 대해서 제62조의3제1항의 개정규정을 적용하는 경우에는 이 영 시행일에 해당 수신동의를 받은 것으로 본다.

제7조(개인정보의 보호조치에 관한 경과조치) 이 영 시행 전에 종전의 제15조제4항제1호 및 제2호에 따른 보안조치를 한 경우에는 제15조제4항제1호 및 제2호의 개정규정에도 불구하고 종전의 규정에 따른다.

제8조(과징금의 산정기준에 관한 경과조치) 이 영 시행 전의 위반행위에 대하여 과징금을 부과할 때에는 별표 8의 개정규정에도 불구하고 종전의 규정에 따른다.

제9조(과태료에 관한 경과조치) ① 이 영 시행 전의 위반행위에 대하여 과태료의 부과기준을 적용할 때에는 별표 9의 개정규정에도 불구하고 종전의 규정에 따른다.

② 이 영 시행 전의 위반행위로 받은 과태료 부과처분은 별표 9의 개정규정에 따른 위반행위의 횟수 산정에 포함한다.

부칙 <제26757호,2015.12.22>

제1조(시행일) 이 영은 2015년 12월 23일부터 시행한다.

제2조(과태료에 관한 경과조치) 이 영 시행 전의 위반행위로 종전의 별표 9 제2호아목에 따라 받은 과태료 부과처분은 별표 9 제2호바목의 개정규정에 따른 위반행위의 횟수 산정에 포함하지 아니한다.

부칙 <제27188호,2016.5.31>

이 영은 2016년 6월 2일부터 시행한다. 다만, 제16조의 개정규정은 공포한 날부터 시행한다.

부칙 <제27510호,2016.9.22>

제1조(시행일) 이 영은 2016년 9월 23일부터 시행한다. 다만, 제16조제2항 단서의 개정규정은 공포 후 1년이 경과한 날부터 시행한다.

제2조(개인정보의 별도 저장ㆍ관리에 관한 적용례) 제16조제2항 단서의 개정규정은 부칙 제1조 단서에 따른 시행일 전에 수집하거나 제공받은 개인정보에 대해서도 적용한다.

부칙 <제27751호,2016.12.30>

제1조(시행일) 이 영은 2017년 1월 1일부터 시행한다. <단서 생략>

제2조부터 제12조까지 생략

[별표 1] <신설 2011.8.29>

본인확인업무의 정지 및 지정취소 기준(제9조의6제1항 관련)

1. 일반기준

가. 위반행위가 둘 이상인 경우로서 그에 해당하는 각각의 처분기준이 다른 경우에는 그 중 무거운 처분기준에 따른다. 다만, 둘 이상의 처분기준 중 경고가 포함되어 있는 경우에는 경고를 함께 부과할 수 있고, 둘 이상의 처분기준이 모두 업무정지인 경우에는 각 처분기준을 합산한 기간을 넘지 않는 범위에서 무거운 처분기준의 2분의 1의 범위에서 가중할 수 있다.

나. 위반행위의 횟수에 따른 행정처분기준은 최근 1년간 같은 위반행위로 행정처분을 받은 경우에 적용한다. 이 경우 위반행위에 대하여 행정처분을 받은 날과 다시 같은 위반행위로 적발된 날을 각각 기준으로 하여 위반횟수를 계산한다.

다. 처분권자는 다음 각 목에 해당하는 사유를 고려하여 처분을 감경(법 제23조의4제1항제1호 및 제2호에 해당하는 경우는 제외한다)할 수 있다. 이 경우 그 처분이 업무정지인 경우에는 그 처분기준의 2분의 1의 범위에서 감경할 수 있고, 지정취소인 경우에는 6개월의 업무정지로 감경할 수 있다.

1) 위반행위가 고의나 중대한 과실이 아닌 사소한 부주의나 단순한 오류로 인한 것으로 인정되는 경우

2) 위반의 내용·정도가 경미하여 즉시 시정할 수 있다고 인정되는 경우

3) 업무정지 또는 지정취소 처분으로 다수의 이용자가 대체수단을 이용하는 데 중대한 지장을 초래할 것으로 인정되는 경우

2. 개별기준

위반행위	근거 법조문	위반횟수별 처분기준		
		1차	2차	3차 이상
가. 거짓이나 그 밖의 부정한 방법으로 본인확인기관의 지정을 받은 경우	법 제23조의4제1항제1호	지정취소		
나. 본인확인업무의 정지명령을 받은 자가 그 명령을 위반하여 업무를 정지하지 않은 경우	법 제23조의4제1항제2호	지정취소		
다. 지정받은 날부터 6개월 이내에 본인확인업무를 개시하지 않거나 6개월 이상 계속하여 본인확인업무를 휴지한 경우	법 제23조의4제1항제3호	업무정지 3개월	지정취소	
라. 법 제23조의3제4항에 따른 지정기준에 적합하지 않게 된 경우	법 제23조의4제1항제4호	경고	업무정지 3개월	업무정지 6개월

[별표 1의2] <개정 2011.8.29>

사업자가 가입하여야 하는 책임보험의 최저보험금액(제38조제2항 관련)

적용대상 사업자	최저보험금액
매출액 100억 이상인 사업자	10억원
매출액 10억 이상 100억 미만인 사업자	1억원
매출액 10억 미만인 사업자	5천만원

비 고

"매출액"이란 책임보험에 가입하여야 할 연도의 직전 사업연도의 매출액을 말하고, 직전 사업연도의 매출액이 없거나 매출액 산정이 곤란할 경우에는 해당 사업자가 예측한 향후 1년간의 매출액을 말한다.

[별표 2] <개정 2013.3.23>

정보보호 기술인력의 자격 기준(제36조의4 관련)

1. 유관자격이나 유관학력을 보유한 자로서 다음 각 목의 어느 하나에 해당하는 자
   가. 학사 이상의 학위를 취득한 후 2년 이상의 정보보호 유관경력이 있거나 3년 이상의 정보통신 유관경력이 있는 자
   나. 기사 또는 기술사 자격을 취득한 후 2년 이상의 정보보호 유관경력이 있거나 3년 이상의 정보통신 유관경력이 있는 자
   다. 전문학사 학위를 취득한 후 4년(3년제 전문대학의 경우에는 3년) 이상의 정보보호 유관경력이 있거나 5년(3년제 전문대학의 경우에는 4년) 이상의 정보통신 유관경력이 있는 자
   라. 산업기사의 자격을 취득한 후 4년 이상의 정보보호 유관경력이 있거나 5년 이상의 정보통신 유관경력이 있는 자
2. 다음 각 목의 어느 하나에 해당하는 자
   가. 학사 이상의 학위를 취득한 후 4년 이상의 정보보호 유관경력이 있거나 5년 이상의 정보통신 유관경력이 있는 자
   나. 전문학사 학위를 취득한 후 6년(3년제 전문대학의 경우에는 5년) 이상의 정보보호 유관경력이 있거나 7년(3년제 전문대학의 경우에는 6년) 이상의 정보통신 유관경력이 있는 자
   다. 한국인터넷진흥원의 정보보호관리체계 인증 심사원 또는 정보보호전문가(SIS), 「전자정부법」 제60조에 따른 감리원, 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 공인정보시스템감사사(CISA) 또는 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 공인정보시스템보호전문가(CISSP)의 자격을 취득한 자
   라. 변호사나 공인회계사로서 2년 이상의 정보보호 유관경력이나 3년 이상의 정보통신 유관경력이 있는 자

<비 고>

1. "유관자격"이란 「국가기술자격법 시행규칙」 별표 7에 따라 미래창조과학부장관 또는 산업통상자원부장관 검정의 소관으로 하는 전자계산기, 정보통신, 통신설비, 통신기기, 통신선로, 정보기기운용, 전파통신, 전파전자, 무선설비, 방송통신, 정보관리, 정보처리, 사무자동화 및 전자계산조직응용 종목의 기술자격을 말한다.
2. "유관학력"이란 「고등교육법」에 따른 해당 학교에서 다음 각 목에 해당하는 학과에서 소정의 과정을 이수하고 졸업하거나 그 밖의 관계법령에 따라 국내 또는 외국에서 이와 같은 수준 이상으로 인정되는 학력을 말한다.
   가. 전자 관련 학과: 정보전자, 전자, 전자계산, 전기전자제어, 전자정보, 전자제어, 전기전자, 전자전기정보, 전자컴퓨터전기제어, 컴퓨터과학, 전기전

자정보, 전자컴퓨터, 메카트로닉스, 전자재료, 제어계측, 반도체

나. 정보통신 관련 학과: 전기통신설비, 국제정보통신, 방송설비, 방송통신, 이동통신, 전자통신, 컴퓨터네트워크, 통신, 컴퓨터정보기술, 전파통신, 전기전자통신, 전기전자정보통신, 전자정보통신, 전자제어통신, 전자통신, 전파, 전파통신, 정보통신, 컴퓨터통신, 항공통신정보, 전자정보통신반도체, 전기전자전파, 통신컴퓨터, 무선통신

다. 정보처리기술 관련 학과: 시스템, 전산, 정보전산, 컴퓨터제어, 컴퓨터응용제어, 컴퓨터응용, 컴퓨터응용설계, 구조시스템, 컴퓨터정보, 멀티미디어, 정보시스템, 전산통계, 정보처리

라. 그 밖에 교육과학기술부장관이나 해당 교육기관의 장으로부터 전자·통신 및 정보처리기술·정보보호 관련 학과로 인정받은 학과

3. "정보통신 유관경력"이란 공공기관, 민간기업, 교육기관 등에서 정보통신서비스(기간통신, 별정통신, 부가통신, 방송서비스 등을 말한다), 정보통신기기(정보기기, 방송기기, 부품 등을 말한다) 또는 소프트웨어 및 컴퓨터 관련 서비스(패키지 소프트웨어, 컴퓨터 관련 서비스, 디지털콘텐츠, 데이터베이스 제작 및 검색 등을 말한다)에 해당되는 분야에서 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 수행한 기간을 말한다.

4. "정보보호 유관경력"이란 공공기관, 민간기업, 교육기관 등에서 정보보호를 위한 공통기반기술(암호 기술, 인증 기술 등을 말한다), 시스템·네트워크 보호(시스템 보호, 해킹·바이러스 대응, 네트워크 보호 등을 말한다) 또는 응용서비스 보호(전자거래 보호, 응용서비스 보호, 정보보호 표준화 등을 말한다)에 해당되는 분야에서 계획·분석·설계·개발·운영·유지보수·컨설팅 또는 연구개발 업무 등을 수행한 기간을 말한다.

[별표 3] 삭제 <2012.8.17>

[별표 4] <개정 2016. 5. 31.>

지정취소 및 업무정지에 관한 행정처분의 기준(제54조 관련)

1. 일반기준

가. 위반행위가 둘 이상인 경우로서 그에 해당하는 각각의 처분기준이 다른 경우에는 그 중 무거운 처분기준에 따른다. 다만, 둘 이상의 처분기준이 같은 업무정지인 경우에는 각 처분기간을 합산한 기간을 넘지 않는 범위에서 무거운 처분기준의 2분의 1까지 가중(가중하는 경우에도 1년을 초과할 수 없다. 이하 같다)할 수 있다.

나. 위반행위의 횟수에 따른 행정처분기준은 최근 2년간 같은 위반행위로 행정처분을 하는 경우에 적용한다. 이 경우 위반행위에 대하여 행정처분을 한 날과 다시 같은 위반행위를 적발한 날을 각각 기준으로 하여 위반횟수를 계산한다.

다. 처분권자는 다음의 사유를 고려하여 처분을 가중하거나 감경(법 제47조의2제1항제1호 및 제2호에 해당하는 경우는 제외한다)할 수 있다. 이 경우 그 처분이 업무정지인 경우에는 처분기준의 2분의 1의 범위에서 가중하거나 감경할 수 있고, 지정취소인 경우에는 6개월의 업무정지로 감경할 수 있다.

1) 가중 사유

가) 위반행위가 사소한 부주의나 단순한 오류가 아닌 고의나 중대한 과실에 따른 것으로 인정되는 경우

나) 위반의 내용과 정도가 중대하여 정보보호 관리체계 운영자 및 정보통신서비스 이용자에게 미치는 피해가 크다고 인정되는 경우

다) 위반행위의 기간 등에 비추어 가중이 필요하다고 인정되는 경우

라) 그 밖에 정보보호 관리체계 업무에 대한 정부 정책상 가중이 필요하다고 인정되는 경우

2) 감경 사유

가) 위반행위가 고의나 중대한 과실이 아닌 사소한 부주의나 단순한 오류로 인한 것으로 인정되는 경우

나) 위반의 내용과 정도가 경미하여 즉시 시정할 수 있다고 인정되는 경우

다) 그 밖에 정보보호 관리체계 업무에 대한 정부 정책상 감경이 필요하다고 인정되는 경우

2. 개별기준

위반행위	근거 법조문	위반횟수별 처분기준		
		1차	2차	3차 이상
가. 거짓이나 그 밖의 부정한 방법으로 정보보호 관리체계 인증기관 또는 정보보호 관리체계 심사기관의 지정을 받은 경우	법 제47조의2제1항제1호	지정취소		
나. 업무정지기간 중에 인증 또는 인증심사를 한 경우	법 제47조의2제1항제2호	지정취소		
다. 정당한 사유 없이 인증 또는 인증심사를 하지 않은 경우	법 제47조의2제1항제3호			
1) 정보보호 관리체계 인증기관 또는 정보보호 관리체계 심사기관으로 지정된 후 3년이 지나도록 정보보호 관리체계 인증실적 또는 인증심사실적이 없는 경우		지정취소		
2) 천재지변, 인증심사원의 부족 등의 사유로 인증 또는 인증심사 업무를 원활하게 수행할 수 없는 경우 등 불가피한 경우가 아님에도 불구하고 인증 또는 인증심사를 거부한 경우		업무정지 1개월	업무정지 2개월	업무정지 3개월
라. 법 제47조제11항을 위반하여 인증 또는 인증심사를 한 경우	법 제47조의2제1항제4호			
1) 인증심사원의 자격요건을 갖추지 않은 자가 인증심사를 수행한 경우		업무정지 3개월	업무정지 6개월	업무정지 9개월
2) 정보보호 관리체계 인증기관 또는 정보보호 관리체계 심사기관이 신청인과 협의 없이 인증의 범위 및 일정을 임의로 정한 경우		업무정지 2개월	업무정지 4개월	업무정지 6개월
3) 제51조에 따른 인증의 사후관리를 실시하지 않은 경우		업무정지 1개월	업무정지 2개월	업무정지 3개월
마. 법 제47조제12항에 따른 지정기준에 적합하지 않게 된 경우	법 제47조의2제1항제5호	업무정지 3개월	업무정지 6개월	지정취소

[별표 5] <개정 2016. 5. 31.>

정보통신망침해사고 민·관합동조사단원 증표 (제60조제2항 관련)

제 호

정보통신망침해사고 민·관합동조사단원증

소 속:
직 위:
성 명:
생년월일:
활동기간: ~

사 진
(2.5cm×3cm)

위 사람은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의4제2항에 따른 정보통신망침해사고 민·관합동조사단원임을 증명합니다.

년 월 일

미래창조과학부장관 [인]

56mm×80mm[보존용지(1종) 120g/㎡]

비 고

1. 규 격: 가로 56mm, 세로 80mm
2. 바탕색: 황 색
3. 복 선: 적 색

[별표 6] <개정 2014.11.28.>

영리목적의 광고성 정보의 명시사항 및 명시방법(제61조제3항 관련)

매체구분	명시사항 및 명시방법
공통	1. (광고)를 표시하는 경우에는 수신자의 수신의 거부 또는 수신동의의 철회를 회피하기 위한 목적으로 빈칸·부호·문자 등을 삽입하거나 표시방법을 조작하는 조치를 해서는 안 된다. 2. 수신자가 수신의 거부 또는 수신동의의 철회를 하는 때에 전송에 이용된 수신자의 연락처 외의 정보를 전송자에게 제공하도록 요구하여 수신거부 또는 수신동의의 철회를 어렵게 해서는 안 된다.
전자우편	1. 제목이 시작되는 부분에 (광고)를 표시해야 한다. 2. 본문에는 다음 사항을 표시해야 한다. 가. 전송자의 명칭·전자우편주소·전화번호 및 주소 나. 수신자가 수신의 거부 또는 수신동의의 철회 의사를 쉽게 표시할 수 있도록 하기 위한 안내문을 명시하고 수신의 거부 또는 수신동의의 철회 여부를 간편하게 선택할 수 있도록 기술적 조치를 해야 한다. 이 경우 그 안내문과 기술적 조치는 한글과 영문으로 명시해야 한다.
모사전송	1. 광고성 정보가 시작되는 부분에 (광고), 전송자의 명칭, 전화번호 및 주소를 표시해야 한다. 2. 수신의 거부 또는 수신동의의 철회용 자동응답전화번호 등의 전화 번호 또는 전화를 걸음하여 쉽게 수신의 거부 또는 수신동의의 철회를 할 수 있는 방식을 해당 광고에 표시된 최대 글자의 3분의 1 이상의 크기로 명시하고, 그 전화번호나 방식을 이용하여 수신의 거부 또는 수신동의의 철회를 하는 때에 수신자가 비용을 부담하지 않는다는 것을 함께 명시해야 한다.
그 밖의 전자적 전송매체	1. 음성형태로 전송되는 광고의 경우 가. 광고성 정보가 시작되는 부분에 광고를 의미하는 음성, 전송자의 명칭, 전화번호 또는 주소, 수신의 거부 또는 수신동의의 철회를 할 수 있는 방식을 안내해야 한다.

	나. 수신의 거부 또는 수신동의의 철회용 자동응답전화번호 등의 전화번호 또는 전화를 갈음하여 쉽게 수신의 거부 또는 수신동의의 철회를 할 수 있는 방식을 이용하여 수신의 거부 또는 수신동의의 철회를 하는 때에 수신자가 비용을 부담하지 않는다는 것을 함께 안내해야 한다. 2. 음성 외의 형태로 전송되는 광고의 경우 가. 광고성 정보가 시작되는 부분에 (광고), 전송자의 명칭과 전화번호 또는 주소를 표시해야 한다. 나. 수신의 거부 또는 수신동의의 철회용 자동응답전화번호 등의 전화번호 또는 전화를 갈음하여 쉽게 수신의 거부 또는 수신동의의 철회를 할 수 있는 방식을 정보가 끝나는 부분에 명시하고, 그 전화번호나 방식을 이용하여 수신의 거부 또는 수신동의의 철회를 하는 때에 수신자가 비용을 부담하지 않는다는 것을 함께 명시해야 한다.

[별표 7] <개정 2013.3.23>

통신과금서비스의 안전성·신뢰성 확보를 위한 필요 조치(제66조의6 관련)

1. 관리적 조치

가. 업무처리지침의 제정·시행

다음의 사항을 포함하는 업무처리지침을 제정·시행하여야 한다.

1) 시스템에 대한 접근 통제 및 감시에 관한 사항
2) 화재·지진·수해 또는 전산장애 등에 대비한 비상 시 시스템 관리에 관한 사항
3) 해킹침해 방지에 관한 사항
4) 바이러스 감염 방지에 관한 사항
5) 인터넷 프로토콜(IP) 주소의 관리에 관한 사항

나. 회계의 구분

통신과금서비스와 관련된 회계와 그 밖의 회계를 구분하여 처리하여야 한다.

다. 정보처리시스템 및 전산자료의 관리

1) 데이터베이스관리시스템, 운영체제 등 주요 프로그램은 정기적으로 유지·보수하고, 그 내용을 기록하여 1년 동안 보관하여야 한다.
2) 정보처리시스템의 장애발생 시 장애내용 및 조치사항 등에 관한 기록을 1년 동안 보관하여야 한다.
3) 전산자료의 유출·파괴를 방지하기 위하여 전산자료에 대한 접근권한을 통제하고, 정기적으로 그 현황을 점검하도록 하며, 중요한 전산자료는 정기적으로 백업하고 그 상태를 정기적으로 검사하여야 한다.

2. 기술적 조치

가. 정보처리시스템은 서버, 통신기기의 정상 작동 여부를 확인하기 위한 모니터링 체계를 갖추어야 한다.

나. 해킹을 방지하고 사이버테러를 방지하기 위하여 해킹방지시스템 등을 구축·운영하여야 한다.

3. 제1호 및 제2호에 따른 관리적 조치와 기술적 조치의 세부내용은 미래창조과학부장관이 정하여 고시한다.

[별표 8] <개정 2015.12.22.>

과징금의 산정기준과 산정절차(제69조의2제4항 관련)

1. 과징금의 산정단계

과징금은 법 제64조의3제3항 각 호에 따른 고려 사항과 이에 영향을 미치는 행위를 종합적으로 고려하여 기준금액에 필수적 가중·감경, 추가적 가중·감경을 거쳐 과징금을 산정한다.

2. 과징금의 산정단계에 따른 산정방식과 고려 사유

가. 기준금액의 산정

1) 기준금액은 제69조의2제1항에 따른 위반행위와 관련한 매출액에 위반행위의 중대성에 따라 다음과 같이 구분된 과징금의 산정비율(부과기준율)을 곱하여 산출한 금액으로 한다.

위반행위의 중대성	부과기준율
매우 중대한 위반행위	1천분의 27
중대한 위반행위	1천분의 21
보통 위반행위	1천분의 15

2) 제69조의2제2항 각 호의 어느 하나에 해당하는 경우에는 1)에도 불구하고, 위반행위의 중대성에 따라 기준금액을 다음과 같이 한다.

위반행위의 중대성	기준금액
매우 중대한 위반행위	3억 6천만원
중대한 위반행위	2억 8천만원
보통 위반행위	2억원

3) 위반행위의 중대성은 고의·중과실 여부, 영리 목적의 유무, 위반행위로 인한 개인정보의 피해규모, 개인정보의 공중에 노출 여부 및 위반행위로 인하여 취득한 이익의 규모 등을 종합적으로 고려하여 판단한다.

나. 필수적 가중·감경

위반행위의 기간과 횟수 등을 고려하여 기준금액의 100분의 50의 범위에서 가중하거나 감경해야 한다.

다. 추가적 가중·감경

개인정보 보호를 위한 노력 정도, 위반행위에 대한 조사의 협조 여부, 위반행위의 주도 여부 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위에서 가중하거나 감경할 수 있다.

3. 세부 기준

위반행위와 관련한 매출액의 산정에 관한 세부 기준, 위반행위의 중대성 판단 기준, 필수적 가중·감경 및 추가적 가중·감경을 위한 세부 기준과 그 밖에 과징금의 부과에 필요한 사항은 방송통신위원회가 정하여 고시한다.

[별표 9] <개정 2016. 9. 22.>

과태료의 부과기준(제74조 관련)

1. 일반기준

가. 위반행위의 횟수에 따른 과태료 부과기준은 최근 3년간 같은 위반행위로 과태료처분을 받은 경우에 적용한다. 이 경우 위반행위에 대하여 과태료처분을 한 날과 다시 같은 위반행위(처분 후의 위반행위만 해당한다)를 적발한 날을 각각 기준으로 하여 위반횟수를 계산한다.

나. 부과권자는 다음의 어느 하나에 해당하는 경우에는 제2호에 따른 과태료 금액의 2분의 1 범위에서 그 금액을 감경할 수 있다. 다만, 과태료를 체납하고 있는 위반행위자에 대해서는 그러하지 아니하다.

1) 위반행위자가 「질서위반행위규제법 시행령」 제2조의2제1항 각 호의 어느 하나에 해당하는 경우

2) 위반행위가 단순 과실에 의한 경우

3) 이용자에게 피해가 발생하지 않은 등 위반행위의 결과가 경미한 경우

4) 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송한 경우로서 법 제50조제4항 또는 제6항을 위반했으나, 법 제50조제1항부터 제3항까지의 규정은 위반하지 않은 경우

5) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우

다. 부과권자는 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 제2호에 따른 과태료 금액의 2분의 1 범위에서 가중할 수 있다. 다만, 가중하는 경우에도 법 제76조제1항부터 제3항까지의 규정에 따른 과태료 금액의 상한을 넘을 수 없다.

2. 개별기준

(단위: 만원)

위반행위	근거 법조문	위반횟수별 과태료 금액		
		1회	2회	3회 이상

가. 법 제23조제3항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 서비스의 제공을 거부한 경우	법 제76조제1항제1호	1,000	2,000	3,000
나. 법 제23조의2제1항을 위반하여 주민등록번호를 수집·이용하거나 같은 조 제2항에 따른 필요한 조치를 하지 않은 경우(법 제67조에 따라 준용되는 경우를 포함한다)	법 제76조제1항제2호	1,000	2,000	3,000
다. 법 제23조의3제1항을 위반하여 본인확인기관의 지정을 받지 않고 본인확인업무를 한 경우	법 제76조제3항제2호의2	1,000	1,000	1,000
라. 법 제23조의3제2항에 따른 본인확인업무의 휴지 또는 같은 조 제3항에 따른 본인확인업무의 폐지 사실을 이용자에게 통보하지 않거나 방송통신위원회에 신고하지 않은 경우	법 제76조제3항제2호의3	300	600	1,000
마. 법 제23조의4제1항에 따른 본인확인업무의 정지 및 지정 취소 처분에도 불구하고 본인확인업무를 계속한 경우	법 제76조제3항제2호의4	1,000	1,000	1,000
바. 법 제24조의2제3항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 제공 또는 처리위탁에 대한 동의를 받을 때 개인정보의 수집·이용에 대한 동의와 구분	법 제76조제1항제2호의2	1,000	2,000	3,000

하여 받지 않거나 이에 동의하지 않는다는 이유로 서비스 제공을 거부한 경우				
사. 법 제25조제2항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자에게 개인정보 처리위탁에 관한 사항을 공개하지 않거나 알리지 않은 경우	법 제76조제2항제1호	600	1,200	2,000
아. 법 제25조제6항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 처리위탁을 할 때에 문서에 의하지 않은 경우	법 제76조제3항제2호의5	300	600	1,000
자. 법 제25조제7항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 처리위탁을 한 정보통신서비스 제공자등의 동의를 받지 않고 제3자에게 재위탁한 경우	법 제76조제2항제1호의2	600	1,200	2,000
차. 법 제26조제1항 및 제2항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자에게 개인정보의 이전 사실을 알리지 않은 경우	법 제76조제2항제2호	600	1,200	2,000
카. 법 제27조제1항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 보호책임자를 지정하지 않은 경우	법 제76조제2항제3호	600	1,200	2,000
타. 법 제27조의2제1항(법 제	법 제76조제2항제4호	600	1,200	2,000

67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 처리방침을 공개하지 않은 경우				
파. 법 제27조의3제1항(법 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자·방송통신위원회 및 한국인터넷진흥원에 통지 또는 신고하지 않거나 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 경우	법 제76조제1항제2호의3	1,000	2,000	3,000
하. 법 제27조의3제3항에 따른 소명을 하지 않거나 거짓으로 한 경우	법 제76조제1항제2호의4	1,000	2,000	3,000
거. 법 제28조제1항(법 제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 않은 경우	법 제76조제1항제3호	1,000	2,000	3,000
너. 법 제29조제2항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 파기 등의 조치를 취하지 않은 경우	법 제76조제1항제4호	1,000	2,000	3,000
더. 법 제30조제3항·제4항 및 제6항(법 제30조제7항, 제31조제3항 및 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 필요한 조치를 하지 않은 경우	법 제76조제1항제5호	1,000	2,000	3,000
러. 법 제30조의2제1항 본문을	법 제76조제1항제5호의	1,000	2,000	3,000

위반하여 개인정보의 이용내역을 통지하지 않은 경우(법 제67조에 따라 준용되는 경우를 포함한다)	2			
머. 법 제42조의3제1항을 위반하여 청소년 보호 책임자를 지정하지 않은 경우	법 제76조제3항제3호	300	600	1,000
버. 법 제43조를 위반하여 정보를 보관하지 않은 경우	법 제76조제3항제4호	300	600	1,000
서. 법 제45조의3제1항을 위반하여 정보보호 최고책임자의 지정을 신고하지 않은 경우	법 제76조제1항제6호의 2	1,000	2,000	3,000
어. 법 제46조제2항을 위반하여 보험에 가입하지 않은 경우	법 제76조제3항제5호	1,000	1,000	1,000
저. 법 제47조제2항을 위반하여 정보보호 관리체계 인증을 받지 않은 경우	법 제76조제1항제6호의 3	3,000	3,000	3,000
처. 법 제47조제9항 및 제47조의3제3항을 위반하여 인증받은 내용을 거짓으로 홍보한 경우	법 제76조제3항제7호	300	600	1,000
커. 법 제47조의4제3항을 위반하여 소프트웨어 사용자에게 알리지 않은 경우	법 제76조제3항제10호	300	600	1,000
터. 법 제48조의2제4항에 따른 시정명령을 이행하지 않은 경우	법 제76조제3항제11호	300	600	1,000
퍼. 법 제48조의3제1항을 위반하여 침해사고의 신고를 하지 않은 경우	법 제76조제3항제11호의2	300	600	1,000
허. 법 제48조의4제4항에 따른	법 제76조제3항제12호	300	600	1,000

사업장 출입 및 조사를 방해하거나 거부 또는 기피한 경우				
고. 법 제49조의2제4항을 위반하여 미래창조과학부장관 또는 방송통신위원회의 명령을 이행하지 않은 경우	법 제76조제3항제12호의2	300	600	1,000
노. 법 제50조제1항부터 제3항까지의 규정을 위반하여 영리목적의 광고성 정보를 전송한 경우	법 제76조제1항제7호	750	1,500	3,000
도. 법 제50조제4항을 위반하여 광고성 정보를 전송할 때 밝혀야 하는 사항을 밝히지 않거나 거짓으로 밝힌 경우	법 제76조제1항제8호	750	1,500	3,000
로. 법 제50조제6항을 위반하여 비용을 수신자에게 부담하도록 한 경우	법 제76조제1항제9호	750	1,500	3,000
모. 법 제50조제7항을 위반하여 수신 동의, 수신거부 또는 수신동의 철회에 대한 처리 결과를 알리지 않은 경우	법 제76조제3항제12호의3	300	600	1,000
보. 법 제50조제8항을 위반하여 수신동의 여부를 확인하지 않은 경우	법 제76조제1항제9호의2	750	1,500	3,000
소. 법 제50조의4제4항을 위반하여 필요한 조치를 하지 않은 경우	법 제76조제3항제12호의4	300	600	1,000
오. 법 제50조의5를 위반하여 이용자의 동의를 받지 않고 프로그램을 설치한 경우	법 제76조제1항제10호	750	1,500	3,000

조. 법 제50조의7제1항 또는 제2항을 위반하여 인터넷 홈페이지에 영리목적의 광고성 정보를 게시한 경우	법 제76조제1항제11호	750	1,500	3,000
초. 법 제52조제6항을 위반하여 한국인터넷진흥원의 명칭을 사용한 경우	법 제76조제3항제13호	300	600	1,000
코. 법 제53조제4항을 위반하여 사업의 휴지·폐지·해산의 신고를 하지 않은 경우	법 제76조제3항제14호	300	600	1,000
토. 법 제56조제1항을 위반하여 약관을 신고하지 않은 경우	법 제76조제3항제15호	300	600	1,000
포. 법 제57조제2항을 위반하여 관리적 조치 또는 기술적 조치를 하지 않은 경우	법 제76조제3항제16호	300	600	1,000
호. 법 제58조제1항을 위반하여 통신과금서비스 이용일시 등을 통신과금서비스이용자에게 고지하지 않은 경우	법 제76조제3항제17호	300	600	1,000
구. 법 제58조제2항을 위반하여 통신과금서비스이용자가 구매·이용 내역을 확인할 수 있는 방법을 제공하지 않거나 통신과금서비스이용자의 제공 요청에 응하지 않은 경우	법 제76조제3항제18호	300	600	1,000
누. 법 제58조제3항을 위반하여 통신과금서비스이용자로부터 받은 통신과금에 대한 정정요구가 이유 있음에도 결제대금의 지급을 유보하지 않거나 통신과금서비스이용자의 요청	법 제76조제3항제19호	300	600	1,000

에 대한 처리 결과를 통신과금서비스이용자에게 알려 주지 않은 경우				
두. 법 제58조제4항을 위반하여 통신과금서비스에 관한 기록을 보존하지 않은 경우	법 제76조제3항제20호	300	600	1,000
투. 법 제58조제5항을 위반하여 통신과금서비스이용자의 동의를 받지 않고 통신과금서비스를 제공하거나 이용한도액을 증액한 경우	법 제76조제3항제20호의2	300	600	1,000
부. 법 제58조제6항을 위반하여 통신과금서비스 약관의 변경에 관한 통지를 하지 않은 경우	법 제76조제3항제20호의3	300	600	1,000
부. 법 제59조제2항을 위반하여 통신과금서비스이용자의 이의신청 및 권리구제를 위한 절차를 마련하지 않거나 통신과금서비스 계약 시 이를 명시하지 않은 경우	법 제76조제3항제21호	300	600	1,000
수. 법 제63조제2항 단서를 위반하여 법 제63조제3항 각 호의 사항 모두를 공개하거나 이용자에게 알리지 않고 이용자의 개인정보를 국외에 처리·위탁·보관한 경우	법 제76조제2항제5호	600	1,200	2,000
우. 법 제64조제1항에 따른 관계 물품·서류 등을 제출하지 않거나 거짓으로 제출한 경우	법 제76조제3항제22호	300	600	1,000
주. 법 제64조제2항에 따른 자	법 제76조제3항제23호	300	600	1,000

료의 열람·제출요청에 따르지 않은 경우				
추. 법 제64조제3항에 따른 출입·검사를 거부·방해 또는 기피한 경우	법 제76조제3항제24호	300	600	1,000
쿠. 이 법을 위반하여 법 제64조제4항에 따라 미래창조과학부장관 또는 방송통신위원회로부터 받은 시정조치 명령을 이행하지 않은 경우	법 제76조제1항제12호			
1) 법 제71조의 위반행위에 대한 시정조치 명령을 이행하지 않은 경우		3,000	3,000	3,000
2) 법 제72조의 위반행위에 대한 시정조치 명령을 이행하지 않은 경우		2,000	2,000	2,000
3) 법 제73조 및 제74조의 위반행위에 대한 시정조치 명령을 이행하지 않은 경우		1,000	1,000	1,000
4) 법 제76조제1항제1호, 제2호, 제2호의2, 제2호의3, 제3호부터 제5호까지, 제5호의2 및 제6호의2의 위반행위에 대한 시정조치 명령을 이행하지 않은 경우		1,000	1,000	1,000
5) 법 제76조제1항제7호부터 제9호까지, 제9호의2, 제10호 및 제11호의 위반행위에 대한 시정조치 명령을 이행하지 않은 경우		750	750	750
6) 법 제76조제2항의 위반행		600	600	600

위에 대한 시정조치 명령을 이행하지 않은 경우				
7) 법 제76조제3항의 위반행위에 대한 시정조치 명령을 이행하지 않은 경우		500	500	500
8) 그 밖의 시정조치 명령을 이행하지 않은 경우		300	300	300

비고: 노목부터 조목까지의 규정(모목과 소목은 제외한다)에 따른 위반행위의 경우에는 해당 위반행위를 하도록 한 경우도 포함한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙

[시행 2016.6.2] [미래창조과학부령 제00070호, 2016.6.2, 일부개정]

제1조(목적) 이 규칙은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 같은 법 시행령에서 위임된 사항과 그 시행에 필요한 사항을 규정함을 목적으로 한다.

제2조(정보보호 최고책임자 지정 신고 등) ① 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」(이하 "영"이라 한다) 제36조의7에 따라 정보보호 최고책임자를 지정하고 신고하려는 정보통신서비스 제공자는 별지 제2호서식의 정보보호 최고책임자 지정신고서를 미래창조과학부장관에게 제출(전자문서를 통한 제출을 포함한다)하여야 한다. <개정 2015.12.23, 2016.6.2>

② 제1항에 따라 정보보호 최고책임자 지정신고서를 제출받은 미래창조과학부장관은 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 법인 등기사항증명서(법인인 경우만 해당한다) 또는 사업자등록증(개인인 경우만 해당한다)을 확인하여야 한다. 다만, 신고인이 사업자등록증의 확인에 동의하지 아니하는 경우에는 해당 서류의 사본을 제출하도록 하여야 한다.

[본조신설 2014.11.28]

[제9조의2에서 이동 <2016.6.2>]

제3조(정보보호 관리체계 인증심사 일부의 생략) ① 미래창조과학부장관은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) 제47조제2항에 따라 인증을 받아야 하는 자가 다음 각 호의 어느 하나에 해당하는 국제표준 정보보호 인증을 받거나 정보보호 조치를 취한 경우에는 같은 조 제3항에 따라 같은 조 제1항에 따른 인증심사의 일부를 생략할 수 있다.

1. 「품질경영 및 공산품안전관리법」 제7조제2항에 따른 국제인정기관협력기구에 가입된 인정기관이 인정한 인증기관으로부터 받은 국제표준 정보보호경영시스템 인증
2. 법 제47조의3 또는 「개인정보 보호법」 제13조제3호에 따른 개인정보보호 관리체계 인증
3. 「정보통신기반 보호법」제9조에 따른 주요정보통신기반시설의 취약점 분석·평가

② 제1항에 따라 정보보호 관리체계 인증심사의 일부를 생략하려는 경우에는 다음 각 호의 요건을 모두 충족하여야 한다.

1. 해당 국제표준 정보보호 인증 또는 정보보호 조치의 범위가 영 제47조제2항에 따른 정보보호 관리체계 인증의 범위와 일치할 것

2. 정보보호 관리체계 인증 신청 및 심사 시에 해당 국제표준 정보보호 인증이나 정보보호 조치가 유효하게 유지되고 있을 것

③ 법 제47조제3항에 따라 정보보호 관리체계 인증심사 일부의 생략을 받으려는 자는 인증심사 일부의 생략을 신청하는 서류에 국제표준 정보보호 인증서, 정보보호 조치 결과보고서 등 인증심사의 일부 생략 대상인 사실을 증명할 수 있는 서류를 첨부하여 제출하여야 한다.

[본조신설 2016.6.2]

제4조 삭제 <2014.11.28>

제5조 삭제 <2014.11.28>

제6조 삭제 <2014.11.28>

제7조 삭제 <2014.11.28>

제8조 삭제 <2014.11.28>

제9조 삭제 <2014.11.28>

제9조의2

[제2조로 이동 <2016.6.2>]

제10조 삭제 <2015.12.23>

부칙 <제34호,2008.9.23>

이 규칙은 공포한 날부터 시행한다.

부칙 <제52호,2008.12.31>

이 규칙은 공포 후 6개월이 경과한 날부터 시행한다.

부칙 <제92호,2009.8.28>

제1조(시행일) 이 규칙은 공포한 날부터 시행한다.

제2조(다른 법령의 개정) ① 생략

② 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙 일부를 다음과 같이 개정한다.

제2조를 삭제한다.

제3조 생략

부칙 <제14호,2013.12.31>

이 규칙은 공포한 날부터 시행한다.

부칙 <제27호,2014.11.28>

이 규칙은 2014년 11월 29일부터 시행한다.

부칙 <제54호,2015.12.23>

이 규칙은 공포한 날부터 시행한다.

부칙 <제70호,2016.6.2>

이 규칙은 공포한 날부터 시행한다.

[별지 제1호서식] 삭제 <2015.12.23.>

■ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙 [별지 제2호서식] <신설 2014.11.28.>

정보보호 최고책임자 지정신고서

접수번호	접수일자	처리기간 30일

신고인	상호명	사업자등록번호
	사무소 소재지 (대표전화:)	
정보보호 최고 책임자	성명	전화번호
	휴대전화번호	전자우편주소

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3 및 같은 법 시행령 제36조의7에 따라 위와 같이 정보보호 최고책임자의 지정을 신고합니다.

년 월 일

신고인(대표자) (서명 또는 인)

미래창조과학부장관 귀하

담당 공무원 확인사항	1. 법인 등기사항증명서(법인인 경우만 해당합니다) 2. 사업자등록증(개인인 경우만 해당합니다)	수수료 없음

행정정보 공동이용 동의서

본인은 이 건 업무처리와 관련하여 담당 공무원이 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 위의 담당 공무원 확인사항 제2호를 확인하는 것에 동의합니다.

※ 담당 공무원의 행정정보 공동이용에 동의하지 않는 경우에는 신고인이 해당 서류를 직접 제출해야 합니다.

신고인 (서명 또는 인)

처리절차

신고서 작성	➡	접수	➡	검토	➡	신고완료
신고인		미래창조과학부				

210㎜×297㎜[백상지 80g/㎡(재활용품)]

정보보호관리체계 인증

[시행 2010.2.3] [고시 제2010 - 3호, 2010.2.3, 타법개정]

제1장 총칙

제1조(목적) 이 고시는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하"법"이라 한다) 제47조제2항 및 같은 법 시행령 제47조제2항、제48조제1항제3호、제5항、제50조제6항에 따른 정보보호관리체계 인증에 관한 정보보호관리기준、지정에 필요한 업무수행능력 심사 등에 관한 세부사항과 그 밖에 정보보호관리체계 인증에 관하여 필요한 사항에 대하여 정하는 것을 목적으로 한다.

제2조(용어의 정의) 이 기준에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "업무수행능력심사"란 정보보호관리체계인증기관으로 지정받고자 신청한 법인 또는 단체의 업무수행능력을 세부평가기준에 따라 심사하는 것을 말한다.
2. "정보보호관리체계인증기관"이란 법 제47조에 따른 한국정보보호진흥원과 방송통신위원회가 지정하는 기관을 말한다.
3. "인증"이란 신청기관이 수립하여 운영하고 있는 정보보호관리체계가 인증심사기준 등에 적합함을 정보보호관리체계인증기관이 승인하는 것을 말한다.
4. "인증심사"란 신청기관이 수립하여 운영하는 정보보호관리체계가 인증심사기준 등에 대하여 서면심사 및 기술심사의 방법으로 확인하는 것을 말한다.
5. "정보보호관리과정(이하 ‘관리과정’이라 한다)"이란 정보보호관리체계를 수립、운영하기 위하여 유지、관리하여야 할 과정으로 다음 각목의 5단계 활동을 말한다.
   가. 정보보호정책 수립
   나. 정보보호관리체계 범위설정
   다. 위험관리
   라. 구현
   마. 사후관리
6. "신청기관"이란 이 고시에 따라 정보보호관리체계 인증을 취득하고자 신청한 업체 및 기관 등을 말한다.
7. "외부자"란 신청기관의 직원이 아닌 자를 말한다.

8. "정보보호대책"이란 신청기관이 정보보호관리체계를 수립·운영하기 위하여 별표 6에서 선택한 통제사항을 말한다.

제2장 정보보호관리체계인증기관의 지정 등

제1절 정보보호관리체계인증기관의 지정신청

제3조(정보보호관리체계인증기관의 지정공고) 방송통신위원회는 법 제47조 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」(이하 "영"이라 한다) 제48조에 따라 정보보호관리체계인증기관을 지정할 필요가 있는 때에는 미리 접수신청기간과 신청요령 등을 정하여 관보 및 인터넷 홈페이지에 20일 이상 공고하여야 한다.

제4조(제출서류 등) ①정보보호관리체계인증기관 지정을 신청하는 자는 별지 제1호서식의 정보보호관리체계인증기관 지정신청서를 방송통신위원회에 제출하여야 한다.
②영 제48조제1항제2호에 따라 제1항의 정보보호관리체계인증기관지정신청서에 첨부하여야 하는 "인증심사업무를 전담하는 직원의 보유현황"의 제출서식은 별지 제2호서식과 같다.
③영 제48조제1항제3호에 따른 "업무수행능력심사를 위하여 필요한 서류"라 함은 별표 1과 같다.

제2절 인증심사업무를 전담하는 직원의 자격요건 및 업무수행능력심사

제5조(인증심사업무를 전담하는 직원의 요건 등) ①영 제47조제1항제1호 및 제2항에 따른 "인증심사업무를 전담하는 직원(이하 "인증심사원"이라 한다)의 요건"은 별표 2와 같다.
②법 제47조에 따른 정보보호관리체계인증기관으로 지정신청 하고자 하는 자는 제1항의 인증심사원의 요건을 만족하여야 한다.

제6조(업무수행능력심사 기준 등) ①영 제47조제1항제2호 및 제2항에 따른 업무수행능력심사의 세부평가기준은 별표 3과 같다.
②심사위원회는 제1항에 따라 심사위원 각자가 부여한 점수 중 최고점과 최저점을 제외한 점수들의 평균이 80점 이상인 자를 선별한다.
③심사위원회는 제2항에 따라 선별된 자에 대하여 심사결과 검증 및 업무수행능력의 적합성을 판단한다.

제7조(업무수행능력의 적합성 인정) 방송통신위원회는 제5조 및 제6조에 따라 심사한 결과를 토대로 정보통신망 안전성 및 신뢰성 확보를 위한 종합적인 정보보호관리체계의 업무를 수행하는 자로서
적합한지 여부를 결정한다.

제8조(정보보호관리체계인증기관지정서) 영 제48조제3항에 따른 "정보보호관리체계인증기관 지정서"는 별지 제4호서식과 같다.

제3절 인증기관 심사위원회 구성·운영

제9조 (심사위원회의 구성) ①방송통신위원회는 영 제48조제1항에 따라 정보보호관리체계인증기관의 지정신청을 받은 경우 영 제48조제4항에 따른 심사위원회를 구성하여 다음 각 호의 심사업무를 수행하게 하여야 한다. 이 경우 방송통신위원회는 필요하다고 인정하는 때에는 분과위원회 또는 작업반을 둘 수 있다.

1. 영 제48조제3항에 따른 현장실사
2. 별표 2에 따른 인증심사원의 자격요건 및 별표 3에 따른 업무수행능력심사 세부평가
3. 정보보호관리체계인증기관 지정의 적합성 결정
4. 그 밖에 지정심사와 관련되는 업무

②심사위원회는 5인이상 10인이내의 위원으로 구성하되, 위원은 정보보호전문가, 회계사, 기술사, 변호사 등 업무수행능력심사를 수행할 수 있는 학식과 경험이 있는 자 중 방송통신위원회가 위촉하며, 위원장은 위원 중에서 호선한다.

③제2항에 따른 심사위원은 최근 2년간 지정신청자와 관련된 업무를 수행하지 않아야 한다.

④위원에 대하여는 예산의 범위안에서 수당과 여비를 지급할 수 있다. 다만, 공무원인 위원이 소관업무와 관련하여 참석한 경우에는 그러하지 아니하다.

제10조(심사위원회의 운영) ①위원장은 심사위원회의 업무를 통할하며 위원회를 대표하여 방송통신위원회에 정보보호관리체계인증기관 지정 적합성 여부에 대한 심사결과를 제출한다.

②위원장이 부득이한 사유로 직무를 수행할 수 없을 때에는 위원장이 미리 지정한 위원이 그 직무를 대행한다.

제3장 정보보호관리체계의 인증기준 등

제1절 정보보호관리체계 인증신청

제11조(신청기관의 준비사항) 신청기관은 다음 각 호의 인증심사기준에 따라 정보보호관리체계를 수립하여 최소 3개월 이상 운영하여야 한다.

1. 별표 4에 따른 관리과정 요구사항
2. 별표 5에 따른 문서 작성 및 관리 통제사항
3. 별표 6에 따른 정보보호관리 통제사항에서 선택한 사항(신청기관은 자신의 정보보호관리체계의 규모 및 사업특성 등을 고려하여 별표 6에서 적절한 항목을 선택할 수 있다)

제12조(인증의 신청) ①영 제50조제1항에 따라 인증을 신청하는 자는 별지 제5호서식의 정보보호관리체계인증신청서를 정보보호관리체계인증기관에 제출하여야 한다. 이 경우 정보보호관리체계의 인증을 받고자 하는 범위를 정하여 신청할 수 있다.

②제1항에 따라 신청을 받은 정보보호관리체계인증기관은 정보보호관리체계 특성상 신청기관이 지정한 정보보호관리체계만을 분리하여 심사할 수 없는 경우에는 신청기관과 상의하여 인증의 범위를 변경할 수 있다.

제13조(인증심사계약의 체결) 정보보호관리체계인증기관은 영 제50조제2항에 따라 신청기관과 협의한 후 심사기간, 심사인원, 심사수수료, 인증의 범위 등을 포함하는 인증심사계약을 체결하여야 한다.

제2절 정보보호관리체계 인증심사 기준 및 방법

제14조(인증심사기준) 정보보호관리체계의 인증심사기준은 별표 4부터 별표 6까지와 같다.

제15조(인증심사요소) ①정보보호관리체계인증기관은 신청기관이 수립한 관리과정을 체계적으로 관리·유지하고 있는지 여부를 판단하기 위하여 다음 각 호의 사항을 심사하여야 한다.

1. 정보보호정책 수립 : 신청기관에 적합한 정보보호정책의 수립, 조직의 구성·운영, 책임성의 명확한 설정 여부
2. 정보보호관리체계 범위설정 : 정보보호관리체계 수립·운영을 위한 관리범위 설정 및 정보자산의 현황조사 여부
3. 위험관리 : 위험관리 전략 및 계획 수립, 위험분석·평가, 정보보호대책 선택의 적절성 여부
4. 구현 : 정보보호대책의 구현 및 정보보호 교육·훈련의 효과성 여부
5. 사후관리 : 정보보호관리체계의 재검토, 모니터링 및 개선, 내부감사 활동의 적절성 여부

②정보보호관리체계인증기관은 신청기관이 정보보호관리체계의 수립 및 이행 활동에 관련된 절차와 운영을 문서화해서 관리하는지에 대하여 심사하여야 한다.

③정보보호관리체계인증기관은 신청기관이 관리과정의 위험평가를 통하여 선택한 통제사항에 대한 정보보호대책을 구현하고 이행하고 있는지에 대하여 심사하여야 한다.

제16조(서면심사) 인증심사원은 신청기관이 영 제50조제1항에 따라 제출한 신청서류를 확인하여 신청기관이 수립한 정보보호관리체계가 별표 4부터 별표 6까지에 따른 인증심사기준에 적합한지에 대하여 심사하여야 한다.

제17조(기술심사) ①인증심사원은 서면심사의 결과를 검증하기 위하여 신청기관이 인증을 신청한 정보보호관리체계가 운영중인 현장을 방문하여 직접 해당 정보보호관리체계의 구축·운영 실태를 확인하여야 한다.

②인증심사원은 제1항에 따른 현장방문시 신청기관의 요청이 있는 경우 인터넷 침해사고 등에 대한 안전성 검사를 위하여 해당 정보보호관리체계에 속한 정보시스템에 대한 모의진단을 실시할 수 있다.

제3절 인증위원회의 구성 및 운영

제18조(인증위원회의 구성) ①정보보호관리체계인증기관의 장은 인증심사원이 실시한 인증심사 결과가 제14조에 따른 인증심사기준에 적합한지 여부를 심의하기 위하여 인증위원회를 구성·운영하여야 한다.
②인증위원회는 5인 이상 10인 이내의 위원으로 구성하되, 위원은 정보보호전문가, 정보시스템감리사, 기술사 등 정보보호분야에 학식과 경험이 있는 자 중 정보보호관리체계인증기관의 장이 위촉하며, 위원장은 위원 중에서 호선한다.

제19조(인증위원회의 운영) ①위원장은 인증위원회의 업무를 통할하며 위원회를 대표하여 정보보호관리체계인증기관의 장에게 인증심사원이 실시한 인증심사 결과가 제14조에 따른 인증심사기준에 적합한지 여부를 심의하고 그 결과를 제출한다.
②정보보호관리체계인증기관의 장은 제1항에 따른 심의를 실시한 때에는 인증심사원이 실시한 심사결과를 위원회 개최 전 5일까지 인증위원회에 제출한다.

제4절 인증서 교부 및 사후관리 등

제20조(인증서 교부) 정보보호관리체계인증기관의 장은 제19조제1항에 따라 인증위원회의 심의결과를 제출받은 경우 신청기관에게 인증심사결과를 통보하고, 신청기관의 정보보호관리체계가 이 고시에서 정한 인증심사기준에 적합하다고 판단된 경우 별지 제6호서식의 정보보호관리체계인증서를 교부하여야 한다.

제21조(정보보호관리체계의 변경) ①인증을 취득한 자는 인증을 받은 정보보호관리체계에 다음 각 호의 어느 하나에 해당하는 중대한 변화가 발생한 경우 발생한 날로부터 3개월 이내에 인증기관의 장에게 변경된 내용을 통보하여야 한다.
1. 신청기관이 수립하여 운영하는 관리체계의 범위가 확대되거나 변경되었을 경우
2. 사업장 변경 및 기업결합 등의 경영환경 변화 등으로 관리체계 운영에 영향을 미치는 경우
②인증기관의 장은 인증을 취득한 자로부터 변경내용을 통보받은 경우 인증을 취득한 자와 협의하여 인증심사 여부를 결정한다.
③제2항에 따라 인증심사를 실시하는 경우에는 제14조부터 제20조까지를 준용한다.

제22조(사후관리) ①영 제52조에 따라 정보보호관리체계인증기관은 인증을 취득한 자가 정보보호관리체계를 지속적으로 유지하고 있는지에 대하여 영 제51조에 따른 유효기간 중 제2절 정보보호관리체계 인증심사 기준 및 방법에 따라 1회 사후관리를 수행한다.
②정보보호관리체계인증기관은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 때에는 인증을 취소하여야 한다.

1. 거짓 그 밖의 부정한 방법으로 정보보호관리체계인증을 받은 때
2. 법 제47조제3항에 따라 인증받은 내용을 홍보하면서 인증의 범위나 유효기간을 속인 경우
3. 제1항에 따른 사후관리에서 정보보호관리체계 인증기준에 적합하지 않게 된 사실이 발견된 때

③정보보호관리체계인증기관이 제2항에 따라 인증을 취소하는 경우에는 인증을 취득한 자에게 통지하고, 제20조에 따라 교부한 정보보호관리체계인증서를 회수하여야 한다.

제23조(인증서 관리) ①정보보호관리체계인증기관은 발급된 인증서의 인증번호, 발급번호, 발급일, 유효기간 등을 관리하여야 한다.

②인증을 취득한 자는 인증서의 분실 등으로 인한 재발급을 받고자 할 경우 별지 제7호서식의 관리체계 인증서 재발급 신청서를 인증기관에 제출하여야 한다.

③인증을 취득한 자가 주소, 업체명 등 인증서 기재사항의 변경을 요청하고자 하는 경우 별지 제8호서식의 인증서 변경신청서를 정보보호관리체계인증기관에 제출하여야 한다.

제24조(재검토기한) 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 고시 발령 후 법령이나 현실여건의 변화 등을 검토하여 이 고시의 폐지, 개정 등 조치를 하여야 하는 기한은 2012년 10월 31일까지로 한다.

부칙 <제2010-3호,2010.2.3>

제1조(시행일) 이 고시는 2010년 2월 3일부터 시행한다.

제2조(서식에 관한 경과조치) 이 고시 시행당시 종전의 규정에 의한 서식은 2010년 6월 30일까지 이 고시에 의한 서식과 함께 사용할 수 있다.

[별표 1]

업무수행능력심사 규정에 따른 제출서류(제4조제3항관련)

구 분	제 출 서 류
1. 정보보호수행실적을 확인하는 데 필요한 서류	가. 별지 제3호서식에 따른 정보보호수행실적 명세서 및 이를 증빙할 수 있는 자료(결과보고서 등) 나. 계약서 사본 및 세금계산서 등
2. 업무수행능력심사평가표 각호의 세부 평가요소를 평가하기 위하여 필요한 서류	가. 총매출액대비 정보보호분야 매출액의 비율 계산내역(공인회계사 또는 회계담당자가 서명 날인한 서류) 나. 부채비율 및 자기자본 이익률의 계산내역(회결산내역 등 관련 증빙자료) 다. 인증업무 운영체계 관련 규정 및 지침 등 ㅇ 인증기관의 운영체계 및 인증의 품질관리 ㅇ 인증업무를 수행하는 직원에 대한 운영관리 등의 내부규정 ㅇ 인증업무 수행 방법 및 절차
비 고 ※ 방송통신위원회는 정보보호관리체계인증기관 지정 공고시 업무수행능력심사에 필요한 자료의 구성 및 그 세부내용, 제출시기 및 방법 등에 관한 사항을 포함하여야 한다.	

[별표 2]

인증심사업무를 전담하는 직원의 요건(제5조 관련)

학력 및 경력기준	자격 및 경력기준
1. 유관학력 보유의 경우 가. 학사학위를 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 6년 이상인 자 나. 석사학위를 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 3년 이상인 자	1. 유관자격 보유의 경우 가. 기사자격을 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 4년 이상인 자 나. 산업기사자격을 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 7년 이상인 자
2. 비 유관학력 보유의 경우 가. 학사학위를 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 8년 이상인 자 나. 전문학사를 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 10년 이상인 자	2. 다음 각목의 1에 해당하는 정보보호자격을 취득한 자로서 2년 이상의 정보보호유관경력이 있는 자 가. 한국정보보호진흥원의 정보보호전문가(SIS) 나. 「정보시스템의 효율적 도입 및 운영 등에 관한 법률」 제14조에 따른 정보시스템감리원 다. 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 공인정보시스템감사사(CISA) 라. 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 공인정보시스템보호전문가(CISSP)

1. "유관자격"이라 함은 「국가기술자격법 시행규칙」 별표 7의 검정대상 기술자격 종목 중 전자계산기, 정보통신, 통신설비, 통신기기, 통신선로, 정보기기운용, 전파통신, 전파전자, 무선설비, 방송통신, 정보관리, 정보처리, 사무자동화 및 전자계산조직응용 종목의 기술자격을 말한다.
2. "유관학력"이라 함은 「고등교육법」에 따른 해당 학교에서 다음 각 목에 해당하는 학과에서 소정의 과정을 이수하고 졸업하거나 그 밖의 관계 법령에 따라 국내 또는 외국에서 이와 동등 이상으로 인정되는 학력을 말한다.
   가. 전자 관련 학과 : 정보전자, 전자, 전자계산, 전기전자제어, 전자정보, 전자제어, 전기전자, 전자전기정보, 전자컴퓨터전기제어, 컴퓨터과학, 전기전자정보, 전자컴퓨터, 메카트로닉스, 전자재료, 제어계측, 반도체

나. 정보통신 관련 학과 : 전기통신설비, 국제정보통신, 방송설비, 방송통신, 이동통신, 전자통신, 컴퓨터네트워크, 통신, 컴퓨터정보기술, 전파통신, 전기전자통신, 전기전자정보통신, 전자정보통신, 전자제어통신, 전자통신, 전파, 전파통신, 정보통신, 컴퓨터통신, 항공통신정보, 전자정보통신반도체, 전기전자전파, 통신컴퓨터, 무선통신

다. 정보처리기술 관련 학과 : 시스템, 전산, 정보전산, 컴퓨터제어, 컴퓨터응용제어, 컴퓨터응용, 컴퓨터응용설계, 구조시스템, 컴퓨터정보, 멀티미디어, 정보시스템, 전산통계, 정보처리

라. 그 밖에 교육인적자원부장관이나 해당 교육기관의 장으로부터 전자·통신 및 정보처리기술·정보보호 관련 학과로 인정받은 학과

3. "정보통신유관경력"이라 함은 공공기관, 민간기업, 교육기관 등에서 정보통신서비스(기간통신, 별정통신, 부가통신, 방송서비스 등을 말한다), 정보통신기기(정보기기, 방송기기, 부품 등을 말한다) 또는 소프트웨어 및 컴퓨터 관련 서비스(패키지 소프트웨어, 컴퓨터 관련 서비스, 디지털콘텐츠, 데이터베이스 제작 및 검색 등을 말한다)에 해당되는 분야에서 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 수행한 기간을 말한다.

5. "정보보호유관경력"이라 함은 공공기관, 민간기업, 교육기관 등에서 정보보호를 위한 공통기반기술(암호 기술, 인증 기술 등을 말한다), 시스템·네트워크 보호(시스템 보호, 해킹·바이러스 대응, 네트워크 보호 등을 말한다) 또는 응용서비스 보호(전자거래 보호, 응용서비스 보호, 정보보호 표준화 등을 말한다)에 해당되는 분야에서 계획·분석·설계·개발·운영·유지보수·컨설팅 또는 연구개발 업무 등을 수행한 기간을 말한다.

[별표 3]

업무수행능력심사 세부평가기준(제6조관련)

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td rowspan="3">1.정보보호 업무수행 경험및 전문화 정도 (40)</td><td>최근 3년간 정보보호수행 실적</td><td>25</td><td>계약금액 총액</td><td>o 지정 공고일 기준으로 최근 3년간 완료한 정보보호수행실적을 인정하고 평가점수는 개별 수행실적의 계약금액을 합한 총액에 따라 산출
<table><tr><th>계약금액총액(단위 : 억원)</th><th>점수</th></tr><tr><td>30억원이상</td><td>배점의 100%</td></tr><tr><td>30억원미만</td><td>배점의 x%</td></tr><tr><td colspan="2">※x = (계약금액 총액/30억원) × 100</td></tr></table></td></tr>
<tr><td>최근 3년간 계약금액 5천만원 이상의 정보보호수행 실적</td><td>10</td><td>수행건수</td><td>o 지정 공고일 기준으로 최근 3년간 완료한 정보보호수행실적으로 계약금액이 5천만원 이상의 실적을 인정
<table><tr><th>수행실적 건수</th><th>점수</th></tr><tr><td>30건이상</td><td>배점의 100%</td></tr><tr><td>30건미만</td><td>배점의 x%</td></tr><tr><td colspan="2">※x = (수행건수/30건) × 100</td></tr></table></td></tr>
<tr><td>총매출액에 대한 정보보호분야 매출액 비율</td><td>5</td><td>비율</td><td>o 지정 공고일 기준으로 직전년도 정보보호분야 매출액의 비율(정보보호분야 매출액/총매출액)
<table><tr><th>비율</th><th>점수</th></tr><tr><td>80%이상</td><td>5점</td></tr><tr><td>80%미만 ~ 60%이상</td><td>4점</td></tr><tr><td>60%미만 ~ 40%이상</td><td>3점</td></tr><tr><td>40%미만 ~ 20%이상</td><td>2점</td></tr><tr><td>20%미만</td><td>1점</td></tr></table></td></tr>
<tr><td>2.신뢰도 및재정상태 건실도 (10)</td><td>부채비율</td><td>5</td><td>비율</td><td>o 지정 공고일 기준으로 직전년도 부채비율 (부채총계/자기자본)
<table><tr><th>비율</th><th>점수</th></tr><tr><td>50%미만</td><td>5점</td></tr><tr><td>50%이상 ~ 100%미만</td><td>4점</td></tr><tr><td>100%이상 ~ 150%미만</td><td>3점</td></tr><tr><td>150%이상 ~ 200%미만</td><td>2점</td></tr><tr><td>200%이상</td><td>1점</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td>자기자본이익률</td><td>5</td><td>비율</td><td>o 지정 공고일 기준으로 직전년도 자기자본이익률(당기순이익/자기자본)
<table><tr><th>비율</th><th>점수</th></tr><tr><td>20%이상</td><td>5점</td></tr><tr><td>20%미만 ~ 15%이상</td><td>4점</td></tr><tr><td>15%미만 ~ 10%이상</td><td>3점</td></tr><tr><td>10%미만 ~ 5%이상</td><td>2점</td></tr><tr><td>5%미만</td><td>1점</td></tr></table></td></tr>
<tr><td rowspan="3">3. 인증업무 운영 체계 (50)</td><td>인증기관의 운영 체계 및 인증의 품질관리</td><td>25</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 인증기관의 공정성·객관성·신뢰성·독립성 보장 방안</td><td>5점</td></tr><tr><td>o 인증기관의 내부감사 실시 및 검토 등에 대한 방안</td><td>5점</td></tr><tr><td>o 인증위원회 구성·운영 방안</td><td>5점</td></tr><tr><td>o 인증의 품질 보장 및 관리방안</td><td>5점</td></tr><tr><td>o 인증업무의 기록 및 문서화 관리체계의 적절성</td><td>5점</td></tr></table></td></tr>
<tr><td>인증업무를 수행하는 직원에 대한 운영관리 등의 내부 규정</td><td>10</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 인증업무를 수행하는 직원에 대한 규정 보유 및 그 규정의 타당성 및 실효성
- 인증업무를 수행하는 직원의 의무와 책임 등 준수사항
- 인증업무를 수행하는 직원의 자체 보안 관리 및 감독 요령</td><td>5점</td></tr><tr><td>o 인증업무를 수행하는 직원의 교육 및 평가 등에 대한 방안 및 그 방안의 적절성 및 타당성</td><td>5점</td></tr></table></td></tr>
<tr><td>인증업무 수행 방법 및 절차</td><td>15</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 인증업무 수행 방법 및 절차 등의 적절성 및 타당성
- 인증심사의 절차 및 방법
- 인증수수료 및 그 징수방법
- 인증심사팀 구성 원칙
- 인증서 발급 기준
- 인증심사 사후관리방안 등</td><td>15점</td></tr></table></td></tr>
<tr><td>4. 가점 및 감점</td><td>인증심사업무를 전담하는 직원의 보유 수</td><td>5
(가점)</td><td>보유
인원수</td><td>o 인증심사업무를 수행하는 전담조직을 갖추고, 그 전담조직에 속한 직원에 대해 인정
<table><tr><th>구분</th><th>점수</th></tr><tr><td>20명 이상</td><td>5점</td></tr><tr><td>20명미만 ~ 10명이상</td><td>배점의 x%</td></tr><tr><td>10명 미만</td><td>없음</td></tr><tr><td colspan="2">※x = (인원수/20명) × 100</td></tr></table></td></tr>
<tr><td></td><td>자격취소 사실</td><td>5
(감점)</td><td>취소사실
및
취소회수</td><td>o 지정 공고일 기준으로 10년이내에 방송통신위원회가 부여한 정보보호 관련 수행자격이 취소된 경우
- 정보보호관리체계인증기관, 정보보호 컨설팅전문업체, 안전진단수행기관 등
※ 취소 1회당 : 감점 5점</td></tr>
</table>

<비 고>

1. 각 평가요소별 세부평가에 필요한 자료의 구성 및 그 세부내용 등에 관한 사항은 지정공고 시 제시한다.
2. 평가항목에 대한 각 평가요소별 세부평가 점수는 소수점 이하 둘째 자리에서 반올림한다.
3. 평가항목에 대한 각 평가요소별 평가점수는 평가결과의 최저점과 최고점을 제외한 점수들의 평균점을 부여한다. 다만, 최저점 또는 최고점이 2개 이상일 경우 각 1개만 제외한다.
4. 가점을 합한 점수가 100점을 초과해도 만점 100점으로 표기한다.
5. 정보보호수행실적으로 인정을 받기 위해서는 다음 각목의 요건을 충족하여야 한다.
   가. 전자적 침해행위에 대비하기 위한 정보관리 및 정보시스템의 안전성에 대한 점검과 이에 기초한 정보보호대책의 제시를 주된 목적으로 직접 수행한 실적을 말하는 것으로 정보보호에 관한 감사, 감리, 진단, 인증, 컨설팅 등을 포함한다.
   나. 지정 공고일 현재 프로젝트가 종료되고 이에 대한 대금지급이 완료되어야 한다.
   다. 하수급업체가 수급업체로부터 하도급을 받아 수행한 실적에 대해서는 인정하지 아니하고 해당 기관에서 직접 계약하여 수행한 실적에 대해서만 인정한다.
   마. 가목 내지 다목의 내용이 계약서 및 증빙자료를 통하여 분명하게 확인되어야 한다.
6. '정보보호분야의 매출액'이라함은 지정 공고일 기준으로 직전년도 결산회기의 정보보호분야 제품 및 서비스관련 매출총액을 말한다.
7. '인증업무 운영체계'에 대한 각 평가요소별 세부평가 점수 부여기준은 각 평가요소의 평가결과에 평가등급(계수)를 곱하여 나온 점수를 합산한다.

평가요소별 세부평가 점수	평가등급(계수)
100점이하 ~ 90점이상	우수(1.0)
90점미만 ~ 80점이상	보통(0.6)
80점미만 ~	미흡(0.2)
미 제출	점수없음(0)

[별표 4]

인증심사기준 - 관리과정 요구사항(제11조 제1호관련)

	관리과정		세부관리과정	관리과정 상세내용
1	정보보호정책 수립	1.1	정보보호정책의 수립	신청기관의 경영목표를 지원할 수 있도록 정보보호의 법적, 규제적 요건과 전략적이고 조직적인 위험관리를 기술한 정보보호정책을 수립하여야 한다.
		1.2	조직 및 책임의 설정	정보보호활동에 대한 경영층의 명확한 지원 및 방향제시를 보증할 수 있는 조직을 수립하여야 한다. 또한 정보보호관리 활동을 수행하고 검증하는 인력들에 대한 책임, 권한 및 상호 연관관계를 정의하고 문서화하여야 한다.
2	정보보호 관리체계 범위설정	2.1	정보보호관리체계 범위설정	신청기관의 특성, 위치, 기술, 자산 등 내·외적 환경에 중대한 영향을 미치는 요소를 고려하여 정보보호관리체계의 범위를 설정하여야 한다.
		2.2	정보자산의 식별	신청기관의 정보자산으로 보호를 받을 가치가 있는 정보자산을 식별하고, 이를 정보자산의 형태, 소유자, 관리자, 특성 등을 포함하여 목록을 만들어야 한다.
3	위험관리	3.1	위험관리전략 및 계획 수립	신청기관의 목표 및 정책, 법적 요구사항 등을 고려하여 조직, 역할, 책임, 주요과정을 포함한 위험관리 전략 및 계획을 수립하고, 신청기관에 적합한 위험관리 방법을 선택하고 문서화하여야 한다. 이 위험분석 방법은 조직과 정보보호 환경변화에 대응할 수 있도록 지속적으로 검토하여야 한다.

	관리과정		세부관리과정	관리과정 상세내용
3	위험관리	3.2	위험분석	신청기관은 「2.2 정보자산의 식별」에서 식별된 정보자산에 영향을 줄 수 있는 모든 위협과 취약성, 위험을 식별하고 분류하여야 하며, 이 정보자산의 가치와 위험을 고려하여, 잠재적 손실에 대한 영향을 식별·분석하여야 한다.
		3.3	위험평가	정보자산에 대한 잠재적 및 알려진 위협과 취약성으로 나타날 수 있는 신청기관의 피해와 현재 구현된 정보보호대책의 실패 가능성 및 영향을 평가하고 수용 가능한 위험수준을 포함하여야 한다. 이를 통해 정보자산의 위험을 관리할 수 있는 적절한 정보보호대책 선택 및 우선순위의 확보를 지원하여야 한다.
		3.4	정보보호대책 선택	신청기관의 정보보호정책과 목적에 부합하도록 위험을 수용 가능한 수준으로 감소시키기 위해, 위험분석 및 평가에 의거하여, 위험처리, 위험수용, 위험회피, 위험전가 등의 전략을 설정하고, [별표3]에서 제시하는 통제사항중에서 선택한다. [별표3]에서 제시되어 있지 않은 통제사항을 추가할 경우에는 [별표1]관리과정의 각 단계간 일관성을 유지하도록 한다. 정보보호대책의 선택은 비용·효과 분석에 의해 정당화 될 필요가 있다.
		3.5	정보보호계획 수립	정보보호대책의 선택이후 구현할 정보보호대책 및 구현의 우선순위, 일정계획, 예산, 책임, 운영계획 등을 포함한 정보보호계획을 수립하고, 각 위험에 대한 정보보호대책 및 선택하게 된 근거를 정보보호대책 명세서로 문서화하여야 한다.

	관리과정		세부관리과정	관리과정 상세내용
4	구 현	4.1	정보보호대책의 효과적 구현	정보보호대책은 적절한 관리 조치와 우선 순위에 의해 구현하여야 한다.
		4.2	정보보호 교육 및 훈련	신청기관의 정보보호 관련직원들 및 최종사용자에게 정보보호에 대한 인식을 제고시키고, 정보보호대책의 필요성을 이해하도록 하며 구현될 정보보호대책들을 정확하게 사용할 수 있도록 교육 및 훈련 프로그램을 수립하고 이행하여야 한다.
5	사후관리	5.1	정보보호관리체계의 재검토	신청기관의 목표, 기술 등 내·외부의 변화와 내부감사 결과, 보안사고 등을 고려하여, 정보보호관리체계의 효율성, 범위의 적절성, 잔류위험의 수준, 절차 등의 문서를 공식적이고 정기적으로 재검토하여야 한다.
		5.2	정보보호관리체계의 모니터링 및 개선	정보보호관리체계가 신청기관의 정보보호정책과 목적을 충족시키는지 여부에 대하여 모니터링하여, 개선사항을 식별하고, 적절한 수정이나 예방조치를 통하여 효과적으로 개선사항을 구현하여야 한다. 이에 관련된 조치와 결과는 신청기관의 임직원에게 전달하여야 하고, 관련자들에게 자문을 구하여야 한다.
		5.3	내부감사	신청기관은 정보보호관리체계가 계획된 절차에 따라 효과적으로 실행되는지를 점검하기 위하여 감사의 기준, 범위, 주기 및 방법을 규정하고, 계획된 주기로 내부감사를 수행하여야 한다. 또한 감사의 기획 및 수행, 그리고 결과보고, 기록 유지 및 이행 모니터링에 대한 책임과 요구사항을 문서화된 절차에 의해 규정하여야 한다. 피감사분야의 관리자는 발견된 보완조치 사항을 처리하고, 검증·보고됨을 보장하여야 한다.

[별표 5]

인증심사기준 - 문서 작성 및 관리 통제사항(제11조 제2호관련)

	문서화	문서화 상세내용
1	문서요건	정보보호관리체계 수립 및 이행에 관련된 모든 문서는 해당 신청기관의 규모, 기능 등을 고려하여 문서화하여야 하며, 신청기관의 정보보호정책에 따라 필요한 모든 임직원 및 관련자들이 쉽게 이용할 수 있어야 한다.
2	문서의 통제	「1. 문서요건」에 의해 작성된 문서는 문서의 발행전 타당성 승인, 주기적 또는 필요시 문서의 검토·갱신 및 재승인, 문서의 변경과 현재 개정상태의 식별, 문서배포, 폐기된 문서의 사용금지 등의 통제를 정의한 절차를 수립하여야 한다.
3	운영기록의 통제	정보보호관리체계를 효과적, 효율적으로 운영하기 위해서 기록을 확인, 유지보수, 보존, 폐기하는 문서화된 절차를 수립하고 유지·관리하여야 한다. 이 문서화된 절차에는 접근자의 신원확인, 기록의 저장, 보호, 검색, 유지기간, 처분 등의 통제에 필요한 절차를 포함하여야 한다. 또한 기록은 읽기 쉽고, 식별 가능하며, 관련 활동을 추적할 수 있어야 한다.

[별표 6]

인증심사기준 - 정보보호관리 통제사항(제11조 제3호관련)

	통제분야		통제목적		통제사항	통제내용
1	정보보호 정책	1.1	정책의 승인 및 공표	1.1.1	정책의 승인	문서화된 정보보호정책은 최고경영자의 승인을 받아야 한다.
				1.1.2	정책의 공표	정보보호정책 문서는 모든 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.
		1.2	정책의 체계	1.2.1	상위 정책과의 일관성	정보보호정책은 신청기관의 사업목표 및 정보기술정책과 일관성을 유지하여야 한다.
				1.2.2	정책 문서의 유형	정보보호정책을 구체적으로 시행하기 위한 정보보호 지침, 절차 및 표준을 수립하여야 한다. 또한 필요한 경우 특정 시스템 또는 서비스에 대한 상세한 정보보호정책을 수립할 수 있다.
		1.3	정책의 유지관리	1.3.1	주기적 검토	정기적으로 정보보호정책의 타당성을 검토하여야 하며, 중대한 보안사고 발생, 새로운 위협 또는 취약성의 발생, 정보보호 환경에 중대한 변화 등이 발생했을 경우에는 관련된 사항의 타당성을 추가로 검토하여야 한다.
2	정보보호 조직	2.1	조직의 체계	2.1.1	조직의 구성	신청기관내 정보보호관리 활동을 계획, 관리하는 정보보호관리자가 있어야 하며, 필요에 따라 정보보호위원회를 구성할 수 있다.

	통제분야		통제목적		통제사항	통제내용
2	정보보호 조직	2.1	조직의 체계	2.1.2	외부전문가 활용	정보보호정책 수립, 위험분석·평가, 통제사항의 선택과 구현, 보안사고 대응 등 중요한 정보보호관리 활동에 도움을 받기 위하여 외부 전문가의 조언을 받을 수 있다. 외부 전문가의 신청기관 자원에 대한 접근은 「3. 외부자 보안」의 대상이 된다.
		2.2	책임과 역할	2.2.1	정보보호 관리자	최고경영자의 지정을 받은 정보보호관리자는 정보보호정책 수립, 정보보호 위원회의 구성 및 운영, 위험분석 및 관리, 보안사고 대응 및 복구 등의 정보보호에 관한 업무를 총괄 관리하여야 한다.
				2.2.2	정보보호 위원회	신청기관 전반에 걸친 중요한 정보보호 관련 심의 및 승인 기능을 수행하며 필요한 자원할당을 통해 정보보호관리 활동이 적절히 수행될 수 있도록 하여야 한다.
3	외부자 보안	3.1	계약 및 서비스 수준협약 보안관리	3.1.1	위부위탁 계약시 보안 요구사항	신청기관의 업무를 외부위탁 하는 경우에는 정보시스템, 네트워크, 인력 및 사무환경 등을 관리·통제하기 위한 보안요구사항을 계약서 상에 명시하여야 하고 요구사항을 서비스수준협약(SLA : Service Level Agreement)에 반영하여야 한다.
				3.1.2	제3자와의 계약시 보안 요구사항	신청기관이 제3자에게 정보자산에 대한 접근을 허용하는 계약을 체결하는 경우에는 신청기관의 정보보호정책 준수 및 필수 보안요건을 포함하는 공식적인 계약을 하여야 한다.

	통제분야		통제목적		통제사항	통제내용
3	외부자 보안	3.2	외부자 보안 실행관리	3.2.1	외부위탁 보안관리	외부위탁 업체가 계약서 및 서비스 수준 협약 명시된 보안요구사항을 충분히 이행하는지 주기적으로 점검하고, 필요시 감사를 수행하여야 한다.
				3.2.2	제3자 보안관리	신청기관의 정보자산에 대한 제3자의 접근을 통제하여야 한다. 업무상 불가피하게 접근을 허용해야 할 경우에는 접근유형 및 접근사유를 파악하고 위험 요소를 고려하여 관리하여야 한다.
4	정보자산 분류	4.1	정보자산의 조사 및 책임할당	4.1.1	정보자산 조사	신청기관의 정보자산을 조사하고 정보자산별로 신청기관에서의 가치, 업무 영향, 법적 준수사항 등을 고려하여 중요도를 결정하여야 한다.
				4.1.2	정보자산별 책임할당	조사된 정보자산에 대하여 소유자, 관리자, 사용자를 확인하고, 적절한 통제 유지를 위해 책임소재를 명확히 하여야 한다.
		4.2	정보자산의 분류 및 취급	4.2.1	정보자산의 분류	정보자산이 신청기관에서 차지하는 가치와 신청기관에 미치는 영향을 고려하여 분류방식을 선택하고 분류하여야 한다.
				4.2.2	보안등급과 취급	중요도에 따라 분류된 정보자산에 보안등급을 부여하고, 물리적, 전자적 보안등급 표시를 부착, 관리하여야 한다. 또한 보안등급의 부여에 따른 취급 절차도 정의하여 이행하여야 한다.

	통제분야		통제목적		통제사항	통제내용
5	정보보호 교육 및 훈련	5.1	교육 및 훈련 프로그램 수립	5.1.1	교육 및 훈련계획	정보보호 인식제고 및 실제 운영에 필요한 교육·훈련 계획을 종합적으로 수립하여 이행하여야 한다
				5.1.2	교육 및 훈련대상	교육 및 훈련의 대상에는 신청기관의 임직원 및 관련 외부자를 포함하여야 한다.
				5.1.3	교육 및 훈련내용	교육 및 훈련은 정보보호정책, 정보보호인식, 보안요구사항, 법적인 책임, 보안사고 대응절차, 업무연속성 관리 등을 포함하여야 하고, 교육대상자의 직위 및 담당하는 업무의 특성에 따라 구분하여 실시하여야 한다.
		5.2	시행 및 평가			교육 및 훈련은 정기적으로 실시하여야 하며, 정보보호정책이나 절차 및 역할의 변경이 있는 경우에는 수시로 실시하고 이에 대한 기록을 남겨야 한다. 또한 교육훈련 종료 후 검토를 통하여 차기 교육에 반영하여야 한다.
6	인적 보안	6.1	책임할당 및 규정화	6.1.1	책임할당	정보보호업무를 이행하는 역할과 책임을 문서화하여야 한다. 문서화의 내용에는 정보보호정책을 수립, 구현, 운영하는 일반적인 책임과 특정 정보자산의 보호와 활동에 대한 구체적인 책임을 포함하여야 한다.
				6.1.2	인사규정	인사규정에는 정보보호에 대하여 직원이 지켜야 할 책임 및 관련 법규상의 책임을 명시하여야 한다. 특히, 정보보호업무를 담당하는 자와 정보시스템 사용자 및 관리자는 보다 명확한 책임을 명시하여야 하며, 직원이 책임을 이행하지 않는 경우를 대비한 적절한 처벌규정을 포함하여야 한다.

	통제분야		통제목적		통제사항	통제내용
6	인적 보안	6.2	적격심사 및 주요 직무담당자 관리	6.2.1	적격심사	계약직 및 임시직원은 물론 정식직원 채용시 신원, 업무능력, 교육정도, 경력 등에 대한 적격심사가 이루어져야 한다. 직원들이 용역회사를 통하여 충원되는 경우에는 용역회사와의 계약서에 적격심사에 따르는 책임사항을 명문화하여야 한다.
				6.2.2	주요직무 담당자 관리	정보시스템 접근 권한을 포함하는 업무가 새로이 할당될 때, 특히 재무정보나 비밀정보와 같이 중요한 정보를 처리하는 담당자는 별도의 관리를 수행하여야 한다.
		6.3	비밀유지	6.3.1	비밀유지 서약서	직원으로부터 비밀유지 서약서에 서명을 받아야 하며, 임시직원이나 제3자에게 정보에 대한 접근 권한을 부여할 경우에도 그들로부터 비밀유지 서약서에 서명을 받아야 한다. 직원의 고용계약에 변경이 있을 경우, 특히 직원이 퇴사하거나 계약기간이 만료될 때에는 비밀유지 서약서를 환기시켜야 한다.
7	물리적 보안	7.1	물리적 보안대책	7.1.1	물리적 보호구역	특별한 보호가 필요한 시설 및 장비를 권한 없는 자의 물리적 접근 및 각종 물리적, 환경적 재난으로부터 보호하기 위하여 보호구역을 정의하고 이에 따른 보안대책을 수립·이행하여야 한다. 이 경우 제한구역, 접견구역, 장비출하구역 등을 별도로 지정하여 각각에 적합한 보안 조치와 절차를 수립하여야 한다.
				7.1.2	물리적 접근통제	보호구역을 출입하는 자를 감시·통제하고 권한 없는 자의 출입을 방지하기 위하여 수립된 보안 절차에 따라 필요한 조치를 수행하고 주기적으로 검토하여야 한다.

	통제분야		통제목적		통제사항	통제내용
7	물리적 보안	7.2	데이터 센터 보안	7.2.1	위치 및 구조 조건	데이터센터는 물리적, 환경적 위험이 적은 곳에 위치하고 구조의 안정성을 확보하여야 한다.
				7.2.2	출입통제	데이터센터의 출입은 적절한 출입통제절차에 의하여 이행되어져야 하며, 출입자를 식별하고 기록·관리하여야 한다. 또한 출입자 기록 대장은 정기적으로 점검하여야 한다.
				7.2.3	내부설비	화재·수재 등의 각종 재해에 대비한 시설을 충분히 설치하여야 하고, 비상연락장치 및 비상구, 물리적 접근통제 및 시건장치를 설치하여야 한다.
		7.3	장비보호	7.3.1	주요 시스템 보호	신청기관내의 주요 시스템에 대한 별도의 출입통제를 실시하거나 이중의 보호장치를 설치하고, 시스템 관리자는 주요 시스템 접근에 대한 보안대책을 수립하여야 한다.
				7.3.2	장비의 배치	장비는 환경적인 위협과 위험, 불법접근에 대한 위험을 감소시키기 위해 적절한 위치에 배치하고 이를 보호하여야 한다.
				7.3.3	전원공급	전원공급 이상이나 기타 전기관련 사고 발생시 전원을 지속적으로 공급하기 위하여 장비 제조업체의 사양에 따라 적절히 관리하여야 한다.
				7.3.4	케이블 보호	데이터를 송·수신하거나 정보서비스를 지원하는 전력 및 통신 케이블은 방해되거나 손상을 입지 않도록 보호하여야 한다.
				7.3.5	장비의 보수	장비는 지속적인 가용성과 무결성을 위하여 장비 제공자가 지시한 명세에 따라 유지보수를 하여야 하고 유지·보수에 대한 기록을 남겨야 한다.

	통제분야		통제목적		통제사항	통제내용
7	물리적 보안	7.3	장비보호	7.3.6	장비의 안전한 폐기 및 재사용	중요한 정보를 담고 있는 저장 매체의 폐기시에는 이를 물리적으로 파기하여야 하며, 중요 데이터나 정품 소프트웨어는 폐기하기 전에 매체에 기록된 내용이 완전히 삭제되어 복구가 불가능한지 확인하고 점검하여야 한다.
		7.4	사무실 보호			책상 위에 중요한 문서나 저장 매체를 남겨놓지 않도록 하고, 통상 근무시간 동안이나 그 외의 시간에 비인가된 자에 의한 정보 접근, 손상을 방지하기 위하여 컴퓨터 화면에 정보처리에 관한 사항을 남겨놓지 않도록 하여야 한다.
8	시스템 개발보안	8.1	분석 및 설계 보안관리	8.1.1	보안 요구사항 정의	새로운 시스템 개발, 기존시스템 개선시 보안요구사항을 문서로 명확히 하여야 하며, 보안요구사항에는 사용자 접근권한의 부여원칙과 접근통제 유형 등을 포함하여야 한다.
				8.1.2	입력 데이터 검증	응용시스템 설계시 입력 요구사항을 정의하고 문서화하여야 하며, 입력 데이터의 정확성, 무결성, 신뢰성을 판단하기 위한 표준을 마련하여야 한다.
				8.1.3	내부 처리의 검증	응용시스템 설계시 내부처리 요구사항을 정의하고 문서화하여야 하며, 응용소프트웨어의 처리 작업을 검증하고, 무결성을 회복할 수 있는 기능을 포함하여야 한다.
				8.1.4	출력 데이터 검증	응용시스템 설계시 출력 요구사항을 정의하고 문서화하여야 하며, 출력 데이터의 정확성, 무결성, 신뢰성을 판단하기 위한 대책을 마련하여야 한다.

	통제분야		통제목적		통제사항	통제내용
8	시스템 개발 보안	8.1	분석 및 설계 보안관리	8.1.5	인증 및 암호	응용시스템 설계시 반드시 사용자 인증에 대한 보안 요구사항을 고려하여야 한다. 중요한 메시지의 경우 무결성이 요구될 때 메시지 인증기법을 적용하고 비밀성이 요구될 시 암호화를 적용하여야 한다.
				8.1.6	보안기록 관리	응용시스템 설계시 사용자의 인증, 데이터 분실, 수정, 오남용 등을 점검하고 방지하기 위하여 보안에 관련된 로그, 감사증적 등을 확보할 수 있는 기능을 반영하여야 한다.
		8.2	구현 및 이행 보안관리	8.2.1	구현 및 시험	응용시스템 구현시 코딩표준에 따라 응용시스템을 구현하고, 보안요구사항에 대한 시험을 수행하여야 한다.
				8.2.2	운영환경 이행보안	운영 프로그램의 수정은 적절한 권한을 지닌 사람만이 시행하여야 하고, 운영시스템은 실행코드만 보유하여야 한다. 실행코드는 성공적인 시험과 사용자 인수 후에 실행하여야 한다.
				8.2.3	시험 데이터의 보안	시험 데이터는 운영데이터에 준하여 보호하고 통제하여야 하며, 운영환경에 대하여 적용되는 접근통제 절차를 시험환경에도 적용하여야 한다. 운영데이터가 시험환경으로 복사될 경우 허가절차를 수립하여 이행하고 시험 완료 후 운영데이터는 시험시스템에서 삭제하여야 한다. 운영데이터 사용 및 복사는 기록을 남겨야 한다.
				8.2.4	소스 프로그램의 접근보안	소스 프로그램은 실제 운영 환경에 보관하지 않는 것을 원칙으로 하며, 소스 프로그램 관리자는 각 운영시스템 별로 지정하여야 한다. 또한 소스 프로그램 접근에 대한 통제절차를 수립하고 이행하여야 한다.

	통제분야		통제목적		통제사항	통제내용
8	시스템 개발 보안	8.3	변경관리	8.3.1	변경관리 절차	정보시스템의 파괴와 손상을 최소화하기 위하여 공식적인 변경관리 절차를 수립하고 이행하여야 한다.
				8.3.2	운영체제 변경시의 검토	운영체제 변경이 필요한 경우 응용시스템의 운영이나 보안에 미치는 영향을 분석, 검토하여야 한다.
				8.3.3	소프트웨어 패키지 변경	소프트웨어 패키지는 가능한 수정하지 않고 사용하고, 패키지 변경시에는 공급자의 동의를 얻으며, 수정이 가능한지 확인하여야 한다. 모든 변경사항은 시험하고 문서화하여야 한다.
9	암호 통제	9.1	암호 정책			암호사용에 대한 정책을 수립하여야 한다.
		9.2	암호사용			암호 정책에 따른 암호 사용시 적절한 암호 알고리즘의 유형, 신뢰성 및 키 길이를 결정하여야 한다.
		9.3	키관리			암호 키에 대한 관리지침, 절차 및 방법을 마련하고 필요시 복구방안을 마련하여야 한다.
10	접근 통제	10.1	접근통제 정책	10.1.1	정책의 문서화	업무 요구사항에 따라 접근 통제의 방법과 범위 등을 정의하고 문서화하여야 한다.
				10.1.2	정책의 내용	접근통제 정책은 데이터, 프로그램, 주요 시스템, 네트워크 등에 대한 접근제한을 포함하여야 하며, 여기에는 보안요구사항, 데이터 및 서비스 접근시의 법적, 계약적 제한, 분산 네트워크상의 접근권한 관리 등을 포함하여야 한다.
				10.1.3	접근 통제 규칙	항상 존재하는 규칙과 일정기간이나 선택적으로 존재하는 규칙에 대한 구분, 실행 전에 관리자의 승인을 필요로 하는 규칙과 그렇지 않은 규칙의 구분 등을 포함한 접근 통제 규칙을 명시하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.1	접근통제 정책	10.1.4	접근통제 방법	접근통제 방법은 정책 및 절차에 의해 결정된 접근권한을 적절하게 반영하여야 한다.
				10.1.5	접근통제 정책 검토	접근에 대한 모니터링을 통해 정책과의 일치성을 주기적으로 검토하고, 접근통제 정책의 적정성을 확인하여야 한다.
		10.2	사용자 접근 관리	10.2.1	사용자 등록	정보시스템 및 서비스에 대한 접근을 통제하기 위한 공식적인 사용자 등록 및 해지 절차를 마련하여야 한다.
				10.2.2	특수권한 관리	시스템이나 응용프로그램에 대한 통제를 우회할 수 있는 특수권한의 할당 및 사용을 관리하여야 한다.
				10.2.3	사용자 패스워드 관리	사용자 패스워드의 관리절차를 수립하고 이행하여야 한다.
				10.2.4	사용자의 접근권한 검토	데이터나 정보 서비스에 대한 접근을 관리하기 위해서 정기적으로 접근 권한에 대하여서 점검을 하여야 한다.
				10.2.5	사용자의 책임	시스템 및 패스워드 관리 책임은 사용자 자신에게 있음을 주지시키고 관리지침을 제공하여야 한다.
		10.3	접근통제 영역	10.3.1	네트워크 접근	비인가된 접근을 막기 위해 네트워크의 내·외부 연결통제, 사용자 터미널과 컴퓨터 서비스간에 물리적 및 논리적 경로의 통제, 사용자 인증, 고장 진단 포트에 대한 접근통제 등을 포함한 네트워크 접근정책을 수립하고 이행하여야 한다.
				10.3.2	운영체제 접근	안전한 로그온 절차, 식별 및 인증 관리, 필요시 터미널 자동확인 등을 포함하여 시스템의 운영체제 접근을 통제하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.3	접근통제 영역	10.3.3	응용 프로그램 접근	사용자 접근이 허가되지 않은 응용 프로그램의 기능들에 대한 정보 제공을 제한하여야 한다. 또한 민감한 정보를 처리하는 응용 프로그램의 출력물은 허가된 위치에서만 전달하여야 한다. 민감한 응용 시스템은 반드시 일반적인 환경과 분리하여야 한다.
				10.3.4	데이터베이스 접근	데이터베이스의 뷰, 레코드 또는 필드 레벨에서의 데이터에 대한 접근통제, 데이터사전 및 데이터베이스 유틸리티에 대한 접근통제, 민감 정보의 암호화 등을 통해 데이터베이스내의 정보를 보호하여야 한다.
11	운영관리	11.1	운영 절차와 책임	11.1.1	운영절차의 문서화	보안정책에 의해 정의된 운영지침과 절차는 문서화하여 관리하여야 한다. 운영관리를 외부에 용역을 주는 경우에도 계약서에 이를 반영하여야 한다.
				11.1.2	정보자산의 변경관리	정보시스템 관련 자산들을 조사하고, 모든 변경사항들을 반영할 수 있는 공식적인 관리책임 및 절차를 수립하여야 한다.
				11.1.3	직무 분리	부주의에 의한 또는 고의적인 시스템 오용의 위험을 감소시키기 위해 직무를 분리하고, 직무 분리가 어려운 특수한 경우 별도의 관리감독 대책을 수립하여야 한다.
				11.1.4	개발과 운영환경의 분리	원칙적으로 개발, 시험, 운영 환경을 분리하여야 한다. 또한 응용프로그램을 개발환경으로부터 운영환경으로 이전하는 절차를 정의하고 문서화하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영 관리	11.1	운영 절차와 책임	11.1.5	외부 운영 설비 관리	외부자가 정보시스템 및 장비를 관리하는 경우 데이터의 손상, 손실 등의 상황을 고려하여 통제방안을 수립하고 계약서에 반영하여야 한다.
		11.2	시스템 운영	11.2.1	시스템 도입	정보시스템의 도입을 위해서 도입 계획 및 정책을 수립하여야 한다.
				11.2.2	시스템 인수	새로운 정보시스템의 설치 또는 수정에 따른 인수기준을 수립하고, 시스템 구매 계약서에 반영하여야 한다. 또한 시스템은 이 기준에 의해 시험을 한 후 인수하여야 한다.
				11.2.3	성능관리	신청기관에서 요구되는 성능 요구사항을 충족시킬 수 있도록 성능관리를 수행하여야 한다.
				11.2.4	용량관리	신청기관에서 요구되는 용량 요구사항을 충족시킬 수 있도록 용량계획을 통해 적정한 용량을 확보하고, 주어진 용량을 최적으로 사용할 수 있는 관리방안을 수립하여 이에 따른 용량관리를 수행하여야 한다.
				11.2.5	백업 및 복구 관리	데이터 및 장비의 무결성과 가용성을 유지하기 위해 백업 계획을 수립하여 이행하여야 하며, 사고 발생시 적시에 복구할 수 있도록 관리하여야 한다.
				11.2.6	장애관리	시스템의 장애시 효과적으로 대응하기 위해 탐지, 기록, 분석, 복구, 보고 등 적절한 조치를 취하여야 한다.
				11.2.7	로그관리	시스템 운영의 확인이나 사고조사를 위해 활동에 대한 기록을 남기고 주기적으로 검토하여야 한다.
				11.2.8	보안 시스템 운영	보안시스템에 대해서는 그 유형별로 설치, 운영에 대한 절차를 수립하고, 절차이행을 주기적으로 검토하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영 관리	11.3	네트워크 운영	11.3.1	네트워크 운영대책	네트워크 운영 보안 유지를 위해 직무 분리, 접근권한 통제, 원격접속 설비 관리, 네트워크 분리 등을 위한 책임 및 절차 등을 포함한 대책을 수립하여야 한다.
				11.3.2	인터넷 접속관리	인터넷망과 접속시 침입차단시스템을 통하여 접근통제를 수행하여야 하며, 필요시 침입탐지시스템 등을 활용하여 접근을 모니터링 하여야 한다.
				11.3.3	원격운영 관리	네트워크를 통해 시스템을 운영하는 경우 원칙적으로 시스템 관리는 내부의 특정 터미널에서만 할 수 있도록 제한하고, 외부에서 네트워크를 통하여 시스템을 관리할 경우에는 사용자 인증, 암호 및 접근통제 기능을 설정하여야 한다.
		11.4	매체 및 문서관리	11.4.1	매체 취급 및 보관	허가되지 않은 유출이나 오용으로부터 정보를 보호하기 위해, 매체의 취급 및 보관에 대한 절차를 수립하고 운영하여야 한다.
				11.4.2	매체의 폐기	매체 폐기를 부주의하게 이행하여 외부자에게 주요정보가 누출되지 않도록 폐기지침을 수립하고 운영하여야 한다.
				11.4.3	시스템 문서의 보안	보안절차, 운영매뉴얼, 운영기록 등 주요 시스템 문서들은 안전하게 보관하고 적절한 폐기절차에 따라 폐기하여야 한다.
		11.5	악성 소프트웨어 통제			바이러스 등의 악성 소프트웨어로부터 시스템을 보호하기 위해 악성 소프트웨어들을 예방하고 탐지, 대응하는 대책을 수립하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영 관리	11.6	이동컴퓨팅 및 원격 작업	11.6.1	이동 컴퓨팅	휴대용 정보통신기기의 사용시에 사업 정보를 보호하기 위한 보안 정책을 수립하고, 내부 네트워크로의 연결 및 공공 장소에서의 사용에 대한 정책을 수립하여야 한다.
				11.6.2	원격 작업	재택 근무와 같은 원격 작업 수행시 이에 대한 물리적, 논리적 보호를 위한 정책과 절차를 마련하여야 한다.
12	전자 거래 보안	12.1	교환 합의서			신청기관간의 정보 및 소프트웨어 교환시에는 이에 대한 합의가 이루어져야 하고, 관리적 책임 및 절차, 전송의 기술적 기준, 인증기준, 데이터의 책임성 등을 반영한 교환 합의서를 작성하여야 한다.
		12.2	전자거래 보안관리			전자거래 시 사기, 계약 분쟁, 정보의 노출 및 수정 등으로부터 보호하기 위해 신원확인, 무결성, 암호화, 부인방지 등의 대책을 수립하여 운영하여야 한다.
		12.3	전자우편			전자 우편 서비스에 대한 가용성, 전자우편 내용에 대한 무결성 및 기밀성과 이에 따른 책임과 위험을 고려한 보안지침 및 대책을 수립하여 운영하여야 한다.
		12.4	공개서버의 보안관리			웹서버 등에 정보를 공개할 경우 정보에 대한 수집, 저장 및 공개에 따른 허가 및 게시절차를 수립하여야 하고, 공개서버에 대한 물리적, 논리적 보안대책을 수립하고 운영하여야 한다.
		12.5	이용자 공지사항			전자거래의 안전한 이행을 위하여 이용자에게 해킹위험, 계정 및 패스워드 관리, 접속관리 등에 대한 공지를 통해 안전거래 준수를 권고하여야 한다.

	통제분야		통제목적		통제사항	통제내용
13	보안사고 관리	13.1	대응 계획 및 체계	13.1.1	대응계획 수립	보안사고의 정의 및 범위, 긴급연락체계 구축, 보안사고 발생시 보고 및 대응 절차, 사고 복구조직의 구성, 교육계획 등을 포함한 보안사고 대응 계획을 수립·이행하여야 한다.
				13.1.2	보안사고 대응체계 구축	보안사고의 대응이 신속하게 이루어질 수 있도록 중앙 집중적인 대응체계를 구축하고, 대응체계에는 내부 직원뿐 아니라 외부기관 및 전문가들과의 협조체계를 반영하여야 한다.
		13.2	대응 및 복구	13.2.1	보안사고 대응 교육 및 훈련	보안사고 대응 계획, 절차 및 방법에 대하여 정기적으로 교육을 실시하여야 하며 사고 처리 후 재발방지를 위하여 필요한 교육훈련을 실시하여야 한다
				13.2.2	보안사고 보고	사고의 징후 또는 보안사고 발생을 인지한 때에는 보고체계에 따라 가능한 한 신속히 보고하여야 한다. 시스템이나 네트워크의 보안 취약점과 소프트웨어 기능장애 또한 신속히 보고하여야 한다.
				13.2.3	보안사고 처리 및 복구	보안사고 보고시 처리, 복구 절차에 따라 처리와 복구를 신속히 이행하여야 한다.
		13.3	사후관리	13.3.1	보안사고 분석 및 정보의 공유	보안사고가 처리되고 종결된 후 이에 대한 분석을 이행하여야 하며, 그 결과를 보고하여야 한다. 또한 사고에 대한 정보와 발견된 취약성들을 관련 신청기관과 임직원에게 공유하여야 한다.
				13.3.2	재발방지	보안사고로부터 얻은 정보를 활용하여, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하여야 한다. 이를 위해 필요한 경우 정책, 절차, 조직 등의 보안체계에 대한 변경을 하여야 한다.

	통제분야		통제목적		통제사항	통제내용
14	검토, 모니터링 및 감사	14.1	법적 요구사항 준수 검토	14.1.1	요구사항 명시	정보시스템에 대해 관련된 모든 법, 규제, 계약, 정책, 기술상의 요구사항을 정의하고 문서화하여야 하며, 이들 요구사항을 만족시키기 위해 필요한 특정 통제나 개별 책임 등도 정의하고 문서화하여야 한다.
				14.1.2	준수 검토	정보통신망이용촉진및정보보호등에관한법률, 신용정보의이용및보호에관한법률 등의 개인정보보호 관련법 및 저작권법, 컴퓨터프로그램보호법 등 지적재산권법 등의 관련 법규의 준수여부를 검토하여야 한다.
				14.1.3	증거자료 수집	보안사고 처리 및 계약 증빙을 위하여 신청기관이나 개인에 대한 소송을 지원하기 위한 적정한 증거 자료를 확보하여야 한다.
		14.2	정보보호 정책 준수 검토	14.2.1	검토 계획	검토의 대상, 주기, 방법, 범위, 절차, 검토자를 포함한 검토계획 및 정책이 수립되어야 한다. 이를 근거로 보안요구사항에 대한 통제와 책임의 준수에 대한 적정성을 검토하여야 한다.
				14.2.2	정책의 준수	모든 정보보호 정책, 절차의 준수여부를 검토하여야 한다.
				14.2.3	기술적 점검	정보시스템이 정보보호표준 및 절차에 따라 운영·관리되고 있는지 정기적으로 기술적 점검을 실시하여야 한다. 이에 따라 취약성들을 발견한 후 필요한 조치를 취하여야 한다.

	통제분야		통제목적		통제사항	통제내용
14	검토, 모니터링 및 감사	14.3	모니터링	14.3.1	접근 및 사용 모니터링	사용자의 시스템, 네트워크 사용 및 접근이 명확하게 허용된 범위 안에 있는지를 확인하기 위해 모니터링 절차를 수립하고 이행하여야 한다. 모니터링 결과는 정기적으로 점검하여야 하고 위험의 정도에 따라 점검 주기를 결정하여야 한다.
				14.3.2	감사기록 분석 및 보관	모니터링을 위한 감사 기록을 생성하고, 분석하며 일정 기간 동안 보관하여야 한다.
				14.3.3	시각 동기화	감사 기록의 명확성을 보장하고 법적인 자료나 징계 자료로서 효력을 갖기 위해서는 시스템 시각을 정확히 설정하여야 한다.
		14.4	보안감사	14.4.1	보안감사 계획 및 이행	보안 감사 대상, 범위, 주기, 방법, 절차, 감사자, 감사도구를 포함한 보안감사 계획을 수립하고 이행하여야 한다.
				14.4.2	감사결과 및 사후관리	감사의 결과에 따라 감사보고서를 작성하고 적정한 책임자에게 보고하며, 감사 지적 내용이 이행되도록 사후관리하여야 한다.
15	업무 연속성 관리	15.1	업무연속성 관리 체계 수립	15.1.1	업무연속성 관리 과정 수립	개시단계, 업무연속성전략수립단계, 구현단계, 운영관리단계 등 업무연속성관리를 위한 과정을 사전에 정의하여야 한다. 개시단계에는 업무연속성관리에 대한 정책 수립 및 범위설정, 자원분배를 포함하여야 하며, 업무연속성전략수립단계는 업무영향분석을 통해 이루어져야 한다. 구현단계에는 재해복구 및 위험감소 대책, 업무연속성계획의 문서화를 포함하여야 하며, 운영관리단계에는 시험, 교육훈련, 검토 및 갱신을 포함하여야 한다.

	통제분야		통제목적		통제사항	통제내용
15	업무 연속성 관리	15.1	업무연속성 관리 체계 수립	15.1.2	업무연속성 계획 프레임워크 수립	업무별 연속성 계획의 이행에 필요한 조건, 응급절차, 대체절차 등을 고려하여 연속성 계획들이 일관성을 유지할 수 있도록 프레임워크를 수립하여야 한다.
		15.2	업무연속성 계획 수립과 구현	15.2.1	업무영향 분석	재난재해별로 업무에 미칠 수 있는 영향을 피해규모와 복구에 소요되는 시간 등을 고려하여 분석하고 그 결과를 기초로 구체적인 업무복구목표 및 복구를 위한 최소한의 요구사항을 설정하여야 한다.
				15.2.2	업무연속성 계획 수립	업무복구목표 및 최소 요구사항을 구현하기 위한 여러 대안들을 평가하여 업무연속성을 위한 전략을 수립하고 대책 구현을 위한 계획을 수립하여야 한다.
				15.2.3	업무연속성 계획 구현	업무연속성계획에서 수립한 위험감소 조치 및 재해복구를 위한 설비를 구현하며 필요한 계획 및 절차 등을 문서화하여야 한다.
		15.3	업무 연속성 계획 시험 및 유지관리	15.3.1	업무연속성 계획 시험	환경의 변화 또는 부정확한 전제 등으로 인한 오류를 제거할 수 있도록 지속적인 시험을 수행하며, 시험 계획에는 시기, 방법, 절차 등을 포함하여야 한다.
				15.3.2	업무연속성 계획 유지·관리	업무연속성계획에 대해 정기적인 교육 및 훈련을 실시하고 지속적인 검토와 평가 및 변경관리를 수행하여야 한다.

[별지 제1호서식]

(앞 쪽)

정보보호관리체계인증기관 지정신청서				처리기간 3 월
신청인	①업 체 명 및 대 표 자 성 명		②설 립 일 자	
	③소 재 지		④전 화 번 호	
	⑤직 원 수	명	⑥인증심사업무를 전담하는 직원의 수	명

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조 및 같은 법 시행령 제48조에 따라 위와 같이 정보보호관리체계인증기관의 지정을 신청합니다.

년 월 일

신청인 (서명 또는 인)

방송통신위원회 귀중

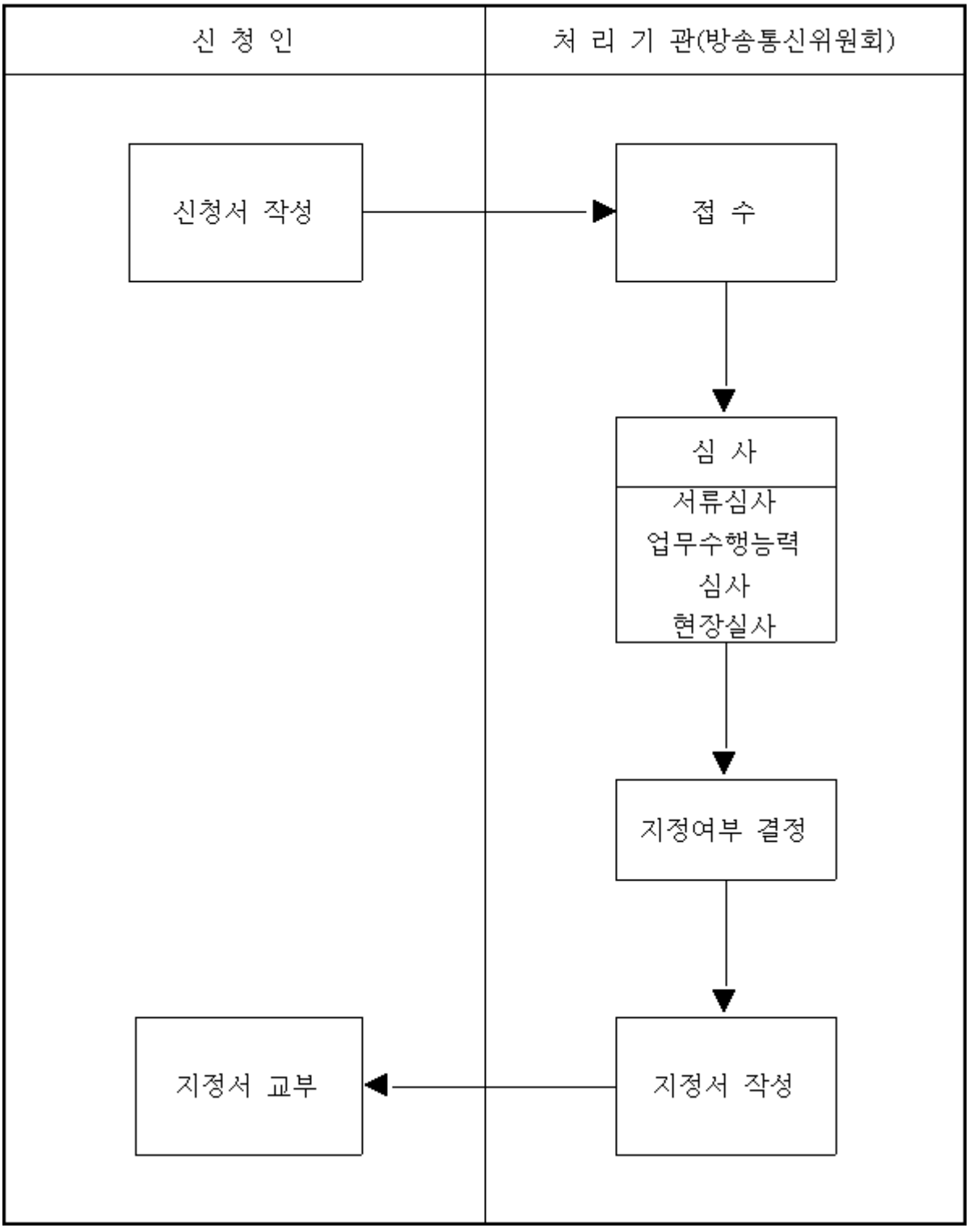
구비서류	신청인(대표자) 제출서류	담당공무원 확인사항 (부동의하는 경우 해당서류 제출)	수 수 료
	1. 정관 2. 별지 제2호서식의 인증심사업무를 전담하는 직원 보유현황과 이를 증명할 수 있는 서류 3. 별표 제1호에 따른 업무수행능력심사를 위하여 필요한 서류	법인등기부 등본 (법인인 경우)	없 음

본인은 이 신청서의 처리와 관련하여 「전자정부법」 제21조제1항에 따른 행정정보의 공동이용을 통하여 담당공무원이 위의 담당공무원 확인사항을 확인하는 것에 동의합니다.

신청인(대표자) (서명 또는 인)

210㎜×297㎜(일반용지 60g/㎡)

이 신청서는 아래와 같이 처리됩니다. (뒤 쪽)



[별지 제2호서식]

(앞 쪽)

인증심사업무를 전담하는 직원의 보유현황

업체명			
대표자 성명			
소 재 지			
종업원수		인증심사업무를 전담하는 직원의 수	

일련번호	성 명 (한 자)	주 소		최종학력	해당 요건
		생년월일	입사일	취득학위 및 학과(전공)	

210mm×297mm[일반용지 60g/㎡(재활용품)]

(뒤 쪽)

일련번호	성 명 (한 자)	주 소		최종학력	해당 요건
		생년월일	입사일	취득학위 및 학과(전공)	

비 고

1. 「해당요건」란에는 별표 1의 요건 중 당해 인증심사업무를 전담하는 직원이 충족하는 요건을 기재한다.
   예시) 학력 및 경력기준 제2호 가목
2. 기재된 최종학위를 증명할 수 있는 직원의 졸업 또는 학위증명서 사본을 제출하여야 한다.
3. 별표 1의 「자격 및 경력기준」을 충족하는 직원은 기술자격증 사본 등 자격을 취득하였음을 확인할 수 있는 서류를 함께 제출하여야 한다.
4. 정보통신유관경력 또는 정보보호유관경력을 증명할 수 있는 경력증명서(근무부서 또는 담당업무 등이 기재되어야 한다)와 해당 직원이 신청업체에 현재 근무하고 있음을 확인할 수 있는 재직증명서를 함께 제출하여야 한다.

[별지 제3호서식]

정보보호수행실적 명세서

업 체 명					
대 표 자 성 명					
소 재 지					
정보보호수행실적 총계		외 건 (총 천원)			
일련번호	정보보호수행실적 (프로젝트명) 대상기관(기업)명	수행 기간	계약 금액 (천원)	과제책임자	구분

비 고

1. 계약금액란에는 정보보호에 관한 업무를 수행한 대가로서 지급받은 대금을 기재하고, 구분란에는 정보보호에 관한 감사, 감리, 진단, 인증, 컨설팅 등으로 실적을 구분하여 기재한다.

[별지 제4호서식]

(제1쪽)

제 호

정보보호관리체계인증기관지정서

업체명 :

대표자 :

소재지 :

지정의 유효기간 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조 및 같은 시행령 제48조에 따라 위와 같이 정보보호관리체계인증기관으로 지정합니다.

년 월 일

방송통신위원회 위원장 [인]

210㎜×297㎜

(보존용지(1종) 120g/㎡)

(제2쪽)

Registry No.

CERTIFICATE OF DESIGNATION
AS
ISMS Certification Authority

Name of Organization :
Name of Representative :
Address :
Period of Validity :

This is to certify that the above-mentioned organization is designated Information Security Management System (ISMS) certification Authority in accordance with Article 47 of the Act on Promotion of Information and Communication Network Utilization and Information Protection, etc. and Article 48 of Promotion of Information and Communication Network Utilization and Information Protection, Etc. Enforcement Ordinance of Act

Signed by the
Chairman of Broadcasting and Communications Commission
Republic of Korea

210㎜×297㎜
(보존용지(1종) 120g/㎡)

[별지 제5호서식] (앞 쪽)

정보보호관리체계인증신청서

신청인	성 명(대 표 자)		생 년 월 일	
	상호 또는 명칭		사업자등록번호	
	소 재 지		전 화 번 호	
인증신청의 구분		□처음으로 인증신청을 하는 때 □유효기간의 만료로 다시 인증신청을 하는 때 □인증의 범위에 중요한 변경이 있어서 다시 인증신청을 하는 때		
정보보호관리체계의 범위				
정보보호관리체계의 범위에 포함되어 있는 종업원의 수				

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제4항, 동법 시행령 제50조에 따라 위와 같이 정보보호관리체계의 인증을 신청합니다.

년 월 일

신청인 (서명 또는 인)

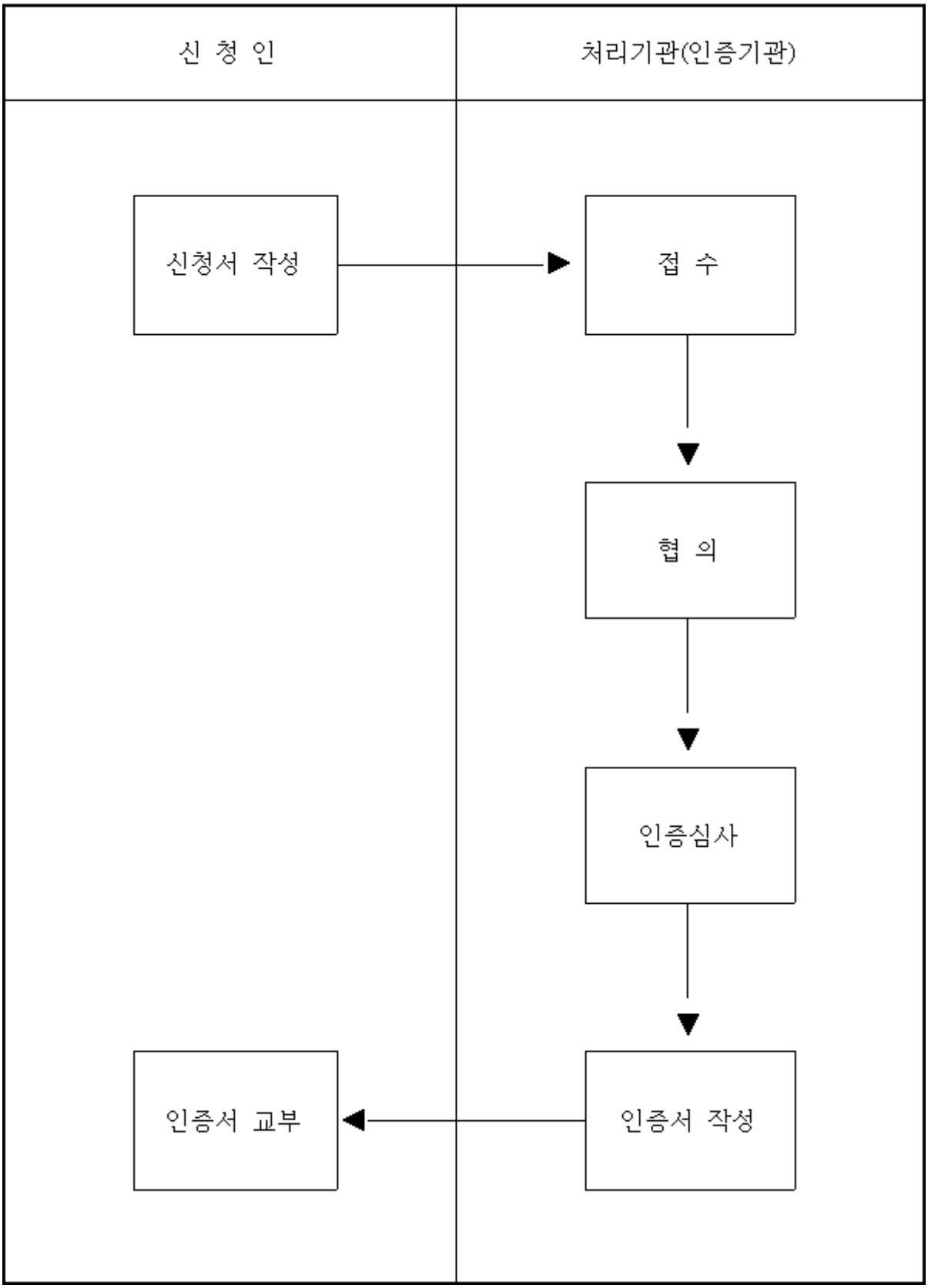
(인증기관명) 귀하

구비서류

1. 법인등기부 등본(법인인 경우에 한합니다)
2. 정보보호관리체계의 내역서

210mm×297mm[일반용지 60g/㎡(재활용품)]

이 신청서는 아래와 같이 처리됩니다. (뒤 쪽)



[별지 제6호서식] (제1쪽)

제 호

정보보호관리체계인증서

상호 또는 명칭 :

대 표 자 :

소 재 지 :

인증의 범위 :

유 효 기 간 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제4항, 같은 법 시행령 제50조에 따라 위와 같이 정보보호관리체계를 인증합니다.

년 월 일

(인증기관장) (인)

210mm×297mm(보존용지(1종) 120g/㎡)

(제2쪽)

Certificate Number :

CERTIFICATE

OF

Information Security Management System

Name of Organization :

Name of Representative :

Address :

Scope of Certification :

Period of Valid :

Date of Issuance :

This is to certify that the above- mentioned organization is compliant to the assessment standard for Information Security Management System certification in accordance with Article 47, Paragraph 1 and 4 of Act on Information Network Utilization and Data Protection, etc., and Article 50 of the Enforcement Ordinance of the Act.

Signed by the

President of ISMS Certification Authority

Republic of Korea

210mm×297mm(보존용지(1종) 120g/㎡)

[별지 제7호서식] 정보보호관리체계 인증서 추가발급 신청서

정보보호관리체계 인증서 추가발급 신청서

신청인	상호 또는 명칭		성 명(대표자)	
	사업자등록번호		전화번호	
	주 소(소재지)			
추가발급 사유				

위와 같이 정보보호관리체계 인증서의 추가발급을 신청합니다.

200 년 월 일

신청인 (서명 또는 인)

[별지 제8호서식] 정보보호관리체계 인증서 변경 신청서

정보보호관리체계 인증서 변경 신청서

신청인	상호 또는 명칭		성 명(대표자)	
	사업자등록번호		전화번호	
	주 소(소재지)			
변경내용	변경전	(국문)		
		(영문)		
	변경후	(국문)		
		(영문)		
변경 사유				

위와 같이 정보보호관리체계 인증서 변경을 신청합니다.

200 년 월 일

신청인 (서명 또는 인)

정보보호관리체계 인증

[시행 2009.11.5] [고시 제2009 - 27호, 2009.11.5, 타법개정]

제1장 총칙

제1조(목적) 이 고시는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하"법"이라 한다) 제47조제2항 및 같은 법 시행령 제47조제2항、제48조제1항제3호、제5항、제50조제6항에 따른 정보보호관리체계 인증에 관한 정보보호관리기준、지정에 필요한 업무수행능력 심사 등에 관한 세부사항과 그 밖에 정보보호관리체계 인증에 관하여 필요한 사항에 대하여 정하는 것을 목적으로 한다.

제2조(용어의 정의) 이 기준에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "업무수행능력심사"란 정보보호관리체계인증기관으로 지정받고자 신청한 법인 또는 단체의 업무수행능력을 세부평가기준에 따라 심사하는 것을 말한다.
2. "정보보호관리체계인증기관"이란 법 제47조에 따른 한국정보보호진흥원과 방송통신위원회가 지정하는 기관을 말한다.
3. "인증"이란 신청기관이 수립하여 운영하고 있는 정보보호관리체계가 인증심사기준 등에 적합함을 정보보호관리체계인증기관이 승인하는 것을 말한다.
4. "인증심사"란 신청기관이 수립하여 운영하는 정보보호관리체계가 인증심사기준 등에 대하여 서면심사 및 기술심사의 방법으로 확인하는 것을 말한다.
5. "정보보호관리과정(이하 ‘관리과정’이라 한다)"이란 정보보호관리체계를 수립、운영하기 위하여 유지、관리하여야 할 과정으로 다음 각목의 5단계 활동을 말한다.
   가. 정보보호정책 수립
   나. 정보보호관리체계 범위설정
   다. 위험관리
   라. 구현
   마. 사후관리
6. "신청기관"이란 이 고시에 따라 정보보호관리체계 인증을 취득하고자 신청한 업체 및 기관 등을 말한다.
7. "외부자"란 신청기관의 직원이 아닌 자를 말한다.

8. "정보보호대책"이란 신청기관이 정보보호관리체계를 수립·운영하기 위하여 별표 6에서 선택한 통제사항을 말한다.

제2장 정보보호관리체계인증기관의 지정 등

제1절 정보보호관리체계인증기관의 지정신청

제3조(정보보호관리체계인증기관의 지정공고) 방송통신위원회는 법 제47조 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」(이하 "영"이라 한다) 제48조에 따라 정보보호관리체계인증기관을 지정할 필요가 있는 때에는 미리 접수신청기간과 신청요령 등을 정하여 관보 및 인터넷 홈페이지에 20일 이상 공고하여야 한다.

제4조(제출서류 등) ①정보보호관리체계인증기관 지정을 신청하는 자는 별지 제1호서식의 정보보호관리체계인증기관 지정신청서를 방송통신위원회에 제출하여야 한다.
②영 제48조제1항제2호에 따라 제1항의 정보보호관리체계인증기관지정신청서에 첨부하여야 하는 "인증심사업무를 전담하는 직원의 보유현황"의 제출서식은 별지 제2호서식과 같다.
③영 제48조제1항제3호에 따른 "업무수행능력심사를 위하여 필요한 서류"라 함은 별표 1과 같다.

제2절 인증심사업무를 전담하는 직원의 자격요건 및 업무수행능력심사

제5조(인증심사업무를 전담하는 직원의 요건 등) ①영 제47조제1항제1호 및 제2항에 따른 "인증심사업무를 전담하는 직원(이하 "인증심사원"이라 한다)의 요건"은 별표 2와 같다.
②법 제47조에 따른 정보보호관리체계인증기관으로 지정신청 하고자 하는 자는 제1항의 인증심사원의 요건을 만족하여야 한다.

제6조(업무수행능력심사 기준 등) ①영 제47조제1항제2호 및 제2항에 따른 업무수행능력심사의 세부평가기준은 별표 3과 같다.
②심사위원회는 제1항에 따라 심사위원 각자가 부여한 점수 중 최고점과 최저점을 제외한 점수들의 평균이 80점 이상인 자를 선별한다.
③심사위원회는 제2항에 따라 선별된 자에 대하여 심사결과 검증 및 업무수행능력의 적합성을 판단한다.

제7조(업무수행능력의 적합성 인정) 방송통신위원회는 제5조 및 제6조에 따라 심사한 결과를 토대로 정보통신망 안전성 및 신뢰성 확보를 위한 종합적인 정보보호관리체계의 업무를 수행하는 자로서
적합한지 여부를 결정한다.

제8조(정보보호관리체계인증기관지정서) 영 제48조제3항에 따른 "정보보호관리체계인증기관 지정서"는 별지 제4호서식과 같다.

제3절 인증기관 심사위원회 구성?운영

제9조 (심사위원회의 구성) ①방송통신위원회는 영 제48조제1항에 따라 정보보호관리체계인증기관의 지정신청을 받은 경우 영 제48조제4항에 따른 심사위원회를 구성하여 다음 각 호의 심사업무를 수행하게 하여야 한다. 이 경우 방송통신위원회는 필요하다고 인정하는 때에는 분과위원회 또는 작업반을 둘 수 있다.

1. 영 제48조제3항에 따른 현장실사
2. 별표 2에 따른 인증심사원의 자격요건 및 별표 3에 따른 업무수행능력심사 세부평가
3. 정보보호관리체계인증기관 지정의 적합성 결정
4. 그 밖에 지정심사와 관련되는 업무

②심사위원회는 5인이상 10인이내의 위원으로 구성하되, 위원은 정보보호전문가, 회계사, 기술사, 변호사 등 업무수행능력심사를 수행할 수 있는 학식과 경험이 있는 자 중 방송통신위원회가 위촉하며, 위원장은 위원 중에서 호선한다.

③제2항에 따른 심사위원은 최근 2년간 지정신청자와 관련된 업무를 수행하지 않아야 한다.

④위원에 대하여는 예산의 범위안에서 수당과 여비를 지급할 수 있다. 다만, 공무원인 위원이 소관업무와 관련하여 참석한 경우에는 그러하지 아니하다.

제10조(심사위원회의 운영) ①위원장은 심사위원회의 업무를 통할하며 위원회를 대표하여 방송통신위원회에 정보보호관리체계인증기관 지정 적합성 여부에 대한 심사결과를 제출한다.

②위원장이 부득이한 사유로 직무를 수행할 수 없을 때에는 위원장이 미리 지정한 위원이 그 직무를 대행한다.

제3장 정보보호관리체계의 인증기준 등

제1절 정보보호관리체계 인증신청

제11조(신청기관의 준비사항) 신청기관은 다음 각 호의 인증심사기준에 따라 정보보호관리체계를 수립하여 최소 3개월 이상 운영하여야 한다.

1. 별표 4에 따른 관리과정 요구사항
2. 별표 5에 따른 문서 작성 및 관리 통제사항
3. 별표 6에 따른 정보보호관리 통제사항에서 선택한 사항(신청기관은 자신의 정보보호관리체계의 규모 및 사업특성 등을 고려하여 별표 6에서 적절한 항목을 선택할 수 있다)

제12조(인증의 신청) ①영 제50조제1항에 따라 인증을 신청하는 자는 별지 제5호서식의 정보보호관리체계인증신청서를 정보보호관리체계인증기관에 제출하여야 한다. 이 경우 정보보호관리체계의 인증을 받고자 하는 범위를 정하여 신청할 수 있다.

②제1항에 따라 신청을 받은 정보보호관리체계인증기관은 정보보호관리체계 특성상 신청기관이 지정한 정보보호관리체계만을 분리하여 심사할 수 없는 경우에는 신청기관과 상의하여 인증의 범위를 변경할 수 있다.

제13조(인증심사계약의 체결) 정보보호관리체계인증기관은 영 제50조제2항에 따라 신청기관과 협의한 후 심사기간, 심사인원, 심사수수료, 인증의 범위 등을 포함하는 인증심사계약을 체결하여야 한다.

제2절 정보보호관리체계 인증심사 기준 및 방법

제14조(인증심사기준) 정보보호관리체계의 인증심사기준은 별표 4부터 별표 6까지와 같다.

제15조(인증심사요소) ①정보보호관리체계인증기관은 신청기관이 수립한 관리과정을 체계적으로 관리·유지하고 있는지 여부를 판단하기 위하여 다음 각 호의 사항을 심사하여야 한다.

1. 정보보호정책 수립 : 신청기관에 적합한 정보보호정책의 수립, 조직의 구성?운영, 책임성의 명확한 설정 여부
2. 정보보호관리체계 범위설정 : 정보보호관리체계 수립?운영을 위한 관리범위 설정 및 정보자산의 현황조사 여부
3. 위험관리 : 위험관리 전략 및 계획 수립, 위험분석·평가, 정보보호대책 선택의 적절성 여부
4. 구현 : 정보보호대책의 구현 및 정보보호 교육·훈련의 효과성 여부
5. 사후관리 : 정보보호관리체계의 재검토, 모니터링 및 개선, 내부감사 활동의 적절성 여부

②정보보호관리체계인증기관은 신청기관이 정보보호관리체계의 수립 및 이행 활동에 관련된 절차와 운영을 문서화해서 관리하는지에 대하여 심사하여야 한다.

③정보보호관리체계인증기관은 신청기관이 관리과정의 위험평가를 통하여 선택한 통제사항에 대한 정보보호대책을 구현하고 이행하고 있는지에 대하여 심사하여야 한다.

제16조(서면심사) 인증심사원은 신청기관이 영 제50조제1항에 따라 제출한 신청서류를 확인하여 신청기관이 수립한 정보보호관리체계가 별표 4부터 별표 6까지에 따른 인증심사기준에 적합한지에 대하여 심사하여야 한다.

제17조(기술심사) ①인증심사원은 서면심사의 결과를 검증하기 위하여 신청기관이 인증을 신청한 정보보호관리체계가 운영중인 현장을 방문하여 직접 해당 정보보호관리체계의 구축?운영 실태를 확인하여야 한다.

②인증심사원은 제1항에 따른 현장방문시 신청기관의 요청이 있는 경우 인터넷 침해사고 등에 대한 안전성 검사를 위하여 해당 정보보호관리체계에 속한 정보시스템에 대한 모의진단을 실시할 수 있다.

제3절 인증위원회의 구성 및 운영

제18조(인증위원회의 구성) ①정보보호관리체계인증기관의 장은 인증심사원이 실시한 인증심사 결과가 제14조에 따른 인증심사기준에 적합한지 여부를 심의하기 위하여 인증위원회를 구성?운영하여야 한다.
②인증위원회는 5인 이상 10인 이내의 위원으로 구성하되, 위원은 정보보호전문가, 정보시스템감리사, 기술사 등 정보보호분야에 학식과 경험이 있는 자 중 정보보호관리체계인증기관의 장이 위촉하며, 위원장은 위원 중에서 호선한다.

제19조(인증위원회의 운영) ①위원장은 인증위원회의 업무를 통할하며 위원회를 대표하여 정보보호관리체계인증기관의 장에게 인증심사원이 실시한 인증심사 결과가 제14조에 따른 인증심사기준에 적합한지 여부를 심의하고 그 결과를 제출한다.
②정보보호관리체계인증기관의 장은 제1항에 따른 심의를 실시한 때에는 인증심사원이 실시한 심사결과를 위원회 개최 전 5일까지 인증위원회에 제출한다.

제4절 인증서 교부 및 사후관리 등

제20조(인증서 교부) 정보보호관리체계인증기관의 장은 제19조제1항에 따라 인증위원회의 심의결과를 제출받은 경우 신청기관에게 인증심사결과를 통보하고, 신청기관의 정보보호관리체계가 이 고시에서 정한 인증심사기준에 적합하다고 판단된 경우 별지 제6호서식의 정보보호관리체계인증서를 교부하여야 한다.

제21조(정보보호관리체계의 변경) ①인증을 취득한 자는 인증을 받은 정보보호관리체계에 다음 각 호의 어느 하나에 해당하는 중대한 변화가 발생한 경우 발생한 날로부터 3개월 이내에 인증기관의 장에게 변경된 내용을 통보하여야 한다.
1. 신청기관이 수립하여 운영하는 관리체계의 범위가 확대되거나 변경되었을 경우
2. 사업장 변경 및 기업결합 등의 경영환경 변화 등으로 관리체계 운영에 영향을 미치는 경우
②인증기관의 장은 인증을 취득한 자로부터 변경내용을 통보받은 경우 인증을 취득한 자와 협의하여 인증심사 여부를 결정한다.
③제2항에 따라 인증심사를 실시하는 경우에는 제14조부터 제20조까지를 준용한다.

제22조(사후관리) ①영 제52조에 따라 정보보호관리체계인증기관은 인증을 취득한 자가 정보보호관리체계를 지속적으로 유지하고 있는지에 대하여 영 제51조에 따른 유효기간 중 제2절 정보보호관리체계 인증심사 기준 및 방법에 따라 1회 사후관리를 수행한다.
②정보보호관리체계인증기관은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 때에는 인증을 취소하여야 한다.

1. 거짓 그 밖의 부정한 방법으로 정보보호관리체계인증을 받은 때
2. 법 제47조제3항에 따라 인증받은 내용을 홍보하면서 인증의 범위나 유효기간을 속인 경우
3. 제1항에 따른 사후관리에서 정보보호관리체계 인증기준에 적합하지 않게 된 사실이 발견된 때

③정보보호관리체계인증기관이 제2항에 따라 인증을 취소하는 경우에는 인증을 취득한 자에게 통지하고, 제20조에 따라 교부한 정보보호관리체계인증서를 회수하여야 한다.

제23조(인증서 관리) ①정보보호관리체계인증기관은 발급된 인증서의 인증번호, 발급번호, 발급일, 유효기간 등을 관리하여야 한다.

②인증을 취득한 자는 인증서의 분실 등으로 인한 재발급을 받고자 할 경우 별지 제7호서식의 관리체계 인증서 재발급 신청서를 인증기관에 제출하여야 한다.

③인증을 취득한 자가 주소, 업체명 등 인증서 기재사항의 변경을 요청하고자 하는 경우 별지 제8호서식의 인증서 변경신청서를 정보보호관리체계인증기관에 제출하여야 한다.

제24조(재검토기한) 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 고시 발령 후 법령이나 현실여건의 변화 등을 검토하여 이 고시의 폐지, 개정 등 조치를 하여야 하는 기한은 2012년 10월 31일까지로 한다.

부칙 <제2009-27호,2009.11.5>

이 고시는 2009년 11월 5일부터 시행한다.

[별표 1]

업무수행능력심사 규정에 따른 제출서류(제4조제3항관련)

구 분	제 출 서 류
1. 정보보호수행실적을 확인하는 데 필요한 서류	가. 별지 제3호서식에 따른 정보보호수행실적 명세서 및 이를 증빙할 수 있는 자료(결과보고서 등) 나. 계약서 사본 및 세금계산서 등
2. 업무수행능력심사평가표 각호의 세부 평가요소를 평가하기 위하여 필요한 서류	가. 총매출액대비 정보보호분야 매출액의 비율 계산내역(공인회계사 또는 회계담당자가 서명 날인한 서류) 나. 부채비율 및 자기자본 이익률의 계산내역(회결산내역 등 관련 증빙자료) 다. 인증업무 운영체계 관련 규정 및 지침 등 ㅇ 인증기관의 운영체계 및 인증의 품질관리 ㅇ 인증업무를 수행하는 직원에 대한 운영관리 등의 내부규정 ㅇ 인증업무 수행 방법 및 절차
비 고 ※ 방송통신위원회는 정보보호관리체계인증기관 지정 공고시 업무수행능력심사에 필요한 자료의 구성 및 그 세부내용, 제출시기 및 방법 등에 관한 사항을 포함하여야 한다.	

[별표 2]

인증심사업무를 전담하는 직원의 요건(제5조 관련)

학력 및 경력기준	자격 및 경력기준
1. 유관학력 보유의 경우 가. 학사학위를 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 6년 이상인 자 나. 석사학위를 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 3년 이상인 자 2. 비 유관학력 보유의 경우 가. 학사학위를 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 8년 이상인 자 나. 전문학사를 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 10년 이상인 자	1. 유관자격 보유의 경우 가. 기사자격을 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 4년 이상인 자 나. 산업기사자격을 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 7년 이상인 자 2. 다음 각목의 1에 해당하는 정보보호자격을 취득한 자로서 2년 이상의 정보보호유관경력이 있는 자 가. 한국정보보호진흥원의 정보보호전문가(SIS) 나. 「정보시스템의 효율적 도입 및 운영 등에 관한 법률」 제14조에 따른 정보시스템감리원 다. 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 공인정보시스템감사사(CISA) 라. 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 공인정보시스템보호전문가(CISSP)

1. "유관자격"이라 함은 「국가기술자격법 시행규칙」 별표 7의 검정대상 기술자격 종목 중 전자계산기, 정보통신, 통신설비, 통신기기, 통신선로, 정보기기운용, 전파통신, 전파전자, 무선설비, 방송통신, 정보관리, 정보처리, 사무자동화 및 전자계산조직응용 종목의 기술자격을 말한다.
2. "유관학력"이라 함은 「고등교육법」에 따른 해당 학교에서 다음 각 목에 해당하는 학과에서 소정의 과정을 이수하고 졸업하거나 그 밖의 관계 법령에 따라 국내 또는 외국에서 이와 동등 이상으로 인정되는 학력을 말한다.
   가. 전자 관련 학과 : 정보전자, 전자, 전자계산, 전기전자제어, 전자정보, 전자제어, 전기전자, 전자전기정보, 전자컴퓨터전기제어, 컴퓨터과학, 전기전자정보, 전자컴퓨터, 메카트로닉스, 전자재료, 제어계측, 반도체
   나. 정보통신 관련 학과 : 전기통신설비, 국제정보통신, 방송설비, 방송통신, 이동통신, 전자통신, 컴퓨터네트워크, 통신, 컴퓨터정보기술, 전파통신, 전기전자통신, 전기전자정

보통신, 전자정보통신, 전자제어통신, 전자통신, 전파, 전파통신, 정보통신, 컴퓨터통신, 항공통신정보, 전자정보통신반도체, 전기전자전파, 통신컴퓨터, 무선통신

다. 정보처리기술 관련 학과 : 시스템, 전산, 정보전산, 컴퓨터제어, 컴퓨터응용제어, 컴퓨터응용, 컴퓨터응용설계, 구조시스템, 컴퓨터정보, 멀티미디어, 정보시스템, 전산통계, 정보처리

라. 그 밖에 교육인적자원부장관이나 해당 교육기관의 장으로부터 전자·통신 및 정보처리기술·정보보호 관련 학과로 인정받은 학과

3. "정보통신유관경력"이라 함은 공공기관, 민간기업, 교육기관 등에서 정보통신서비스(기간통신, 별정통신, 부가통신, 방송서비스 등을 말한다), 정보통신기기(정보기기, 방송기기, 부품 등을 말한다) 또는 소프트웨어 및 컴퓨터 관련 서비스(패키지 소프트웨어, 컴퓨터 관련 서비스, 디지털콘텐츠, 데이터베이스 제작 및 검색 등을 말한다)에 해당되는 분야에서 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 수행한 기간을 말한다.

5. "정보보호유관경력"이라 함은 공공기관, 민간기업, 교육기관 등에서 정보보호를 위한 공통기반기술(암호 기술, 인증 기술 등을 말한다), 시스템·네트워크 보호(시스템 보호, 해킹·바이러스 대응, 네트워크 보호 등을 말한다) 또는 응용서비스 보호(전자거래 보호, 응용서비스 보호, 정보보호 표준화 등을 말한다)에 해당되는 분야에서 계획·분석·설계·개발·운영·유지보수·컨설팅 또는 연구개발 업무 등을 수행한 기간을 말한다.

[별표 3]

업무수행능력심사 세부평가기준(제6조관련)

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td rowspan="3">1.정보보호 업무수행 경험및 전문화 정도 (40)</td><td>최근 3년간 정보보호수행 실적</td><td>25</td><td>계약금액 총액</td><td>o 지정 공고일 기준으로 최근 3년간 완료한 정보보호수행실적을 인정하고 평가점수는 개별 수행실적의 계약금액을 합한 총액에 따라 산출
<table><tr><th>계약금액총액(단위 : 억원)</th><th>점수</th></tr><tr><td>30억원이상</td><td>배점의 100%</td></tr><tr><td>30억원미만</td><td>배점의 x%</td></tr><tr><td colspan="2">※x = (계약금액 총액/30억원) × 100</td></tr></table></td></tr>
<tr><td>최근 3년간 계약금액 5천만원 이상의 정보보호수행 실적</td><td>10</td><td>수행건수</td><td>o 지정 공고일 기준으로 최근 3년간 완료한 정보보호수행실적으로 계약금액이 5천만원 이상의 실적을 인정
<table><tr><th>수행실적 건수</th><th>점수</th></tr><tr><td>30건이상</td><td>배점의 100%</td></tr><tr><td>30건미만</td><td>배점의 x%</td></tr><tr><td colspan="2">※x = (수행건수/30건) × 100</td></tr></table></td></tr>
<tr><td>총매출액에 대한 정보보호분야 매출액 비율</td><td>5</td><td>비율</td><td>o 지정 공고일 기준으로 직전년도 정보보호분야 매출액의 비율(정보보호분야 매출액/총매출액)
<table><tr><th>비율</th><th>점수</th></tr><tr><td>80%이상</td><td>5점</td></tr><tr><td>80%미만 ~ 60%이상</td><td>4점</td></tr><tr><td>60%미만 ~ 40%이상</td><td>3점</td></tr><tr><td>40%미만 ~ 20%이상</td><td>2점</td></tr><tr><td>20%미만</td><td>1점</td></tr></table></td></tr>
<tr><td>2.신뢰도 및재정상태 건실도 (10)</td><td>부채비율</td><td>5</td><td>비율</td><td>o 지정 공고일 기준으로 직전년도 부채비율 (부채총계/자기자본)
<table><tr><th>비율</th><th>점수</th></tr><tr><td>50%미만</td><td>5점</td></tr><tr><td>50%이상 ~ 100%미만</td><td>4점</td></tr><tr><td>100%이상 ~ 150%미만</td><td>3점</td></tr><tr><td>150%이상 ~ 200%미만</td><td>2점</td></tr><tr><td>200%이상</td><td>1점</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td>자기자본이익률</td><td>5</td><td>비율</td><td>o 지정 공고일 기준으로 직전년도 자기자본이익률(당기순이익/자기자본)
<table><tr><th>비율</th><th>점수</th></tr><tr><td>20%이상</td><td>5점</td></tr><tr><td>20%미만 ~ 15%이상</td><td>4점</td></tr><tr><td>15%미만 ~ 10%이상</td><td>3점</td></tr><tr><td>10%미만 ~ 5%이상</td><td>2점</td></tr><tr><td>5%미만</td><td>1점</td></tr></table></td></tr>
<tr><td rowspan="3">3. 인증업무 운영 체계 (50)</td><td>인증기관의 운영 체계 및 인증의 품질관리</td><td>25</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 인증기관의 공정성·객관성·신뢰성·독립성 보장 방안</td><td>5점</td></tr><tr><td>o 인증기관의 내부감사 실시 및 검토 등에 대한 방안</td><td>5점</td></tr><tr><td>o 인증위원회 구성·운영 방안</td><td>5점</td></tr><tr><td>o 인증의 품질 보장 및 관리방안</td><td>5점</td></tr><tr><td>o 인증업무의 기록 및 문서화 관리체계의 적절성</td><td>5점</td></tr></table></td></tr>
<tr><td>인증업무를 수행하는 직원에 대한 운영관리 등의 내부 규정</td><td>10</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 인증업무를 수행하는 직원에 대한 규정 보유 및 그 규정의 타당성 및 실효성
- 인증업무를 수행하는 직원의 의무와 책임 등 준수사항
- 인증업무를 수행하는 직원의 자체 보안 관리 및 감독 요령</td><td>5점</td></tr><tr><td>o 인증업무를 수행하는 직원의 교육 및 평가 등에 대한 방안 및 그 방안의 적절성 및 타당성</td><td>5점</td></tr></table></td></tr>
<tr><td>인증업무 수행 방법 및 절차</td><td>15</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 인증업무 수행 방법 및 절차 등의 적절성 및 타당성
- 인증심사의 절차 및 방법
- 인증수수료 및 그 징수방법
- 인증심사팀 구성 원칙
- 인증서 발급 기준
- 인증심사 사후관리방안 등</td><td>15점</td></tr></table></td></tr>
<tr><td>4. 가점 및 감점</td><td>인증심사업무를 전담하는 직원의 보유 수</td><td>5 (가점)</td><td>보유 인원수</td><td>o 인증심사업무를 수행하는 전담조직을 갖추고, 그 전담조직에 속한 직원에 대해 인정
<table><tr><th>구분</th><th>점수</th></tr><tr><td>20명 이상</td><td>5점</td></tr><tr><td>20명미만 ~ 10명이상</td><td>배점의 x%</td></tr><tr><td>10명 미만</td><td>없음</td></tr><tr><td colspan="2">※x = (인원수/20명) × 100</td></tr></table></td></tr>
<tr><td></td><td>자격취소 사실</td><td>5 (감점)</td><td>취소사실 및 취소회수</td><td>o 지정 공고일 기준으로 10년이내에 방송통신위원회가 부여한 정보보호 관련 수행자격이 취소된 경우
- 정보보호관리체계인증기관, 정보보호 컨설팅전문업체, 안전진단수행기관 등
※ 취소 1회당 : 감점 5점</td></tr>
</table>

<비 고>

1. 각 평가요소별 세부평가에 필요한 자료의 구성 및 그 세부내용 등에 관한 사항은 지정공고 시 제시한다.
2. 평가항목에 대한 각 평가요소별 세부평가 점수는 소수점 이하 둘째 자리에서 반올림한다.
3. 평가항목에 대한 각 평가요소별 평가점수는 평가결과의 최저점과 최고점을 제외한 점수들의 평균점을 부여한다. 다만, 최저점 또는 최고점이 2개 이상일 경우 각 1개만 제외한다.
4. 가점을 합한 점수가 100점을 초과해도 만점 100점으로 표기한다.
5. 정보보호수행실적으로 인정을 받기 위해서는 다음 각목의 요건을 충족하여야 한다.
   가. 전자적 침해행위에 대비하기 위한 정보관리 및 정보시스템의 안전성에 대한 점검과 이에 기초한 정보보호대책의 제시를 주된 목적으로 직접 수행한 실적을 말하는 것으로 정보보호에 관한 감사, 감리, 진단, 인증, 컨설팅 등을 포함한다.
   나. 지정 공고일 현재 프로젝트가 종료되고 이에 대한 대금지급이 완료되어야 한다.
   다. 하수급업체가 수급업체로부터 하도급을 받아 수행한 실적에 대해서는 인정하지 아니하고 해당 기관에서 직접 계약하여 수행한 실적에 대해서만 인정한다.
   마. 가목 내지 다목의 내용이 계약서 및 증빙자료를 통하여 분명하게 확인되어야 한다.
6. '정보보호분야의 매출액'이라함은 지정 공고일 기준으로 직전년도 결산회기의 정보보호분야 제품 및 서비스관련 매출총액을 말한다.
7. '인증업무 운영체계'에 대한 각 평가요소별 세부평가 점수 부여기준은 각 평가요소의 평가결과에 평가등급(계수)를 곱하여 나온 점수를 합산한다.

평가요소별 세부평가 점수	평가등급(계수)
100점이하 ~ 90점이상	우수(1.0)
90점미만 ~ 80점이상	보통(0.6)
80점미만 ~	미흡(0.2)
미 제출	점수없음(0)

[별표 4] 인증심사기준 - 관리과정 요구사항(제11조 제1호관련)

	관리과정		세부관리과정	관리과정 상세내용
1	정보보호정책 수립	1.1	정보보호정책의 수립	신청기관의 경영목표를 지원할 수 있도록 정보보호의 법적, 규제적 요건과 전략적이고 조직적인 위험관리를 기술한 정보보호정책을 수립하여야 한다.
		1.2	조직 및 책임의 설정	정보보호활동에 대한 경영층의 명확한 지원 및 방향제시를 보증할 수 있는 조직을 수립하여야 한다. 또한 정보보호관리 활동을 수행하고 검증하는 인력들에 대한 책임, 권한 및 상호 연관관계를 정의하고 문서화하여야 한다.
2	정보보호 관리체계 범위설정	2.1	정보보호관리체계 범위설정	신청기관의 특성, 위치, 기술, 자산 등 내·외적 환경에 중대한 영향을 미치는 요소를 고려하여 정보보호관리체계의 범위를 설정하여야 한다.
		2.2	정보자산의 식별	신청기관의 정보자산으로 보호를 받을 가치가 있는 정보자산을 식별하고, 이를 정보자산의 형태, 소유자, 관리자, 특성 등을 포함하여 목록을 만들어야 한다.
3	위험관리	3.1	위험관리전략 및 계획 수립	신청기관의 목표 및 정책, 법적 요구사항 등을 고려하여 조직, 역할, 책임, 주요과정을 포함한 위험관리 전략 및 계획을 수립하고, 신청기관에 적합한 위험관리 방법을 선택하고 문서화하여야 한다. 이 위험분석 방법은 조직과 정보보호 환경변화에 대응할 수 있도록 지속적으로 검토하여야 한다.

	관리과정		세부관리과정	관리과정 상세내용
3	위험관리	3.2	위험분석	신청기관은 「2.2 정보자산의 식별」에서 식별된 정보자산에 영향을 줄 수 있는 모든 위협과 취약성, 위험을 식별하고 분류하여야 하며, 이 정보자산의 가치와 위험을 고려하여, 잠재적 손실에 대한 영향을 식별·분석하여야 한다.
		3.3	위험평가	정보자산에 대한 잠재적 및 알려진 위협과 취약성으로 나타날 수 있는 신청기관의 피해와 현재 구현된 정보보호대책의 실패 가능성 및 영향을 평가하고 수용 가능한 위험수준을 포함하여야 한다. 이를 통해 정보자산의 위험을 관리할 수 있는 적절한 정보보호대책 선택 및 우선순위의 확보를 지원하여야 한다.
		3.4	정보보호대책 선택	신청기관의 정보보호정책과 목적에 부합하도록 위험을 수용 가능한 수준으로 감소시키기 위해, 위험분석 및 평가에 의거하여, 위험처리, 위험수용, 위험회피, 위험전가 등의 전략을 설정하고, [별표3]에서 제시하는 통제사항중에서 선택한다. [별표3]에서 제시되어 있지 않은 통제사항을 추가할 경우에는 [별표1]관리과정의 각 단계간 일관성을 유지하도록 한다. 정보보호대책의 선택은 비용·효과 분석에 의해 정당화 될 필요가 있다.
		3.5	정보보호계획 수립	정보보호대책의 선택이후 구현할 정보보호대책 및 구현의 우선순위, 일정계획, 예산, 책임, 운영계획 등을 포함한 정보보호계획을 수립하고, 각 위험에 대한 정보보호대책 및 선택하게 된 근거를 정보보호대책 명세서로 문서화하여야 한다.

	관리과정		세부관리과정	관리과정 상세내용
4	구 현	4.1	정보보호대책의 효과적 구현	정보보호대책은 적절한 관리 조치와 우선 순위에 의해 구현하여야 한다.
		4.2	정보보호 교육 및 훈련	신청기관의 정보보호 관련직원들 및 최종사용자에게 정보보호에 대한 인식을 제고시키고, 정보보호대책의 필요성을 이해하도록 하며 구현될 정보보호대책들을 정확하게 사용할 수 있도록 교육 및 훈련 프로그램을 수립하고 이행하여야 한다.
5	사후관리	5.1	정보보호관리체계의 재검토	신청기관의 목표, 기술 등 내·외부의 변화와 내부감사 결과, 보안사고 등을 고려하여, 정보보호관리체계의 효율성, 범위의 적절성, 잔류위험의 수준, 절차 등의 문서를 공식적이고 정기적으로 재검토하여야 한다.
		5.2	정보보호관리체계의 모니터링 및 개선	정보보호관리체계가 신청기관의 정보보호정책과 목적을 충족시키는지 여부에 대하여 모니터링하여, 개선사항을 식별하고, 적절한 수정이나 예방조치를 통하여 효과적으로 개선사항을 구현하여야 한다. 이에 관련된 조치와 결과는 신청기관의 임직원에게 전달하여야 하고, 관련자들에게 자문을 구하여야 한다.
		5.3	내부감사	신청기관은 정보보호관리체계가 계획된 절차에 따라 효과적으로 실행되는지를 점검하기 위하여 감사의 기준, 범위, 주기 및 방법을 규정하고, 계획된 주기로 내부감사를 수행하여야 한다. 또한 감사의 기획 및 수행, 그리고 결과보고, 기록 유지 및 이행 모니터링에 대한 책임과 요구사항을 문서화된 절차에 의해 규정하여야 한다. 피감사분야의 관리자는 발견된 보완조치 사항을 처리하고, 검증·보고됨을 보장하여야 한다.

[별표 5] 인증심사기준 - 문서 작성 및 관리 통제사항(제11조 제2호관련)

	문서화	문서화 상세내용
1	문서요건	정보보호관리체계 수립 및 이행에 관련된 모든 문서는 해당 신청기관의 규모, 기능 등을 고려하여 문서화하여야 하며, 신청기관의 정보보호정책에 따라 필요한 모든 임직원 및 관련자들이 쉽게 이용할 수 있어야 한다.
2	문서의 통제	「1. 문서요건」에 의해 작성된 문서는 문서의 발행전 타당성 승인, 주기적 또는 필요시 문서의 검토·갱신 및 재승인, 문서의 변경과 현재 개정상태의 식별, 문서배포, 폐기된 문서의 사용금지 등의 통제를 정의한 절차를 수립하여야 한다.
3	운영기록의 통제	정보보호관리체계를 효과적, 효율적으로 운영하기 위해서 기록을 확인, 유지보수, 보존, 폐기하는 문서화된 절차를 수립하고 유지·관리하여야 한다. 이 문서화된 절차에는 접근자의 신원확인, 기록의 저장, 보호, 검색, 유지기간, 처분 등의 통제에 필요한 절차를 포함하여야 한다. 또한 기록은 읽기 쉽고, 식별 가능하며, 관련 활동을 추적할 수 있어야 한다.

[별표 6] 인증심사기준 - 정보보호관리 통제사항(제11조 제3호관련)

	통제분야		통제목적		통제사항	통제내용
1	정보보호 정책	1.1	정책의 승인 및 공표	1.1.1	정책의 승인	문서화된 정보보호정책은 최고경영자의 승인을 받아야 한다.
				1.1.2	정책의 공표	정보보호정책 문서는 모든 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.
		1.2	정책의 체계	1.2.1	상위 정책과의 일관성	정보보호정책은 신청기관의 사업목표 및 정보기술정책과 일관성을 유지하여야 한다.
				1.2.2	정책 문서의 유형	정보보호정책을 구체적으로 시행하기 위한 정보보호 지침, 절차 및 표준을 수립하여야 한다. 또한 필요한 경우 특정 시스템 또는 서비스에 대한 상세한 정보보호정책을 수립할 수 있다.
		1.3	정책의 유지관리	1.3.1	주기적 검토	정기적으로 정보보호정책의 타당성을 검토하여야 하며, 중대한 보안사고 발생, 새로운 위협 또는 취약성의 발생, 정보보호 환경에 중대한 변화 등이 발생했을 경우에는 관련된 사항의 타당성을 추가로 검토하여야 한다.
2	정보보호 조직	2.1	조직의 체계	2.1.1	조직의 구성	신청기관내 정보보호관리 활동을 계획, 관리하는 정보보호관리자가 있어야 하며, 필요에 따라 정보보호위원회를 구성할 수 있다.

	통제분야		통제목적		통제사항	통제내용
2	정보보호 조직	2.1	조직의 체계	2.1.2	외부전문가 활용	정보보호정책 수립, 위험분석·평가, 통제사항의 선택과 구현, 보안사고 대응 등 중요한 정보보호관리 활동에 도움을 받기 위하여 외부 전문가의 조언을 받을 수 있다. 외부 전문가의 신청기관 자원에 대한 접근은 「3. 외부자 보안」의 대상이 된다.
		2.2	책임과 역할	2.2.1	정보보호 관리자	최고경영자의 지정을 받은 정보보호관리자는 정보보호정책 수립, 정보보호 위원회의 구성 및 운영, 위험분석 및 관리, 보안사고 대응 및 복구 등의 정보보호에 관한 업무를 총괄 관리하여야 한다.
				2.2.2	정보보호 위원회	신청기관 전반에 걸친 중요한 정보보호 관련 심의 및 승인 기능을 수행하며 필요한 자원할당을 통해 정보보호관리 활동이 적절히 수행될 수 있도록 하여야 한다.
3	외부자 보안	3.1	계약 및 서비스 수준협약 보안관리	3.1.1	위부위탁 계약시 보안 요구사항	신청기관의 업무를 외부위탁 하는 경우에는 정보시스템, 네트워크, 인력 및 사무환경 등을 관리·통제하기 위한 보안요구사항을 계약서 상에 명시하여야 하고 요구사항을 서비스수준협약(SLA : Service Level Agreement)에 반영하여야 한다.
				3.1.2	제3자와의 계약시 보안 요구사항	신청기관이 제3자에게 정보자산에 대한 접근을 허용하는 계약을 체결하는 경우에는 신청기관의 정보보호정책 준수 및 필수 보안요건을 포함하는 공식적인 계약을 하여야 한다.

	통제분야		통제목적		통제사항	통제내용
3	외부자 보안	3.2	외부자 보안 실행관리	3.2.1	외부위탁 보안관리	외부위탁 업체가 계약서 및 서비스 수준 협약 명시된 보안요구사항을 충분히 이행하는지 주기적으로 점검하고, 필요시 감사를 수행하여야 한다.
				3.2.2	제3자 보안관리	신청기관의 정보자산에 대한 제3자의 접근을 통제하여야 한다. 업무상 불가피하게 접근을 허용해야 할 경우에는 접근유형 및 접근사유를 파악하고 위험 요소를 고려하여 관리하여야 한다.
4	정보자산 분류	4.1	정보자산의 조사 및 책임할당	4.1.1	정보자산 조사	신청기관의 정보자산을 조사하고 정보자산별로 신청기관에서의 가치, 업무 영향, 법적 준수사항 등을 고려하여 중요도를 결정하여야 한다.
				4.1.2	정보자산별 책임할당	조사된 정보자산에 대하여 소유자, 관리자, 사용자를 확인하고, 적절한 통제 유지를 위해 책임소재를 명확히 하여야 한다.
		4.2	정보자산의 분류 및 취급	4.2.1	정보자산의 분류	정보자산이 신청기관에서 차지하는 가치와 신청기관에 미치는 영향을 고려하여 분류방식을 선택하고 분류하여야 한다.
				4.2.2	보안등급과 취급	중요도에 따라 분류된 정보자산에 보안등급을 부여하고, 물리적, 전자적 보안등급 표시를 부착, 관리하여야 한다. 또한 보안등급의 부여에 따른 취급 절차도 정의하여 이행하여야 한다.

	통제분야		통제목적		통제사항	통제내용
5	정보보호 교육 및 훈련	5.1	교육 및 훈련 프로그램 수립	5.1.1	교육 및 훈련계획	정보보호 인식제고 및 실제 운영에 필요한 교육·훈련 계획을 종합적으로 수립하여 이행하여야 한다
				5.1.2	교육 및 훈련대상	교육 및 훈련의 대상에는 신청기관의 임직원 및 관련 외부자를 포함하여야 한다.
				5.1.3	교육 및 훈련내용	교육 및 훈련은 정보보호정책, 정보보호인식, 보안요구사항, 법적인 책임, 보안사고 대응절차, 업무연속성 관리 등을 포함하여야 하고, 교육대상자의 직위 및 담당하는 업무의 특성에 따라 구분하여 실시하여야 한다.
		5.2	시행 및 평가			교육 및 훈련은 정기적으로 실시하여야 하며, 정보보호정책이나 절차 및 역할의 변경이 있는 경우에는 수시로 실시하고 이에 대한 기록을 남겨야 한다. 또한 교육훈련 종료 후 검토를 통하여 차기 교육에 반영하여야 한다.
6	인적 보안	6.1	책임할당 및 규정화	6.1.1	책임할당	정보보호업무를 이행하는 역할과 책임을 문서화하여야 한다. 문서화의 내용에는 정보보호정책을 수립, 구현, 운영하는 일반적인 책임과 특정 정보자산의 보호와 활동에 대한 구체적인 책임을 포함하여야 한다.
				6.1.2	인사규정	인사규정에는 정보보호에 대하여 직원이 지켜야 할 책임 및 관련 법규상의 책임을 명시하여야 한다. 특히, 정보보호업무를 담당하는 자와 정보시스템 사용자 및 관리자는 보다 명확한 책임을 명시하여야 하며, 직원이 책임을 이행하지 않는 경우를 대비한 적절한 처벌규정을 포함하여야 한다.

	통제분야		통제목적		통제사항	통제내용
6	인적 보안	6.2	적격심사 및 주요 직무담당자 관리	6.2.1	적격심사	계약직 및 임시직원은 물론 정식직원 채용시 신원, 업무능력, 교육정도, 경력 등에 대한 적격심사가 이루어져야 한다. 직원들이 용역회사를 통하여 충원되는 경우에는 용역회사와의 계약서에 적격심사에 따르는 책임사항을 명문화하여야 한다.
				6.2.2	주요직무 담당자 관리	정보시스템 접근 권한을 포함하는 업무가 새로이 할당될 때, 특히 재무정보나 비밀정보와 같이 중요한 정보를 처리하는 담당자는 별도의 관리를 수행하여야 한다.
		6.3	비밀유지	6.3.1	비밀유지 서약서	직원으로부터 비밀유지 서약서에 서명을 받아야 하며, 임시직원이나 제3자에게 정보에 대한 접근 권한을 부여할 경우에도 그들로부터 비밀유지 서약서에 서명을 받아야 한다. 직원의 고용계약에 변경이 있을 경우, 특히 직원이 퇴사하거나 계약기간이 만료될 때에는 비밀유지 서약서를 환기시켜야 한다.
7	물리적 보안	7.1	물리적 보안대책	7.1.1	물리적 보호구역	특별한 보호가 필요한 시설 및 장비를 권한 없는 자의 물리적 접근 및 각종 물리적, 환경적 재난으로부터 보호하기 위하여 보호구역을 정의하고 이에 따른 보안대책을 수립·이행하여야 한다. 이 경우 제한구역, 접견구역, 장비출하구역 등을 별도로 지정하여 각각에 적합한 보안 조치와 절차를 수립하여야 한다.
				7.1.2	물리적 접근통제	보호구역을 출입하는 자를 감시·통제하고 권한 없는 자의 출입을 방지하기 위하여 수립된 보안 절차에 따라 필요한 조치를 수행하고 주기적으로 검토하여야 한다.

	통제분야		통제목적		통제사항	통제내용
7	물리적 보안	7.2	데이터 센터 보안	7.2.1	위치 및 구조 조건	데이터센터는 물리적, 환경적 위험이 적은 곳에 위치하고 구조의 안정성을 확보하여야 한다.
				7.2.2	출입통제	데이터센터의 출입은 적절한 출입통제절차에 의하여 이행되어져야 하며, 출입자를 식별하고 기록·관리하여야 한다. 또한 출입자 기록 대장은 정기적으로 점검하여야 한다.
				7.2.3	내부설비	화재·수재 등의 각종 재해에 대비한 시설을 충분히 설치하여야 하고, 비상연락장치 및 비상구, 물리적 접근통제 및 시건장치를 설치하여야 한다.
		7.3	장비보호	7.3.1	주요 시스템 보호	신청기관내의 주요 시스템에 대한 별도의 출입통제를 실시하거나 이중의 보호장치를 설치하고, 시스템 관리자는 주요 시스템 접근에 대한 보안대책을 수립하여야 한다.
				7.3.2	장비의 배치	장비는 환경적인 위협과 위험, 불법접근에 대한 위험을 감소시키기 위해 적절한 위치에 배치하고 이를 보호하여야 한다.
				7.3.3	전원공급	전원공급 이상이나 기타 전기관련 사고 발생시 전원을 지속적으로 공급하기 위하여 장비 제조업체의 사양에 따라 적절히 관리하여야 한다.
				7.3.4	케이블 보호	데이터를 송·수신하거나 정보서비스를 지원하는 전력 및 통신 케이블은 방해되거나 손상을 입지 않도록 보호하여야 한다.
				7.3.5	장비의 보수	장비는 지속적인 가용성과 무결성을 위하여 장비 제공자가 지시한 명세에 따라 유지보수를 하여야 하고 유지·보수에 대한 기록을 남겨야 한다.

	통제분야		통제목적		통제사항	통제내용
7	물리적 보안	7.3	장비보호	7.3.6	장비의 안전한 폐기 및 재사용	중요한 정보를 담고 있는 저장 매체의 폐기시에는 이를 물리적으로 파기하여야 하며, 중요 데이터나 정품 소프트웨어는 폐기하기 전에 매체에 기록된 내용이 완전히 삭제되어 복구가 불가능한지 확인하고 점검하여야 한다.
		7.4	사무실 보호			책상 위에 중요한 문서나 저장 매체를 남겨놓지 않도록 하고, 통상 근무시간 동안이나 그 외의 시간에 비인가된 자에 의한 정보 접근, 손상을 방지하기 위하여 컴퓨터 화면에 정보처리에 관한 사항을 남겨놓지 않도록 하여야 한다.
8	시스템 개발보안	8.1	분석 및 설계 보안관리	8.1.1	보안 요구사항 정의	새로운 시스템 개발, 기존시스템 개선시 보안요구사항을 문서로 명확히 하여야 하며, 보안요구사항에는 사용자 접근권한의 부여원칙과 접근통제 유형 등을 포함하여야 한다.
				8.1.2	입력 데이터 검증	응용시스템 설계시 입력 요구사항을 정의하고 문서화하여야 하며, 입력 데이터의 정확성, 무결성, 신뢰성을 판단하기 위한 표준을 마련하여야 한다.
				8.1.3	내부 처리의 검증	응용시스템 설계시 내부처리 요구사항을 정의하고 문서화하여야 하며, 응용소프트웨어의 처리 작업을 검증하고, 무결성을 회복할 수 있는 기능을 포함하여야 한다.
				8.1.4	출력 데이터 검증	응용시스템 설계시 출력 요구사항을 정의하고 문서화하여야 하며, 출력 데이터의 정확성, 무결성, 신뢰성을 판단하기 위한 대책을 마련하여야 한다.

	통제분야		통제목적		통제사항	통제내용
8	시스템 개발 보안	8.1	분석 및 설계 보안관리	8.1.5	인증 및 암호	응용시스템 설계시 반드시 사용자 인증에 대한 보안 요구사항을 고려하여야 한다. 중요한 메시지의 경우 무결성이 요구될 때 메시지 인증기법을 적용하고 비밀성이 요구될 시 암호화를 적용하여야 한다.
				8.1.6	보안기록 관리	응용시스템 설계시 사용자의 인증, 데이터 분실, 수정, 오남용 등을 점검하고 방지하기 위하여 보안에 관련된 로그, 감사증적 등을 확보할 수 있는 기능을 반영하여야 한다.
		8.2	구현 및 이행 보안관리	8.2.1	구현 및 시험	응용시스템 구현시 코딩표준에 따라 응용시스템을 구현하고, 보안요구사항에 대한 시험을 수행하여야 한다.
				8.2.2	운영환경 이행보안	운영 프로그램의 수정은 적절한 권한을 지닌 사람만이 시행하여야 하고, 운영시스템은 실행코드만 보유하여야 한다. 실행코드는 성공적인 시험과 사용자 인수 후에 실행하여야 한다.
				8.2.3	시험 데이터의 보안	시험 데이터는 운영데이터에 준하여 보호하고 통제하여야 하며, 운영환경에 대하여 적용되는 접근통제 절차를 시험환경에도 적용하여야 한다. 운영데이터가 시험환경으로 복사될 경우 허가절차를 수립하여 이행하고 시험 완료 후 운영데이터는 시험시스템에서 삭제하여야 한다. 운영데이터 사용 및 복사는 기록을 남겨야 한다.
				8.2.4	소스 프로그램의 접근보안	소스 프로그램은 실제 운영 환경에 보관하지 않는 것을 원칙으로 하며, 소스 프로그램 관리자는 각 운영시스템 별로 지정하여야 한다. 또한 소스 프로그램 접근에 대한 통제절차를 수립하고 이행하여야 한다.

	통제분야		통제목적		통제사항	통제내용
8	시스템 개발 보안	8.3	변경관리	8.3.1	변경관리 절차	정보시스템의 파괴와 손상을 최소화하기 위하여 공식적인 변경관리 절차를 수립하고 이행하여야 한다.
				8.3.2	운영체제 변경시의 검토	운영체제 변경이 필요한 경우 응용시스템의 운영이나 보안에 미치는 영향을 분석, 검토하여야 한다.
				8.3.3	소프트웨어 패키지 변경	소프트웨어 패키지는 가능한 수정하지 않고 사용하고, 패키지 변경시에는 공급자의 동의를 얻으며, 수정이 가능한지 확인하여야 한다. 모든 변경사항은 시험하고 문서화하여야 한다.
9	암호 통제	9.1	암호 정책			암호사용에 대한 정책을 수립하여야 한다.
		9.2	암호사용			암호 정책에 따른 암호 사용시 적절한 암호 알고리즘의 유형, 신뢰성 및 키 길이를 결정하여야 한다.
		9.3	키관리			암호 키에 대한 관리지침, 절차 및 방법을 마련하고 필요시 복구방안을 마련하여야 한다.
10	접근 통제	10.1	접근통제 정책	10.1.1	정책의 문서화	업무 요구사항에 따라 접근 통제의 방법과 범위 등을 정의하고 문서화하여야 한다.
				10.1.2	정책의 내용	접근통제 정책은 데이터, 프로그램, 주요 시스템, 네트워크 등에 대한 접근제한을 포함하여야 하며, 여기에는 보안요구사항, 데이터 및 서비스 접근시의 법적, 계약적 제한, 분산 네트워크상의 접근권한 관리 등을 포함하여야 한다.
				10.1.3	접근 통제 규칙	항상 존재하는 규칙과 일정기간이나 선택적으로 존재하는 규칙에 대한 구분, 실행 전에 관리자의 승인을 필요로 하는 규칙과 그렇지 않은 규칙의 구분 등을 포함한 접근 통제 규칙을 명시하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.1	접근통제 정책	10.1.4	접근통제 방법	접근통제 방법은 정책 및 절차에 의해 결정된 접근권한을 적절하게 반영하여야 한다.
				10.1.5	접근통제 정책 검토	접근에 대한 모니터링을 통해 정책과의 일치성을 주기적으로 검토하고, 접근통제 정책의 적정성을 확인하여야 한다.
		10.2	사용자 접근 관리	10.2.1	사용자 등록	정보시스템 및 서비스에 대한 접근을 통제하기 위한 공식적인 사용자 등록 및 해지 절차를 마련하여야 한다.
				10.2.2	특수권한 관리	시스템이나 응용프로그램에 대한 통제를 우회할 수 있는 특수권한의 할당 및 사용을 관리하여야 한다.
				10.2.3	사용자 패스워드 관리	사용자 패스워드의 관리절차를 수립하고 이행하여야 한다.
				10.2.4	사용자의 접근권한 검토	데이터나 정보 서비스에 대한 접근을 관리하기 위해서 정기적으로 접근 권한에 대하여서 점검을 하여야 한다.
				10.2.5	사용자의 책임	시스템 및 패스워드 관리 책임은 사용자 자신에게 있음을 주지시키고 관리지침을 제공하여야 한다.
		10.3	접근통제 영역	10.3.1	네트워크 접근	비인가된 접근을 막기 위해 네트워크의 내·외부 연결통제, 사용자 터미널과 컴퓨터 서비스간에 물리적 및 논리적 경로의 통제, 사용자 인증, 고장 진단 포트에 대한 접근통제 등을 포함한 네트워크 접근정책을 수립하고 이행하여야 한다.
				10.3.2	운영체제 접근	안전한 로그온 절차, 식별 및 인증 관리, 필요시 터미널 자동확인 등을 포함하여 시스템의 운영체제 접근을 통제하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.3	접근통제 영역	10.3.3	응용 프로그램 접근	사용자 접근이 허가되지 않은 응용 프로그램의 기능들에 대한 정보 제공을 제한하여야 한다. 또한 민감한 정보를 처리하는 응용 프로그램의 출력물은 허가된 위치에서만 전달하여야 한다. 민감한 응용 시스템은 반드시 일반적인 환경과 분리하여야 한다.
				10.3.4	데이터베이스 접근	데이터베이스의 뷰, 레코드 또는 필드 레벨에서의 데이터에 대한 접근통제, 데이터사전 및 데이터베이스 유틸리티에 대한 접근통제, 민감 정보의 암호화 등을 통해 데이터베이스내의 정보를 보호하여야 한다.
11	운영관리	11.1	운영 절차와 책임	11.1.1	운영절차의 문서화	보안정책에 의해 정의된 운영지침과 절차는 문서화하여 관리하여야 한다. 운영관리를 외부에 용역을 주는 경우에도 계약서에 이를 반영하여야 한다.
				11.1.2	정보자산의 변경관리	정보시스템 관련 자산들을 조사하고, 모든 변경사항들을 반영할 수 있는 공식적인 관리책임 및 절차를 수립하여야 한다.
				11.1.3	직무 분리	부주의에 의한 또는 고의적인 시스템 오용의 위험을 감소시키기 위해 직무를 분리하고, 직무 분리가 어려운 특수한 경우 별도의 관리감독 대책을 수립하여야 한다.
				11.1.4	개발과 운영환경의 분리	원칙적으로 개발, 시험, 운영 환경을 분리하여야 한다. 또한 응용프로그램을 개발환경으로부터 운영환경으로 이전하는 절차를 정의하고 문서화하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영 관리	11.1	운영 절차와 책임	11.1.5	외부 운영 설비 관리	외부자가 정보시스템 및 장비를 관리하는 경우 데이터의 손상, 손실 등의 상황을 고려하여 통제방안을 수립하고 계약서에 반영하여야 한다.
		11.2	시스템 운영	11.2.1	시스템 도입	정보시스템의 도입을 위해서 도입 계획 및 정책을 수립하여야 한다.
				11.2.2	시스템 인수	새로운 정보시스템의 설치 또는 수정에 따른 인수기준을 수립하고, 시스템 구매 계약서에 반영하여야 한다. 또한 시스템은 이 기준에 의해 시험을 한 후 인수하여야 한다.
				11.2.3	성능관리	신청기관에서 요구되는 성능 요구사항을 충족시킬 수 있도록 성능관리를 수행하여야 한다.
				11.2.4	용량관리	신청기관에서 요구되는 용량 요구사항을 충족시킬 수 있도록 용량계획을 통해 적정한 용량을 확보하고, 주어진 용량을 최적으로 사용할 수 있는 관리방안을 수립하여 이에 따른 용량관리를 수행하여야 한다.
				11.2.5	백업 및 복구 관리	데이터 및 장비의 무결성과 가용성을 유지하기 위해 백업 계획을 수립하여 이행하여야 하며, 사고 발생시 적시에 복구할 수 있도록 관리하여야 한다.
				11.2.6	장애관리	시스템의 장애시 효과적으로 대응하기 위해 탐지, 기록, 분석, 복구, 보고 등 적절한 조치를 취하여야 한다.
				11.2.7	로그관리	시스템 운영의 확인이나 사고조사를 위해 활동에 대한 기록을 남기고 주기적으로 검토하여야 한다.
				11.2.8	보안 시스템 운영	보안시스템에 대해서는 그 유형별로 설치, 운영에 대한 절차를 수립하고, 절차이행을 주기적으로 검토하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영 관리	11.3	네트워크 운영	11.3.1	네트워크 운영대책	네트워크 운영 보안 유지를 위해 직무 분리, 접근권한 통제, 원격접속 설비 관리, 네트워크 분리 등을 위한 책임 및 절차 등을 포함한 대책을 수립하여야 한다.
				11.3.2	인터넷 접속관리	인터넷망과 접속시 침입차단시스템을 통하여 접근통제를 수행하여야 하며, 필요시 침입탐지시스템 등을 활용하여 접근을 모니터링 하여야 한다.
				11.3.3	원격운영 관리	네트워크를 통해 시스템을 운영하는 경우 원칙적으로 시스템 관리는 내부의 특정 터미널에서만 할 수 있도록 제한하고, 외부에서 네트워크를 통하여 시스템을 관리할 경우에는 사용자 인증, 암호 및 접근통제 기능을 설정하여야 한다.
		11.4	매체 및 문서관리	11.4.1	매체 취급 및 보관	허가되지 않은 유출이나 오용으로부터 정보를 보호하기 위해, 매체의 취급 및 보관에 대한 절차를 수립하고 운영하여야 한다.
				11.4.2	매체의 폐기	매체 폐기를 부주의하게 이행하여 외부자에게 주요정보가 누출되지 않도록 폐기지침을 수립하고 운영하여야 한다.
				11.4.3	시스템 문서의 보안	보안절차, 운영매뉴얼, 운영기록 등 주요 시스템 문서들은 안전하게 보관하고 적절한 폐기절차에 따라 폐기하여야 한다.
		11.5	악성 소프트웨어 통제			바이러스 등의 악성 소프트웨어로부터 시스템을 보호하기 위해 악성 소프트웨어들을 예방하고 탐지, 대응하는 대책을 수립하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영 관리	11.6	이동컴퓨팅 및 원격 작업	11.6.1	이동 컴퓨팅	휴대용 정보통신기기의 사용시에 사업 정보를 보호하기 위한 보안 정책을 수립하고, 내부 네트워크로의 연결 및 공공 장소에서의 사용에 대한 정책을 수립하여야 한다.
				11.6.2	원격 작업	재택 근무와 같은 원격 작업 수행시 이에 대한 물리적, 논리적 보호를 위한 정책과 절차를 마련하여야 한다.
12	전자 거래 보안	12.1	교환 합의서			신청기관간의 정보 및 소프트웨어 교환시에는 이에 대한 합의가 이루어져야 하고, 관리적 책임 및 절차, 전송의 기술적 기준, 인증기준, 데이터의 책임성 등을 반영한 교환 합의서를 작성하여야 한다.
		12.2	전자거래 보안관리			전자거래 시 사기, 계약 분쟁, 정보의 노출 및 수정 등으로부터 보호하기 위해 신원확인, 무결성, 암호화, 부인방지 등의 대책을 수립하여 운영하여야 한다.
		12.3	전자우편			전자 우편 서비스에 대한 가용성, 전자우편 내용에 대한 무결성 및 기밀성과 이에 따른 책임과 위험을 고려한 보안지침 및 대책을 수립하여 운영하여야 한다.
		12.4	공개서버의 보안관리			웹서버 등에 정보를 공개할 경우 정보에 대한 수집, 저장 및 공개에 따른 허가 및 게시절차를 수립하여야 하고, 공개서버에 대한 물리적, 논리적 보안대책을 수립하고 운영하여야 한다.
		12.5	이용자 공지사항			전자거래의 안전한 이행을 위하여 이용자에게 해킹위험, 계정 및 패스워드 관리, 접속관리 등에 대한 공지를 통해 안전거래 준수를 권고하여야 한다.

	통제분야		통제목적		통제사항	통제내용
13	보안사고 관리	13.1	대응 계획 및 체계	13.1.1	대응계획 수립	보안사고의 정의 및 범위, 긴급연락체계 구축, 보안사고 발생시 보고 및 대응 절차, 사고 복구조직의 구성, 교육계획 등을 포함한 보안사고 대응 계획을 수립·이행하여야 한다.
				13.1.2	보안사고 대응체계 구축	보안사고의 대응이 신속하게 이루어질 수 있도록 중앙 집중적인 대응체계를 구축하고, 대응체계에는 내부 직원뿐 아니라 외부기관 및 전문가들과의 협조체계를 반영하여야 한다.
		13.2	대응 및 복구	13.2.1	보안사고 대응 교육 및 훈련	보안사고 대응 계획, 절차 및 방법에 대하여 정기적으로 교육을 실시하여야 하며 사고 처리 후 재발방지를 위하여 필요한 교육훈련을 실시하여야 한다
				13.2.2	보안사고 보고	사고의 징후 또는 보안사고 발생을 인지한 때에는 보고체계에 따라 가능한 한 신속히 보고하여야 한다. 시스템이나 네트워크의 보안 취약점과 소프트웨어 기능장애 또한 신속히 보고하여야 한다.
				13.2.3	보안사고 처리 및 복구	보안사고 보고시 처리, 복구 절차에 따라 처리와 복구를 신속히 이행하여야 한다.
		13.3	사후관리	13.3.1	보안사고 분석 및 정보의 공유	보안사고가 처리되고 종결된 후 이에 대한 분석을 이행하여야 하며, 그 결과를 보고하여야 한다. 또한 사고에 대한 정보와 발견된 취약성들을 관련 신청기관과 임직원에게 공유하여야 한다.
				13.3.2	재발방지	보안사고로부터 얻은 정보를 활용하여, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하여야 한다. 이를 위해 필요한 경우 정책, 절차, 조직 등의 보안체계에 대한 변경을 하여야 한다.

	통제분야		통제목적		통제사항	통제내용
14	검토, 모니터링 및 감사	14.1	법적 요구사항 준수 검토	14.1.1	요구사항 명시	정보시스템에 대해 관련된 모든 법, 규제, 계약, 정책, 기술상의 요구사항을 정의하고 문서화하여야 하며, 이들 요구사항을 만족시키기 위해 필요한 특정 통제나 개별 책임 등도 정의하고 문서화하여야 한다.
				14.1.2	준수 검토	정보통신망이용촉진및정보보호등에관한법률, 신용정보의이용및보호에관한법률 등의 개인정보보호 관련법 및 저작권법, 컴퓨터프로그램보호법 등 지적재산권법 등의 관련 법규의 준수여부를 검토하여야 한다.
				14.1.3	증거자료 수집	보안사고 처리 및 계약 증빙을 위하여 신청기관이나 개인에 대한 소송을 지원하기 위한 적정한 증거 자료를 확보하여야 한다.
		14.2	정보보호 정책 준수 검토	14.2.1	검토 계획	검토의 대상, 주기, 방법, 범위, 절차, 검토자를 포함한 검토계획 및 정책이 수립되어야 한다. 이를 근거로 보안요구사항에 대한 통제와 책임의 준수에 대한 적정성을 검토하여야 한다.
				14.2.2	정책의 준수	모든 정보보호 정책, 절차의 준수여부를 검토하여야 한다.
				14.2.3	기술적 점검	정보시스템이 정보보호표준 및 절차에 따라 운영·관리되고 있는지 정기적으로 기술적 점검을 실시하여야 한다. 이에 따라 취약성들을 발견한 후 필요한 조치를 취하여야 한다.

	통제분야		통제목적		통제사항	통제내용
14	검토, 모니터링 및 감사	14.3	모니터링	14.3.1	접근 및 사용 모니터링	사용자의 시스템, 네트워크 사용 및 접근이 명확하게 허용된 범위 안에 있는지를 확인하기 위해 모니터링 절차를 수립하고 이행하여야 한다. 모니터링 결과는 정기적으로 점검하여야 하고 위험의 정도에 따라 점검 주기를 결정하여야 한다.
				14.3.2	감사기록 분석 및 보관	모니터링을 위한 감사 기록을 생성하고, 분석하며 일정 기간 동안 보관하여야 한다.
				14.3.3	시각 동기화	감사 기록의 명확성을 보장하고 법적인 자료나 징계 자료로서 효력을 갖기 위해서는 시스템 시각을 정확히 설정하여야 한다.
		14.4	보안감사	14.4.1	보안감사 계획 및 이행	보안 감사 대상, 범위, 주기, 방법, 절차, 감사자, 감사도구를 포함한 보안감사 계획을 수립하고 이행하여야 한다.
				14.4.2	감사결과 및 사후관리	감사의 결과에 따라 감사보고서를 작성하고 적정한 책임자에게 보고하며, 감사 지적 내용이 이행되도록 사후관리하여야 한다.
15	업무 연속성 관리	15.1	업무연속성 관리 체계 수립	15.1.1	업무연속성 관리 과정 수립	개시단계, 업무연속성전략수립단계, 구현단계, 운영관리단계 등 업무연속성관리를 위한 과정을 사전에 정의하여야 한다. 개시단계에는 업무연속성관리에 대한 정책 수립 및 범위설정, 자원분배를 포함하여야 하며, 업무연속성전략수립단계는 업무영향분석을 통해 이루어져야 한다. 구현단계에는 재해복구 및 위험감소 대책, 업무연속성계획의 문서화를 포함하여야 하며, 운영관리단계에는 시험, 교육훈련, 검토 및 갱신을 포함하여야 한다.

	통제분야		통제목적		통제사항	통제내용
15	업무 연속성 관리	15.1	업무연속성 관리 체계 수립	15.1.2	업무연속성 계획 프레임워크 수립	업무별 연속성 계획의 이행에 필요한 조건, 응급절차, 대체절차 등을 고려하여 연속성 계획들이 일관성을 유지할 수 있도록 프레임워크를 수립하여야 한다.
		15.2	업무연속성 계획 수립과 구현	15.2.1	업무영향 분석	재난재해별로 업무에 미칠 수 있는 영향을 피해규모와 복구에 소요되는 시간 등을 고려하여 분석하고 그 결과를 기초로 구체적인 업무복구목표 및 복구를 위한 최소한의 요구사항을 설정하여야 한다.
				15.2.2	업무연속성 계획 수립	업무복구목표 및 최소 요구사항을 구현하기 위한 여러 대안들을 평가하여 업무연속성을 위한 전략을 수립하고 대책 구현을 위한 계획을 수립하여야 한다.
				15.2.3	업무연속성 계획 구현	업무연속성계획에서 수립한 위험감소 조치 및 재해복구를 위한 설비를 구현하며 필요한 계획 및 절차 등을 문서화하여야 한다.
		15.3	업무 연속성 계획 시험 및 유지관리	15.3.1	업무연속성 계획 시험	환경의 변화 또는 부정확한 전제 등으로 인한 오류를 제거할 수 있도록 지속적인 시험을 수행하며, 시험 계획에는 시기, 방법, 절차 등을 포함하여야 한다.
				15.3.2	업무연속성 계획 유지·관리	업무연속성계획에 대해 정기적인 교육 및 훈련을 실시하고 지속적인 검토와 평가 및 변경관리를 수행하여야 한다.

[별지 제1호서식]

(앞 쪽)

정보보호관리체계인증기관 지정신청서				처리기간 3 월
신청인	①업 체 명 및 대 표 자 성 명		②설 립 일 자	
	③소 재 지		④전 화 번 호	
	⑤직 원 수	명	⑥인증심사업무를 전담하는 직원의 수	명

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조 및 같은 법 시행령 제48조에 따라 위와 같이 정보보호관리체계인증기관의 지정을 신청합니다.

년 월 일

신청인 (서명 또는 인)

방송통신위원회 귀중

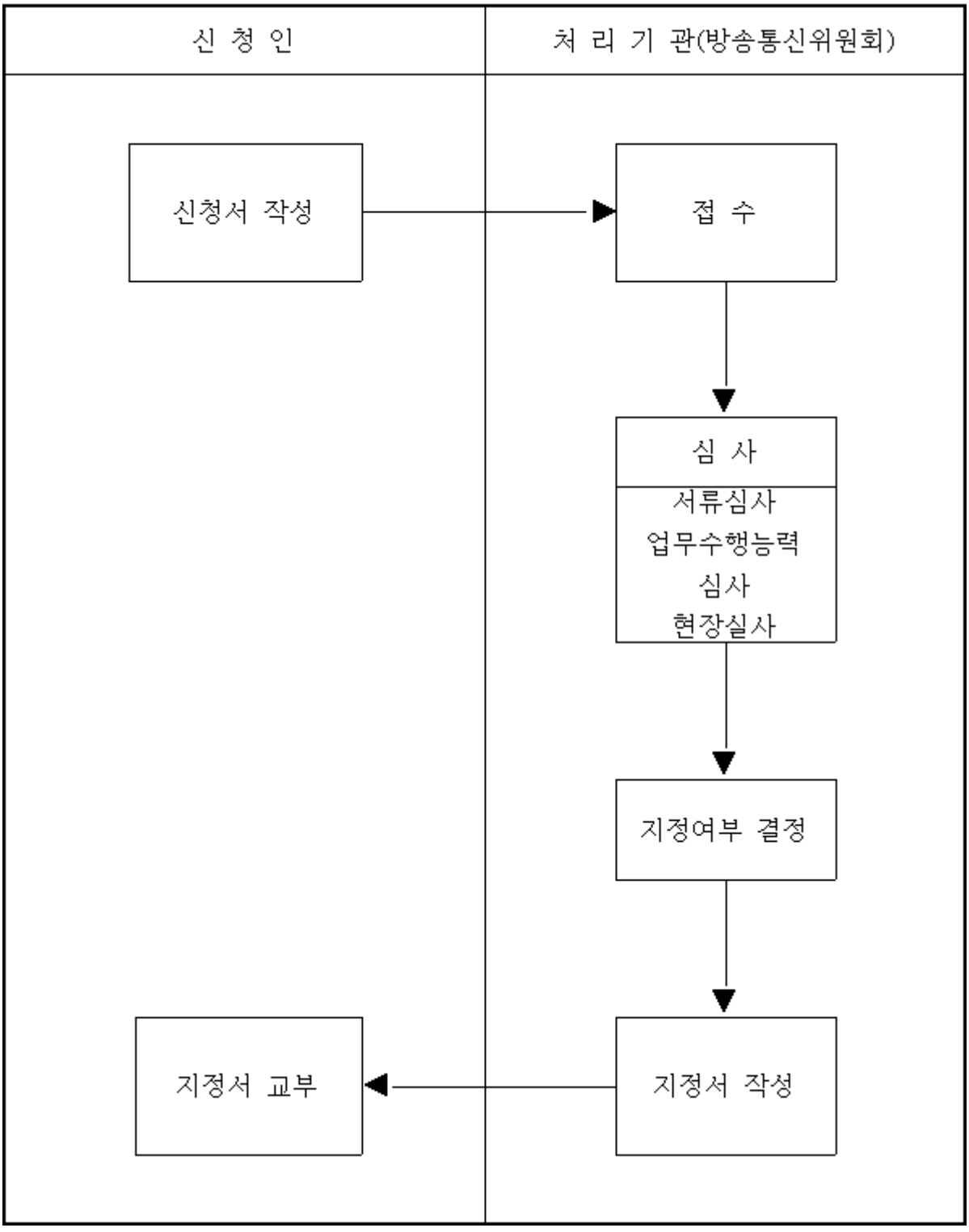
구비서류	신청인(대표자) 제출서류	담당공무원 확인사항 (부동의하는 경우 해당서류 제출)	수수료
	1. 정관 2. 별지 제2호서식의 인증심사업무를 전담하는 직원 보유현황과 이를 증명할 수 있는 서류 3. 별표 제1호에 따른 업무수행능력심사를 위하여 필요한 서류	법인등기부 등본 (법인인 경우)	없 음

본인은 이 신청서의 처리와 관련하여 「전자정부법」 제21조제1항에 따른 행정정보의 공동이용을 통하여 담당공무원이 위의 담당공무원 확인사항을 확인하는 것에 동의합니다.

신청인(대표자) (서명 또는 인)

210㎜×297㎜(일반용지 60g/㎡)

이 신청서는 아래와 같이 처리됩니다. (뒤 쪽)



[별지 제2호서식]

(제1쪽)

인증심사업무를 전담하는 직원의 보유현황					
업체명					
대표자 성명					
소 재 지					
종업원수		인증심사업무를 전담하는 직원의 수			

일련번호	성 명 (한 자)	주 소 / 주민등록번호	입사일	최종학위 / 취득학교 및 학과(전공)	해당 요건

(제2쪽)

일련번호	성 명 (한 자)	주 소		최종학위	해당 요건
		주민등록번호	입사일	취득학교 및 학과(전공)	

비 고

1. 「해당요건」란에는 별표 1의 요건 중 당해 인증심사업무를 전담하는 직원이 충족하는 요건을 기재한다.
   예시) 학력 및 경력기준 제2호 가목
2. 기재된 최종학위를 증명할 수 있는 직원의 졸업 또는 학위증명서 사본을 제출하여야 한다.
3. 별표 1의 「자격 및 경력기준」을 충족하는 직원은 기술자격증 사본 등 자격을 취득하였음을 확인할 수 있는 서류를 함께 제출하여야 한다.
4. 정보통신유관경력 또는 정보보호유관경력을 증명할 수 있는 경력증명서(근무부서 또는 담당업무 등이 기재되어야 한다)와 해당 직원이 신청업체에 현재 근무하고 있음을 확인할 수 있는 재직증명서를 함께 제출하여야 한다.

[별지 제3호서식]

정보보호수행실적 명세서

업 체 명					
대 표 자 성 명					
소 재 지					
정보보호수행실적 총계		외 건 (총 천원)			
일련번호	정보보호수행실적(프로젝트명) 대상기관(기업)명	수행 기간	계약 금액(천원)	과제책임자	구분

비 고

1. 계약금액란에는 정보보호에 관한 업무를 수행한 대가로서 지급받은 대금을 기재하고, 구분란에는 정보보호에 관한 감사, 감리, 진단, 인증, 컨설팅 등으로 실적을 구분하여 기재한다.

[별지 제4호서식]

(제1쪽)

제 호

정보보호관리체계인증기관지정서

업체명 :

대표자 :

소재지 :

지정의 유효기간 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조 및 같은 시행령 제48조에 따라 위와 같이 정보보호관리체계인증기관으로 지정합니다.

년 월 일

방송통신위원회 위원장 [인]

210㎜×297㎜

(보존용지(1종) 120g/㎡)

(제2쪽)

Registry No.

CERTIFICATE OF DESIGNATION
AS
ISMS Certification Authority

Name of Organization :
Name of Representative :
Address :
Period of Validity :

This is to certify that the above-mentioned organization is designated Information Security Management System (ISMS) certification Authority in accordance with Article 47 of the Act on Promotion of Information and Communication Network Utilization and Information Protection, etc. and Article 48 of Promotion of Information and Communication Network Utilization and Information Protection, Etc. Enforcement Ordinance of Act

Signed by the
Chairman of Broadcasting and Communications Commission
Republic of Korea

210㎜×297㎜
(보존용지(1종) 120g/㎡)

[별지 제5호서식] (앞 쪽)

정보보호관리체계인증신청서				
신청인	성 명(대 표 자)		주민등록번호	
	상호 또는 명칭		사업자등록번호	
	소 재 지		전 화 번 호	
인증신청의 구분		□처음으로 인증신청을 하는 때 □유효기간의 만료로 다시 인증신청을 하는 때 □인증의 범위에 중요한 변경이 있어서 다시 인증신청을 하는 때		
정보보호관리체계의 범위				
정보보호관리체계의 범위에 포함되어 있는 종업원의 수				

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제4항, 동법 시행령 제50조에 따라 위와 같이 정보보호관리체계의 인증을 신청합니다.

년 월 일

신청인 (서명 또는 인)

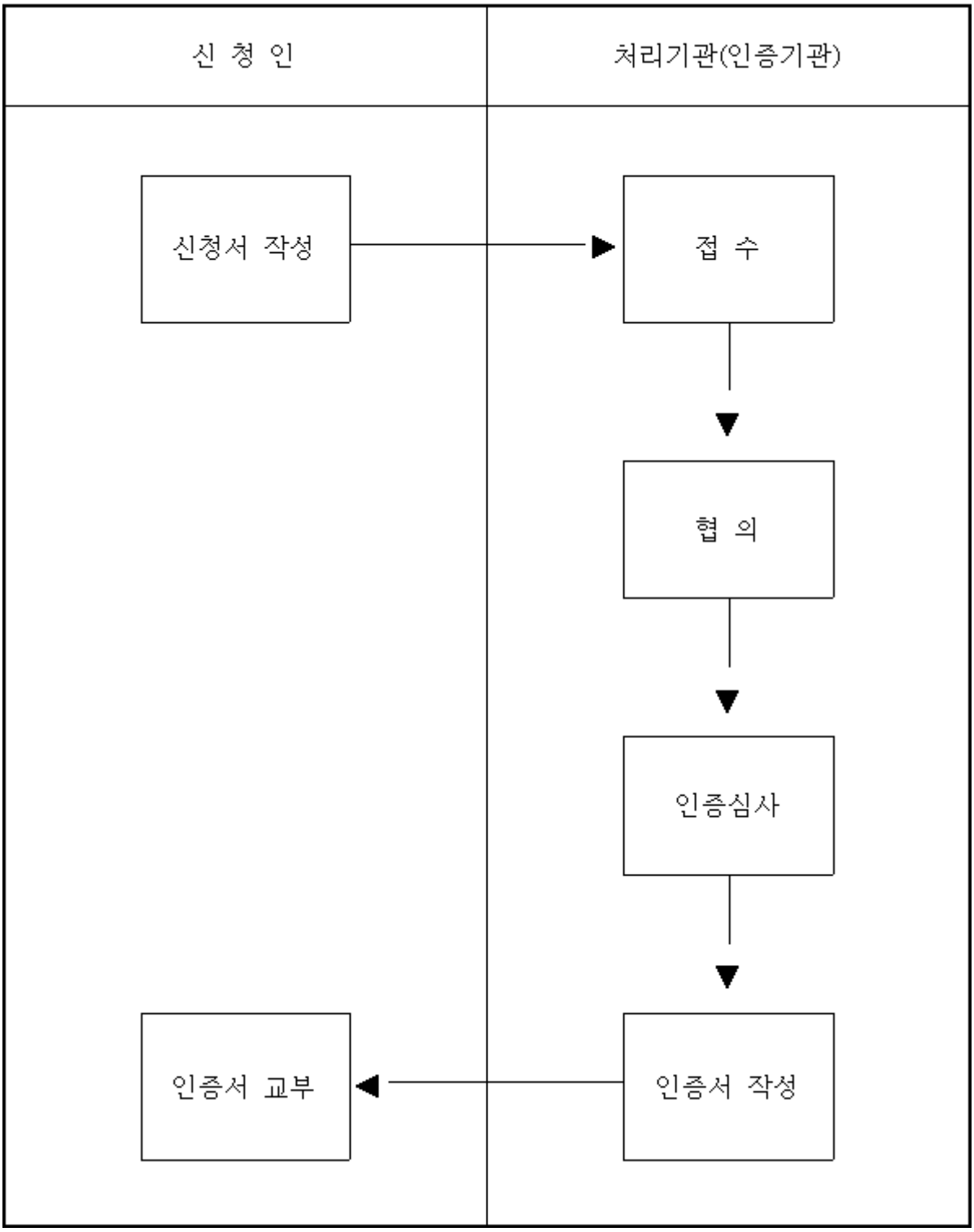
(인증기관명) 귀하

구비서류

1. 법인등기부 등본(법인인 경우에 한합니다)
2. 정보보호관리체계의 내역서

210mm×297mm(신문용지 54g/㎡)

이 신청서는 아래와 같이 처리됩니다. (뒤 쪽)



[별지 제6호서식] (제1쪽)

제 호

정보보호관리체계인증서

상호 또는 명칭 :

대 표 자 :

소 재 지 :

인증의 범위 :

유 효 기 간 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제4항, 같은 법 시행령 제50조에 따라 위와 같이 정보보호관리체계를 인증합니다.

년 월 일

(인증기관장) (인)

210mm×297mm(보존용지(1종) 120g/㎡)

(제2쪽)

Certificate Number :

CERTIFICATE

OF

Information Security Management System

Name of Organization :

Name of Representative :

Address :

Scope of Certification :

Period of Valid :

Date of Issuance :

This is to certify that the above- mentioned organization is compliant to the assessment standard for Information Security Management System certification in accordance with Article 47, Paragraph 1 and 4 of Act on Information Network Utilization and Data Protection, etc., and Article 50 of the Enforcement Ordinance of the Act.

Signed by the
President of ISMS Certification Authority
Republic of Korea

210mm×297mm(보존용지(1종) 120g/㎡)

[별지 제7호서식] 정보보호관리체계 인증서 추가발급 신청서

정보보호관리체계 인증서 추가발급 신청서

신청인	상호 또는 명칭		성 명(대표자)	
	사업자등록번호		전화번호	
	주 소(소재지)			
추가발급 사유				

위와 같이 정보보호관리체계 인증서의 추가발급을 신청합니다.

200 년 월 일

신청인 (서명 또는 인)

[별지 제8호서식] 정보보호관리체계 인증서 변경 신청서

정보보호관리체계 인증서 변경 신청서

신청인	상호 또는 명칭		성 명(대표자)	
	사업자등록번호		전화번호	
	주 소(소재지)			
변경내용	변경전	(국문)		
		(영문)		
	변경후	(국문)		
		(영문)		
변경 사유				

위와 같이 정보보호관리체계 인증서 변경을 신청합니다.

200 년 월 일

신청인 (서명 또는 인)

정보보호 관리체계 인증 등에 관한 고시

[시행 2016.4.8] [고시 제2016 - 38호, 2016.4.8, 일부개정]

제1장 총칙

제1조(목적) 이 고시는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) 제47조제3항 및 같은 법 시행령(이하 "영"이라 한다) 제47조부터 제53조의2의 규정에 따라 정보보호 관리체계 인증에 관하여 필요한 사항에 대해 정하는 것을 목적으로 한다.

제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "정보보호 관리체계 인증기관(이하 ‘ 인증기관 ’ 이라 한다)"이란 법 제47조제5항에 따라 미래창조과학부가 인증에 관한 업무를 수행할 수 있도록 지정한 기관을 말한다.
2. "업무수행 요건·능력 심사"란 인증기관으로 지정받고자 신청한 법인 또는 단체의 업무수행 요건·능력을 별표 2의 세부기준에 따라 심사하는 것을 말한다.
3. "인증"이란 신청기관이 수립하여 운영하고 있는 정보보호 관리체계가 별표 6의 정보보호 관리체계 인증기준(이하 "인증기준"이라 한다)에 적합함을 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다) 또는 인증기관이 증명하는 것을 말한다.
4. "인증심사"란 신청기관이 수립하여 운영하는 정보보호 관리체계가 인증기준에 적합한지의 여부를 인터넷진흥원 또는 인증기관이 서면심사 및 현장심사의 방법으로 확인하는 것을 말한다.
5. "정보보호관리과정(이하 ‘ 관리과정 ’ 이라 한다)"이란 정보보호 관리체계를 수립·운영하기 위하여 유지·관리하여야 할 과정으로 다음 각 목의 5단계 활동을 말한다.
   가. 정보보호정책 수립 및 범위설정
   나. 경영진 책임 및 조직구성
   다. 위험관리
   라. 정보보호대책 구현
   마. 사후관리
6. "정보보호대책"이란 신청기관이 정보보호 관리체계를 수립·운영하기 위하여 별표 6에서 선택한 통제사항을 말한다.
7. "신청기관"이란 이 고시에 따라 정보보호 관리체계 인증을 취득하고자 신청한 자를 말한다.

8. "인증심사원"이란 별표 3의 자격요건을 갖춘 자를 말한다.
9. "최초심사"란 처음으로 인증을 신청하거나 인증의 범위에 중요한 변경이 있어서 다시 인증을 신청한 때 실시하는 인증심사를 말한다.
10. "사후심사"란 정보보호 관리체계 인증(인증이 갱신된 경우를 포함한다)을 받고난 후 매년 사후관리를 위하여 실시하는 인증심사를 말한다.
11. "갱신심사"란 유효기간 만료로 다시 인증을 신청한 때 실시하는 인증심사를 말한다.

제2장 정보보호 관리체계 인증기관

제3조(인증기관의 지정 등) ① 미래창조과학부는 법 제47조제5항 및 영 제53조의2에 따라 인증기관을 지정할 필요가 있는 때에는 지정대상 기관의 수, 업무의 범위 및 신청방법 등을 정하여 관보 및 인터넷 홈페이지에 20일 이상 공고하여야 한다.

② 제1항에 따라 인증기관으로 지정받으려는 자는 다음 각 호의 서류를 미래창조과학부에 제출하여야 한다.

1. 별지 제1호서식의 정보보호 관리체계 인증기관 지정 신청서
2. 영 제53조의2제1항제2호에 따른 별지 제2호서식의 인증심사원 보유현황과 이를 증명할 수 있는 서류
3. 영 제53조의2제1항제3호에 따른 별표 1의 업무수행 요건·능력 심사를 위하여 필요한 서류

제4조(업무수행 요건·능력 심사 세부기준 등) ① 영 제53조제2항에 따른 업무수행 요건·능력 심사를 위한 세부기준은 별표 2와 같다.

② 미래창조과학부는 제3조제2항에 따라 인증기관의 지정 신청을 받은 때에는 제1항에 따라 업무수행 요건·능력을 심사하여 지정 대상기관의 순위를 정한다.

제5조(업무수행 능력의 적합성 인정) ① 미래창조과학부는 제4조제1항에 따라 업무수행 요건·능력을 심사하여 지정에 필요한 수만큼 점수의 합이 높은 순으로 선별한다.

② 미래창조과학부는 제1항에 따라 심사한 결과를 바탕으로 하여 인증기관으로의 지정 여부를 최종 결정한다.

제6조(인증기관 지정서) 영 제53조의2제3항에 따른 정보보호 관리체계 인증기관 지정서는 별지 제3호서식과 같다.

제7조(인증기관의 사후관리) 영 제53조의4제1항에 따른 인증기관의 전년도 인증실적 보고서는 별지 제4호서식과 같다.

제8조(인증기관 재지정) ① 인증기관은 유효기간이 끝나기 전 6개월부터 끝나는 날까지 별지 제1호서식에 따라 미래창조과학부에 재지정 신청을 할 수 있다.

② 제1항에 따른 재지정의 심사, 재지정 결과 통지, 재지정서 교부 등에 관하여는 영 제53조의2제3항을 준용한다.

제3장 인증심사원의 자격 및 관리

제9조(인증심사원의 자격 요건 등) ① 인증심사원은 심사원보, 심사원, 선임심사원으로 구분하며, 인증심사원 등급별 자격 요건은 별표 3과 같다.

② 인증심사원이 되려는 자는 별표 3의 학력 및 경력 요건을 갖추고 인터넷진흥원이 지정하는 기관에서 인증심사원 양성교육 과정을 수료하여야 한다.

제10조(인증심사원 자격 신청) 인증심사원의 자격을 신청하고자 하는 자는 제9조제2항에 따라 인증심사원 양성교육 과정을 수료한 날로부터 1개월 이내에 인터넷진흥원에 다음 각 호의 모든 서류를 제출하여야 한다.

1. 별지 제5호서식 정보보호 관리체계 인증심사원 자격 신청서
2. 학위증명서, 자격증 사본(해당 시)
3. 별지 제6호서식 경력증명서
4. 별지 제7호서식 상세 재직증명서 등 경력증빙서류
5. 별지 제8호서식 기술실적증명서(해당 시)

제11조(인증심사원 자격 부여) ① 인터넷진흥원은 인증심사원 자격 신청서를 접수한 때에는 신청서류를 검토하여 서류 보완 및 추가제출을 요청할 수 있다.

② 서류 보완 및 추가제출을 요청받은 자격 신청자는 1개월 이내에 관련 서류 등을 제출하여야 한다.

③ 인터넷진흥원은 인증심사원 자격의 적합 여부를 확인하여 통과한 자에게 별지 제9호서식의 인증심사원 자격 증명서를 발급하여야 한다.

제12조(인증심사원 자격 유지) ① 인증심사원의 자격 유효기간은 자격 부여를 받은 날로부터 3년으로 한다.

② 인증심사원은 자격 유지를 위해 유효기간 내에 인터넷진흥원이 지정하는 기관에서 시행하는 인증심사원 보수교육을 이수해야 한다. 다만, 부득이한 사유로 보수교육을 받지 못한 경우에는 인터넷진흥원이 인정하는 대체교육을 받아야 한다.

③ 보수교육을 이수한 자에 한하여 자격 유효기간이 3년간 연장된다.

제13조(인증심사원 자격 취소) ① 인증심사원 자격 신청 시 제출한 서류가 허위이거나, 제12조에 따른 자격 유지 기준을 충족하지 못한 경우에는 자격을 취소한다.

② 인증심사원으로서 객관적이고 공정한 인증심사를 수행하지 않거나, 인증심사와 관련된 부당한 금전, 금품 등을 수수하거나 인증심사 수행 중 취득한 정보를 누설하는 경우에는 자격을 취소한다.

제4장 인증심사의 신청 및 계약

제14조(인증 의무대상자 범위) ① 인증 의무대상자란 법 제47조제2항, 영 제49조에 따라 정보보호 관리체계 인증을 받아야 하는 자를 말한다.

② 법 제47조제2항제2호에 따라 정보보호 관리체계 인증을 받아야 하는 자 중 집적정보통신시설 사업자가 마련한 시설의 일부를 임대하여 집적정보통신시설 사업을 하는 자에 대하여는 영 제49조제2항의 기준을 준용한다.

③ 인증 의무대상자는 매년 1월1일부터 12월31일까지 인증을 받아야 한다.

제15조(신청기관의 사전 준비사항) 신청기관은 정보보호 관리체계 인증을 신청하기 전에 인증기준에 따른 정보보호 관리체계를 구축하여 최소 2개월 이상 운영하여야 한다.

제16조(인증의 신청 등) ① 법 제47조제1항 또는 제2항에 따라 정보보호 관리체계 인증을 받으려는 자는 별지 제10호서식의 정보보호 관리체계 인증 신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

② 신청기관은 인증의 범위 및 일정 등을 인터넷진흥원 또는 인증기관과 사전 협의하여 신청하여야 한다.

③ 인터넷진흥원 또는 인증기관은 제14조에 따른 인증 의무대상자가 사업자 등록일이 속한 분기가 끝나는 날의 1개월 전까지 인증 신청을 한 경우 인증심사를 우선적으로 처리할 수 있다.

제17조(인증심사 계약 체결) 신청기관은 인터넷진흥원 또는 인증기관과 협의한 후 심사기간, 심사인원, 인증 수수료, 인증의 범위 등을 포함하는 인증심사 계약을 체결한다.

제5장 인증심사의 기준과 방법

제18조(인증기준) 인증기준은 별표 6과 같다.

제19조(인증심사팀 구성) ① 인터넷진흥원 또는 인증기관은 제17조에 따른 인증심사 계약을 체결한 때에는 지체 없이 인증심사원으로 인증심사팀을 구성하여야 한다.

② 인증심사팀 구성 시 심사팀장은 인터넷진흥원 또는 인증기관 소속의 심사원 이상으로 선정하여야 한다.

③ 신청기관의 정보보호 관리체계 인증을 위한 컨설팅에 참여한 인증심사원 또는 신청기관의 소속직원은 인증심사팀의 구성원에서 배제하여야 한다.

제20조(인증심사 방법 및 보완조치) ① 인증심사는 신청기관을 방문하여 서면심사와 현장심사를 병행한다.

② 서면심사는 인증기준에 적합한지에 대하여 정보보호 관리체계 구축·운영 관련 정보보호 정책, 지침, 절차 및 이행의 증적자료 검토, 정보보호대책 적용 여부 확인 등의 방법으로 관리

적 요소를 심사한다.

③ 현장심사는 서면심사의 결과와 기술적·물리적 보호대책 이행 여부를 확인하기 위하여 담당자 면담, 관련 시스템 확인 및 취약점 점검 등의 방법으로 기술적 요소를 심사한다.

④ 인터넷진흥원 또는 인증기관은 인증심사에서 발견된 결함에 대해 최대 90일(재조치 요구 60일 포함) 이내에 보완조치를 완료하도록 신청기관에게 요청할 수 있다.

⑤ 인터넷진흥원 또는 인증기관은 인증위원회 심의결과에 따라 30일 이내에 보완조치를 요구할 수 있다.

제6장 인증위원회 구성과 운영

제21조(인증위원회의 구성) ① 법 제47조제5항에 따라 인터넷진흥원 또는 인증기관의 장은 다음 각 호의 사항을 심의·의결하기 위하여 인증위원회를 설치·운영하여야 한다.

1. 최초심사 또는 갱신심사 결과가 인증기준에 적합한지 여부
2. 사후심사 결과 법 제47조제8항 각 호에 해당하는 사유를 발견한 경우에 그 결과의 적합성 여부
3. 그 밖에 정보보호 관리체계 인증과 관련하여 위원장이 필요하다고 인정하는 사항

② 인증위원회는 5인 이상 10인 이내의 위원으로 구성하되, 위원은 정보보호전문가, 정보시스템감리사, 기술사, 대학교수 등 정보보호분야에 학식과 경험이 있는 자 중에서 인터넷진흥원 또는 인증기관의 장이 위촉하며, 위원장은 위원 중에서 호선한다.

③ 위원장은 인증위원회의 업무를 통할하며 위원회를 대표한다.

제22조(인증위원회의 운영) ① 인터넷진흥원 또는 인증기관의 장은 인증위원회의 심의안건을 검토하여 위원회 개최 5일 전까지 인증위원회에 제출한다.

② 인증위원회 위원장은 제21조제1항 각 호의 사항에 대한 심의·의결 결과를 인터넷진흥원 또는 인증기관의 장에게 제출한다.

제7장 인증서의 발급·관리 및 홍보

제23조(인증서 발급) 인터넷진흥원 또는 인증기관의 장은 제22조제1항에 따라 인증위원회의 심의·의결 결과를 제출받은 때에는 신청기관의 정보보호 관리체계가 이 고시에서 정한 인증기준에 적합하다고 판단된 경우 별지 제11호서식의 정보보호 관리체계 인증서를 발급하여야 한다.

제24조(인증서 관리) ① 인터넷진흥원 또는 인증기관은 발급된 인증서의 인증번호, 발급일, 유효기간 등 인증서를 관리하여야 한다.

② 인증을 취득한 자는 인증서의 분실 등으로 인해 재발급을 받고자 할 경우 별지 제12호서식의 정보보호 관리체계 인증서 추가발급 신청서를 인터넷진흥원 또는 인증기관에 제출하여야

한다.

③ 인증을 취득한 자가 주소, 업체명 등 인증서 기재사항의 변경을 요청하고자 하는 경우 별지 제13호서식의 정보보호 관리체계 인증서 변경신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

제25조(인증의 표시 및 홍보) ① 영 제52조에 따른 인증의 표시는 별표 4와 같다.

② 제1항에 따른 인증의 표시를 사용하는 경우에는 영 제52조에 따라 인증의 범위와 유효기간을 함께 표시하여야 한다.

제8장 정보보호 관리체계 인증 수수료

제26조(수수료의 산정) ① 인증 수수료는 다음 각 호의 기준을 준용하되 별표 5의 정보보호 관리체계 인증 수수료 산정기준을 적용하여 산정한다.

1. 「엔지니어링산업 진흥법」 제31조제2항에 따른 엔지니어링사업의 대가 기준
2. 한국소프트웨어산업협회가 제공하는 「SW사업 대가산정 가이드」의 정보보안 컨설팅비

② 인터넷진흥원 또는 인증기관은 제1항에 따라 산정된 인증 수수료를 공지하여야 한다. 다만, 「중소기업기본법」 제2조에 따른 중소기업이 인증을 신청하는 경우 수수료 감면 등 필요한 지원을 할 수 있다.

③ 인터넷진흥원 또는 인증기관은 신청기관의 인증범위가 정보보호 관련 타 인증과 중복될 경우 신청기관과 협의하여 수수료를 조정할 수 있다.

제27조(수수료의 납부) ① 신청기관은 최초심사, 사후심사 및 갱신심사 신청 시 수수료를 납부한다. 다만, 수수료 납부 방법(일괄 또는 분할)은 인증심사 계약 시 신청기관과 협의하여 조정할 수 있다.

② 신청기관은 인증심사 계약을 체결한 날로부터 1개월 이내에 인증 수수료를 인터넷진흥원 또는 인증기관에 납부하여야 한다.

제28조(인증업무 지침) 인터넷진흥원 또는 인증기관은 인증업무 수행을 위해 필요한 경우 인증업무에 관한 지침을 마련하여 시행할 수 있다.

제29조(재검토기한) 「훈령ㆍ예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제334호)에 따라 이 고시에 대하여 2017년 1월 1일 기준으로 매 3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2013-4호,2013.1.17>

제1조(시행일) 이 고시는 2013년 2월 18일부터 시행한다.

제2조(인증심사원에 관한 경과조치) 이 고시 시행 이전에 종전 고시에 따라 인증 심사업무를 전담하는 직원의 요건을 갖추고 인터넷진흥원으로부터 위촉된 자는 이 고시에 의한 인증심사원

자격을 취득한 것으로 본다.

부칙 <제2013 - 36호,2013.8.8>

제1조(시행일) 이 고시는 2013년 8월 8일부터 시행한다.

부칙 <제2016 - 38호,2016.4.8>

제1조(시행일) 이 고시는 공포한 날부터 시행한다.

[별표 1]

업무수행 요건·능력 심사 규정에 따른 제출서류(제3조제2항 관련)

구 분	제 출 서 류
1. 정보보호 관리체계 인증심사 참여 실적을 확인하는 데 필요한 서류	가. 별지 제4호서식에 따른 정보보호 관리체계 인증심사 참여실적 명세서 및 이를 증빙할 수 있는 자료 (인증심사 참여통지 문서 등) 나. 인증심사원 자격 증빙 자료
2. 업무수행 요건·능력 심사를 위하여 필요한 서류	가. 자본금 5억원 이상 내역(공인회계사 또는 회계담당자가 서명 날인한 서류) 나. 부채비율 및 자기자본 이익률의 계산내역(회계결산내역 등 관련 증빙자료) 다. 인증심사 업무 운영체계 관련 규정 및 지침 등 o 심사기관의 운영체계 및 인증의 품질관리 o 인증심사 업무를 수행하는 직원에 대한 운영관리 등의 내부규정 o 인증심사 업무 수행 방법 및 절차

[별표 2]

업무수행 요건·능력 심사 세부기준(제4조제1항 관련)

가. 업무수행 요건 심사 세부기준

평가항목	세부 평가 기준
1. 인증심사원 5명 이상 상시 고용 여부	o 인증심사원 5명 이상을 상시 고용하고 있어야 함 - 다만, 심사팀장급 심사원 1명 이상 확보해야 함
2. 인증기관 공정성 확보 여부	o 정보보호 관리체계 인증기관으로 지정을 받으려는 기관은 인증업무의 독립성, 객관성, 공정성, 신뢰성을 확보하기 위하여 정보보호 관리체계 구축과 관련된 컨설팅 업무를 수행하지 않아야 함

나. 업무수행 능력 심사 세부기준

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td rowspan="3">1. 조직 내 직원들의 정보보호 전문성 (30)</td><td rowspan="3">정보보호 업무 전문성</td><td>10</td><td>비율</td><td>o 심사원 이상 인력 수
<table><tr><td>심사원 수</td><td>점수</td></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (심사원 수/5명) × 100</td></tr></table></td></tr>
<tr><td>5</td><td>비율</td><td>o 정보보호 관련 박사학위 소지자 · 기술사 인력의 수
<table><tr><td>박사학위소지자·기술사 수</td><td>점수</td></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (박사학위 소지자, 기술사 수/5명) × 100</td></tr></table></td></tr>
<tr><td>5</td><td>비율</td><td>o CISM, SIS, CISSP, CISA, CPPG, 정보보안기사/산업기사 자격증 소지자 수
<table><tr><td>자격증 소지자· 수</td><td>점수</td></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (자격증 소지자 수/5명) × 100</td></tr></table></td></tr>
<tr><td rowspan="2">정보보호 관리체계 인증심사 참여실적</td><td>10</td><td>비율</td><td>o 상시 고용하고 있는 인증심사원이 최근 3년간 참여한 정보보호 관리체계 인증심사 참여 실적을 인정하고 평가점수는 개별 참여 실적을 합한 총 참여일수에 따라 산출
<table><tr><td>총 참여 일수(단위 : 일)</td><td>점수</td></tr><tr><td>200일 이상</td><td>배점의 100%</td></tr><tr><td>200일 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (총 참여일수/200일) × 100</td></tr></table></td></tr>
</table>

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td>2. 시설(10)</td><td>사무공간 · 인증심사 서류 보관 창소 및 보안설비·시설 확보</td><td>10</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 인증심사의 상담, 인증심사 업무의 처리를 위해 필요한 사무실</td><td>2점</td></tr>
<tr><td>o 사무 관련 장비 확보</td><td>2점</td></tr>
<tr><td>o 사무실 출입자에 대한 신원확인 및 출입통제를 위한 설비</td><td>2점</td></tr>
<tr><td>o 기록물 및 자료의 안전한 관리를 위한 보관 창소</td><td>2점</td></tr>
<tr><td>o 인증심사 서류의 분실, 도난 등 예방을 위한 보안 사설</td><td>2점</td></tr>
</table>
</td></tr>
<tr><td rowspan="2">3. 신뢰도 및 재정상태 건실도 (10)

※비영리기관 평가제외</td><td>부채비율</td><td>5</td><td>비율</td><td>o 지정 공고일 기준으로 직전년도 부채비율
(부채총계/자기자본)
<table>
<tr><th>비율</th><th>점수</th></tr>
<tr><td>50% 미만</td><td>5점</td></tr>
<tr><td>50% 이상 ~ 100% 미만</td><td>4점</td></tr>
<tr><td>100% 이상 ~ 150% 미만</td><td>3점</td></tr>
<tr><td>150% 이상 ~ 200% 미만</td><td>2점</td></tr>
<tr><td>200% 이상</td><td>1점</td></tr>
</table>
</td></tr>
<tr><td>자기자본 이익률</td><td>5</td><td>비율</td><td>o 지정 공고일 기준으로 직전년도 자기자본이익률
(당기순이익/자기자본)
<table>
<tr><th>비율</th><th>점수</th></tr>
<tr><td>20% 이상</td><td>5점</td></tr>
<tr><td>20% 미만 ~ 15% 이상</td><td>4점</td></tr>
<tr><td>15% 미만 ~ 10% 이상</td><td>3점</td></tr>
<tr><td>10% 미만 ~ 5% 이상</td><td>2점</td></tr>
<tr><td>5% 미만</td><td>1점</td></tr>
</table>
</td></tr>
<tr><td rowspan="3">4. 인증업무 운영 체계 (50)</td><td>인증기관의 운영 체계 및 인증의 품질관리</td><td>20</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 인증기관의 공정성·객관성·신뢰성·독립성 보증 방안</td><td>5점</td></tr>
<tr><td>o 인증기관의 내부감사 실시 및 검토 등에 대한 방안</td><td>5점</td></tr>
<tr><td>o 인증의 품질 보증 및 관리방안</td><td>5점</td></tr>
<tr><td>o 인증업무의 기록 및 문서화 관리체계의 적절성</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td>인증업무를 수행하는 직원에 대한 운영 · 관리 등의 내부 규정</td><td>10</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 인증업무를 수행하는 직원에 대한 규정 보유 및 그 규정의 타당성 및 실효성
- 인증업무를 수행하는 직원의 의무와 책임 등 준수사항
- 인증업무를 수행하는 직원의 자체 보안관리 및 감독 요령</td><td>5점</td></tr>
<tr><td>o 인증업무를 수행하는 직원의 교육 및 평가 등에 대한 방안 및 그 방안의 적절성 및 타당성</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td>인증업무 수행 방법 및 절차</td><td>5</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 인증업무 수행 방법 및 절차 등의 적절성 및 타당성
- 인증심사의 절차 및 방법
- 인증수수료 및 그 징수방법
- 인증심사팀 구성 원칙
- 인증심사 사후관리방안 등</td><td>5점</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td></td><td>인증업무
지원체계</td><td>15</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 운영자금 법인통장 보유 및 유지 수준</td><td>5점</td></tr>
<tr><td>o 지정취소, 부도 · 해산 등에 따른 신청기관 피해 보상 관련 보험 가입 여부</td><td>5점</td></tr>
<tr><td>o 인증의 품질 제고를 위한 지원방안</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td>5. 가점 및 감점</td><td>인증심사 업무를 전담하는 인증심사원 보유수</td><td>5
(가점)</td><td>보유
인원수</td><td>o 인증심사업무를 수행하는 전담조직을 갖추고, 그 전담조직에 속한 직원에 대해 인정
<table>
<tr><th>구분</th><th>점수</th></tr>
<tr><td>10명 이상</td><td>5점</td></tr>
<tr><td>10명 미만 ~ 5명 이상</td><td>배점의 X%</td></tr>
<tr><td>5명 미만</td><td>없음</td></tr>
<tr><td colspan="2">※X = (인원수/10명) × 100</td></tr>
</table>
</td></tr>
<tr><td></td><td>정보보호
관리체계 인증의 취득 및 유지</td><td>2
(가점)</td><td>인증 취득
및 유지</td><td>o 정보보호 관리체계 인증을 취득하고, 인증을 유지하고 있을 때</td></tr>
<tr><td></td><td>자격취소 사실</td><td>5
(감점)</td><td>취소사실
및
취소회수</td><td>o 지정 공고일 기준으로 10년 이내에 미래창조과학부가 부여한 정보보호 관련 수행자격이 취소된 경우
- 정보보호 관리체계 인증기관, 안전진단 수행기관 등
※ 취소 1회당 : 감점 5점</td></tr>
</table>

<비 고>

1. 평가항목에 대한 각 평가요소별 세부평가 점수는 소수점 이하 둘째 자리에서 반올림한다.
2. 평가항목에 대한 각 평가요소별 평가점수는 평가결과의 최저점과 최고점을 제외한 점수들의 평균점을 부여한다. 다만, 최저점 또는 최고점이 2개 이상일 경우 각 1개만 제외한다.
3. 가점을 합한 점수가 100점을 초과해도 만점 100점으로 표기한다.
4. '시설', '인증업무 운영체계'에 대한 각 평가요소별 세부평가 점수 부여기준은 각 평가요소의 평가결과에 평가등급(계수)를 곱하여 나온 점수를 합산한다.

평가요소별 세부평가 점수	평가등급(계수)
100점 이하 ~ 90점 이상	우수(1.0)
90점 미만 ~ 80점 이상	보통(0.6)
80점 미만 ~	미흡(0.2)
미 제출	점수없음(0)

[별표 3]

인증심사원 자격 요건(제9조 관련)

1. 인증심사원 등급별 자격 요건

구 분	자격 요건
심사원보	o 인증심사원 학력 및 경력요건을 만족하는 자로서 인터넷진흥원이 지정하는 기관에서 인증심사원 양성교육 과정을 수료한 자
심사원	o 심사원보 자격 취득자로서 인증심사 4회 이상 참여하고 심사일수의 합이 20일 이상인 자
선임심사원	o 심사원 자격 취득자로서 3회 이상 심사 총괄업무를 수행하고 심사일수의 합이 15일 이상인 자

2. 인증심사원 학력 및 경력 요건

o 학사학위를 취득한 후 정보통신 또는 정보보호 유관경력 6년(전문학사의 경우 8년, 수업연한이 3년인 전문학사의 경우 7년, 고등학교 졸업자의 경우 10년을 말한다) 이상을 보유한 자(최근 10년 이내의 경력에 한함)

o 유관자격 소지자 또는 유관학력을 취득한 자로서 다음 각 목의 어느 하나에 해당하는 경우 정보통신 유관경력을 인정한다.
가. 기술사 자격 소지자 또는 박사 학위를 취득한 자의 경우 3년
나. 기사 자격 소지자 또는 석사 학위를 취득한 자의 경우 2년
다. 산업기사 자격 소지자 또는 학사 학위를 취득한 자의 경우 1년

o 다음 각 목의 어느 하나에 해당하는 자격을 취득한 자는 정보통신 또는 정보보호 유관경력 1년을 추가 인정한다.
가. 한국인터넷진흥원 정보보호전문가(SIS)
나. 전자정부법 제60조에 따른 감리원
다. 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 정보시스템감사사(CISA)
라. 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 정보시스템보호전문가(CISSP)

<비 고>
1. "정보통신 유관경력", "정보보호 유관경력", "유관자격" 및 "유관학력"은 영 별표 2 "정보보호 기술인력의 자격 기준"을 준용한다.

[별표 4]

정보보호 관리체계 인증의 표시(제25조 관련)

□ 출입구 부착용

1. 도안모형



2. 인증명판 제작 유의사항

가. 소재는 가급적 동판으로 제작한다(전체 두께 1.0㎝, 바탕 0.4㎝, 테두리 폭 0.5㎝)

나. 바탕색은 가급적 연마하지 않은 황동색으로 한다

다. 도안 모형은 인증의 표시를 중앙에 둔다

라. 글씨 및 도형은 양각으로 한다.

마. 크기는 사각형으로 하며 인증마크는 중앙에 위치하도록 하며 가로와 세로 비율을 3 : 2로 하여 일정 비율로 조정할 수 있다

□ 서류 및 제품 등 표시용

1. 도안모형



2. 도안 및 표시방법

가. 'Information Security Management System'은 검청색으로, '정보보호 관리체계 인증'은 군청색으로 한다. 게시장소의 칼라표시가 불합리한 경우에는 흑백으로 할 수 있다.

나. 마크의 크기는 제품과 그 제품의 포장 또는 용기의 크기에 따라 일정 비율로 조정할 수 있다.

[별표 5]

정보보호 관리체계 인증 수수료 산정기준(제26조 관련)

1. 인증 수수료 산정 방식

인증 수수료 = 직접인건비 + 직접경비 + 제경비 + 기술료

① 직접인건비는 인증심사에 투입되는 인증심사원에 대한 인건비로 산정한다. 인건비는 SW사업 대가 산정 가이드의 정보보안 컨설팅비를 준용한다

인증심사원 등급	컨설턴트 등급
선임심사원	선임 컨설턴트 이상
심사원	
심사원보	컨설턴트

② 직접경비는 인증심사업무의 수행에 따라 발생하는 교통비, 숙박비 및 식대 등 인증심사업무에 소요되는 직접적인 경비를 산정한다.

③ 제경비는 최대 (직접인건비×120%) 로 산정한다.

④ 기술료는 최대 {(직접인건비+제경비)×40% } 로 산정한다.

[별표 6]

정보보호 관리체계 인증기준(제18조 관련)

가. 정보보호관리과정 요구사항

	관리과정		세부관리과정	관리과정 상세내용
1	정보보호정책 수립 및 범위설정	1.1	정보보호정책의 수립	조직이 수행하는 모든 정보보호 활동의 근거를 포함할 수 있도록 정보보호정책을 수립하고 동 정책은 국가나 관련 산업에서 정하는 정보보호 관련 법, 규제를 만족하여야 한다.
		1.2	범위설정	조직에 미치는 영향을 고려하여 중요한 업무, 서비스, 조직, 자산 등을 포함할 수 있도록 정보보호 관리체계 범위를 설정하고 범위 내 모든 자산을 식별하여 문서화하여야 한다.
2	경영진 책임 및 조직구성	2.1	경영진 참여	정보보호 관리체계 수립 및 운영 등 조직이 수행하는 정보보호 활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여야 한다.
		2.2	정보보호 조직 구성 및 자원 할당	최고경영자는 조직의 규모, 업무 중요도 분석을 통해 정보보호 관리체계의 지속적인 운영이 가능하도록 정보보호 최고책임자, 실무조직 등 정보보호 조직을 구성하고 정보보호 관리체계 운영 활동을 수행하는데 필요한 자원(예산 및 인력)을 확보하여야 한다.
3	위험관리	3.1	위험관리 방법 및 계획 수립	관리적, 기술적, 물리적, 법적 분야 등 조직의 정보보호 전 영역에 대한 위험식별 및 평가가 가능하도록 위험관리 방법을 선정하고 위험관리의 전문성을 보장할 수 있도록 수행인원, 기간, 대상, 방법 등을 구체적으로 포함한 위험관리계획을 사전에 수립하여야 한다.
		3.2	위험식별 및 평가	위험관리 방법 및 계획에 따라 정보보호 전 영역에 대한 위험 식별 및 평가를 연 1회 이상 수행하고 그 결과에 따라 조직에서 수용 가능한 위험수준을 설정하여 관리하여야 한다.

	관리과정		세부관리과정	관리과정 상세내용
3	위험관리	3.3	정보보호대책 선정 및 이행계획 수립	위험을 수용 가능한 수준으로 감소시키기 위해 정보보호대책을 선정하고 그 보호대책의 구현 우선순위, 일정, 담당부서 및 담당자 지정, 예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.
4	정보보호대책 구현	4.1	정보보호대책의 효과적 구현	정보보호대책 이행계획에 따라 보호대책을 구현하고 경영진은 이행결과의 정확성 및 효과성 여부를 확인하여야 한다.
		4.2	내부 공유 및 교육	구현된 정보보호대책을 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여야 한다.
5	사후관리	5.1	법적요구사항 준수검토	조직이 준수해야 할 정보보호 관련 법적요구사항을 지속적으로 파악하여 최신성을 유지하고 준수여부를 지속적으로 검토하여야 한다.
		5.2	정보보호 관리체계 운영현황 관리	정보보호 관리체계 범위 내에서 주기적 또는 상시적으로 수행해야 하는 활동을 문서화하고 그 운영현황을 지속적으로 관리하여야 한다.
		5.3	내부감사	조직은 정보보호 관리체계가 정해진 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는 지를 점검하기 위하여 연 1회 이상 내부감사를 수행하여야 한다. 이를 위해 감사 기준, 범위, 주기, 방법 등을 구체적으로 정하고 내부감사를 통해 발견된 문제점은 보완조치를 완료하여 경영진 및 관련 책임자에게 보고하여야 한다. 또한 감사의 독립성 및 전문성을 확보할 수 있도록 감사인력에 대한 자격요건을 정의하여야 한다.

나. 정보보호대책

	통제분야		통제목적		통제사항	통제내용
1	정보보호 정책	1.1	정책의 승인 및 공표	1.1.1	정책의 승인	정보보호정책은 이해관련자의 검토와 최고경영자의 승인을 받아야 한다.
				1.1.2	정책의 공표	정보보호정책 문서는 모든 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.
		1.2	정책의 체계	1.2.1	상위 정책과의 연계성	정보보호정책은 상위조직 및 관련 기관의 정책과 연계성을 유지하여야 한다.
				1.2.2	정책시행 문서수립	정보보호정책의 구체적인 시행을 위한 정보보호지침, 절차를 수립하고 관련 문서간의 일관성을 유지하여야 한다.
		1.3	정책의 유지관리	1.3.1	정책의 검토	정기적으로 정보보호정책 및 정책 시행문서의 타당성을 검토하고, 중대한 보안사고 발생, 새로운 위협 또는 취약성의 발견, 정보보호 환경에 중대한 변화 등이 정보보호정책에 미치는 영향을 분석하여 필요한 경우 제·개정하여야 한다.
				1.3.2	정책문서 관리	정보보호정책 및 정책 시행문서의 이력관리를 위해 제정, 개정, 배포, 폐기 등의 관리절차를 수립하고 문서는 최신본으로 유지하여야 한다. 또한 정책문서 시행에 따른 운영기록을 생성하여 유지하여야 한다.
2	정보보호 조직	2.1	조직 체계	2.1.1	정보보호 최고 책임자 지정	최고경영자는 임원급의 정보보호 최고책임자를 지정하고 정보보호 최고책임자는 정보보호정책 수립, 정보보호 조직 구성, 위험관리, 정보보호위원회 운영 등의 정보보호에 관한 업무를 총괄 관리하여야 한다.

	통제분야		통제목적		통제사항	통제내용
2	정보보호 조직	2.1	조직의 체계	2.1.2	실무조직 구성	최고경영자는 정보보호 최고책임자의 역할을 지원하고 조직의 정보보호 활동을 체계적으로 이행하기 위해 실무조직을 구성하고 조직 구성원의 정보보호 전문성을 고려하여 구성한다.
				2.1.3	정보보호 위원회	정보보호 자원할당 등 조직 전반에 걸친 중요한 정보보호 관련사항에 대한 검토 및 의사결정을 할 수 있도록 정보보호위원회를 구성하여 운영하여야 한다.
		2.2	역할 및 책임	2.2.1	역할 및 책임	정보보호 최고책임자와 정보보호 관련 담당자에 대한 역할 및 책임을 정의하고 그 활동을 평가할 수 있는 체계를 마련하여야 한다.
3	외부자 보안	3.1	보안 요구사항 정의	3.1.1	외부자 계약 시 보안요구사항	조직의 정보처리 업무를 외부자에게 위탁하거나 정보자산에 대한 접근을 허용할 경우, 또는 업무를 위해 클라우드 서비스 등 외부 서비스를 이용하는 경우에는 보안요구사항을 식별하고 관련 내용을 계약서 및 협정서 등에 명시하여야 한다.
		3.2	외부자 보안 이행	3.2.1	외부자 보안 이행 관리	외부자가 계약서 및 협정서에 명시된 보안요구사항의 이행여부를 관리 감독하고 주기적인 점검 또는 감사를 수행하여야 한다.
				3.2.2	외부자 계약 만료 시 보안	외부자와의 계약 만료, 업무 종료, 담당자 변경 시 조직이 외부자에게 제공한 정보자산의 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 업무 수행 시 알게 된 정보의 비밀유지 확약서 등의 내용을 확인하여야 한다.

	통제분야		통제목적		통제사항	통제내용
4	정보자산 분류	4.1	정보자산 식별 및 책임	4.1.1	정보자산 식별	조직의 업무특성에 따라 정보자산 분류기준을 수립하고 정보보호 관리체계 범위 내 모든 정보자산을 식별하여야 한다. 또한 식별된 정보자산을 목록으로 관리하여야 한다.
				4.1.2	정보자산별 책임할당	식별된 정보자산에 대한 책임자 및 관리자를 지정하여 책임소재를 명확히 하여야 한다.
		4.2	정보자산의 분류 및 취급	4.2.1	보안등급과 취급	기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 정보자산이 조직에 미치는 중요도를 평가하고 그 중요도에 따라 보안등급을 부여하여야 한다. 또한 보안등급을 표시하고 등급 부여에 따른 취급절차를 정의하여 이행하여야 한다.
5	정보보호 교육	5.1	교육 프로그램 수립	5.1.1	교육 계획	교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 정보보호 교육 계획을 수립하여야 한다.
				5.1.2	교육 대상	교육 대상에는 정보보호 관리체계 범위 내 임직원 및 외부자를 모두 포함하여야 한다.
				5.1.3	교육 내용 및 방법	교육에는 정보보호 및 정보보호 관리체계 개요, 보안사고 사례, 내부 규정 및 절차, 법적 책임 등의 내용을 포함하고 일반 임직원, 책임자, IT 및 정보보호 담당자 등 각 직무별 전문성 제고에 적합한 교육내용 및 방법을 정하여야 한다.
		5.2	교육 시행 및 평가	5.2.1	교육 시행 및 평가	정보보호 관리체계 범위 내 임직원 및 외부자를 대상으로 연 1회 이상 교육을 시행하고 정보보호 정책 및 절차의 중대한 변경, 조직 내·외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생할 경우 추가 교육을 수행하여야 한다. 또한 교육 시행에 대한 기록을 남기고 평가하여야 한다.

	통제분야		통제목적		통제사항	통제내용
6	인적 보안	6.1	정보보호 책임	6.1.1	주요 직무자 지정 및 감독	인사정보, 영업비밀, 산업기밀, 개인정보 등 중요정보를 대량으로 취급하는 임직원의 경우 주요직무자로 지정하고 주요직무자 지정을 최소화 하는 등 관리할 수 있는 보호대책을 수립하여야 한다.
				6.1.2	직무 분리	권한 오남용 등 고의적인 행위로 인해 발생할 수 있는 잠재적인 피해를 줄이기 위하여 직무 분리 기준을 수립하고 적용하여야 한다. 다만 인적 자원 부족 등 불가피하게 직무분리가 어려운 경우 별도의 보완통제를 마련하여야 한다.
				6.1.3	비밀유지 서약서	임직원으로부터 비밀유지 서약서를 받아야 하고 임시직원이나 외부자에게 정보시스템에 대한 접근권한을 부여할 경우에도 비밀유지서약서를 받아야 한다.
		6.2	인사규정	6.2.1	퇴직 및 직무변경 관리	퇴직 및 직무변경 시 인사부서와 정보보호 및 시스템 운영 부서 등 관련 부서에서 이행해야 할 자산반납, 접근권한 회수·조정, 결과 확인 등의 절차를 수립하여야 한다.
				6.2.2	상벌규정	인사규정에 직원이 정보보호 책임과 의무를 충실히 이행했는지 여부 등 정보보호 활동 수행에 따른 상벌 규정을 포함하여야 한다.

	통제분야		통제목적		통제사항	통제내용
7	물리적 보안	7.1	물리적 보호구역	7.1.1	보호구역 지정	비인가자의 물리적 접근 및 각종 물리적, 환경적 재난으로부터 주요 설비 및 시스템을 보호하기 위하여 통제구역, 제한구역, 접견구역 등 물리적 보호구역을 지정하고 각 구역별 보호대책을 수립·이행하여야 한다.
				7.1.2	보호설비	각 보호구역의 중요도 및 특성에 따라 화재, 전력이상 등 인·재해에 대비하여 온습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 설비를 충분히 갖추고 운영절차를 수립하여 운영하여야 한다. 또한 주요 시스템을 외부 집적정보통신시설에 위탁운영하는 경우 관련 요구사항을 계약서에 반영하고 주기적으로 검토를 수행하여야 한다.
				7.1.3	보호구역 내 작업	유지보수 등 주요 설비 및 시스템이 위치한 보호구역 내에서의 작업 절차를 수립하고 작업에 대한 기록을 주기적으로 검토하여야 한다.
				7.1.4	출입통제	보호구역 및 보호구역 내 주요 설비 및 시스템은 인가된 사람만이 접근할 수 있도록 출입을 통제하고 책임추적성을 확보할 수 있도록 출입 및 접근 이력을 주기적으로 검토하여야 한다.
				7.1.5	모바일 기기 반출입	노트북 등 모바일 기기 미승인 반출입을 통한 중요정보 유출, 내부망 악성코드 감염 등의 보안사고 예방을 위하여 보호구역 내 임직원 및 외부자 모바일 기기 반출입 통제절차를 수립하고 기록·관리하여야 한다.
		7.2	시스템 보호	7.2.1	케이블 보안	데이터를 송수신하는 통신케이블이나 전력을 공급하는 전력 케이블은 손상을 입지 않도록 보호하여야 한다.
				7.2.2	시스템 배치 및 관리	시스템은 그 특성에 따라 분리하여 배치하고 장애 또는 보안사고 발생 시 주요 시스템의 위치를 즉시 확인할 수 있는 체계를 수립하여야 한다.

	통제분야		통제목적		통제사항	통제내용
		7.3	사무실 보안	7.3.1	개인업무 환경 보안	일정시간 동안 자리를 비울 경우에는 책상 위에 중요한 문서나 저장매체를 남겨놓지 않고 컴퓨터 화면에 중요정보가 노출되지 않도록 화면보호기 설정, 패스워드 노출 금지 등 보호대책을 수립하여야 한다.
				7.3.2	공용업무 환경 보안	사무실에서 공용으로 사용하는 사무처리 기기, 문서고, 공용 PC, 파일서버 등을 통해 중요정보 유출이 발생하지 않도록 보호대책을 마련하여야 한다.
8	시스템 개발보안	8.1	분석 및 설계 보안관리	8.1.1	보안 요구사항 정의	신규 정보시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안취약점, 정보보호 기본요소(기밀성, 무결성, 가용성) 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용하여야 한다.
				8.1.2	인증 및 암호화 기능	정보시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입·출력 및 송수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다.
				8.1.3	보안로그 기능	정보시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 하여야 한다.
				8.1.4	접근권한 기능	정보시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다.

	통제분야		통제목적		통제사항	통제내용
8	시스템 개발 보안	8.2	구현 및 이관 보안	8.2.1	구현 및 시험	안전한 코딩방법에 따라 정보시스템을 구현 하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다. 또한 알려진 기술적 보안 취약성에 대한 노출여부를 점검하고 이에 대한 보안대책을 수립하여야 한다.
				8.2.2	개발과 운영 환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다.
				8.2.3	운영환경 이관	운영환경으로의 이관은 통제된 절차에 따라 이루어져야 하고 실행코드는 시험과 사용자 인수 후 실행하여야 한다.
				8.2.4	시험 데이터 보안	시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다.
				8.2.5	소스 프로그램 보안	소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행하여야 한다. 또한 소스 프로그램은 운영환경에 보관하지 않는 것을 원칙으로 한다.
		8.3	외주개발 보안	8.3.1	외주개발 보안	정보시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독하여야 한다.

	통제분야		통제목적		통제사항	통제내용
9	암호통제	9.1	암호 정책	9.1.1	암호 정책 수립	조직의 중요정보 보호를 위하여 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 수립하고 이행하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.
		9.2	암호키 관리	9.2.1	암호키 생성 및 이용	암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고 필요 시 복구방안을 마련하여야 한다.
10	접근 통제	10.1	접근통제 정책	10.1.1	접근통제 정책 수립	비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다.
		10.2	접근권한 관리	10.2.1	사용자 등록 및 권한부여	정보시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다.
				10.2.2	관리자 및 특수 권한 관리	정보시스템 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.
				10.2.3	접근권한 검토	정보시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 점검하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.3	사용자 인증 및 식별	10.3.1	사용자 인증	정보시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제되어야 하고, 필요한 경우 법적요구사항 등을 고려하여 중요 정보시스템 접근 시 강화된 인증방식을 적용하여야 한다.
				10.3.2	사용자 식별	정보시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다. 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.
				10.3.3	사용자 패스워드 관리	법적요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경주기 등 사용자 패스워드 관리절차를 수립·이행하고 패스워드 관리 책임이 사용자에게 있음을 주지시켜야 한다. 특히 관리자 패스워드는 별도 보호대책을 수립하여 관리하여야 한다.
				10.3.4	이용자 패스워드 관리	고객, 회원 등 외부 이용자가 접근하는 정보시스템 또는 웹서비스의 안전한 이용을 위하여 계정 및 패스워드 등의 관리절차를 마련하고 관련 내용을 공지하여야 한다.
		10.4	접근통제 영역	10.4.1	네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 접근통제 리스트, 네트워크 식별자 등에 대한 관리절차를 수립하고 서비스, 사용자 그룹, 정보자산의 중요도에 따라 내·외부 네트워크를 분리하여야 한다.
				10.4.2	서버 접근	서버별로 접근이 허용되는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 적용하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.4	접근통제 영역	10.4.3	응용 프로그램 접근	사용자의 업무 또는 직무에 따라 응용프로그램 접근권한을 제한하고 불필요한 중요정보 노출을 최소화해야 한다.
				10.4.4	데이터베이스 접근	데이터베이스 접근을 허용하는 응용프로그램 및 사용자 직무를 명확하게 정의하고 응용프로그램 및 직무별 접근통제 정책을 수립하여야 한다. 또한 중요정보를 저장하고 있는 데이터베이스의 경우 사용자 접근내역을 기록하고 접근의 타당성을 정기적으로 검토하여야 한다.
				10.4.5	모바일 기기 접근	모바일기기를 업무 목적으로 내·외부 네트워크에 연결하여 활용하는 경우 중요정보 유출 및 침해사고 예방을 위해 기기 인증 및 승인, 접근 범위, 기기 보안설정, 오남용 모니터링 등의 접근통제 대책을 수립하여야 한다.
				10.4.6	인터넷 접속	인사정보, 영업비밀, 산업기밀, 개인정보 등 중요정보를 대량으로 취급·운영하는 주요직무자의 경우 인터넷 접속 또는 서비스(P2P, 웹메일, 웹하드, 메신저 등)를 제한하고 인터넷 접속은 침입차단시스템을 통해 통제하여야 한다. 필요시 침입탐지시스템 등을 통해 인터넷 접속내역을 모니터링하여야 한다.
11	운영보안	11.1	운영 절차 및 변경 관리	11.1.1	운영절차 수립	정보시스템 동작, 문제 발생 시 재 동작 및 복구, 오류 및 예외사항 처리 등 시스템 운영을 위한 절차를 수립하여야 한다.
				11.1.2	변경관리	정보시스템 관련 자산의 모든 변경내역을 관리할 수 있도록 절차를 수립하고 변경 전 시스템의 전반적인 성능 및 보안에 미치는 영향을 분석하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영보안	11.2	시스템 및 서비스 운영 보안	11.2.1	정보 시스템 인수	새로운 정보시스템 도입 또는 개선 시 필수 보안요구사항을 포함한 인수 기준을 수립하고 인수 전 기준 적합성을 검토하여야 한다.
				11.2.2	보안 시스템 운영	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립하고 보안시스템 별 정책적용 현황을 관리하여야 한다.
				11.2.3	성능 및 용량관리	정보시스템 및 서비스 가용성 보장을 위해 성능 및 용량 요구사항을 정의하고 현황을 지속적으로 모니터링할 수 있는 방법 및 절차를 수립하여야 한다.
				11.2.4	장애관리	정보시스템 장애 발생 시 효과적으로 대응하기 위한 탐지, 기록, 분석, 복구, 보고 등의 절차를 수립하여야 한다.
				11.2.5	원격운영 관리	내부 네트워크를 통하여 정보시스템을 관리하는 경우 특정 단말에서만 접근을 할 수 있도록 제한하고, 원격지에서 인터넷 등 외부 네트워크를 통하여 정보시스템을 관리하는 것은 원칙적으로 금지하고 부득이한 사유로 인해 허용하는 경우에는 책임자 승인, 접속 단말 및 사용자 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등의 보호대책을 수립하여야 한다.
				11.2.6	스마트 워크 보안	재택근무, 원격협업 등과 같은 원격 업무 수행 시 이에 대한 관리적·기술적 보호대책을 수립하고 이행하여야 한다.
				11.2.7	무선네트워크 보안	무선랜 등을 통해 무선인터넷을 사용하는 경우 무선 네트워크 구간에 대한 보안을 강화하기 위해 사용자 인증, 송수신 데이터 암호화 등의 보호대책을 수립하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영보안			11.2.8	공개서버 보안	웹사이트 등에 정보를 공개하는 경우 정보 수집, 저장, 공개에 따른 허가 및 게시절차를 수립하고 공개서버에 대한 물리적, 기술적 보호대책을 수립하여야 한다.
				11.2.9	백업관리	데이터의 무결성 및 정보시스템의 가용성을 유지하기 위해 백업 대상, 주기, 방법 등의 절차를 수립하고 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다.
				11.2.10	취약점 점검	정보시스템이 알려진 취약점에 노출되어 있는 지 여부를 확인하기 위하여 정기적으로 기술적 취약점 점검을 수행하고 발견된 취약점들은 조치하여야 한다.
		11.3	전자거래 및 정보전송 보안	11.3.1	전자거래 보안	전자거래 서비스 제공 시 정보유출, 데이터 조작, 사기 등의 침해사고를 예방하기 위해 사용자 인증, 암호화, 부인방지 등의 보호대책을 수립하고 결제시스템 등 외부 시스템과의 연계가 필요한 경우 연계 안전성을 점검하여야 한다.
				11.3.2	정보전송 정책 수립 및 협약 체결	타 조직에 중요정보를 전송할 경우 안전한 전송을 위한 정책을 수립하고 조직 간 정보전송 합의를 통해 관리 책임, 전송 기술 표준, 중요정보의 보호를 위한 기술적 보호조치 등을 포함한 협약서를 작성하여야 한다.
		11.4	매체 보안	11.4.1	정보 시스템 저장매체 관리	정보시스템 폐기 또는 재사용 시 중요정보를 담고 있는 하드디스크, 스토리지, 테잎 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제하여야 한다.
				11.4.2	휴대용 저장매체 관리	조직의 중요정보 유출을 예방하기 위해 외장하드, USB, CD 등 휴대용 저장매체 취급, 보관, 폐기, 재사용에 대한 절차를 수립하여야 한다. 또한 매체를 통한 악성코드 감염 방지 대책을 마련하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영보안	11.5	악성코드 관리	11.5.1	악성코드 통제	바이러스, 웜, 트로이목마 등의 악성코드로부터 정보시스템을 보호하기 위해 악성코드 예방, 탐지, 대응 등의 보호대책을 수립하여야 한다.
				11.5.2	패치관리	소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인해 발생할 수 있는 침해사고를 예방하기 위해 최신 패치를 정기적으로 적용하고 필요한 경우 시스템에 미치는 영향을 분석하여야 한다.
		11.6	로그관리 및 모니터링	11.6.1	시각 동기화	로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 정보시스템 시각을 공식 표준시각으로 정확하게 동기화 하여야 한다.
				11.6.2	로그 기록 및 보존	정보시스템, 응용프로그램, 보안시스템, 네트워크 장비 등 기록해야 할 로그 유형을 정의하여 일정기간 보존하고 주기적으로 검토하여야 한다. 보존기간 및 검토주기는 법적요구사항을 고려하여야 한다.
				11.6.3	접근 및 사용 모니터링	중요정보, 정보시스템, 응용프로그램, 네트워크 장비에 대한 사용자 접근이 업무상 허용된 범위에 있는 지 주기적으로 확인하여야 한다.
				11.6.4	침해시도 모니터링	외부로부터의 침해시도를 모니터링하기 위한 체계 및 절차를 수립하여야 한다.
12	침해사고 관리	12.1	절차 및 체계	12.1.1	침해사고 대응절차 수립	DDoS 등 침해사고 유형별 중요도 분류, 유형별 보고·대응·복구 절차, 비상연락체계, 훈련 시나리오 등을 포함한 침해사고 대응 절차를 수립하여야 한다.
				12.1.2	침해사고 대응체계 구축	침해사고 대응이 신속하게 이루어질 수 있도록 중앙 집중적인 대응체계를 구축하고 외부기관 및 전문가들과의 협조체계를 수립하여야 한다.
		12.2	대응 및 복구	12.2.1	침해사고 훈련	침해사고 대응 절차를 임직원들이 숙지할 수 있도록 시나리오에 따른 모의훈련을 실시하여야 한다.

	통제분야		통제목적		통제사항	통제내용
12	침해사고 관리	12.2	대응 및 복구	12.2.2	침해사고 보고	침해사고 징후 또는 사고 발생을 인지한 때에는 침해사고 유형별 보고 절차에 따라 신속히 보고하고 법적 통지 및 신고 의무를 준수하여야 한다.
				12.2.3	침해사고 처리 및 복구	침해사고 대응절차에 따라 처리와 복구를 신속하게 수행하여야 한다.
		12.3	사후관리	12.3.1	침해사고 분석 및 공유	침해사고가 처리되고 종결된 후 이에 대한 분석을 수행하고 그 결과를 보고하여야 한다. 또한 사고에 대한 정보와 발견된 취약점들을 관련 조직 및 임직원들과 공유하여야 한다.
				12.3.2	재발방지	침해사고로부터 얻은 정보를 활용하여, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하고 이를 위해 필요한 경우 정책, 절차, 조직 등의 대응체계를 변경하여야 한다.
13	IT 재해복구	13.1	체계 구축	13.1.1	IT 재해복구 체계 구축	자연재앙, 해킹, 통신장애, 전력중단 등의 요인으로 인해 IT 시스템 중단 또는 파손 등 피해가 발생할 경우를 대비하여 비상 시 복구조직, 비상연락체계, 복구절차 등 IT 재해복구 체계를 구축하여야 한다.
		13.2	대책 구현	13.2.1	영향분석에 따른 복구대책 수립	조직의 핵심 서비스 연속성을 위협할 수 있는 IT 재해 유형을 식별하고 유형별 예상 피해규모 및 영향을 분석하여야 한다. 또한 IT 서비스 및 시스템 복구목표시간, 복구시점을 정의하고 적절한 복구전략 및 대책을 수립·이행하여야 한다.
				13.2.2	시험 및 유지관리	IT 서비스 복구전략 및 대책에 따라 효과적인 복구가 가능한 지 시험을 실시하고 시험계획에는 시나리오, 일정, 방법, 절차 등을 포함하여야 한다. 또한 시험결과, IT 환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완하여야 한다.

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제1호서식] <개정 2013.8.8>

정보보호 관리체계 인증기관 지정 신청서

* 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	처리기간	3개월이내

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	총 직원 수	인증심사원 직원 수	
신청구분	☐ 신규	☐ 재지정	
인증에 관한 업무의 범위			

「정보보호 관리체계 인증 등에 관한 고시」 제3조제2항의 규정에 따라 위와 같이 정보보호 관리체계 인증기관 지정을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

미래창조과학부 귀중

신청인 제출서류	1. 정관 또는 규약 1부. 2. 별지 제2호서식의 인증심사원의 보유현황과 이를 증명할 수 있는 서류 1부. 3. 별표 1에 따른 업무수행 요건·능력 심사를 위하여 필요한 서류 1부.	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

처 리 절 차

신청서 작성	→	접 수	→	심 사	→	지정여부 결정	→	지정서 교부
신청인		처리기관 (미래창조과학부)		처리기관 (미래창조과학부)		처리기관 (미래창조과학부)		처리기관 (미래창조과학부)

210mm×297mm[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제2호서식] <개정 2013.8.8>

인증심사원의 보유현황

(제1쪽)

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	직원 수	인증심사원 직원 수	

일련번호	성명	주소		최종학력	해당요건
		생년월일	입사일	취득학위 및 학과	

유의사항

1. 「해당요건」란에는 선임심사원, 심사원, 심사원보 요건을 기재한다.
2. 기재된 최종학위를 증명할 수 있는 직원의 졸업 또는 학위증명서 사본을 제출하여야 한다.
3. 별표 3의 「인증 심사원 학력 및 경력 요건」을 충족하는 직원은 기술자격증 사본 등 자격을 취득하였음을 확인할 수 있는 서류를 함께 제출하여야 한다.
4. 정보통신유관경력 또는 정보보호유관경력을 증명할 수 있는 경력증명서(근무부서 또는 담당업무 등이 기재되어야 한다)와 해당 직원이 신청업체에 현재 근무하고 있음을 확인할 수 있는 재직증명서를 함께 제출하여야 한다.

210㎜×297㎜[백상지(80g/㎡)]

인증심사업무를 전담하는 직원의 보유현황

(제2쪽)

일련번호	성명	주소		최종학력	해당요건
		생년월일	입사일	취득학위 및 학과	

10㎜×297㎜[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제3호서식] <개정 2013.8.8> (제1쪽)

정보보호 관리체계 인증기관 지정서

등록번호 :

업체명 :

대표자 :

주소 :

지정의 유효기간 :

인증업무의 범위 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제5항 및 같은 법 시행령 제53조의2에 따라 위와 같이 정보보호 관리체계 인증기관으로 지정합니다.

년 월 일

미래창조과학부장관 직인

210mm×297mm[백상지(120g/㎡)]

(제2쪽)

CERTIFICATE OF DESIGNATION
AS
ISMS Certification Authority

Registry Number :

Name of Organization :

Name of Representative :

Address :

Period of Validity :

Scope of Certification work :

This is to certify that the abovementioned organization is designated Information Security Management System (ISMS) Certification Authority in accordance with Article 47, Paragraph 5 of 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」 and Article 53-2 of the Enforcement Decree of the same Act.

Date of Issuance:

Signed by the
Minister of Ministry of Science, ICT and Future Planning
Republic of Korea

210㎜×297㎜[백상지 120g/㎡]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제4호서식] <개정 2013.8.8>

인증실적 보고서

정보보호 관리체계 인증기관	업체명		사업자등록번호	
	주소		전화번호	
	대표자			
	정보보호 관리체계 인증심사 실적 총계	최초심사	외	건
		사후관리심사	외	건

일련 번호	인증 번호	대상기관(기업)명	인증범위	유효기간	구분	
					최초심사	사후관리 심사

년 월 일

신청인(대표자) (서명 또는 인)

미래창조과학부 귀중

신청(신고)인 제출서류	1. 정보보호 관리체계 인증기관 지정서 1부.	수수료 없음

처 리 절 차

신청서 작성	→	접 수	→	검 토	→	심 사	→	자정서 교부
신청인		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)

210mm×297mm[백상지(80g/㎡)]

■「정보보호 관리체계 인증 등에 관한 고시」 [별지 제5호서식] <개정 2013.8.8> (제1쪽)

정보보호 관리체계 인증심사원 자격 신청서

신청자 인적사항	성 명		생년월일		사진	
	주 소	(우: -)				
	회 사 명					
	회사주소	(우: -)				
	이 메 일					
	전화번호		휴대전화			
신청사항	신청 구분	□ 자격인증 □ 전문분야 변경				
학력사항	최종학력	□ 고졸	□ 전문학사	□ 학사	□ 석사	□ 박사
	학사	전공		기간		
	석사	전공		기간		
	박사	전공		기간		
인증심사원 교육이수	교육기간	년 월 일 ~ 년 월 일		수료증번호		

자격사항 ※해당자에 한함	자격증번호	자격증명/등급	취득일자	수여기관

경력사항 ※최근 10년 내 경력사항 기술	총 경력	정보기술	총 년 개월	정보보호	총 년 개월

No.	구분	기간	회사명	부서	직책
1	□정보기술 □정보보호	~ (년 개월)			
2	□정보기술 □정보보호	~ (년 개월)			
3	□정보기술 □정보보호	~ (년 개월)			
4	□정보기술 □정보보호	~ (년 개월)			
5	□정보기술 □정보보호	~ (년 개월)			

※ 칸이 부족할 경우 추가 작성

(제2쪽)

(1) 개인별 전문분야 (복수 선택 가능, 우선순위 표기요망)					
대분류	중분류	소분류	순위	실무경력	
관리적 정보 보호	정책, 조직 및 인적보안	정보보호정책수립 및 조직구성			년
		인적보안, 외부자 보안, 외부위탁관리			년
		정보보호교육 및 훈련			년
		국내외 표준 기준 및 법령			년
	위험관리	자산분류, 위험평가 수행, 대책 및 계획수립			년
	업무연속성관리	업무연속성 계획수립 및 시험, 유지관리			년
	침해사고대응	침해사고 대응계획 및 체계, 복구			년
	정보시스템 감사/감리	정보시스템 및 정보보호시스템 감사/감리			년
기술적 정보 보호	네트워크	네트워크 설계기술			년
		라우팅 제어, 프로토콜 제어, 접근통제, 암호화, NAT, 운용관리(로그, SNMP, 설정도구)등 통신기술			년
		라우터, 스위치(L2~L7), RAS, VPN, SSL, DHCP, 네트워크 감시 등 기기기술			년
		기타( )			년
	운영체제 및 시스템	OS 기본지식, 계정관리, 접근권한, 서비스관리, 로그관리, 패치, 보안 S/W 사용 등 유닉스/리눅스 시스템			년
		OS 기본지식, 계정관리, 접근권한, 서비스관리, 로그관리, 패치, 보안 S/W 사용 등 윈도우 시스템			년
		메인프레임 등 기타( )			년
	응용서비스	HTTP 프로토콜, 브라우저, SQL-Injection 등 Web 위협에 대한 대응책, SSL, CGI 보안 프로그래밍 등 Web 서비스			년
		부하분산, DNSSEC, 보안설정 등 DNS 서비스			년
		메일 프로토콜, 스팸대응, 웜/바이러스 필터링 등 메일 서비스			년
		DB 기본지식, 이중화, 데이터백업, 암호화 등 데이터베이스			년
		ERP, KMS, CRM 등 사내정보시스템			년
		분산시스템 등 기타( )			년
	정보보호 솔루션	FW 기본지식, 접근통제, 라우팅, 네트워크 정책설계, 구성(이중화, 망분리, 로드밸런싱 등) 등 침입차단시스템			년
		웜/바이러스 기본지식, 웜/바이러스별 감염 증상과 대책 등 바이러스 월			년
		IDS 기본지식, 방화벽 연동, 패턴 매칭 방법, 구성(에이전트 위치, 통합콘솔 등) 등 침입탐지시스템			년
		SecureOS 기본지식, 계정관리, 접근권한, 서비스관리, 로그관리, 패치 등 SecureOS			년
		기타( )			년

(제3쪽)

(1) 개인별 전문분야 (복수 선택 가능, 우선순위 표기요망) (계속)					
대분류	중분류	소분류	순위	실무경력	
기술적 정보 보호 (계속)	취약성분석	사회공학적 방법, 스캔, Sniffing, DOS, Buffer Overflow, 웜/바이러스, 백도어 등 취약성 분석 및 점검			년
	보안 운영	통합관제(ESM, NMS 등), 망관리, 백업, 로그 분석, 모니터링, 패치, 문제해결(원인규명)			년
	기반기술	IPSec, PPTP, L2TP, SSH, SSL/TLS, MPLS, IKE, S/MIME, PGP 등 보안 프로토콜			년
		패스워드인증, 생체인증, 인증디바이스, 인증프로토콜, WEB인증, RADIUS, SSO 등 인증기술			년
		증명서 인증 및 실효, 신뢰모델, 기술 및 데이터방식, 인증센터 구축과 운영, 법적구조 등 PKI			년
		암호알고리즘, Key 관리, 암호방식 등 암호기술			년
		디지털서명, 디지털 봉투, 코드 서명			년
물리적 정보 보호	접근보안	출입 및 접근통제, 모니터링 등			년
	시설관리	소방시설, 비상전원, 비상조명, 항온항습 등			년
개인정보보호		개인정보보호 책임자, 취급자, 컨설턴트, 법률 담당, 소비자 민원 및 상담 등			년
기타		( )			년

※ 경력 및 전문 분야에 대한 관련 내용을 상세히 기술
※ 칸이 부족할 경우 별지 사용

No.	상세내용
1	
2	
3	
4	
5	
6	

(제4쪽)

(2) 통제분야별 전문분야 (5순위까지 선택, 우선순위 표기요망)							
통제분야	순위	실무경력		통제분야	순위	실무경력	
1. 정보보호정책			년	9. 암호통제			년
2. 정보보호조직			년	10. 접근통제			년
3. 외부자 보안			년	11. 운영관리			년
4. 정보자산분류			년	12. 전자거래보안			년
5. 정보보호교육 및 훈련			년	13. 보안사고관리			년
6. 인적 보안			년	14. 검토, 모니터링 및 감사			년
7. 물리적 보안			년	15. 업무연속성 관리			년
8. 시스템개발 보안			년	16. 개인정보보호			년
관련 경력기술							
※ 5순위까지 선택한 전문분야 관련 실무경력, 전문기술, 인증심사실적 등 관련경력을 상세히 기술							

<개인정보 수집·이용>

- 개인정보 수집 이용 목적 : 정보보호 관리체계(ISMS) 인증심사원 양성 교육, 자격부여 및 관리, 자문료 지급, 심사팀구성
- 수집하는 개인정보 항목 : 성명, 생년월일, 주소, 이메일, 전화번호, 학력, 자격경력, 발령사항, 기술실적사항
- 보유 및 이용기간 : 인증심사원 자격 종료시까지
- 개인정보의 수집·이용을 거부할 수 있으며, 이 경우 인증심사원 등록 및 위촉에 불이익이 발생할 수 있음을 알려드립니다.

▷ **개인정보 수집·이용 동의여부** 동의 □ 미동의 □

<인증심사원 의무사항>

- 인증심사원은 객관적이고 공정한 인증심사를 수행한다.
- 인증심사원으로서의 성실한 직무수행 및 품위유지를 한다.
- 인증심사와 관련된 부당한 금전, 금품 등의 수수를 금지한다.
- 인증심사의 수행에서 취득한 정보를 관련 법령 또는 신청기관의 동의 없이 외부에 누설하여서는 안된다.
- 인증심사원은 인증업무지침을 성실히 준수한다.
- 인증심사원은 본인이 ISMS 인증 취득을 위한 컨설팅을 수행한 기업에 대하여는 인증심사에 참여할 수 없다.
- 인증심사원은 인증심사의 수행과 관련하여 상업적, 재정적 그리고 기타 모든 압력으로부터 배제되어야 한다.

1. 위의 인증심사원 의무사항을 읽고 이해하였으며, 성실히 준수하겠습니다.
2. 본 신청서의 기재사항은 사실과 틀림없으며, 만약 허위로 판명될 경우에는 자격취소 등 불이익을 감수하겠습니다.

※ 필요시 학력, 경력 등 증빙서류 제출을 요청받을 수 있으며 반드시 이에 응해야 함

위와 같이 인증심사원 자격을 신청합니다.

년 월 일

신청자		(서명 또는 인)

한국인터넷진흥원 귀중

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제6호서식] <개정 2013.8.8>

경력증명서

인적사항	성명		생년월일	
	주소		연락처	

경력사항	전 근무처 명				
	근무기간		부서	직위	담당업무
	부터	까지			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			

근무년수	년 개월	최종직위	
용도	정보보호 관리체계 인증심사원 자격 신청		

위와 같이 경력을 증명합니다.

년 월 일

회사명

대표자 (서명 또는 인)

확인자	성명	부서	연락처	비고

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제7호서식] <개정 2013.8.8>

상세 재직증명서

인적사항	성명		생년월일	
	주소		연락처	
소속사항	회사명			
	부서		직위	
	근속기간	~	근무년수	년 개월

발령사항	근무기간		부서	직위	담당업무
	부터	까지			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			

용도	정보보호 관리체계 인증심사원 자격 신청

위와 같이 재직하고 있음을 증명합니다.

년 월 일

회사명

대표자 (서명 또는 인)

확인자	성명	부서	연락처	비고

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제8호서식] <개정 2013.8.8>

기술실적증명서

인적사항	성명		생년월일	
	주소		연락처	

실적사항	소속				
	수행기간		참여사업명	발주처	담당업무
	부터	까지			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			

용도	정보보호 관리체계 인증심사원 자격 신청

위와 같이 기술실적을 증명합니다.

년 월 일

회사명

대표자 (서명 또는 인)

확인자	성명	부서	연락처	비고

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제9호서식] <개정 2013.8.8>

제 호

인증심사원 자격 증명서

성 명 : (. . .)

인증심사원 등급 :

유효기간 :

※ 인증심사원 유지조건을 만족하지 못할 경우 자격이 취소될 수 있습니다.

귀하에게 정보보호 관리체계 인증심사원 자격을 부여합니다.

년 월 일

한국인터넷진흥원 원장 직인

210mm×297mm[백상지(120g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제10호서식] <개정 2013.8.8>

정보보호 관리체계 인증 신청서

※ [ ]에는 해당되는 곳에 √표를 하고, 어두운 부분은 신청인이 작성하지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명	사업자등록번호
	주소	전화번호
	대표자	

인증신청의 구분	[ ]최초심사 [ ]사후심사 [ ]갱신심사
정보보호 관리체계의 범위	
정보보호 관리체계의 범위에 포함되어 있는 종업원의 수	
정보보호 관리체계의 범위에 포함되어 있는 서버의 수	

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제9항, 같은 법 시행령 제47조에 따라 위와 같이 정보보호 관리체계의 인증을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

(한국인터넷진흥원 또는 정보보호 관리체계 인증기관명) 귀중

신청(신고)인 제출서류	정보보호 관리체계의 내역서 1부.	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

210㎜×297㎜[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제11호서식] <개정 2013.8.8> (제1쪽)

정보보호 관리체계 인증서

인증번호 :

업체명 :

대표자 :

주소 :

인증의 범위 :

유효기간 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제9항, 같은 법 시행령 제47조에 따라 위와 같이 정보보호 관리체계를 인증합니다.

년 월 일

한국인터넷진흥원 원장
또는 정보보호 관리체계
인증기관 장

직인

210mm×297mm[백상지(120g/㎡)]

(제2쪽)

CERTIFICATE
OF
Information Security Management System

Certificate Number :

Name of Organization :

Name of Representative :

Address :

Scope of Certification :

Period of Validity :

This is to certify that the abovementioned organization is compliant to the assessment standard for Information Security Management System certification in accordance with Article 47, Paragraph 1 and 9 of 「Act on Information Network Utilization and Data Protection, etc.」 and Article 47 of the Enforcement Decree of the same Act.

Date of Issuance :

Signed by the
President of Korea Internet & Security Agency or certification body

210㎜×297㎜[백상지(120g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제12호서식] <개정 2013.8.8>

정보보호 관리체계 인증서 추가발급 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명	사업자등록번호
	주소	전화번호
	대표자	

추가발급 사유	

위와 같이 정보보호 관리체계 인증서의 추가발급을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

한국인터넷진흥원 또는 정보보호 관리체계 인증기관명 귀중

제출서류	해당없음	수수료 없 음

210mm×297mm[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제13호서식] <개정 2013.8.8>

정보보호 관리체계 인증서 변경 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		

변경 내용	변경전	(국문)
		(영문)
	변경후	(국문)
		(영문)
변경사유		

위와 같이 정보보호 관리체계 인증서 변경을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

한국인터넷진흥원 또는 정보보호 관리체계 인증기관명 귀중

제출서류	해당없음	수수료 없 음

210mm×297mm[백상지(80g/㎡)]

정보보호 관리체계 인증 등에 관한 고시

[시행 2013.8.8] [고시 제2013 - 36호, 2013.8.8, 일부개정]

제1장 총칙

제1조(목적) 이 고시는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) 제47조제3항 및 같은 법 시행령(이하 "영"이라 한다) 제47조부터 제53조의2의 규정에 따라 정보보호 관리체계 인증에 관하여 필요한 사항에 대해 정하는 것을 목적으로 한다.

제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "정보보호 관리체계 인증기관(이하 ‘ 인증기관 ’ 이라 한다)"이란 법 제47조제5항에 따라 미래창조과학부가 인증에 관한 업무를 수행할 수 있도록 지정한 기관을 말한다.
2. "업무수행 요건·능력 심사"란 인증기관으로 지정받고자 신청한 법인 또는 단체의 업무수행 요건·능력을 별표 2의 세부기준에 따라 심사하는 것을 말한다.
3. "인증"이란 신청기관이 수립하여 운영하고 있는 정보보호 관리체계가 별표 6의 정보보호 관리체계 인증기준(이하 "인증기준"이라 한다)에 적합함을 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다) 또는 인증기관이 증명하는 것을 말한다.
4. "인증심사"란 신청기관이 수립하여 운영하는 정보보호 관리체계가 인증기준에 적합한지의 여부를 인터넷진흥원 또는 인증기관이 서면심사 및 현장심사의 방법으로 확인하는 것을 말한다.
5. "정보보호관리과정(이하 ‘ 관리과정 ’ 이라 한다)"이란 정보보호 관리체계를 수립·운영하기 위하여 유지·관리하여야 할 과정으로 다음 각 목의 5단계 활동을 말한다.
   가. 정보보호정책 수립 및 범위설정
   나. 경영진 책임 및 조직구성
   다. 위험관리
   라. 정보보호대책 구현
   마. 사후관리
6. "정보보호대책"이란 신청기관이 정보보호 관리체계를 수립·운영하기 위하여 별표 6에서 선택한 통제사항을 말한다.
7. "신청기관"이란 이 고시에 따라 정보보호 관리체계 인증을 취득하고자 신청한 자를 말한다.

8. "인증심사원"이란 별표 3의 자격요건을 갖춘 자를 말한다.
9. "최초심사"란 처음으로 인증을 신청하거나 인증의 범위에 중요한 변경이 있어서 다시 인증을 신청한 때 실시하는 인증심사를 말한다.
10. "사후심사"란 정보보호 관리체계 인증(인증이 갱신된 경우를 포함한다)을 받고난 후 매년 사후관리를 위하여 실시하는 인증심사를 말한다.
11. "갱신심사"란 유효기간 만료로 다시 인증을 신청한 때 실시하는 인증심사를 말한다.

제2장 정보보호 관리체계 인증기관

제3조(인증기관의 지정 등) ① 미래창조과학부는 법 제47조제5항 및 영 제53조의2에 따라 인증기관을 지정할 필요가 있는 때에는 지정대상 기관의 수, 업무의 범위 및 신청방법 등을 정하여 관보 및 인터넷 홈페이지에 20일 이상 공고하여야 한다.

② 제1항에 따라 인증기관으로 지정받으려는 자는 다음 각 호의 서류를 미래창조과학부에 제출하여야 한다.

1. 별지 제1호서식의 정보보호 관리체계 인증기관 지정 신청서
2. 영 제53조의2제1항제2호에 따른 별지 제2호서식의 인증심사원 보유현황과 이를 증명할 수 있는 서류
3. 영 제53조의2제1항제3호에 따른 별표 1의 업무수행 요건·능력 심사를 위하여 필요한 서류

제4조(업무수행 요건·능력 심사 세부기준 등) ① 영 제53조제2항에 따른 업무수행 요건·능력 심사를 위한 세부기준은 별표 2와 같다.

② 미래창조과학부는 제3조제2항에 따라 인증기관의 지정 신청을 받은 때에는 제1항에 따라 업무수행 요건·능력을 심사하여 지정 대상기관의 순위를 정한다.

제5조(업무수행 능력의 적합성 인정) ① 미래창조과학부는 제4조제1항에 따라 업무수행 요건·능력을 심사하여 지정에 필요한 수만큼 점수의 합이 높은 순으로 선별한다.

② 미래창조과학부는 제1항에 따라 심사한 결과를 바탕으로 하여 인증기관으로의 지정 여부를 최종 결정한다.

제6조(인증기관 지정서) 영 제53조의2제3항에 따른 정보보호 관리체계 인증기관 지정서는 별지 제3호서식과 같다.

제7조(인증기관의 사후관리) 영 제53조의4제1항에 따른 인증기관의 전년도 인증실적 보고서는 별지 제4호서식과 같다.

제8조(인증기관 재지정) ① 인증기관은 유효기간이 끝나기 전 6개월부터 끝나는 날까지 별지 제1호서식에 따라 미래창조과학부에 재지정 신청을 할 수 있다.

② 제1항에 따른 재지정의 심사, 재지정 결과 통지, 재지정서 교부 등에 관하여는 영 제53조의2제3항을 준용한다.

제3장 인증심사원의 자격 및 관리

제9조(인증심사원의 자격 요건 등) ① 인증심사원은 심사원보, 심사원, 선임심사원으로 구분하며, 인증심사원 등급별 자격 요건은 별표 3과 같다.

② 인증심사원이 되려는 자는 별표 3의 학력 및 경력 요건을 갖추고 인터넷진흥원이 지정하는 기관에서 인증심사원 양성교육 과정을 수료하여야 한다.

제10조(인증심사원 자격 신청) 인증심사원의 자격을 신청하고자 하는 자는 제9조제2항에 따라 인증심사원 양성교육 과정을 수료한 날로부터 1개월 이내에 인터넷진흥원에 다음 각 호의 모든 서류를 제출하여야 한다.

1. 별지 제5호서식 정보보호 관리체계 인증심사원 자격 신청서
2. 학위증명서, 자격증 사본(해당 시)
3. 별지 제6호서식 경력증명서
4. 별지 제7호서식 상세 재직증명서 등 경력증빙서류
5. 별지 제8호서식 기술실적증명서(해당 시)

제11조(인증심사원 자격 부여) ① 인터넷진흥원은 인증심사원 자격 신청서를 접수한 때에는 신청서류를 검토하여 서류 보완 및 추가제출을 요청할 수 있다.

② 서류 보완 및 추가제출을 요청받은 자격 신청자는 1개월 이내에 관련 서류 등을 제출하여야 한다.

③ 인터넷진흥원은 인증심사원 자격의 적합 여부를 확인하여 통과한 자에게 별지 제9호서식의 인증심사원 자격 증명서를 발급하여야 한다.

제12조(인증심사원 자격 유지) ① 인증심사원의 자격 유효기간은 자격 부여를 받은 날로부터 3년으로 한다.

② 인증심사원은 자격 유지를 위해 유효기간 내에 인터넷진흥원이 지정하는 기관에서 시행하는 인증심사원 보수교육을 이수해야 한다. 다만, 부득이한 사유로 보수교육을 받지 못한 경우에는 인터넷진흥원이 인정하는 대체교육을 받아야 한다.

③ 보수교육을 이수한 자에 한하여 자격 유효기간이 3년간 연장된다.

제13조(인증심사원 자격 취소) ① 인증심사원 자격 신청 시 제출한 서류가 허위이거나, 제12조에 따른 자격 유지 기준을 충족하지 못한 경우에는 자격을 취소한다.

② 인증심사원으로서 객관적이고 공정한 인증심사를 수행하지 않거나, 인증심사와 관련된 부당한 금전, 금품 등을 수수하거나 인증심사 수행 중 취득한 정보를 누설하는 경우에는 자격을 취소한다.

제4장 인증심사의 신청 및 계약

제14조(인증 의무대상자 범위) ① 인증 의무대상자란 법 제47조제2항, 영 제49조에 따라 정보보호 관리체계 인증을 받아야 하는 자를 말한다.

② 법 제47조제2항제2호에 따라 정보보호 관리체계 인증을 받아야 하는 자 중 집적정보통신시설 사업자가 마련한 시설의 일부를 임대하여 집적정보통신시설 사업을 하는 자에 대하여는 영 제49조제2항의 기준을 준용한다.

③ 인증 의무대상자는 매년 1월1일부터 12월31일까지 인증을 받아야 한다.

제15조(신청기관의 사전 준비사항) 신청기관은 정보보호 관리체계 인증을 신청하기 전에 인증기준에 따른 정보보호 관리체계를 구축하여 최소 2개월 이상 운영하여야 한다.

제16조(인증의 신청 등) ① 법 제47조제1항 또는 제2항에 따라 정보보호 관리체계 인증을 받으려는 자는 별지 제10호서식의 정보보호 관리체계 인증 신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

② 신청기관은 인증의 범위 및 일정 등을 인터넷진흥원 또는 인증기관과 사전 협의하여 신청하여야 한다.

③ 인터넷진흥원 또는 인증기관은 제14조에 따른 인증 의무대상자가 사업자 등록일이 속한 분기가 끝나는 날의 1개월 전까지 인증 신청을 한 경우 인증심사를 우선적으로 처리할 수 있다.

제17조(인증심사 계약 체결) 신청기관은 인터넷진흥원 또는 인증기관과 협의한 후 심사기간, 심사인원, 인증 수수료, 인증의 범위 등을 포함하는 인증심사 계약을 체결한다.

제5장 인증심사의 기준과 방법

제18조(인증기준) 인증기준은 별표 6과 같다.

제19조(인증심사팀 구성) ① 인터넷진흥원 또는 인증기관은 제17조에 따른 인증심사 계약을 체결한 때에는 지체 없이 인증심사원으로 인증심사팀을 구성하여야 한다.

② 인증심사팀 구성 시 심사팀장은 인터넷진흥원 또는 인증기관 소속의 심사원 이상으로 선정하여야 한다.

③ 신청기관의 정보보호 관리체계 인증을 위한 컨설팅에 참여한 인증심사원 또는 신청기관의 소속직원은 인증심사팀의 구성원에서 배제하여야 한다.

제20조(인증심사 방법 및 보완조치) ① 인증심사는 신청기관을 방문하여 서면심사와 현장심사를 병행한다.

② 서면심사는 인증기준에 적합한지에 대하여 정보보호 관리체계 구축·운영 관련 정보보호 정책, 지침, 절차 및 이행의 증적자료 검토, 정보보호대책 적용 여부 확인 등의 방법으로 관리

적 요소를 심사한다.

③ 현장심사는 서면심사의 결과와 기술적·물리적 보호대책 이행 여부를 확인하기 위하여 담당자 면담, 관련 시스템 확인 및 취약점 점검 등의 방법으로 기술적 요소를 심사한다.

④ 인터넷진흥원 또는 인증기관은 인증심사에서 발견된 결함에 대해 최대 90일(재조치 요구 60일 포함) 이내에 보완조치를 완료하도록 신청기관에게 요청할 수 있다.

⑤ 인터넷진흥원 또는 인증기관은 인증위원회 심의결과에 따라 30일 이내에 보완조치를 요구할 수 있다.

제6장 인증위원회 구성과 운영

제21조(인증위원회의 구성) ① 법 제47조제5항에 따라 인터넷진흥원 또는 인증기관의 장은 다음 각 호의 사항을 심의·의결하기 위하여 인증위원회를 설치·운영하여야 한다.

1. 최초심사 또는 갱신심사 결과가 인증기준에 적합한지 여부
2. 사후심사 결과 법 제47조제8항 각 호에 해당하는 사유를 발견한 경우에 그 결과의 적합성 여부
3. 그 밖에 정보보호 관리체계 인증과 관련하여 위원장이 필요하다고 인정하는 사항

② 인증위원회는 5인 이상 10인 이내의 위원으로 구성하되, 위원은 정보보호전문가, 정보시스템감리사, 기술사, 대학교수 등 정보보호분야에 학식과 경험이 있는 자 중에서 인터넷진흥원 또는 인증기관의 장이 위촉하며, 위원장은 위원 중에서 호선한다.

③ 위원장은 인증위원회의 업무를 통할하며 위원회를 대표한다.

제22조(인증위원회의 운영) ① 인터넷진흥원 또는 인증기관의 장은 인증위원회의 심의안건을 검토하여 위원회 개최 5일 전까지 인증위원회에 제출한다.

② 인증위원회 위원장은 제21조제1항 각 호의 사항에 대한 심의·의결 결과를 인터넷진흥원 또는 인증기관의 장에게 제출한다.

제7장 인증서의 발급·관리 및 홍보

제23조(인증서 발급) 인터넷진흥원 또는 인증기관의 장은 제22조제1항에 따라 인증위원회의 심의·의결 결과를 제출받은 때에는 신청기관의 정보보호 관리체계가 이 고시에서 정한 인증기준에 적합하다고 판단된 경우 별지 제11호서식의 정보보호 관리체계 인증서를 발급하여야 한다.

제24조(인증서 관리) ① 인터넷진흥원 또는 인증기관은 발급된 인증서의 인증번호, 발급일, 유효기간 등 인증서를 관리하여야 한다.

② 인증을 취득한 자는 인증서의 분실 등으로 인해 재발급을 받고자 할 경우 별지 제12호서식의 정보보호 관리체계 인증서 추가발급 신청서를 인터넷진흥원 또는 인증기관에 제출하여야

한다.

③ 인증을 취득한 자가 주소, 업체명 등 인증서 기재사항의 변경을 요청하고자 하는 경우 별지 제13호서식의 정보보호 관리체계 인증서 변경신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

제25조(인증의 표시 및 홍보) ① 영 제52조에 따른 인증의 표시는 별표 4와 같다.

② 제1항에 따른 인증의 표시를 사용하는 경우에는 영 제52조에 따라 인증의 범위와 유효기간을 함께 표시하여야 한다.

제8장 정보보호 관리체계 인증 수수료

제26조(수수료의 산정) ① 인증 수수료는 다음 각 호의 기준을 준용하되 별표 5의 정보보호 관리체계 인증 수수료 산정기준을 적용하여 산정한다.

1. 「엔지니어링산업 진흥법」 제31조제2항에 따른 엔지니어링사업의 대가 기준
2. 한국소프트웨어산업협회가 제공하는 「SW사업 대가산정 가이드」의 정보보안 컨설팅비

② 인터넷진흥원 또는 인증기관은 제1항에 따라 산정된 인증 수수료를 공지하여야 한다. 다만, 「중소기업기본법」 제2조에 따른 중소기업이 인증을 신청하는 경우 수수료 감면 등 필요한 지원을 할 수 있다.

③ 인터넷진흥원 또는 인증기관은 신청기관의 인증범위가 정보보호 관련 타 인증과 중복될 경우 신청기관과 협의하여 수수료를 조정할 수 있다.

제27조(수수료의 납부) ① 신청기관은 최초심사, 사후심사 및 갱신심사 신청 시 수수료를 납부한다. 다만, 수수료 납부 방법(일괄 또는 분할)은 인증심사 계약 시 신청기관과 협의하여 조정할 수 있다.

② 신청기관은 인증심사 계약을 체결한 날로부터 1개월 이내에 인증 수수료를 인터넷진흥원 또는 인증기관에 납부하여야 한다.

제28조(인증업무 지침) 인터넷진흥원 또는 인증기관은 인증업무 수행을 위해 필요한 경우 인증업무에 관한 지침을 마련하여 시행할 수 있다.

제29조(재검토기한) 「훈령ㆍ예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 고시 발령 후 법령이나 현실여건의 변화 등을 검토하여 이 고시의 폐지, 개정 등 조치를 하여야 하는 기한은 2016년 3월 23일까지로 한다.

부칙 <제2008 - 11호,2008.5.19>

이 고시는 고시한 날부터 시행한다.

부칙 <제2009 - 27호,2009.11.5>

이 고시는 2009년 11월 5일부터 시행한다.

부칙 <제2010 - 3호,2010.2.3>

제1조(시행일) 이 고시는 2010년 2월 3일부터 시행한다.

제2조(서식에 관한 경과조치) 이 고시 시행당시 종전의 규정에 의한 서식은 2010년 6월 30일까지 이 고시에 의한 서식과 함께 사용할 수 있다.

부칙 <제2012 - 23호,2012.3.15>

이 고시는 발령한 날부터 시행한다

부칙 <제2013 - 4호,2013.1.17>

제1조(시행일) 이 고시는 2013년 2월 18일부터 시행한다.

제2조(인증심사원에 관한 경과조치) 이 고시 시행 이전에 종전 고시에 따라 인증 심사업무를 전담하는 직원의 요건을 갖추고 인터넷진흥원으로부터 위촉된 자는 이 고시에 의한 인증심사원 자격을 취득한 것으로 본다.

부칙 <제2013 - 36호,2013.8.8>

제1조(시행일) 이 고시는 2013년 8월 8일부터 시행한다.

[별표 1]

업무수행 요건·능력 심사 규정에 따른 제출서류(제3조제2항 관련)

구 분	제 출 서 류
1. 정보보호 관리체계 인증심사 참여 실적을 확인하는 데 필요한 서류	가. 별지 제4호서식에 따른 정보보호 관리체계 인증심사 참여실적 명세서 및 이를 증빙할 수 있는 자료 (인증심사 참여통지 문서 등) 나. 인증심사원 자격 증빙 자료
2. 업무수행 요건·능력 심사를 위하여 필요한 서류	가. 자본금 5억원 이상 내역(공인회계사 또는 회계담당자가 서명날인한 서류) 나. 부채비율 및 자기자본 이익률의 계산내역(회계결산내역 등 관련 증빙자료) 다. 인증심사 업무 운영체계 관련 규정 및 지침 등 o 심사기관의 운영체계 및 인증의 품질관리 o 인증심사 업무를 수행하는 직원에 대한 운영관리 등의 내부규정 o 인증심사 업무 수행 방법 및 절차

[별표 2]

업무수행 요건·능력 심사 세부기준(제4조제1항 관련)

가. 업무수행 요건 심사 세부기준

평가항목	세부 평가 기준
1. 인증심사원 5명 이상 상시 고용 여부	o 인증심사원 5명 이상을 상시 고용하고 있어야 함 - 다만, 심사팀장급 심사원 1명 이상 확보해야 함
2. 인증기관 공정성 확보 여부	o 정보보호 관리체계 인증기관으로 지정을 받으려는 기관은 인증업무의 독립성, 객관성, 공정성, 신뢰성을 확보하기 위하여 정보보호 관리체계 구축과 관련된 컨설팅 업무를 수행하지 않아야 함

나. 업무수행 능력 심사 세부기준

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td rowspan="3">1. 조직 내 직원들의 정보보호 전문성 (30)</td><td rowspan="3">정보보호 업무 전문성</td><td>10</td><td>비율</td><td>o 심사원 이상 인력 수
<table><tr><td>심사원 수</td><td>점수</td></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (심사원 수/5명) × 100</td></tr></table></td></tr>
<tr><td>5</td><td>비율</td><td>o 정보보호 관련 박사학위 소지자 · 기술사 인력의 수
<table><tr><td>박사학위소지자·기술사 수</td><td>점수</td></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (박사학위 소지자, 기술사 수/5명) × 100</td></tr></table></td></tr>
<tr><td>5</td><td>비율</td><td>o CISM, SIS, CISSP, CISA, CPPG, 정보보안기사/산업기사 자격증 소지자 수
<table><tr><td>자격증 소지자 · 수</td><td>점수</td></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (자격증 소지자 수/5명) × 100</td></tr></table></td></tr>
<tr><td>정보보호 관리체계 인증심사 참여실적</td><td>10</td><td>비율</td><td>o 상시 고용하고 있는 인증심사원이 최근 3년간 참여한 정보보호 관리체계 인증심사 참여 실적을 인정하고 평가점수는 개별 참여 실적을 합한 총 참여일수에 따라 산출
<table><tr><td>총 참여 일수(단위 : 일)</td><td>점수</td></tr><tr><td>200일 이상</td><td>배점의 100%</td></tr><tr><td>200일 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (총 참여일수/200일) × 100</td></tr></table></td></tr>
</table>

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td>2. 시설(10)</td><td>사무공간·인증심사 서류 보관 장소 및 보안설비·시설 확보</td><td>10</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>○ 인증심사의 상담, 인증심사 업무의 처리를 위해 필요한 사무실</td><td>2점</td></tr>
<tr><td>○ 사무 관련 장비 확보</td><td>2점</td></tr>
<tr><td>○ 사무실 출입자에 대한 신원확인 및 출입통제를 위한 설비</td><td>2점</td></tr>
<tr><td>○ 기록물 및 자료의 안전한 관리를 위한 보관 장소</td><td>2점</td></tr>
<tr><td>○ 인증심사 서류의 분실, 도난 등 예방을 위한 보안 시설</td><td>2점</td></tr>
</table>
</td></tr>
<tr><td rowspan="2">3. 신뢰도 및 재정상태 건실도 (10)

※비영리기관 평가제외</td><td>부채비율</td><td>5</td><td>비율</td><td>○ 지정 공고일 기준으로 직전년도 부채비율
(부채총계/자기자본)
<table>
<tr><th>비율</th><th>점수</th></tr>
<tr><td>50% 미만</td><td>5점</td></tr>
<tr><td>50% 이상 ~ 100% 미만</td><td>4점</td></tr>
<tr><td>100% 이상 ~ 150% 미만</td><td>3점</td></tr>
<tr><td>150% 이상 ~ 200% 미만</td><td>2점</td></tr>
<tr><td>200% 이상</td><td>1점</td></tr>
</table>
</td></tr>
<tr><td>자기자본 이익률</td><td>5</td><td>비율</td><td>○ 지정 공고일 기준으로 직전년도 자기자본이익률
(당기순이익/자기자본)
<table>
<tr><th>비율</th><th>점수</th></tr>
<tr><td>20% 이상</td><td>5점</td></tr>
<tr><td>20% 미만 ~ 15% 이상</td><td>4점</td></tr>
<tr><td>15% 미만 ~ 10% 이상</td><td>3점</td></tr>
<tr><td>10% 미만 ~ 5% 이상</td><td>2점</td></tr>
<tr><td>5% 미만</td><td>1점</td></tr>
</table>
</td></tr>
<tr><td rowspan="3">4. 인증업무 운영 체계 (50)</td><td>인증기관의 운영 체계 및 인증의 품질관리</td><td>20</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>○ 인증기관의 공정성·객관성·신뢰성·독립성 보장 방안</td><td>5점</td></tr>
<tr><td>○ 인증기관의 내부감사 실시 및 검토 등에 대한 방안</td><td>5점</td></tr>
<tr><td>○ 인증의 품질 보장 및 관리방안</td><td>5점</td></tr>
<tr><td>○ 인증업무의 기록 및 문서화 관리체계의 적절성</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td>인증업무를 수행하는 직원에 대한 운영·관리 등의 내부 규정</td><td>10</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>○ 인증업무를 수행하는 직원에 대한 규정 보유 및 그 규정의 타당성 및 실효성
- 인증업무를 수행하는 직원의 의무와 책임 등 준수사항
- 인증업무를 수행하는 직원의 자체 보안관리 및 감독 요령</td><td>5점</td></tr>
<tr><td>○ 인증업무를 수행하는 직원의 교육 및 평가 등에 대한 방안 및 그 방안의 적절성 및 타당성</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td>인증업무 수행 방법 및 절차</td><td>5</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>○ 인증업무 수행 방법 및 절차 등의 적절성 및 타당성
- 인증심사의 절차 및 방법
- 인증수수료 및 그 징수방법
- 인증심사팀 구성 원칙
- 인증심사 사후관리방안 등</td><td>5점</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td></td><td>인증업무
지원체계</td><td>15</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 운영자금 법인통장 보유 및 유지 수준</td><td>5점</td></tr>
<tr><td>o 지정취소, 부도 · 해산 등에 따른 신청기관 피해 보상 관련 보험 가입 여부</td><td>5점</td></tr>
<tr><td>o 인증의 품질 제고를 위한 지원방안</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td rowspan="3">5. 가점 및 감점</td><td>인증심사 업무를 전담하는 인증심사원 보유수</td><td>5
(가점)</td><td>보유
인원수</td><td>o 인증심사업무를 수행하는 전담조직을 갖추고, 그 전담조직에 속한 직원에 대해 인정
<table>
<tr><th>구분</th><th>점수</th></tr>
<tr><td>10명 이상</td><td>5점</td></tr>
<tr><td>10명 미만 ~ 5명 이상</td><td>배점의 X%</td></tr>
<tr><td>5명 미만</td><td>없음</td></tr>
<tr><td colspan="2">※X = (인원수/10명) × 100</td></tr>
</table>
</td></tr>
<tr><td>정보보호
관리체계 인증의 취득 및 유지</td><td>2
(가점)</td><td>인증 취득
및 유지</td><td>o 정보보호 관리체계 인증을 취득하고, 인증을 유지하고 있을 때</td></tr>
<tr><td>자격취소 사실</td><td>5
(감점)</td><td>취소사실
및
취소회수</td><td>o 지정 공고일 기준으로 10년 이내에 미래창조과학부가 부여한 정보보호 관련 수행자격이 취소된 경우
- 정보보호 관리체계 인증기관, 안전진단 수행기관 등
※ 취소 1회당 : 감점 5점</td></tr>
</table>

<비 고>

1. 평가항목에 대한 각 평가요소별 세부평가 점수는 소수점 이하 둘째 자리에서 반올림한다.
2. 평가항목에 대한 각 평가요소별 평가점수는 평가결과의 최저점과 최고점을 제외한 점수들의 평균점을 부여한다. 다만, 최저점 또는 최고점이 2개 이상일 경우 각 1개만 제외한다.
3. 가점을 합한 점수가 100점을 초과해도 만점 100점으로 표기한다.
4. '시설', '인증업무 운영체계'에 대한 각 평가요소별 세부평가 점수 부여기준은 각 평가요소의 평가결과에 평가등급(계수)를 곱하여 나온 점수를 합산한다.

평가요소별 세부평가 점수	평가등급(계수)
100점 이하 ~ 90점 이상	우수(1.0)
90점 미만 ~ 80점 이상	보통(0.6)
80점 미만 ~	미흡(0.2)
미 제출	점수 없음(0)

[별표 3]

인증심사원 자격 요건(제9조 관련)

1. 인증심사원 등급별 자격 요건

구 분	자격 요건
심사원보	o 인증심사원 학력 및 경력요건을 만족하는 자로서 인터넷진흥원이 지정하는 기관에서 인증심사원 양성교육 과정을 수료한 자
심사원	o 심사원보 자격 취득자로서 인증심사 4회 이상 참여하고 심사일수의 합이 20일 이상인 자
선임심사원	o 심사원 자격 취득자로서 3회 이상 심사 총괄업무를 수행하고 심사일수의 합이 15일 이상인 자

2. 인증심사원 학력 및 경력 요건

o 학사학위를 취득한 후 정보통신 또는 정보보호 유관경력 6년(전문학사의 경우 8년, 수업연한이 3년인 전문학사의 경우 7년, 고등학교 졸업자의 경우 10년을 말한다) 이상을 보유한 자(최근 10년 이내의 경력에 한함)

o 유관자격 소지자 또는 유관학력을 취득한 자로서 다음 각 목의 어느 하나에 해당하는 경우 정보통신 유관경력을 인정한다.
가. 기술사 자격 소지자 또는 박사 학위를 취득한 자의 경우 3년
나. 기사 자격 소지자 또는 석사 학위를 취득한 자의 경우 2년
다. 산업기사 자격 소지자 또는 학사 학위를 취득한 자의 경우 1년

o 다음 각 목의 어느 하나에 해당하는 자격을 취득한 자는 정보통신 또는 정보보호 유관경력 1년을 추가 인정한다.
가. 한국인터넷진흥원 정보보호전문가(SIS)
나. 전자정부법 제60조에 따른 감리원
다. 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 정보시스템감사사(CISA)
라. 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 정보시스템보호전문가(CISSP)

<비 고>
1. "정보통신 유관경력", "정보보호 유관경력", "유관자격" 및 "유관학력"은 영 별표 2 "정보보호 기술인력의 자격기준"을 준용한다.

[별표 4]

정보보호 관리체계 인증의 표시(제25조 관련)

□ 출입구 부착용

1. 도안모형



2. 인증명판 제작 유의사항

가. 소재는 가급적 동판으로 제작한다(전체 두께 1.0㎝, 바탕 0.4㎝, 테두리 폭 0.5㎝)

나. 바탕색은 가급적 연마하지 않은 황동색으로 한다

다. 도안 모형은 인증의 표시를 중앙에 둔다

라. 글씨 및 도형은 양각으로 한다.

마. 크기는 사각형으로 하며 인증마크는 중앙에 위치하도록 하며 가로와 세로 비율을 3 : 2로 하여 일정 비율로 조정할 수 있다

□ 서류 및 제품 등 표시용

1. 도안모형



2. 도안 및 표시방법

가. 'Information Security Management System'은 검정색으로, '정보보호 관리체계 인증'은 군청색으로 한다. 게시장소의 칼라표시가 불합리한 경우에는 흑백으로 할 수 있다.

나. 마크의 크기는 제품과 그 제품의 포장 또는 용기의 크기에 따라 일정 비율로 조정할 수 있다.

[별표 5]

정보보호 관리체계 인증 수수료 산정기준(제26조 관련)

1. 인증 수수료 산정 방식

인증 수수료 = 직접인건비 + 직접경비 + 제경비 + 기술료

① 직접인건비는 인증심사에 투입되는 인증심사원에 대한 인건비로 산정한다. 인건비는 SW사업 대가산정 가이드의 정보보안 컨설팅비를 준용한다

인증심사원 등급	컨설턴트 등급
선임심사원	전임 컨설턴트 이상
심사원	
심사원보	컨설턴트

② 직접경비는 인증심사업무의 수행에 따라 발생하는 교통비, 숙박비 및 식대 등 인증심사업무에 소요되는 직접적인 경비를 산정한다.

③ 제경비는 최대 (직접인건비×120%) 로 산정한다.

④ 기술료는 최대 {(직접인건비+제경비)×40% } 로 산정한다.

[별표 6]

정보보호 관리체계 인증기준(제18조 관련)

가. 정보보호관리과정 요구사항

	관리과정		세부관리과정	관리과정 상세내용
1	정보보호정책 수립 및 범위설정	1.1	정보보호정책의 수립	조직이 수행하는 모든 정보보호 활동의 근거를 포함할 수 있도록 정보보호정책을 수립하고 동 정책은 국가나 관련 산업에서 정하는 정보보호 관련 법, 규제를 만족하여야 한다.
		1.2	범위설정	조직에 미치는 영향을 고려하여 중요한 업무, 서비스, 조직, 자산 등을 포함할 수 있도록 정보보호 관리체계 범위를 설정하고 범위 내 모든 자산을 식별하여 문서화하여야 한다.
2	경영진 책임 및 조직구성	2.1	경영진 참여	정보보호 관리체계 수립 및 운영 등 조직이 수행하는 정보보호 활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여야 한다.
		2.2	정보보호 조직 구성 및 자원 할당	최고경영자는 조직의 규모, 업무 중요도 분석을 통해 정보보호 관리체계의 지속적인 운영이 가능하도록 정보보호 최고책임자, 실무조직 등 정보보호 조직을 구성하고 정보보호 관리체계 운영 활동을 수행하는데 필요한 자원(예산 및 인력)을 확보하여야 한다.
3	위험관리	3.1	위험관리 방법 및 계획 수립	관리적, 기술적, 물리적, 법적 분야 등 조직의 정보보호 전 영역에 대한 위험식별 및 평가가 가능하도록 위험관리 방법을 선정하고 위험관리의 전문성을 보장할 수 있도록 수행인원, 기간, 대상, 방법 등을 구체적으로 포함한 위험관리계획을 사전에 수립하여야 한다.
		3.2	위험식별 및 평가	위험관리 방법 및 계획에 따라 정보보호 전 영역에 대한 위험 식별 및 평가를 연 1회 이상 수행하고 그 결과에 따라 조직에서 수용 가능한 위험수준을 설정하여 관리하여야 한다.

	관리과정		세부관리과정	관리과정 상세내용
3	위험관리	3.3	정보보호대책 선정 및 이행계획 수립	위험을 수용 가능한 수준으로 감소시키기 위해 정보보호대책을 선정하고 그 보호대책의 구현 우선순위, 일정, 담당부서 및 담당자 지정, 예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.
4	정보보호대책 구현	4.1	정보보호대책의 효과적 구현	정보보호대책 이행계획에 따라 보호대책을 구현하고 경영진은 이행결과의 정확성 및 효과성 여부를 확인하여야 한다.
		4.2	내부 공유 및 교육	구현된 정보보호대책을 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여야 한다.
5	사후관리	5.1	법적요구사항 준수검토	조직이 준수해야 할 정보보호 관련 법적요구사항을 지속적으로 파악하여 최신성을 유지하고 준수여부를 지속적으로 검토하여야 한다.
		5.2	정보보호 관리체계 운영현황 관리	정보보호 관리체계 범위 내에서 주기적 또는 상시적으로 수행해야 하는 활동을 문서화하고 그 운영현황을 지속적으로 관리하여야 한다.
		5.3	내부감사	조직은 정보보호 관리체계가 정해진 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는 지를 점검하기 위하여 연 1회 이상 내부감사를 수행하여야 한다. 이를 위해 감사 기준, 범위, 주기, 방법 등을 구체적으로 정하고 내부감사를 통해 발견된 문제점은 보완조치를 완료하여 경영진 및 관련 책임자에게 보고하여야 한다. 또한 감사의 독립성 및 전문성을 확보할 수 있도록 감사인력에 대한 자격요건을 정의하여야 한다.

나. 정보보호대책

	통제분야		통제목적		통제사항	통제내용
1	정보보호 정책	1.1	정책의 승인 및 공표	1.1.1	정책의 승인	정보보호정책은 이해관련자의 검토와 최고경영자의 승인을 받아야 한다.
				1.1.2	정책의 공표	정보보호정책 문서는 모든 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.
		1.2	정책의 체계	1.2.1	상위 정책과의 연계성	정보보호정책은 상위조직 및 관련 기관의 정책과 연계성을 유지하여야 한다.
				1.2.2	정책시행 문서수립	정보보호정책의 구체적인 시행을 위한 정보보호지침, 절차를 수립하고 관련 문서간의 일관성을 유지하여야 한다.
		1.3	정책의 유지관리	1.3.1	정책의 검토	정기적으로 정보보호정책 및 정책 시행문서의 타당성을 검토하고, 중대한 보안사고 발생, 새로운 위협 또는 취약성의 발견, 정보보호 환경에 중대한 변화 등이 정보보호정책에 미치는 영향을 분석하여 필요한 경우 제·개정하여야 한다.
				1.3.2	정책문서 관리	정보보호정책 및 정책 시행문서의 이력관리를 위해 제정, 개정, 배포, 폐기 등의 관리절차를 수립하고 문서는 최신본으로 유지하여야 한다. 또한 정책문서 시행에 따른 운영기록을 생성하여 유지하여야 한다.
2	정보보호 조직	2.1	조직 체계	2.1.1	정보보호 최고 책임자 지정	최고경영자는 임원급의 정보보호 최고책임자를 지정하고 정보보호 최고책임자는 정보보호정책 수립, 정보보호 조직 구성, 위험관리, 정보보호위원회 운영 등의 정보보호에 관한 업무를 총괄 관리하여야 한다.

	통제분야		통제목적		통제사항	통제내용
2	정보보호 조직	2.1	조직의 체계	2.1.2	실무조직 구성	최고경영자는 정보보호 최고책임자의 역할을 지원하고 조직의 정보보호 활동을 체계적으로 이행하기 위해 실무조직을 구성하고 조직 구성원의 정보보호 전문성을 고려하여 구성한다.
				2.1.3	정보보호 위원회	정보보호 자원할당 등 조직 전반에 걸친 중요한 정보보호 관련사항에 대한 검토 및 의사결정을 할 수 있도록 정보보호위원회를 구성하여 운영하여야 한다.
		2.2	역할 및 책임	2.2.1	역할 및 책임	정보보호 최고책임자와 정보보호 관련 담당자에 대한 역할 및 책임을 정의하고 그 활동을 평가할 수 있는 체계를 마련하여야 한다.
3	외부자 보안	3.1	보안 요구사항 정의	3.1.1	외부자 계약 시 보안요구사항	조직의 정보처리 업무를 외부자에게 위탁하거나 정보자산에 대한 접근을 허용할 경우, 또는 업무를 위해 클라우드 서비스 등 외부 서비스를 이용하는 경우에는 보안요구사항을 식별하고 관련 내용을 계약서 및 협정서 등에 명시하여야 한다.
		3.2	외부자 보안 이행	3.2.1	외부자 보안 이행 관리	외부자가 계약서 및 협정서에 명시된 보안요구사항의 이행여부를 관리 감독하고 주기적인 점검 또는 감사를 수행하여야 한다.
				3.2.2	외부자 계약 만료 시 보안	외부자와의 계약 만료, 업무 종료, 담당자 변경 시 조직이 외부자에게 제공한 정보자산의 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 업무 수행 시 알게 된 정보의 비밀유지 확약서 등의 내용을 확인하여야 한다.

	통제분야		통제목적		통제사항	통제내용
4	정보자산 분류	4.1	정보자산 식별 및 책임	4.1.1	정보자산 식별	조직의 업무특성에 따라 정보자산 분류기준을 수립하고 정보보호 관리체계 범위 내 모든 정보자산을 식별하여야 한다. 또한 식별된 정보자산을 목록으로 관리하여야 한다.
				4.1.2	정보자산별 책임할당	식별된 정보자산에 대한 책임자 및 관리자를 지정하여 책임소재를 명확히 하여야 한다.
		4.2	정보자산의 분류 및 취급	4.2.1	보안등급과 취급	기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 정보자산이 조직에 미치는 중요도를 평가하고 그 중요도에 따라 보안등급을 부여하여야 한다. 또한 보안등급을 표시하고 등급 부여에 따른 취급절차를 정의하여 이행하여야 한다.
5	정보보호 교육	5.1	교육 프로그램 수립	5.1.1	교육 계획	교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 정보보호 교육 계획을 수립하여야 한다.
				5.1.2	교육 대상	교육 대상에는 정보보호 관리체계 범위 내 임직원 및 외부자를 모두 포함하여야 한다.
				5.1.3	교육 내용 및 방법	교육에는 정보보호 및 정보보호 관리체계 개요, 보안사고 사례, 내부 규정 및 절차, 법적 책임 등의 내용을 포함하고 일반 임직원, 책임자, IT 및 정보보호 담당자 등 각 직무별 전문성 제고에 적합한 교육내용 및 방법을 정하여야 한다.
		5.2	교육 시행 및 평가	5.2.1	교육 시행 및 평가	정보보호 관리체계 범위 내 임직원 및 외부자를 대상으로 연 1회 이상 교육을 시행하고 정보보호 정책 및 절차의 중대한 변경, 조직 내·외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생할 경우 추가 교육을 수행하여야 한다. 또한 교육 시행에 대한 기록을 남기고 평가하여야 한다.

	통제분야		통제목적		통제사항	통제내용
6	인적 보안	6.1	정보보호 책임	6.1.1	주요 직무자 지정 및 감독	인사정보, 영업비밀, 산업기밀, 개인정보 등 중요정보를 대량으로 취급하는 임직원의 경우 주요직무자로 지정하고 주요직무자 지정을 최소화 하는 등 관리할 수 있는 보호대책을 수립하여야 한다.
				6.1.2	직무 분리	권한 오남용 등 고의적인 행위로 인해 발생할 수 있는 잠재적인 피해를 줄이기 위하여 직무 분리 기준을 수립하고 적용하여야 한다. 다만 인적 자원 부족 등 불가피하게 직무분리가 어려운 경우 별도의 보완통제를 마련하여야 한다.
				6.1.3	비밀유지 서약서	임직원으로부터 비밀유지 서약서를 받아야 하고 임시직원이나 외부자에게 정보시스템에 대한 접근권한을 부여할 경우에도 비밀유지서약서를 받아야 한다.
		6.2	인사규정	6.2.1	퇴직 및 직무변경 관리	퇴직 및 직무변경 시 인사부서와 정보보호 및 시스템 운영 부서 등 관련 부서에서 이행해야 할 자산반납, 접근권한 회수·조정, 결과 확인 등의 절차를 수립하여야 한다.
				6.2.2	상벌규정	인사규정에 직원이 정보보호 책임과 의무를 충실히 이행했는지 여부 등 정보보호 활동 수행에 따른 상벌 규정을 포함하여야 한다.

	통제분야		통제목적		통제사항	통제내용
7	물리적 보안	7.1	물리적 보호구역	7.1.1	보호구역 지정	비인가자의 물리적 접근 및 각종 물리적, 환경적 재난으로부터 주요 설비 및 시스템을 보호하기 위하여 통제구역, 제한구역, 접견구역 등 물리적 보호구역을 지정하고 각 구역별 보호대책을 수립·이행하여야 한다.
				7.1.2	보호설비	각 보호구역의 중요도 및 특성에 따라 화재, 전력이상 등 인·재해에 대비하여 온습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 설비를 충분히 갖추고 운영절차를 수립하여 운영하여야 한다. 또한 주요 시스템을 외부 집적정보통신시설에 위탁운영하는 경우 관련 요구사항을 계약서에 반영하고 주기적으로 검토를 수행하여야 한다.
				7.1.3	보호구역 내 작업	유지보수 등 주요 설비 및 시스템이 위치한 보호구역 내에서의 작업 절차를 수립하고 작업에 대한 기록을 주기적으로 검토하여야 한다.
				7.1.4	출입통제	보호구역 및 보호구역 내 주요 설비 및 시스템은 인가된 사람만이 접근할 수 있도록 출입을 통제하고 책임추적성을 확보할 수 있도록 출입 및 접근 이력을 주기적으로 검토하여야 한다.
				7.1.5	모바일 기기 반출입	노트북 등 모바일 기기 미승인 반출입을 통한 중요정보 유출, 내부망 악성코드 감염 등의 보안사고 예방을 위하여 보호구역 내 임직원 및 외부자 모바일 기기 반출입 통제절차를 수립하고 기록·관리하여야 한다.
		7.2	시스템 보호	7.2.1	케이블 보안	데이터를 송수신하는 통신케이블이나 전력을 공급하는 전력 케이블은 손상을 입지 않도록 보호하여야 한다.
				7.2.2	시스템 배치 및 관리	시스템은 그 특성에 따라 분리하여 배치하고 장애 또는 보안사고 발생 시 주요 시스템의 위치를 즉시 확인할 수 있는 체계를 수립하여야 한다.

	통제분야		통제목적		통제사항	통제내용
		7.3	사무실 보안	7.3.1	개인업무 환경 보안	일정시간 동안 자리를 비울 경우에는 책상 위에 중요한 문서나 저장매체를 남겨놓지 않고 컴퓨터 화면에 중요정보가 노출되지 않도록 화면보호기 설정, 패스워드 노출 금지 등 보호대책을 수립하여야 한다.
				7.3.2	공용업무 환경 보안	사무실에서 공용으로 사용하는 사무처리 기기, 문서고, 공용 PC, 파일서버 등을 통해 중요정보 유출이 발생하지 않도록 보호대책을 마련하여야 한다.
8	시스템 개발보안	8.1	분석 및 설계 보안관리	8.1.1	보안 요구사항 정의	신규 정보시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안취약점, 정보보호 기본요소(기밀성, 무결성, 가용성) 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용하여야 한다.
				8.1.2	인증 및 암호화 기능	정보시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입·출력 및 송수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다.
				8.1.3	보안로그 기능	정보시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 하여야 한다.
				8.1.4	접근권한 기능	정보시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다.

	통제분야		통제목적		통제사항	통제내용
8	시스템 개발 보안	8.2	구현 및 이관 보안	8.2.1	구현 및 시험	안전한 코딩방법에 따라 정보시스템을 구현 하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다. 또한 알려진 기술적 보안 취약성에 대한 노출여부를 점검하고 이에 대한 보안대책을 수립하여야 한다.
				8.2.2	개발과 운영 환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다.
				8.2.3	운영환경 이관	운영환경으로의 이관은 통제된 절차에 따라 이루어져야 하고 실행코드는 시험과 사용자 인수 후 실행하여야 한다.
				8.2.4	시험 데이터 보안	시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다.
				8.2.5	소스 프로그램 보안	소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행하여야 한다. 또한 소스 프로그램은 운영환경에 보관하지 않는 것을 원칙으로 한다.
		8.3	외주개발 보안	8.3.1	외주개발 보안	정보시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독하여야 한다.

	통제분야		통제목적		통제사항	통제내용
9	암호통제	9.1	암호 정책	9.1.1	암호 정책 수립	조직의 중요정보 보호를 위하여 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 수립하고 이행하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.
		9.2	암호키 관리	9.2.1	암호키 생성 및 이용	암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고 필요 시 복구방안을 마련하여야 한다.
10	접근 통제	10.1	접근통제 정책	10.1.1	접근통제 정책 수립	비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다.
		10.2	접근권한 관리	10.2.1	사용자 등록 및 권한부여	정보시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다.
				10.2.2	관리자 및 특수 권한 관리	정보시스템 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.
				10.2.3	접근권한 검토	정보시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 점검하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.3	사용자 인증 및 식별	10.3.1	사용자 인증	정보시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제되어야 하고, 필요한 경우 법적요구사항 등을 고려하여 중요 정보시스템 접근 시 강화된 인증방식을 적용하여야 한다.
				10.3.2	사용자 식별	정보시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다. 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.
				10.3.3	사용자 패스워드 관리	법적요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경주기 등 사용자 패스워드 관리절차를 수립·이행하고 패스워드 관리 책임이 사용자에게 있음을 주지시켜야 한다. 특히 관리자 패스워드는 별도 보호대책을 수립하여 관리하여야 한다.
				10.3.4	이용자 패스워드 관리	고객, 회원 등 외부 이용자가 접근하는 정보시스템 또는 웹서비스의 안전한 이용을 위하여 계정 및 패스워드 등의 관리절차를 마련하고 관련 내용을 공지하여야 한다.
		10.4	접근통제 영역	10.4.1	네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 접근통제 리스트, 네트워크 식별자 등에 대한 관리절차를 수립하고 서비스, 사용자 그룹, 정보자산의 중요도에 따라 내·외부 네트워크를 분리하여야 한다.
				10.4.2	서버 접근	서버별로 접근이 허용되는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 적용하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.4	접근통제 영역	10.4.3	응용 프로그램 접근	사용자의 업무 또는 직무에 따라 응용프로그램 접근권한을 제한하고 불필요한 중요정보 노출을 최소화해야 한다.
				10.4.4	데이터베이스 접근	데이터베이스 접근을 허용하는 응용프로그램 및 사용자 직무를 명확하게 정의하고 응용프로그램 및 직무별 접근통제 정책을 수립하여야 한다. 또한 중요정보를 저장하고 있는 데이터베이스의 경우 사용자 접근내역을 기록하고 접근의 타당성을 정기적으로 검토하여야 한다.
				10.4.5	모바일 기기 접근	모바일기기를 업무 목적으로 내·외부 네트워크에 연결하여 활용하는 경우 중요정보 유출 및 침해사고 예방을 위해 기기 인증 및 승인, 접근 범위, 기기 보안설정, 오남용 모니터링 등의 접근통제 대책을 수립하여야 한다.
				10.4.6	인터넷 접속	인사정보, 영업비밀, 산업기밀, 개인정보 등 중요정보를 대량으로 취급·운영하는 주요직무자의 경우 인터넷 접속 또는 서비스(P2P, 웹메일, 웹하드, 메신저 등)를 제한하고 인터넷 접속은 침입차단시스템을 통해 통제하여야 한다. 필요시 침입탐지시스템 등을 통해 인터넷 접속내역을 모니터링하여야 한다.
11	운영보안	11.1	운영 절차 및 변경 관리	11.1.1	운영절차 수립	정보시스템 동작, 문제 발생 시 재 동작 및 복구, 오류 및 예외사항 처리 등 시스템 운영을 위한 절차를 수립하여야 한다.
				11.1.2	변경관리	정보시스템 관련 자산의 모든 변경내역을 관리할 수 있도록 절차를 수립하고 변경 전 시스템의 전반적인 성능 및 보안에 미치는 영향을 분석하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영보안	11.2	시스템 및 서비스 운영 보안	11.2.1	정보 시스템 인수	새로운 정보시스템 도입 또는 개선 시 필수 보안요구사항을 포함한 인수 기준을 수립하고 인수 전 기준 적합성을 검토하여야 한다.
				11.2.2	보안 시스템 운영	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립하고 보안시스템 별 정책적용 현황을 관리하여야 한다.
				11.2.3	성능 및 용량관리	정보시스템 및 서비스 가용성 보장을 위해 성능 및 용량 요구사항을 정의하고 현황을 지속적으로 모니터링할 수 있는 방법 및 절차를 수립하여야 한다.
				11.2.4	장애관리	정보시스템 장애 발생 시 효과적으로 대응하기 위한 탐지, 기록, 분석, 복구, 보고 등의 절차를 수립하여야 한다.
				11.2.5	원격운영 관리	내부 네트워크를 통하여 정보시스템을 관리하는 경우 특정 단말에서만 접근을 할 수 있도록 제한하고, 원격지에서 인터넷 등 외부 네트워크를 통하여 정보시스템을 관리하는 것은 원칙적으로 금지하고 부득이한 사유로 인해 허용하는 경우에는 책임자 승인, 접속 단말 및 사용자 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등의 보호대책을 수립하여야 한다.
				11.2.6	스마트 워크 보안	재택근무, 원격협업 등과 같은 원격 업무 수행 시 이에 대한 관리적·기술적 보호대책을 수립하고 이행하여야 한다.
				11.2.7	무선네트워크 보안	무선랜 등을 통해 무선인터넷을 사용하는 경우 무선 네트워크 구간에 대한 보안을 강화하기 위해 사용자 인증, 송수신 데이터 암호화 등의 보호대책을 수립하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영보안			11.2.8	공개서버 보안	웹사이트 등에 정보를 공개하는 경우 정보 수집, 저장, 공개에 따른 허가 및 게시절차를 수립하고 공개서버에 대한 물리적, 기술적 보호대책을 수립하여야 한다.
				11.2.9	백업관리	데이터의 무결성 및 정보시스템의 가용성을 유지하기 위해 백업 대상, 주기, 방법 등의 절차를 수립하고 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다.
				11.2.10	취약점 점검	정보시스템이 알려진 취약점에 노출되어 있는 지 여부를 확인하기 위하여 정기적으로 기술적 취약점 점검을 수행하고 발견된 취약점들은 조치하여야 한다.
		11.3	전자거래 및 정보전송 보안	11.3.1	전자거래 보안	전자거래 서비스 제공 시 정보유출, 데이터 조작, 사기 등의 침해사고를 예방하기 위해 사용자 인증, 암호화, 부인방지 등의 보호대책을 수립하고 결제시스템 등 외부 시스템과의 연계가 필요한 경우 연계 안전성을 점검하여야 한다.
				11.3.2	정보전송 정책 수립 및 협약 체결	타 조직에 중요정보를 전송할 경우 안전한 전송을 위한 정책을 수립하고 조직 간 정보전송 합의를 통해 관리책임, 전송 기술 표준, 중요정보의 보호를 위한 기술적 보호조치 등을 포함한 협약서를 작성하여야 한다.
		11.4	매체 보안	11.4.1	정보 시스템 저장매체 관리	정보시스템 폐기 또는 재사용 시 중요정보를 담고 있는 하드디스크, 스토리지, 테잎 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제하여야 한다.
				11.4.2	휴대용 저장매체 관리	조직의 중요정보 유출을 예방하기 위해 외장하드, USB, CD 등 휴대용 저장매체 취급, 보관, 폐기, 재사용에 대한 절차를 수립하여야 한다. 또한 매체를 통한 악성코드 감염 방지 대책을 마련하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영보안	11.5	악성코드 관리	11.5.1	악성코드 통제	바이러스, 웜, 트로이목마 등의 악성코드로부터 정보시스템을 보호하기 위해 악성코드 예방, 탐지, 대응 등의 보호대책을 수립하여야 한다.
				11.5.2	패치관리	소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인해 발생할 수 있는 침해사고를 예방하기 위해 최신 패치를 정기적으로 적용하고 필요한 경우 시스템에 미치는 영향을 분석하여야 한다.
		11.6	로그관리 및 모니터링	11.6.1	시각 동기화	로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 정보시스템 시각을 공식 표준시각으로 정확하게 동기화 하여야 한다.
				11.6.2	로그 기록 및 보존	정보시스템, 응용프로그램, 보안시스템, 네트워크 장비 등 기록해야 할 로그 유형을 정의하여 일정기간 보존하고 주기적으로 검토하여야 한다. 보존기간 및 검토주기는 법적요구사항을 고려하여야 한다.
				11.6.3	접근 및 사용 모니터링	중요정보, 정보시스템, 응용프로그램, 네트워크 장비에 대한 사용자 접근이 업무상 허용된 범위에 있는 지 주기적으로 확인하여야 한다.
				11.6.4	침해시도 모니터링	외부로부터의 침해시도를 모니터링하기 위한 체계 및 절차를 수립하여야 한다.
12	침해사고 관리	12.1	절차 및 체계	12.1.1	침해사고 대응절차 수립	DDoS 등 침해사고 유형별 중요도 분류, 유형별 보고·대응·복구 절차, 비상연락체계, 훈련 시나리오 등을 포함한 침해사고 대응 절차를 수립하여야 한다.
				12.1.2	침해사고 대응체계 구축	침해사고 대응이 신속하게 이루어질 수 있도록 중앙 집중적인 대응체계를 구축하고 외부기관 및 전문가들과의 협조체계를 수립하여야 한다.
		12.2	대응 및 복구	12.2.1	침해사고 훈련	침해사고 대응 절차를 임직원들이 숙지할 수 있도록 시나리오에 따른 모의훈련을 실시하여야 한다.

	통제분야		통제목적		통제사항	통제내용
12	침해사고 관리	12.2	대응 및 복구	12.2.2	침해사고 보고	침해사고 징후 또는 사고 발생을 인지한 때에는 침해사고 유형별 보고 절차에 따라 신속히 보고하고 법적 통지 및 신고 의무를 준수하여야 한다.
				12.2.3	침해사고 처리 및 복구	침해사고 대응절차에 따라 처리와 복구를 신속하게 수행하여야 한다.
		12.3	사후관리	12.3.1	침해사고 분석 및 공유	침해사고가 처리되고 종결된 후 이에 대한 분석을 수행하고 그 결과를 보고하여야 한다. 또한 사고에 대한 정보와 발견된 취약점들을 관련 조직 및 임직원들과 공유하여야 한다.
				12.3.2	재발방지	침해사고로부터 얻은 정보를 활용하여, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하고 이를 위해 필요한 경우 정책, 절차, 조직 등의 대응체계를 변경하여야 한다.
13	IT 재해복구	13.1	체계 구축	13.1.1	IT 재해복구 체계 구축	자연재앙, 해킹, 통신장애, 전력중단 등의 요인으로 인해 IT 시스템 중단 또는 파손 등 피해가 발생할 경우를 대비하여 비상 시 복구조직, 비상연락체계, 복구절차 등 IT 재해복구 체계를 구축하여야 한다.
		13.2	대책 구현	13.2.1	영향분석에 따른 복구대책 수립	조직의 핵심 서비스 연속성을 위협할 수 있는 IT 재해 유형을 식별하고 유형별 예상 피해규모 및 영향을 분석하여야 한다. 또한 IT 서비스 및 시스템 복구목표시간, 복구시점을 정의하고 적절한 복구전략 및 대책을 수립·이행하여야 한다.
				13.2.2	시험 및 유지관리	IT 서비스 복구전략 및 대책에 따라 효과적인 복구가 가능한 지 시험을 실시하고 시험계획에는 시나리오, 일정, 방법, 절차 등을 포함하여야 한다. 또한 시험결과, IT 환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완하여야 한다.

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제1호서식] <개정 2013.8.8>

정보보호 관리체계 인증기관 지정 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	처리기간	3개월이내

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	총 직원 수	인증심사원 직원 수	
신청구분	☐ 신규	☐ 재지정	
인증에 관한 업무의 범위			

「정보보호 관리체계 인증 등에 관한 고시」 제3조제2항의 규정에 따라 위와 같이 정보보호 관리체계 인증기관 지정을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

미래창조과학부 귀중

신청인 제출서류	1. 정관 또는 규약 1부. 2. 별지 제2호서식의 인증심사원의 보유현황과 이를 증명할 수 있는 서류 1부. 3. 별표 1에 따른 업무수행 요건·능력 심사를 위하여 필요한 서류 1부.	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

처 리 절 차

신청서 작성	→	접 수	→	심 사	→	지정여부 결정	→	지정서 교부
신청인		처리기관 (미래창조과학부)		처리기관 (미래창조과학부)		처리기관 (미래창조과학부)		처리기관 (미래창조과학부)

210㎜×297㎜[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제2호서식] <개정 2013. 8. 8>

인증심사원의 보유현황

(제1쪽)

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	직원 수	인증심사원 직원 수	

일련번호	성명	주소		최종학력	해당요건
		생년월일	입사일	취득학위 및 학과	

유의사항

1. 「해당요건」란에는 선임심사원, 심사원, 심사원보 요건을 기재한다.
2. 기재된 최종학위를 증명할 수 있는 직원의 졸업 또는 학위증명서 사본을 제출하여야 한다.
3. 별표 3의 「인증 심사원 학력 및 경력 요건」을 충족하는 직원은 기술자격증 사본 등 자격을 취득하였음을 확인할 수 있는 서류를 함께 제출하여야 한다.
4. 정보통신유관경력 또는 정보보호유관경력을 증명할 수 있는 경력증명서(근무부서 또는 담당업무 등이 기재되어야 한다)와 해당 직원이 신청업체에 현재 근무하고 있음을 확인할 수 있는 재직증명서를 함께 제출하여야 한다.

210mm×297mm[백상지(80g/㎡)]

인증심사업무를 전담하는 직원의 보유현황

(제2쪽)

일련번호	성명	주소		최종학력	해당요건
		생년월일	입사일	취득학위 및 학과	

10mm×297mm[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제3호서식] <개정 2013.8.8> (제1쪽)

정보보호 관리체계 인증기관 지정서

등록번호 :

업체명 :

대표자 :

주소 :

지정의 유효기간 :

인증업무의 범위 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제5항 및 같은 법 시행령 제53조의2에 따라 위와 같이 정보보호 관리체계 인증기관으로 지정합니다.

년 월 일

미래창조과학부장관 직인

210mm×297mm[백상지(120g/㎡)]

(제2쪽)

CERTIFICATE OF DESIGNATION
AS
ISMS Certification Authority

Registry Number :

Name of Organization :

Name of Representative :

Address :

Period of Validity :

Scope of Certification work :

This is to certify that the abovementioned organization is designated Information Security Management System (ISMS) Certification Authority in accordance with Article 47, Paragraph 5 of 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」 and Article 53-2 of the Enforcement Decree of the same Act.

Date of Issuance:

Signed by the
Minister of Ministry of Science, ICT and Future Planning
Republic of Korea

210㎜×297㎜[백상지 120g/㎡]

■「정보보호 관리체계 인증 등에 관한 고시」 [별지 제4호서식] <개정 2013.8.8>

인증실적 보고서

정보보호 관리체계 인증기관	업체명		사업자등록번호	
	주소		전화번호	
	대표자			
	정보보호 관리체계 인증심사 실적 총계	최초심사	외	건
		사후관리심사	외	건

일련번호	인증 번호	대상기관(기업)명	인증범위	유효기간	구분	
					최초심사	사후관리심사

년 월 일

신청인(대표자) (서명 또는 인)

미래창조과학부 귀중

신청(신고)인 제출서류	1. 정보보호 관리체계 인증기관 지정서 1부.	수수료 없음

처 리 절 차

신청서 작성	→	접 수	→	검 토	→	심 사	→	지정서 교부
신청인		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)

210㎜×297㎜[백상지(80g/㎡)]

■「정보보호 관리체계 인증 등에 관한 고시」 [별지 제5호서식] <개정 2013.8.6> (제1쪽)

정보보호 관리체계 인증심사원 자격 신청서

신청자 인적사항	성 명		생년월일		사진	
	주 소	(우: -)				
	회 사 명					
	회사주소	(우: -)				
	이 메 일					
	전화번호		휴대전화			
신청사항	신청 구분	□ 자격인증 □ 전문분야 변경				
학력사항	최종학력	□ 고졸	□ 전문학사	□ 학사	□ 석사	□ 박사
	학사	전공		기간		
	석사	전공		기간		
	박사	전공		기간		
인증심사원 교육이수	교육기간	년 월 일 ~ 년 월 일		수료증번호		

자격사항 ※해당자에 한함	자격증번호	자격증명/등급	취득일자	수여기관

경력사항 ※최근 10년 내 경력사항 기술	총 경력	정보기술	총 년 개월	정보보호	총 년 개월

No.	구분	기간	회사명	부서	직책
1	□정보기술 □정보보호	~ (년 개월)			
2	□정보기술 □정보보호	~ (년 개월)			
3	□정보기술 □정보보호	~ (년 개월)			
4	□정보기술 □정보보호	~ (년 개월)			
5	□정보기술 □정보보호	~ (년 개월)			

※ 칸이 부족할 경우 추가 작성

(제2쪽)

(1) 개인별 전문분야 (복수 선택 가능, 우선순위 표기요망)					
대분류	중분류	소분류	순위	실무경력	
관리적 정보 보호	정책, 조직 및 인적보안	정보보호정책수립 및 조직구성			년
		인적보안, 외부자 보안, 외부위탁관리			년
		정보보호교육 및 훈련			년
		국내외 표준 기준 및 법령			년
	위험관리	자산분류, 위험평가 수행, 대책 및 계획수립			년
	업무연속성관리	업무연속성 계획수립 및 시험, 유지관리			년
	침해사고대응	침해사고 대응계획 및 체계, 복구			년
	정보시스템 감사/감리	정보시스템 및 정보보호시스템 감사/감리			년
기술적 정보 보호	네트워크	네트워크 설계기술			년
		라우팅 제어, 프로토콜 제어, 접근통제, 암호화, NAT, 운용관리(로그, SNMP, 설정도구)등 통신기술			년
		라우터, 스위치(L2~L7), RAS, VPN, SSL, DHCP, 네트워크 감시 등 기기기술			년
		기타( )			년
	운영체제 및 시스템	OS 기본지식, 계정관리, 접근권한, 서비스관리, 로그관리, 패치, 보안 S/W 사용 등 유닉스/리눅스 시스템			년
		OS 기본지식, 계정관리, 접근권한, 서비스관리, 로그관리, 패치, 보안 S/W 사용 등 윈도우 시스템			년
		메인프레임 등 기타( )			년
	응용서비스	HTTP 프로토콜, 브라우저, SQL-Injection 등 Web 위협에 대한 대응책, SSL, CGI 보안 프로그래밍 등 Web 서비스			년
		부하분산, DNSSEC, 보안설정 등 DNS 서비스			년
		메일 프로토콜, 스팸대응, 윔/바이러스 필터링 등 메일 서비스			년
		DB 기본지식, 이중화, 데이터백업, 암호화 등 데이터베이스			년
		ERP, KMS, CRM 등 사내정보시스템			년
		분산시스템 등 기타( )			년
	정보보호 솔루션	FW 기본지식, 접근통제, 라우팅, 네트워크 정책설계, 구성(이중화, 망분리, 로드밸런싱 등) 등 침입차단시스템			년
		윔/바이러스 기본지식, 윔/바이러스별 감염 증상과 대책 등 바이러스 월			년
		IDS 기본지식, 방화벽 연동, 패턴 매칭 방법, 구성(에이전트 위치, 통합콘솔 등) 등 침입탐지시스템			년
		SecureOS 기본지식, 계정관리, 접근권한, 서비스관리, 로그관리, 패치 등 SecureOS			년
		기타( )			년

(제3쪽)

(1) 개인별 전문분야 (복수 선택 가능, 우선순위 표기요망) (계속)					
대분류	중분류	소분류	순위	실무경력	
기술적 정보 보호 (계속)	취약성분석	사회공학적 방법, 스캔, Sniffing, DOS, Buffer Overflow, 윔/바이러스, 백도어 등 취약성 분석 및 점검			년
	보안 운영	통합관제(ESM, NMS 등), 망관리, 백업, 로그 분석, 모니터링, 패치, 문제해결(원인규명)			년
	기반기술	IPSec, PPTP, L2TP, SSH, SSL/TLS, MPLS, IKE, S/MIME, PGP 등 보안 프로토콜			년
		패스워드인증, 생체인증, 인증디바이스, 인증프로토콜, WEB인증, RADIUS, SSO 등 인증기술			년
		증명서 인증 및 실효, 신뢰모델, 기술 및 데이터방식, 인증센터 구축과 운영, 법적구조 등 PKI			년
		암호알고리즘, Key 관리, 암호방식 등 암호기술			년
		디지털서명, 디지털 봉투, 코드 서명			년
물리적 정보 보호	접근보안	출입 및 접근통제, 모니터링 등			년
	시설관리	소방시설, 비상전원, 비상조명, 항온항습 등			년
개인정보보호		개인정보보호 책임자, 취급자, 컨설턴트, 법률 담당, 소비자 민원 및 상담 등			년
기타		( )			년

※ 경력 및 전문 분야에 대한 관련 내용을 상세히 기술
※ 칸이 부족할 경우 별지 사용

No.	상세내용
1	
2	
3	
4	
5	
6	

(제4쪽)

(2) 통제분야별 전문분야 (5순위까지 선택, 우선순위 표기요망)

통제분야	순위	실무경력		통제분야	순위	실무경력	
1. 정보보호정책			년	9. 암호통제			년
2. 정보보호조직			년	10. 접근통제			년
3. 외부자 보안			년	11. 운영관리			년
4. 정보자산분류			년	12. 전자거래보안			년
5. 정보보호교육 및 훈련			년	13. 보안사고관리			년
6. 인적 보안			년	14. 검토, 모니터링 및 감사			년
7. 물리적 보안			년	15. 업무연속성 관리			년
8. 시스템개발 보안			년	16. 개인정보보호			년

관련 경력기술

※ 5순위까지 선택한 전문분야 관련 실무경력, 전문기술, 인증심사실적 등 관련경력을 상세히 기술

<개인정보 수집·이용>

o 개인정보 수집 이용 목적 : 정보보호 관리체계(ISMS) 인증심사원 양성 교육, 자격부여 및 관리, 자문료 지급, 심사팀구성

o 수집하는 개인정보 항목 : 성명, 생년월일, 주소, 이메일, 전화번호, 학력, 자격경력, 발령사항, 기술실적사항

o 보유 및 이용기간 : 인증심사원 자격 종료시까지

o 개인정보의 수집·이용을 거부할 수 있으며, 이 경우 인증심사원 등록 및 위촉에 불이익이 발생할 수 있음을 알려드립니다.

▷ 개인정보 수집·이용 동의여부 **동의 □** **미동의 □**

<인증심사원 의무사항>

- 인증심사원은 객관적이고 공정한 인증심사를 수행한다.
- 인증심사원으로서의 성실한 직무수행 및 품위유지를 한다.
- 인증심사와 관련된 부당한 금전, 금품 등의 수수를 금지한다.
- 인증심사의 수행에서 취득한 정보를 관련 법령 또는 신청기관의 동의 없이 외부에 누설하여서는 안된다.
- 인증심사원은 인증업무지침을 성실히 준수한다.
- 인증심사원은 본인이 ISMS 인증 취득을 위한 컨설팅을 수행한 기업에 대하여는 인증심사에 참여할 수 없다.
- 인증심사원은 인증심사의 수행과 관련하여 상업적, 재정적 그리고 기타 모든 압력으로부터 배제되어야 한다.

1. 위의 인증심사원 의무사항을 읽고 이해하였으며, 성실히 준수하겠습니다.
2. 본 신청서의 기재사항은 사실과 틀림없으며, 만약 허위로 판명될 경우에는 자격취소 등 불이익을 감수하겠습니다.

※ 필요시 학력, 경력 등 증빙서류 제출을 요청받을 수 있으며 반드시 이에 응해야 함

위와 같이 인증심사원 자격을 신청합니다.

년 월 일

신청자		(서명 또는 인)

한국인터넷진흥원 귀중

■「정보보호 관리체계 인증 등에 관한 고시」 [별지 제6호서식] <개정 2013.8.8>

경력증명서

인적사항	성명		생년월일	
	주소		연락처	

경력사항	전 근무처 명				
	근무기간		부서	직위	담당업무
	부터	까지			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			

근무년수	년 개월	최종직위	
용도	정보보호 관리체계 인증심사원 자격 신청		

위와 같이 경력을 증명합니다.

년 월 일

회사명

대표자 (서명 또는 인)

확인자	성명	부서	연락처	비고

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제7호서식] <개정 2013.8.8>

상세 재직증명서

인적사항	성명		생년월일	
	주소		연락처	
소속사항	회사명			
	부서		직위	
	근속기간	~	근무년수	년 개월

발령사항	근무기간		부서	직위	담당업무
	부터	까지			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			

용도	정보보호 관리체계 인증심사원 자격 신청

위와 같이 재직하고 있음을 증명합니다.

년 월 일

회사명

대표자 (서명 또는 인)

확인자	성명	부서	연락처	비고

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제8호서식] <개정 2013.8.8>

기술실적증명서

<table>
<tr><td rowspan="2">인적사항</td><td>성명</td><td colspan="2"></td><td>생년월일</td><td></td></tr>
<tr><td>주소</td><td colspan="2"></td><td>연락처</td><td></td></tr>
<tr><td rowspan="13">실적사항</td><td>소속</td><td colspan="4"></td></tr>
<tr><td colspan="2">수행기간</td><td rowspan="2">참여사업명</td><td rowspan="2">발주처</td><td rowspan="2">담당업무</td></tr>
<tr><td>부터</td><td>까지</td></tr>
<tr><td>. .</td><td>. .</td><td></td><td></td><td></td></tr>
<tr><td>. .</td><td>. .</td><td></td><td></td><td></td></tr>
<tr><td>. .</td><td>. .</td><td></td><td></td><td></td></tr>
<tr><td>. .</td><td>. .</td><td></td><td></td><td></td></tr>
<tr><td>. .</td><td>. .</td><td></td><td></td><td></td></tr>
<tr><td>. .</td><td>. .</td><td></td><td></td><td></td></tr>
<tr><td>. .</td><td>. .</td><td></td><td></td><td></td></tr>
<tr><td>. .</td><td>. .</td><td></td><td></td><td></td></tr>
<tr><td>. .</td><td>. .</td><td></td><td></td><td></td></tr>
<tr><td>. .</td><td>. .</td><td></td><td></td><td></td></tr>
<tr><td>용도</td><td colspan="5">정보보호 관리체계 인증심사원 자격 신청</td></tr>
<tr><td colspan="6">위와 같이 기술실적을 증명합니다.
년 월 일

회사명
대표자 (서명 또는 인)</td></tr>
<tr><td rowspan="2">확인자</td><td>성명</td><td>부서</td><td>연락처</td><td colspan="2">비고</td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="6"></td></tr>
</table>

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제9호서식] <개정 2013.8.8>

제 호

인증심사원 자격 증명서

성 명 : (. . .)

인증심사원 등급 :

유효기간 :

※ 인증심사원 유지조건을 만족하지 못할 경우 자격이 취소될 수 있습니다.

귀하에게 정보보호 관리체계 인증심사원 자격을 부여합니다.

년 월 일

한국인터넷진흥원 원장 직인

210mm×297mm[백상지(120g/㎡)]

■「정보보호 관리체계 인증 등에 관한 고시」 [별지 제10호서식] <개정 2013.8.8>

정보보호 관리체계 인증 신청서

※ [ ]에는 해당되는 곳에 √표를 하고, 어두운 부분은 신청인이 작성하지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명	사업자등록번호
	주소	전화번호
	대표자	

인증신청의 구분	[ ]최초심사 [ ]사후심사 [ ]갱신심사
정보보호 관리체계의 범위	
정보보호 관리체계의 범위에 포함되어 있는 종업원의 수	
정보보호 관리체계의 범위에 포함되어 있는 서버의 수	

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제9항, 같은 법 시행령 제47조에 따라 위와 같이 정보보호 관리체계의 인증을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

(한국인터넷진흥원 또는 정보보호 관리체계 인증기관명) 귀중

신청(신고)인 제출서류	정보보호 관리체계의 내역서 1부.	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

210mm×297mm[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제11호서식] <개정 2013.8.8> (제1쪽)

정보보호 관리체계 인증서

인증번호 :

업체명 :

대표자 :

주소 :

인증의 범위 :

유효기간 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제9항, 같은 법 시행령 제47조에 따라 위와 같이 정보보호 관리체계를 인증합니다.

년 월 일

한국인터넷진흥원 원장
또는 정보보호 관리체계
인증기관 장

직인

210mm×297mm[백상지(120g/㎡)]

(제2쪽)

CERTIFICATE
OF
Information Security Management System

Certificate Number :

Name of Organization :

Name of Representative :

Address :

Scope of Certification :

Period of Validity :

This is to certify that the abovementioned organization is compliant to the assessment standard for Information Security Management System certification in accordance with Article 47, Paragraph 1 and 9 of 「Act on Information Network Utilization and Data Protection, etc.」 and Article 47 of the Enforcement Decree of the same Act.

Date of Issuance :

Signed by the
President of Korea Internet & Security Agency or certification body

210㎜×297㎜[백상지(120g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제12호서식] <개정 2013.8.8>

정보보호 관리체계 인증서 추가발급 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명	사업자등록번호
	주소	전화번호
	대표자	
추가발급 사유		

위와 같이 정보보호 관리체계 인증서의 추가발급을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

한국인터넷진흥원 또는 정보보호 관리체계 인증기관명 귀중

제출서류	해당없음	수수료 없 음

210mm×297mm[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제13호서식] <개정 2013.8.8>

정보보호 관리체계 인증서 변경 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		

변경 내용	변경전	(국문)
		(영문)
	변경후	(국문)
		(영문)
변경사유		

위와 같이 정보보호 관리체계 인증서 변경을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

한국인터넷진흥원 또는 정보보호 관리체계 인증기관명 귀중

제출서류	해당없음	수수료 없 음

210mm×297mm[백상지(80g/㎡)]

정보보호 관리체계 인증 등에 관한 고시

[시행 2013.2.18] [고시 제2013 - 4호, 2013.1.17, 전부개정]

제1장 총칙

제1조(목적) 이 고시는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) 제47조제3항 및 같은 법 시행령(이하 "영"이라 한다) 제47조부터 제53조의2의 규정에 따라 정보보호 관리체계 인증에 관하여 필요한 사항에 대해 정하는 것을 목적으로 한다.

제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "정보보호 관리체계 인증기관(이하 ‘ 인증기관 ’ 이라 한다)"이란 법 제47조제5항에 따라 방송통신위원회가 인증에 관한 업무를 수행할 수 있도록 지정한 기관을 말한다.
2. "업무수행 요건·능력 심사"란 인증기관으로 지정받고자 신청한 법인 또는 단체의 업무수행 요건·능력을 별표 2의 세부기준에 따라 심사하는 것을 말한다.
3. "인증"이란 신청기관이 수립하여 운영하고 있는 정보보호 관리체계가 별표 6의 정보보호 관리체계 인증기준(이하 "인증기준"이라 한다)에 적합함을 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다) 또는 인증기관이 증명하는 것을 말한다.
4. "인증심사"란 신청기관이 수립하여 운영하는 정보보호 관리체계가 인증기준에 적합한지의 여부를 인터넷진흥원 또는 인증기관이 서면심사 및 현장심사의 방법으로 확인하는 것을 말한다.
5. "정보보호관리과정(이하 ‘ 관리과정 ’ 이라 한다)"이란 정보보호 관리체계를 수립·운영하기 위하여 유지·관리하여야 할 과정으로 다음 각 목의 5단계 활동을 말한다.
   가. 정보보호정책 수립 및 범위설정
   나. 경영진 책임 및 조직구성
   다. 위험관리
   라. 정보보호대책 구현
   마. 사후관리
6. "정보보호대책"이란 신청기관이 정보보호 관리체계를 수립·운영하기 위하여 별표 6에서 선택한 통제사항을 말한다.
7. "신청기관"이란 이 고시에 따라 정보보호 관리체계 인증을 취득하고자 신청한 자를 말한다.

8. "인증심사원"이란 별표 3의 자격요건을 갖춘 자를 말한다.
9. "최초심사"란 처음으로 인증을 신청하거나 인증의 범위에 중요한 변경이 있어서 다시 인증을 신청한 때 실시하는 인증심사를 말한다.
10. "사후심사"란 정보보호 관리체계 인증(인증이 갱신된 경우를 포함한다)을 받고난 후 매년 사후관리를 위하여 실시하는 인증심사를 말한다.
11. "갱신심사"란 유효기간 만료로 다시 인증을 신청한 때 실시하는 인증심사를 말한다.

제2장 정보보호 관리체계 인증기관

제3조(인증기관의 지정 등) ① 방송통신위원회는 법 제47조제5항 및 영 제53조의2에 따라 인증기관을 지정할 필요가 있는 때에는 지정대상 기관의 수, 업무의 범위 및 신청방법 등을 정하여 관보 및 인터넷 홈페이지에 20일 이상 공고하여야 한다.

② 제1항에 따라 인증기관으로 지정받으려는 자는 다음 각 호의 서류를 방송통신위원회에 제출하여야 한다.

1. 별지 제1호서식의 정보보호 관리체계 인증기관 지정 신청서
2. 영 제53조의2제1항제2호에 따른 별지 제2호서식의 인증심사원 보유현황과 이를 증명할 수 있는 서류
3. 영 제53조의2제1항제3호에 따른 별표 1의 업무수행 요건·능력 심사를 위하여 필요한 서류

제4조(업무수행 요건·능력 심사 세부기준 등) ① 영 제53조제2항에 따른 업무수행 요건·능력 심사를 위한 세부기준은 별표 2와 같다.

② 방송통신위원회는 제3조제2항에 따라 인증기관의 지정 신청을 받은 때에는 제1항에 따라 업무수행 요건·능력을 심사하여 지정 대상기관의 순위를 정한다.

제5조(업무수행 능력의 적합성 인정) ① 방송통신위원회는 제4조제1항에 따라 업무수행 요건·능력을 심사하여 지정에 필요한 수만큼 점수의 합이 높은 순으로 선별한다.

② 방송통신위원회는 제1항에 따라 심사한 결과를 바탕으로 하여 인증기관으로의 지정 여부를 최종 결정한다.

제6조(인증기관 지정서) 영 제53조의2제3항에 따른 정보보호 관리체계 인증기관 지정서는 별지 제3호서식과 같다.

제7조(인증기관의 사후관리) 영 제53조의4제1항에 따른 인증기관의 전년도 인증실적 보고서는 별지 제4호서식과 같다.

제8조(인증기관 재지정) ① 인증기관은 유효기간이 끝나기 전 6개월부터 끝나는 날까지 별지 제1호서식에 따라 방송통신위원회에 재지정 신청을 할 수 있다.

② 제1항에 따른 재지정의 심사, 재지정 결과 통지, 재지정서 교부 등에 관하여는 영 제53조의2제3항을 준용한다.

제3장 인증심사원의 자격 및 관리

제9조(인증심사원의 자격 요건 등) ① 인증심사원은 심사원보, 심사원, 선임심사원으로 구분하며, 인증심사원 등급별 자격 요건은 별표 3과 같다.

② 인증심사원이 되려는 자는 별표 3의 학력 및 경력 요건을 갖추고 인터넷진흥원이 지정하는 기관에서 인증심사원 양성교육 과정을 수료하여야 한다.

제10조(인증심사원 자격 신청) 인증심사원의 자격을 신청하고자 하는 자는 제9조제2항에 따라 인증심사원 양성교육 과정을 수료한 날로부터 1개월 이내에 인터넷진흥원에 다음 각 호의 모든 서류를 제출하여야 한다.

1. 별지 제5호서식 정보보호 관리체계 인증심사원 자격 신청서
2. 학위증명서, 자격증 사본(해당 시)
3. 별지 제6호서식 경력증명서
4. 별지 제7호서식 상세 재직증명서 등 경력증빙서류
5. 별지 제8호서식 기술실적증명서(해당 시)

제11조(인증심사원 자격 부여) ① 인터넷진흥원은 인증심사원 자격 신청서를 접수한 때에는 신청서류를 검토하여 서류 보완 및 추가제출을 요청할 수 있다.

② 서류 보완 및 추가제출을 요청받은 자격 신청자는 1개월 이내에 관련 서류 등을 제출하여야 한다.

③ 인터넷진흥원은 인증심사원 자격의 적합 여부를 확인하여 통과한 자에게 별지 제9호서식의 인증심사원 자격 증명서를 발급하여야 한다.

제12조(인증심사원 자격 유지) ① 인증심사원의 자격 유효기간은 자격 부여를 받은 날로부터 3년으로 한다.

② 인증심사원은 자격 유지를 위해 유효기간 내에 인터넷진흥원이 지정하는 기관에서 시행하는 인증심사원 보수교육을 이수해야 한다. 다만, 부득이한 사유로 보수교육을 받지 못한 경우에는 인터넷진흥원이 인정하는 대체교육을 받아야 한다.

③ 보수교육을 이수한 자에 한하여 자격 유효기간이 3년간 연장된다.

제13조(인증심사원 자격 취소) ① 인증심사원 자격 신청 시 제출한 서류가 허위이거나, 제12조에 따른 자격 유지 기준을 충족하지 못한 경우에는 자격을 취소한다.

② 인증심사원으로서 객관적이고 공정한 인증심사를 수행하지 않거나, 인증심사와 관련된 부당한 금전, 금품 등을 수수하거나 인증심사 수행 중 취득한 정보를 누설하는 경우에는 자격을 취소한다.

제4장 인증심사의 신청 및 계약

제14조(인증 의무대상자 범위) ① 인증 의무대상자란 법 제47조제2항, 영 제49조에 따라 정보보호 관리체계 인증을 받아야 하는 자를 말한다.

② 법 제47조제2항제2호에 따라 정보보호 관리체계 인증을 받아야 하는 자 중 집적정보통신시설 사업자가 마련한 시설의 일부를 임대하여 집적정보통신시설 사업을 하는 자에 대하여는 영 제49조제2항의 기준을 준용한다.

③ 인증 의무대상자는 매년 1월1일부터 12월31일까지 인증을 받아야 한다.

제15조(신청기관의 사전 준비사항) 신청기관은 정보보호 관리체계 인증을 신청하기 전에 인증기준에 따른 정보보호 관리체계를 구축하여 최소 2개월 이상 운영하여야 한다.

제16조(인증의 신청 등) ① 법 제47조제1항 또는 제2항에 따라 정보보호 관리체계 인증을 받으려는 자는 별지 제10호서식의 정보보호 관리체계 인증 신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

② 신청기관은 인증의 범위 및 일정 등을 인터넷진흥원 또는 인증기관과 사전 협의하여 신청하여야 한다.

③ 인터넷진흥원 또는 인증기관은 제14조에 따른 인증 의무대상자가 사업자 등록일이 속한 분기가 끝나는 날의 1개월 전까지 인증 신청을 한 경우 인증심사를 우선적으로 처리할 수 있다.

제17조(인증심사 계약 체결) 신청기관은 인터넷진흥원 또는 인증기관과 협의한 후 심사기간, 심사인원, 인증 수수료, 인증의 범위 등을 포함하는 인증심사 계약을 체결한다.

제5장 인증심사의 기준과 방법

제18조(인증기준) 인증기준은 별표 6과 같다.

제19조(인증심사팀 구성) ① 인터넷진흥원 또는 인증기관은 제17조에 따른 인증심사 계약을 체결한 때에는 지체 없이 인증심사원으로 인증심사팀을 구성하여야 한다.

② 인증심사팀 구성 시 심사팀장은 인터넷진흥원 또는 인증기관 소속의 심사원 이상으로 선정하여야 한다.

③ 신청기관의 정보보호 관리체계 인증을 위한 컨설팅에 참여한 인증심사원 또는 신청기관의 소속직원은 인증심사팀의 구성원에서 배제하여야 한다.

제20조(인증심사 방법 및 보완조치) ① 인증심사는 신청기관을 방문하여 서면심사와 현장심사를 병행한다.

② 서면심사는 인증기준에 적합한지에 대하여 정보보호 관리체계 구축·운영 관련 정보보호 정책, 지침, 절차 및 이행의 증적자료 검토, 정보보호대책 적용 여부 확인 등의 방법으로 관리

적 요소를 심사한다.

③ 현장심사는 서면심사의 결과와 기술적·물리적 보호대책 이행 여부를 확인하기 위하여 담당자 면담, 관련 시스템 확인 및 취약점 점검 등의 방법으로 기술적 요소를 심사한다.

④ 인터넷진흥원 또는 인증기관은 인증심사에서 발견된 결함에 대해 최대 90일(재조치 요구 60일 포함) 이내에 보완조치를 완료하도록 신청기관에게 요청할 수 있다.

⑤ 인터넷진흥원 또는 인증기관은 인증위원회 심의결과에 따라 30일 이내에 보완조치를 요구할 수 있다.

제6장 인증위원회 구성과 운영

제21조(인증위원회의 구성) ① 법 제47조제5항에 따라 인터넷진흥원 또는 인증기관의 장은 다음 각 호의 사항을 심의·의결하기 위하여 인증위원회를 설치·운영하여야 한다.

1. 최초심사 또는 갱신심사 결과가 인증기준에 적합한지 여부
2. 사후심사 결과 법 제47조제8항 각 호에 해당하는 사유를 발견한 경우에 그 결과의 적합성 여부
3. 그 밖에 정보보호 관리체계 인증과 관련하여 위원장이 필요하다고 인정하는 사항

② 인증위원회는 5인 이상 10인 이내의 위원으로 구성하되, 위원은 정보보호전문가, 정보시스템감리사, 기술사, 대학교수 등 정보보호분야에 학식과 경험이 있는 자 중에서 인터넷진흥원 또는 인증기관의 장이 위촉하며, 위원장은 위원 중에서 호선한다.

③ 위원장은 인증위원회의 업무를 통할하며 위원회를 대표한다.

제22조(인증위원회의 운영) ① 인터넷진흥원 또는 인증기관의 장은 인증위원회의 심의안건을 검토하여 위원회 개최 5일 전까지 인증위원회에 제출한다.

② 인증위원회 위원장은 제21조제1항 각 호의 사항에 대한 심의·의결 결과를 인터넷진흥원 또는 인증기관의 장에게 제출한다.

제7장 인증서의 발급·관리 및 홍보

제23조(인증서 발급) 인터넷진흥원 또는 인증기관의 장은 제22조제1항에 따라 인증위원회의 심의·의결 결과를 제출받은 때에는 신청기관의 정보보호 관리체계가 이 고시에서 정한 인증기준에 적합하다고 판단된 경우 별지 제11호서식의 정보보호 관리체계 인증서를 발급하여야 한다.

제24조(인증서 관리) ① 인터넷진흥원 또는 인증기관은 발급된 인증서의 인증번호, 발급일, 유효기간 등 인증서를 관리하여야 한다.

② 인증을 취득한 자는 인증서의 분실 등으로 인해 재발급을 받고자 할 경우 별지 제12호서식의 정보보호 관리체계 인증서 추가발급 신청서를 인터넷진흥원 또는 인증기관에 제출하여야

한다.

③ 인증을 취득한 자가 주소, 업체명 등 인증서 기재사항의 변경을 요청하고자 하는 경우 별지 제13호서식의 정보보호 관리체계 인증서 변경신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

제25조(인증의 표시 및 홍보) ① 영 제52조에 따른 인증의 표시는 별표 4와 같다.

② 제1항에 따른 인증의 표시를 사용하는 경우에는 영 제52조에 따라 인증의 범위와 유효기간을 함께 표시하여야 한다.

제8장 정보보호 관리체계 인증 수수료

제26조(수수료의 산정) ① 인증 수수료는 다음 각 호의 기준을 준용하되 별표 5의 정보보호 관리체계 인증 수수료 산정기준을 적용하여 산정한다.

1. 「엔지니어링산업 진흥법」 제31조제2항에 따른 엔지니어링사업의 대가 기준
2. 한국소프트웨어산업협회가 제공하는 「SW사업 대가산정 가이드」의 정보보안 컨설팅비

② 인터넷진흥원 또는 인증기관은 제1항에 따라 산정된 인증 수수료를 공지하여야 한다. 다만, 「중소기업기본법」 제2조에 따른 중소기업이 인증을 신청하는 경우 수수료 감면 등 필요한 지원을 할 수 있다.

③ 인터넷진흥원 또는 인증기관은 신청기관의 인증범위가 정보보호 관련 타 인증과 중복될 경우 신청기관과 협의하여 수수료를 조정할 수 있다.

제27조(수수료의 납부) ① 신청기관은 최초심사, 사후심사 및 갱신심사 신청 시 수수료를 납부한다. 다만, 수수료 납부 방법(일괄 또는 분할)은 인증심사 계약 시 신청기관과 협의하여 조정할 수 있다.

② 신청기관은 인증심사 계약을 체결한 날로부터 1개월 이내에 인증 수수료를 인터넷진흥원 또는 인증기관에 납부하여야 한다.

제28조(인증업무 지침) 인터넷진흥원 또는 인증기관은 인증업무 수행을 위해 필요한 경우 인증업무에 관한 지침을 마련하여 시행할 수 있다.

제29조(재검토기한) 「훈령ㆍ예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 고시 발령 후 법령이나 현실여건의 변화 등을 검토하여 이 고시의 폐지, 개정 등 조치를 하여야 하는 기한은 2016년 2월 17일까지로 한다.

부칙 <제2013 - 4호,2013.1.17>

제1조(시행일) 이 고시는 2013년 2월 18일부터 시행한다.

제2조(인증심사원에 관한 경과조치) 이 고시 시행 이전에 종전 고시에 따라 인증 심사업무를 전담하는 직원의 요건을 갖추고 인터넷진흥원으로부터 위촉된 자는 이 고시에 의한 인증심사원

자격을 취득한 것으로 본다.

[별표 1]

업무수행 요건·능력 심사 규정에 따른 제출서류(제3조제2항 관련)

구 분	제 출 서 류
1. 정보보호 관리체계 인증심사 참여 실적을 확인하는 데 필요한 서류	가. 별지 제4호서식에 따른 정보보호 관리체계 인증심사 참여실적 명세서 및 이를 증빙할 수 있는 자료 (인증심사 참여통지 문서 등) 나. 인증심사원 자격 증빙 자료
2. 업무수행 요건·능력 심사를 위하여 필요한 서류	가. 자본금 5억원 이상 내역(공인회계사 또는 회계담당자가 서명날인한 서류) 나. 부채비율 및 자기자본 이익률의 계산내역(회계결산내역 등 관련 증빙자료) 다. 인증심사 업무 운영체계 관련 규정 및 지침 등 o 심사기관의 운영체계 및 인증의 품질관리 o 인증심사 업무를 수행하는 직원에 대한 운영관리 등의 내부규정 o 인증심사 업무 수행 방법 및 절차

[별표 2]

업무수행 요건·능력 심사 세부기준(제4조제1항 관련)

가. 업무수행 요건 심사 세부기준

평가항목	세부 평가 기준
1. 인증심사원 5명 이상 상시 고용 여부	o 인증심사원 5명 이상을 상시 고용하고 있어야 함 - 다만, 심사팀장급 심사원 1명 이상 확보해야 함
2. 인증기관 공정성 확보 여부	o 정보보호 관리체계 인증기관으로 지정을 받으려는 기관은 인증업무의 독립성, 객관성, 공정성, 신뢰성을 확보하기 위하여 정보보호 관리체계 구축과 관련된 컨설팅 업무를 수행하지 않아야 함

나. 업무수행 능력 심사 세부기준

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td rowspan="3">1. 조직 내 직원들의 정보보호 전문성 (30)</td><td rowspan="3">정보보호 업무 전문성</td><td>10</td><td>비율</td><td>o 심사원 이상 인력 수
<table><tr><td>심사원 수</td><td>점수</td></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (심사원 수/5명) × 100</td></tr></table></td></tr>
<tr><td>5</td><td>비율</td><td>o 정보보호 관련 박사학위 소지자 · 기술사 인력의 수
<table><tr><td>박사학위소지자·기술사 수</td><td>점수</td></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (박사학위 소지자, 기술사 수/5명) × 100</td></tr></table></td></tr>
<tr><td>5</td><td>비율</td><td>o CISM, SIS, CISSP, CISA, CPPG, 정보보안기사/산업기사 자격증 소지자 수
<table><tr><td>자격증 소지자 · 수</td><td>점수</td></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (자격증 소지자 수/5명) × 100</td></tr></table></td></tr>
<tr><td>정보보호 관리체계 인증심사 참여실적</td><td>10</td><td>비율</td><td>o 상시 고용하고 있는 인증심사원이 최근 3년간 참여한 정보보호 관리체계 인증심사 참여 실적을 인정하고 평가점수는 개별 참여 실적을 합한 총 참여일수에 따라 산출
<table><tr><td>총 참여 일수(단위 : 일)</td><td>점수</td></tr><tr><td>200일 이상</td><td>배점의 100%</td></tr><tr><td>200일 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (총 참여일수/200일) × 100</td></tr></table></td></tr>
</table>

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td>2. 시설(10)</td><td>사무공간·인증심사 서류 보관 장소 및 보안설비·시설 확보</td><td>10</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>○ 인증심사의 상담, 인증심사 업무의 처리를 위해 필요한 사무실</td><td>2점</td></tr>
<tr><td>○ 사무 관련 장비 확보</td><td>2점</td></tr>
<tr><td>○ 사무실 출입자에 대한 신원확인 및 출입통제를 위한 설비</td><td>2점</td></tr>
<tr><td>○ 기록물 및 자료의 안전한 관리를 위한 보관 장소</td><td>2점</td></tr>
<tr><td>○ 인증심사 서류의 분실, 도난 등 예방을 위한 보안 시설</td><td>2점</td></tr>
</table>
</td></tr>
<tr><td rowspan="2">3. 신뢰도 및 재정상태 건실도 (10)

※비영리기관 평가제외</td><td>부채비율</td><td>5</td><td>비율</td><td>○ 지정 공고일 기준으로 직전년도 부채비율
(부채총계/자기자본)
<table>
<tr><th>비율</th><th>점수</th></tr>
<tr><td>50% 미만</td><td>5점</td></tr>
<tr><td>50% 이상 ~ 100% 미만</td><td>4점</td></tr>
<tr><td>100% 이상 ~ 150% 미만</td><td>3점</td></tr>
<tr><td>150% 이상 ~ 200% 미만</td><td>2점</td></tr>
<tr><td>200% 이상</td><td>1점</td></tr>
</table>
</td></tr>
<tr><td>자기자본 이익률</td><td>5</td><td>비율</td><td>○ 지정 공고일 기준으로 직전년도 자기자본이익률
(당기순이익/자기자본)
<table>
<tr><th>비율</th><th>점수</th></tr>
<tr><td>20% 이상</td><td>5점</td></tr>
<tr><td>20% 미만 ~ 15% 이상</td><td>4점</td></tr>
<tr><td>15% 미만 ~ 10% 이상</td><td>3점</td></tr>
<tr><td>10% 미만 ~ 5% 이상</td><td>2점</td></tr>
<tr><td>5% 미만</td><td>1점</td></tr>
</table>
</td></tr>
<tr><td rowspan="3">4. 인증업무 운영 체계 (50)</td><td>인증기관의 운영 체계 및 인증의 품질관리</td><td>20</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>○ 인증기관의 공정성·객관성·신뢰성·독립성 보장 방안</td><td>5점</td></tr>
<tr><td>○ 인증기관의 내부감사 실시 및 검토 등에 대한 방안</td><td>5점</td></tr>
<tr><td>○ 인증의 품질 보장 및 관리방안</td><td>5점</td></tr>
<tr><td>○ 인증업무의 기록 및 문서화 관리체계의 적절성</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td>인증업무를 수행하는 직원에 대한 운영·관리 등의 내부 규정</td><td>10</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>○ 인증업무를 수행하는 직원에 대한 규정 보유 및 그 규정의 타당성 및 실효성
- 인증업무를 수행하는 직원의 의무와 책임 등 준수사항
- 인증업무를 수행하는 직원의 자체 보안관리 및 감독 요령</td><td>5점</td></tr>
<tr><td>○ 인증업무를 수행하는 직원의 교육 및 평가 등에 대한 방안 및 그 방안의 적절성 및 타당성</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td>인증업무 수행 방법 및 절차</td><td>5</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>○ 인증업무 수행 방법 및 절차 등의 적절성 및 타당성
- 인증심사의 절차 및 방법
- 인증수수료 및 그 징수방법
- 인증심사팀 구성 원칙
- 인증심사 사후관리방안 등</td><td>5점</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td></td><td>인증업무
지원체계</td><td>15</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 운영자금 법인통장 보유 및 유지 수준</td><td>5점</td></tr>
<tr><td>o 지정취소, 부도 · 해산 등에 따른 신청기관 피해 보상 관련 보험 가입 여부</td><td>5점</td></tr>
<tr><td>o 인증의 품질 제고를 위한 지원방안</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td rowspan="3">5. 가점 및 감점</td><td>인증심사 업무를 전담하는 인증심사원 보유수</td><td>5
(가점)</td><td>보유
인원수</td><td>o 인증심사업무를 수행하는 전담조직을 갖추고, 그 전담조직에 속한 직원에 대해 인정
<table>
<tr><th>구분</th><th>점수</th></tr>
<tr><td>10명 이상</td><td>5점</td></tr>
<tr><td>10명 미만 ~ 5명 이상</td><td>배점의 X%</td></tr>
<tr><td>5명 미만</td><td>없음</td></tr>
<tr><td colspan="2">※X = (인원수/10명) × 100</td></tr>
</table>
</td></tr>
<tr><td>정보보호
관리체계 인증의 취득 및 유지</td><td>2
(가점)</td><td>인증 취득
및 유지</td><td>o 정보보호 관리체계 인증을 취득하고, 인증을 유지하고 있을 때</td></tr>
<tr><td>자격취소 사실</td><td>5
(감점)</td><td>취소사실
및
취소회수</td><td>o 지정 공고일 기준으로 10년 이내에 방송통신위원회가 부여한 정보보호 관련 수행자격이 취소된 경우
- 정보보호 관리체계 인증기관, 안전진단 수행기관 등
※ 취소 1회당 : 감점 5점</td></tr>
</table>

<비 고>

1. 평가항목에 대한 각 평가요소별 세부평가 점수는 소수점 이하 둘째 자리에서 반올림한다.
2. 평가항목에 대한 각 평가요소별 평가점수는 평가결과의 최저점과 최고점을 제외한 점수들의 평균점을 부여한다. 다만, 최저점 또는 최고점이 2개 이상일 경우 각 1개만 제외한다.
3. 가점을 합한 점수가 100점을 초과해도 만점 100점으로 표기한다.
4. '시설', '인증업무 운영체계'에 대한 각 평가요소별 세부평가 점수 부여기준은 각 평가요소의 평가결과에 평가등급(계수)를 곱하여 나온 점수를 합산한다.

평가요소별 세부평가 점수	평가등급(계수)
100점 이하 ~ 90점 이상	우수(1.0)
90점 미만 ~ 80점 이상	보통(0.6)
80점 미만 ~	미흡(0.2)
미 제출	점수 없음(0)

[별표 3]

인증심사원 자격 요건(제9조 관련)

1. 인증심사원 등급별 자격 요건

구 분	자격 요건
심사원보	o 인증심사원 학력 및 경력요건을 만족하는 자로서 인터넷진흥원이 지정하는 기관에서 인증심사원 양성교육 과정을 수료한 자
심사원	o 심사원보 자격 취득자로서 인증심사 4회 이상 참여하고 심사일수의 합이 20일 이상인 자
선임심사원	o 심사원 자격 취득자로서 3회 이상 심사 총괄업무를 수행하고 심사일수의 합이 15일 이상인 자

2. 인증심사원 학력 및 경력 요건

o 학사학위를 취득한 후 정보통신 또는 정보보호 유관경력 6년(전문학사의 경우 8년, 수업연한이 3년인 전문학사의 경우 7년, 고등학교 졸업자의 경우 10년을 말한다) 이상을 보유한 자(최근 10년 이내의 경력에 한함)

o 유관자격 소지자 또는 유관학력을 취득한 자로서 다음 각 목의 어느 하나에 해당하는 경우 정보통신 유관경력을 인정한다.
가. 기술사 자격 소지자 또는 박사 학위를 취득한 자의 경우 3년
나. 기사 자격 소지자 또는 석사 학위를 취득한 자의 경우 2년
다. 산업기사 자격 소지자 또는 학사 학위를 취득한 자의 경우 1년

o 다음 각 목의 어느 하나에 해당하는 자격을 취득한 자는 정보통신 또는 정보보호 유관경력 1년을 추가 인정한다.
가. 한국인터넷진흥원 정보보호전문가(SIS)
나. 전자정부법 제60조에 따른 감리원
다. 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 정보시스템감사사(CISA)
라. 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 정보시스템보호전문가(CISSP)

<비 고>
1. "정보통신 유관경력", "정보보호 유관경력", "유관자격" 및 "유관학력"은 영 별표 2 "정보보호 기술인력의 자격기준"을 준용한다.

[별표 4]

정보보호 관리체계 인증의 표시(제25조 관련)

□ 출입구 부착용

1. 도안모형



2. 인증명판 제작 유의사항

가. 소재는 가급적 동판으로 제작한다(전체 두께 1.0㎝, 바탕 0.4㎝, 테두리 폭 0.5㎝)

나. 바탕색은 가급적 연마하지 않은 황동색으로 한다

다. 도안 모형은 인증의 표시를 중앙에 둔다

라. 글씨 및 도형은 양각으로 한다.

마. 크기는 사각형으로 하며 인증마크는 중앙에 위치하도록 하며 가로와 세로 비율을 3 : 2로 하여 일정 비율로 조정할 수 있다

□ 서류 및 제품 등 표시용

1. 도안모형



2. 도안 및 표시방법

가. 'Information Security Management System'은 검정색으로, '정보보호 관리체계 인증'은 군청색으로 한다. 게시장소의 칼라표시가 불합리한 경우에는 흑백으로 할 수 있다.

나. 마크의 크기는 제품과 그 제품의 포장 또는 용기의 크기에 따라 일정 비율로 조정할 수 있다.

[별표 5]

정보보호 관리체계 인증 수수료 산정기준(제26조 관련)

1. 인증 수수료 산정 방식

인증 수수료 = 직접인건비 + 직접경비 + 제경비 + 기술료

① 직접인건비는 인증심사에 투입되는 인증심사원에 대한 인건비로 산정한다. 인건비는 SW사업 대가산정 가이드의 정보보안 컨설팅비를 준용한다

인증심사원 등급	컨설턴트 등급
선임심사원	전임 컨설턴트 이상
심사원	
심사원보	컨설턴트

② 직접경비는 인증심사업무의 수행에 따라 발생하는 교통비, 숙박비 및 식대 등 인증심사업무에 소요되는 직접적인 경비를 산정한다.

③ 제경비는 최대 (직접인건비×120%) 로 산정한다.

④ 기술료는 최대 {(직접인건비+제경비)×40% } 로 산정한다.

[별표 6]

정보보호 관리체계 인증기준(제18조 관련)

가. 정보보호관리과정 요구사항

	관리과정		세부관리과정	관리과정 상세내용
1	정보보호정책 수립 및 범위설정	1.1	정보보호정책의 수립	조직이 수행하는 모든 정보보호 활동의 근거를 포함할 수 있도록 정보보호정책을 수립하고 동 정책은 국가나 관련 산업에서 정하는 정보보호 관련 법, 규제를 만족하여야 한다.
		1.2	범위설정	조직에 미치는 영향을 고려하여 중요한 업무, 서비스, 조직, 자산 등을 포함할 수 있도록 정보보호 관리체계 범위를 설정하고 범위 내 모든 자산을 식별하여 문서화하여야 한다.
2	경영진 책임 및 조직구성	2.1	경영진 참여	정보보호 관리체계 수립 및 운영 등 조직이 수행하는 정보보호 활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여야 한다.
		2.2	정보보호 조직 구성 및 자원 할당	최고경영자는 조직의 규모, 업무 중요도 분석을 통해 정보보호 관리체계의 지속적인 운영이 가능하도록 정보보호 최고책임자, 실무조직 등 정보보호 조직을 구성하고 정보보호 관리체계 운영 활동을 수행하는데 필요한 자원(예산 및 인력)을 확보하여야 한다.
3	위험관리	3.1	위험관리 방법 및 계획 수립	관리적, 기술적, 물리적, 법적 분야 등 조직의 정보보호 전 영역에 대한 위험식별 및 평가가 가능하도록 위험관리 방법을 선정하고 위험관리의 전문성을 보장할 수 있도록 수행인원, 기간, 대상, 방법 등을 구체적으로 포함한 위험관리계획을 사전에 수립하여야 한다.
		3.2	위험식별 및 평가	위험관리 방법 및 계획에 따라 정보보호 전 영역에 대한 위험 식별 및 평가를 연 1회 이상 수행하고 그 결과에 따라 조직에서 수용 가능한 위험수준을 설정하여 관리하여야 한다.

	관리과정		세부관리과정	관리과정 상세내용
3	위험관리	3.3	정보보호대책 선정 및 이행계획 수립	위험을 수용 가능한 수준으로 감소시키기 위해 정보보호대책을 선정하고 그 보호대책의 구현 우선순위, 일정, 담당부서 및 담당자 지정, 예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.
4	정보보호대책 구현	4.1	정보보호대책의 효과적 구현	정보보호대책 이행계획에 따라 보호대책을 구현하고 경영진은 이행결과의 정확성 및 효과성 여부를 확인하여야 한다.
		4.2	내부 공유 및 교육	구현된 정보보호대책을 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여야 한다.
5	사후관리	5.1	법적요구사항 준수검토	조직이 준수해야 할 정보보호 관련 법적요구사항을 지속적으로 파악하여 최신성을 유지하고 준수여부를 지속적으로 검토하여야 한다.
		5.2	정보보호 관리체계 운영현황 관리	정보보호 관리체계 범위 내에서 주기적 또는 상시적으로 수행해야 하는 활동을 문서화하고 그 운영현황을 지속적으로 관리하여야 한다.
		5.3	내부감사	조직은 정보보호 관리체계가 정해진 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는 지를 점검하기 위하여 연 1회 이상 내부감사를 수행하여야 한다. 이를 위해 감사 기준, 범위, 주기, 방법 등을 구체적으로 정하고 내부감사를 통해 발견된 문제점은 보완조치를 완료하여 경영진 및 관련 책임자에게 보고하여야 한다. 또한 감사의 독립성 및 전문성을 확보할 수 있도록 감사인력에 대한 자격요건을 정의하여야 한다.

나. 정보보호대책

	통제분야		통제목적		통제사항	통제내용
1	정보보호 정책	1.1	정책의 승인 및 공표	1.1.1	정책의 승인	정보보호정책은 이해관련자의 검토와 최고경영자의 승인을 받아야 한다.
				1.1.2	정책의 공표	정보보호정책 문서는 모든 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.
		1.2	정책의 체계	1.2.1	상위 정책과의 연계성	정보보호정책은 상위조직 및 관련 기관의 정책과 연계성을 유지하여야 한다.
				1.2.2	정책시행 문서수립	정보보호정책의 구체적인 시행을 위한 정보보호지침, 절차를 수립하고 관련 문서간의 일관성을 유지하여야 한다.
		1.3	정책의 유지관리	1.3.1	정책의 검토	정기적으로 정보보호정책 및 정책 시행문서의 타당성을 검토하고, 중대한 보안사고 발생, 새로운 위협 또는 취약성의 발견, 정보보호 환경에 중대한 변화 등이 정보보호정책에 미치는 영향을 분석하여 필요한 경우 제·개정하여야 한다.
				1.3.2	정책문서 관리	정보보호정책 및 정책 시행문서의 이력관리를 위해 제정, 개정, 배포, 폐기 등의 관리절차를 수립하고 문서는 최신본으로 유지하여야 한다. 또한 정책문서 시행에 따른 운영기록을 생성하여 유지하여야 한다.
2	정보보호 조직	2.1	조직 체계	2.1.1	정보보호 최고 책임자 지정	최고경영자는 임원급의 정보보호 최고책임자를 지정하고 정보보호 최고책임자는 정보보호정책 수립, 정보보호 조직 구성, 위험관리, 정보보호위원회 운영 등의 정보보호에 관한 업무를 총괄 관리하여야 한다.

	통제분야		통제목적		통제사항	통제내용
2	정보보호 조직	2.1	조직의 체계	2.1.2	실무조직 구성	최고경영자는 정보보호 최고책임자의 역할을 지원하고 조직의 정보보호 활동을 체계적으로 이행하기 위해 실무조직을 구성하고 조직 구성원의 정보보호 전문성을 고려하여 구성한다.
				2.1.3	정보보호 위원회	정보보호 자원할당 등 조직 전반에 걸친 중요한 정보보호 관련사항에 대한 검토 및 의사결정을 할 수 있도록 정보보호위원회를 구성하여 운영하여야 한다.
		2.2	역할 및 책임	2.2.1	역할 및 책임	정보보호 최고책임자와 정보보호 관련 담당자에 대한 역할 및 책임을 정의하고 그 활동을 평가할 수 있는 체계를 마련하여야 한다.
3	외부자 보안	3.1	보안 요구사항 정의	3.1.1	외부자 계약 시 보안요구사항	조직의 정보처리 업무를 외부자에게 위탁하거나 정보자산에 대한 접근을 허용할 경우, 또는 업무를 위해 클라우드 서비스 등 외부 서비스를 이용하는 경우에는 보안요구사항을 식별하고 관련 내용을 계약서 및 협정서 등에 명시하여야 한다.
		3.2	외부자 보안 이행	3.2.1	외부자 보안 이행 관리	외부자가 계약서 및 협정서에 명시된 보안요구사항의 이행여부를 관리 감독하고 주기적인 점검 또는 감사를 수행하여야 한다.
				3.2.2	외부자 계약 만료 시 보안	외부자와의 계약 만료, 업무 종료, 담당자 변경 시 조직이 외부자에게 제공한 정보자산의 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 업무 수행 시 알게 된 정보의 비밀유지 확약서 등의 내용을 확인하여야 한다.

	통제분야		통제목적		통제사항	통제내용
4	정보자산 분류	4.1	정보자산 식별 및 책임	4.1.1	정보자산 식별	조직의 업무특성에 따라 정보자산 분류기준을 수립하고 정보보호 관리체계 범위 내 모든 정보자산을 식별하여야 한다. 또한 식별된 정보자산을 목록으로 관리하여야 한다.
				4.1.2	정보자산별 책임할당	식별된 정보자산에 대한 책임자 및 관리자를 지정하여 책임소재를 명확히 하여야 한다.
		4.2	정보자산의 분류 및 취급	4.2.1	보안등급과 취급	기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 정보자산이 조직에 미치는 중요도를 평가하고 그 중요도에 따라 보안등급을 부여하여야 한다. 또한 보안등급을 표시하고 등급 부여에 따른 취급절차를 정의하여 이행하여야 한다.
5	정보보호 교육	5.1	교육 프로그램 수립	5.1.1	교육 계획	교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 정보보호 교육 계획을 수립하여야 한다.
				5.1.2	교육 대상	교육 대상에는 정보보호 관리체계 범위 내 임직원 및 외부자를 모두 포함하여야 한다.
				5.1.3	교육 내용 및 방법	교육에는 정보보호 및 정보보호 관리체계 개요, 보안사고 사례, 내부 규정 및 절차, 법적 책임 등의 내용을 포함하고 일반 임직원, 책임자, IT 및 정보보호 담당자 등 각 직무별 전문성 제고에 적합한 교육내용 및 방법을 정하여야 한다.
		5.2	교육 시행 및 평가	5.2.1	교육 시행 및 평가	정보보호 관리체계 범위 내 임직원 및 외부자를 대상으로 연 1회 이상 교육을 시행하고 정보보호 정책 및 절차의 중대한 변경, 조직 내·외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생할 경우 추가 교육을 수행하여야 한다. 또한 교육 시행에 대한 기록을 남기고 평가하여야 한다.

	통제분야		통제목적		통제사항	통제내용
6	인적 보안	6.1	정보보호 책임	6.1.1	주요 직무자 지정 및 감독	인사정보, 영업비밀, 산업기밀, 개인정보 등 중요정보를 대량으로 취급하는 임직원의 경우 주요직무자로 지정하고 주요직무자 지정을 최소화 하는 등 관리할 수 있는 보호대책을 수립하여야 한다.
				6.1.2	직무 분리	권한 오남용 등 고의적인 행위로 인해 발생할 수 있는 잠재적인 피해를 줄이기 위하여 직무 분리 기준을 수립하고 적용하여야 한다. 다만 인적 자원 부족 등 불가피하게 직무분리가 어려운 경우 별도의 보완통제를 마련하여야 한다.
				6.1.3	비밀유지 서약서	임직원으로부터 비밀유지 서약서를 받아야 하고 임시직원이나 외부자에게 정보시스템에 대한 접근권한을 부여할 경우에도 비밀유지서약서를 받아야 한다.
		6.2	인사규정	6.2.1	퇴직 및 직무변경 관리	퇴직 및 직무변경 시 인사부서와 정보보호 및 시스템 운영 부서 등 관련 부서에서 이행해야 할 자산반납, 접근권한 회수·조정, 결과 확인 등의 절차를 수립하여야 한다.
				6.2.2	상벌규정	인사규정에 직원이 정보보호 책임과 의무를 충실히 이행했는지 여부 등 정보보호 활동 수행에 따른 상벌 규정을 포함하여야 한다.

	통제분야		통제목적		통제사항	통제내용
7	물리적 보안	7.1	물리적 보호구역	7.1.1	보호구역 지정	비인가자의 물리적 접근 및 각종 물리적, 환경적 재난으로부터 주요 설비 및 시스템을 보호하기 위하여 통제구역, 제한구역, 접견구역 등 물리적 보호구역을 지정하고 각 구역별 보호대책을 수립·이행하여야 한다.
				7.1.2	보호설비	각 보호구역의 중요도 및 특성에 따라 화재, 전력이상 등 인·재해에 대비하여 온습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 설비를 충분히 갖추고 운영절차를 수립하여 운영하여야 한다. 또한 주요 시스템을 외부 집적정보통신시설에 위탁운영하는 경우 관련 요구사항을 계약서에 반영하고 주기적으로 검토를 수행하여야 한다.
				7.1.3	보호구역 내 작업	유지보수 등 주요 설비 및 시스템이 위치한 보호구역 내에서의 작업 절차를 수립하고 작업에 대한 기록을 주기적으로 검토하여야 한다.
				7.1.4	출입통제	보호구역 및 보호구역 내 주요 설비 및 시스템은 인가된 사람만이 접근할 수 있도록 출입을 통제하고 책임추적성을 확보할 수 있도록 출입 및 접근 이력을 주기적으로 검토하여야 한다.
				7.1.5	모바일 기기 반출입	노트북 등 모바일 기기 미승인 반출입을 통한 중요정보 유출, 내부망 악성코드 감염 등의 보안사고 예방을 위하여 보호구역 내 임직원 및 외부자 모바일 기기 반출입 통제절차를 수립하고 기록·관리하여야 한다.
		7.2	시스템 보호	7.2.1	케이블 보안	데이터를 송수신하는 통신케이블이나 전력을 공급하는 전력 케이블은 손상을 입지 않도록 보호하여야 한다.
				7.2.2	시스템 배치 및 관리	시스템은 그 특성에 따라 분리하여 배치하고 장애 또는 보안사고 발생 시 주요 시스템의 위치를 즉시 확인할 수 있는 체계를 수립하여야 한다.

	통제분야		통제목적		통제사항	통제내용
		7.3	사무실 보안	7.3.1	개인업무 환경 보안	일정시간 동안 자리를 비울 경우에는 책상 위에 중요한 문서나 저장매체를 남겨놓지 않고 컴퓨터 화면에 중요정보가 노출되지 않도록 화면보호기 설정, 패스워드 노출 금지 등 보호대책을 수립하여야 한다.
				7.3.2	공용업무 환경 보안	사무실에서 공용으로 사용하는 사무처리 기기, 문서고, 공용 PC, 파일서버 등을 통해 중요정보 유출이 발생하지 않도록 보호대책을 마련하여야 한다.
8	시스템 개발보안	8.1	분석 및 설계 보안관리	8.1.1	보안 요구사항 정의	신규 정보시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안취약점, 정보보호 기본요소(기밀성, 무결성, 가용성) 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용하여야 한다.
				8.1.2	인증 및 암호화 기능	정보시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입·출력 및 송수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다.
				8.1.3	보안로그 기능	정보시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 하여야 한다.
				8.1.4	접근권한 기능	정보시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다.

	통제분야		통제목적		통제사항	통제내용
8	시스템 개발 보안	8.2	구현 및 이관 보안	8.2.1	구현 및 시험	안전한 코딩방법에 따라 정보시스템을 구현 하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다. 또한 알려진 기술적 보안 취약성에 대한 노출여부를 점검하고 이에 대한 보안대책을 수립하여야 한다.
				8.2.2	개발과 운영 환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다.
				8.2.3	운영환경 이관	운영환경으로의 이관은 통제된 절차에 따라 이루어져야 하고 실행코드는 시험과 사용자 인수 후 실행하여야 한다.
				8.2.4	시험 데이터 보안	시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다.
				8.2.5	소스 프로그램 보안	소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행하여야 한다. 또한 소스 프로그램은 운영환경에 보관하지 않는 것을 원칙으로 한다.
		8.3	외주개발 보안	8.3.1	외주개발 보안	정보시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독하여야 한다.

	통제분야		통제목적		통제사항	통제내용
9	암호통제	9.1	암호 정책	9.1.1	암호 정책 수립	조직의 중요정보 보호를 위하여 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 수립하고 이행하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.
		9.2	암호키 관리	9.2.1	암호키 생성 및 이용	암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고 필요 시 복구방안을 마련하여야 한다.
10	접근 통제	10.1	접근통제 정책	10.1.1	접근통제 정책 수립	비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다.
		10.2	접근권한 관리	10.2.1	사용자 등록 및 권한부여	정보시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다.
				10.2.2	관리자 및 특수 권한 관리	정보시스템 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.
				10.2.3	접근권한 검토	정보시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 점검하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.3	사용자 인증 및 식별	10.3.1	사용자 인증	정보시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제되어야 하고, 필요한 경우 법적요구사항 등을 고려하여 중요 정보시스템 접근 시 강화된 인증방식을 적용하여야 한다.
				10.3.2	사용자 식별	정보시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다. 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.
				10.3.3	사용자 패스워드 관리	법적요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경주기 등 사용자 패스워드 관리절차를 수립·이행하고 패스워드 관리 책임이 사용자에게 있음을 주지시켜야 한다. 특히 관리자 패스워드는 별도 보호대책을 수립하여 관리하여야 한다.
				10.3.4	이용자 패스워드 관리	고객, 회원 등 외부 이용자가 접근하는 정보시스템 또는 웹서비스의 안전한 이용을 위하여 계정 및 패스워드 등의 관리절차를 마련하고 관련 내용을 공지하여야 한다.
		10.4	접근통제 영역	10.4.1	네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 접근통제 리스트, 네트워크 식별자 등에 대한 관리절차를 수립하고 서비스, 사용자 그룹, 정보자산의 중요도에 따라 내·외부 네트워크를 분리하여야 한다.
				10.4.2	서버 접근	서버별로 접근이 허용되는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 적용하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.4	접근통제 영역	10.4.3	응용 프로그램 접근	사용자의 업무 또는 직무에 따라 응용프로그램 접근권한을 제한하고 불필요한 중요정보 노출을 최소화해야 한다.
				10.4.4	데이터베이스 접근	데이터베이스 접근을 허용하는 응용프로그램 및 사용자 직무를 명확하게 정의하고 응용프로그램 및 직무별 접근통제 정책을 수립하여야 한다. 또한 중요정보를 저장하고 있는 데이터베이스의 경우 사용자 접근내역을 기록하고 접근의 타당성을 정기적으로 검토하여야 한다.
				10.4.5	모바일 기기 접근	모바일기기를 업무 목적으로 내·외부 네트워크에 연결하여 활용하는 경우 중요정보 유출 및 침해사고 예방을 위해 기기 인증 및 승인, 접근 범위, 기기 보안설정, 오남용 모니터링 등의 접근통제 대책을 수립하여야 한다.
				10.4.6	인터넷 접속	인사정보, 영업비밀, 산업기밀, 개인정보 등 중요정보를 대량으로 취급·운영하는 주요직무자의 경우 인터넷 접속 또는 서비스(P2P, 웹메일, 웹하드, 메신저 등)를 제한하고 인터넷 접속은 침입차단시스템을 통해 통제하여야 한다. 필요시 침입탐지시스템 등을 통해 인터넷 접속내역을 모니터링하여야 한다.
11	운영보안	11.1	운영 절차 및 변경 관리	11.1.1	운영절차 수립	정보시스템 동작, 문제 발생 시 재 동작 및 복구, 오류 및 예외사항 처리 등 시스템 운영을 위한 절차를 수립하여야 한다.
				11.1.2	변경관리	정보시스템 관련 자산의 모든 변경내역을 관리할 수 있도록 절차를 수립하고 변경 전 시스템의 전반적인 성능 및 보안에 미치는 영향을 분석하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영보안	11.2	시스템 및 서비스 운영 보안	11.2.1	정보 시스템 인수	새로운 정보시스템 도입 또는 개선 시 필수 보안요구사항을 포함한 인수 기준을 수립하고 인수 전 기준 적합성을 검토하여야 한다.
				11.2.2	보안 시스템 운영	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립하고 보안시스템 별 정책적용 현황을 관리하여야 한다.
				11.2.3	성능 및 용량관리	정보시스템 및 서비스 가용성 보장을 위해 성능 및 용량 요구사항을 정의하고 현황을 지속적으로 모니터링할 수 있는 방법 및 절차를 수립하여야 한다.
				11.2.4	장애관리	정보시스템 장애 발생 시 효과적으로 대응하기 위한 탐지, 기록, 분석, 복구, 보고 등의 절차를 수립하여야 한다.
				11.2.5	원격운영 관리	내부 네트워크를 통하여 정보시스템을 관리하는 경우 특정 단말에서만 접근을 할 수 있도록 제한하고, 원격지에서 인터넷 등 외부 네트워크를 통하여 정보시스템을 관리하는 것은 원칙적으로 금지하고 부득이한 사유로 인해 허용하는 경우에는 책임자 승인, 접속 단말 및 사용자 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등의 보호대책을 수립하여야 한다.
				11.2.6	스마트 워크 보안	재택근무, 원격협업 등과 같은 원격 업무 수행 시 이에 대한 관리적·기술적 보호대책을 수립하고 이행하여야 한다.
				11.2.7	무선네트워크 보안	무선랜 등을 통해 무선인터넷을 사용하는 경우 무선 네트워크 구간에 대한 보안을 강화하기 위해 사용자 인증, 송수신 데이터 암호화 등의 보호대책을 수립하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영보안			11.2.8	공개서버 보안	웹사이트 등에 정보를 공개하는 경우 정보 수집, 저장, 공개에 따른 허가 및 게시절차를 수립하고 공개서버에 대한 물리적, 기술적 보호대책을 수립하여야 한다.
				11.2.9	백업관리	데이터의 무결성 및 정보시스템의 가용성을 유지하기 위해 백업 대상, 주기, 방법 등의 절차를 수립하고 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다.
				11.2.10	취약점 점검	정보시스템이 알려진 취약점에 노출되어 있는 지 여부를 확인하기 위하여 정기적으로 기술적 취약점 점검을 수행하고 발견된 취약점들은 조치하여야 한다.
		11.3	전자거래 및 정보전송 보안	11.3.1	전자거래 보안	전자거래 서비스 제공 시 정보유출, 데이터 조작, 사기 등의 침해사고를 예방하기 위해 사용자 인증, 암호화, 부인방지 등의 보호대책을 수립하고 결제시스템 등 외부 시스템과의 연계가 필요한 경우 연계 안전성을 점검하여야 한다.
				11.3.2	정보전송 정책 수립 및 협약 체결	타 조직에 중요정보를 전송할 경우 안전한 전송을 위한 정책을 수립하고 조직 간 정보전송 합의를 통해 관리책임, 전송 기술 표준, 중요정보의 보호를 위한 기술적 보호조치 등을 포함한 협약서를 작성하여야 한다.
		11.4	매체 보안	11.4.1	정보 시스템 저장매체 관리	정보시스템 폐기 또는 재사용 시 중요정보를 담고 있는 하드디스크, 스토리지, 테잎 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제하여야 한다.
				11.4.2	휴대용 저장매체 관리	조직의 중요정보 유출을 예방하기 위해 외장하드, USB, CD 등 휴대용 저장매체 취급, 보관, 폐기, 재사용에 대한 절차를 수립하여야 한다. 또한 매체를 통한 악성코드 감염 방지 대책을 마련하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영보안	11.5	악성코드 관리	11.5.1	악성코드 통제	바이러스, 웜, 트로이목마 등의 악성코드로부터 정보시스템을 보호하기 위해 악성코드 예방, 탐지, 대응 등의 보호대책을 수립하여야 한다.
				11.5.2	패치관리	소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인해 발생할 수 있는 침해사고를 예방하기 위해 최신 패치를 정기적으로 적용하고 필요한 경우 시스템에 미치는 영향을 분석하여야 한다.
		11.6	로그관리 및 모니터링	11.6.1	시각 동기화	로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 정보시스템 시각을 공식 표준시각으로 정확하게 동기화 하여야 한다.
				11.6.2	로그 기록 및 보존	정보시스템, 응용프로그램, 보안시스템, 네트워크 장비 등 기록해야 할 로그 유형을 정의하여 일정기간 보존하고 주기적으로 검토하여야 한다. 보존기간 및 검토주기는 법적요구사항을 고려하여야 한다.
				11.6.3	접근 및 사용 모니터링	중요정보, 정보시스템, 응용프로그램, 네트워크 장비에 대한 사용자 접근이 업무상 허용된 범위에 있는 지 주기적으로 확인하여야 한다.
				11.6.4	침해시도 모니터링	외부로부터의 침해시도를 모니터링하기 위한 체계 및 절차를 수립하여야 한다.
12	침해사고 관리	12.1	절차 및 체계	12.1.1	침해사고 대응절차 수립	DDoS 등 침해사고 유형별 중요도 분류, 유형별 보고·대응·복구 절차, 비상연락체계, 훈련 시나리오 등을 포함한 침해사고 대응 절차를 수립하여야 한다.
				12.1.2	침해사고 대응체계 구축	침해사고 대응이 신속하게 이루어질 수 있도록 중앙 집중적인 대응체계를 구축하고 외부기관 및 전문가들과의 협조체계를 수립하여야 한다.
		12.2	대응 및 복구	12.2.1	침해사고 훈련	침해사고 대응 절차를 임직원들이 숙지할 수 있도록 시나리오에 따른 모의훈련을 실시하여야 한다.

	통제분야		통제목적		통제사항	통제내용
12	침해사고 관리	12.2	대응 및 복구	12.2.2	침해사고 보고	침해사고 징후 또는 사고 발생을 인지한 때에는 침해사고 유형별 보고 절차에 따라 신속히 보고하고 법적 통지 및 신고 의무를 준수하여야 한다.
				12.2.3	침해사고 처리 및 복구	침해사고 대응절차에 따라 처리와 복구를 신속하게 수행하여야 한다.
		12.3	사후관리	12.3.1	침해사고 분석 및 공유	침해사고가 처리되고 종결된 후 이에 대한 분석을 수행하고 그 결과를 보고하여야 한다. 또한 사고에 대한 정보와 발견된 취약점들을 관련 조직 및 임직원들과 공유하여야 한다.
				12.3.2	재발방지	침해사고로부터 얻은 정보를 활용하여, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하고 이를 위해 필요한 경우 정책, 절차, 조직 등의 대응체계를 변경하여야 한다.
13	IT 재해복구	13.1	체계 구축	13.1.1	IT 재해복구 체계 구축	자연재앙, 해킹, 통신장애, 전력중단 등의 요인으로 인해 IT 시스템 중단 또는 파손 등 피해가 발생할 경우를 대비하여 비상 시 복구조직, 비상연락체계, 복구절차 등 IT 재해복구 체계를 구축하여야 한다.
		13.2	대책 구현	13.2.1	영향분석에 따른 복구대책 수립	조직의 핵심 서비스 연속성을 위협할 수 있는 IT 재해 유형을 식별하고 유형별 예상 피해규모 및 영향을 분석하여야 한다. 또한 IT 서비스 및 시스템 복구목표시간, 복구시점을 정의하고 적절한 복구전략 및 대책을 수립·이행하여야 한다.
				13.2.2	시험 및 유지관리	IT 서비스 복구전략 및 대책에 따라 효과적인 복구가 가능한 지 시험을 실시하고 시험계획에는 시나리오, 일정, 방법, 절차 등을 포함하여야 한다. 또한 시험결과, IT 환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완하여야 한다.

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제1호서식] <개정 2013.1.17.>

정보보호 관리체계 인증기관 지정 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	처리기간	3개월이내

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	총 직원 수	인증심사원 직원 수	
신청구분	☐ 신규	☐ 재지정	
인증에 관한 업무의 범위			

「정보보호 관리체계 인증 등에 관한 고시」 제3조제2항의 규정에 따라 위와 같이 정보보호 관리체계 인증기관 지정을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

방송통신위원회 귀중

신청인 제출서류	1. 정관 또는 규약 1부. 2. 별지 제2호서식의 인증심사원의 보유현황과 이를 증명할 수 있는 서류 1부. 3. 별표 1에 따른 업무수행 요건·능력 심사를 위하여 필요한 서류 1부.	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

처 리 절 차

신청서 작성	→	접 수	→	심 사	→	지정여부 결정	→	지정서 교부
신청인		처리기관 (방송통신위원회)		처리기관 (방송통신위원회)		처리기관 (방송통신위원회)		처리기관 (방송통신위원회)

210㎜×297㎜[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제2호서식] <개정 2013.1.17.>

인증심사원의 보유현황

(제1쪽)

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	직원 수	인증심사원 직원 수	

일련번호	성명	주소		최종학력	해당요건
		생년월일	입사일	취득학위 및 학과	

유의사항

1. 「해당요건」란에는 선임심사원, 심사원, 심사원보 요건을 기재한다.
2. 기재된 최종학위를 증명할 수 있는 직원의 졸업 또는 학위증명서 사본을 제출하여야 한다.
3. 별표 3의 「인증 심사원 학력 및 경력 요건」을 충족하는 직원은 기술자격증 사본 등 자격을 취득하였음을 확인할 수 있는 서류를 함께 제출하여야 한다.
4. 정보통신유관경력 또는 정보보호유관경력을 증명할 수 있는 경력증명서(근무부서 또는 담당업무 등이 기재되어야 한다)와 해당 직원이 신청업체에 현재 근무하고 있음을 확인할 수 있는 재직증명서를 함께 제출하여야 한다.

210mm×297mm[백상지(80g/㎡)]

인증심사업무를 전담하는 직원의 보유현황

(제2쪽)

일련번호	성명	주소		최종학력	해당요건
		생년월일	입사일	취득학위 및 학과	

10mm×297mm[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제3호서식] <개정 2013.1.17.> (제1쪽)

정보보호 관리체계 인증기관 지정서

등록번호 :

업체명 :

대표자 :

주소 :

지정의 유효기간 :

인증업무의 범위 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제5항 및 같은 법 시행령 제53조의2에 따라 위와 같이 정보보호 관리체계 인증기관으로 지정합니다.

년 월 일

방송통신위원회위원장 직인

210mm×297mm[백상지(120g/㎡)]

(제2쪽)

CERTIFICATE OF DESIGNATION
AS
ISMS Certification Authority

Registry Number :

Name of Organization :

Name of Representative :

Address :

Period of Validity :

Scope of Certification work :

This is to certify that the abovementioned organization is designated Information Security Management System (ISMS) Certification Authority in accordance with Article 47, Paragraph 5 of 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」 and Article 53-2 of the Enforcement Decree of the same Act.

Date of Issuance:

Signed by the
Chairman of Korea Communications Commission
Republic of Korea

210㎜×297㎜[백상지120g/㎡]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제4호서식] <개정 2013.1.17.>

인증실적 보고서

정보보호 관리체계 인증기관	업체명		사업자등록번호
	주소		전화번호
	대표자		
	정보보호 관리체계 인증심사 실적 총계	최초심사 외 건	
		사후관리심사 외 건	

일련번호	인증 번호	대상기관(기업)명	인증범위	유효기간	구분	
					최초심사	사후관리심사

년 월 일

신청인(대표자) (서명 또는 인)

방송통신위원회 귀중

신청(신고)인 제출서류	1. 정보보호 관리체계 인증기관 지정서 1부.	수수료 없음

처 리 절 차

신청서 작성	→	접 수	→	검 토	→	심 사	→	지정서 교부
신청인		처 리 기 관 (방송통신위원회)		처 리 기 관 (방송통신위원회)		처 리 기 관 (방송통신위원회)		처 리 기 관 (방송통신위원회)

210mm×297mm[백상지(80g/㎡)]

■「정보보호 관리체계 인증 등에 관한 고시」 [별지 제5호서식] <개정 2013.1.17.> (제1쪽)

정보보호 관리체계 인증심사원 자격 신청서

신청자 인적사항	성 명		생년월일		사진	
	주 소	(우: -)				
	회 사 명					
	회사주소	(우: -)				
	이 메 일					
	전화번호		휴대전화			
신청사항	신청 구분	□ 자격인증 □ 전문분야 변경				
학력사항	최종학력	□ 고졸	□ 전문학사	□ 학사	□ 석사	□ 박사
	학사	전공		기간		
	석사	전공		기간		
	박사	전공		기간		
인증심사원 교육이수	교육기간	년 월 일 ~ 년 월 일		수료증번호		

자격사항 ※해당자에 한함	자격증번호	자격증명/등급	취득일자	수여기관

경력사항 ※최근 10년 내 경력사항 기술	총 경력	정보기술	총 년 개월	정보보호	총 년 개월

No.	구분	기간	회사명	부서	직책
1	□정보기술 □정보보호	~ (년 개월)			
2	□정보기술 □정보보호	~ (년 개월)			
3	□정보기술 □정보보호	~ (년 개월)			
4	□정보기술 □정보보호	~ (년 개월)			
5	□정보기술 □정보보호	~ (년 개월)			

※ 칸이 부족할 경우 추가 작성

(제2쪽)

(1) 개인별 전문분야 (복수 선택 가능, 우선순위 표기요망)					
대분류	중분류	소분류	순위	실무경력	
관리적 정보 보호	정책, 조직 및 인적보안	정보보호정책수립 및 조직구성			년
		인적보안, 외부자 보안, 외부위탁관리			년
		정보보호교육 및 훈련			년
		국내외 표준 기준 및 법령			년
	위험관리	자산분류, 위험평가 수행, 대책 및 계획수립			년
	업무연속성관리	업무연속성 계획수립 및 시험, 유지관리			년
	침해사고대응	침해사고 대응계획 및 체계, 복구			년
	정보시스템 감사/감리	정보시스템 및 정보보호시스템 감사/감리			년
기술적 정보 보호	네트워크	네트워크 설계기술			년
		라우팅 제어, 프로토콜 제어, 접근통제, 암호화, NAT, 운용관리(로그, SNMP, 설정도구)등 통신기술			년
		라우터, 스위치(L2~L7), RAS, VPN, SSL, DHCP, 네트워크 감시 등 기기기술			년
		기타( )			년
	운영체제 및 시스템	OS 기본지식, 계정관리, 접근권한, 서비스관리, 로그관리, 패치, 보안 S/W 사용 등 유닉스/리눅스 시스템			년
		OS 기본지식, 계정관리, 접근권한, 서비스관리, 로그관리, 패치, 보안 S/W 사용 등 윈도우 시스템			년
		메인프레임 등 기타( )			년
	응용서비스	HTTP 프로토콜, 브라우저, SQL-Injection 등 Web 위협에 대한 대응책, SSL, CGI 보안 프로그래밍 등 Web 서비스			년
		부하분산, DNSSEC, 보안설정 등 DNS 서비스			년
		메일 프로토콜, 스팸대응, 웜/바이러스 필터링 등 메일 서비스			년
		DB 기본지식, 이중화, 데이터백업, 암호화 등 데이터베이스			년
		ERP, KMS, CRM 등 사내정보시스템			년
		분산시스템 등 기타( )			년
	정보보호 솔루션	FW 기본지식, 접근통제, 라우팅, 네트워크 정책설계, 구성(이중화, 망분리, 로드밸런싱 등) 등 침입차단시스템			년
		웜/바이러스 기본지식, 웜/바이러스별 감염 증상과 대책 등 바이러스 월			년
		IDS 기본지식, 방화벽 연동, 패턴 매칭 방법, 구성(에이전트 위치, 통합콘솔 등) 등 침입탐지시스템			년
		SecureOS 기본지식, 계정관리, 접근권한, 서비스관리, 로그관리, 패치 등 SecureOS			년
		기타( )			년

(제3쪽)

(1) 개인별 전문분야 (복수 선택 가능, 우선순위 표기요망) (계속)					
대분류	중분류	소분류	순위	실무경력	
기술적 정보 보호 (계속)	취약성분석	사회공학적 방법, 스캔, Sniffing, DOS, Buffer Overflow, 웜/바이러스, 백도어 등 취약성 분석 및 점검			년
	보안 운영	통합관제(ESM, NMS 등), 망관리, 백업, 로그 분석, 모니터링, 패치, 문제해결(원인규명)			년
	기반기술	IPSec, PPTP, L2TP, SSH, SSL/TLS, MPLS, IKE, S/MIME, PGP 등 보안 프로토콜			년
		패스워드인증, 생체인증, 인증디바이스, 인증프로토콜, WEB인증, RADIUS, SSO 등 인증기술			년
		증명서 인증 및 실효, 신뢰모델, 기술 및 데이터방식, 인증센터 구축과 운영, 법적구조 등 PKI			년
		암호알고리즘, Key 관리, 암호방식 등 암호기술			년
		디지털서명, 디지털 봉투, 코드 서명			년
물리적 정보 보호	접근보안	출입 및 접근통제, 모니터링 등			년
	시설관리	소방시설, 비상전원, 비상조명, 항온항습 등			년
개인정보보호		개인정보보호 책임자, 취급자, 컨설턴트, 법률 담당, 소비자 민원 및 상담 등			년
기타		( )			년

※ 경력 및 전문 분야에 대한 관련 내용을 상세히 기술
※ 칸이 부족할 경우 별지 사용

No.	상세내용
1	
2	
3	
4	
5	
6	

(제4쪽)

(2) 통제분야별 전문분야 (5순위까지 선택, 우선순위 표기요망)

통제분야	순위	실무경력		통제분야	순위	실무경력	
1. 정보보호정책			년	9. 암호통제			년
2. 정보보호조직			년	10. 접근통제			년
3. 외부자 보안			년	11. 운영관리			년
4. 정보자산분류			년	12. 전자거래보안			년
5. 정보보호교육 및 훈련			년	13. 보안사고관리			년
6. 인적 보안			년	14. 검토, 모니터링 및 감사			년
7. 물리적 보안			년	15. 업무연속성 관리			년
8. 시스템개발 보안			년	16. 개인정보보호			년

관련 경력기술

※ 5순위까지 선택한 전문분야 관련 실무경력, 전문기술, 인증심사실적 등 관련경력을 상세히 기술

<개인정보 수집·이용>

o 개인정보 수집 이용 목적 : 정보보호 관리체계(ISMS) 인증심사원 양성 교육, 자격부여 및 관리, 자문료 지급, 심사팀구성

o 수집하는 개인정보 항목 : 성명, 생년월일, 주소, 이메일, 전화번호, 학력, 자격경력, 발령사항, 기술실적사항

o 보유 및 이용기간 : 인증심사원 자격 종료시까지

o 개인정보의 수집·이용을 거부할 수 있으며, 이 경우 인증심사원 등록 및 위촉에 불이익이 발생할 수 있음을 알려드립니다.

▷ 개인정보 수집·이용 동의여부 **동의 □** **미동의 □**

<인증심사원 의무사항>

- 인증심사원은 객관적이고 공정한 인증심사를 수행한다.
- 인증심사원으로서의 성실한 직무수행 및 품위유지를 한다.
- 인증심사와 관련된 부당한 금전, 금품 등의 수수를 금지한다.
- 인증심사의 수행에서 취득한 정보를 관련 법령 또는 신청기관의 동의 없이 외부에 누설하여서는 안된다.
- 인증심사원은 인증업무지침을 성실히 준수한다.
- 인증심사원은 본인이 ISMS 인증 취득을 위한 컨설팅을 수행한 기업에 대하여는 인증심사에 참여할 수 없다.
- 인증심사원은 인증심사의 수행과 관련하여 상업적, 재정적 그리고 기타 모든 압력으로부터 배제되어야 한다.

1. 위의 인증심사원 의무사항을 읽고 이해하였으며, 성실히 준수하겠습니다.
2. 본 신청서의 기재사항은 사실과 틀림없으며, 만약 허위로 판명될 경우에는 자격취소 등 불이익을 감수하겠습니다.

※ 필요시 학력, 경력 등 증빙서류 제출을 요청받을 수 있으며 반드시 이에 응해야 함

위와 같이 인증심사원 자격을 신청합니다.

년 월 일

신청자		(서명 또는 인)

한국인터넷진흥원 귀중

■「정보보호 관리체계 인증 등에 관한 고시」 [별지 제6호서식] <개정 2013.1.17.>

경력증명서

인적사항	성명		생년월일	
	주소		연락처	

경력사항	전 근무처 명				
	근무기간		부서	직위	담당업무
	부터	까지			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			

근무년수	년 개월	최종직위	
용도	정보보호 관리체계 인증심사원 자격 신청		

위와 같이 경력을 증명합니다.

년 월 일

회사명

대표자 (서명 또는 인)

확인자	성명	부서	연락처	비고

■「정보보호 관리체계 인증 등에 관한 고시」 [별지 제7호서식] <개정 2013.1.17.>

상세 재직증명서

인적사항	성명		생년월일	
	주소		연락처	
소속사항	회사명			
	부서		직위	
	근속기간	~	근무년수	년 개월

발령사항	근무기간		부서	직위	담당업무
	부터	까지			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			

용도	정보보호 관리체계 인증심사원 자격 신청

위와 같이 재직하고 있음을 증명합니다.

년 월 일

회사명

대표자 (서명 또는 인)

확인자	성명	부서	연락처	비고

■「정보보호 관리체계 인증 등에 관한 고시」 [별지 제8호서식] <개정 2013.1.17.>

기술실적증명서

인적사항	성명			생년월일	
	주소			연락처	
실적사항	소속				
	수행기간		참여사업명	발주처	담당업무
	부터	까지			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
용도	정보보호 관리체계 인증심사원 자격 신청				

위와 같이 기술실적을 증명합니다.

년 월 일

회사명

대표자 (서명 또는 인)

확인자	성명	부서	연락처	비고

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제9호서식] <개정 2013.1.17.>

제 호

인증심사원 자격 증명서

성 명 : (. . .)

인증심사원 등급 :

유효기간 :

※ 인증심사원 유지조건을 만족하지 못할 경우 자격이 취소될 수 있습니다.

귀하에게 정보보호 관리체계 인증심사원 자격을 부여합니다.

년 월 일

한국인터넷진흥원 원장 직인

210mm×297mm[백상지(120g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제10호서식] <개정 2013.1.17.>

정보보호 관리체계 인증 신청서

※ [ ]에는 해당되는 곳에 √표를 하고, 어두운 부분은 신청인이 작성하지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명	사업자등록번호
	주소	전화번호
	대표자	

인증신청의 구분	[ ]최초심사 [ ]사후심사 [ ]갱신심사
정보보호 관리체계의 범위	
정보보호 관리체계의 범위에 포함되어 있는 종업원의 수	
정보보호 관리체계의 범위에 포함되어 있는 서버의 수	

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제9항, 같은 법 시행령 제47조에 따라 위와 같이 정보보호 관리체계의 인증을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

(한국인터넷진흥원 또는 정보보호 관리체계 인증기관명) 귀중

신청(신고)인 제출서류	정보보호 관리체계의 내역서 1부.	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

210㎜×297㎜[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제11호서식] <개정 2013.1.17.> (제1쪽)

정보보호 관리체계 인증서

인증번호 :

업체명 :

대표자 :

주소 :

인증의 범위 :

유효기간 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제9항, 같은 법 시행령 제47조에 따라 위와 같이 정보보호 관리체계를 인증합니다.

년 월 일

한국인터넷진흥원 원장
또는 정보보호 관리체계
인증기관 장 직인

210mm×297mm[백상지(120g/㎡)]

(제2쪽)

CERTIFICATE
OF
Information Security Management System

Certificate Number :

Name of Organization :

Name of Representative :

Address :

Scope of Certification :

Period of Validity :

This is to certify that the abovementioned organization is compliant to the assessment standard for Information Security Management System certification in accordance with Article 47, Paragraph 1 and 9 of 「Act on Information Network Utilization and Data Protection, etc.」 and Article 47 of the Enforcement Decree of the same Act.

Date of Issuance :

Signed by the
President of Korea Internet & Security Agency or certification body

210㎜×297㎜[백상지(120g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제12호서식] <개정 2013.1.17.>

정보보호 관리체계 인증서 추가발급 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명	사업자등록번호
	주소	전화번호
	대표자	

추가발급 사유	

위와 같이 정보보호 관리체계 인증서의 추가발급을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

한국인터넷진흥원 또는 정보보호 관리체계 인증기관명 귀중

제출서류	해당없음	수수료 없 음

210㎜×297㎜[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제13호서식] <개정 2013.1.17.>

정보보호 관리체계 인증서 변경 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		

변경 내용	변경전	(국문)
		(영문)
	변경후	(국문)
		(영문)
변경사유		

위와 같이 정보보호 관리체계 인증서 변경을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

한국인터넷진흥원 또는 정보보호 관리체계 인증기관명 귀중

제출서류	해당없음	수수료 없 음

210㎜×297㎜[백상지(80g/㎡)]

정보보호관리체계 인증 등에 관한 고시

[시행 2012.3.15] [고시 제2012 - 23호, 2012.3.15, 일부개정]

제1장 총칙

제1조(목적) 이 고시는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하"법"이라 한다) 제47조제2항 및 같은 법 시행령 제47조제2항、제48조제1항제3호、제5항、제50조제6항에 따른 정보보호관리체계 인증에 관한 정보보호관리기준、지정에 필요한 업무수행능력 심사 등에 관한 세부사항과 그 밖에 정보보호관리체계 인증에 관하여 필요한 사항에 대하여 정하는 것을 목적으로 한다.

제2조(용어의 정의) 이 기준에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "업무수행능력심사"란 정보보호관리체계인증기관으로 지정받고자 신청한 법인 또는 단체의 업무수행능력을 세부평가기준에 따라 심사하는 것을 말한다.
2. "정보보호관리체계인증기관"이란 법 제47조에 따른 한국인터넷진흥원과 방송통신위원회가 지정하는 기관을 말한다.
3. "인증"이란 신청기관이 수립하여 운영하고 있는 정보보호관리체계가 인증심사기준 등에 적합함을 정보보호관리체계인증기관이 승인하는 것을 말한다.
4. "인증심사"란 신청기관이 수립하여 운영하는 정보보호관리체계가 인증심사기준 등에 대하여 서면심사 및 기술심사의 방법으로 확인하는 것을 말한다.
5. "정보보호관리과정(이하 ‘관리과정’이라 한다)"이란 정보보호관리체계를 수립、운영하기 위하여 유지、관리하여야 할 과정으로 다음 각목의 5단계 활동을 말한다.
   가. 정보보호정책 수립
   나. 정보보호관리체계 범위설정
   다. 위험관리
   라. 구현
   마. 사후관리
6. "신청기관"이란 이 고시에 따라 정보보호관리체계 인증을 취득하고자 신청한 업체 및 기관 등을 말한다.
7. "외부자"란 신청기관의 직원이 아닌 자를 말한다.

8. "정보보호대책"이란 신청기관이 정보보호관리체계를 수립·운영하기 위하여 별표 6에서 선택한 통제사항을 말한다.

제2장 정보보호관리체계인증기관의 지정 등

제1절 정보보호관리체계인증기관의 지정신청

제3조(정보보호관리체계인증기관의 지정공고) 방송통신위원회는 법 제47조 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」(이하 "영"이라 한다) 제48조에 따라 정보보호관리체계인증기관을 지정할 필요가 있는 때에는 미리 접수신청기간과 신청요령 등을 정하여 관보 및 인터넷 홈페이지에 20일 이상 공고하여야 한다.

제4조(제출서류 등) ①정보보호관리체계인증기관 지정을 신청하는 자는 별지 제1호서식의 정보보호관리체계인증기관 지정신청서를 방송통신위원회에 제출하여야 한다.

②영 제48조제1항제2호에 따라 제1항의 정보보호관리체계인증기관지정신청서에 첨부하여야 하는 "인증심사업무를 전담하는 직원의 보유현황"의 제출서식은 별지 제2호서식과 같다.

③영 제48조제1항제3호에 따른 "업무수행능력심사를 위하여 필요한 서류"라 함은 별표 1과 같다.

제2절 인증심사업무를 전담하는 직원의 자격요건 및 업무수행능력심사

제5조(인증심사업무를 전담하는 직원의 요건 등) ①영 제47조제1항제1호 및 제2항에 따른 "인증심사업무를 전담하는 직원(이하 "인증심사원"이라 한다)의 요건"은 별표 2와 같다.

②법 제47조에 따른 정보보호관리체계인증기관으로 지정신청 하고자 하는 자는 제1항의 인증심사원의 요건을 만족하여야 한다.

제6조(업무수행능력심사 기준 등) ①영 제47조제1항제2호 및 제2항에 따른 업무수행능력심사의 세부평가기준은 별표 3과 같다.

②심사위원회는 제1항에 따라 심사위원 각자가 부여한 점수 중 최고점과 최저점을 제외한 점수들의 평균이 80점 이상인 자를 선별한다.

③심사위원회는 제2항에 따라 선별된 자에 대하여 심사결과 검증 및 업무수행능력의 적합성을 판단한다.

제7조(업무수행능력의 적합성 인정) 방송통신위원회는 제5조 및 제6조에 따라 심사한 결과를 토대로 정보통신망 안전성 및 신뢰성 확보를 위한 종합적인 정보보호관리체계의 업무를 수행하는 자로서 적합한지 여부를 결정한다.

제8조(정보보호관리체계인증기관지정서) 영 제48조제3항에 따른 "정보보호관리체계인증기관지정서"는 별지 제4호서식과 같다.

제3절 인증기관 심사위원회 구성·운영

제9조 (심사위원회의 구성) ①방송통신위원회는 영 제48조제1항에 따라 정보보호관리체계인증기관의 지정신청을 받은 경우 영 제48조제4항에 따른 심사위원회를 구성하여 다음 각 호의 심사업무를 수행하게 하여야 한다. 이 경우 방송통신위원회는 필요하다고 인정하는 때에는 분과위원회 또는 작업반을 둘 수 있다.

1. 영 제48조제3항에 따른 현장실사
2. 별표 2에 따른 인증심사원의 자격요건 및 별표 3에 따른 업무수행능력심사 세부평가
3. 정보보호관리체계인증기관 지정의 적합성 결정
4. 그 밖에 지정심사와 관련되는 업무

②심사위원회는 5인이상 10인이내의 위원으로 구성하되, 위원은 정보보호전문가, 회계사, 기술사, 변호사 등 업무수행능력심사를 수행할 수 있는 학식과 경험이 있는 자 중 방송통신위원회가 위촉하며, 위원장은 위원 중에서 호선한다.

③제2항에 따른 심사위원은 최근 2년간 지정신청자와 관련된 업무를 수행하지 않아야 한다.

④위원에 대하여는 예산의 범위안에서 수당과 여비를 지급할 수 있다. 다만, 공무원인 위원이 소관업무와 관련하여 참석한 경우에는 그러하지 아니하다.

제10조(심사위원회의 운영) ①위원장은 심사위원회의 업무를 통할하며 위원회를 대표하여 방송통신위원회에 정보보호관리체계인증기관 지정 적합성 여부에 대한 심사결과를 제출한다.

②위원장이 부득이한 사유로 직무를 수행할 수 없을 때에는 위원장이 미리 지정한 위원이 그 직무를 대행한다.

제3장 정보보호관리체계의 인증기준 등

제1절 정보보호관리체계 인증신청

제11조(신청기관의 준비사항) 신청기관은 다음 각 호의 인증심사기준에 따라 정보보호관리체계를 수립하여 최소 3개월 이상 운영하여야 한다.

1. 별표 4에 따른 관리과정 요구사항
2. 별표 5에 따른 문서 작성 및 관리 통제사항
3. 별표 6에 따른 정보보호관리 통제사항에서 선택한 사항(신청기관은 자신의 정보보호관리체계의 규모 및 사업특성 등을 고려하여 별표 6에서 적절한 항목을 선택할 수 있다)

제12조(인증의 신청) ①영 제50조제1항에 따라 인증을 신청하는 자는 별지 제5호서식의 정보보호관리체계인증신청서를 정보보호관리체계인증기관에 제출하여야 한다. 이 경우 정보보호관리체계의 인증을 받고자 하는 범위를 정하여 신청할 수 있다.

②제1항에 따라 신청을 받은 정보보호관리체계인증기관은 정보보호관리체계 특성상 신청기관이 지정한 정보보호관리체계만을 분리하여 심사할 수 없는 경우에는 신청기관과 상의하여

인증의 범위를 변경할 수 있다.

제13조(인증심사계약의 체결) 정보보호관리체계인증기관은 영 제50조제2항에 따라 신청기관과 협의한 후 심사기간, 심사인원, 심사수수료, 인증의 범위 등을 포함하는 인증심사계약을 체결하여야 한다.

제2절 정보보호관리체계 인증심사 기준 및 방법

제14조(인증심사기준) 정보보호관리체계의 인증심사기준은 별표 4부터 별표 6까지와 같다.

제15조(인증심사요소) ①정보보호관리체계인증기관은 신청기관이 수립한 관리과정을 체계적으로 관리·유지하고 있는지 여부를 판단하기 위하여 다음 각 호의 사항을 심사하여야 한다.

1. 정보보호정책 수립 : 신청기관에 적합한 정보보호정책의 수립, 조직의 구성·운영, 책임성의 명확한 설정 여부
2. 정보보호관리체계 범위설정 : 정보보호관리체계 수립·운영을 위한 관리범위 설정 및 정보자산의 현황조사 여부
3. 위험관리 : 위험관리 전략 및 계획 수립, 위험분석·평가, 정보보호대책 선택의 적절성 여부
4. 구현 : 정보보호대책의 구현 및 정보보호 교육·훈련의 효과성 여부
5. 사후관리 : 정보보호관리체계의 재검토, 모니터링 및 개선, 내부감사 활동의 적절성 여부

②정보보호관리체계인증기관은 신청기관이 정보보호관리체계의 수립 및 이행 활동에 관련된 절차와 운영을 문서화해서 관리하는지에 대하여 심사하여야 한다.

③정보보호관리체계인증기관은 신청기관이 관리과정의 위험평가를 통하여 선택한 통제사항에 대한 정보보호대책을 구현하고 이행하고 있는지에 대하여 심사하여야 한다.

제16조(서면심사) 인증심사원은 신청기관이 영 제50조제1항에 따라 제출한 신청서류를 확인하여 신청기관이 수립한 정보보호관리체계가 별표 4부터 별표 6까지에 따른 인증심사기준에 적합한지에 대하여 심사하여야 한다.

제17조(기술심사) ①인증심사원은 서면심사의 결과를 검증하기 위하여 신청기관이 인증을 신청한 정보보호관리체계가 운영중인 현장을 방문하여 직접 해당 정보보호관리체계의 구축·운영 실태를 확인하여야 한다.

②인증심사원은 제1항에 따른 현장방문시 신청기관의 요청이 있는 경우 인터넷 침해사고 등에 대한 안전성 검사를 위하여 해당 정보보호관리체계에 속한 정보시스템에 대한 모의진단을 실시할 수 있다.

제3절 인증위원회의 구성 및 운영

제18조(인증위원회의 구성) ①정보보호관리체계인증기관의 장은 인증심사원이 실시한 인증심사 결과가 제14조에 따른 인증심사기준에 적합한지 여부를 심의하기 위하여 인증위원회를 구성·운영하여야 한다.

②인증위원회는 5인 이상 10인 이내의 위원으로 구성하되, 위원은 정보보호전문가, 정보시스템감리사, 기술사 등 정보보호분야에 학식과 경험이 있는 자 중 정보보호관리체계인증기관의 장이 위촉하며, 위원장은 위원 중에서 호선한다.

제19조(인증위원회의 운영) ①위원장은 인증위원회의 업무를 통할하며 위원회를 대표하여 정보보호관리체계인증기관의 장에게 인증심사원이 실시한 인증심사 결과가 제14조에 따른 인증심사기준에 적합한지 여부를 심의하고 그 결과를 제출한다.

②정보보호관리체계인증기관의 장은 제1항에 따른 심의를 실시한 때에는 인증심사원이 실시한 심사결과를 위원회 개최 전 5일까지 인증위원회에 제출한다.

제4절 인증서 교부 및 사후관리 등

제20조(인증서 교부) 정보보호관리체계인증기관의 장은 제19조제1항에 따라 인증위원회의 심의결과를 제출받은 경우 신청기관에게 인증심사결과를 통보하고, 신청기관의 정보보호관리체계가 이 고시에서 정한 인증심사기준에 적합하다고 판단된 경우 별지 제6호서식의 정보보호관리체계인증서를 교부하여야 한다.

제21조(정보보호관리체계의 변경) ①인증을 취득한 자는 인증을 받은 정보보호관리체계에 다음 각 호의 어느 하나에 해당하는 중대한 변화가 발생한 경우 발생한 날로부터 3개월 이내에 인증기관의 장에게 변경된 내용을 통보하여야 한다.

1. 신청기관이 수립하여 운영하는 관리체계의 범위가 확대되거나 변경되었을 경우
2. 사업장 변경 및 기업결합 등의 경영환경 변화 등으로 관리체계 운영에 영향을 미치는 경우

②인증기관의 장은 인증을 취득한 자로부터 변경내용을 통보받은 경우 인증을 취득한 자와 협의하여 인증심사 여부를 결정한다.

③제2항에 따라 인증심사를 실시하는 경우에는 제14조부터 제20조까지를 준용한다.

제22조(사후관리) ①영 제52조에 따라 정보보호관리체계인증기관은 인증을 취득한 자가 정보보호관리체계를 지속적으로 유지하고 있는지에 대하여 영 제51조에 따른 유효기간 중 제2절 정보보호관리체계 인증심사 기준 및 방법에 따라 연 1회 사후관리를 수행한다.

②정보보호관리체계인증기관은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 때에는 인증을 취소하여야 한다.

1. 거짓 그 밖의 부정한 방법으로 정보보호관리체계인증을 받은 때
2. 법 제47조제3항에 따라 인증받은 내용을 홍보하면서 인증의 범위나 유효기간을 속인 경우
3. 제1항에 따른 사후관리에서 정보보호관리체계 인증기준에 적합하지 않게 된 사실이 발견된 때

③정보보호관리체계인증기관이 제2항에 따라 인증을 취소하는 경우에는 인증을 취득한 자에게 통지하고, 제20조에 따라 교부한 정보보호관리체계인증서를 회수하여야 한다.

제23조(인증서 관리) ①정보보호관리체계인증기관은 발급된 인증서의 인증번호, 발급번호, 발급일, 유효기간 등을 관리하여야 한다.

②인증을 취득한 자는 인증서의 분실 등으로 인한 재발급을 받고자 할 경우 별지 제7호서식의 관리체계 인증서 재발급 신청서를 인증기관에 제출하여야 한다.

③인증을 취득한 자가 주소, 업체명 등 인증서 기재사항의 변경을 요청하고자 하는 경우 별지 제8호서식의 인증서 변경신청서를 정보보호관리체계인증기관에 제출하여야 한다.

제24조(재검토기한) 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 고시 발령 후 법령이나 현실여건의 변화 등을 검토하여 이 고시의 폐지, 개정 등 조치를 하여야 하는 기한은 2015년 1월 31일까지로 한다.

부칙 <제2012-23호,2012.3.15>

이 고시는 발령한 날부터 시행한다

[별표 1]

업무수행능력심사 규정에 따른 제출서류(제4조제3항관련)

구 분	제 출 서 류
1. 정보보호수행실적을 확인하는 데 필요한 서류	가. 별지 제3호서식에 따른 정보보호수행실적 명세서 및 이를 증빙할 수 있는 자료(결과보고서 등) 나. 계약서 사본 및 세금계산서 등
2. 업무수행능력심사평가표 각호의 세부 평가요소를 평가하기 위하여 필요한 서류	가. 총매출액대비 정보보호분야 매출액의 비율 계산내역(공인회계사 또는 회계담당자가 서명 날인한 서류) 나. 부채비율 및 자기자본 이익률의 계산내역(회결산내역 등 관련 증빙자료) 다. 인증업무 운영체계 관련 규정 및 지침 등 ㅇ 인증기관의 운영체계 및 인증의 품질관리 ㅇ 인증업무를 수행하는 직원에 대한 운영관리 등의 내부규정 ㅇ 인증업무 수행 방법 및 절차
비 고 ※ 방송통신위원회는 정보보호관리체계인증기관 지정 공고시 업무수행능력심사에 필요한 자료의 구성 및 그 세부내용, 제출시기 및 방법 등에 관한 사항을 포함하여야 한다.	

[별표 2]

인증심사업무를 전담하는 직원의 요건(제5조 관련)

학력 및 경력기준	자격 및 경력기준
1. 유관학력 보유의 경우 가. 학사학위를 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 6년 이상인 자 나. 석사학위를 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 4년 이상인 자 2. 비 유관학력 보유의 경우 가. 학사학위를 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 8년 이상인 자 나. 전문학사를 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 10년 이상인 자	1. 유관자격 보유의 경우 가. 기사자격을 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 4년 이상인 자 나. 산업기사자격을 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 7년 이상인 자 2. 다음 각목의 1에 해당하는 정보보호자격을 취득한 자로서 2년 이상의 정보보호유관경력이 있는 자 가. 한국인터넷진흥원의 정보보호전문가(SIS) 나. 「정보시스템의 효율적 도입 및 운영 등에 관한 법률」 제14조에 따른 정보시스템감리원 다. 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 공인정보시스템감사사(CISA) 라. 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 공인정보시스템보호전문가(CISSP)

1. "유관자격"이라 함은 「국가기술자격법 시행규칙」 별표 7의 검정대상 기술자격 종목 중 전자계산기, 정보통신, 통신설비, 통신기기, 통신선로, 정보기기운용, 전파통신, 전파전자, 무선설비, 방송통신, 정보관리, 정보처리, 사무자동화 및 전자계산조직응용 종목의 기술자격을 말한다.
2. "유관학력"이라 함은 「고등교육법」에 따른 해당 학교에서 다음 각 목에 해당하는 학과에서 소정의 과정을 이수하고 졸업하거나 그 밖의 관계 법령에 따라 국내 또는 외국에서 이와 동등 이상으로 인정되는 학력을 말한다.
   가. 전자 관련 학과 : 정보전자, 전자, 전자계산, 전기전자제어, 전자정보, 전자제어, 전기

전자, 전자전기정보, 전자컴퓨터전기제어, 컴퓨터과학, 전기전자정보, 전자컴퓨터, 메카트로닉스, 전자재료, 제어계측, 반도체

나. 정보통신 관련 학과 : 전기통신설비, 국제정보통신, 방송설비, 방송통신, 이동통신, 전자통신, 컴퓨터네트워크, 통신, 컴퓨터정보기술, 전파통신, 전기전자통신, 전기전자정보통신, 전자정보통신, 전자제어통신, 전자통신, 전파, 전파통신, 정보통신, 컴퓨터통신, 항공통신정보, 전자정보통신반도체, 전기전자전파, 통신컴퓨터, 무선통신

다. 정보처리기술 관련 학과 : 시스템, 전산, 정보전산, 컴퓨터제어, 컴퓨터응용제어, 컴퓨터응용, 컴퓨터응용설계, 구조시스템, 컴퓨터정보, 멀티미디어, 정보시스템, 전산통계, 정보처리

라. 그 밖에 교육인적자원부장관이나 해당 교육기관의 장으로부터 전자·통신 및 정보처리기술·정보보호 관련 학과로 인정받은 학과

3. "정보통신유관경력"이라 함은 공공기관, 민간기업, 교육기관 등에서 정보통신서비스(기간통신, 별정통신, 부가통신, 방송서비스 등을 말한다), 정보통신기기(정보기기, 방송기기, 부품 등을 말한다) 또는 소프트웨어 및 컴퓨터 관련 서비스(패키지 소프트웨어, 컴퓨터 관련 서비스, 디지털콘텐츠, 데이터베이스 제작 및 검색 등을 말한다)에 해당되는 분야에서 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 수행한 기간을 말한다.

5. "정보보호유관경력"이라 함은 공공기관, 민간기업, 교육기관 등에서 정보보호를 위한 공통기반기술(암호 기술, 인증 기술 등을 말한다), 시스템·네트워크 보호(시스템 보호, 해킹·바이러스 대응, 네트워크 보호 등을 말한다) 또는 응용서비스 보호(전자거래 보호, 응용서비스 보호, 정보보호 표준화 등을 말한다)에 해당되는 분야에서 계획·분석·설계·개발·운영·유지보수·컨설팅 또는 연구개발 업무 등을 수행한 기간을 말한다.

[별표 3]

업무수행능력심사 세부평가기준(제6조관련)

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td rowspan="3">1. 정보보호 업무수행 경험 및 전문화 정도 (40)</td><td>최근3년간 정보보호수행 실적</td><td>25</td><td>계약금액 총액</td><td>o 지정 공고일 기준으로 최근 3년간 완료한 정보보호수행실적을 인정하고 평가점수는 개별 수행실적의 계약금액을 합한 총액에 따라 산출
<table><tr><th>계약금액총액(단위 : 억원)</th><th>점수</th></tr><tr><td>30억원이상</td><td>배점의 100%</td></tr><tr><td>30억원미만</td><td>배점의 x%</td></tr><tr><td colspan="2">※ = (계약금액 총액/30억원) × 100</td></tr></table></td></tr>
<tr><td>최근 3년간 계약금액 5천만원 이상의 정보보호수행 실적</td><td>10</td><td>수행건수</td><td>o 지정 공고일 기준으로 최근 3년간 완료한 정보보호수행실적으로 계약금액이 5천만원이상의 실적을 인정
<table><tr><th>수행실적 건수</th><th>점수</th></tr><tr><td>30건이상</td><td>배점의 100%</td></tr><tr><td>30건미만</td><td>배점의 x%</td></tr><tr><td colspan="2">※ = (수행건수/30건) × 100</td></tr></table></td></tr>
<tr><td>총매출액에 대한 정보보호분야 매출액 비율</td><td>5</td><td>비율</td><td>o 지정 공고일 기준으로 직전년도 정보보호분야 매출액의 비율(정보보호분야 매출액/총매출액)
<table><tr><th>비율</th><th>점수</th></tr><tr><td>80%이상</td><td>5점</td></tr><tr><td>80%미만 ~ 60%이상</td><td>4점</td></tr><tr><td>60%미만 ~ 40%이상</td><td>3점</td></tr><tr><td>40%미만 ~ 20%이상</td><td>2점</td></tr><tr><td>20%미만</td><td>1점</td></tr></table></td></tr>
<tr><td>2. 신뢰도 및 재정상태 건실도 (10)</td><td>부채비율</td><td>5</td><td>비율</td><td>o 지정 공고일 기준으로 직전년도 부채비율 (부채총계/자기자본)
<table><tr><th>비율</th><th>점수</th></tr><tr><td>50%미만</td><td>5점</td></tr><tr><td>50%이상 ~ 100%미만</td><td>4점</td></tr><tr><td>100%이상 ~ 150%미만</td><td>3점</td></tr><tr><td>150%이상 ~ 200%미만</td><td>2점</td></tr><tr><td>200%이상</td><td>1점</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td>자기자본이익률</td><td>5</td><td>비율</td><td>o 지정 공고일 기준으로 직전년도 자기자본이익률(당기순이익/자기자본)
<table><tr><th>비율</th><th>점수</th></tr><tr><td>20%이상</td><td>5점</td></tr><tr><td>20%미만 ~ 15%이상</td><td>4점</td></tr><tr><td>15%미만 ~ 10%이상</td><td>3점</td></tr><tr><td>10%미만 ~ 5%이상</td><td>2점</td></tr><tr><td>5%미만</td><td>1점</td></tr></table></td></tr>
<tr><td>3. 인증업무 운영 체계 (50)</td><td>인증기관의 운영 체계 및 인증의 품질관리</td><td>25</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 인증기관의 공정성·객관성·신뢰성·독립성 보장 방안</td><td>5점</td></tr><tr><td>o 인증기관의 내부감사 실시 및 검토 등에 대한 방안</td><td>5점</td></tr><tr><td>o 인증위원회 구성·운영 방안</td><td>5점</td></tr><tr><td>o 인증의 품질 보증 및 관리방안</td><td>5점</td></tr><tr><td>o 인증업무의 기록 및 문서화 관리체계의 적절성</td><td>5점</td></tr></table></td></tr>
<tr><td></td><td>인증업무를 수행하는 직원에 대한 운영·관리 등의 내부 규정</td><td>10</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 인증업무를 수행하는 직원에 대한 규정 보유 및 그 규정의 타당성 및 실효성
- 인증업무를 수행하는 직원의 의무와 책임 등 준수사항
- 인증업무를 수행하는 직원의 자체 보안 관리 및 감독 요령</td><td>5점</td></tr><tr><td>o 인증업무를 수행하는 직원의 교육 및 평가 등에 대한 방안 및 그 방안의 적절성 및 타당성</td><td>5점</td></tr></table></td></tr>
<tr><td></td><td>인증업무 수행 방법 및 절차</td><td>15</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 인증업무 수행 방법 및 절차 등의 적절성 및 타당성
- 인증심사의 절차 및 방법
- 인증수수료 및 그 징수방법
- 인증심사팀 구성 원칙
- 인증서 발급 기준
- 인증심사 사후관리방안 등</td><td>15점</td></tr></table></td></tr>
<tr><td>4. 가점 및 감점</td><td>인증심사업무를 전담하는 직원의 보유수</td><td>5
(가점)</td><td>보유
인원수</td><td>o 인증심사업무를 수행하는 전담조직을 갖추고, 그 전담조직에 속한 직원에 대해 인정
<table><tr><th>구분</th><th>점수</th></tr><tr><td>20명 이상</td><td>5점</td></tr><tr><td>20명미만 ~ 10명이상</td><td>배점의 x%</td></tr><tr><td>10명 미만</td><td>없음</td></tr><tr><td colspan="2">※x = (인원수/20명) × 100</td></tr></table></td></tr>
<tr><td></td><td>자격취소 사실</td><td>5
(감점)</td><td>취소사실
및
취소횟수</td><td>o 지정 공고일 기준으로 10년이내에 방송통신위원회가 부여한 정보보호 관련 수행자격이 취소된 경우
- 정보보호관리체계인증기관, 정보보호컨설팅전문업체, 안전진단수행기관 등
※ 취소 1회당 : 감점 5점</td></tr>
</table>

<비 고>

1. 각 평가요소별 세부평가에 필요한 자료의 구성 및 그 세부내용 등에 관한 사항은 지정공고 시 제시한다.
2. 평가항목에 대한 각 평가요소별 세부평가 점수는 소수점 이하 둘째 자리에서 반올림한다.
3. 평가항목에 대한 각 평가요소별 평가점수는 평가결과의 최저점과 최고점을 제외한 점수들의 평균점을 부여한다. 다만, 최저점 또는 최고점이 2개 이상일 경우 각 1개만 제외한다.
4. 가점을 합한 점수가 100점을 초과해도 만점 100점으로 표기한다.
5. 정보보호수행실적으로 인정을 받기 위해서는 다음 각목의 요건을 충족하여야 한다.
   가. 전자적 침해행위에 대비하기 위한 정보관리 및 정보시스템의 안전성에 대한 점검과 이에 기초한 정보보호대책의 제시를 주된 목적으로 직접 수행한 실적을 말하는 것으로 정보보호에 관한 감사, 감리, 진단, 인증, 컨설팅 등을 포함한다.
   나. 지정 공고일 현재 프로젝트가 종료되고 이에 대한 대금지급이 완료되어야 한다.
   다. 하수급업체가 수급업체로부터 하도급을 받아 수행한 실적에 대해서는 인정하지 아니하고 해당 기관에서 직접 계약하여 수행한 실적에 대해서만 인정한다.
   마. 가목 내지 다목의 내용이 계약서 및 증빙자료를 통하여 분명하게 확인되어야 한다.
6. '정보보호분야의 매출액'이라함은 지정 공고일 기준으로 직전년도 결산회기의 정보보호분야 제품 및 서비스관련 매출총액을 말한다.
7. '인증업무 운영체계'에 대한 각 평가요소별 세부평가 점수 부여기준은 각 평가요소의 평가결과에 평가등급(계수)를 곱하여 나온 점수를 합산한다.

평가요소별 세부평가 점수	평가등급(계수)
100점이하 ~ 90점이상	우수(1.0)
90점미만 ~ 80점이상	보통(0.6)
80점미만 ~	미흡(0.2)
미 제출	점수없음(0)

[별표 4] 인증심사기준 - 관리과정 요구사항(제11조 제1호관련)

	관리과정		세부관리과정	관리과정 상세내용
1	정보보호정책 수립	1.1	정보보호정책의 수립	신청기관의 경영목표를 지원할 수 있도록 정보보호의 법적, 규제적 요건과 전략적이고 조직적인 위험관리를 기술한 정보보호정책을 수립하여야 한다.
		1.2	조직 및 책임의 설정	정보보호활동에 대한 경영층의 명확한 지원 및 방향제시를 보증할 수 있는 조직을 수립하여야 한다. 또한 정보보호관리 활동을 수행하고 검증하는 인력들에 대한 책임, 권한 및 상호연관관계를 정의하고 문서화하여야 한다.
2	정보보호 관리체계 범위설정	2.1	정보보호관리체계 범위설정	신청기관의 특성, 위치, 기술, 자산 등 내·외적 환경에 중대한 영향을 미치는 요소를 고려하여 정보보호관리체계의 범위를 설정하여야 한다.
		2.2	정보자산의 식별	신청기관의 정보자산으로 보호를 받을 가치가 있는 정보자산을 식별하고, 이를 정보자산의 형태, 소유자, 관리자, 특성 등을 포함하여 목록을 만들어야 한다.
3	위험관리	3.1	위험관리전략 및 계획 수립	신청기관의 목표 및 정책, 법적 요구사항 등을 고려하여 조직, 역할, 책임, 주요과정을 포함한 위험관리 전략 및 계획을 수립하고, 신청기관에 적합한 위험관리 방법을 선택하고 문서화하여야 한다. 이 위험분석 방법은 조직과 정보보호 환경변화에 대응할 수 있도록 지속적으로 검토하여야 한다.

	관리과정		세부관리과정	관리과정 상세내용
3	위험관리	3.2	위험분석	신청기관은 「2.2 정보자산의 식별」에서 식별된 정보자산에 영향을 줄 수 있는 모든 위협과 취약성, 위험을 식별하고 분류하여야 하며, 이 정보자산의 가치와 위험을 고려하여, 잠재적 손실에 대한 영향을 식별·분석하여야 한다.
		3.3	위험평가	정보자산에 대한 잠재적 및 알려진 위협과 취약성으로 나타날 수 있는 신청기관의 피해와 현재 구현된 정보보호대책의 실패 가능성 및 영향을 평가하고 수용 가능한 위험 수준을 포함하여야 한다. 이를 통해 정보자산의 위험을 관리할 수 있는 적절한 정보보호대책 선택 및 우선순위의 확보를 지원하여야 한다.
		3.4	정보보호대책 선택	신청기관의 정보보호정책과 목적에 부합하도록 위험을 수용 가능한 수준으로 감소시키기 위해, 위험분석 및 평가에 의거하여, 위험처리, 위험수용, 위험회피, 위험전가 등의 전략을 설정하고, [별표3]에서 제시하는 통제사항중에서 선택한다. [별표3]에서 제시되어 있지 않은 통제사항을 추가할 경우에는 [별표1]관리과정의 각 단계간 일관성을 유지하도록 한다. 정보보호대책의 선택은 비용·효과 분석에 의해 정당화 될 필요가 있다.
		3.5	정보보호계획 수립	정보보호대책의 선택이후 구현할 정보보호대책 및 구현의 우선순위, 일정계획, 예산, 책임, 운영계획 등을 포함한 정보보호계획을 수립하고, 각 위험에 대한 정보보호대책 및 선택하게 된 근거를 정보보호대책 명세서로 문서화하여야 한다.

	관리과정		세부관리과정	관리과정 상세내용
4	구 현	4.1	정보보호대책의 효과적 구현	정보보호대책은 적절한 관리 조치와 우선순위에 의해 구현하여야 한다.
		4.2	정보보호 교육 및 훈련	신청기관의 정보보호 관련직원들 및 최종사용자에게 정보보호에 대한 인식을 제고시키고, 정보보호대책의 필요성을 이해하도록 하며 구현될 정보보호대책들을 정확하게 사용할 수 있도록 교육 및 훈련 프로그램을 수립하고 이행하여야 한다.
5	사후관리	5.1	정보보호관리체계의 재검토	신청기관의 목표, 기술 등 내·외부의 변화와 내부감사 결과, 보안사고 등을 고려하여, 정보보호관리체계의 효율성, 범위의 적절성, 잔류위험의 수준, 절차 등의 문서를 공식적이고 정기적으로 재검토하여야 한다.
		5.2	정보보호관리체계의 모니터링 및 개선	정보보호관리체계가 신청기관의 정보보호 정책과 목적을 충족시키는지 여부에 대하여 모니터링하여, 개선사항을 식별하고, 적절한 수정이나 예방 조치를 통하여 효과적으로 개선사항을 구현하여야 한다. 이에 관련된 조치와 결과는 신청기관의 임직원에게 전달하여야 하고, 관련자들에게 자문을 구하여야 한다.
		5.3	내부감사	신청기관은 정보보호관리체계가 계획된 절차에 따라 효과적으로 실행되는지를 점검하기 위하여 감사의 기준, 범위, 주기 및 방법을 규정하고, 계획된 주기로 내부감사를 수행하여야 한다. 또한 감사의 기획 및 수행, 그리고 결과보고, 기록 유지 및 이행 모니터링에 대한 책임과 요구사항을 문서화된 절차에 의해 규정하여야 한다. 피감사분야의 관리자는 발견된 보완조치 사항을 처리하고, 검증·보고됨을 보장하여야 한다.

[별표 5] 인증심사기준 - 문서 작성 및 관리 통제사항(제11조 제2호관련)

	문서화	문서화 상세내용
1	문서요건	정보보호관리체계 수립 및 이행에 관련된 모든 문서는 해당 신청기관의 규모, 기능 등을 고려하여 문서화하여야 하며, 신청기관의 정보보호정책에 따라 필요한 모든 임직원 및 관련자들이 쉽게 이용할 수 있어야 한다.
2	문서의 통제	「1. 문서요건」에 의해 작성된 문서는 문서의 발행전 타당성 승인, 주기적 또는 필요시 문서의 검토·갱신 및 재승인, 문서의 변경과 현재 개정상태의 식별, 문서배포, 폐기된 문서의 사용금지 등의 통제를 정의한 절차를 수립하여야 한다.
3	운영기록의 통제	정보보호관리체계를 효과적, 효율적으로 운영하기 위해서 기록을 확인, 유지보수, 보존, 폐기하는 문서화된 절차를 수립하고 유지·관리하여야 한다. 이 문서화된 절차에는 접근자의 신원확인, 기록의 저장, 보호, 검색, 유지기간, 처분 등의 통제에 필요한 절차를 포함하여야 한다. 또한 기록은 읽기 쉽고, 식별 가능하며, 관련 활동을 추적할 수 있어야 한다.

[별표 6] 인증심사기준 - 정보보호관리 통제사항(제11조 제3호관련)

	통제분야		통제목적		통제사항	통제내용
1	정보보호 정책	1.1	정책의 승인 및 공표	1.1.1	정책의 승인	문서화된 정보보호정책은 최고경영자의 승인을 받아야 한다.
				1.1.2	정책의 공표	정보보호정책 문서는 모든 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.
		1.2	정책의 체계	1.2.1	상위 정책과의 일관성	정보보호정책은 신청기관의 사업목표 및 정보기술정책과 일관성을 유지하여야 한다.
				1.2.2	정책 문서의 유형	정보보호정책을 구체적으로 시행하기 위한 정보보호 지침, 절차 및 표준을 수립하여야 한다. 또한 필요한 경우 특정 시스템 또는 서비스에 대한 상세한 정보보호정책을 수립할 수 있다.
		1.3	정책의 유지관리	1.3.1	주기적 검토	정기적으로 정보보호정책의 타당성을 검토하여야 하며, 중대한 보안사고 발생, 새로운 위협 또는 취약성의 발생, 정보보호 환경에 중대한 변화 등이 발생했을 경우에는 관련된 사항의 타당성을 추가로 검토하여야 한다.
2	정보보호 조직	2.1	조직의 체계	2.1.1	조직의 구성	신청기관내 정보보호관리 활동을 계획, 관리하는 정보보호관리자가 있어야 하며, 필요에 따라 정보보호위원회를 구성할 수 있다.

	통제분야		통제목적		통제사항	통제내용
2	정보보호 조직	2.1	조직의 체계	2.1.2	외부전문가 활용	정보보호정책 수립, 위험분석·평가, 통제사항의 선택과 구현, 보안사고 대응 등 중요한 정보보호관리 활동에 도움을 받기 위하여 외부 전문가의 조언을 받을 수 있다. 외부 전문가의 신청기관 자원에 대한 접근은 「3. 외부자 보안」의 대상이 된다.
		2.2	책임과 역할	2.2.1	정보보호 관리자	최고경영자의 지정을 받은 정보보호관리자는 정보보호정책 수립, 정보보호위원회의 구성 및 운영, 위험분석 및 관리, 보안사고 대응 및 복구 등의 정보보호에 관한 업무를 총괄 관리하여야 한다.
				2.2.2	정보보호 위원회	신청기관 전반에 걸친 중요한 정보보호 관련 심의 및 승인 기능을 수행하며 필요한 자원할당을 통해 정보보호관리 활동이 적절히 수행될 수 있도록 하여야 한다.
3	외부자 보안	3.1	계약 및 서비스 수준협약 보안관리	3.1.1	위부위탁 계약시 보안 요구사항	신청기관의 업무를 외부위탁 하는 경우에는 정보시스템, 네트워크, 인력 및 사무환경 등을 관리·통제하기 위한 보안요구사항을 계약서 상에 명시하여야 하고 요구사항을 서비스수준협약(SLA : Service Level Agreement)에 반영하여야 한다.
				3.1.2	제3자와의 계약시 보안 요구사항	신청기관이 제3자에게 정보자산에 대한 접근을 허용하는 계약을 체결하는 경우에는 신청기관의 정보보호정책 준수 및 필수 보안요건을 포함하는 공식적인 계약을 하여야 한다.

	통제분야		통제목적		통제사항	통제내용
3	외부자 보안	3.2	외부자 보안 실행관리	3.2.1	외부위탁 보안관리	외부위탁 업체가 계약서 및 서비스 수준 협약 명시된 보안요구사항을 충분히 이행하는지 주기적으로 점검하고, 필요시 감사를 수행하여야 한다.
				3.2.2	제3자 보안관리	신청기관의 정보자산에 대한 제3자의 접근을 통제하여야 한다. 업무상 불가피하게 접근을 허용해야 할 경우에는 접근유형 및 접근사유를 파악하고 위험요소를 고려하여 관리하여야 한다.
4	정보자산 분류	4.1	정보자산의 조사 및 책임할당	4.1.1	정보자산 조사	신청기관의 정보자산을 조사하고 정보자산별로 신청기관에서의 가치, 업무영향, 법적 준수사항 등을 고려하여 중요도를 결정하여야 한다.
				4.1.2	정보자산별 책임할당	조사된 정보자산에 대하여 소유자, 관리자, 사용자를 확인하고, 적절한 통제 유지를 위해 책임 소재를 명확히 하여야 한다.
		4.2	정보자산의 분류 및 취급	4.2.1	정보자산의 분류	정보자산이 신청기관에서 차지하는 가치와 신청기관에 미치는 영향을 고려하여 분류방식을 선택하고 분류하여야 한다.
				4.2.2	보안등급과 취급	중요도에 따라 분류된 정보자산에 보안등급을 부여하고, 물리적, 전자적 보안등급 표시를 부착, 관리하여야 한다. 또한 보안등급의 부여에 따른 취급 절차도 정의하여 이행하여야 한다.

	통제분야		통제목적		통제사항	통제내용
5	정보보호 교육 및 훈련	5.1	교육 및 훈련 프로그램 수립	5.1.1	교육 및 훈련계획	정보보호 인식제고 및 실제 운영에 필요한 교육·훈련 계획을 종합적으로 수립하여 이행하여야 한다
				5.1.2	교육 및 훈련대상	교육 및 훈련의 대상에는 신청기관의 임직원 및 관련 외부자를 포함하여야 한다.
				5.1.3	교육 및 훈련내용	교육 및 훈련은 정보보호정책, 정보보호인식, 보안요구사항, 법적인 책임, 보안사고 대응절차, 업무연속성관리 등을 포함하여야 하고, 교육대상자의 직위 및 담당하는 업무의 특성에 따라 구분하여 실시하여야 한다.
		5.2	시행 및 평가			교육 및 훈련은 정기적으로 실시하여야 하며, 정보보호정책이나 절차 및 역할의 변경이 있는 경우에는 수시로 실시하고 이에 대한 기록을 남겨야 한다. 또한 교육훈련 종료 후 검토를 통하여 차기 교육에 반영하여야 한다.
6	인적 보안	6.1	책임할당 및 규정화	6.1.1	책임할당	정보보호업무를 이행하는 역할과 책임을 문서화하여야 한다. 문서화의 내용에는 정보보호정책을 수립, 구현, 운영하는 일반적인 책임과 특정 정보자산의 보호와 활동에 대한 구체적인 책임을 포함하여야 한다.
				6.1.2	인사규정	인사규정에는 정보보호에 대하여 직원이 지켜야 할 책임 및 관련 법규상의 책임을 명시하여야 한다. 특히, 정보보호업무를 담당하는 자와 정보시스템 사용자 및 관리자는 보다 명확한 책임을 명시하여야 하며, 직원이 책임을 이행하지 않는 경우를 대비한 적절한 처벌규정을 포함하여야 한다.

	통제분야		통제목적		통제사항	통제내용
6	인적 보안	6.2	적격심사 및 주요 직무담당자 관리	6.2.1	적격심사	계약직 및 임시직원은 물론 정식직원 채용시 신원, 업무능력, 교육정도, 경력 등에 대한 적격심사가 이루어져야 한다. 직원들이 용역회사를 통하여 충원되는 경우에는 용역회사와의 계약서에 적격심사에 따르는 책임사항을 명문화하여야 한다.
				6.2.2	주요직무 담당자 관리	정보시스템 접근 권한을 포함하는 업무가 새로이 할당될 때, 특히 재무정보나 비밀정보와 같이 중요한 정보를 처리하는 담당자는 별도의 관리를 수행하여야 한다.
		6.3	비밀유지	6.3.1	비밀유지 서약서	직원으로부터 비밀유지 서약서에 서명을 받아야 하며, 임시직원이나 제3자에게 정보에 대한 접근 권한을 부여할 경우에도 그들로부터 비밀유지 서약서에 서명을 받아야 한다. 직원의 고용계약에 변경이 있을 경우, 특히 직원이 퇴사하거나 계약기간이 만료될 때에는 비밀유지 서약서를 환기시켜야 한다.
7	물리적 보안	7.1	물리적 보안대책	7.1.1	물리적 보호구역	특별한 보호가 필요한 시설 및 장비를 권한 없는 자의 물리적 접근 및 각종 물리적, 환경적 재난으로부터 보호하기 위하여 보호구역을 정의하고 이에 따른 보안대책을 수립·이행하여야 한다. 이 경우 제한구역, 접견구역, 장비출하구역 등을 별도로 지정하여 각각에 적합한 보안 조치와 절차를 수립하여야 한다.
				7.1.2	물리적 접근통제	보호구역을 출입하는 자를 감시·통제하고 권한 없는 자의 출입을 방지하기 위하여 수립된 보안 절차에 따라 필요한 조치를 수행하고 주기적으로 검토하여야 한다.

	통제분야		통제목적		통제사항	통제내용
7	물리적 보안	7.2	데이터 센터 보안	7.2.1	위치 및 구조 조건	데이터센터는 물리적, 환경적 위험이 적은 곳에 위치하고 구조의 안정성을 확보하여야 한다.
				7.2.2	출입통제	데이터센터의 출입은 적절한 출입통제절차에 의하여 이행되어져야 하며, 출입자를 식별하고 기록·관리하여야 한다. 또한 출입자 기록 대장은 정기적으로 점검하여야 한다.
				7.2.3	내부설비	화재·수재 등의 각종 재해에 대비한 시설을 충분히 설치하여야 하고, 비상연락장치 및 비상구, 물리적 접근통제 및 시건장치를 설치하여야 한다.
		7.3	장비보호	7.3.1	주요 시스템 보호	신청기관내의 주요 시스템에 대한 별도의 출입통제를 실시하거나 이중의 보호장치를 설치하고, 시스템관리자는 주요 시스템 접근에 대한 보안대책을 수립하여야 한다.
				7.3.2	장비의 배치	장비는 환경적인 위협과 위험, 불법 접근에 대한 위험을 감소시키기 위해 적절한 위치에 배치하고 이를 보호하여야 한다.
				7.3.3	전원공급	전원공급 이상이나 기타 전기관련 사고 발생시 전원을 지속적으로 공급하기 위하여 장비 제조업체의 사양에 따라 적절히 관리하여야 한다.
				7.3.4	케이블 보호	데이터를 송·수신하거나 정보서비스를 지원하는 전력 및 통신 케이블은 방해되거나 손상을 입지 않도록 보호하여야 한다.
				7.3.5	장비의 보수	장비는 지속적인 가용성과 무결성을 위하여 장비 제공자가 지시한 명세에 따라 유지보수를 하여야 하고 유지·보수에 대한 기록을 남겨야 한다.

	통제분야		통제목적		통제사항	통제내용
7	물리적 보안	7.3	장비보호	7.3.6	장비의 안전한 폐기 및 재사용	중요한 정보를 담고 있는 저장 매체의 폐기시에는 이를 물리적으로 파기하여야 하며, 중요 데이터나 정품 소프트웨어는 폐기하기 전에 매체에 기록된 내용이 완전히 삭제되어 복구가 불가능한지 확인하고 점검하여야 한다.
		7.4	사무실 보호			책상 위에 중요한 문서나 저장 매체를 남겨놓지 않도록 하고, 통상 근무시간 동안이나 그 외의 시간에 비인가된 자에 의한 정보 접근, 손상을 방지하기 위하여 컴퓨터 화면에 정보처리에 관한 사항을 남겨놓지 않도록 하여야 한다.
8	시스템 개발보안	8.1	분석 및 설계 보안관리	8.1.1	보안 요구사항 정의	새로운 시스템 개발, 기존시스템 개선시 보안요구사항을 문서로 명확히 하여야 하며, 보안요구사항에는 사용자 접근권한의 부여원칙과 접근통제 유형 등을 포함하여야 한다.
				8.1.2	입력 데이터 검증	응용시스템 설계시 입력 요구사항을 정의하고 문서화하여야 하며, 입력 데이터의 정확성, 무결성, 신뢰성을 판단하기 위한 표준을 마련하여야 한다.
				8.1.3	내부 처리의 검증	응용시스템 설계시 내부처리 요구사항을 정의하고 문서화하여야 하며, 응용소프트웨어의 처리 작업을 검증하고, 무결성을 회복할 수 있는 기능을 포함하여야 한다.
				8.1.4	출력 데이터 검증	응용시스템 설계시 출력 요구사항을 정의하고 문서화하여야 하며, 출력 데이터의 정확성, 무결성, 신뢰성을 판단하기 위한 대책을 마련하여야 한다.

	통제분야		통제목적		통제사항	통제내용
8	시스템 개발 보안	8.1	분석 및 설계 보안관리	8.1.5	인증 및 암호	응용시스템 설계시 반드시 사용자 인증에 대한 보안 요구사항을 고려하여야 한다. 중요한 메시지의 경우 무결성이 요구될 때 메시지 인증기법을 적용하고 비밀성이 요구될 시 암호화를 적용하여야 한다.
				8.1.6	보안기록 관리	응용시스템 설계시 사용자의 인증, 데이터 분실, 수정, 오남용 등을 점검하고 방지하기 위하여 보안에 관련된 로그, 감사증적 등을 확보할 수 있는 기능을 반영하여야 한다.
		8.2	구현 및 이행 보안관리	8.2.1	구현 및 시험	응용시스템 구현시 코딩표준에 따라 응용시스템을 구현하고, 보안요구사항에 대한 시험을 수행하여야 한다.
				8.2.2	운영환경 이행보안	운영 프로그램의 수정은 적절한 권한을 지닌 사람만이 시행하여야 하고, 운영시스템은 실행코드만 보유하여야 한다. 실행코드는 성공적인 시험과 사용자 인수 후에 실행하여야 한다.
				8.2.3	시험 데이터의 보안	시험 데이터는 운영데이터에 준하여 보호하고 통제하여야 하며, 운영환경에 대하여 적용되는 접근통제 절차를 시험환경에도 적용하여야 한다. 운영데이터가 시험환경으로 복사될 경우 허가절차를 수립하여 이행하고 시험 완료 후 운영데이터는 시험시스템에서 삭제하여야 한다. 운영데이터 사용 및 복사는 기록을 남겨야 한다.
				8.2.4	소스 프로그램의 접근보안	소스 프로그램은 실제 운영 환경에 보관하지 않는 것을 원칙으로 하며, 소스 프로그램 관리자는 각 운영시스템 별로 지정하여야 한다. 또한 소스 프로그램 접근에 대한 통제절차를 수립하고 이행하여야 한다.

	통제분야		통제목적		통제사항	통제내용
8	시스템 개발 보안	8.3	변경관리	8.3.1	변경관리 절차	정보시스템의 파괴와 손상을 최소화하기 위하여 공식적인 변경관리 절차를 수립하고 이행하여야 한다.
				8.3.2	운영체제 변경시의 검토	운영체제 변경이 필요한 경우 응용시스템의 운영이나 보안에 미치는 영향을 분석, 검토하여야 한다.
				8.3.3	소프트웨어 패키지 변경	소프트웨어 패키지는 가능한 수정하지 않고 사용하고, 패키지 변경시에는 공급자의 동의를 얻으며, 수정이 가능한지 확인하여야 한다. 모든 변경사항은 시험하고 문서화하여야 한다.
9	암호 통제	9.1	암호 정책			암호사용에 대한 정책을 수립하여야 한다.
		9.2	암호사용			암호 정책에 따른 암호 사용시 적절한 암호 알고리즘의 유형, 신뢰성 및 키 길이를 결정하여야 한다.
		9.3	키관리			암호 키에 대한 관리지침, 절차 및 방법을 마련하고 필요시 복구방안을 마련하여야 한다.
10	접근 통제	10.1	접근통제 정책	10.1.1	정책의 문서화	업무 요구사항에 따라 접근 통제의 방법과 범위 등을 정의하고 문서화하여야 한다.
				10.1.2	정책의 내용	접근통제 정책은 데이터, 프로그램, 주요 시스템, 네트워크 등에 대한 접근제한을 포함하여야 하며, 여기에는 보안요구사항, 데이터 및 서비스 접근시의 법적, 계약적 제한, 분산 네트워크상의 접근권한 관리 등을 포함하여야 한다.
				10.1.3	접근 통제 규칙	항상 존재하는 규칙과 일정기간이나 선택적으로 존재하는 규칙에 대한 구분, 실행 전에 관리자의 승인을 필요로 하는 규칙과 그렇지 않은 규칙의 구분 등을 포함한 접근 통제 규칙을 명시하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.1	접근통제 정책	10.1.4	접근통제 방법	접근통제 방법은 정책 및 절차에 의해 결정된 접근권한을 적절하게 반영하여야 한다.
				10.1.5	접근통제 정책 검토	접근에 대한 모니터링을 통해 정책과의 일치성을 주기적으로 검토하고, 접근통제 정책의 적정성을 확인하여야 한다.
		10.2	사용자 접근 관리	10.2.1	사용자 등록	정보시스템 및 서비스에 대한 접근을 통제하기 위한 공식적인 사용자 등록 및 해지 절차를 마련하여야 한다.
				10.2.2	특수권한 관리	시스템이나 응용프로그램에 대한 통제를 우회할 수 있는 특수권한의 할당 및 사용을 관리하여야 한다.
				10.2.3	사용자 패스워드 관리	사용자 패스워드의 관리절차를 수립하고 이행하여야 한다.
				10.2.4	사용자의 접근권한 검토	데이터나 정보 서비스에 대한 접근을 관리하기 위해서 정기적으로 접근 권한에 대하여서 점검을 하여야 한다.
				10.2.5	사용자의 책임	시스템 및 패스워드 관리 책임은 사용자 자신에게 있음을 주지시키고 관리지침을 제공하여야 한다.
		10.3	접근통제 영역	10.3.1	네트워크 접근	비인가된 접근을 막기 위해 네트워크의 내·외부 연결통제, 사용자 터미널과 컴퓨터 서비스간에 물리적 및 논리적 경로의 통제, 사용자 인증, 고장 진단 포트에 대한 접근 통제 등을 포함한 네트워크 접근정책을 수립하고 이행하여야 한다.
				10.3.2	운영체제 접근	안전한 로그온 절차, 식별 및 인증관리, 필요시 터미널 자동확인 등을 포함하여 시스템의 운영체제 접근을 통제하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.3	접근통제 영역	10.3.3	응용 프로그램 접근	사용자 접근이 허가되지 않은 응용 프로그램의 기능들에 대한 정보 제공을 제한하여야 한다. 또한 민감한 정보를 처리하는 응용 프로그램의 출력물은 허가된 위치에서만 전달하여야 한다. 민감한 응용 시스템은 반드시 일반적인 환경과 분리하여야 한다.
				10.3.4	데이터베이스 접근	데이터베이스의 뷰, 레코드 또는 필드 레벨에서의 데이터에 대한 접근통제, 데이터사전 및 데이터베이스 유틸리티에 대한 접근통제, 민감 정보의 암호화 등을 통해 데이터베이스내의 정보를 보호하여야 한다.
11	운영관리	11.1	운영 절차와 책임	11.1.1	운영절차의 문서화	보안정책에 의해 정의된 운영지침과 절차는 문서화하여 관리하여야 한다. 운영관리를 외부에 용역을 주는 경우에도 계약서에 이를 반영하여야 한다.
				11.1.2	정보자산의 변경관리	정보시스템 관련 자산들을 조사하고, 모든 변경사항들을 반영할 수 있는 공식적인 관리책임 및 절차를 수립하여야 한다.
				11.1.3	직무 분리	부주의에 의한 또는 고의적인 시스템 오용의 위험을 감소시키기 위해 직무를 분리하고, 직무 분리가 어려운 특수한 경우 별도의 관리감독 대책을 수립하여야 한다.
				11.1.4	개발과 운영환경의 분리	원칙적으로 개발, 시험, 운영 환경을 분리하여야 한다. 또한 응용프로그램을 개발환경으로부터 운영환경으로 이전하는 절차를 정의하고 문서화하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영 관리	11.1	운영 절차와 책임	11.1.5	외부 운영 설비·관리	외부자가 정보시스템 및 장비를 관리하는 경우 데이터의 손상, 손실 등의 상황을 고려하여 통제방안을 수립하고 계약서에 반영하여야 한다.
		11.2	시스템 운영	11.2.1	시스템 도입	정보시스템의 도입을 위해서 도입계획 및 정책을 수립하여야 한다.
				11.2.2	시스템 인수	새로운 정보시스템의 설치 또는 수정에 따른 인수기준을 수립하고, 시스템 구매 계약서에 반영하여야 한다. 또한 시스템은 이 기준에 의해 시험을 한 후 인수하여야 한다.
				11.2.3	성능관리	신청기관에서 요구되는 성능 요구사항을 충족시킬 수 있도록 성능관리를 수행하여야 한다.
				11.2.4	용량관리	신청기관에서 요구되는 용량 요구사항을 충족시킬 수 있도록 용량계획을 통해 적정한 용량을 확보하고, 주어진 용량을 최적으로 사용할 수 있는 관리방안을 수립하여 이에 따른 용량관리를 수행하여야 한다.
				11.2.5	백업 및 복구 관리	데이터 및 장비의 무결성과 가용성을 유지하기 위해 백업 계획을 수립하여 이행하여야 하며, 사고 발생시 적시에 복구할 수 있도록 관리하여야 한다.
				11.2.6	장애관리	시스템의 장애시 효과적으로 대응하기 위해 탐지, 기록, 분석, 복구, 보고 등 적절한 조치를 취하여야 한다.
				11.2.7	로그관리	시스템 운영의 확인이나 사고조사를 위해 활동에 대한 기록을 남기고 주기적으로 검토하여야 한다.
				11.2.8	보안 시스템 운영	보안시스템에 대해서는 그 유형별로 설치, 운영에 대한 절차를 수립하고, 절차이행을 주기적으로 검토하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영 관리	11.3	네트워크 운영	11.3.1	네트워크 운영대책	네트워크 운영 보안 유지를 위해 직무 분리, 접근권한 통제, 원격접속 설비 관리, 네트워크 분리 등을 위한 책임 및 절차 등을 포함한 대책을 수립하여야 한다.
				11.3.2	인터넷 접속관리	인터넷망과 접속시 침입차단시스템을 통하여 접근통제를 수행하여야 하며, 필요시 침입탐지시스템 등을 활용하여 접근을 모니터링 하여야 한다.
				11.3.3	원격운영 관리	네트워크를 통해 시스템을 운영하는 경우 원칙적으로 시스템 관리는 내부의 특정 터미널에서만 할 수 있도록 제한하고, 외부에서 네트워크를 통하여 시스템을 관리할 경우에는 사용자 인증, 암호 및 접근통제 기능을 설정하여야 한다.
		11.4	매체 및 문서관리	11.4.1	매체 취급 및 보관	허가되지 않은 유출이나 오용으로부터 정보를 보호하기 위해, 매체의 취급 및 보관에 대한 절차를 수립하고 운영하여야 한다.
				11.4.2	매체의 폐기	매체 폐기를 부주의하게 이행하여 외부자에게 주요정보가 누출되지 않도록 폐기지침을 수립하고 운영하여야 한다.
				11.4.3	시스템 문서의 보안	보안절차, 운영매뉴얼, 운영기록 등 주요 시스템 문서들은 안전하게 보관하고 적절한 폐기절차에 따라 폐기하여야 한다.
		11.5	악성 소프트웨어 통제			바이러스 등의 악성 소프트웨어로부터 시스템을 보호하기 위해 악성 소프트웨어들을 예방하고 탐지, 대응하는 대책을 수립하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영 관리	11.6	이동컴퓨팅 및 원격 작업	11.6.1	이동 컴퓨팅	휴대용 정보통신기기의 사용시에 사업정보를 보호하기 위한 보안 정책을 수립하고, 내부 네트워크로의 연결 및 공공장소에서의 사용에 대한 정책을 수립하여야 한다.
				11.6.2	원격 작업	재택 근무와 같은 원격 작업 수행시 이에 대한 물리적, 논리적 보호를 위한 정책과 절차를 마련하여야 한다.
12	전자 거래 보안	12.1	교환 합의서			신청기관간의 정보 및 소프트웨어 교환시에는 이에 대한 합의가 이루어져야 하고, 관리적 책임 및 절차, 전송의 기술적 기준, 인증기준, 데이터의 책임성 등을 반영한 교환 합의서를 작성하여야 한다.
		12.2	전자거래 보안관리			전자거래 시 사기, 계약 분쟁, 정보의 노출 및 수정 등으로부터 보호하기 위해 신원확인, 무결성, 암호화, 부인방지 등의 대책을 수립하여 운영하여야 한다.
		12.3	전자우편			전자 우편 서비스에 대한 가용성, 전자우편 내용에 대한 무결성 및 기밀성과 이에 따른 책임과 위험을 고려한 보안지침 및 대책을 수립하여 운영하여야 한다.
		12.4	공개서버의 보안관리			웹서버 등에 정보를 공개할 경우 정보에 대한 수집, 저장 및 공개에 따른 허가 및 게시절차를 수립하여야 하고, 공개서버에 대한 물리적, 논리적 보안대책을 수립하고 운영하여야 한다.
		12.5	이용자 공지사항			전자거래의 안전한 이행을 위하여 이용자에게 해킹위험, 계정 및 패스워드 관리, 접속관리 등에 대한 공지를 통해 안전거래 준수를 권고하여야 한다.

	통제분야		통제목적		통제사항	통제내용
13	보안사고 관리	13.1	대응 계획 및 체계	13.1.1	대응계획 수립	보안사고의 정의 및 범위, 긴급연락체계 구축, 보안사고 발생시 보고 및 대응 절차, 사고 복구조직의 구성, 교육계획 등을 포함한 보안사고 대응 계획을 수립·이행하여야 한다.
				13.1.2	보안사고 대응체계 구축	보안사고의 대응이 신속하게 이루어질 수 있도록 중앙 집중적인 대응체계를 구축하고, 대응체계에는 내부직원뿐 아니라 외부기관 및 전문가들과의 협조체계를 반영하여야 한다.
		13.2	대응 및 복구	13.2.1	보안사고 대응 교육 및 훈련	보안사고 대응 계획, 절차 및 방법에 대하여 정기적으로 교육을 실시하여야 하며 사고 처리 후 재발 방지를 위하여 필요한 교육훈련을 실시하여야 한다
				13.2.2	보안사고 보고	사고의 징후 또는 보안사고 발생을 인지한 때에는 보고체계에 따라 가능한 한 신속히 보고하여야 한다. 시스템이나 네트워크의 보안취약점과 소프트웨어 기능장애 또한 신속히 보고하여야 한다.
				13.2.3	보안사고 처리 및 복구	보안사고 보고시 처리, 복구 절차에 따라 처리와 복구를 신속히 이행하여야 한다.
		13.3	사후관리	13.3.1	보안사고 분석 및 정보의 공유	보안사고가 처리되고 종결된 후 이에 대한 분석을 이행하여야 하며, 그 결과를 보고하여야 한다. 또한 사고에 대한 정보와 발견된 취약성들을 관련 신청기관과 임직원에게 공유하여야 한다.
				13.3.2	재발방지	보안사고로부터 얻은 정보를 활용하여, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하여야 한다. 이를 위해 필요한 경우 정책, 절차, 조직 등의 보안체계에 대한 변경을 하여야 한다.

	통제분야		통제목적		통제사항	통제내용
14	검토, 모니터링 및 감사	14.1	법적 요구사항 준수 검토	14.1.1	요구사항 명시	정보시스템에 대해 관련된 모든 법, 규제, 계약, 정책, 기술상의 요구사항을 정의하고 문서화하여야 하며, 이들 요구사항을 만족시키기 위해 필요한 특정 통제나 개별 책임 등도 정의하고 문서화하여야 한다.
				14.1.2	준수 검토	정보통신망이용촉진및정보보호등에관한법률, 신용정보의이용및보호에관한법률 등의 개인정보보호 관련법 및 저작권법, 컴퓨터프로그램보호법 등 지적재산권법 등의 관련 법규의 준수여부를 검토하여야 한다.
				14.1.3	증거자료 수집	보안사고 처리 및 계약 증빙을 위하여 신청기관이나 개인에 대한 소송을 지원하기 위한 적정한 증거 자료를 확보하여야 한다.
		14.2	정보보호 정책 준수 검토	14.2.1	검토 계획	검토의 대상, 주기, 방법, 범위, 절차, 검토자를 포함한 검토계획 및 정책이 수립되어야 한다. 이를 근거로 보안요구사항에 대한 통제와 책임의 준수에 대한 적정성을 검토하여야 한다.
				14.2.2	정책의 준수	모든 정보보호 정책, 절차의 준수여부를 검토하여야 한다.
				14.2.3	기술적 점검	정보시스템이 정보보호표준 및 절차에 따라 운영·관리되고 있는지 정기적으로 기술적 점검을 실시하여야 한다. 이에 따라 취약성들을 발견한 후 필요한 조치를 취하여야 한다.

	통제분야		통제목적		통제사항	통제내용
14	검토, 모니터링 및 감사	14.3	모니터링	14.3.1	접근 및 사용 모니터링	사용자의 시스템, 네트워크 사용 및 접근이 명확하게 허용된 범위 안에 있는지를 확인하기 위해 모니터링 절차를 수립하고 이행하여야 한다. 모니터링 결과는 정기적으로 점검하여야 하고 위험의 정도에 따라 점검 주기를 결정하여야 한다.
				14.3.2	감사기록 분석 및 보관	모니터링을 위한 감사 기록을 생성하고, 분석하며 일정 기간 동안 보관하여야 한다.
				14.3.3	시각 동기화	감사 기록의 명확성을 보장하고 법적인 자료나 징계 자료로서 효력을 갖기 위해서는 시스템 시각을 정확히 설정하여야 한다.
		14.4	보안감사	14.4.1	보안감사 계획 및 이행	보안 감사 대상, 범위, 주기, 방법, 절차, 감사자, 감사도구를 포함한 보안감사 계획을 수립하고 이행하여야 한다.
				14.4.2	감사결과 및 사후관리	감사의 결과에 따라 감사보고서를 작성하고 적정한 책임자에게 보고하며, 감사 지적 내용이 이행되도록 사후관리하여야 한다.
15	업무 연속성 관리	15.1	업무연속성 관리 체계 수립	15.1.1	업무연속성 관리 과정 수립	개시단계, 업무연속성전략수립단계, 구현단계, 운영관리단계 등 업무연속성관리를 위한 과정을 사전에 정의하여야 한다. 개시단계에는 업무연속성관리에 대한 정책 수립 및 범위설정, 자원분배를 포함하여야 하며, 업무연속성전략수립단계는 업무영향분석을 통해 이루어져야 한다. 구현단계에는 재해복구 및 위험감소 대책, 업무연속성계획의 문서화를 포함하여야 하며, 운영관리단계에는 시험, 교육훈련, 검토 및 갱신을 포함하여야 한다.

	통제분야		통제목적		통제사항	통제내용
15	업무 연속성 관리	15.1	업무연속성 관리 체계 수립	15.1.2	업무연속성 계획 프레임워크 수립	업무별 연속성 계획의 이행에 필요한 조건, 응급절차, 대체절차 등을 고려하여 연속성 계획들이 일관성을 유지할 수 있도록 프레임워크를 수립하여야 한다.
		15.2	업무연속성 계획 수립과 구현	15.2.1	업무영향 분석	재난재해별로 업무에 미칠 수 있는 영향을 피해규모와 복구에 소요되는 시간 등을 고려하여 분석하고 그 결과를 기초로 구체적인 업무복구목표 및 복구를 위한 최소한의 요구사항을 설정하여야 한다.
				15.2.2	업무연속성 계획 수립	업무복구목표 및 최소 요구사항을 구현하기 위한 여러 대안들을 평가하여 업무연속성을 위한 전략을 수립하고 대책 구현을 위한 계획을 수립하여야 한다.
				15.2.3	업무연속성 계획 구현	업무연속성계획에서 수립한 위험감소 조치 및 재해복구를 위한 설비를 구현하며 필요한 계획 및 절차 등을 문서화하여야 한다.
		15.3	업무 연속성 계획 시험 및 유지관리	15.3.1	업무연속성 계획 시험	환경의 변화 또는 부정확한 전제 등으로 인한 오류를 제거할 수 있도록 지속적인 시험을 수행하며, 시험 계획에는 시기, 방법, 절차 등을 포함하여야 한다.
				15.3.2	업무연속성 계획 유지·관리	업무연속성계획에 대해 정기적인 교육 및 훈련을 실시하고 지속적인 검토와 평가 및 변경관리를 수행하여야 한다.

■ 「정보보호관리체계 인증 등에 관한 고시」 [별지 제1호서식] <개정 2012. 3. 15.>

정보보호관리체계인증기관 지정신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	처리기간	90일

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	직원 수	인증심사업무를 전담하는 직원 수	

「정보보호관리체계 인증 등에 관한 고시」 제4조제1항의 규정에 따라 위와 같이 정보보호관리체계 인증기관 지정을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

방송통신위원회 귀중

신청(신고)인 제출서류	1. 정관 1부. 2. 별지 제2호서식의 인증심사업무를 전담하는 직원 보유현황과 이를 증명할 수 있는 서류 1부. 3. 별표 제1호에 따른 업무수행능력심사를 위하여 필요한 서류 1부.	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

처 리 절 차

신청서 작성	→	접 수	→	심 사	→	지정여부 결정	→	지정서 교부
신청인		처 리 기 관 (방송통신위원회)		처 리 기 관 (방송통신위원회)		처 리 기 관 (방송통신위원회)		처 리 기 관 (방송통신위원회)

210㎜×297㎜[백상지(80g/㎡)]

■ 「정보보호관리체계 인증 등에 관한 고시」 [별지 제2호서식] <개정 2012. 3. 15.>

인증심사업무를 전담하는 직원의 보유현황

(제1쪽)

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	직원 수	인증심사업무를 전담하는 직원 수	

일련번호	성명	주소		최종학력	해당요건
		생년월일	입사일	취득학위 및 학과	

유의사항

1. 「해당요건」란에는 별표 1의 요건 중 당해 인증심사업무를 전담하는 직원이 충족하는 요건을 기재한다.
   예시) 학력 및 경력기준 제2호 가목
2. 기재된 최종학위를 증명할 수 있는 직원의 졸업 또는 학위증명서 사본을 제출하여야 한다.
3. 별표 2의 「자격 및 경력기준」을 충족하는 직원은 기술자격증 사본 등 자격을 취득하였음을 확인할 수 있는 서류를 함께 제출하여야 한다.
4. 정보통신유관경력 또는 정보보호유관경력을 증명할 수 있는 경력증명서(근무부서 또는 담당업무 등이 기재되어야 한다)와 해당 직원이 신청업체에 현재 근무하고 있음을 확인할 수 있는 재직증명서를 함께 제출하여야 한다.

210mm×297mm[백상지(80g/㎡)]

인증심사업무를 전담하는 직원의 보유현황

(제2쪽)

일련번호	성명	주소		최종학력	해당요건
		생년월일	입사일	취득학위 및 학과	

210mm×297mm[백상지(80g/㎡)]

■ 「정보보호관리체계 인증 등에 관한 고시」 [별지 제3호서식] <개정 2012.3.15.>

정보보호수행실적 명세서

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	정보보호 수행실적 총계	외 건 (총 천원)	

일련번호	정보보호 수행실적(프로젝트명) 대상기관(기업)명	수행 기간	계약 금액(천원)	과제책임자	구분

유의사항

1. 계약금액란에는 정보보호에 관한 업무를 수행한 대가로서 지급받은 대금을 기재하고, 구분란에는 정보보호에 관한 감사, 감리, 진단, 인증, 컨설팅 등으로 실적을 구분하여 기재한다.

210mm×297mm[백상지(80g/㎡)]

■ 「정보보호관리체계 인증 등에 관한 고시」 [별지 제4호서식] <개정 2012.3.15.> (제1쪽)

정보보호관리체계인증기관 지정서

등록번호 :

업체명 :

대표자 :

주소 :

지정의 유효기간 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조 및 같은 시행령 제48조에 따라 위와 같이 정보보호관리체계인증기관으로 지정합니다.

년 월 일

방송통신위원회위원장 직인

210mm×297mm[백상지(120g/㎡)]

(제2쪽)

CERTIFICATE OF DESIGNATION
AS
ISMS Certification Authority

Registry Number :

Name of Organization :

Name of Representative :

Address :

Period of Validity :

This is to certify that the above mentioned organization is designated Information Security Management System (ISMS) Certification Authority in accordance with Article 47 of 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」 and Article 48 of the Enforcement Decree of the same Act.

Date of Issuance:

Signed by
the Chairman of Korea Communications Commission
Republic of Korea

210㎜×297㎜[백상지120g/㎡]

■ 「정보보호관리체계 인증 등에 관한 고시」 [별지 제5호서식] <개정 2012. 3. 15.>

정보보호관리체계인증 신청서

※ [ ]에는 해당되는 곳에 √표를 하고, 어두운 부분은 신청인이 작성하지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명	사업자등록번호
	주소	전화번호
	대표자	

인증신청의 구분	[ ] 처음으로 인증신청을 하는 때 [ ] 유효기간의 만료로 다시 인증신청을 하는 때 [ ] 인증의 범위에 중요한 변경이 있어서 다시 인증신청을 하는 때
정보보호관리체계의 범위	
정보보호관리체계의 범위에 포함되어 있는 종업원의 수	
정보보호관리체계의 범위에 포함되어 있는 서버의 수	

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제4항, 동법 시행령 제50조에 따라 위와 같이 정보보호관리체계의 인증을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

(인증기관명) 귀하

신청(신고)인 제출서류	정보보호관리체계의 내역서 1부.	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

처 리 절 차

신청서 작성	→	접 수	→	협 의	→	인증심사	→	인증서 교부
신청인		처 리 기 관 (인증기관)		처 리 기 관 (인증기관)		처 리 기 관 (인증기관)		처 리 기 관 (인증기관)

210㎜×297㎜[백상지(80g/㎡)]

■ 「정보보호관리체계 인증 등에 관한 고시」 [별지 제6호서식] <개정 2012.3.15.> (제1쪽)

정보보호관리체계인증서

인증번호 :

업체명 :

대표자 :

주소 :

인증의 범위 :

유효기간 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제4항, 같은 법 시행령 제50조에 따라 위와 같이 정보보호관리체계를 인증합니다.

년 월 일

(인증기관장) 직인

210mm×297mm[백상지(120g/㎡)]

(제2쪽)

CERTIFICATE
OF
Information Security Management System

Certificate Number :

Name of Organization :

Name of Representative :

Address :

Scope of Certification :

Period of Validity :

This is to certify that the above mentioned organization is compliant to the assessment standard for Information Security Management System certification in accordance with Article 47, Paragraph 1 and 4 of 「Act on Information Network Utilization and Data Protection, etc.」 and Article 50 of the Enforcement Decree of the same Act.

Date of Issuance :

Signed by
the President of ISMS Certification Authority
Republic of Korea

210mm×297mm[백상지(120g/㎡)]

■ 「정보보호관리체계 인증 등에 관한 고시」 [별지 제7호서식] <개정 2012. 3. 15.>

정보보호관리체계 인증서 추가발급 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명	사업자등록번호
	주소	전화번호
	대표자	

변경사유	

위와 같이 정보보호관리체계 인증서의 추가발급을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

(인증기관명) 귀하

제출서류	해당없음	수수료 없 음

210mm×297mm[백상지(80g/㎡)]

■ 「정보보호관리체계 인증 등에 관한 고시」 [별지 제8호서식] <개정 2012. 3. 15.>

정보보호관리체계 인증서 변경 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		

변경 내용	변경전	(국문)
		(영문)
	변경후	(국문)
		(영문)
변경사유		

위와 같이 정보보호관리체계 인증서 변경을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

(인증기관명) 귀하

제출서류	해당없음	수수료 없 음

210mm×297mm[백상지(80g/㎡)]

정보보호관리체계 인증 등에 관한 고시

[시행 2008.5.19] [고시 제2008 - 11호, 2008.5.19, 제정]

제1장 총칙

제1조(목적) 이 고시는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하"법"이라 한다) 제47조제2항 및 같은 법 시행령 제47조제2항·제48조제1항제3호·제5항·제50조제6항에 따른 정보보호관리체계 인증에 관한 정보보호관리기준·지정에 필요한 업무수행능력 심사 등에 관한 세부사항과 그 밖에 정보보호관리체계 인증에 관하여 필요한 사항에 대하여 정하는 것을 목적으로 한다.

제2조(용어의 정의) 이 기준에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "업무수행능력심사"란 정보보호관리체계인증기관으로 지정받고자 신청한 법인 또는 단체의 업무수행능력을 세부평가기준에 따라 심사하는 것을 말한다.
2. "정보보호관리체계인증기관"이란 법 제47조에 따른 한국정보보호진흥원과 방송통신위원회가 지정하는 기관을 말한다.
3. "인증"이란 신청기관이 수립하여 운영하고 있는 정보보호관리체계가 인증심사기준 등에 적합함을 정보보호관리체계인증기관이 승인하는 것을 말한다.
4. "인증심사"란 신청기관이 수립하여 운영하는 정보보호관리체계가 인증심사기준 등에 대하여 서면심사 및 기술심사의 방법으로 확인하는 것을 말한다.
5. "정보보호관리과정(이하 ‘관리과정’이라 한다)"이란 정보보호관리체계를 수립·운영하기 위하여 유지·관리하여야 할 과정으로 다음 각목의 5단계 활동을 말한다.
   가. 정보보호정책 수립
   나. 정보보호관리체계 범위설정
   다. 위험관리
   라. 구현
   마. 사후관리
6. "신청기관"이란 이 고시에 따라 정보보호관리체계 인증을 취득하고자 신청한 업체 및 기관 등을 말한다.
7. "외부자"란 신청기관의 직원이 아닌 자를 말한다.

8. "정보보호대책"이란 신청기관이 정보보호관리체계를 수립·운영하기 위하여 별표 6에서 선택한 통제사항을 말한다.

제2장 정보보호관리체계인증기관의 지정 등

제1절 정보보호관리체계인증기관의 지정신청

제3조(정보보호관리체계인증기관의 지정공고) 방송통신위원회는 법 제47조 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」(이하 "영"이라 한다) 제48조에 따라 정보보호관리체계인증기관을 지정할 필요가 있는 때에는 미리 접수신청기간과 신청요령 등을 정하여 관보 및 인터넷 홈페이지에 20일 이상 공고하여야 한다.

제4조(제출서류 등) ①정보보호관리체계인증기관 지정을 신청하는 자는 별지 제1호서식의 정보보호관리체계인증기관 지정신청서를 방송통신위원회에 제출하여야 한다.

②영 제48조제1항제2호에 따라 제1항의 정보보호관리체계인증기관지정신청서에 첨부하여야 하는 "인증심사업무를 전담하는 직원의 보유현황"의 제출서식은 별지 제2호서식과 같다.

③영 제48조제1항제3호에 따른 "업무수행능력심사를 위하여 필요한 서류"라 함은 별표 1과 같다.

제2절 인증심사업무를 전담하는 직원의 자격요건 및 업무수행능력심사

제5조(인증심사업무를 전담하는 직원의 요건 등) ①영 제47조제1항제1호 및 제2항에 따른 "인증심사업무를 전담하는 직원(이하 "인증심사원"이라 한다)의 요건"은 별표 2와 같다.

②법 제47조에 따른 정보보호관리체계인증기관으로 지정신청 하고자 하는 자는 제1항의 인증심사원의 요건을 만족하여야 한다.

제6조(업무수행능력심사 기준 등) ①영 제47조제1항제2호 및 제2항에 따른 업무수행능력심사의 세부평가기준은 별표 3과 같다.

②심사위원회는 제1항에 따라 심사위원 각자가 부여한 점수 중 최고점과 최저점을 제외한 점수들의 평균이 80점 이상인 자를 선별한다.

③심사위원회는 제2항에 따라 선별된 자에 대하여 심사결과 검증 및 업무수행능력의 적합성을 판단한다.

제7조(업무수행능력의 적합성 인정) 방송통신위원회는 제5조 및 제6조에 따라 심사한 결과를 토대로 정보통신망 안전성 및 신뢰성 확보를 위한 종합적인 정보보호관리체계의 업무를 수행하는 자로서
적합한지 여부를 결정한다.

제8조(정보보호관리체계인증기관지정서) 영 제48조제3항에 따른 "정보보호관리체계인증기관 지정서"는 별지 제4호서식과 같다.

제3절 인증기관 심사위원회 구성·운영

제9조 (심사위원회의 구성) ①방송통신위원회는 영 제48조제1항에 따라 정보보호관리체계인증기관의 지정신청을 받은 경우 영 제48조제4항에 따른 심사위원회를 구성하여 다음 각 호의 심사업무를 수행하게 하여야 한다. 이 경우 방송통신위원회는 필요하다고 인정하는 때에는 분과위원회 또는 작업반을 둘 수 있다.

1. 영 제48조제3항에 따른 현장실사
2. 별표 2에 따른 인증심사원의 자격요건 및 별표 3에 따른 업무수행능력심사 세부평가
3. 정보보호관리체계인증기관 지정의 적합성 결정
4. 그 밖에 지정심사와 관련되는 업무

②심사위원회는 5인이상 10인이내의 위원으로 구성하되, 위원은 정보보호전문가, 회계사, 기술사, 변호사 등 업무수행능력심사를 수행할 수 있는 학식과 경험이 있는 자 중 방송통신위원회가 위촉하며, 위원장은 위원 중에서 호선한다.

③제2항에 따른 심사위원은 최근 2년간 지정신청자와 관련된 업무를 수행하지 않아야 한다.

④위원에 대하여는 예산의 범위안에서 수당과 여비를 지급할 수 있다. 다만, 공무원인 위원이 소관업무와 관련하여 참석한 경우에는 그러하지 아니하다.

제10조(심사위원회의 운영) ①위원장은 심사위원회의 업무를 통할하며 위원회를 대표하여 방송통신위원회에 정보보호관리체계인증기관 지정 적합성 여부에 대한 심사결과를 제출한다.

②위원장이 부득이한 사유로 직무를 수행할 수 없을 때에는 위원장이 미리 지정한 위원이 그 직무를 대행한다.

제3장 정보보호관리체계의 인증기준 등

제1절 정보보호관리체계 인증신청

제11조(신청기관의 준비사항) 신청기관은 다음 각 호의 인증심사기준에 따라 정보보호관리체계를 수립하여 최소 3개월 이상 운영하여야 한다.

1. 별표 4에 따른 관리과정 요구사항
2. 별표 5에 따른 문서 작성 및 관리 통제사항
3. 별표 6에 따른 정보보호관리 통제사항에서 선택한 사항(신청기관은 자신의 정보보호관리체계의 규모 및 사업특성 등을 고려하여 별표 6에서 적절한 항목을 선택할 수 있다)

제12조(인증의 신청) ①영 제50조제1항에 따라 인증을 신청하는 자는 별지 제5호서식의 정보보호관리체계인증신청서를 정보보호관리체계인증기관에 제출하여야 한다. 이 경우 정보보호관리체계의 인증을 받고자 하는 범위를 정하여 신청할 수 있다.

②제1항에 따라 신청을 받은 정보보호관리체계인증기관은 정보보호관리체계 특성상 신청기관이 지정한 정보보호관리체계만을 분리하여 심사할 수 없는 경우에는 신청기관과 상의하여 인증의 범위를 변경할 수 있다.

제13조(인증심사계약의 체결) 정보보호관리체계인증기관은 영 제50조제2항에 따라 신청기관과 협의한 후 심사기간, 심사인원, 심사수수료, 인증의 범위 등을 포함하는 인증심사계약을 체결하여야 한다.

제2절 정보보호관리체계 인증심사 기준 및 방법

제14조(인증심사기준) 정보보호관리체계의 인증심사기준은 별표 4부터 별표 6까지와 같다.

제15조(인증심사요소) ①정보보호관리체계인증기관은 신청기관이 수립한 관리과정을 체계적으로 관리·유지하고 있는지 여부를 판단하기 위하여 다음 각 호의 사항을 심사하여야 한다.

1. 정보보호정책 수립 : 신청기관에 적합한 정보보호정책의 수립, 조직의 구성·운영, 책임성의 명확한 설정 여부
2. 정보보호관리체계 범위설정 : 정보보호관리체계 수립·운영을 위한 관리범위 설정 및 정보자산의 현황조사 여부
3. 위험관리 : 위험관리 전략 및 계획 수립, 위험분석·평가, 정보보호대책 선택의 적절성 여부
4. 구현 : 정보보호대책의 구현 및 정보보호 교육·훈련의 효과성 여부
5. 사후관리 : 정보보호관리체계의 재검토, 모니터링 및 개선, 내부감사 활동의 적절성 여부

②정보보호관리체계인증기관은 신청기관이 정보보호관리체계의 수립 및 이행 활동에 관련된 절차와 운영을 문서화해서 관리하는지에 대하여 심사하여야 한다.

③정보보호관리체계인증기관은 신청기관이 관리과정의 위험평가를 통하여 선택한 통제사항에 대한 정보보호대책을 구현하고 이행하고 있는지에 대하여 심사하여야 한다.

제16조(서면심사) 인증심사원은 신청기관이 영 제50조제1항에 따라 제출한 신청서류를 확인하여 신청기관이 수립한 정보보호관리체계가 별표 4부터 별표 6까지에 따른 인증심사기준에 적합한지에 대하여 심사하여야 한다.

제17조(기술심사) ①인증심사원은 서면심사의 결과를 검증하기 위하여 신청기관이 인증을 신청한 정보보호관리체계가 운영중인 현장을 방문하여 직접 해당 정보보호관리체계의 구축·운영 실태를 확인하여야 한다.

②인증심사원은 제1항에 따른 현장방문시 신청기관의 요청이 있는 경우 인터넷 침해사고 등에 대한 안전성 검사를 위하여 해당 정보보호관리체계에 속한 정보시스템에 대한 모의진단을 실시할 수 있다.

제3절 인증위원회의 구성 및 운영

제18조(인증위원회의 구성) ①정보보호관리체계인증기관의 장은 인증심사원이 실시한 인증심사 결과가 제14조에 따른 인증심사기준에 적합한지 여부를 심의하기 위하여 인증위원회를 구성·운영하여야 한다.

②인증위원회는 5인 이상 10인 이내의 위원으로 구성하되, 위원은 정보보호전문가, 정보시스템감리사, 기술사 등 정보보호분야에 학식과 경험이 있는 자 중 정보보호관리체계인증기관의 장이 위촉하며, 위원장은 위원 중에서 호선한다.

제19조(인증위원회의 운영) ①위원장은 인증위원회의 업무를 통할하며 위원회를 대표하여 정보보호관리체계인증기관의 장에게 인증심사원이 실시한 인증심사 결과가 제14조에 따른 인증심사기준에 적합한지 여부를 심의하고 그 결과를 제출한다.

②정보보호관리체계인증기관의 장은 제1항에 따른 심의를 실시한 때에는 인증심사원이 실시한 심사결과를 위원회 개최 전 5일까지 인증위원회에 제출한다.

제4절 인증서 교부 및 사후관리 등

제20조(인증서 교부) 정보보호관리체계인증기관의 장은 제19조제1항에 따라 인증위원회의 심의결과를 제출받은 경우 신청기관에게 인증심사결과를 통보하고, 신청기관의 정보보호관리체계가 이 고시에서 정한 인증심사기준에 적합하다고 판단된 경우 별지 제6호서식의 정보보호관리체계인증서를 교부하여야 한다.

제21조(정보보호관리체계의 변경) ①인증을 취득한 자는 인증을 받은 정보보호관리체계에 다음 각 호의 어느 하나에 해당하는 중대한 변화가 발생한 경우 발생한 날로부터 3개월 이내에 인증기관의 장에게 변경된 내용을 통보하여야 한다.

1. 신청기관이 수립하여 운영하는 관리체계의 범위가 확대되거나 변경되었을 경우
2. 사업장 변경 및 기업결합 등의 경영환경 변화 등으로 관리체계 운영에 영향을 미치는 경우

②인증기관의 장은 인증을 취득한 자로부터 변경내용을 통보받은 경우 인증을 취득한 자와 협의하여 인증심사 여부를 결정한다.

③제2항에 따라 인증심사를 실시하는 경우에는 제14조부터 제20조까지를 준용한다.

제22조(사후관리) ①영 제52조에 따라 정보보호관리체계인증기관은 인증을 취득한 자가 정보보호관리체계를 지속적으로 유지하고 있는지에 대하여 영 제51조에 따른 유효기간 중 제2절 정보보호관리체계 인증심사 기준 및 방법에 따라 1회 사후관리를 수행한다.

②정보보호관리체계인증기관은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 때에는 인증을 취소하여야 한다.

1. 거짓 그 밖의 부정한 방법으로 정보보호관리체계인증을 받은 때
2. 법 제47조제3항에 따라 인증받은 내용을 홍보하면서 인증의 범위나 유효기간을 속인 경우
3. 제1항에 따른 사후관리에서 정보보호관리체계 인증기준에 적합하지 않게 된 사실이 발견된 때

③정보보호관리체계인증기관이 제2항에 따라 인증을 취소하는 경우에는 인증을 취득한 자에게 통지하고, 제20조에 따라 교부한 정보보호관리체계인증서를 회수하여야 한다.

제23조(인증서 관리) ①정보보호관리체계인증기관은 발급된 인증서의 인증번호, 발급번호, 발급일, 유효기간 등을 관리하여야 한다.

②인증을 취득한 자는 인증서의 분실 등으로 인한 재발급을 받고자 할 경우 별지 제7호서식의 관리체계 인증서 재발급 신청서를 인증기관에 제출하여야 한다.

③인증을 취득한 자가 주소, 업체명 등 인증서 기재사항의 변경을 요청하고자 하는 경우 별지 제8호서식의 인증서 변경신청서를 정보보호관리체계인증기관에 제출하여야 한다.

부칙 <제2008 - 11호,2008.5.19>

이 고시는 고시한 날부터 시행한다.

[별표 1]

업무수행능력심사 규정에 따른 제출서류(제4조제3항관련)

구 분	제 출 서 류
1. 정보보호수행실적을 확인하는 데 필요한 서류	가. 별지 제3호서식에 따른 정보보호수행실적 명세서 및 이를 증빙할 수 있는 자료(결과보고서 등) 나. 계약서 사본 및 세금계산서 등
2. 업무수행능력심사평가표 각호의 세부 평가요소를 평가하기 위하여 필요한 서류	가. 총매출액대비 정보보호분야 매출액의 비율 계산내역(공인회계사 또는 회계담당자가 서명 날인한 서류) 나. 부채비율 및 자기자본 이익률의 계산내역(회결산내역 등 관련 증빙자료) 다. 인증업무 운영체계 관련 규정 및 지침 등 ㅇ 인증기관의 운영체계 및 인증의 품질관리 ㅇ 인증업무를 수행하는 직원에 대한 운영관리 등의 내부규정 ㅇ 인증업무 수행 방법 및 절차
비 고 ※ 방송통신위원회는 정보보호관리체계인증기관 지정 공고시 업무수행능력심사에 필요한 자료의 구성 및 그 세부내용, 제출시기 및 방법 등에 관한 사항을 포함하여야 한다.	

[별표 2]

인증심사업무를 전담하는 직원의 요건(제5조 관련)

학력 및 경력기준	자격 및 경력기준
1. 유관학력 보유의 경우 가. 학사학위를 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 6년 이상인 자 나. 석사학위를 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 3년 이상인 자	1. 유관자격 보유의 경우 가. 기사자격을 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 4년 이상인 자 나. 산업기사자격을 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 7년 이상인 자
2. 비 유관학력 보유의 경우 가. 학사학위를 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 8년 이상인 자 나. 전문학사를 취득한 자로서 정보통신유관경력과 정보보호유관경력의 합이 10년 이상인 자	2. 다음 각목의 1에 해당하는 정보보호자격을 취득한 자로서 2년 이상의 정보보호유관경력이 있는 자 가. 한국정보보호진흥원의 정보보호전문가(SIS) 나. 「정보시스템의 효율적 도입 및 운영 등에 관한 법률」 제14조에 따른 정보시스템감리원 다. 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 공인정보시스템감사사(CISA) 라. 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 공인정보시스템보호전문가(CISSP)

1. "유관자격"이라 함은 「국가기술자격법 시행규칙」 별표 7의 검정대상 기술자격 종목 중 전자계산기, 정보통신, 통신설비, 통신기기, 통신선로, 정보기기운용, 전파통신, 전파전자, 무선설비, 방송통신, 정보관리, 정보처리, 사무자동화 및 전자계산조직응용 종목의 기술자격을 말한다.
2. "유관학력"이라 함은 「고등교육법」에 따른 해당 학교에서 다음 각 목에 해당하는 학과에서 소정의 과정을 이수하고 졸업하거나 그 밖의 관계 법령에 따라 국내 또는 외국에서 이와 동등 이상으로 인정되는 학력을 말한다.
   가. 전자 관련 학과 : 정보전자, 전자, 전자계산, 전기전자제어, 전자정보, 전자제어, 전기전자, 전자전기정보, 전자컴퓨터전기제어, 컴퓨터과학, 전기전자정보, 전자컴퓨터, 메카트로닉스, 전자재료, 제어계측, 반도체
   나. 정보통신 관련 학과 : 전기통신설비, 국제정보통신, 방송설비, 방송통신, 이동통신, 전자통신, 컴퓨터네트워크, 통신, 컴퓨터정보기술, 전파통신, 전기전자통신, 전기전자정

보통신, 전자정보통신, 전자제어통신, 전자통신, 전파, 전파통신, 정보통신, 컴퓨터통신, 항공통신정보, 전자정보통신반도체, 전기전자전파, 통신컴퓨터, 무선통신

다. 정보처리기술 관련 학과 : 시스템, 전산, 정보전산, 컴퓨터제어, 컴퓨터응용제어, 컴퓨터응용, 컴퓨터응용설계, 구조시스템, 컴퓨터정보, 멀티미디어, 정보시스템, 전산통계, 정보처리

라. 그 밖에 교육인적자원부장관이나 해당 교육기관의 장으로부터 전자·통신 및 정보처리기술·정보보호 관련 학과로 인정받은 학과

3. "정보통신유관경력"이라 함은 공공기관, 민간기업, 교육기관 등에서 정보통신서비스(기간통신, 별정통신, 부가통신, 방송서비스 등을 말한다), 정보통신기기(정보기기, 방송기기, 부품 등을 말한다) 또는 소프트웨어 및 컴퓨터 관련 서비스(패키지 소프트웨어, 컴퓨터 관련 서비스, 디지털콘텐츠, 데이터베이스 제작 및 검색 등을 말한다)에 해당되는 분야에서 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 수행한 기간을 말한다.

5. "정보보호유관경력"이라 함은 공공기관, 민간기업, 교육기관 등에서 정보보호를 위한 공통기반기술(암호 기술, 인증 기술 등을 말한다), 시스템·네트워크 보호(시스템 보호, 해킹·바이러스 대응, 네트워크 보호 등을 말한다) 또는 응용서비스 보호(전자거래 보호, 응용서비스 보호, 정보보호 표준화 등을 말한다)에 해당되는 분야에서 계획·분석·설계·개발·운영·유지보수·컨설팅 또는 연구개발 업무 등을 수행한 기간을 말한다.

[별표 3]

업무수행능력심사 세부평가기준(제6조관련)

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td rowspan="3">1.정보보호 업무수행 경험및 전문화 정도 (40)</td><td>최근 3년간 정보보호수행 실적</td><td>25</td><td>계약금액 총액</td><td>o 지정 공고일 기준으로 최근 3년간 완료한 정보보호수행실적을 인정하고 평가점수는 개별 수행실적의 계약금액을 합한 총액에 따라 산출
<table><tr><th>계약금액총액(단위 : 억원)</th><th>점수</th></tr><tr><td>30억원이상</td><td>배점의 100%</td></tr><tr><td>30억원미만</td><td>배점의 x%</td></tr><tr><td colspan="2">※ = (계약금액 총액/30억원) × 100</td></tr></table></td></tr>
<tr><td>최근 3년간 계약금액 5천만원 이상의 정보보호수행 실적</td><td>10</td><td>수행건수</td><td>o 지정 공고일 기준으로 최근 3년간 완료한 정보보호수행실적으로 계약금액이 5천만원 이상의 실적을 인정
<table><tr><th>수행실적 건수</th><th>점수</th></tr><tr><td>30건이상</td><td>배점의 100%</td></tr><tr><td>30건미만</td><td>배점의 x%</td></tr><tr><td colspan="2">※ = (수행건수/30건) × 100</td></tr></table></td></tr>
<tr><td>총매출액에 대한 정보보호분야 매출액 비율</td><td>5</td><td>비율</td><td>o 지정 공고일 기준으로 직전년도 정보보호분야 매출액의 비율(정보보호분야 매출액/총매출액)
<table><tr><th>비율</th><th>점수</th></tr><tr><td>80%이상</td><td>5점</td></tr><tr><td>80%미만 ~ 60%이상</td><td>4점</td></tr><tr><td>60%미만 ~ 40%이상</td><td>3점</td></tr><tr><td>40%미만 ~ 20%이상</td><td>2점</td></tr><tr><td>20%미만</td><td>1점</td></tr></table></td></tr>
<tr><td>2.신뢰도 및재정상태 건실도 (10)</td><td>부채비율</td><td>5</td><td>비율</td><td>o 지정 공고일 기준으로 직전년도 부채비율 (부채총계/자기자본)
<table><tr><th>비율</th><th>점수</th></tr><tr><td>50%미만</td><td>5점</td></tr><tr><td>50%이상 ~ 100%미만</td><td>4점</td></tr><tr><td>100%이상 ~ 150%미만</td><td>3점</td></tr><tr><td>150%이상 ~ 200%미만</td><td>2점</td></tr><tr><td>200%이상</td><td>1점</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td>자기자본이익률</td><td>5</td><td>비율</td><td>o 지정 공고일 기준으로 직전년도 자기자본이익률(당기순이익/자기자본)
<table><tr><th>비율</th><th>점수</th></tr><tr><td>20%이상</td><td>5점</td></tr><tr><td>20%미만 ~ 15%이상</td><td>4점</td></tr><tr><td>15%미만 ~ 10%이상</td><td>3점</td></tr><tr><td>10%미만 ~ 5%이상</td><td>2점</td></tr><tr><td>5%미만</td><td>1점</td></tr></table></td></tr>
<tr><td rowspan="3">3. 인증업무 운영 체계 (50)</td><td>인증기관의 운영 체계 및 인증의 품질관리</td><td>25</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 인증기관의 공정성·객관성·신뢰성·독립성 보장 방안</td><td>5점</td></tr><tr><td>o 인증기관의 내부감사 실시 및 검토 등에 대한 방안</td><td>5점</td></tr><tr><td>o 인증위원회 구성·운영 방안</td><td>5점</td></tr><tr><td>o 인증의 품질 보장 및 관리방안</td><td>5점</td></tr><tr><td>o 인증업무의 기록 및 문서화 관리체계의 적절성</td><td>5점</td></tr></table></td></tr>
<tr><td>인증업무를 수행하는 직원에 대한 운영관리 등의 내부 규정</td><td>10</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 인증업무를 수행하는 직원에 대한 규정 보유 및 그 규정의 타당성 및 실효성
- 인증업무를 수행하는 직원의 의무와 책임 등 준수사항
- 인증업무를 수행하는 직원의 자체 보안 관리 및 감독 요령</td><td>5점</td></tr><tr><td>o 인증업무를 수행하는 직원의 교육 및 평가 등에 대한 방안 및 그 방안의 적절성 및 타당성</td><td>5점</td></tr></table></td></tr>
<tr><td>인증업무 수행 방법 및 절차</td><td>15</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 인증업무 수행 방법 및 절차 등의 적절성 및 타당성
- 인증심사의 절차 및 방법
- 인증수수료 및 그 징수방법
- 인증심사팀 구성 원칙
- 인증서 발급 기준
- 인증심사 사후관리방안 등</td><td>15점</td></tr></table></td></tr>
<tr><td>4. 가점 및 감점</td><td>인증심사업무를 전담하는 직원의 보유 수</td><td>5
(가점)</td><td>보유
인원수</td><td>o 인증심사업무를 수행하는 전담조직을 갖추고, 그 전담조직에 속한 직원에 대해 인정
<table><tr><th>구분</th><th>점수</th></tr><tr><td>20명 이상</td><td>5점</td></tr><tr><td>20명미만 ~ 10명이상</td><td>배점의 x%</td></tr><tr><td>10명 미만</td><td>없음</td></tr><tr><td colspan="2">※x = (인원수/20명) × 100</td></tr></table></td></tr>
<tr><td></td><td>자격취소 사실</td><td>5
(감점)</td><td>취소사실
및
취소회수</td><td>o 지정 공고일 기준으로 10년이내에 방송통신위원회가 부여한 정보보호 관련 수행자격이 취소된 경우
- 정보보호관리체계인증기관, 정보보호 컨설팅전문업체, 안전진단수행기관 등
※ 취소 1회당 : 감점 5점</td></tr>
</table>

<비 고>

1. 각 평가요소별 세부평가에 필요한 자료의 구성 및 그 세부내용 등에 관한 사항은 지정공고 시 제시한다.
2. 평가항목에 대한 각 평가요소별 세부평가 점수는 소수점 이하 둘째 자리에서 반올림한다.
3. 평가항목에 대한 각 평가요소별 평가점수는 평가결과의 최저점과 최고점을 제외한 점수들의 평균점을 부여한다. 다만, 최저점 또는 최고점이 2개 이상일 경우 각 1개만 제외한다.
4. 가점을 합한 점수가 100점을 초과해도 만점 100점으로 표기한다.
5. 정보보호수행실적으로 인정을 받기 위해서는 다음 각목의 요건을 충족하여야 한다.
   가. 전자적 침해행위에 대비하기 위한 정보관리 및 정보시스템의 안전성에 대한 점검과 이에 기초한 정보보호대책의 제시를 주된 목적으로 직접 수행한 실적을 말하는 것으로 정보보호에 관한 감사, 감리, 진단, 인증, 컨설팅 등을 포함한다.
   나. 지정 공고일 현재 프로젝트가 종료되고 이에 대한 대금지급이 완료되어야 한다.
   다. 하수급업체가 수급업체로부터 하도급을 받아 수행한 실적에 대해서는 인정하지 아니하고 해당 기관에서 직접 계약하여 수행한 실적에 대해서만 인정한다.
   마. 가목 내지 다목의 내용이 계약서 및 증빙자료를 통하여 분명하게 확인되어야 한다.
6. '정보보호분야의 매출액'이라함은 지정 공고일 기준으로 직전년도 결산회기의 정보보호분야 제품 및 서비스관련 매출총액을 말한다.
7. '인증업무 운영체계'에 대한 각 평가요소별 세부평가 점수 부여기준은 각 평가요소의 평가결과에 평가등급(계수)를 곱하여 나온 점수를 합산한다.

평가요소별 세부평가 점수	평가등급(계수)
100점이하 ~ 90점이상	우수(1.0)
90점미만 ~ 80점이상	보통(0.6)
80점미만 ~	미흡(0.2)
미 제출	점수없음(0)

[별표 4] 인증심사기준 - 관리과정 요구사항(제11조 제1호관련)

	관리과정		세부관리과정	관리과정 상세내용
1	정보보호정책 수립	1.1	정보보호정책의 수립	신청기관의 경영목표를 지원할 수 있도록 정보보호의 법적, 규제적 요건과 전략적이고 조직적인 위험관리를 기술한 정보보호정책을 수립하여야 한다.
		1.2	조직 및 책임의 설정	정보보호활동에 대한 경영층의 명확한 지원 및 방향제시를 보증할 수 있는 조직을 수립하여야 한다. 또한 정보보호관리 활동을 수행하고 검증하는 인력들에 대한 책임, 권한 및 상호 연관관계를 정의하고 문서화하여야 한다.
2	정보보호 관리체계 범위설정	2.1	정보보호관리체계 범위설정	신청기관의 특성, 위치, 기술, 자산 등 내·외적 환경에 중대한 영향을 미치는 요소를 고려하여 정보보호관리체계의 범위를 설정하여야 한다.
		2.2	정보자산의 식별	신청기관의 정보자산으로 보호를 받을 가치가 있는 정보자산을 식별하고, 이를 정보자산의 형태, 소유자, 관리자, 특성 등을 포함하여 목록을 만들어야 한다.
3	위험관리	3.1	위험관리전략 및 계획 수립	신청기관의 목표 및 정책, 법적 요구사항 등을 고려하여 조직, 역할, 책임, 주요과정을 포함한 위험관리 전략 및 계획을 수립하고, 신청기관에 적합한 위험관리 방법을 선택하고 문서화하여야 한다. 이 위험분석 방법은 조직과 정보보호 환경변화에 대응할 수 있도록 지속적으로 검토하여야 한다.

	관리과정		세부관리과정	관리과정 상세내용
3	위험관리	3.2	위험분석	신청기관은 「2.2 정보자산의 식별」에서 식별된 정보자산에 영향을 줄 수 있는 모든 위협과 취약성, 위험을 식별하고 분류하여야 하며, 이 정보자산의 가치와 위험을 고려하여, 잠재적 손실에 대한 영향을 식별·분석하여야 한다.
		3.3	위험평가	정보자산에 대한 잠재적 및 알려진 위협과 취약성으로 나타날 수 있는 신청기관의 피해와 현재 구현된 정보보호대책의 실패 가능성 및 영향을 평가하고 수용 가능한 위험수준을 포함하여야 한다. 이를 통해 정보자산의 위험을 관리할 수 있는 적절한 정보보호대책 선택 및 우선순위의 확보를 지원하여야 한다.
		3.4	정보보호대책 선택	신청기관의 정보보호정책과 목적에 부합하도록 위험을 수용 가능한 수준으로 감소시키기 위해, 위험분석 및 평가에 의거하여, 위험처리, 위험수용, 위험회피, 위험전가 등의 전략을 설정하고, [별표3]에서 제시하는 통제사항중에서 선택한다. [별표3]에서 제시되어 있지 않은 통제사항을 추가할 경우에는 [별표1]관리과정의 각 단계간 일관성을 유지하도록 한다. 정보보호대책의 선택은 비용·효과 분석에 의해 정당화 될 필요가 있다.
		3.5	정보보호계획 수립	정보보호대책의 선택이후 구현할 정보보호대책 및 구현의 우선순위, 일정계획, 예산, 책임, 운영계획 등을 포함한 정보보호계획을 수립하고, 각 위험에 대한 정보보호대책 및 선택하게 된 근거를 정보보호대책 명세서로 문서화하여야 한다.

	관리과정		세부관리과정	관리과정 상세내용
4	구 현	4.1	정보보호대책의 효과적 구현	정보보호대책은 적절한 관리 조치와 우선 순위에 의해 구현하여야 한다.
		4.2	정보보호 교육 및 훈련	신청기관의 정보보호 관련직원들 및 최종사용자에게 정보보호에 대한 인식을 제고시키고, 정보보호대책의 필요성을 이해하도록 하며 구현될 정보보호대책들을 정확하게 사용할 수 있도록 교육 및 훈련 프로그램을 수립하고 이행하여야 한다.
5	사후관리	5.1	정보보호관리체계의 재검토	신청기관의 목표, 기술 등 내·외부의 변화와 내부감사 결과, 보안사고 등을 고려하여, 정보보호관리체계의 효율성, 범위의 적절성, 잔류위험의 수준, 절차 등의 문서를 공식적이고 정기적으로 재검토하여야 한다.
		5.2	정보보호관리체계의 모니터링 및 개선	정보보호관리체계가 신청기관의 정보보호정책과 목적을 충족시키는지 여부에 대하여 모니터링하여, 개선사항을 식별하고, 적절한 수정이나 예방조치를 통하여 효과적으로 개선사항을 구현하여야 한다. 이에 관련된 조치와 결과는 신청기관의 임직원에게 전달하여야 하고, 관련자들에게 자문을 구하여야 한다.
		5.3	내부감사	신청기관은 정보보호관리체계가 계획된 절차에 따라 효과적으로 실행되는지를 점검하기 위하여 감사의 기준, 범위, 주기 및 방법을 규정하고, 계획된 주기로 내부감사를 수행하여야 한다. 또한 감사의 기획 및 수행, 그리고 결과보고, 기록 유지 및 이행 모니터링에 대한 책임과 요구사항을 문서화된 절차에 의해 규정하여야 한다. 피감사분야의 관리자는 발견된 보완조치 사항을 처리하고, 검증·보고됨을 보장하여야 한다.

[별표 5] 인증심사기준 - 문서 작성 및 관리 통제사항(제11조 제2호관련)

	문서화	문서화 상세내용
1	문서요건	정보보호관리체계 수립 및 이행에 관련된 모든 문서는 해당 신청기관의 규모, 기능 등을 고려하여 문서화하여야 하며, 신청기관의 정보보호정책에 따라 필요한 모든 임직원 및 관련자들이 쉽게 이용할 수 있어야 한다.
2	문서의 통제	「1. 문서요건」에 의해 작성된 문서는 문서의 발행전 타당성 승인, 주기적 또는 필요시 문서의 검토·갱신 및 재승인, 문서의 변경과 현재 개정상태의 식별, 문서배포, 폐기된 문서의 사용금지 등의 통제를 정의한 절차를 수립하여야 한다.
3	운영기록의 통제	정보보호관리체계를 효과적, 효율적으로 운영하기 위해서 기록을 확인, 유지보수, 보존, 폐기하는 문서화된 절차를 수립하고 유지·관리하여야 한다. 이 문서화된 절차에는 접근자의 신원확인, 기록의 저장, 보호, 검색, 유지기간, 처분 등의 통제에 필요한 절차를 포함하여야 한다. 또한 기록은 읽기 쉽고, 식별 가능하며, 관련 활동을 추적할 수 있어야 한다.

[별표 6] 인증심사기준 - 정보보호관리 통제사항(제11조 제3호관련)

	통제분야		통제목적		통제사항	통제내용
1	정보보호 정책	1.1	정책의 승인 및 공표	1.1.1	정책의 승인	문서화된 정보보호정책은 최고경영자의 승인을 받아야 한다.
				1.1.2	정책의 공표	정보보호정책 문서는 모든 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.
		1.2	정책의 체계	1.2.1	상위 정책과의 일관성	정보보호정책은 신청기관의 사업목표 및 정보기술정책과 일관성을 유지하여야 한다.
				1.2.2	정책 문서의 유형	정보보호정책을 구체적으로 시행하기 위한 정보보호 지침, 절차 및 표준을 수립하여야 한다. 또한 필요한 경우 특정 시스템 또는 서비스에 대한 상세한 정보보호정책을 수립할 수 있다.
		1.3	정책의 유지관리	1.3.1	주기적 검토	정기적으로 정보보호정책의 타당성을 검토하여야 하며, 중대한 보안사고 발생, 새로운 위협 또는 취약성의 발생, 정보보호 환경에 중대한 변화 등이 발생했을 경우에는 관련된 사항의 타당성을 추가로 검토하여야 한다.
2	정보보호 조직	2.1	조직의 체계	2.1.1	조직의 구성	신청기관내 정보보호관리 활동을 계획, 관리하는 정보보호관리자가 있어야 하며, 필요에 따라 정보보호위원회를 구성할 수 있다.

	통제분야		통제목적		통제사항	통제내용
2	정보보호 조직	2.1	조직의 체계	2.1.2	외부전문가 활용	정보보호정책 수립, 위험분석·평가, 통제사항의 선택과 구현, 보안사고 대응 등 중요한 정보보호관리 활동에 도움을 받기 위하여 외부 전문가의 조언을 받을 수 있다. 외부 전문가의 신청기관 자원에 대한 접근은 「3. 외부자 보안」의 대상이 된다.
		2.2	책임과 역할	2.2.1	정보보호 관리자	최고경영자의 지정을 받은 정보보호관리자는 정보보호정책 수립, 정보보호 위원회의 구성 및 운영, 위험분석 및 관리, 보안사고 대응 및 복구 등의 정보보호에 관한 업무를 총괄 관리하여야 한다.
				2.2.2	정보보호 위원회	신청기관 전반에 걸친 중요한 정보보호 관련 심의 및 승인 기능을 수행하며 필요한 자원할당을 통해 정보보호관리 활동이 적절히 수행될 수 있도록 하여야 한다.
3	외부자 보안	3.1	계약 및 서비스 수준협약 보안관리	3.1.1	위부위탁 계약시 보안 요구사항	신청기관의 업무를 외부위탁 하는 경우에는 정보시스템, 네트워크, 인력 및 사무환경 등을 관리·통제하기 위한 보안요구사항을 계약서 상에 명시하여야 하고 요구사항을 서비스수준협약(SLA : Service Level Agreement)에 반영하여야 한다.
				3.1.2	제3자와의 계약시 보안 요구사항	신청기관이 제3자에게 정보자산에 대한 접근을 허용하는 계약을 체결하는 경우에는 신청기관의 정보보호정책 준수 및 필수 보안요건을 포함하는 공식적인 계약을 하여야 한다.

	통제분야		통제목적		통제사항	통제내용
3	외부자 보안	3.2	외부자 보안 실행관리	3.2.1	외부위탁 보안관리	외부위탁 업체가 계약서 및 서비스 수준 협약 명시된 보안요구사항을 충분히 이행하는지 주기적으로 점검하고, 필요시 감사를 수행하여야 한다.
				3.2.2	제3자 보안관리	신청기관의 정보자산에 대한 제3자의 접근을 통제하여야 한다. 업무상 불가피하게 접근을 허용해야 할 경우에는 접근유형 및 접근사유를 파악하고 위험 요소를 고려하여 관리하여야 한다.
4	정보자산 분류	4.1	정보자산의 조사 및 책임할당	4.1.1	정보자산 조사	신청기관의 정보자산을 조사하고 정보자산별로 신청기관에서의 가치, 업무 영향, 법적 준수사항 등을 고려하여 중요도를 결정하여야 한다.
				4.1.2	정보자산별 책임할당	조사된 정보자산에 대하여 소유자, 관리자, 사용자를 확인하고, 적절한 통제 유지를 위해 책임소재를 명확히 하여야 한다.
		4.2	정보자산의 분류 및 취급	4.2.1	정보자산의 분류	정보자산이 신청기관에서 차지하는 가치와 신청기관에 미치는 영향을 고려하여 분류방식을 선택하고 분류하여야 한다.
				4.2.2	보안등급과 취급	중요도에 따라 분류된 정보자산에 보안등급을 부여하고, 물리적, 전자적 보안등급 표시를 부착, 관리하여야 한다. 또한 보안등급의 부여에 따른 취급 절차도 정의하여 이행하여야 한다.

	통제분야		통제목적		통제사항	통제내용
5	정보보호 교육 및 훈련	5.1	교육 및 훈련 프로그램 수립	5.1.1	교육 및 훈련계획	정보보호 인식제고 및 실제 운영에 필요한 교육·훈련 계획을 종합적으로 수립하여 이행하여야 한다
				5.1.2	교육 및 훈련대상	교육 및 훈련의 대상에는 신청기관의 임직원 및 관련 외부자를 포함하여야 한다.
				5.1.3	교육 및 훈련내용	교육 및 훈련은 정보보호정책, 정보보호인식, 보안요구사항, 법적인 책임, 보안사고 대응절차, 업무연속성 관리 등을 포함하여야 하고, 교육대상자의 직위 및 담당하는 업무의 특성에 따라 구분하여 실시하여야 한다.
		5.2	시행 및 평가			교육 및 훈련은 정기적으로 실시하여야 하며, 정보보호정책이나 절차 및 역할의 변경이 있는 경우에는 수시로 실시하고 이에 대한 기록을 남겨야 한다. 또한 교육훈련 종료 후 검토를 통하여 차기 교육에 반영하여야 한다.
6	인적 보안	6.1	책임할당 및 규정화	6.1.1	책임할당	정보보호업무를 이행하는 역할과 책임을 문서화하여야 한다. 문서화의 내용에는 정보보호정책을 수립, 구현, 운영하는 일반적인 책임과 특정 정보자산의 보호와 활동에 대한 구체적인 책임을 포함하여야 한다.
				6.1.2	인사규정	인사규정에는 정보보호에 대하여 직원이 지켜야 할 책임 및 관련 법규상의 책임을 명시하여야 한다. 특히, 정보보호업무를 담당하는 자와 정보시스템 사용자 및 관리자는 보다 명확한 책임을 명시하여야 하며, 직원이 책임을 이행하지 않는 경우를 대비한 적절한 처벌규정을 포함하여야 한다.

	통제분야		통제목적		통제사항	통제내용
6	인적 보안	6.2	적격심사 및 주요 직무담당자 관리	6.2.1	적격심사	계약직 및 임시직원은 물론 정식직원 채용시 신원, 업무능력, 교육정도, 경력 등에 대한 적격심사가 이루어져야 한다. 직원들이 용역회사를 통하여 충원되는 경우에는 용역회사와의 계약서에 적격심사에 따르는 책임사항을 명문화하여야 한다.
				6.2.2	주요직무 담당자 관리	정보시스템 접근 권한을 포함하는 업무가 새로이 할당될 때, 특히 재무정보나 비밀정보와 같이 중요한 정보를 처리하는 담당자는 별도의 관리를 수행하여야 한다.
		6.3	비밀유지	6.3.1	비밀유지 서약서	직원으로부터 비밀유지 서약서에 서명을 받아야 하며, 임시직원이나 제3자에게 정보에 대한 접근 권한을 부여할 경우에도 그들로부터 비밀유지 서약서에 서명을 받아야 한다. 직원의 고용계약에 변경이 있을 경우, 특히 직원이 퇴사하거나 계약기간이 만료될 때에는 비밀유지 서약서를 환기시켜야 한다.
7	물리적 보안	7.1	물리적 보안대책	7.1.1	물리적 보호구역	특별한 보호가 필요한 시설 및 장비를 권한 없는 자의 물리적 접근 및 각종 물리적, 환경적 재난으로부터 보호하기 위하여 보호구역을 정의하고 이에 따른 보안대책을 수립·이행하여야 한다. 이 경우 제한구역, 접견구역, 장비출하구역 등을 별도로 지정하여 각각에 적합한 보안 조치와 절차를 수립하여야 한다.
				7.1.2	물리적 접근통제	보호구역을 출입하는 자를 감시·통제하고 권한 없는 자의 출입을 방지하기 위하여 수립된 보안 절차에 따라 필요한 조치를 수행하고 주기적으로 검토하여야 한다.

	통제분야		통제목적		통제사항	통제내용
7	물리적 보안	7.2	데이터 센터 보안	7.2.1	위치 및 구조 조건	데이터센터는 물리적, 환경적 위험이 적은 곳에 위치하고 구조의 안정성을 확보하여야 한다.
				7.2.2	출입통제	데이터센터의 출입은 적절한 출입통제절차에 의하여 이행되어져야 하며, 출입자를 식별하고 기록·관리하여야 한다. 또한 출입자 기록 대장은 정기적으로 점검하여야 한다.
				7.2.3	내부설비	화재·수재 등의 각종 재해에 대비한 시설을 충분히 설치하여야 하고, 비상연락장치 및 비상구, 물리적 접근통제 및 시건장치를 설치하여야 한다.
		7.3	장비보호	7.3.1	주요 시스템 보호	신청기관내의 주요 시스템에 대한 별도의 출입통제를 실시하거나 이중의 보호장치를 설치하고, 시스템 관리자는 주요 시스템 접근에 대한 보안대책을 수립하여야 한다.
				7.3.2	장비의 배치	장비는 환경적인 위협과 위험, 불법접근에 대한 위험을 감소시키기 위해 적절한 위치에 배치하고 이를 보호하여야 한다.
				7.3.3	전원공급	전원공급 이상이나 기타 전기관련 사고 발생시 전원을 지속적으로 공급하기 위하여 장비 제조업체의 사양에 따라 적절히 관리하여야 한다.
				7.3.4	케이블 보호	데이터를 송·수신하거나 정보서비스를 지원하는 전력 및 통신 케이블은 방해되거나 손상을 입지 않도록 보호하여야 한다.
				7.3.5	장비의 보수	장비는 지속적인 가용성과 무결성을 위하여 장비 제공자가 지시한 명세에 따라 유지보수를 하여야 하고 유지·보수에 대한 기록을 남겨야 한다.

	통제분야		통제목적		통제사항	통제내용
7	물리적 보안	7.3	장비보호	7.3.6	장비의 안전한 폐기 및 재사용	중요한 정보를 담고 있는 저장 매체의 폐기시에는 이를 물리적으로 파기하여야 하며, 중요 데이터나 정품 소프트웨어는 폐기하기 전에 매체에 기록된 내용이 완전히 삭제되어 복구가 불가능한지 확인하고 점검하여야 한다.
		7.4	사무실 보호			책상 위에 중요한 문서나 저장 매체를 남겨놓지 않도록 하고, 통상 근무시간 동안이나 그 외의 시간에 비인가된 자에 의한 정보 접근, 손상을 방지하기 위하여 컴퓨터 화면에 정보처리에 관한 사항을 남겨놓지 않도록 하여야 한다.
8	시스템 개발보안	8.1	분석 및 설계 보안관리	8.1.1	보안 요구사항 정의	새로운 시스템 개발, 기존시스템 개선시 보안요구사항을 문서로 명확히 하여야 하며, 보안요구사항에는 사용자 접근권한의 부여원칙과 접근통제 유형 등을 포함하여야 한다.
				8.1.2	입력 데이터 검증	응용시스템 설계시 입력 요구사항을 정의하고 문서화하여야 하며, 입력 데이터의 정확성, 무결성, 신뢰성을 판단하기 위한 표준을 마련하여야 한다.
				8.1.3	내부 처리의 검증	응용시스템 설계시 내부처리 요구사항을 정의하고 문서화하여야 하며, 응용소프트웨어의 처리 작업을 검증하고, 무결성을 회복할 수 있는 기능을 포함하여야 한다.
				8.1.4	출력 데이터 검증	응용시스템 설계시 출력 요구사항을 정의하고 문서화하여야 하며, 출력 데이터의 정확성, 무결성, 신뢰성을 판단하기 위한 대책을 마련하여야 한다.

	통제분야		통제목적		통제사항	통제내용
8	시스템 개발 보안	8.1	분석 및 설계 보안관리	8.1.5	인증 및 암호	응용시스템 설계시 반드시 사용자 인증에 대한 보안 요구사항을 고려하여야 한다. 중요한 메시지의 경우 무결성이 요구될 때 메시지 인증기법을 적용하고 비밀성이 요구될 시 암호화를 적용하여야 한다.
				8.1.6	보안기록 관리	응용시스템 설계시 사용자의 인증, 데이터 분실, 수정, 오남용 등을 점검하고 방지하기 위하여 보안에 관련된 로그, 감사증적 등을 확보할 수 있는 기능을 반영하여야 한다.
		8.2	구현 및 이행 보안관리	8.2.1	구현 및 시험	응용시스템 구현시 코딩표준에 따라 응용시스템을 구현하고, 보안요구사항에 대한 시험을 수행하여야 한다.
				8.2.2	운영환경 이행보안	운영 프로그램의 수정은 적절한 권한을 지닌 사람만이 시행하여야 하고, 운영시스템은 실행코드만 보유하여야 한다. 실행코드는 성공적인 시험과 사용자 인수 후에 실행하여야 한다.
				8.2.3	시험 데이터의 보안	시험 데이터는 운영데이터에 준하여 보호하고 통제하여야 하며, 운영환경에 대하여 적용되는 접근통제 절차를 시험환경에도 적용하여야 한다. 운영데이터가 시험환경으로 복사될 경우 허가절차를 수립하여 이행하고 시험 완료 후 운영데이터는 시험시스템에서 삭제하여야 한다. 운영데이터 사용 및 복사는 기록을 남겨야 한다.
				8.2.4	소스 프로그램의 접근보안	소스 프로그램은 실제 운영 환경에 보관하지 않는 것을 원칙으로 하며, 소스 프로그램 관리자는 각 운영시스템 별로 지정하여야 한다. 또한 소스 프로그램 접근에 대한 통제절차를 수립하고 이행하여야 한다.

	통제분야		통제목적		통제사항	통제내용
8	시스템 개발 보안	8.3	변경관리	8.3.1	변경관리 절차	정보시스템의 파괴와 손상을 최소화하기 위하여 공식적인 변경관리 절차를 수립하고 이행하여야 한다.
				8.3.2	운영체제 변경시의 검토	운영체제 변경이 필요한 경우 응용시스템의 운영이나 보안에 미치는 영향을 분석, 검토하여야 한다.
				8.3.3	소프트웨어 패키지 변경	소프트웨어 패키지는 가능한 수정하지 않고 사용하고, 패키지 변경시에는 공급자의 동의를 얻으며, 수정이 가능한지 확인하여야 한다. 모든 변경사항은 시험하고 문서화하여야 한다.
9	암호 통제	9.1	암호 정책			암호사용에 대한 정책을 수립하여야 한다.
		9.2	암호사용			암호 정책에 따른 암호 사용시 적절한 암호 알고리즘의 유형, 신뢰성 및 키 길이를 결정하여야 한다.
		9.3	키관리			암호 키에 대한 관리지침, 절차 및 방법을 마련하고 필요시 복구방안을 마련하여야 한다.
10	접근 통제	10.1	접근통제 정책	10.1.1	정책의 문서화	업무 요구사항에 따라 접근 통제의 방법과 범위 등을 정의하고 문서화하여야 한다.
				10.1.2	정책의 내용	접근통제 정책은 데이터, 프로그램, 주요 시스템, 네트워크 등에 대한 접근제한을 포함하여야 하며, 여기에는 보안요구사항, 데이터 및 서비스 접근시의 법적, 계약적 제한, 분산 네트워크상의 접근권한 관리 등을 포함하여야 한다.
				10.1.3	접근 통제 규칙	항상 존재하는 규칙과 일정기간이나 선택적으로 존재하는 규칙에 대한 구분, 실행 전에 관리자의 승인을 필요로 하는 규칙과 그렇지 않은 규칙의 구분 등을 포함한 접근 통제 규칙을 명시하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.1	접근통제 정책	10.1.4	접근통제 방법	접근통제 방법은 정책 및 절차에 의해 결정된 접근권한을 적절하게 반영하여야 한다.
				10.1.5	접근통제 정책 검토	접근에 대한 모니터링을 통해 정책과의 일치성을 주기적으로 검토하고, 접근통제 정책의 적정성을 확인하여야 한다.
		10.2	사용자 접근 관리	10.2.1	사용자 등록	정보시스템 및 서비스에 대한 접근을 통제하기 위한 공식적인 사용자 등록 및 해지 절차를 마련하여야 한다.
				10.2.2	특수권한 관리	시스템이나 응용프로그램에 대한 통제를 우회할 수 있는 특수권한의 할당 및 사용을 관리하여야 한다.
				10.2.3	사용자 패스워드 관리	사용자 패스워드의 관리절차를 수립하고 이행하여야 한다.
				10.2.4	사용자의 접근권한 검토	데이터나 정보 서비스에 대한 접근을 관리하기 위해서 정기적으로 접근 권한에 대하여서 점검을 하여야 한다.
				10.2.5	사용자의 책임	시스템 및 패스워드 관리 책임은 사용자 자신에게 있음을 주지시키고 관리지침을 제공하여야 한다.
		10.3	접근통제 영역	10.3.1	네트워크 접근	비인가된 접근을 막기 위해 네트워크의 내·외부 연결통제, 사용자 터미널과 컴퓨터 서비스간에 물리적 및 논리적 경로의 통제, 사용자 인증, 고장 진단 포트에 대한 접근통제 등을 포함한 네트워크 접근정책을 수립하고 이행하여야 한다.
				10.3.2	운영체제 접근	안전한 로그온 절차, 식별 및 인증 관리, 필요시 터미널 자동확인 등을 포함하여 시스템의 운영체제 접근을 통제하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.3	접근통제 영역	10.3.3	응용 프로그램 접근	사용자 접근이 허가되지 않은 응용 프로그램의 기능들에 대한 정보 제공을 제한하여야 한다. 또한 민감한 정보를 처리하는 응용 프로그램의 출력물은 허가된 위치에서만 전달하여야 한다. 민감한 응용 시스템은 반드시 일반적인 환경과 분리하여야 한다.
				10.3.4	데이터베이스 접근	데이터베이스의 뷰, 레코드 또는 필드 레벨에서의 데이터에 대한 접근통제, 데이터사전 및 데이터베이스 유틸리티에 대한 접근통제, 민감 정보의 암호화 등을 통해 데이터베이스내의 정보를 보호하여야 한다.
11	운영관리	11.1	운영 절차와 책임	11.1.1	운영절차의 문서화	보안정책에 의해 정의된 운영지침과 절차는 문서화하여 관리하여야 한다. 운영관리를 외부에 용역을 주는 경우에도 계약서에 이를 반영하여야 한다.
				11.1.2	정보자산의 변경관리	정보시스템 관련 자산들을 조사하고, 모든 변경사항들을 반영할 수 있는 공식적인 관리책임 및 절차를 수립하여야 한다.
				11.1.3	직무 분리	부주의에 의한 또는 고의적인 시스템 오용의 위험을 감소시키기 위해 직무를 분리하고, 직무 분리가 어려운 특수한 경우 별도의 관리감독 대책을 수립하여야 한다.
				11.1.4	개발과 운영환경의 분리	원칙적으로 개발, 시험, 운영 환경을 분리하여야 한다. 또한 응용프로그램을 개발환경으로부터 운영환경으로 이전하는 절차를 정의하고 문서화하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영 관리	11.1	운영 절차와 책임	11.1.5	외부 운영 설비 관리	외부자가 정보시스템 및 장비를 관리하는 경우 데이터의 손상, 손실 등의 상황을 고려하여 통제방안을 수립하고 계약서에 반영하여야 한다.
		11.2	시스템 운영	11.2.1	시스템 도입	정보시스템의 도입을 위해서 도입 계획 및 정책을 수립하여야 한다.
				11.2.2	시스템 인수	새로운 정보시스템의 설치 또는 수정에 따른 인수기준을 수립하고, 시스템 구매 계약서에 반영하여야 한다. 또한 시스템은 이 기준에 의해 시험을 한 후 인수하여야 한다.
				11.2.3	성능관리	신청기관에서 요구되는 성능 요구사항을 충족시킬 수 있도록 성능관리를 수행하여야 한다.
				11.2.4	용량관리	신청기관에서 요구되는 용량 요구사항을 충족시킬 수 있도록 용량계획을 통해 적정한 용량을 확보하고, 주어진 용량을 최적으로 사용할 수 있는 관리방안을 수립하여 이에 따른 용량관리를 수행하여야 한다.
				11.2.5	백업 및 복구 관리	데이터 및 장비의 무결성과 가용성을 유지하기 위해 백업 계획을 수립하여 이행하여야 하며, 사고 발생시 적시에 복구할 수 있도록 관리하여야 한다.
				11.2.6	장애관리	시스템의 장애시 효과적으로 대응하기 위해 탐지, 기록, 분석, 복구, 보고 등 적절한 조치를 취하여야 한다.
				11.2.7	로그관리	시스템 운영의 확인이나 사고조사를 위해 활동에 대한 기록을 남기고 주기적으로 검토하여야 한다.
				11.2.8	보안 시스템 운영	보안시스템에 대해서는 그 유형별로 설치, 운영에 대한 절차를 수립하고, 절차이행을 주기적으로 검토하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영 관리	11.3	네트워크 운영	11.3.1	네트워크 운영대책	네트워크 운영 보안 유지를 위해 직무 분리, 접근권한 통제, 원격접속 설비 관리, 네트워크 분리 등을 위한 책임 및 절차 등을 포함한 대책을 수립하여야 한다.
				11.3.2	인터넷 접속관리	인터넷망과 접속시 침입차단시스템을 통하여 접근통제를 수행하여야 하며, 필요시 침입탐지시스템 등을 활용하여 접근을 모니터링 하여야 한다.
				11.3.3	원격운영 관리	네트워크를 통해 시스템을 운영하는 경우 원칙적으로 시스템 관리는 내부의 특정 터미널에서만 할 수 있도록 제한하고, 외부에서 네트워크를 통하여 시스템을 관리할 경우에는 사용자 인증, 암호 및 접근통제 기능을 설정하여야 한다.
		11.4	매체 및 문서관리	11.4.1	매체 취급 및 보관	허가되지 않은 유출이나 오용으로부터 정보를 보호하기 위해, 매체의 취급 및 보관에 대한 절차를 수립하고 운영하여야 한다.
				11.4.2	매체의 폐기	매체 폐기를 부주의하게 이행하여 외부자에게 주요정보가 누출되지 않도록 폐기지침을 수립하고 운영하여야 한다.
				11.4.3	시스템 문서의 보안	보안절차, 운영매뉴얼, 운영기록 등 주요 시스템 문서들은 안전하게 보관하고 적절한 폐기절차에 따라 폐기하여야 한다.
		11.5	악성 소프트웨어 통제			바이러스 등의 악성 소프트웨어로부터 시스템을 보호하기 위해 악성 소프트웨어들을 예방하고 탐지, 대응하는 대책을 수립하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영 관리	11.6	이동컴퓨팅 및 원격 작업	11.6.1	이동 컴퓨팅	휴대용 정보통신기기의 사용시에 사업 정보를 보호하기 위한 보안 정책을 수립하고, 내부 네트워크로의 연결 및 공공 장소에서의 사용에 대한 정책을 수립하여야 한다.
				11.6.2	원격 작업	재택 근무와 같은 원격 작업 수행시 이에 대한 물리적, 논리적 보호를 위한 정책과 절차를 마련하여야 한다.
12	전자 거래 보안	12.1	교환 합의서			신청기관간의 정보 및 소프트웨어 교환시에는 이에 대한 합의가 이루어져야 하고, 관리적 책임 및 절차, 전송의 기술적 기준, 인증기준, 데이터의 책임성 등을 반영한 교환 합의서를 작성하여야 한다.
		12.2	전자거래 보안관리			전자거래 시 사기, 계약 분쟁, 정보의 노출 및 수정 등으로부터 보호하기 위해 신원확인, 무결성, 암호화, 부인방지 등의 대책을 수립하여 운영하여야 한다.
		12.3	전자우편			전자 우편 서비스에 대한 가용성, 전자우편 내용에 대한 무결성 및 기밀성과 이에 따른 책임과 위험을 고려한 보안지침 및 대책을 수립하여 운영하여야 한다.
		12.4	공개서버의 보안관리			웹서버 등에 정보를 공개할 경우 정보에 대한 수집, 저장 및 공개에 따른 허가 및 게시절차를 수립하여야 하고, 공개서버에 대한 물리적, 논리적 보안대책을 수립하고 운영하여야 한다.
		12.5	이용자 공지사항			전자거래의 안전한 이행을 위하여 이용자에게 해킹위험, 계정 및 패스워드 관리, 접속관리 등에 대한 공지를 통해 안전거래 준수를 권고하여야 한다.

	통제분야		통제목적		통제사항	통제내용
13	보안사고 관리	13.1	대응 계획 및 체계	13.1.1	대응계획 수립	보안사고의 정의 및 범위, 긴급연락체계 구축, 보안사고 발생시 보고 및 대응 절차, 사고 복구조직의 구성, 교육계획 등을 포함한 보안사고 대응 계획을 수립·이행하여야 한다.
				13.1.2	보안사고 대응체계 구축	보안사고의 대응이 신속하게 이루어질 수 있도록 중앙 집중적인 대응체계를 구축하고, 대응체계에는 내부 직원뿐 아니라 외부기관 및 전문가들과의 협조체계를 반영하여야 한다.
		13.2	대응 및 복구	13.2.1	보안사고 대응 교육 및 훈련	보안사고 대응 계획, 절차 및 방법에 대하여 정기적으로 교육을 실시하여야 하며 사고 처리 후 재발방지를 위하여 필요한 교육훈련을 실시하여야 한다
				13.2.2	보안사고 보고	사고의 징후 또는 보안사고 발생을 인지한 때에는 보고체계에 따라 가능한 한 신속히 보고하여야 한다. 시스템이나 네트워크의 보안 취약점과 소프트웨어 기능장애 또한 신속히 보고하여야 한다.
				13.2.3	보안사고 처리 및 복구	보안사고 보고시 처리, 복구 절차에 따라 처리와 복구를 신속히 이행하여야 한다.
		13.3	사후관리	13.3.1	보안사고 분석 및 정보의 공유	보안사고가 처리되고 종결된 후 이에 대한 분석을 이행하여야 하며, 그 결과를 보고하여야 한다. 또한 사고에 대한 정보와 발견된 취약성들을 관련 신청기관과 임직원에게 공유하여야 한다.
				13.3.2	재발방지	보안사고로부터 얻은 정보를 활용하여, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하여야 한다. 이를 위해 필요한 경우 정책, 절차, 조직 등의 보안체계에 대한 변경을 하여야 한다.

	통제분야		통제목적		통제사항	통제내용
14	검토, 모니터링 및 감사	14.1	법적 요구사항 준수 검토	14.1.1	요구사항 명시	정보시스템에 대해 관련된 모든 법, 규제, 계약, 정책, 기술상의 요구사항을 정의하고 문서화하여야 하며, 이들 요구사항을 만족시키기 위해 필요한 특정 통제나 개별 책임 등도 정의하고 문서화하여야 한다.
				14.1.2	준수 검토	정보통신망이용촉진및정보보호등에관한법률, 신용정보의이용및보호에관한법률 등의 개인정보보호 관련법 및 저작권법, 컴퓨터프로그램보호법 등 지적재산권법 등의 관련 법규의 준수여부를 검토하여야 한다.
				14.1.3	증거자료 수집	보안사고 처리 및 계약 증빙을 위하여 신청기관이나 개인에 대한 소송을 지원하기 위한 적정한 증거 자료를 확보하여야 한다.
		14.2	정보보호 정책 준수 검토	14.2.1	검토 계획	검토의 대상, 주기, 방법, 범위, 절차, 검토자를 포함한 검토계획 및 정책이 수립되어야 한다. 이를 근거로 보안요구사항에 대한 통제와 책임의 준수에 대한 적정성을 검토하여야 한다.
				14.2.2	정책의 준수	모든 정보보호 정책, 절차의 준수여부를 검토하여야 한다.
				14.2.3	기술적 점검	정보시스템이 정보보호표준 및 절차에 따라 운영·관리되고 있는지 정기적으로 기술적 점검을 실시하여야 한다. 이에 따라 취약성들을 발견한 후 필요한 조치를 취하여야 한다.

	통제분야		통제목적		통제사항	통제내용
14	검토, 모니터링 및 감사	14.3	모니터링	14.3.1	접근 및 사용 모니터링	사용자의 시스템, 네트워크 사용 및 접근이 명확하게 허용된 범위 안에 있는지를 확인하기 위해 모니터링 절차를 수립하고 이행하여야 한다. 모니터링 결과는 정기적으로 점검하여야 하고 위험의 정도에 따라 점검 주기를 결정하여야 한다.
				14.3.2	감사기록 분석 및 보관	모니터링을 위한 감사 기록을 생성하고, 분석하며 일정 기간 동안 보관하여야 한다.
				14.3.3	시각 동기화	감사 기록의 명확성을 보장하고 법적인 자료나 징계 자료로서 효력을 갖기 위해서는 시스템 시각을 정확히 설정하여야 한다.
		14.4	보안감사	14.4.1	보안감사 계획 및 이행	보안 감사 대상, 범위, 주기, 방법, 절차, 감사자, 감사도구를 포함한 보안감사 계획을 수립하고 이행하여야 한다.
				14.4.2	감사결과 및 사후관리	감사의 결과에 따라 감사보고서를 작성하고 적정한 책임자에게 보고하며, 감사 지적 내용이 이행되도록 사후관리하여야 한다.
15	업무 연속성 관리	15.1	업무연속성 관리 체계 수립	15.1.1	업무연속성 관리 과정 수립	개시단계, 업무연속성전략수립단계, 구현단계, 운영관리단계 등 업무연속성관리를 위한 과정을 사전에 정의하여야 한다. 개시단계에는 업무연속성관리에 대한 정책 수립 및 범위설정, 자원분배를 포함하여야 하며, 업무연속성전략수립단계는 업무영향분석을 통해 이루어져야 한다. 구현단계에는 재해복구 및 위험감소 대책, 업무연속성계획의 문서화를 포함하여야 하며, 운영관리단계에는 시험, 교육훈련, 검토 및 갱신을 포함하여야 한다.

	통제분야		통제목적		통제사항	통제내용
15	업무 연속성 관리	15.1	업무연속성 관리 체계 수립	15.1.2	업무연속성 계획 프레임워크 수립	업무별 연속성 계획의 이행에 필요한 조건, 응급절차, 대체절차 등을 고려하여 연속성 계획들이 일관성을 유지할 수 있도록 프레임워크를 수립하여야 한다.
		15.2	업무연속성 계획 수립과 구현	15.2.1	업무영향 분석	재난재해별로 업무에 미칠 수 있는 영향을 피해규모와 복구에 소요되는 시간 등을 고려하여 분석하고 그 결과를 기초로 구체적인 업무복구목표 및 복구를 위한 최소한의 요구사항을 설정하여야 한다.
				15.2.2	업무연속성 계획 수립	업무복구목표 및 최소 요구사항을 구현하기 위한 여러 대안들을 평가하여 업무연속성을 위한 전략을 수립하고 대책 구현을 위한 계획을 수립하여야 한다.
				15.2.3	업무연속성 계획 구현	업무연속성계획에서 수립한 위험감소 조치 및 재해복구를 위한 설비를 구현하며 필요한 계획 및 절차 등을 문서화하여야 한다.
		15.3	업무 연속성 계획 시험 및 유지관리	15.3.1	업무연속성 계획 시험	환경의 변화 또는 부정확한 전제 등으로 인한 오류를 제거할 수 있도록 지속적인 시험을 수행하며, 시험 계획에는 시기, 방법, 절차 등을 포함하여야 한다.
				15.3.2	업무연속성 계획 유지·관리	업무연속성계획에 대해 정기적인 교육 및 훈련을 실시하고 지속적인 검토와 평가 및 변경관리를 수행하여야 한다.

[별지 제1호서식]

(앞 쪽)

정보보호관리체계인증기관 지정신청서				처리기간 3 월
신청인	①업 체 명 및 대 표 자 성 명		②설 립 일 자	
	③소 재 지		④전 화 번 호	
	⑤직 원 수	명	⑥인증심사업무를 전담하는 직원의 수	명

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조 및 같은 법 시행령 제48조에 따라 위와 같이 정보보호관리체계인증기관의 지정을 신청합니다.

년 월 일

신청인 (서명 또는 인)

방송통신위원회 귀중

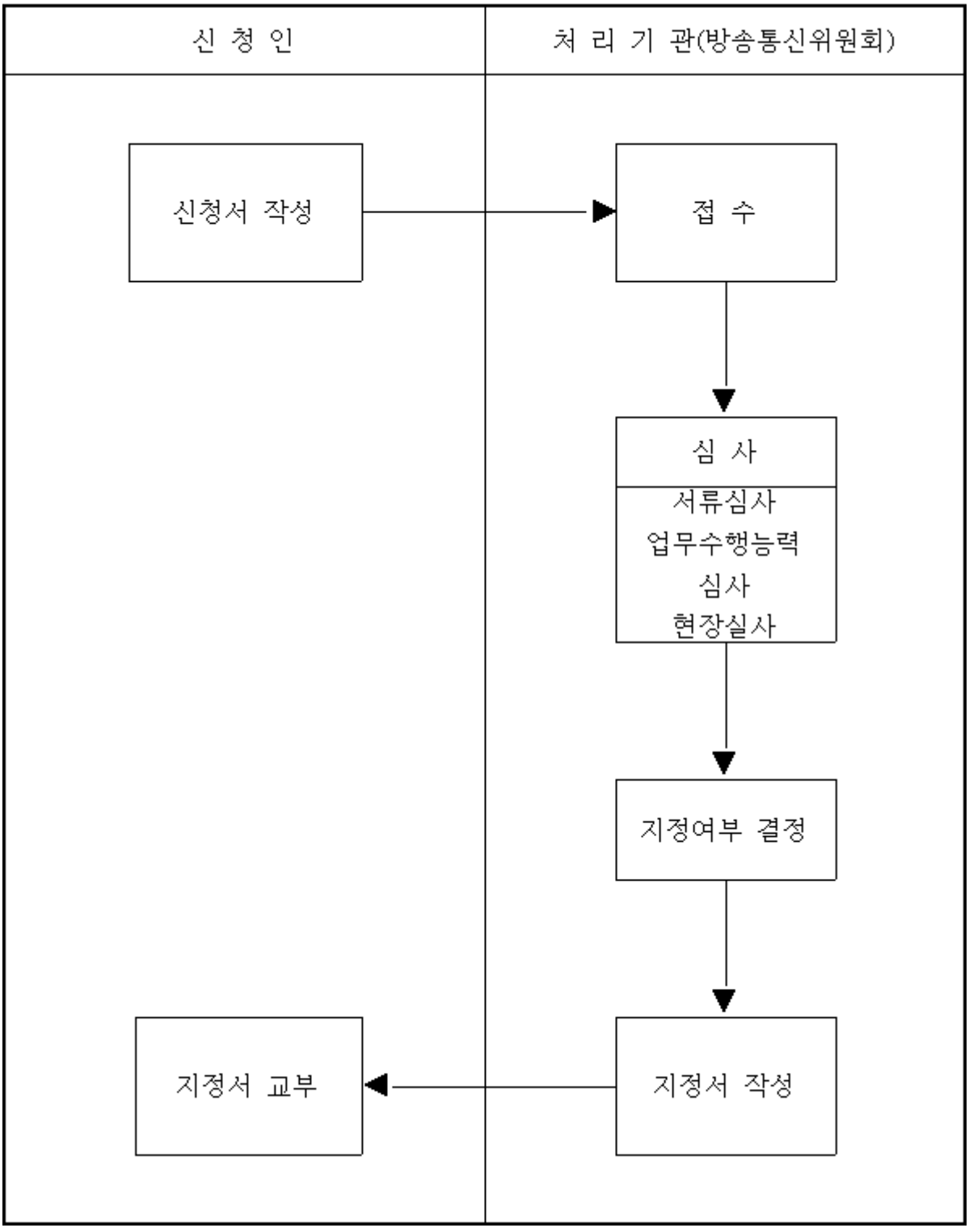
구비서류	신청인(대표자) 제출서류	담당공무원 확인사항 (부동의하는 경우 해당서류 제출)	수 수 료
	1. 정관 2. 별지 제2호서식의 인증심사업무를 전담하는 직원 보유현황과 이를 증명할 수 있는 서류 3. 별표 제1호에 따른 업무수행능력심사를 위하여 필요한 서류	법인등기부 등본 (법인인 경우)	없 음

본인은 이 신청서의 처리와 관련하여 「전자정부법」 제21조제1항에 따른 행정정보의 공동이용을 통하여 담당공무원이 위의 담당공무원 확인사항을 확인하는 것에 동의합니다.

신청인(대표자) (서명 또는 인)

210㎜×297㎜(일반용지 60g/㎡)

이 신청서는 아래와 같이 처리됩니다. (뒤 쪽)



(제1쪽)

[별지 제2호서식]

인증심사업무를 전담하는 직원의 보유현황

업체명			
대표자 성명			
소 재 지			
종업원수		인증심사업무를 전담하는 직원의 수	

일련번호	성 명 (한 자)	주 소 / 주민등록번호	입사일	최종학위 / 취득학교 및 학과(전공)	해당 요건

(제2쪽)

일련번호	성 명 (한 자)	주 소		최종학위	해당 요건
		주민등록번호	입사일	취득학교 및 학과(전공)	

비 고

1. 「해당요건」란에는 별표 1의 요건 중 당해 인증심사업무를 전담하는 직원이 충족하는 요건을 기재한다.
   예시) 학력 및 경력기준 제2호 가목
2. 기재된 최종학위를 증명할 수 있는 직원의 졸업 또는 학위증명서 사본을 제출하여야 한다.
3. 별표 1의 「자격 및 경력기준」을 충족하는 직원은 기술자격증 사본 등 자격을 취득하였음을 확인할 수 있는 서류를 함께 제출하여야 한다.
4. 정보통신유관경력 또는 정보보호유관경력을 증명할 수 있는 경력증명서(근무부서 또는 담당업무 등이 기재되어야 한다)와 해당 직원이 신청업체에 현재 근무하고 있음을 확인할 수 있는 재직증명서를 함께 제출하여야 한다.

[별지 제3호서식]

정보보호수행실적 명세서

업 체 명					
대 표 자 성 명					
소 재 지					
정보보호수행실적 총계		외 건 (총 천원)			
일련번호	정보보호수행실적(프로젝트명) 대상기관(기업)명	수행 기간	계약 금액(천원)	과제책임자	구분

비 고

1. 계약금액란에는 정보보호에 관한 업무를 수행한 대가로서 지급받은 대금을 기재하고, 구분란에는 정보보호에 관한 감사, 감리, 진단, 인증, 컨설팅 등으로 실적을 구분하여 기재한다.

[별지 제4호서식]

(제1쪽)

제 호

정보보호관리체계인증기관지정서

업체명 :

대표자 :

소재지 :

지정의 유효기간 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조 및 같은 시행령 제48조에 따라 위와 같이 정보보호관리체계인증기관으로 지정합니다.

년 월 일

방송통신위원회 위원장 [인]

210㎜×297㎜

(보존용지(1종) 120g/㎡)

(제2쪽)

Registry No.

CERTIFICATE OF DESIGNATION
AS
ISMS Certification Authority

Name of Organization :
Name of Representative :
Address :
Period of Validity :

This is to certify that the above-mentioned organization is designated Information Security Management System (ISMS) certification Authority in accordance with Article 47 of the Act on Promotion of Information and Communication Network Utilization and Information Protection, etc. and Article 48 of Promotion of Information and Communication Network Utilization and Information Protection, Etc. Enforcement Ordinance of Act

Signed by the
Chairman of Broadcasting and Communications Commission
Republic of Korea

210㎜×297㎜
(보존용지(1종) 120g/㎡)

[별지 제5호서식] (앞 쪽)

정보보호관리체계인증신청서				
신청인	성 명(대 표 자)		주민등록번호	
	상호 또는 명칭		사업자등록번호	
	소 재 지		전 화 번 호	
인증신청의 구분		□처음으로 인증신청을 하는 때 □유효기간의 만료로 다시 인증신청을 하는 때 □인증의 범위에 중요한 변경이 있어서 다시 인증신청을 하는 때		
정보보호관리체계의 범위				
정보보호관리체계의 범위에 포함되어 있는 종업원의 수				

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제4항, 동법 시행령 제50조에 따라 위와 같이 정보보호관리체계의 인증을 신청합니다.

년 월 일

신청인 (서명 또는 인)

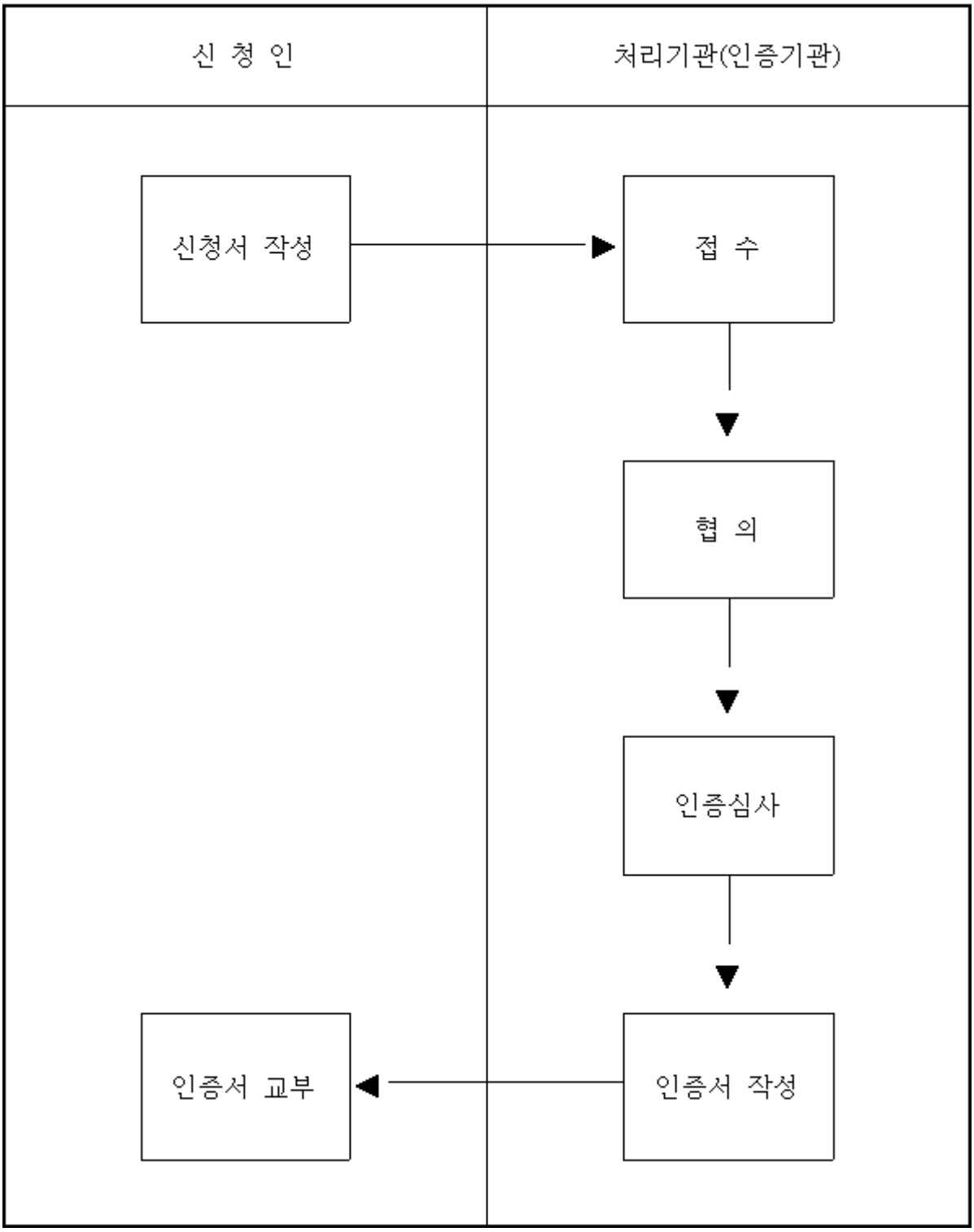
(인증기관명) 귀하

구비서류

1. 법인등기부 등본(법인인 경우에 한합니다)
2. 정보보호관리체계의 내역서

210mm×297mm(신문용지 54g/㎡)

이 신청서는 아래와 같이 처리됩니다. (뒤 쪽)



[별지 제6호서식] (제1쪽)

제 호

정보보호관리체계인증서

상호 또는 명칭 :

대 표 자 :

소 재 지 :

인증의 범위 :

유 효 기 간 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제4항, 같은 법 시행령 제50조에 따라 위와 같이 정보보호관리체계를 인증합니다.

년 월 일

(인증기관장) (인)

210mm×297mm(보존용지(1종) 120g/㎡)

(제2쪽)

Certificate Number :

CERTIFICATE

OF

Information Security Management System

Name of Organization :

Name of Representative :

Address :

Scope of Certification :

Period of Valid :

Date of Issuance :

This is to certify that the above- mentioned organization is compliant to the assessment standard for Information Security Management System certification in accordance with Article 47, Paragraph 1 and 4 of Act on Information Network Utilization and Data Protection, etc., and Article 50 of the Enforcement Ordinance of the Act.

Signed by the

President of ISMS Certification Authority

Republic of Korea

210mm×297mm(보존용지(1종) 120g/㎡)

[별지 제7호서식]

정보보호관리체계 인증서 추가발급 신청서

신청인	상호 또는 명칭		성 명(대표자)	
	사업자등록번호		전화번호	
	주 소(소재지)			
추가발급 사유				

위와 같이 정보보호관리체계 인증서의 추가발급을 신청합니다.

200 년 월 일

신청인 (서명 또는 인)

[별지 제8호서식]

정보보호관리체계 인증서 변경 신청서

신청인	상호 또는 명칭		성 명(대표자)	
	사업자등록번호		전화번호	
	주 소(소재지)			
변경내용	변경전	(국문)		
		(영문)		
	변경후	(국문)		
		(영문)		
변경 사유				

위와 같이 정보보호관리체계 인증서 변경을 신청합니다.

200 년 월 일

신청인 (서명 또는 인)

정보보호조치에 관한 지침

[시행 2014.1.1] [고시 제2013 - 196호, 2013.12.31, 타법개정]

제1장 총칙

제1조(목적) 이 지침은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) 제45조제2항에 따라 정보통신서비스 제공자가 정보통신서비스를 제공하는데 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치의 구체적인 내용에 대하여 정하는 것을 목적으로 한다.

제2조(정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. "정보보호조직"이라 함은 정보통신서비스를 안전하게 제공하고 정보보호 활동을 체계적으로 이행할 수 있도록 하는 업무 조직을 말한다.
2. "정보통신설비"라 함은 컴퓨터 장치 등 정보의 수집、가공、저장、검색、송신、수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 말한다.
3. "서비스수준협약"이라 함은 서비스 제공자가 서비스 가입자와 합의를 통하여 사전에 정의된 수준의 서비스를 제공하기로 맺는 협약을 말한다.
4. "정보보호시스템"이라 함은 정보처리시스템 내 정보를 유출、위조、변조、훼손하거나 정보처리시스템의 정상적인 서비스를 방해하는 행위로부터 정보 등을 보호하기 위한 장비 및 프로그램을 말한다.
5. "침입차단시스템"이라 함은 외부 네트워크로부터 내부 네트워크로 침입하는 트래픽을 정해진 규칙에 따라 제어하는 기능을 가진 장비 또는 프로그램을 말한다.
6. "침입탐지시스템"이라 함은 네트워크 또는 시스템에 대한 인가되지 않은 행위와 비정상적인 행동을 탐지하고, 탐지된 위법 행위를 구별하여 실시간으로 침입을 차단하는 기능을 가진 장비 또는 프로그램을 말한다.
7. "웹서버"라 함은 인터넷 이용자들이 웹페이지를 자유롭게 보고 웹서비스(월드 와이드 웹을 이용한 서비스를 말한다)를 이용할 수 있게 해주는 프로그램이 실행되는 장치를 말한다.
8. "DNS서버"라 함은 컴퓨터가 인식하는 IP주소를 사람이 인식하기 쉬운 도메인 이름으로 상호 변환하는 시스템을 운영하는 장치를 말한다.
9. "DB서버"라 함은 여러 사람에 의해 공유되어 사용될 목적으로 통합하여 관리되는 데이터베이스 처리를 위한 서버를 말한다.

10. "DHCP서버"라 함은 네트워크 관리자들이 조직 내의 네트워크 상에서 IP주소를 중앙에서 관리하고 할당할 수 있도록 해주는 동적 호스트 설정 통신규약 서버를 말한다.
11. "라우터"라 함은 국제관문 게이트웨이, 무선응용프로토콜(WAP) 게이트웨이, 백본 라우터 등을 말한다.
12. "스위치"라 함은 백본 스위치, L4 L7 스위치, 인터넷접속교환기 등을 말한다.
13. "ACL(Access Control List)"이라 함은 특정 시스템에 접근할 수 있는 권한을 컴퓨터 운영체계에 알리기 위해 설정해 놓은 목록을 말한다.
14. "프로토콜"이라 함은 정보기기 사이에서 정보교환이 필요한 경우, 이를 원활하게 하기 위하여 정한 여러 가지 통신규칙과 방법 등 통신규약을 말한다.
15. "취약점 점검"이라 함은 컴퓨터의 하드웨어 또는 소프트웨어의 결함이나 체계 설계상의 허점으로 인해 사용자에게 허용된 권한 이상의 동작이나 허용된 범위 이상의 정보 열람·변조·유출을 가능하게 하는 약점에 대하여 점검하는 것을 말한다.
16. "관리용 단말"이라 함은 네트워크 장비, 웹서버, DB서버 등 주요 정보통신설비 유지·보수 및 관리를 위하여 정보통신설비와 접속되어 있는 장비 등을 말한다.

제2장 정보보호조치

제3조(정보보호조치의 내용) 법 제45조제2항에 따라 정보통신서비스 제공자가 정보통신망의 안전성 및 정보의 신뢰성을 확보하기 위하여 마련하여야 하는 관리적·기술적·물리적 보호조치의 구체적인 내용은 별표 1과 같다.

제4조(정보보호조치 이행여부 점검) 정보통신서비스 제공자는 매년 별표 1의 정보보호조치의 이행여부를 자체적으로 점검하거나 외부 전문기관으로 하여금 점검하게 할 수 있다.

제5조(규제의 재검토) 「미래창조과학부장관은「행정규제기본법」제8조 및 「훈령·예규 등의 발령 및 관리에 관한 규정(대통령훈령 제248호)」에 따라 이 고시에 대하여 2014년 1월 1일을 기준으로 매 3년마다(매 3년이 되는 해의 1월 1일 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2008 - 12호,2008.5.19>

이 지침은 고시한 날부터 시행한다.

부칙 <제2009 - 27호,2009.11.5>

이 고시는 2009년 11월 5일부터 시행한다.

부칙 <제2010 - 3호,2010.2.3>

제1조(시행일) 이 고시는 2010년 2월 3일부터 시행한다.

제2조(서식에 관한 경과조치) 이 고시 시행당시 종전의 규정에 의한 서식은 2010년 6월 30일까지 이 고시에 의한 서식과 함께 사용할 수 있다.

부칙 <제2012 - 24호,2012.3.15>

이 고시는 발령한 날부터 시행한다

부칙 <제2013 - 3호,2013.1.17>

이 고시는 2013년 2월 18일부터 시행한다.

부칙 <제2013 - 34호,2013.8.8>

이 고시는 발령일부터 시행한다.

부칙 <제2013 - 196호,2013.12.31>

제1조(시행일) 이 고시는 2014년 1월 1일부터 시행한다.

[별표 1]

보호조치의 구체적인 내용(제3조 관련)

구 분			세 부 조 치 사 항
1. 관리적 보호조치	1.1. 정보보호 조직의 구성·운영	1.1.1. 정보보호조직의 구성	▸ 정보보호 최고책임자, 정보보호관리자, 정보보호담당자로 구성된 정보보호조직을 운영
		1.1.2. 정보보호 최고책임자의 지정	▸ 기업의 정보보호를 책임지는 이사 이상의 상근임원으로 지정
		1.1.3. 정보보호조직 구성원의 역할	▸ 정보보호 최고책임자는 정보보호 업무와 조직을 총괄 지휘 ▸ 정보보호관리자는 정보보호 업무의 실무를 총괄하고 관리 ▸ 정보보호담당자는 정보보호 업무의 분야별 실무를 담당
	1.2. 정보보호 계획 등의 수립 및 관리	1.2.1. 정보보호 방침의 수립·이행	▸ 정보보호 목표, 범위, 책임 등을 포함한 정보보호 방침(policy) 수립 ▸ 정보통신서비스와 관련된 모든 법, 규제, 계약, 정책, 기술상의 요구사항을 문서화하고 시행
		1.2.2. 정보보호 실행계획의 수립·이행	▸ 정보보호 방침을 토대로 예산, 일정 등을 포함한 당해 연도의 정보보호 실행계획을 수립 ▸ 최고경영층이 실행계획을 승인하고 정보보호 최고책임자가 추진 상황을 매 반기마다 점검
		1.2.3. 정보보호 실무지침의 마련·준수	▸ 정보통신설비 및 시설에 대한 관리적·기술적·물리적 보호조치의 구체적인 시행 방법·절차 등을 규정한 정보보호 실무지침을 마련 ▸ 정보보호 최고책임자가 실무지침을 승인하고 관련 법·제도, 설비의 교체 등 변경사유가 발생할 경우 보완하여 관리
		1.2.4. 정보보호 사전점검	▸ 새로운 정보통신망을 구축하거나 정보통신서비스를 제공하고자 하는 때에는 그 계획, 설계, 구현, 테스트 등에서 정보보호에 관한 사항을 고려
	1.3. 인적 보안	1.3.1. 내부인력 보안	▸ 임직원의 전보 또는 퇴직시 즉시 관련 계정 등에 대한 접근권한을 제거 ▸ 임직원에게 정보보호 인식을 제고할 수 있는 홍보(정보보호 실천수칙 보급 등)를 실시 ▸ 정보보호조직의 구성원 및 정보보호와 관련된 업무에 종사하는 자에게 정기적으로 정보보호 교육 실시
		1.3.2. 외부인력 보안	▸ 자사 직원이 아닌 자를 업무에 활용할 경우 보안서약을 징구
		1.3.3. 위탁운영 보안	▸ 전산업무를 외부에 위탁할 경우 보안계약서 또는 서비스수준협약 등에 '정보보호에 관한 위탁업체의 책임범위', '위탁업무 종단에 따른 비상대책' 등을 반영
	1.4. 이용자 보호	1.4.1. 정보보호 정보 제공	▸ 이용자에게 침해사고 예·경보, 보안취약점, 계정·비밀번호 관리방안 등의 정보를 지속적으로 제공
		1.4.2. 정보보호 현황	▸ 정보보호 투자 및 인력 현황, 정보보호 관련 인증 등 정보보호 현황을 자사 홈페이지 등에 공개

구 분			세 부 조 치 사 항
		공개	
	1.5. 침해사고 대응	1.5.1. 침해사고 대응 계획의 수립·이행	▸ 침해사고 정의 및 범위, 대응체계(보고 및 조치 체계), 대응 방법 및 절차, 복구 방법 및 절차, 증거자료 수집 및 보관 등을 포함한 침해사고 대응계획을 마련·시행
	1.6. 정보보호 조치 점검	1.6.1. 정보보호조치의 자체 점검	▸ 정보보호관리자는 매년 정보보호조치 및 정보보호 실무지침의 기준에 따라 자체적으로 정보보호 현황을 점검
	1.7. 정보자산 관리	1.7.1. 정보통신설비 및 시설의 현황 관리	▸ 정보통신망 구성도를 마련하고 변경사항이 있을 경우 보완·관리 ▸ 정보통신설비, 시설의 목록(용도 및 위치 등 포함) 작성 및 네트워크와 분리된 환경에서 안전하게 관리
	1.8. 정보보호 투자	1.8.1. 정보보호 투자계획 수립·이행	▸ 기업의 정보보호를 위해 위험관리에 기반한 적정 수준(정보기술 부문 예산의 5%이상)의 정보보호 예산 편성 및 집행
2. 기술적 보호조치	2.1. 네트워크 보안	2.1.1. 트래픽 모니터링	▸ 네트워크 모니터링 도구를 이용하여 백본망, 주요노드 및 외부망과 연계되는 주요회선의 트래픽 소통량을 24시간 모니터링
		2.1.2. 무선서비스 보안	▸ 무선랜서비스, 무선인터넷서비스를 제공할 경우에는 사용자인증, 데이터암호화 등 보안조치를 마련
		2.1.3. 정보보호시스템 설치·운영	▸ 외부망과 연계되는 구간에 침입차단시스템, 침입탐지시스템 등 네트워크의 안전성을 제고할 수 있는 정보보호시스템을 설치·운영
		2.1.4. 정보보호를 위한 모니터링	▸ 주요시스템·네크워크 사용 및 접근이 명확하게 허용된 범위 안에 있는지를 확인하기 위한 모니터링 시스템 구축 또는 위탁운영을 통하여 침해사고 탐지·대응 체계 운영
	2.2. 정보통신 설비 보안	2.2.1. 웹서버 보안	▸ 외부에 서비스를 제공하는 웹서버는 단독서버로 운영하고 DMZ에 설치
		2.2.2. DNS서버 보안	▸ 과부하에 대비한 부하분산 대책을 마련 ▸ 설정파일 백업 실시
		2.2.3. DHCP서버 보안	▸ 과부하에 대비한 부하분산 대책을 마련 ▸ 설정파일 백업 실시 ▸ IP 할당 상황 등에 대한 로그기록 유지·관리
		2.2.4. DB서버 보안	▸ 내부망에 설치 ▸ 외부망에서 직접 접속할 수 없도록 네트워크를 구성
		2.2.5. 라우터/스위치 보안	▸ ACL(Access Control List) 등의 접근제어 기능을 적용할 수 있는 설비를 사용
		2.2.6. 정보보호시스템 보안	▸ 이상징후 탐지를 알리는 경고 기능을 설정하여 운영 ▸ 정보보호시스템 보안기능(비정상 트래픽 차단 등)의 정상 작동 여부를 주기적으로 점검(월 1회 이상)

구 분			세 부 조 치 사 항
		2.2.7. 취약점 점검	▸ 연 1회 이상 취약점 점검을 실시하고 발견된 취약점을 보완
		2.2.8. 접근통제 및 보안설정 관리	▸ 인가된 자만 시스템에 접속할 수 있도록 설정하고, 인터넷 등을 통해 외부에서 접속할 경우 일회용 패스워드 사용 등 인가 절차를 강화 ▸ 불필요한 프로토콜 및 서비스 제거 등 보안설정
		2.2.9. 관리자 계정의 비밀번호 관리	▸ 관리자 계정의 비밀번호는 8자리 이상으로 설정. 단, 설정 가능한 자리수가 8자리 미만일 때는 설정 가능한 최대의 자리수로 설정 ▸ 최소 3개월에 1회 이상 비밀번호 변경
		2.2.10. 로그 관리	▸ 최소 1개월 이상 로그기록 유지·관리(정보보호시스템은 3개월)
		2.2.11. 보안패치 관리	▸ 보안패치 정보를 주기적으로 입수하고 적용 ▸ 주요 보안패치에 대해서는 적용일 등 패치정보를 기록·관리
		2.2.12. 백업 및 복구	▸ 주요정보를 주기적으로 백업 ▸ 백업 담당자, 백업 및 복구 방법·절차·주기 등을 기록·관리
		2.2.13. 중요정보의 암호화	▸ 비밀번호는 복호화 되지 않도록 일방향 암호화하여 저장 ▸ 주민등록번호, 신용카드번호 및 계좌번호, 정보자산현황 등은 안전한 암호알고리듬으로 암호화하여 저장
		2.2.14. 관리용 단말 보안	▸ 일반적인 업무 및 개인적인 용도의 사용을 금지하고 DB서버, 웹서버 등 주요 정보통신설비의 접속에만 사용 ▸ 전용 또는 인터넷과 격리된 환경(필요시 접근통제 정책을 수립하고 제한적 접속 허용)에서 인가된 이용자만 이용할 수 있도록 통제 ▸ 관리용 단말로의 외부접속 차단, 주기적 보안패치 및 악성 소프트웨어 예방·탐지 활동 실시
3. 물리적 보호조치	3.1. 출입 및 접근 보안	3.1.1. 정보통신시설의 출입·접근 통제	▸ 비인가자가 출입할 수 없도록 잠금장치를 설치 ▸ 출입자의 기록을 1개월 이상 유지·보관
	3.2. 부대설비 및 시설 운영·관리	3.2.1. 백업설비 및 시설 설치·운영	▸ 주요정보를 백업하여 보관할 수 있는 백업설비 및 시설을 설치·운영

<비 고>

1. 2.2.7~2.2.14의 사항은 2.2.1~2.2.6에 해당하는 설비에 적용된다.
2. 2.1.1.의 규정에 따른 주요회선에 대한 트래픽 소통량 모니터링은 관리자 등이 모니터링 현장에 상주하지 않는 방법으로 실시할 수 있다.
3. 2.2.11.의 규정에 따른 보안패치 정보의 입수·적용 주기는 정보보호관리자의 판단에 따라 정한다.

4. 2.2.12.의 규정에 따른 주요정보의 백업 주기는 정보보호관리자의 판단에 따라 정한다.

정보보호 사전점검에 관한 고시

[시행 2016.4.8] [고시 제2016 - 39호, 2016.4.8, 일부개정]

제1장 총칙

제1조(목적) 이 고시는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) 제45조의2 및 같은 법 시행령(이하 "영"이라 한다) 제36조의2부터 제36조의5까지의 규정에 따라 정보보호 사전점검의 방법·절차·수수료에 관한 세부사항과 그 밖의 정보보호 사전점검에 필요한 사항에 대하여 정하는 것을 목적으로 한다.

제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "정보보호 사전점검(이하 ‘사전점검’이라 한다)"이란 정보통신망의 구축 또는 정보통신서비스의 제공 이전에 계획 또는 설계 등의 과정에서 정보보호를 고려하여 필요한 조치를 하거나 계획을 마련하는 것을 말한다.
2. "정보보호컨설팅"이란 전자적 침해행위에 대비하기 위한 정보시스템의 취약점 분석·평가와 이에 기초한 보호대책의 제시 또는 정보보호 관리체계 구축 등을 주된 목적으로 수행한 컨설팅을 말한다.
3. "정보보호 사전점검 대상자(이하 ‘대상자’라 한다)"란 정보보호 사전점검을 받으려는 자를 말한다.

제2장 사전점검의 실시 시기

제3조(사전점검 실시 시기) 사전점검은 대상자가 새로이 정보통신망을 구축하거나 정보통신서비스를 제공하고자 하는 때에는 그 계획 또는 설계 단계부터 실시한다.

제3장 정보보호 사전점검 대상

제4조(사전점검 실시 우대) 미래창조과학부는 사업자가 사전점검을 실시하거나 실시 계약을 체결한 경우 해당 사업 또는 서비스에 대하여 가점을 부여하는 등 우대조치를 할 수 있다.

제5조(사전점검 대상 범위) 사전점검 대상 범위는 제공하려는 사업 또는 정보통신서비스를 구성하는 하드웨어, 소프트웨어, 네트워크 등의 유·무형 설비 및 시설을 대상으로 한다.

제4장 정보보호 사전점검 수행기관

제6조(사전점검 수행기관 지정 공고) ① 미래창조과학부는 영 제36조의4제3항에 따라 사전점검을 수행하는 외부 전문기관(이하 "사전점검 수행기관"이라 한다)을 지정할 수 있다.
② 미래창조과학부는 사전점검 수행기관을 지정할 필요가 있을 때에는 미리 접수 신청기간과 신청요령 등을 정하여 관보 및 인터넷 홈페이지에 20일 이상 공고하여야 한다.

제7조(사전점검 수행기관 지정 요건) ① 사전점검 수행기관으로 지정받으려는 자는 시스템·네트워크·데이터베이스·소프트웨어 개발 보안 및 취약점 분석·평가 분야 등의 정보보호 기술인력을 보유하여야 한다.
② 사전점검 수행기관이 되기 위해서는 정보보호컨설팅 수행실적이 있어야 한다.
③ 사전점검 수행기관으로 지정 받으려는 자는 사전점검 과정에서 발생하는 자료를 보호하기 위하여 다음 각 호를 포함한 보호대책을 별표 1과 같이 수립·시행하여야 한다.
1. 사전점검 수행구역 및 설비에 대한 보호대책
2. 사전점검 수행인력에 대한 보호대책
3. 문서 및 전산자료에 대한 보호대책
4. 일반 관리적 보호대책

제8조(사전점검 수행기관 지정 절차) 사전점검 수행기관 지정 절차는 별표 2와 같다.

제9조(사전점검 수행기관 지정 신청) ① 사전점검 수행기관으로 지정받으려는 자는 별지 제1호서식의 수행기관 지정신청서를 미래창조과학부에 제출하여야 한다.
② "정보보호 기술인력 보유현황"의 제출 서식은 별지 제2호서식과 같다.
③ "정보보호컨설팅 수행실적 명세서"의 제출 서식은 별지 제3호서식과 같다.

제10조(사전점검 수행기관 지정 심사) ① 미래창조과학부는 사전점검 수행기관 지정신청서를 접수한 경우 심사위원회를 구성하여 다음 각 호의 심사업무를 수행하게 할 수 있다.
1. 정보보호 기술인력 현황 확인
2. 신청인의 정보보호컨설팅 수행실적 검토
3. 사전점검 수행기관 보호대책의 검토
② 심사위원회는 사전점검 수행기관 지정 신청을 검토하기 위하여 서류심사 또는 현장실사를 할 수 있다.
③ 심사위원회는 서류심사 또는 현장실사 결과를 종합적으로 검토하여 심사 결과를 작성하여야 한다.

제11조(사전점검 수행기관 지정) ① 미래창조과학부는 심사위원회의 심사결과를 검증하여야 한다.

② 미래창조과학부는 지정신청서 및 관련 자료 검토 결과에 따라 사전점검 수행기관 지정을 받으려는 신청인에게 별지 제4호서식에 따른 "정보보호 사전점검 수행기관 지정서"를 교부한다.

제12조(사전점검 수행기관 사후관리) 미래창조과학부는 수행기관이 제7조제3항 각호에 따른 보호대책의 준수 여부를 점검할 수 있다.

제13조(사전점검 수행기관 지정의 유효기간) ① 사전점검 수행기관의 유효기간은 3년으로 한다.

② 사전점검 수행기관이 수행기관 지정을 계속 유지하려고 할 경우 유효기간 만료 3개월 전에 재지정 신청을 하여야 하며, 재지정 절차는 지정 절차를 따른다.

③ 사전점검 수행기관이 인수·합병 등에 따른 법인격 변동이 있을 경우 재지정 절차를 따른다.

제14조(사전점검 수행기관 지정 취소) ① 미래창조과학부는 사전점검 수행기관이 다음 각 호에 해당할 경우 사전점검 수행기관 지정을 취소하고, 이를 관보에 게재할 수 있다.

1. 거짓이나 그 밖의 부정한 방법으로 지정을 받은 경우
2. 제7조 각 항에 따른 사전점검 수행기관 지정 요건에 미달한 경우

② 사전점검 수행기관이 폐업하거나, 수행기관 지정을 반납하려 할 경우 해당 의사를 명시한 문서에 수행기관 지정서를 첨부하여 미래창조과학부에 제출하여야 한다.

제5장 정보보호 사전점검 수행 인력

제15조(사전점검 수행인력의 요건) 사전점검을 수행하려는 자는 영 제36조의4제3항 별표 2에 따른 정보보호 기술인력의 자격 기준을 갖추어야 한다.

제16조(사전점검 수행인력의 교육) ① 한국인터넷진흥원은 정보보호 사전점검의 품질관리 및 수행인력의 전문성 확보를 위하여 필요한 교육을 할 수 있다.

② 사전점검 교육과정은 정보통신서비스 구조 분석, 보호자산 식별, 위협 및 취약점 분석, 위협 시나리오 작성 등 사전점검 절차·방법 및 프로젝트관리를 포함한다.

제6장 정보보호 사전점검 수행

제17조(사전점검 계약) 대상자가 자체적으로 사전점검을 수행하지 않고 한국인터넷진흥원 또는 사전점검 수행기관으로부터 사전점검을 받으려는 경우 점검기간, 참여인력, 사전점검 수수료, 사전점검 범위 등에 대한 합의를 포함하는 사전점검 실시 계약을 체결하여야 한다.

제18조(사전점검기준) 영 제36조의2에 따른 사전점검기준은 별표 3과 같다.

제19조(사전점검 준비) 대상자는 사전점검을 수행하기 위하여 사업 또는 정보통신서비스 담당자 및 제15조의 요건을 갖춘 내·외부의 사전점검 수행인력 등으로 정보보호 사전점검 수행팀(이하 "점검팀"이라 한다)을 구성하고, 사전점검 수행계획서를 작성한다.

제20조(설계 검토) 점검팀은 사전점검을 하려는 사업 또는 정보통신서비스에 대하여 아래 각 호의 순서로 설계 검토 단계를 진행한다.

1. 서비스 정의
2. 서비스 구조 분석
3. 보호자산 식별
4. 위협 분석
5. 취약점 분석
6. 위험 분석
7. 위협 시나리오 도출
8. 보호대책 도출

제21조(보호대책 적용) 대상자는 사전점검 대상 정보통신서비스의 설계 및 구현 단계에서 도출한 보호대책을 적용한다.

제22조(보호대책 구현 현황 점검 및 시험) 점검팀은 아래 각 호의 순서로 보호대책 구현 현황을 점검한다.

1. 권고한 보호대책에 대한 실제 구현 현황을 파악
2. 위협 시나리오에 따라 현장에서 모의해킹 및 침투시험 등을 통해 위협 가능성을 확인

제23조(사전점검 결과 정리) 점검팀은 사전점검 결과보고서를 작성하여 대상자에게 제출한다.

제24조(사전점검 결과 처리) ① 대상자는 사전점검 결과에 따라 적용하지 아니한 보호대책이 있을 경우 보호조치 계획을 수립하고 정보통신망 또는 정보통신서비스의 운영과정에 반영한다.
② 사전점검 과정에서 심각한 위험이 발견된 경우 그에 대한 보호대책을 구현한 이후에 정보통신망 또는 정보통신서비스를 운영하여야 한다.

제25조(해설서) 한국인터넷진흥원장은 이 고시에 대한 해설서를 마련하여 미래창조과학부장관의 승인을 받아 공표할 수 있다.

제7장 정보보호 사전점검 수수료

제26조(사전점검 수수료) 사전점검 수수료는 다음 각 호의 기준을 준용하여 별표 4에 따라 산정한다. 다만, 대상자와 한국인터넷진흥원 또는 사전점검 수행기관이 이와 다르게 합의할 경우에는 다음 각 호를 적용하지 아니할 수 있다.

1. 「엔지니어링산업 진흥법」 제31조제2항에 따른 엔지니어링사업의 대가 기준
2. 한국소프트웨어산업협회가 제공하는 「SW사업 대가산정 가이드」의 정보보안 컨설팅비

제27조(재검토기한) 「훈령ㆍ예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제334호)에 따라 이 고시에 대하여 2017년 1월 1일 기준으로 매 3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2013-5호,2013.1.17>

제1조(시행일) 이 고시는 2013년 2월 18일부터 시행한다.

제2조(재검토 기한) 「훈령ㆍ예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 고시 발령 후 법령이나 현실여건의 변화 등을 검토하여 이 고시의 폐지, 개정 등 조치를 하여야 하는 기한은 2016년 2월 17일까지로 한다.

부칙 <제2013-39호,2013.8.8>

제1조(시행일) 이 고시는 2013년 8월 8일부터 시행한다.

제2조(재검토 기한) 「훈령ㆍ예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 고시 발령 후 법령이나 현실여건의 변화 등을 검토하여 이 고시의 폐지, 개정 등 조치를 하여야 하는 기한은 2016년 3월 23일까지로 한다.

부칙 <제2016-39호,2016.4.8>

제1조(시행일) 이 고시는 공포한 날부터 시행한다.

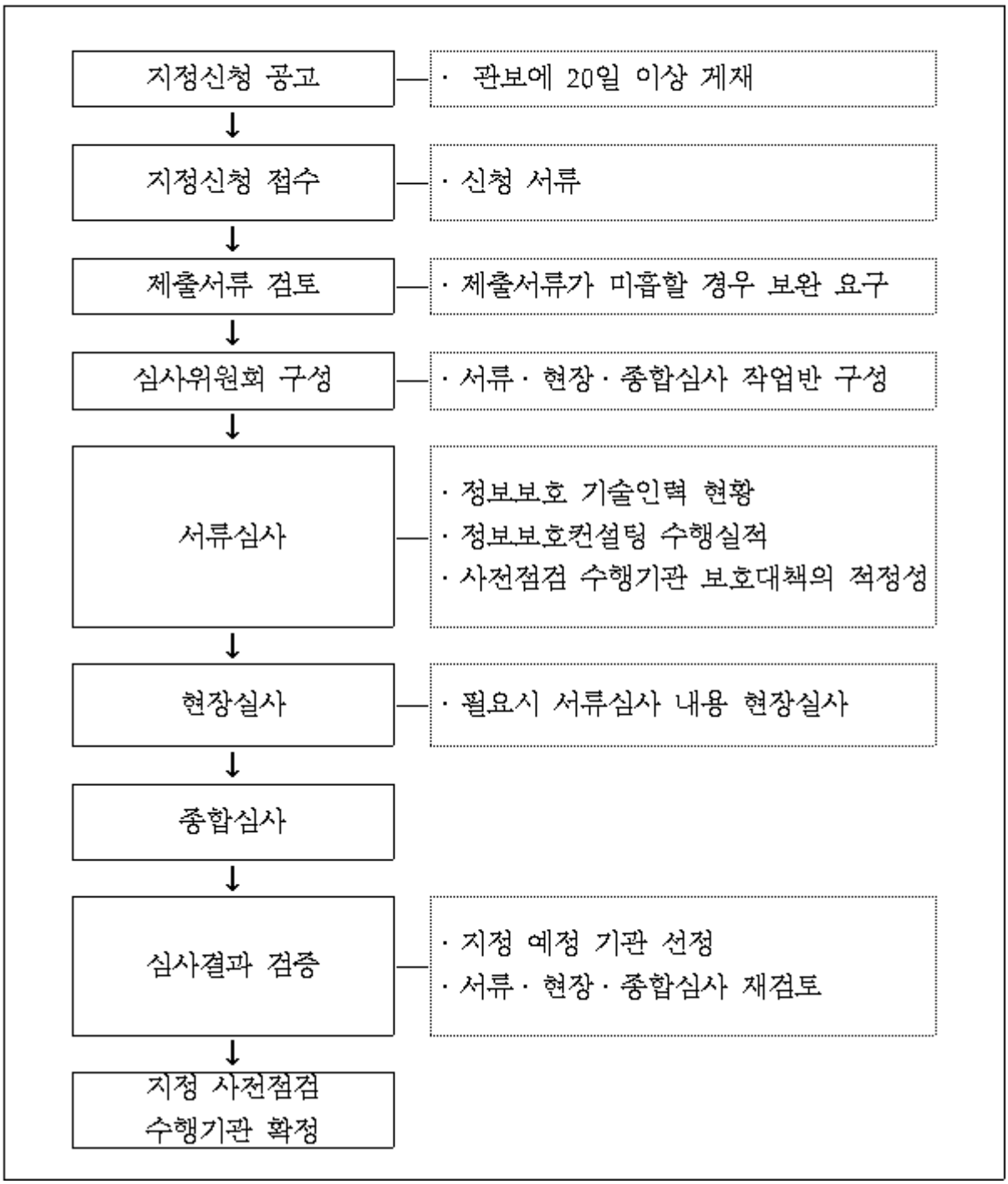
[별표 1]

정보보호 사전점검 수행기관 보호대책의 주요 내용(제7조 관련)

항 목	주 요 내 용
Ⅰ. 사전점검 수행구역 및 설비에 대한 보호대책	1. 사전점검을 수행하는 구역을 지정하여야 한다. 이 구역은 해당 사전점검 수행인력이 아닌 자의 출입이 제한되어야 한다. 2. 사전점검 분석 자료를 처리·전송·저장하는 정보통신망에 대하여 위험분석에 따른 통제대책을 강구하여야 한다. 이 경우 노트북 컴퓨터, 그 밖에 휴대용 정보처리기기에 대한 통제대책을 포함하여야 한다.
Ⅱ. 사전점검 수행인원에 대한 보호대책	3. 사전점검 수행인력이 관계 법령에 따르는 비밀유지의무를 포함한 제반 의무를 숙지하고 이의 준수를 확약하는 내용의 서약서를 작성하는 지침과 절차를 마련하여야 한다. 4. 사전점검 수행기관이 사전점검 수행인력을 채용할 때의 적격 심사와 퇴직할 때의 퇴직자 관리를 위한 지침과 절차를 마련하여야 한다. 5. 사전점검 수행인력이 사전점검 대상기관의 보안대책을 위반하는 경우에 제재 및 처리에 관한 내부규정을 마련하여야 한다.
Ⅲ. 문서 및 전산자료에 대한 보호대책	6. 사전점검 수행을 위한 자료를 보호하기 위하여 관련 보안대책을 마련하여야 한다. 7. 사전점검 수행인력이 아닌 자는 해당 사전점검 관련 자료에 접근·열람하거나 편집·반출·폐기하지 못하도록 통제대책을 강구하여야 한다. 8. 정보통신망을 통하여 처리·전송·저장하는 사전점검 관련 자료에 대하여 위험분석에 따른 보호대책을 강구하여야 한다. 9. 서면, 도면, 마이크로필름·전산출력물 등 출력물 형태의 사전점검 관련 자료에 대한 보관·복사·배포·폐기 등에 관한 보호대책을 강구하여야 한다.
Ⅳ. 일반 관리적 보호대책	10. 사전점검에 관한 수행기관의 기본방침을 대표자가 서면으로 공표하고 사전점검 수행인력을 포함한 임직원이 이를 숙지하여야 한다. 11. 사전점검 업무에 대한 위험분석 및 보호대책의 관리·운영 실태를 주기적으로 점검·평가하여야 한다.

[별표 2]

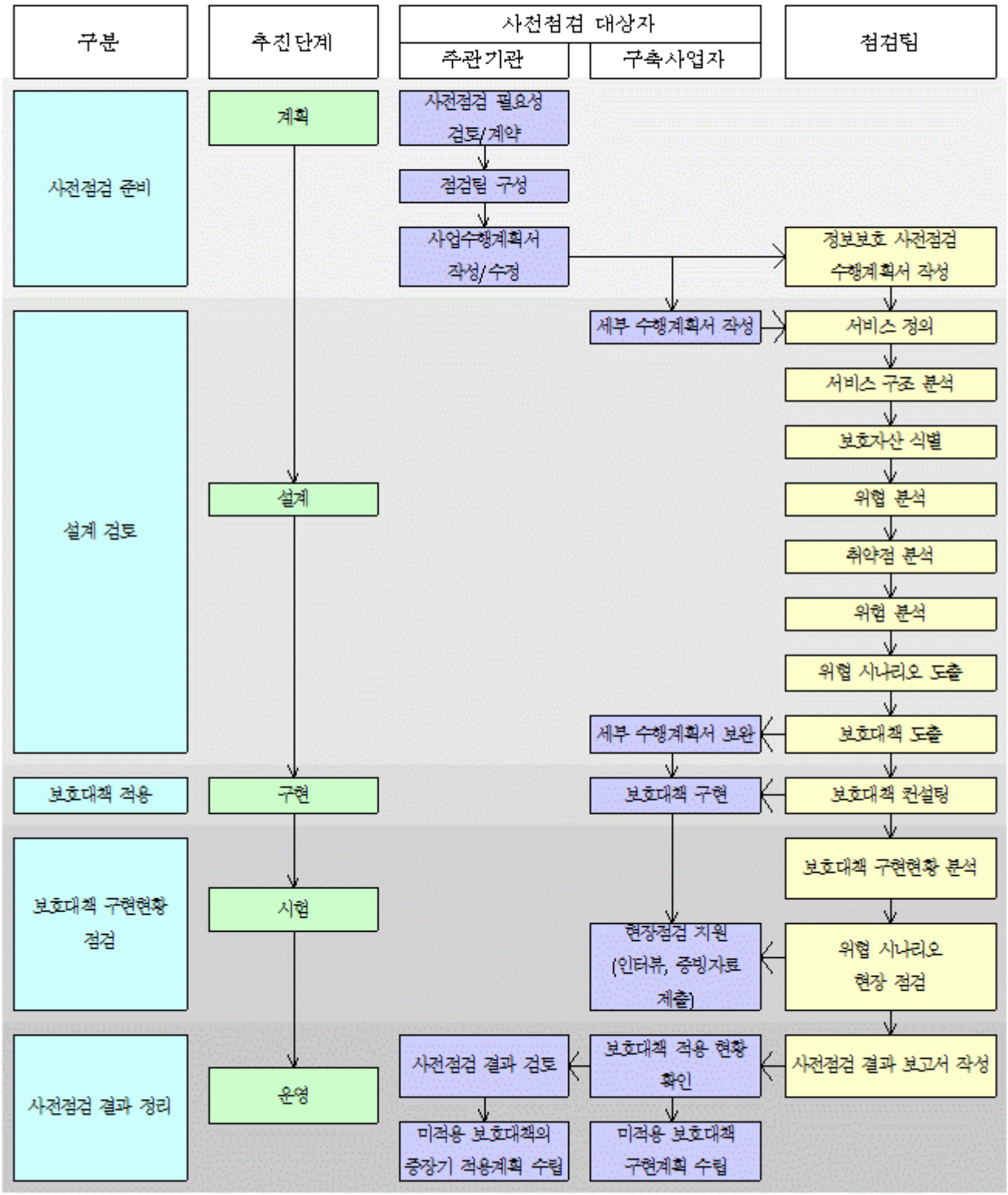
정보보호 사전점검 수행기관 지정 절차(제8조 관련)



[별표 3]

정보보호 사전점검기준(제18조 관련)

1. 설계 검토 단계를 포함한 사전점검 절차는 아래와 같다.



2. 보호자산 식별 단계에서 보호자산의 중요도 평가 기준

가. 대상 서비스를 구성하는 정보자산의 평가요소 도출 및 평가등급 설정은 아래 표와 같다.

평가요소	평가등급	평가점수	설 명
기밀성 (Confidentiality)	H	3	매우 민감한 정보이므로 업무관련 책임자만 접근가능
	M	2	민감한 정보이므로 내부담당자, 책임자 등 일부 허가된 직원만 접근가능
	L	1	민감한 정보는 아니나 내부인만 접근가능
무결성 (Integrity)	H	3	정보의 무결성 손상시 서비스 제공에 치명적인 영향을 주며, 주요업무 및 회사기능에 마비를 초래할 수 있음
	M	2	정보의 무결성 손상시 서비스 제공에 중대한 영향을 줌
	L	1	정보의 무결성 손상시 서비스 제공에 경미한 영향을 주지만, 충분히 해결할 수 있음
가용성 (Availability)	H	3	24시간 항상 가동이 필요하며 중단이 되어서는 안 됨
	M	2	근무시간 중에는 항상 접근 가능해야 함
	L	1	근무시간 중에 50%이상 사용 가능해야하고 접근 가능해야 함

나. 서비스의 특성에 따라 추가하는 평가요소의 등급 산정은 아래 사항을 고려한다.

평가등급	평가점수	설 명
H	3	피해발생시 서비스 품질의 현저한 저하 및 직원이나 시스템 운영자가 업무에 심각한 지장을 초래하는 등급
M	2	피해발생시 서비스 품질의 저하 및 운영자의 작업 효율성을 감소시킬 수 있는 등급
L	1	피해발생시 서비스 품질에 거의 영향을 끼치지 못하는 등급

다. 보호자산의 중요도 평가 결과 및 방법은 아래와 같으며 평균값에 따라 보호자산별 중요도를 부여한다.

평가요소별 평가등급의 평균값	보호자산 중요도
2.0이상 ~	H
1.0이상 ~ 2.0미만	M
0.0이상 ~ 1.0미만	L

※ 평가요소별 평가등급에 따른 점수의 평균값 계산 방법

평균값 = {(C의 점수) + (I의 점수) + (A의 점수) + (추가 점수)} ÷ (평가요소 개수)}

3. 위협 분석 단계에서 위협 평가 기준

가. 대상 서비스를 구성하는 보호자산의 내·외부적 위협요소를 식별하고, 해당 위협의 위협 등급을 평가하는 기준은 아래와 같다.

평가등급	위협에 의한 영향	발생주기 또는 발생가능성
H	보호자산 손실로 인해 업무중단 등 심각한 영향을 초래	서비스 제공시 손실이 자주 발생함 (6개월 이내)
M	보호자산의 손실이 있으나, 업무에 심각하게 영향을 끼치지 않음	서비스를 운영하는 동안 여러 번 손실이 발생할 수 있는 상태(1년 이내)
L	보호자산의 손실이 매우 경미함	서비스를 운영하는 동안 손실이 거의 발생하지 않음

나. 서비스 특성에 따라 추가하는 평가요소의 위협등급은 아래사항을 고려하여 산정한다.

위협영향	발생주기	위협등급
H	H	H
H	M	H
H	L	M
M	H	M
M	M	M
M	L	L
L	H	M
L	M	L
L	L	L

4. 취약점 분석 단계에서 취약점 평가 기준

가. 위협분석 단계에서 도출된 위협 분류와 내용을 활용하여 취약점 관련 정보를 수집하고 관리적·물리적·기술적 사항에 대한 취약점을 식별하고 아래 취약점 평가 기준표를 참고하여 평가한다.

매우 취약 (VH)	보호자산의 복구가 불가능하거나 피해규모가 아주 큰 경우
비교적 취약(H)	최고 경영자나 상급관리자의 정밀한 검색 및 승인을 필요로 하는 위협을 발생 시킬 수 있는 경우. 보호자산의 복구는 가능하나 그 피해규모가 비교적 큰 경우
보통(M)	취약점이 상급관리자의 검토 및 승인을 필요로 하는 정도의 위협을 발생 시킬 수 있는 경우
거의 취약하지 않음(L)	취약점이 보호자산에 별다른 영향을 끼치지 않거나 취약점이 자산에 약간의 영향은 끼치지만 그 영향이 미미해서 해당 보호자산이 하위 관리자의 조치만으로 문제해결이 가능한 경우

나. 점검팀이 자체 평가기준을 보유하고 있을 경우 해당 기준을 활용할 수 있다.

5. 위험 분석 단계에서 위험 평가 기준

가. 보호자산에 발생 가능한 위험을 평가하는 등급 부여 기준은 아래와 같다.

평가등급	내용설명
H	- 위협이 발생될 가능성이 매우 높고, 발생 시 서비스 품질의 현저한 저하 및 직원이나 시스템 운용자가 업무에 심각한 지장을 초래
M	- 위협의 발생가능성이 높고, 발생 시 서비스 품질에 미미한 영향을 미침 - 위협의 발생가능성이 보통이거나 낮고, 발생 시 서비스 품질의 저하 및 운영자의 작업 효율성을 감소시킴
L	- 위협발생 가능성이 낮고, 피해발생시 서비스 품질에 거의 영향을 끼치지 못함

나. 보호자산의 중요도, 위협 등급, 취약점 등급 등을 고려한 위험 등급은 아래와 같다.

보호자산 중요도	위협등급	취약점등급	위험등급
H	H	VH	H
H	H	H	H
H	H	M	H
H	H	L	M
H	M	VH	H
H	M	H	H
H	M	M	H
H	M	L	M
H	L	VH	H
H	L	H	M
H	L	M	M
H	L	L	L
M	H	VH	H
M	H	H	H
M	H	M	H
M	H	L	M
M	M	VH	H
M	M	H	H
M	M	M	M
M	M	L	L
M	L	VH	M
M	L	H	M
M	L	M	L
M	L	L	L
L	H	VH	M
L	H	H	M
L	H	M	L
L	H	L	L
L	M	VH	M
L	M	H	M
L	M	M	L
L	M	L	L
L	L	VH	L
L	L	H	L
L	L	M	L
L	L	L	L

[별표 4]

정보보호 사전점검 수수료 산정기준(제26조 관련)

1. 수수료 산정 방식

수수료 = 직접인건비 + 직접경비 + 제경비 + 기술료

① 직접인건비는 사전점검에 투입되는 컨설턴트에 대한 인건비로 산정한다. 인건비는 「SW사업 대가산정 가이드」의 정보보안 컨설팅비에 따른다

② 직접경비는 사점점검 업무의 수행에 따라 발생하는 교통비, 숙박비 및 식대 등 사전점검에 소요되는 직접적인 경비를 산정한다.

③ 제경비는 최대 (직접인건비 × 120%) 로 산정한다.

④ 기술료는 최대 {(직접인건비 + 제경비) × 40%} 로 산정한다.

■ 정보보호 사전점검에 관한 고시[별지 제1호서식]

정보보호 사전점검 수행기관 지정신청서

※ 색상이 어두운 란은 신청인이 적지 않습니다.

접수번호	접수일	처리기간 30일

신청인	회사명 또는 상호	설립일자
	대표자 성명	전화번호
	주소(주된 사무소의 소재지)	
	자본금 백만 원(외국인 투자비율 %)	

최근 3년 이내의 연도별 정보보호컨설팅 수행실적	신청일 기준 1년 이내의 실적	총 백만 원
	신청일 기준 1년 초과 2년 이내의 실적	총 백만 원
	신청일 기준 2년 초과 3년 이내의 실적	총 백만 원
	최근 3년간 평균 실적	총 백만 원

정보보호 기술인력의 수	명

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의2 및 같은 법 시행령 제36조의4에 따라 위와 같이 정보보호 사전점검 수행기관의 지정을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

미래창조과학부 귀중

신청인(대표자) 제출서류	1. 법인의 정관 1부. 2. 별지 제2호서식의 정보보호 기술인력 보유현황과 이를 증명할 수 있는 서류 1부. 3. 별지 제3호서식의 정보보호컨설팅 수행실적 명세서와 이를 증명할 수 있는 서류 1부. 4. 별표 1의 수행기관 보호대책을 확인할 수 있는 서류 1부.	수수료 없 음
담당공무원 확인사항	법인등기사항증명서	

처 리 절 차

이 신청서는 아래와 같이 처리됩니다.

신청서 제출	→	접 수	→	심 사	→	지정여부 결정	→	지정서 교부	→	지정서 수령
신청인		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)		신청인

■ 정보보호 사전점검에 관한 고시[별지 제2호서식]

정보보호 기술인력 보유현황

(앞 쪽)

신청인	회사명 또는 상호	대표자 성명
	주소 또는 소재지	
	정보보호 기술인력의 총 수	

일련번호	성명	주소		최종학력	자격증	비 고
		생년월일	입사일	취득학위 및 학과(전공)		

210mm×297mm[백상지(80g/㎡)]

(뒤 쪽)

일련번호	성명	주소		최종학력	자격증	비 고
		생년월일	입사일	취득학위 및 학과(전공)		

제출서류	1. 졸업증명서 또는 학위증명서 사본 1부. 2. 자격증 사본 1부. 3. 경력증명서 또는 재직증명서(근무부서 또는 담당업무 등이 기재되어야 합니다) 1부.

210mm×297mm[백상지(80g/㎡)]

■ 정보보호 사전점검에 관한 고시[별지 제8호서식]

정보보호컨설팅 수행실적 명세서

신청인	회사명 또는 상호	대표자 성명
	주소 또는 소재지	
	최근 3년 이내의 정보보호컨설팅 수행실적 총계 외 건 (총 천 원)	

일련번호	컨설팅 프로젝트명 대상기관(법인)명	수행기관	계약 금액 (천원)	과제 책임자

제출서류	1. 정보보호컨설팅 계약서 사본(계약금액 및 내역을 확인할 수 있는 것이어야 합니다) 1부. 2. 납품확인증명서 또는 세금계산서 사본 1부.

유의사항

1. 신청인이 직접 수행한 최근 3년 이내의 정보보호컨설팅 수행실적을 모두 기재합니다.
2. 취약점 분석·평가, 보호대책의 제시, 정보보호 관리체계 또는 개인정보보호 관리체계 구축 등을 동시에 수행하였을 경우에는 하나의 건수로 작성합니다.
3. 계약 금액란에는 정보보호컨설팅의 대가로서 지급받은 금액을 기재하되, 다른 업체와 실적을 적정한 비율로 배분한 경우에는 배분받은 금액만을 기재합니다.

210mm×297mm[일반용지 60g/㎡(재활용품)]

■ 정보보호 사전점검에 관한 고시[별지 제1호서식]

(제1쪽)

정보보호 사전점검 수행기관 지정서

제 호

법 인 명 :

대 표 자 :

소 재 지 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의2제3항 및 같은 법 시행령 제36조의4에 따라 위와 같이 정보보호 사전점검 수행기관으로 지정합니다.

년 월 일

미래창조과학부장관 직인

210mm×297mm[백상지(120g/㎡)]

(제2조)

CERTIFICATE
of an Information Security
Precheck Service Provider

Registry No.

Name of Service Provider :

Name of Representative :

Address :

This is to certify that the above Service Provider is designated as an Information Security Precheck Service Provider in accordance with the provision of article 45.2, Clause 3 of Promotion of Information and Communication Network Utilization and Information Protection, Etc. Act and Article 36.4 of Promotion of Information and Communication Network Utilization and Information Protection, Etc. Enforcement Ordinance of Act.

20xx. . .

Signed by the
Minister of Ministry of Science, ICT and Future Planning
Republic of Korea

210mm×297mm[백상지(120g/㎡)]]

집적정보 통신시설 보호지침

[시행 2014.12.30] [고시 제2014 - 109호, 2014.12.30, 일부개정]

제1장 총칙

제1조(목적) 이 지침은「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) 제46조 및 같은 법 시행령 제37조제2항에 따라 집적정보통신시설을 운영·관리하는 사업자가 취하여야 하는 보호조치의 세부적 기준 등 집적정보통신시설 보호를 위해 필요한 사항에 대하여 정하는 것을 목적으로 한다.

제2조(정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. "집적정보통신시설"이라 함은 법 제2조제2호에 따른 정보통신서비스를 제공하는 고객의 위탁을 받아 컴퓨터장치 등 전자정부법 제2조제13호에 따른 정보시스템을 구성하는 장비(이하 "정보시스템 장비"라 한다)를 일정한 공간(이하 "전산실"이라 한다)에 집중하여 관리하는 시설을 말한다.
2. "주요시설"이라 함은 중앙감시실, 항온항습시설, 전산실, 전력감시실, 전력관련시설(축전지설비, 자가발전설비, 수변전설비), 통신장비실 및 방재센터를 말한다.
3. "중앙감시실"이라 함은 주요 시설물의 작동상황을 파악할 수 있는 시설로서, 경보장치, 화재감지센서, CCTV 등 집적정보통신시설을 보호하기 위한 장비의 작동상황을 통합적으로 감시하고 제어하는 장소를 말한다.
4. "전력감시실"이라 함은 각종 전력의 작동상황을 감시·제어하기 위하여 필요한 장비가 설치된 장소를 말하며 중앙감시실과 통합하여 운영될 수 있다.
5. "수변전설비"라 함은 전기를 공급하는 사업자로부터 여러 가지 수전방법에 의하여 전원을 공급받아 집적정보통신시설에서 사용할 수 있도록 하는 수전·변전 및 배전 기능을 수행하는 설비를 말한다.
6. "통신장비실"이라 함은 전송장비, 주배선반(MDF), 라우터, 기타회선 관련 장비 등 전기통신사업법 제2조제3호에 따른 전기통신설비가 설치된 장소를 말한다.
7. "방재센터"라 함은 화재의 발생에 대비하여 이를 감시하기 위하여 필요한 장비가 설치된 장소를 말하며 중앙감시실과 통합하여 운영될 수 있다.
8. "업무연속성계획"이라 함은 집적정보통신시설이 재난시에도 핵심업무를 수행하기 위한 예방, 대응, 복구계획을 포함한 총괄 운영계획을 말한다.

제2장 보호조치

제3조(출입자의 접근제어 및 감시) ① 집적정보통신시설을 관리·운영하는 사업자(이하 "사업자"라 한다)는 집적정보통신시설을 출입하는 자를 감시·통제하고 권한 없는 자의 출입을 방지하기 위하여 다음 각 호에 해당하는 조치를 하여야 한다.

1. 주요시설의 출입구에 신원확인이 가능한 출입통제장치를 설치할 것
2. 집적정보통신시설을 출입하는 자의 신원 등 출입기록을 유지·보관할 것
3. 주요시설 출입구와 전산실 및 통신장비실 내부에 CCTV를 설치할 것
4. 고객의 정보시스템 장비를 잠금장치가 있는 구조물에 설치할 것

② 사업자는 제1항에 따른 보호조치를 효율적으로 수행하기 위하여 중앙감시실을 설치·운용하여야 한다.

제4조(각종 재난에 대비한 보호조치) ① 사업자는 집적정보통신시설에 안정적으로 전원을 공급하고 지진, 수해 및 화재 등으로 인한 전원공급이 중단되는 경우에 대비하기 위하여 다음 각호에 해당하는 조치를 하여야 한다.

1. 전력관련시설(축전지설비, 자가발전설비, 수변전설비)의 상황파악 및 통제를 위한 전력감시실 또는 중앙감시실을 설치할 것
2. 전력공급의 중단을 방지하기 위하여 UPS(무정전전원장치)와 축전지설비를 보유하고, 장시간 외부에서의 전원공급이 중단될 경우에 대비하여 자체 전력공급을 위한 자가발전설비를 구비할 것
3. 수전, 변전 및 배전기능을 갖춘 수변전실을 두어야 하며 배전반에 단락, 지락, 과전류 및 누전을 방지하기 위하여 필요한 장비를 설치할 것
4. 주요시설에는 기존 조명설비의 작동이 멈추는 경우에 대비하여 비상조명을 설치할 것

② 사업자는 각종 전원장비를 보호하기 위하여 다음 각 호에 해당하는 조치를 하여야 한다.

1. 주요시설의 각종 전원장비에 대한 접지시설을 할 것
2. 전산실에 온습도 측정이 가능하도록 항온항습기를 설치할 것

③ 사업자는 도난 및 테러 등으로부터 집적정보통신시설을 보호하기 위하여 다음 각 호에 해당하는 조치를 하여야 한다.

1. 전산실은 천장을 통하여 외부와의 왕래가 불가능하도록 차단하는 조치를 할 것
2. 주요시설이 설치된 건물내부의 창문을 강화유리로 설치하고 개폐가 되지 않도록 할 것

④ 사업자는 지진, 수해 및 화재 등 재난으로부터 집적정보통신시설을 보호하기 위하여 다음 각호에 해당하는 조치를 하여야 한다.

1. 건물은 UPS 등 무거운 장비의 하중에 견딜 수 있도록 필요한 내력구조를 갖추어야 하며 필요시 하중분산시설을 설치할 것
2. 건물은 물리적 충격 및 화재에 견딜 수 있도록 철골조, 철근 콘크리트 및 내화 건축자재를 사용하고 방화문을 설치할 것

3. 누수에 의한 피해를 예방하기 위하여 주요시설의 천장 및 바닥은 방수시공을 할 것

⑤ 사업자는 지진, 수해, 화재 등 각종 재난으로부터 주요시설 설비의 안전운영을 위하여 주요시설 설비 안전운영매뉴얼을 수립하여 관련 직원을 대상으로 교육하고 주기적으로 관리감독하여야 한다.

⑥ 사업자는 주요시설 설비의 변경이 발생한 때에는 관련분야 전문가로부터 변경사항에 대한 안전성 검토를 받아야 한다. 이때 관련전문가는 건축ㆍ전기설비ㆍ소방설비ㆍ재난 등 변경사항에 관련한 전문지식을 지닌 자를 말한다.

제5조(관리인원의 선발 및 배치) ① 사업자는 24시간 경비가 가능하도록 상근 경비원을 두어야 한다.

② 사업자는 주요시설의 유지ㆍ관리를 수행하는 관련분야 2년이상의 경험이 있는 전문인력을 두어야 한다.

③ 사업자는 집적정보통신시설의 효율적 관리ㆍ운영을 위하여 제2항에 따른 전문인력과 소속 인력에 대한 교육ㆍ훈련을 실시하여야 한다.

④ 사업자는 집적정보통신시설의 보호를 위하여 다음 각 호에 해당하는 업무를 수행하는 관리책임자를 두어야 한다.

1. 집적정보통신시설 보호계획의 수립 및 시행
2. 집적정보통신시설에 대한 물리적ㆍ기술적, 인적ㆍ제도적 안전성 점검 ㆍ지도
3. 제3항에 따른 교육ㆍ훈련의 실시
4. 재난대비 업무연속성계획의 수립 및 시행
5. 기타 집적정보통신시설의 보호를 위하여 사업자가 지시하는 관리ㆍ감독 업무

제6조(시설보호계획과 업무연속성계획의 수립 및 시행) ① 사업자는 해킹ㆍ컴퓨터바이러스 유포 등의 전자적 침해행위와 정전ㆍ화재 기타 각종 재난으로부터 집적정보통신시설을 보호하기 위하여 다음 각 호의 사항을 포함하는 계획(이하 "시설보호계획 ” 이라고 한다.)을 수립ㆍ시행하여야 한다.

1. 시설 보호의 목적 및 범위
2. 시설보호 조직ㆍ인력의 구성 및 운영에 관한 사항
3. 시설보호를 위한 교육ㆍ훈련에 관한 사항
4. 침해사고 예방ㆍ대응 및 복구 대책
5. 기타 시설의 안전한 운영ㆍ관리를 위한 지침

② 사업자는 해킹ㆍ컴퓨터바이러스 유포 등의 전자적 침해행위와 정전ㆍ화재 기타 각종 재난으로부터 업무기능을 중단없이 수행하기 위하여 다음 각 호의 사항을 포함하는 계획(이하 "업무연속성계획 ” 이라고 한다.)을 수립ㆍ시행하여야 한다.

1. 재난대응 및 업무재개, 복원활동 수행을 위한 조직 및 운영에 관한 사항
2. 재난 유형별 긴급대응 및 업무재개, 복원활동을 위한 세부절차 및 활동내용

3. 주기적인 모의훈련 수행을 위한 계획수립, 훈련실시, 사후 평가 및 개선방안 반영
4. 기타 재난대응 및 업무재개 등을 위해 필요한 사항

③ 사업자는 제1항 및 제2항에 따른 시설보호계획 및 업무연속성계획을 성실히 준수하여야 하며 업무환경의 변화 등으로 인하여 계획의 수정·보완이 필요한 경우에는 지체없이 검토·보완하여야 한다.

제8조(세부기준) 제3조부터 제6조까지에 따라 사업자가 의무적으로 준수하여야 하는 보호조치의 세부적인 기준은 별표와 같다.

제3장 보호조치 이행 검사 및 평가

제9조(검사의 실시) ① 미래창조과학부는 사업자가 제3조부터 제8조까지에 따른 보호조치 의무를 성실히 이행하였는지 여부를 확인하기 위하여 법 제64조제3항에 따른 검사(이하 "검사"라 한다)를 실시한다.

② 미래창조과학부가 검사를 실시하는 때에는 법 제64조제10항에 따라 한국인터넷진흥원장(이하 "인터넷진흥원장"이라 한다)에게 필요한 지원을 요청할 수 있다.

③ 인터넷진흥원장은 제2항에 따라 검사를 지원하는 때에는 건축·전기설비·소방설비·재난에 관한 전문지식을 지닌 자, 정보보호에 관한 전문지식을 지닌 자가 참여하는 전담반을 구성하여야 한다.

④ 인터넷진흥원장은 검사를 효율적으로 지원하기 위하여 전담반의 구성·운영, 지원 절차 및 방법에 관하여 필요한 사항을 정하여야 한다.

제10조(검사결과의 처리) ① 인터넷진흥원장은 제9조에 따라 검사를 지원한 때에는 그 결과를 미래창조과학부에 통지하여야 한다.

제11조(평가) ① 미래창조과학부는 사업자가 희망하는 때에는 인터넷진흥원장으로 하여금 사업자의 신청을 받아 집적정보통신시설의 안전·신뢰성에 대한 평가를 실시하게 할 수 있다.

② 인터넷진흥원장은 제1항에 따른 평가를 실시하는 경우에는 평가기준, 절차 및 방법 등에 관하여 필요한 사항을 정하여야 한다.

제12조(재검토기한) 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 고시 발령 후 법령이나 현실여건의 변화 등을 검토하여 이 고시의 폐지, 개정 등 조치를 하여야 하는 기한은 2017년 12월 29일까지로 한다.

부칙 <제2008 - 15호,2008.5.19>

이 지침은 고시한 날부터 시행한다.

부칙 <제2009 - 27호,2009.11.5>

이 고시는 2009년 11월 5일부터 시행한다.

부칙 <제2012 - 29호,2012.3.15>

이 고시는 발령한 날부터 시행한다.

부칙 <제2013 - 35호,2013.8.8>

이 고시는 발령한 날부터 시행한다.

부칙 <제2014 - 109호,2014.12.30>

이 고시는 발령한 날부터 시행한다.

[별 표]

집적정보통신시설 보호조치 세부기준(제8조관련)

구분	목표	항 목	내 용
물리적·기술적 보호조치	접근제어 및 감시	출입통제장치	· 주요시설중 중앙감시실, 전산실, 전력감시실, 통신장비실, 방재센터의 출입구에는 출입자의 신원확인을 통해 개폐되는 잠금장치를 설치한다.
		출입기록	· 주요시설에 대한 출입기록(모든 출입자의 신원과 방문목적 및 방문일시에 대한 기록, CCTV녹화, 출입통제장치의 로그기록)을 출입일로부터 2개월 이상 유지되도록 보관한다. · 주요시설이외의 시설에 대한 출입기록(외부 방문자의 신원과 방문목적 및 방문일시에 대한 기록)을 출입일로부터 1개월 이상 유지되도록 보관한다.
		고객 정보시스템 장비 보호	· 전산실내에 보관하여 관리하는 고객의 컴퓨터장비 등 정보시스템 장비는 잠금장치가 있는 구조물(Rack)에 설치한다.
		중앙감시실	· 주요시설중 전산실 및 통신장비실에 대하여 각 시설의 기능별 작동상황 및 사고발생여부를 확인한다. · CCTV가 촬영한 영상을 24시간 감시할 수 있는 모니터를 설치한다.
		CCTV	· 주요시설의 출입구와 주요시설중 전산실 및 통신장비실 내부에 CCTV를 설치한다.
		경보장치	· 방재센터는 화재감시센서의 작동상황이 실시간으로 파악되도록 하고, 화재발생시에 경보신호를 통해 상황을 알 수 있도록 화재감지센서와 연동된 경보장치를 설치한다. · 방재센터는 중앙감시실과 통합하여 운영할 수 있다.
	가용성	전력 및 관련 설비 보호	· 전력(비상전력을 포함), 축전지설비, 자가발전설비, 수변전설비, UPS에 대한 상황파악 및 제어가 가능하도록 전력감시실을 두되, 중앙감시실과 통합하여 운영할 수 있다.
		무정전전원장치(UPS)	· 전산실내 고객 정보시스템 장비의 3개월간 평균 순간사용전력의 130%에 해당하는 전력을 최소 20분 이상 공급할 수 있는 UPS를 설치한다.
		축전지설비	· 별도의 축전지실 또는 잠금장치가 있는 폐쇄형 판넬(Cubicle)로 설비한다. · 축전지는 UPS 장비와 통합하여 관리되어도 무방하다.
		자가발전설비	· 자가발전설비의 발전용량은 전산실내 고객의 정보시스템 장비 및 항온항습기와 집적정보통신시설내에 설치된 유도등의 3개월간 평균 순간사용전력의 130%에 해당하는 전력을 공급할 수 있어야 하고 추가적인 연료의 보충 없이도 2시간이상 발전할 수 있는 연료 공급 저장시설이 있어야 한다.
		수변전설비	· 배전반에 단락·지락 및 과전류를 방지할 수 있도록 계전기(Relay)를 설치하고 누전이 발생하였을 때 이를 차단할 수 있도록 누전차단기 또는 누전경보기를 설치한다. · 수변전설비는 중앙감시실 또는 전력감시실과 연동되어야 한다.
		접지시설	· 주요시설의 정보시스템 장비 등 각종 전원장비에 대한 접지시설을 한다.
		항온항습기	· 전산실에 24시간 항온·항습을 유지하기 위하여 온습도 측정이 가능하도록 항온항습기를 설치한다.
		비상조명 및 유도등 설비	· 주요시설에는 기존 조명설비의 작동이 멈추는 경우에 바닥 또는 작업면의 조도가 최소 10룩스(lux)이상이 유지되도록 비상조명을 설치한다. · 집적정보통신시설 전지역에 유도등 및 유도표지를 설치한다.

구분	목표	항 목	내 용
물리적·기술적 보호조치	방호성	벽면의 구성	· 전산실은 천창을 통하여 외부와의 왕래가 불가능하도록 전산실의 벽면과 접한 천창을 차단하는 조치를 한다.
		유리창문 설비	· 주요시설관련 건물내부의 창문은 강화유리를 사용하고 개폐가 되지 않도록 설치한다.
	방재성	하중안전성	· UPS, 변압기, 배전반, 자가발전설비가 설치된 장소의 바닥은 최소 500kg/㎡ 이상의 하중에 견디도록 필요한 조치를 하되, 적재하중치(장비의 단위면적당 중량과 건축물의 구조를 고려하여 계산한 하중치에 2.5<안전율>를 곱한 값)가 500kg/㎡을 초과할 경우에는 그 값에 해당하는 하중에 견디도록 필한 조치를 하여야 한다.
		소방시설	· 집적정보통신시설 전 지역에 열감지 또는 연기감지 센서를 설치한다. · 주요시설은 소화시 장비에 피해를 주지 않도록 가스 소화장비를 설치하고 주요시설외의 지역에는 가스 소화장비 또는 살수 소화장비(스프링클러)를 설치한다. · 화재가 발생한 경우 주요시설로 화재가 번지는 것을 방지하기 위하여 방화문을 설치한다.
		건축자재	· 집적정보통신시설의 건물은 화재 및 물리적 충격에 견디기 위해 철골조, 철근 콘크리트를 사용한 건축물이어야 한다. · 바닥재, 내벽, 천창 등의 건물 내부에 사용하는 자재는 화재발생시에도 잘 연소되지 않는 불연재료·준불연재료 또는 난연재료를 사용한다. · 건축물의 외벽에는 불연재료 또는 준불연재료를 마감재료로 사용한다.
		수해방지	· 주요시설의 천창 및 바닥(주요시설이 지하에 위치한 경우에는 벽을 포함한다)은 수해를 방지하기 위하여 물이 들어갈 수 없도록 시공(방수시공 등) 하여야 한다.
관리적 보호조치	보호관리 체계화	상근경비원	· 24시간 경비업무를 수행하는 상근 경비원을 둔다.
		전문기술자	· 주요시설의 유지관리를 위하여 시스템관리, 네트워크관리, 전기를 각각 담당하는 전문인력(관련분야 2년이상 경력자)을 두되, 해당 인력을 확보하기 어려운 경우에는 외부 전문업체에 해당 업무를 위탁할 수 있다.
		관리책임자	· 집적정보통신시설내의 모든 보호조치를 계획, 감독, 통제하며 비상시 재난관리활동을 수행한다.
		시설보호계획 및 업무연속성계획	· 시설보호계획 및 업무연속성계획을 수립하는 때에는 제6조제1항 및 제2항의 규정에 의한 내용이 포함되도록 한다. · 시설보호계획 및 업무연속성계획을 주된 사업장에 비치하고 교육하는 등 소속 직원이 내용을 숙지할 수 있도록 필요한 조치를 한다. · 업무환경의 변화 등으로 인하여 시설보호계획 및 업무연속성계획의 수정·보완이 필요한 경우에는 지체없이 검토·보완하여야 한다.

정보보호 관리체계 인증 등에 관한 고시

[시행 2016.6.2] [고시 제2016 - 59호, 2016.6.2, 일부개정]

제1장 총 칙

제1조(목적) 이 고시는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) 제47조제3항ㆍ제4항, 같은 법 시행령(이하 "영"이라 한다) 제47조부터 제53조의2까지의 규정 및 같은 법 시행규칙(이하 "규칙"이라 한다) 제3조에 따라 정보보호 관리체계 인증에 관하여 필요한 사항에 대해 정하는 것을 목적으로 한다.

제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "정보보호 관리체계 인증기관(이하 ‘ 인증기관 ’ 이라 한다)"이란 법 제47조제6항에 따라 미래창조과학부가 인증에 관한 업무를 수행할 수 있도록 지정한 기관을 말한다.
2. "정보보호 관리체계 심사기관(이하 ‘ 심사기관 ’ 이라 한다)"이란 법 제47조제7항에 따라 미래창조과학부가 인증심사 업무를 수행할 수 있도록 지정한 기관을 말한다.
3. "업무수행 요건ㆍ능력 심사"란 인증기관 또는 심사기관으로 지정받고자 신청한 법인 또는 단체의 업무수행 요건ㆍ능력을 별표 2의 세부기준에 따라 심사하는 것을 말한다.
4. "인증"이란 신청기관이 수립하여 운영하고 있는 정보보호 관리체계가 별표 7의 정보보호 관리체계 인증기준(이하 "인증기준"이라 한다)에 적합함을 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다) 또는 인증기관이 증명하는 것을 말한다.
5. "인증심사"란 신청기관이 수립하여 운영하는 정보보호 관리체계가 인증기준에 적합한지의 여부를 인터넷진흥원ㆍ인증기관 또는 심사기관이 서면심사 및 현장심사의 방법으로 확인하는 것을 말한다.
6. "정보보호관리과정(이하 ‘ 관리과정 ’ 이라 한다)"이란 정보보호 관리체계를 수립ㆍ운영하기 위하여 유지ㆍ관리하여야 할 과정으로 다음 각 목의 5단계 활동을 말한다.
   가. 정보보호정책 수립 및 범위설정
   나. 경영진 책임 및 조직구성
   다. 위험관리
   라. 정보보호대책 구현
   마. 사후관리

7. "정보보호대책"이란 신청기관이 정보보호 관리체계를 수립·운영하기 위하여 별표 7에서 선택한 통제사항을 말한다.
8. "신청기관"이란 이 고시에 따라 정보보호 관리체계 인증을 취득하고자 신청한 자를 말한다.
9. "인증심사원"이란 별표 3의 자격요건을 갖춘 자를 말한다.
10. "최초심사"란 처음으로 인증을 신청하거나 인증의 범위에 중요한 변경이 있어서 다시 인증을 신청한 때 실시하는 인증심사를 말한다.
11. "사후심사"란 정보보호 관리체계 인증(인증이 갱신된 경우를 포함한다)을 받고난 후 매년 사후관리를 위하여 실시하는 인증심사를 말한다.
12. "갱신심사"란 유효기간 만료로 다시 인증을 신청한 때 실시하는 인증심사를 말한다.

제2장 정보보호 관리체계 인증기관 및 심사기관

제3조(인증기관 및 심사기관의 지정공고 등) ① 미래창조과학부는 법 제47조제6항·제7항 및 영 제53조의2에 따라 인증기관 또는 심사기관을 지정할 필요가 있는 때에는 지정대상 기관의 수, 업무의 범위 및 신청방법 등을 정하여 관보 및 인터넷 홈페이지에 20일 이상 공고하여야 한다.

② 제1항에 따라 인증기관으로 지정받으려는 자는 다음 각 호의 서류를 미래창조과학부에 제출하여야 한다.

1. 별지 1호 서식의 정보보호 관리체계 인증기관 지정 신청서
2. 영 제53조의2제1항제2호에 따른 별지 3호서식의 인증심사원 보유현황과 이를 증명할 수 있는 서류
3. 영 제53조의2제1항제3호에 따른 별표 1의 업무수행 요건·능력 심사를 위하여 필요한 서류

③ 제1항에 따라 심사기관으로 지정받으려는 자는 다음 각 호의 서류를 미래창조과학부에 제출하여야 한다.

1. 별지 2호서식의 정보보호 관리체계 심사기관 지정 신청서
2. 영 제53조의2제1항제2호에 따른 별지 제3호서식의 인증심사원 보유현황과 이를 증명할 수 있는 서류
3. 영 제53조의2제1항제3호에 따른 별표 1의 업무수행 요건·능력 심사를 위하여 필요한 서류

제4조(업무수행 요건·능력 심사 세부기준 등) ① 영 제53조제2항에 따른 업무수행 요건·능력 심사를 위한 세부기준은 별표 2와 같다.

② 미래창조과학부는 제3조제2항에 따라 인증기관 또는 심사기관의 지정 신청을 받은 때에는 제1항에 따라 업무수행 요건·능력을 심사하여 지정 대상기관의 순위를 정한다.

제5조(업무수행 능력의 적합성 인정) ① 미래창조과학부는 제4조제1항에 따라 업무수행 요건·능력을 심사하여 지정에 필요한 수만큼 점수의 합이 높은 순으로 선별한다.
② 미래창조과학부는 제1항에 따라 심사한 결과를 바탕으로 하여 인증기관 또는 심사기관으로의 지정 여부를 최종 결정한다.

제6조(인증기관 및 심사기관의 지정서) ① 영 제53조의2제3항에 따른 정보보호 관리체계 인증기관 지정서는 별지 제4호서식과 같다.
② 영 제53조의2제3항에 따른 정보보호 관리체계 심사기관 지정서는 별지 제5호서식과 같다.

제7조(인증기관 및 심사기관의 사후관리) ① 영 제53조의4제1항에 따른 인증기관의 전년도 인증실적 보고서는 별지 제6호서식과 같다.
② 영 제53조의4제1항에 따른 심사기관의 전년도 인증심사실적 보고서는 별지 제7호서식과 같다.

제8조(인증기관 및 심사기관의 재지정) ① 인증기관은 유효기간이 끝나기 전 6개월부터 끝나는 날까지 별지 제1호서식에 따라 미래창조과학부에 재지정 신청을 할 수 있다.
② 심사기관은 유효기간이 끝나기 전 6개월부터 끝나는 날까지 별지 제2호서식에 따라 미래창조과학부에 재지정 신청을 할 수 있다.
③ 제1항 또는 제2항에 따른 재지정의 심사, 재지정 결과 통지, 재지정서 발급 등에 관하여는 영 제53조의2제3항을 준용한다.

제3장 인증심사원의 자격 및 관리

제9조(인증심사원의 자격 요건 등) ① 인증심사원은 심사원보, 심사원, 선임심사원으로 구분하며, 인증심사원 등급별 자격 요건은 별표 3과 같다.
② 인증심사원이 되려는 자는 별표 3의 학력 및 경력 요건을 갖추고 인터넷진흥원이 지정하는 기관에서 인증심사원 양성교육 과정을 수료하여야 한다.

제10조(인증심사원 자격 신청) 인증심사원의 자격을 신청하고자 하는 자는 제9조제2항에 따라 인증심사원 양성교육 과정을 수료한 날로부터 1개월 이내에 인터넷진흥원에 다음 각 호의 모든 서류를 제출하여야 한다.
1. 별지 제8호서식 정보보호 관리체계 인증심사원 자격 신청서
2. 학위증명서, 자격증 사본(해당 시)
3. 별지 제9호서식 경력증명서
4. 별지 제10호서식 상세 재직증명서 등 경력증빙서류
5. 별지 제11호서식 기술실적증명서(해당 시)

제11조(인증심사원 자격 부여) ① 인터넷진흥원은 인증심사원 자격 신청서를 접수한 때에는 신청서류를 검토하여 서류 보완 및 추가제출을 요청할 수 있다.

② 서류 보완 및 추가제출을 요청받은 자격 신청자는 1개월 이내에 관련 서류 등을 제출하여야 한다.

③ 인터넷진흥원은 인증심사원 자격의 적합 여부를 확인하여 통과한 자에게 별지 제12호서식의 인증심사원 자격 증명서를 발급하여야 한다.

제12조(인증심사원 자격 유지) ① 인증심사원의 자격 유효기간은 자격 부여를 받은 날로부터 3년으로 한다.

② 인증심사원은 자격 유지를 위해 유효기간 내에 인터넷진흥원이 지정하는 기관에서 시행하는 인증심사원 보수교육을 이수해야 한다. 다만, 부득이한 사유로 보수교육을 받지 못한 경우에는 인터넷진흥원이 인정하는 대체교육을 받아야 한다.

③ 보수교육을 이수한 자에 한하여 자격 유효기간이 3년간 연장된다.

제13조(인증심사원 자격 취소) ① 인증심사원 자격 신청 시 제출한 서류가 허위이거나, 제12조에 따른 자격 유지 기준을 충족하지 못한 경우에는 자격을 취소한다.

② 인증심사원으로서 객관적이고 공정한 인증심사를 수행하지 않거나, 인증심사와 관련된 부당한 금전, 금품 등을 수수하거나 인증심사 수행 중 취득한 정보를 누설하는 경우에는 자격을 취소한다.

제4장 인증심사의 신청 및 계약

제14조(인증 의무대상자 범위) ① 인증 의무대상자란 법 제47조제2항, 영 제49조에 따라 정보보호 관리체계 인증을 받아야 하는 자를 말한다.

② 법 제47조제2항제2호에 따라 정보보호 관리체계 인증을 받아야 하는 자 중 집적정보통신시설 사업자가 마련한 시설의 일부를 임대하여 집적정보통신시설 사업을 하는 자에 대하여는 영 제49조제2항의 기준을 준용한다.

③ 인증 의무대상자는 매년 1월1일부터 12월31일까지 인증을 받아야 한다.

제15조(신청기관의 사전 준비사항) 신청기관은 정보보호 관리체계 인증을 신청하기 전에 인증기준에 따른 정보보호 관리체계를 구축하여 최소 2개월 이상 운영하여야 한다.

제16조(인증의 신청 등) ① 법 제47조제1항 또는 제2항에 따라 정보보호 관리체계 인증을 받으려는 자는 별지 제13호서식의 정보보호 관리체계 인증 신청서를 인터넷진흥원·인증기관 또는 심사기관에 제출하여야 한다.

② 신청기관은 인증의 범위 및 일정 등을 인터넷진흥원·인증기관 또는 심사기관과 사전 협의하여 신청하여야 한다.

③ 인터넷진흥원·인증기관 또는 심사기관은 제14조에 따른 인증 의무대상자가 사업자 등록일이 속한 분기가 끝나는 날의 1개월 전까지 인증 신청을 한 경우 인증심사를 우선적으로 처리할 수 있다.

제17조(인증심사의 일부 생략 신청 등) ① 규칙 제3조에 따른 인증을 받았거나 정보보호 조치를 취한 자가 정보보호 관리체계 인증심사의 일부 생략을 신청하는 경우 인터넷진흥원·인증기관 또는 심사기관은 별표 4의 범위 내에서 정보보호 관리체계 인증심사를 생략할 수 있다. 다만, 인증 또는 정보보호 조치의 항목이 별표 7의 항목과 동일하다는 것을 증명하는 서류를 별도로 제출하는 경우에는 별표 4의 범위 외의 항목에 대해서도 정보보호 관리체계 인증심사를 생략할 수 있다.

② 제1항 단서에 따라 신청자가 별도로 제출한 인증 또는 정보보호 조치 항목에 대한 인증심사 생략 여부는 제22조에 따른 인증위원회 심의, 인터넷진흥원과 인증기관간의 협의, 미래창조과학부 장관의 승인을 거쳐 확정하고, 미래창조과학부, 인터넷진흥원·인증기관 및 심사기관 홈페이지에 게시한다.

제18조(인증심사 계약 체결) 신청기관은 인터넷진흥원·인증기관 또는 심사기관과 협의한 후 심사기간, 심사인원, 인증 수수료, 인증의 범위 등을 포함하는 인증심사 계약을 체결한다.

제5장 인증심사의 기준과 방법

제19조(인증기준) 인증기준은 별표 7과 같다.

제20조(인증심사팀 구성) ① 인터넷진흥원·인증기관 또는 심사기관은 제18조에 따른 인증심사 계약을 체결한 때에는 지체 없이 인증심사원으로 인증심사팀을 구성하여야 한다.

② 인증심사팀 구성 시 심사팀장은 인터넷진흥원·인증기관 또는 심사기관 소속의 심사원 이상으로 선정하여야 한다.

③ 신청기관의 정보보호 관리체계 인증을 위한 컨설팅에 참여한 인증심사원 또는 신청기관의 소속직원은 인증심사팀의 구성원에서 배제하여야 한다.

제21조(인증심사 방법 및 보완조치) ① 인증심사는 신청기관을 방문하여 서면심사와 현장심사를 병행한다.

② 서면심사는 인증기준에 적합한지에 대하여 정보보호 관리체계 구축·운영 관련 정보보호 정책, 지침, 절차 및 이행의 증적자료 검토, 정보보호대책 적용 여부 확인 등의 방법으로 관리적 요소를 심사한다.

③ 현장심사는 서면심사의 결과와 기술적·물리적 보호대책 이행 여부를 확인하기 위하여 담당자 면담, 관련 시스템 확인 및 취약점 점검 등의 방법으로 기술적 요소를 심사한다.

④ 인터넷진흥원·인증기관 또는 심사기관은 인증심사에서 발견된 결함에 대해 최대 90일(재조치 요구 60일 포함) 이내에 보완조치를 완료하도록 신청기관에게 요청할 수 있다.

⑤ 인터넷진흥원 또는 인증기관은 인증위원회 심의결과에 따라 신청기관에 30일 이내에 보완조치를 요구할 수 있다. 심사기관은 인터넷진흥원 또는 인증기관으로부터 인증위원회 심의결과를 통보받아 신청기관에 30일 이내에 보완조치를 요구할 수 있다.

제6장 인증위원회 구성과 운영

제22조(인증위원회의 구성) ① 법 제47조제6항에 따라 인터넷진흥원 또는 인증기관의 장은 다음 각 호의 사항을 심의·의결하기 위하여 인증위원회를 설치·운영하여야 한다.

1. 최초심사 또는 갱신심사 결과가 인증기준에 적합한지 여부
2. 사후심사 결과 법 제47조제10항 각 호에 해당하는 사유를 발견한 경우에 그 결과의 적합성 여부
3. 그 밖에 정보보호 관리체계 인증과 관련하여 위원장이 필요하다고 인정하는 사항

② 인증위원회는 5인 이상 10인 이내의 위원으로 구성하되, 위원은 정보보호 전문가, 정보시스템감리사, 기술사, 교수 등 정보보호 분야에 학식과 경험이 있는 자 중에서 인터넷진흥원 또는 인증기관의 장이 위촉하며, 위원장은 위원 중에서 호선한다.

③ 위원장은 인증위원회의 업무를 통할하며 위원회를 대표한다.

제23조(인증위원회의 운영) ① 인터넷진흥원 또는 인증기관의 장은 인증위원회의 심의안건을 검토하여 위원회 개최 5일 전까지 인증위원회에 제출한다.

② 인증위원회 위원장은 제22조제1항 각 호의 사항에 대한 심의·의결 결과를 인터넷진흥원 또는 인증기관의 장에게 제출한다.

제7장 인증서의 발급·관리 및 홍보

제24조(인증서 발급) 인터넷진흥원 또는 인증기관의 장은 제23조제2항에 따라 인증위원회의 심의·의결 결과를 제출받은 때에는 신청기관의 정보보호 관리체계가 이 고시에서 정한 인증기준에 적합하다고 판단된 경우 별지 제14호서식의 정보보호 관리체계 인증서를 발급하여야 한다.

제25조(인증서 관리) ① 인터넷진흥원 또는 인증기관은 발급된 인증서의 인증번호, 발급일, 유효기간 등 인증서를 관리하여야 한다.

② 인증을 취득한 자는 인증서의 분실 등으로 인해 재발급을 받고자 할 경우 별지 제15호서식의 정보보호 관리체계 인증서 추가발급 신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

③ 인증을 취득한 자가 주소, 업체명 등 인증서 기재사항의 변경을 요청하고자 하는 경우 별지 제16호서식의 정보보호 관리체계 인증서 변경신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

제26조(인증의 표시 및 홍보) ① 영 제52조에 따른 인증의 표시는 별표 5와 같다.

② 제1항에 따른 인증의 표시를 사용하는 경우에는 영 제52조에 따라 인증의 범위와 유효기간을 함께 표시하여야 한다.

제8장 정보보호 관리체계 인증 수수료

제27조(수수료의 산정) ① 인증 수수료는 다음 각 호의 기준을 준용하되 별표 6의 정보보호 관리체계 인증 수수료 산정기준을 적용하여 산정한다.

1. 「엔지니어링산업 진흥법」 제31조제2항에 따른 엔지니어링사업의 대가 기준
2. 한국소프트웨어산업협회가 제공하는 「SW사업 대가산정 가이드」의 정보보안 컨설팅비

② 인터넷진흥원·인증기관 또는 심사기관은 제1항에 따라 산정된 인증 수수료를 공지하여야 한다. 다만, 「중소기업기본법」 제2조에 따른 중소기업이 인증을 신청하는 경우 수수료 감면 등 필요한 지원을 할 수 있다.

③ 인터넷진흥원·인증기관 또는 심사기관은 신청기관의 인증범위가 정보보호 관련 타 인증과 중복되거나 제17조에 따른 인증심사 일부를 생략하는 경우 신청기관과 협의하여 수수료를 조정할 수 있다.

제28조(수수료의 납부) ① 신청기관은 최초심사, 사후심사 및 갱신심사 신청 시 수수료를 납부한다. 다만, 수수료 납부 방법(일괄 또는 분할)은 인증심사 계약 시 신청기관과 협의하여 조정할 수 있다.

② 신청기관은 인증심사 계약을 체결한 날로부터 1개월 이내에 인증 수수료를 인터넷진흥원·인증기관 또는 심사기관에 납부하여야 한다.

제29조(인증업무 지침 등) ① 인터넷진흥원 또는 인증기관은 인증업무 수행을 위해 필요한 경우 인증업무에 관한 지침을 마련하여 시행할 수 있다.

② 심사기관은 인증심사업무 수행에 필요한 지침을 마련하여 시행할 수 있다.

제30조(재검토기한) 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제334호)에 따라 이 고시에 대하여 2017년 1월 1일 기준으로 매 3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2013-4호,2013.1.17>

제1조(시행일) 이 고시는 2013년 2월 18일부터 시행한다.

제2조(인증심사원에 관한 경과조치) 이 고시 시행 이전에 종전 고시에 따라 인증 심사업무를 전담하는 직원의 요건을 갖추고 인터넷진흥원으로부터 위촉된 자는 이 고시에 의한 인증심사원 자격을 취득한 것으로 본다.

부칙 <제2013-36호,2013.8.8>

제1조(시행일) 이 고시는 2013년 8월 8일부터 시행한다.

부칙 <제2016 - 38호,2016.4.8>

제1조(시행일) 이 고시는 공포한 날부터 시행한다.

부칙 <제2016 - 59호,2016.6.2>

제1조(시행일) 이 고시는 공포한 날부터 시행한다.

[별표 1]

업무수행 요건·능력 심사 규정에 따른 제출서류(제3조제2항·제3항 관련)

구 분	제 출 서 류
1. 정보보호 관리체계 인증심사 참여 실적을 확인하는 데 필요한 서류	가. 정보보호 관리체계 인증심사 참여실적 명세서 및 이를 증빙할 수 있는 자료 (인증심사 참여통지 문서 등) 나. 인증심사원 자격 증빙 자료
2. 업무수행 요건·능력 심사를 위하여 필요한 서류	가. 자본금 5억원 이상 내역(공인회계사 또는 회계담당자가 서명날인한 서류) 나. 부채비율 및 자기자본 이익률의 계산내역(회계결산내역 등 관련 증빙자료) 다. 인증업무 운영체계(인증기관에 해당) o 인증기관의 운영체계 및 인증의 품질관리 o 인증업무를 수행하는 직원에 대한 운영관리 등의 내부 규정 o 인증업무 수행 방법 및 절차 라. 심사업무 운영체계(심사기관에 해당) o 심사기관의 운영 체계 및 심사의 품질관리 o 심사업무를 수행하는 직원에 대한 운영관리 등의 내부 규정 o 심사업무 수행 방법 및 절차

[별표 2]

업무수행 요건·능력 심사 세부기준(제4조제1항 관련)

가. 업무수행 요건 심사 세부기준

평가항목	세부 평가 기준
1. 인증심사원 5명 이상 상시 고용 여부	o 인증심사원 5명 이상을 상시 고용하고 있어야 함 - 다만, 심사팀장급 심사원 1명 이상 확보해야 함
2. 인증기관 또는 심사기관 공정성 확보 여부	o 정보보호 관리체계 인증기관 또는 심사기관으로 지정을 받으려는 기관은 인증업무 또는 심사업무의 독립성, 객관성, 공정성, 신뢰성을 확보하기 위하여 정보보호 관리체계 구축과 관련된 컨설팅 업무를 수행하지 않아야 함

나. 인증기관 업무수행 능력 심사 세부기준

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td rowspan="5">1. 조직 및 직원들의 정보보호 전문성 (30)</td><td>전담조직</td><td>2</td><td>평가점수</td><td>o 인증에 관한 업무 전담조직 유무
<table><tr><th>전담조직 유무</th><th>점수</th></tr><tr><td>있음</td><td>2점</td></tr><tr><td>없음</td><td>0점</td></tr></table></td></tr>
<tr><td rowspan="4">정보보호 업무 전문성</td><td>10</td><td>평가점수</td><td>o 조직 내 인증심사원 상시 고용 인력 수
<table><tr><th>인증심사원 수</th><th>점수</th></tr><tr><td>10명 이상</td><td>배점의 100%</td></tr><tr><td>5명 이상 ~ 10명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (인증심사원 수/10명) × 100</td></tr></table></td></tr>
<tr><td>4</td><td>비율</td><td>o 정보보호 관련 박사학위 소지자·기술사 인력의 수
<table><tr><th>박사학위소지자기술사 수</th><th>점수</th></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (박사학위 소지자, 기술사 수/5명) × 100</td></tr></table></td></tr>
<tr><td>4</td><td>비율</td><td>o CISM, SIS, CISSP, CISA, CPPG, 정보보안기사/산업기사 자격증 소지자 수
<table><tr><th>자격증 소지자·수</th><th>점수</th></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (자격증 소지자 수/5명) × 100</td></tr></table></td></tr>
<tr><td>정보보호 관리체계 인증심사 참여실적</td><td>10</td><td>비율</td><td>o 상시 고용하고 있는 인증심사원이 최근 3년간 참여한 정보보호 관리체계 인증심사 참여 실적을 인정하고 평가점수는 개별 참여 실적을 합한 총 참여일수에 따라 산출
<table><tr><th>총 참여 일수(단위 : 일)</th><th>점수</th></tr><tr><td>200일 이상</td><td>배점의 100%</td></tr><tr><td>200일 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (총 참여일수/200일) × 100</td></tr></table></td></tr>
</table>

<table>
<tr><td>2. 시설(10)</td><td>사무공간·인증심사 서류 보관 창소 및 보안설비·시설 확보</td><td>10</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 인증심사의 상담, 인증심사 업무의 처리를 위해 필요한 사무실</td><td>2점</td></tr>
<tr><td>o 사무 관련 장비 확보</td><td>2점</td></tr>
<tr><td>o 사무실 출입자에 대한 신원확인 및 출입통제를 위한 설비</td><td>2점</td></tr>
<tr><td>o 기록물 및 자료의 안전한 관리를 위한 보관 창소</td><td>2점</td></tr>
<tr><td>o 인증심사 서류의 분실, 도난 등 예방을 위한 보안시설</td><td>2점</td></tr>
</table>
</td></tr>
<tr><td rowspan="2">3. 신뢰도 및 재정상태 건실도 (10)

※비영리기관 평가제외</td><td>부채비율</td><td>5</td><td>평가점수</td><td>o 지정 공고일 기준으로 직전년도 부채비율 (부채총계/자기자본)
<table>
<tr><th>비율</th><th>점수</th></tr>
<tr><td>50% 미만</td><td>5점</td></tr>
<tr><td>50% 이상 ~ 100% 미만</td><td>4점</td></tr>
<tr><td>100% 이상 ~ 150% 미만</td><td>3점</td></tr>
<tr><td>150% 이상 ~ 200% 미만</td><td>2점</td></tr>
<tr><td>200% 이상</td><td>1점</td></tr>
</table>
</td></tr>
<tr><td>자기자본 이익률</td><td>5</td><td>평가점수</td><td>o 지정 공고일 기준으로 직전년도 자기자본이익률 (당기순이익/자기자본)
<table>
<tr><th>비율</th><th>점수</th></tr>
<tr><td>20% 이상</td><td>5점</td></tr>
<tr><td>20% 미만 ~ 15% 이상</td><td>4점</td></tr>
<tr><td>15% 미만 ~ 10% 이상</td><td>3점</td></tr>
<tr><td>10% 미만 ~ 5% 이상</td><td>2점</td></tr>
<tr><td>5% 미만</td><td>1점</td></tr>
</table>
</td></tr>
<tr><td rowspan="3">4. 인증업무 운영 체계 (50)</td><td>인증기관의 운영 체계 및 인증의 품질관리</td><td>20</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 인증기관의 공정성·객관성·신뢰성·독립성 보증 방안</td><td>5점</td></tr>
<tr><td>o 인증기관의 내부감사 실시 및 검토 등에 대한 방안</td><td>5점</td></tr>
<tr><td>o 인증의 품질 보증 및 관리방안</td><td>5점</td></tr>
<tr><td>o 인증업무의 기록 및 문서화 관리체계의 적절성</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td>인증업무를 수행하는 직원에 대한 운영·관리 등의 내부 규정</td><td>10</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 인증업무를 수행하는 직원에 대한 규정 보유 및 그 규정의 타당성 및 실효성
- 인증업무를 수행하는 직원의 의무와 책임 등 준수사항
- 인증업무를 수행하는 직원의 자체 보안관리 및 감독 요령</td><td>5점</td></tr>
<tr><td>o 인증업무를 수행하는 직원의 교육 및 평가 등에 대한 방안 및 그 방안의 적절성 및 타당성</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td>인증업무 수행 방법 및 절차</td><td>10</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 심사업무 수행 방법 및 절차 등의 적절성 및 타당성</td><td>5점</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td></td><td>
<table>
<tr><td>- 인증심사의 절차 및 방법
- 인증수수료 및 그 징수방법
- 인증심사팀 구성 원칙
- 인증심사 사후관리방안 등</td><td></td></tr>
<tr><td>o 인증위원회 구성 및 운영
- 인증심사 결과의 공정성 확보를 위한 인증위원 구성 원칙
- 인증위원회 운영의 독립성·객관성이 확보 방안</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td></td><td>인증업무
지원체계</td><td>10</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 운영자금 법인통장 보유 및 유지 수준</td><td>5점</td></tr>
<tr><td>o 지정취소, 부도·해산 등에 따른 신청기관 피해 보상 관련 대책마련 여부</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td>5. 가점 및 감점</td><td>정보보호
관리체계
인증의 취득 및 유지</td><td>2
(가점)</td><td>인증
취득 및
유지</td><td>o 정보보호 관리체계 인증을 취득하고, 인증을 유지하고 있을 때</td></tr>
<tr><td></td><td>자격취소 사실</td><td>5
(감점)</td><td>취소사실
및
취소회수</td><td>o 지정 공고일 기준으로 10년 이내에 미래창조과학부가 부여한 정보보호 관련 수행자격이 취소된 경우
- 정보보호 관리체계 인증기관, 안전진단 수행기관 등
※ 취소 1회당 : 감점 5점</td></tr>
</table>

<비 고>

1. 평가항목에 대한 각 평가요소별 세부평가 점수는 소수점 이하 둘째 자리에서 반올림한다.
2. 평가항목에 대한 각 평가요소별 평가점수는 평가결과의 최저점과 최고점을 제외한 점수들의 평균점을 부여한다. 다만, 최저점 또는 최고점이 2개 이상일 경우 각 1개만 제외한다.
3. 가점을 합한 점수가 100점을 초과해도 만점 100점으로 표기한다.
4. '시설', '인증업무 운영체계'에 대한 각 평가요소별 세부평가 점수 부여기준은 각 평가요소의 평가결과에 평가등급(계수)를 곱하여 나온 점수를 합산한다.

평가요소별 세부평가 점수	평가등급(계수)
100점 이하 ~ 90점 이상	우수(1.0)
90점 미만 ~ 80점 이상	보통(0.6)
80점 미만 ~	미흡(0.2)
미 제출	점수없음(0)

다. 심사기관 업무수행 능력심사 세부기준

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td rowspan="5">1. 조직 및 직원들의 정보보호 전문성 (30)</td><td>전담조직</td><td>2</td><td>평가점수</td><td>o 심사업무 전담조직 유무
<table><tr><th>전담조직 유무</th><th>점수</th></tr><tr><td>있음</td><td>2점</td></tr><tr><td>없음</td><td>0점</td></tr></table></td></tr>
<tr><td rowspan="3">정보보호 업무 전문성</td><td>10</td><td>평가점수</td><td>o 조직 내 인증심사원 상시 고용 인력 수
<table><tr><th>인증심사원 수</th><th>점수</th></tr><tr><td>10명 이상</td><td>배점의 100%</td></tr><tr><td>5명 이상 ~ 10명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (인증심사원 수/10명) × 100</td></tr></table></td></tr>
<tr><td>4</td><td>비율</td><td>o 정보보호 관련 박사학위 소지자 · 기술사 인력의 수
<table><tr><th>박사학위소지자·기술사 수</th><th>점수</th></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (박사학위 소지자, 기술사 수/5명) × 100</td></tr></table></td></tr>
<tr><td>4</td><td>비율</td><td>o CISM, SIS, CISSP, CISA, CPPG, 정보보안기사/산업기사 자격증 소지자 수
<table><tr><th>자격증 소지자 수</th><th>점수</th></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (자격증 소지자 수/5명) × 100</td></tr></table></td></tr>
<tr><td>정보보호 관리체계 인증심사 참여실적</td><td>10</td><td>비율</td><td>o 상시 고용하고 있는 인증심사원이 최근 3년간 참여한 정보보호 관리체계 인증심사 참여 실적을 인정하고 평가점수는 개별 참여 실적을 합한 총 참여일수에 따라 산출
<table><tr><th>총 참여 일수(단위 : 일)</th><th>점수</th></tr><tr><td>200일 이상</td><td>배점의 100%</td></tr><tr><td>200일 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (총 참여일수/200일) × 100</td></tr></table></td></tr>
<tr><td>2. 시설(10)</td><td>사무공간·인증심사 서류 보관 창소 및 보안설비·시설 확보</td><td>10</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 인증심사의 상담, 인증심사 업무의 처리를 위해 필요한 사무실</td><td>2점</td></tr><tr><td>o 사무 관련 장비 확보</td><td>2점</td></tr><tr><td>o 사무실 출입자에 대한 신원확인 및 출입통제를 위한 설비</td><td>2점</td></tr><tr><td>o 기록물 및 자료의 안전한 관리를 위한 보관 창소</td><td>2점</td></tr><tr><td>o 인증심사 서류의 분실, 도난 등 예방을 위한 보안시설</td><td>2점</td></tr></table></td></tr>
<tr><td>3. 신뢰도 및 재정상태 건실도 (10)</td><td>부채비율</td><td>5</td><td>평가점수</td><td>o 지정 공고일 기준으로 직전년도 부채비율
(부채총계/자기자본)</td></tr>
</table>

<table>
<tr><td>※비영리기관
평가제외</td><td></td><td></td><td></td><td><table><tr><th>비율</th><th>첨수</th></tr><tr><td>50% 미만</td><td>5점</td></tr><tr><td>50% 이상 ~ 100% 미만</td><td>4점</td></tr><tr><td>100% 이상 ~ 150% 미만</td><td>3점</td></tr><tr><td>150% 이상 ~ 200% 미만</td><td>2점</td></tr><tr><td>200% 이상</td><td>1점</td></tr></table></td></tr>
<tr><td></td><td>자기자본
이익률</td><td>5</td><td>평가점수</td><td>o 지정 공고일 기준으로 직전년도 자기자본이익률
(당기순이익/자기자본)<table><tr><th>비율</th><th>첨수</th></tr><tr><td>20% 이상</td><td>5점</td></tr><tr><td>20% 미만 ~ 15% 이상</td><td>4점</td></tr><tr><td>15% 미만 ~ 10% 이상</td><td>3점</td></tr><tr><td>10% 미만 ~ 5% 이상</td><td>2점</td></tr><tr><td>5% 미만</td><td>1점</td></tr></table></td></tr>
<tr><td>4. 심사업무
운영 체계
(50)</td><td>심사기관의
운영 체계 및
심사의
품질관리</td><td>20</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>첨수</th></tr><tr><td>o 심사기관의 공정성과 독립성 보증 방안</td><td>5점</td></tr><tr><td>o 심사기관의 내부감사 실시 및 검토 등에 대한 방안</td><td>5점</td></tr><tr><td>o 심사의 품질 보증 및 관리방안</td><td>5점</td></tr><tr><td>o 심사업무의 기록 및 문서화 관리체계의 적절성</td><td>5점</td></tr></table></td></tr>
<tr><td></td><td>심사업무를
수행하는
직원에 대한
운영관리
등의 내부
규정</td><td>10</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>첨수</th></tr><tr><td>o 심사업무를 수행하는 직원에 대한 규정 보유 및 그 규정의 타당성 및 실효성
- 심사업무를 수행하는 직원의 의무와 책임 등 준수사항
- 심사업무를 수행하는 직원의 자체 보안관리 및 감독 요령</td><td>5점</td></tr><tr><td>o 심사업무를 수행하는 직원의 교육 및 평가 등에 대한 방안 및 그 방안의 적절성 및 타당성</td><td>5점</td></tr></table></td></tr>
<tr><td></td><td>심사업무
수행 방법 및
절차</td><td>10</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>첨수</th></tr><tr><td>o 심사업무 수행 방법 및 절차 등의 적절성 및 타당성
- 인증심사의 절차 및 방법
- 인증수수료 및 그 징수방법
- 인증심사팀 구성 원칙
- 인증심사 사후관리방안 등</td><td>10점</td></tr></table></td></tr>
<tr><td></td><td>심사업무
지원체계</td><td>10</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>첨수</th></tr><tr><td>o 운영자금 법인통장 보유 및 유지 수준</td><td>5점</td></tr><tr><td>o 지정취소, 부도·해산 등에 따른 신청기관 피해보상 관련 대책마련 여부</td><td>5점</td></tr></table></td></tr>
<tr><td>5. 가점 및 감점</td><td>정보보호
관리체계
인증의 취득
및 유지</td><td>2
(가점)</td><td>인증
취득 및
유지</td><td>o 정보보호 관리체계 인증을 취득하고, 인증을 유지하고 있을 때</td></tr>
<tr><td></td><td>자격취소 사실</td><td>5
(감점)</td><td>취소사실
및
취소회수</td><td>o 지정 공고일 기준으로 10년 이내에 미래창조과학부가 부여한 정보보호 관련 수행자격이 취소된 경우
- 정보보호 관리체계 인증기관, 안전진단 수행기관 등
※ 취소 1회당 : 감점 5점</td></tr>
</table>

<비 고>

1. 평가항목에 대한 각 평가요소별 세부평가 점수는 소수점 이하 둘째 자리에서 반올림한다.
2. 평가항목에 대한 각 평가요소별 평가점수는 평가결과의 최저점과 최고점을 제외한 점수들의 평균점을 부여한다. 다만, 최저점 또는 최고점이 2개 이상일 경우 각 1개만 제외한다.

3. 가점을 합한 점수가 100점을 초과해도 만점 100점으로 표기한다.
4. '시설', '심사업무 운영체계'에 대한 각 평가요소별 세부평가 점수 부여기준은 각 평가요소의 평가결과에 평가등급(계수)를 곱하여 나온 점수를 합산한다.

평가요소별 세부평가 점수	평가등급(계수)
100점 이하 ~ 90점 이상	우수(1.0)
90점 미만 ~ 80점 이상	보통(0.6)
80점 미만 ~	미흡(0.2)
미 제출	점수없음(0)

[별표 3]

인증심사원 자격 요건(제9조 관련)

1. 인증심사원 등급별 자격 요건

구 분	자격 요건
심사원보	o 인증심사원 학력 및 경력요건을 만족하는 자로서 인터넷진흥원이 지정하는 기관에서 인증심사원 양성교육 과정을 수료한 자
심사원	o 심사원보 자격 취득자로서 인증심사 4회 이상 참여하고 심사일수의 합이 20일 이상인 자
선임심사원	o 심사원 자격 취득자로서 3회 이상 심사 총괄업무를 수행하고 심사일수의 합이 15일 이상인 자

2. 인증심사원 학력 및 경력 요건

o 학사학위를 취득한 후 정보통신 또는 정보보호 유관경력 6년(전문학사의 경우 8년, 수업연한이 3년인 전문학사의 경우 7년, 고등학교 졸업자의 경우 10년을 말한다) 이상을 보유한 자(최근 10년 이내의 경력에 한함)

o 유관자격 소지자 또는 유관학력을 취득한 자로서 다음 각 목의 어느 하나에 해당하는 경우 정보통신 유관경력을 인정한다.
가. 기술사 자격 소지자 또는 박사 학위를 취득한 자의 경우 3년
나. 기사 자격 소지자 또는 석사 학위를 취득한 자의 경우 2년
다. 산업기사 자격 소지자 또는 학사 학위를 취득한 자의 경우 1년

o 다음 각 목의 어느 하나에 해당하는 자격을 취득한 자는 정보통신 또는 정보보호 유관경력 1년을 추가 인정한다.
가. 한국인터넷진흥원 정보보호전문가(SIS)
나. 전자정부법 제60조에 따른 감리원
다. 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 정보시스템감사사(CISA)
라. 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 정보시스템보호전문가(CISSP)

<비 고>
1. "정보통신 유관경력", "정보보호 유관경력", "유관자격" 및 "유관학력"은 영 별표 2 "정보보호 기술인력의 자격 기준"을 준용한다.

[별표 4]

정보보호 관리체계 인증심사 일부 생략의 범위(제17조 관련)

<table>
<tr><th>인증 또는 정보보호 조치</th><th>정보보호 관리체계 인증심사 생략범위</th></tr>
<tr><td>국제표준 정보보호경영시스템 인증</td><td>나. 정보보호대책
<table>
<tr><td>1.1 정책의 승인 및 공표</td><td>1.3 정책의 유지관리</td></tr>
<tr><td>2.2 역할 및 책임</td><td>3.1 보안 요구사항의 정의</td></tr>
<tr><td>3.2 외부자 보안 이행</td><td>4.1 정보자산 식별 및 책임</td></tr>
<tr><td>4.2 정보자산의 분류 및 취급</td><td>5.1 교육 프로그램 수립</td></tr>
<tr><td>6.1 정보보호 책임</td><td>6.2 인사규정</td></tr>
<tr><td>7.1 물리적 보호구역</td><td>7.2 시스템 보호</td></tr>
<tr><td>7.3 사무실 환경보안</td><td>8.1 분석 및 설계 보안관리</td></tr>
<tr><td>8.3 외부개발 보안</td><td>9.1 암호정책</td></tr>
<tr><td>9.2 암호키 관리</td><td>10.1 접근통제 정책</td></tr>
<tr><td>11.4 매체보안</td><td>11.6 로그관리 및 모니터링</td></tr>
<tr><td>12.1 절차 및 체계</td><td>12.2 대응 및 복구</td></tr>
<tr><td>13.1 체계구축</td><td>13.2 대책구현</td></tr>
</table></td></tr>
<tr><td>개인정보보호 관리체계 인증</td><td>나. 정보보호대책
<table>
<tr><td>1.1 정책의 승인 및 공표</td><td>1.3 정책의 유지관리</td></tr>
<tr><td>2.1 조직체계</td><td>2.2 역할 및 책임</td></tr>
<tr><td>5.1 교육프로그램 수립</td><td>5.2 교육시행 및 평가</td></tr>
<tr><td>6.1 정보보호 책임</td><td>7.1 물리적 보호구역</td></tr>
<tr><td>7.2 시스템 보호</td><td>7.3 사무실 환경보안</td></tr>
<tr><td>9.1 암호정책</td><td>9.2 암호키 관리</td></tr>
<tr><td>10.1 접근통제 정책</td><td>11.1 운영절차 및 변경관리</td></tr>
<tr><td>11.4 매체관리</td><td>11.6 로그관리 및 모니터링</td></tr>
<tr><td>12.1 절차 및 체계</td><td>12.2 대응 및 복구</td></tr>
</table></td></tr>
<tr><td>「정보통신기반 보호법」 제9조에 따른 취약점의 분석·평가</td><td>나. 정보보호대책
<table>
<tr><td>1.3 정책의 유지관리</td><td>2.1 조직체계</td></tr>
<tr><td>3.1 보안요구사항의 정의</td><td>3.2 외부자보안 이행</td></tr>
<tr><td>4.1 정보자산식별 및 책임</td><td>4.2 정보자산의 분류 및 취급</td></tr>
<tr><td>5.1 교육프로그램 수립</td><td>6.1 정보보호 책임</td></tr>
<tr><td>7.1 물리적 보호구역</td><td>7.2 시스템 보호</td></tr>
<tr><td>8.2 구현 및 이관보안</td><td>10.1 접근통제 정책</td></tr>
<tr><td>10.3 식별 및 인증</td><td>12.1 절차 및 체계</td></tr>
</table></td></tr>
</table>

[별표 5]

정보보호 관리체계 인증의 표시(제26조 관련)

□ 출입구 부착용

1. 도안모형



2. 인증명판 제작 유의사항

가. 소재는 가급적 동판으로 제작한다(전체 두께 1.0㎝, 바탕 0.4㎝, 테두리 폭 0.5㎝)

나. 바탕색은 가급적 연마하지 않은 황동색으로 한다

다. 도안 모형은 인증의 표시를 중앙에 둔다

라. 글씨 및 도형은 양각으로 한다.

마. 크기는 사각형으로 하며 인증마크는 중앙에 위치하도록 하며 가로와 세로 비율을 3 : 2로 하여 일정 비율로 조정할 수 있다

□ 서류 등 표시용

1. 도안모형



2. 도안 및 표시방법

가. 'Information Security Management System'은 검청색으로, '정보보호 관리체계 인증'은 군청색으로 한다. 게시장소의 칼라표시가 불합리한 경우에는 흑백으로 할 수 있다.

나. 마크의 크기는 제품과 그 제품의 포장 또는 용기의 크기에 따라 일정 비율로 조정할 수 있다.

[별표 6]

정보보호 관리체계 인증 수수료 산정기준(제27조 관련)

1. 인증 수수료 산정 방식

인증 수수료 = 직접인건비 + 직접경비 + 제경비 + 기술료

① 직접인건비는 인증심사에 투입되는 인증심사원에 대한 인건비로 산정한다. 인건비는 SW사업 대가 산정 가이드의 정보보안 컨설팅비를 준용한다

인증심사원 등급	컨설턴트 등급
선임심사원	선임 컨설턴트 이상
심사원	
심사원보	컨설턴트

② 직접경비는 인증심사업무의 수행에 따라 발생하는 교통비, 숙박비 및 식대 등 인증심사업무에 소요되는 직접적인 경비를 산정한다.

③ 제경비는 최대 (직접인건비×120%) 로 산정한다.

④ 기술료는 최대 {(직접인건비+제경비)×40% } 로 산정한다.

[별표 7]

정보보호 관리체계 인증기준(제19조 관련)

가. 정보보호관리과정

	관리과정		세부관리과정	관리과정 상세내용
1	정보보호정책 수립 및 범위설정	1.1	정보보호정책의 수립	조직이 수행하는 모든 정보보호 활동의 근거를 포함할 수 있도록 정보보호정책을 수립하고 동 정책은 국가나 관련 산업에서 정하는 정보보호 관련 법, 규제를 만족하여야 한다.
		1.2	범위설정	조직에 미치는 영향을 고려하여 중요한 업무, 서비스, 조직, 자산 등을 포함할 수 있도록 정보보호 관리체계 범위를 설정하고 범위 내 모든 자산을 식별하여 문서화하여야 한다.
2	경영진 책임 및 조직구성	2.1	경영진 참여	정보보호 관리체계 수립 및 운영 등 조직이 수행하는 정보보호 활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여야 한다.
		2.2	정보보호 조직 구성 및 자원 할당	최고경영자는 조직의 규모, 업무 중요도 분석을 통해 정보보호 관리체계의 지속적인 운영이 가능하도록 정보보호 최고책임자, 실무조직 등 정보보호 조직을 구성하고 정보보호 관리체계 운영 활동을 수행하는데 필요한 자원(예산 및 인력)을 확보하여야 한다.
3	위험관리	3.1	위험관리 방법 및 계획 수립	관리적, 기술적, 물리적, 법적 분야 등 조직의 정보보호 전 영역에 대한 위험식별 및 평가가 가능하도록 위험관리 방법을 선정하고 위험관리의 전문성을 보장할 수 있도록 수행인원, 기간, 대상, 방법 등을 구체적으로 포함한 위험관리계획을 사전에 수립하여야 한다.
		3.2	위험식별 및 평가	위험관리 방법 및 계획에 따라 정보보호 전 영역에 대한 위험 식별 및 평가를 연 1회 이상 수행하고 그 결과에 따라 조직에서 수용 가능한 위험수준을 설정하여 관리하여야 한다.

	관리과정		세부관리과정	관리과정 상세내용
3	위험관리	3.3	정보보호대책 선정 및 이행계획 수립	위험을 수용 가능한 수준으로 감소시키기 위해 정보보호대책을 선정하고 그 보호대책의 구현 우선순위, 일정, 담당부서 및 담당자 지정, 예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.
4	정보보호대책 구현	4.1	정보보호대책의 효과적 구현	정보보호대책 이행계획에 따라 보호대책을 구현하고 경영진은 이행결과의 정확성 및 효과성 여부를 확인하여야 한다.
		4.2	내부 공유 및 교육	구현된 정보보호대책을 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여야 한다.
5	사후관리	5.1	법적요구사항 준수검토	조직이 준수해야 할 정보보호 관련 법적요구사항을 지속적으로 파악하여 최신성을 유지하고 준수여부를 지속적으로 검토하여야 한다.
		5.2	정보보호 관리체계 운영현황 관리	정보보호 관리체계 범위 내에서 주기적 또는 상시적으로 수행해야 하는 활동을 문서화하고 그 운영현황을 지속적으로 관리하여야 한다.
		5.3	내부감사	조직은 정보보호 관리체계가 정해진 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는 지를 점검하기 위하여 연 1회 이상 내부감사를 수행하여야 한다. 이를 위해 감사기준, 범위, 주기, 방법 등을 구체적으로 정하고 내부감사를 통해 발견된 문제점은 보완조치를 완료하여 경영진 및 관련 책임자에게 보고하여야 한다. 또한 감사의 독립성 및 전문성을 확보할 수 있도록 감사인력에 대한 자격요건을 정의하여야 한다.

나. 정보보호대책

	통제분야		통제목적		통제사항	통제내용
1	정보보호 정책	1.1	정책의 승인 및 공표	1.1.1	정책의 승인	정보보호정책은 이해관련자의 검토와 최고경영자의 승인을 받아야 한다.
				1.1.2	정책의 공표	정보보호정책 문서는 모든 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.
		1.2	정책의 체계	1.2.1	상위 정책과의 연계성	정보보호정책은 상위조직 및 관련 기관의 정책과 연계성을 유지하여야 한다.
				1.2.2	정책시행 문서수립	정보보호정책의 구체적인 시행을 위한 정보보호지침, 절차를 수립하고 관련 문서간의 일관성을 유지하여야 한다.
		1.3	정책의 유지관리	1.3.1	정책의 검토	정기적으로 정보보호정책 및 정책 시행문서의 타당성을 검토하고, 중대한 보안사고 발생, 새로운 위협 또는 취약성의 발견, 정보보호 환경에 중대한 변화 등이 정보보호정책에 미치는 영향을 분석하여 필요한 경우 제·개정하여야 한다.
				1.3.2	정책문서 관리	정보보호정책 및 정책 시행문서의 이력관리를 위해 제정, 개정, 배포, 폐기 등의 관리절차를 수립하고 문서는 최신본으로 유지하여야 한다. 또한 정책문서 시행에 따른 운영기록을 생성하여 유지하여야 한다.
2	정보보호 조직	2.1	조직 체계	2.1.1	정보보호 최고 책임자 지정	최고경영자는 임원급의 정보보호 최고책임자를 지정하고 정보보호 최고책임자는 정보보호정책 수립, 정보보호 조직 구성, 위험관리, 정보보호위원회 운영 등의 정보보호에 관한 업무를 총괄 관리하여야 한다.

	통제분야		통제목적		통제사항	통제내용
2	정보보호 조직	2.1	조직의 체계	2.1.2	실무조직 구성	최고경영자는 정보보호 최고책임자의 역할을 지원하고 조직의 정보보호 활동을 체계적으로 이행하기 위해 실무조직을 구성하고 조직 구성원의 정보보호 전문성을 고려하여 구성한다.
				2.1.3	정보보호 위원회	정보보호 자원할당 등 조직 전반에 걸친 중요한 정보보호 관련사항에 대한 검토 및 의사결정을 할 수 있도록 정보보호위원회를 구성하여 운영하여야 한다.
		2.2	역할 및 책임	2.2.1	역할 및 책임	정보보호 최고책임자와 정보보호 관련 담당자에 대한 역할 및 책임을 정의하고 그 활동을 평가할 수 있는 체계를 마련하여야 한다.
3	외부자 보안	3.1	보안 요구사항 정의	3.1.1	외부자 계약 시 보안요구사항	조직의 정보처리 업무를 외부자에게 위탁하거나 정보자산에 대한 접근을 허용할 경우, 또는 업무를 위해 클라우드 서비스 등 외부 서비스를 이용하는 경우에는 보안요구사항을 식별하고 관련 내용을 계약서 및 협정서 등에 명시하여야 한다.
		3.2	외부자 보안 이행	3.2.1	외부자 보안 이행 관리	외부자가 계약서 및 협정서에 명시된 보안요구사항의 이행여부를 관리 감독하고 주기적인 점검 또는 감사를 수행하여야 한다.
				3.2.2	외부자 계약 만료 시 보안	외부자와의 계약 만료, 업무 종료, 담당자 변경 시 조직이 외부자에게 제공한 정보자산의 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 업무 수행 시 알게 된 정보의 비밀유지 확약서 등의 내용을 확인하여야 한다.

	통제분야		통제목적		통제사항	통제내용
4	정보자산 분류	4.1	정보자산 식별 및 책임	4.1.1	정보자산 식별	조직의 업무특성에 따라 정보자산 분류기준을 수립하고 정보보호 관리체계 범위 내 모든 정보자산을 식별하여야 한다. 또한 식별된 정보자산을 목록으로 관리하여야 한다.
				4.1.2	정보자산별 책임할당	식별된 정보자산에 대한 책임자 및 관리자를 지정하여 책임소재를 명확히 하여야 한다.
		4.2	정보자산의 분류 및 취급	4.2.1	보안등급과 취급	기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 정보자산이 조직에 미치는 중요도를 평가하고 그 중요도에 따라 보안등급을 부여하여야 한다. 또한 보안등급을 표시하고 등급 부여에 따른 취급절차를 정의하여 이행하여야 한다.
5	정보보호 교육	5.1	교육 프로그램 수립	5.1.1	교육 계획	교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 정보보호 교육 계획을 수립하여야 한다.
				5.1.2	교육 대상	교육 대상에는 정보보호 관리체계 범위 내 임직원 및 외부자를 모두 포함하여야 한다.
				5.1.3	교육 내용 및 방법	교육에는 정보보호 및 정보보호 관리체계 개요, 보안사고 사례, 내부 규정 및 절차, 법적 책임 등의 내용을 포함하고 일반 임직원, 책임자, IT 및 정보보호 담당자 등 각 직무별 전문성 제고에 적합한 교육내용 및 방법을 정하여야 한다.
		5.2	교육 시행 및 평가	5.2.1	교육 시행 및 평가	정보보호 관리체계 범위 내 임직원 및 외부자를 대상으로 연 1회 이상 교육을 시행하고 정보보호 정책 및 절차의 중대한 변경, 조직 내·외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생할 경우 추가 교육을 수행하여야 한다. 또한 교육 시행에 대한 기록을 남기고 평가하여야 한다.

	통제분야		통제목적		통제사항	통제내용
6	인적 보안	6.1	정보보호 책임	6.1.1	주요 직무자 지정 및 감독	인사정보, 영업비밀, 산업기밀, 개인정보 등 중요정보를 대량으로 취급하는 임직원의 경우 주요직무자로 지정하고 주요직무자 지정을 최소화 하는 등 관리할 수 있는 보호대책을 수립하여야 한다.
				6.1.2	직무 분리	권한 오남용 등 고의적인 행위로 인해 발생할 수 있는 잠재적인 피해를 줄이기 위하여 직무 분리 기준을 수립하고 적용하여야 한다. 다만 인적 자원 부족 등 불가피하게 직무분리가 어려운 경우 별도의 보완통제를 마련하여야 한다.
				6.1.3	비밀유지 서약서	임직원으로부터 비밀유지 서약서를 받아야 하고 임시직원이나 외부자에게 정보시스템에 대한 접근권한을 부여할 경우에도 비밀유지서약서를 받아야 한다.
		6.2	인사규정	6.2.1	퇴직 및 직무변경 관리	퇴직 및 직무변경 시 인사부서와 정보보호 및 시스템 운영 부서 등 관련 부서에서 이행해야 할 자산반납, 접근권한 회수·조정, 결과 확인 등의 절차를 수립하여야 한다.
				6.2.2	상벌규정	인사규정에 직원이 정보보호 책임과 의무를 충실히 이행했는지 여부 등 정보보호 활동 수행에 따른 상벌 규정을 포함하여야 한다.

	통제분야		통제목적		통제사항	통제내용
7	물리적 보안	7.1	물리적 보호구역	7.1.1	보호구역 지정	비인가자의 물리적 접근 및 각종 물리적, 환경적 재난으로부터 주요 설비 및 시스템을 보호하기 위하여 통제구역, 제한구역, 접견구역 등 물리적 보호구역을 지정하고 각 구역별 보호대책을 수립·이행하여야 한다.
				7.1.2	보호설비	각 보호구역의 중요도 및 특성에 따라 화재, 전력이상 등 인·재해에 대비하여 온습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 설비를 충분히 갖추고 운영절차를 수립하여 운영하여야 한다. 또한 주요 시스템을 외부 집적정보통신시설에 위탁운영하는 경우 관련 요구사항을 계약서에 반영하고 주기적으로 검토를 수행하여야 한다.
				7.1.3	보호구역 내 작업	유지보수 등 주요 설비 및 시스템이 위치한 보호구역 내에서의 작업 절차를 수립하고 작업에 대한 기록을 주기적으로 검토하여야 한다.
				7.1.4	출입통제	보호구역 및 보호구역 내 주요 설비 및 시스템은 인가된 사람만이 접근할 수 있도록 출입을 통제하고 책임추적성을 확보할 수 있도록 출입 및 접근 이력을 주기적으로 검토하여야 한다.
				7.1.5	모바일 기기 반출입	노트북 등 모바일 기기 미승인 반출입을 통한 중요정보 유출, 내부망 악성코드 감염 등의 보안사고 예방을 위하여 보호구역 내 임직원 및 외부자 모바일 기기 반출입 통제절차를 수립하고 기록·관리하여야 한다.
		7.2	시스템 보호	7.2.1	케이블 보안	데이터를 송수신하는 통신케이블이나 전력을 공급하는 전력 케이블은 손상을 입지 않도록 보호하여야 한다.
				7.2.2	시스템 배치 및 관리	시스템은 그 특성에 따라 분리하여 배치하고 장애 또는 보안사고 발생 시 주요 시스템의 위치를 즉시 확인할 수 있는 체계를 수립하여야 한다.

	통제분야		통제목적		통제사항	통제내용
		7.3	사무실 보안	7.3.1	개인업무 환경 보안	일정시간 동안 자리를 비울 경우에는 책상 위에 중요한 문서나 저장매체를 남겨놓지 않고 컴퓨터 화면에 중요정보가 노출되지 않도록 화면보호기 설정, 패스워드 노출 금지 등 보호대책을 수립하여야 한다.
				7.3.2	공용업무 환경 보안	사무실에서 공용으로 사용하는 사무처리 기기, 문서고, 공용 PC, 파일서버 등을 통해 중요정보 유출이 발생하지 않도록 보호대책을 마련하여야 한다.
8	시스템 개발보안	8.1	분석 및 설계 보안관리	8.1.1	보안 요구사항 정의	신규 정보시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안취약점, 정보보호 기본요소(기밀성, 무결성, 가용성) 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용하여야 한다.
				8.1.2	인증 및 암호화 기능	정보시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입·출력 및 송수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다.
				8.1.3	보안로그 기능	정보시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 하여야 한다.
				8.1.4	접근권한 기능	정보시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다.

	통제분야		통제목적		통제사항	통제내용
8	시스템 개발 보안	8.2	구현 및 이관 보안	8.2.1	구현 및 시험	안전한 코딩방법에 따라 정보시스템을 구현 하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다. 또한 알려진 기술적 보안 취약성에 대한 노출여부를 점검하고 이에 대한 보안대책을 수립하여야 한다.
				8.2.2	개발과 운영 환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다.
				8.2.3	운영환경 이관	운영환경으로의 이관은 통제된 절차에 따라 이루어져야 하고 실행코드는 시험과 사용자 인수 후 실행하여야 한다.
				8.2.4	시험 데이터 보안	시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다.
				8.2.5	소스 프로그램 보안	소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행하여야 한다. 또한 소스 프로그램은 운영환경에 보관하지 않는 것을 원칙으로 한다.
		8.3	외주개발 보안	8.3.1	외주개발 보안	정보시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독하여야 한다.

	통제분야		통제목적		통제사항	통제내용
9	암호통제	9.1	암호 정책	9.1.1	암호 정책 수립	조직의 중요정보 보호를 위하여 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 수립하고 이행하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.
		9.2	암호키 관리	9.2.1	암호키 생성 및 이용	암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고 필요 시 복구방안을 마련하여야 한다.
10	접근 통제	10.1	접근통제 정책	10.1.1	접근통제 정책 수립	비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다.
		10.2	접근권한 관리	10.2.1	사용자 등록 및 권한부여	정보시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다.
				10.2.2	관리자 및 특수 권한 관리	정보시스템 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.
				10.2.3	접근권한 검토	정보시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 점검하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.3	사용자 인증 및 식별	10.3.1	사용자 인증	정보시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제되어야 하고, 필요한 경우 법적요구사항 등을 고려하여 중요 정보시스템 접근 시 강화된 인증방식을 적용하여야 한다.
				10.3.2	사용자 식별	정보시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다. 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.
				10.3.3	사용자 패스워드 관리	법적요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경주기 등 사용자 패스워드 관리절차를 수립·이행하고 패스워드 관리 책임이 사용자에게 있음을 주지시켜야 한다. 특히 관리자 패스워드는 별도 보호대책을 수립하여 관리하여야 한다.
				10.3.4	이용자 패스워드 관리	고객, 회원 등 외부 이용자가 접근하는 정보시스템 또는 웹서비스의 안전한 이용을 위하여 계정 및 패스워드 등의 관리절차를 마련하고 관련 내용을 공지하여야 한다.
		10.4	접근통제 영역	10.4.1	네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 접근통제 리스트, 네트워크 식별자 등에 대한 관리절차를 수립하고 서비스, 사용자 그룹, 정보자산의 중요도에 따라 내·외부 네트워크를 분리하여야 한다.
				10.4.2	서버 접근	서버별로 접근이 허용되는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 적용하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.4	접근통제 영역	10.4.3	응용 프로그램 접근	사용자의 업무 또는 직무에 따라 응용프로그램 접근권한을 제한하고 불필요한 중요정보 노출을 최소화해야 한다.
				10.4.4	데이터베이스 접근	데이터베이스 접근을 허용하는 응용프로그램 및 사용자 직무를 명확하게 정의하고 응용프로그램 및 직무별 접근통제 정책을 수립하여야 한다. 또한 중요정보를 저장하고 있는 데이터베이스의 경우 사용자 접근내역을 기록하고 접근의 타당성을 정기적으로 검토하여야 한다.
				10.4.5	모바일 기기 접근	모바일기기를 업무 목적으로 내·외부 네트워크에 연결하여 활용하는 경우 중요정보 유출 및 침해사고 예방을 위해 기기 인증 및 승인, 접근 범위, 기기 보안설정, 오남용 모니터링 등의 접근통제 대책을 수립하여야 한다.
				10.4.6	인터넷 접속	인사정보, 영업비밀, 산업기밀, 개인정보 등 중요정보를 대량으로 취급·운영하는 주요직무자의 경우 인터넷 접속 또는 서비스(P2P, 웹메일, 웹하드, 메신저 등)를 제한하고 인터넷 접속은 침입차단시스템을 통해 통제하여야 한다. 필요시 침입탐지시스템 등을 통해 인터넷 접속내역을 모니터링하여야 한다.
11	운영보안	11.1	운영 절차 및 변경 관리	11.1.1	운영절차 수립	정보시스템 동작, 문제 발생 시 재 동작 및 복구, 오류 및 예외사항 처리 등 시스템 운영을 위한 절차를 수립하여야 한다.
				11.1.2	변경관리	정보시스템 관련 자산의 모든 변경내역을 관리할 수 있도록 절차를 수립하고 변경 전 시스템의 전반적인 성능 및 보안에 미치는 영향을 분석하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영보안	11.2	시스템 및 서비스 운영 보안	11.2.1	정보 시스템 인수	새로운 정보시스템 도입 또는 개선 시 필수 보안요구사항을 포함한 인수 기준을 수립하고 인수 전 기준 적합성을 검토하여야 한다.
				11.2.2	보안 시스템 운영	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립하고 보안시스템 별 정책적용 현황을 관리하여야 한다.
				11.2.3	성능 및 용량관리	정보시스템 및 서비스 가용성 보장을 위해 성능 및 용량 요구사항을 정의하고 현황을 지속적으로 모니터링할 수 있는 방법 및 절차를 수립하여야 한다.
				11.2.4	장애관리	정보시스템 장애 발생 시 효과적으로 대응하기 위한 탐지, 기록, 분석, 복구, 보고 등의 절차를 수립하여야 한다.
				11.2.5	원격운영 관리	내부 네트워크를 통하여 정보시스템을 관리하는 경우 특정 단말에서만 접근을 할 수 있도록 제한하고, 원격지에서 인터넷 등 외부 네트워크를 통하여 정보시스템을 관리하는 것은 원칙적으로 금지하고 부득이한 사유로 인해 허용하는 경우에는 책임자 승인, 접속 단말 및 사용자 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등의 보호대책을 수립하여야 한다.
				11.2.6	스마트 워크 보안	재택근무, 원격협업 등과 같은 원격 업무 수행 시 이에 대한 관리적·기술적 보호대책을 수립하고 이행하여야 한다.
				11.2.7	무선네트워크 보안	무선랜 등을 통해 무선인터넷을 사용하는 경우 무선 네트워크 구간에 대한 보안을 강화하기 위해 사용자 인증, 송수신 데이터 암호화 등의 보호대책을 수립하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영보안			11.2.8	공개서버 보안	웹사이트 등에 정보를 공개하는 경우 정보 수집, 저장, 공개에 따른 허가 및 게시절차를 수립하고 공개서버에 대한 물리적, 기술적 보호대책을 수립하여야 한다.
				11.2.9	백업관리	데이터의 무결성 및 정보시스템의 가용성을 유지하기 위해 백업 대상, 주기, 방법 등의 절차를 수립하고 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다.
				11.2.10	취약점 점검	정보시스템이 알려진 취약점에 노출되어 있는 지 여부를 확인하기 위하여 정기적으로 기술적 취약점 점검을 수행하고 발견된 취약점들은 조치하여야 한다.
		11.3	전자거래 및 정보전송 보안	11.3.1	전자거래 보안	전자거래 서비스 제공 시 정보유출, 데이터 조작, 사기 등의 침해사고를 예방하기 위해 사용자 인증, 암호화, 부인방지 등의 보호대책을 수립하고 결제시스템 등 외부 시스템과의 연계가 필요한 경우 연계 안전성을 점검하여야 한다.
				11.3.2	정보전송 정책 수립 및 협약 체결	타 조직에 중요정보를 전송할 경우 안전한 전송을 위한 정책을 수립하고 조직 간 정보전송 합의를 통해 관리 책임, 전송 기술 표준, 중요정보의 보호를 위한 기술적 보호조치 등을 포함한 협약서를 작성하여야 한다.
		11.4	매체 보안	11.4.1	정보 시스템 저장매체 관리	정보시스템 폐기 또는 재사용 시 중요정보를 담고 있는 하드디스크, 스토리지, 테잎 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제하여야 한다.
				11.4.2	휴대용 저장매체 관리	조직의 중요정보 유출을 예방하기 위해 외장하드, USB, CD 등 휴대용 저장매체 취급, 보관, 폐기, 재사용에 대한 절차를 수립하여야 한다. 또한 매체를 통한 악성코드 감염 방지 대책을 마련하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영보안	11.5	악성코드 관리	11.5.1	악성코드 통제	바이러스, 웜, 트로이목마 등의 악성코드로부터 정보시스템을 보호하기 위해 악성코드 예방, 탐지, 대응 등의 보호대책을 수립하여야 한다.
				11.5.2	패치관리	소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인해 발생할 수 있는 침해사고를 예방하기 위해 최신 패치를 정기적으로 적용하고 필요한 경우 시스템에 미치는 영향을 분석하여야 한다.
		11.6	로그관리 및 모니터링	11.6.1	시각 동기화	로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 정보시스템 시각을 공식 표준시각으로 정확하게 동기화 하여야 한다.
				11.6.2	로그 기록 및 보존	정보시스템, 응용프로그램, 보안시스템, 네트워크 장비 등 기록해야 할 로그 유형을 정의하여 일정기간 보존하고 주기적으로 검토하여야 한다. 보존기간 및 검토주기는 법적요구사항을 고려하여야 한다.
				11.6.3	접근 및 사용 모니터링	중요정보, 정보시스템, 응용프로그램, 네트워크 장비에 대한 사용자 접근이 업무상 허용된 범위에 있는 지 주기적으로 확인하여야 한다.
				11.6.4	침해시도 모니터링	외부로부터의 침해시도를 모니터링하기 위한 체계 및 절차를 수립하여야 한다.
12	침해사고 관리	12.1	절차 및 체계	12.1.1	침해사고 대응절차 수립	DDoS 등 침해사고 유형별 중요도 분류, 유형별 보고·대응·복구 절차, 비상연락체계, 훈련 시나리오 등을 포함한 침해사고 대응 절차를 수립하여야 한다.
				12.1.2	침해사고 대응체계 구축	침해사고 대응이 신속하게 이루어질 수 있도록 중앙 집중적인 대응체계를 구축하고 외부기관 및 전문가들과의 협조체계를 수립하여야 한다.
		12.2	대응 및 복구	12.2.1	침해사고 훈련	침해사고 대응 절차를 임직원들이 숙지할 수 있도록 시나리오에 따른 모의훈련을 실시하여야 한다.

	통제분야		통제목적		통제사항	통제내용
12	침해사고 관리	12.2	대응 및 복구	12.2.2	침해사고 보고	침해사고 징후 또는 사고 발생을 인지한 때에는 침해사고 유형별 보고 절차에 따라 신속히 보고하고 법적 통지 및 신고 의무를 준수하여야 한다.
				12.2.3	침해사고 처리 및 복구	침해사고 대응절차에 따라 처리와 복구를 신속하게 수행하여야 한다.
		12.3	사후관리	12.3.1	침해사고 분석 및 공유	침해사고가 처리되고 종결된 후 이에 대한 분석을 수행하고 그 결과를 보고하여야 한다. 또한 사고에 대한 정보와 발견된 취약점들을 관련 조직 및 임직원들과 공유하여야 한다.
				12.3.2	재발방지	침해사고로부터 얻은 정보를 활용하여, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하고 이를 위해 필요한 경우 정책, 절차, 조직 등의 대응체계를 변경하여야 한다.
13	IT 재해복구	13.1	체계 구축	13.1.1	IT 재해복구 체계 구축	자연재앙, 해킹, 통신장애, 전력중단 등의 요인으로 인해 IT 시스템 중단 또는 파손 등 피해가 발생할 경우를 대비하여 비상 시 복구조직, 비상연락체계, 복구절차 등 IT 재해복구 체계를 구축하여야 한다.
		13.2	대책 구현	13.2.1	영향분석에 따른 복구대책 수립	조직의 핵심 서비스 연속성을 위협할 수 있는 IT 재해 유형을 식별하고 유형별 예상 피해규모 및 영향을 분석하여야 한다. 또한 IT 서비스 및 시스템 복구목표시간, 복구시점을 정의하고 적절한 복구전략 및 대책을 수립·이행하여야 한다.
				13.2.2	시험 및 유지관리	IT 서비스 복구전략 및 대책에 따라 효과적인 복구가 가능한 지 시험을 실시하고 시험계획에는 시나리오, 일정, 방법, 절차 등을 포함하여야 한다. 또한 시험결과, IT 환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완하여야 한다.

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제1호서식] <개정 2016.0.0>

정보보호 관리체계 인증기관 지정 신청서

* 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	처리기간	3개월이내

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	총 직원 수	인증심사원 직원 수	
신청구분	☐ 신규	☐ 재지정	

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제6항 및 같은 법 시행령 제53조의2에 따라 정보보호 관리체계 인증기관 지정을 위와 같이 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

미래창조과학부 귀중

신청인 제출서류	1. 정관 또는 규약 1부. 2. 별지 제3호서식의 인증심사원의 보유현황과 이를 증명할 수 있는 서류 1부. 3. 별표 1에 따른 업무수행 요건·능력 심사를 위하여 필요한 서류 1부.	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

처 리 절 차

신청서 작성	→	접 수	→	심 사	→	지정여부 결정	→	지정서 교부
신청인		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)

210mm×297mm[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제2호서식] <개정 2016.0.0>

정보보호 관리체계 심사기관 지정 신청서

* 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	처리기간	3개월이내

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	총 직원 수	인증심사원 직원 수	
신청구분	☐ 신규	☐ 재지정	

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제7항 및 같은 법 시행령 제53조의2에 따라 정보보호 관리체계 심사기관 지정을 위와 같이 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

미래창조과학부 귀중

신청인 제출서류	1. 정관 또는 규약 1부. 2. 별지 제3호서식의 인증심사원의 보유현황과 이를 증명할 수 있는 서류 1부. 3. 별표 1에 따른 업무수행 요건·능력 심사를 위하여 필요한 서류 1부.	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

처 리 절 차

신청서 작성	→	접 수	→	심 사	→	지정여부 결정	→	지정서 교부
신청인		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)

210mm×297mm[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제3호서식] <개정 2016.0.0>

인증심사원의 보유현황

(제1쪽)

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	직원 수	인증심사원 직원 수	

일련번호	성명	주소		최종학력	해당요건
		생년월일	입사일	취득학위 및 학과	

유의사항

1. 「해당요건」란에는 선임심사원, 심사원, 심사원보 요건을 기재한다.
2. 기재된 최종학위를 증명할 수 있는 직원의 졸업 또는 학위증명서 사본을 제출하여야 한다.
3. 별표 3의 「인증 심사원 학력 및 경력 요건」을 충족하는 직원은 기술자격증 사본 등 자격을 취득하였음을 확인할 수 있는 서류를 함께 제출하여야 한다.
4. 정보통신유관경력 또는 정보보호유관경력을 증명할 수 있는 경력증명서(근무부서 또는 담당업무 등이 기재되어야 한다)와 해당 직원이 신청업체에 현재 근무하고 있음을 확인할 수 있는 재직증명서를 함께 제출하여야 한다.

210㎜×297㎜[백상지(80g/㎡)]

인증심사업무를 전담하는 직원의 보유현황

(제2쪽)

일련번호	성명	주소		최종학력	해당요건
		생년월일	입사일	취득학위 및 학과	

10㎜×297㎜[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제4호서식] <개정 2016.0.0> (제1쪽)

정보보호 관리체계 인증기관 지정서

등록번호 :

업체명 :

대표자 :

주소 :

지정의 유효기간 :

인증업무의 범위 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제6항 및 같은 법 시행령 제53조의2에 따라 위와 같이 정보보호 관리체계 인증기관으로 지정합니다.

년 월 일

미래창조과학부장관 직인

210mm×297mm[백상지(120g/㎡)]

(제2쪽)

CERTIFICATE OF DESIGNATION
AS
ISMS Certification Authority

Registry Number :

Name of Organization :

Name of Representative :

Address :

Period of Validity :

Scope of Certification work :

This is to certify that the abovementioned organization is designated Information Security Management System (ISMS) Certification Authority in accordance with Article 47, Paragraph 6 of 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」 and Article 53-2 of the Enforcement Decree of the same Act.

Date of Issuance:

Signed by the
Minister of Ministry of Science, ICT and Future Planning
Republic of Korea

210㎜×297㎜[백상지 120g/㎡]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제5호서식] <개정 2016.0.0> (제1쪽)

정보보호 관리체계 심사기관 지정서

등록번호 :

업체명 :

대표자 :

주소 :

지정의 유효기간 :

심사업무의 범위 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제7항 및 같은 법 시행령 제53조의2에 따라 위와 같이 정보보호 관리체계 심사기관으로 지정합니다.

년 월 일

미래창조과학부장관 직인

210mm×297mm[백상지(120g/㎡)]

(제2쪽)

CERTIFICATE OF DESIGNATION
AS
ISMS Audit Authority

Registry Number :

Name of Organization :

Name of Representative :

Address :

Period of Validity :

Scope of Audit work :

This is to certify that the abovementioned organization is designated Information Security Management System (ISMS) Audit Authority in accordance with Article 47, Paragraph 7 of 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」 and Article 53-2 of the Enforcement Decree of the same Act.

Date of Issuance:

Signed by the
Minister of Ministry of Science, ICT and Future Planning
Republic of Korea

210㎜×297㎜[백상지 120g/㎡]

■「정보보호 관리체계 인증 등에 관한 고시」 [별지 제6호서식] <개정 2013.8.8>

인증실적 보고서

정보보호 관리체계 인증기관	업체명		사업자등록번호
	주소		전화번호
	대표자		
	정보보호 관리체계 인증실적 총계		

일련번호	인증 번호	대상기관(기업)명	인증범위	유효기간

년 월 일

신청인(대표자) (서명 또는 인)

미래창조과학부 귀중

■「정보보호 관리체계 인증 등에 관한 고시」 [별지 제7호서식] <개정 2016.0.0>

인증심사실적 보고서

정보보호 관리체계 심사기관	업체명		사업자등록번호
	주소		전화번호
	대표자		
	정보보호 관리체계 인증심사 실적 총계	최초심사	건
		갱신심사	건
		사후심사	건

일련 번호	대상기관(기업)명	인증심사 범위	인증심사 기간	구분 (최초/갱신/사후)

년 월 일

신청인(대표자) (서명 또는 인)

미래창조과학부 귀중

■「정보보호 관리체계 인증 등에 관한 고시」 [별지 제8호서식] <개정 2013.8.8> (제1쪽)

정보보호 관리체계 인증심사원 자격 신청서

신청자 인적사항	성 명		생년월일		사진	
	주 소	(우: -)				
	회 사 명					
	회사주소	(우: -)				
	이 메 일					
	전화번호		휴대전화			
신청사항	신청 구분	□ 자격인증 □ 전문분야 변경				
학력사항	최종학력	□ 고졸	□ 전문학사	□ 학사	□ 석사	□ 박사
	학사	전공		기간		
	석사	전공		기간		
	박사	전공		기간		
인증심사원 교육이수	교육기간	년 월 일 ~ 년 월 일		수료증번호		

자격사항 ※해당자에 한함	자격증번호	자격증명/등급	취득일자	수여기관

경력사항 ※최근 10년 내 경력사항 기술	총 경력	정보기술	총 년 개월	정보보호	총 년 개월

No.	구분	기간	회사명	부서	직책
1	□정보기술 □정보보호	~ (년 개월)			
2	□정보기술 □정보보호	~ (년 개월)			
3	□정보기술 □정보보호	~ (년 개월)			
4	□정보기술 □정보보호	~ (년 개월)			
5	□정보기술 □정보보호	~ (년 개월)			

※ 칸이 부족할 경우 추가 작성

(제2쪽)

(1) 개인별 전문분야 (복수 선택 가능, 우선순위 표기요망)					
대분류	중분류	소분류	순위	실무경력	
관리적 정보 보호	정책, 조직 및 인적보안	정보보호정책수립 및 조직구성			년
		인적보안, 외부자 보안, 외부위탁관리			년
		정보보호교육 및 훈련			년
		국내외 표준 기준 및 법령			년
	위험관리	자산분류, 위험평가 수행, 대책 및 계획수립			년
	업무연속성관리	업무연속성 계획수립 및 시험, 유지관리			년
	침해사고대응	침해사고 대응계획 및 체계, 복구			년
	정보시스템 감사/감리	정보시스템 및 정보보호시스템 감사/감리			년
기술적 정보 보호	네트워크	네트워크 설계기술			년
		라우팅 제어, 프로토콜 제어, 접근통제, 암호화, NAT, 운용관리(로그, SNMP, 설정도구)등 통신기술			년
		라우터, 스위치(L2~L7), RAS, VPN, SSL, DHCP, 네트워크 감시 등 기기기술			년
		기타( )			년
	운영체제 및 시스템	OS 기본지식, 계정관리, 접근권한, 서비스관리, 로그관리, 패치, 보안 S/W 사용 등 유닉스/리눅스 시스템			년
		OS 기본지식, 계정관리, 접근권한, 서비스관리, 로그관리, 패치, 보안 S/W 사용 등 윈도우 시스템			년
		메인프레임 등 기타( )			년
	응용서비스	HTTP 프로토콜, 브라우저, SQL-Injection 등 Web 위협에 대한 대응책, SSL, CGI 보안 프로그래밍 등 Web 서비스			년
		부하분산, DNSSEC, 보안설정 등 DNS 서비스			년
		메일 프로토콜, 스팸대응, 웜/바이러스 필터링 등 메일 서비스			년
		DB 기본지식, 이중화, 데이터백업, 암호화 등 데이터베이스			년
		ERP, KMS, CRM 등 사내정보시스템			년
		분산시스템 등 기타( )			년
	정보보호 솔루션	FW 기본지식, 접근통제, 라우팅, 네트워크 정책설계, 구성(이중화, 망분리, 로드밸런싱 등) 등 침입차단시스템			년
		웜/바이러스 기본지식, 웜/바이러스별 감염 증상과 대책 등 바이러스 월			년
		IDS 기본지식, 방화벽 연동, 패턴 매칭 방법, 구성(에이전트 위치, 통합콘솔 등) 등 침입탐지시스템			년
		SecureOS 기본지식, 계정관리, 접근권한, 서비스관리, 로그관리, 패치 등 SecureOS			년
		기타( )			년

(제3쪽)

(1) 개인별 전문분야 (복수 선택 가능, 우선순위 표기요망) (계속)					
대분류	중분류	소분류	순위	실무경력	
기술적 정보 보호 (계속)	취약성분석	사회공학적 방법, 스캔, Sniffing, DOS, Buffer Overflow, 웜/바이러스, 백도어 등 취약성 분석 및 점검			년
	보안 운영	통합관제(ESM, NMS 등), 망관리, 백업, 로그 분석, 모니터링, 패치, 문제해결(원인규명)			년
	기반기술	IPSec, PPTP, L2TP, SSH, SSL/TLS, MPLS, IKE, S/MIME, PGP 등 보안 프로토콜			년
		패스워드인증, 생체인증, 인증디바이스, 인증프로토콜, WEB인증, RADIUS, SSO 등 인증기술			년
		증명서 인증 및 실효, 신뢰모델, 기술 및 데이터방식, 인증센터 구축과 운영, 법적구조 등 PKI			년
		암호알고리즘, Key 관리, 암호방식 등 암호기술			년
		디지털서명, 디지털 봉투, 코드 서명			년
물리적 정보 보호	접근보안	출입 및 접근통제, 모니터링 등			년
	시설관리	소방시설, 비상전원, 비상조명, 항온항습 등			년
개인정보보호		개인정보보호 책임자, 취급자, 컨설턴트, 법률 담당, 소비자 민원 및 상담 등			년
기타		( )			년

※ 경력 및 전문 분야에 대한 관련 내용을 상세히 기술
※ 칸이 부족할 경우 별지 사용

No.	상세내용
1	
2	
3	
4	
5	
6	

(제4쪽)

(2) 통제분야별 전문분야 (5순위까지 선택, 우선순위 표기요망)

통제분야	순위	실무경력		통제분야	순위	실무경력	
1. 정보보호정책			년	9. 암호통제			년
2. 정보보호조직			년	10. 접근통제			년
3. 외부자 보안			년	11. 운영관리			년
4. 정보자산분류			년	12. 전자거래보안			년
5. 정보보호교육 및 훈련			년	13. 보안사고관리			년
6. 인적 보안			년	14. 검토, 모니터링 및 감사			년
7. 물리적 보안			년	15. 업무연속성 관리			년
8. 시스템개발 보안			년	16. 개인정보보호			년

관련 경력기술

※ 5순위까지 선택한 전문분야 관련 실무경력, 전문기술, 인증심사실적 등 관련경력을 상세히 기술

<개인정보 수집·이용>

- 개인정보 수집 이용 목적 : 정보보호 관리체계(ISMS) 인증심사원 양성 교육, 자격부여 및 관리, 자문료 지급, 심사팀구성
- 수집하는 개인정보 항목 : 성명, 생년월일, 주소, 이메일, 전화번호, 학력, 자격경력, 발령사항, 기술실적사항
- 보유 및 이용기간 : 인증심사원 자격 종료시까지
- 개인정보의 수집·이용을 거부할 수 있으며, 이 경우 인증심사원 등록 및 위촉에 불이익이 발생할 수 있음을 알려드립니다.

▷ 개인정보 수집·이용 동의여부 **동의 □** **미동의 □**

<인증심사원 의무사항>

- 인증심사원은 객관적이고 공정한 인증심사를 수행한다.
- 인증심사원으로서의 성실한 직무수행 및 품위유지를 한다.
- 인증심사와 관련된 부당한 금전, 금품 등의 수수를 금지한다.
- 인증심사의 수행에서 취득한 정보를 관련 법령 또는 신청기관의 동의 없이 외부에 누설하여서는 안된다.
- 인증심사원은 인증업무지침을 성실히 준수한다.
- 인증심사원은 본인이 ISMS 인증 취득을 위한 컨설팅을 수행한 기업에 대하여는 인증심사에 참여할 수 없다.
- 인증심사원은 인증심사의 수행과 관련하여 상업적, 재정적 그리고 기타 모든 압력으로부터 배제되어야 한다.

1. 위의 인증심사원 의무사항을 읽고 이해하였으며, 성실히 준수하겠습니다.
2. 본 신청서의 기재사항은 사실과 틀림없으며, 만약 허위로 판명될 경우에는 자격취소 등 불이익을 감수하겠습니다.

※ 필요시 학력, 경력 등 증빙서류 제출을 요청받을 수 있으며 반드시 이에 응해야 함

위와 같이 인증심사원 자격을 신청합니다.

년 월 일

신청자		(서명 또는 인)

한국인터넷진흥원 귀중

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제9호서식] <개정 2013.8.8>

경력증명서

인적사항	성명		생년월일	
	주소		연락처	

경력사항	전 근무처 명				
	근무기간		부서	직위	담당업무
	부터	까지			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			

근무년수	년 개월	최종직위	
용도	정보보호 관리체계 인증심사원 자격 신청		

위와 같이 경력을 증명합니다.

년 월 일

회사명

대표자 (서명 또는 인)

확인자	성명	부서	연락처	비고

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제10호서식] <개정 2013.8.8>

상세 재직증명서

인적사항	성명		생년월일	
	주소		연락처	
소속사항	회사명			
	부서		직위	
	근속기간	~	근무년수	년 개월

발령사항	근무기간		부서	직위	담당업무
	부터	까지			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			

용도	정보보호 관리체계 인증심사원 자격 신청

위와 같이 재직하고 있음을 증명합니다.

년 월 일

회사명

대표자 (서명 또는 인)

확인자	성명	부서	연락처	비고

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제11호서식] <개정 2013.8.8>

기술실적증명서

인적사항	성명		생년월일	
	주소		연락처	

실적사항	소속				
	수행기간		참여사업명	발주처	담당업무
	부터	까지			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			

용도	정보보호 관리체계 인증심사원 자격 신청

위와 같이 기술실적을 증명합니다.

년 월 일

회사명

대표자 (서명 또는 인)

확인자	성명	부서	연락처	비고

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제12호서식] <개정 2013.8.8>

제 호

인증심사원 자격 증명서

성 명 : (. . .)

인증심사원 등급 :

유효기간 :

※ 인증심사원 유지조건을 만족하지 못할 경우 자격이 취소될 수 있습니다.

귀하에게 정보보호 관리체계 인증심사원 자격을 부여합니다.

년 월 일

한국인터넷진흥원 원장 직인

210mm×297mm[백상지(120g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제13호서식] <개정 2016.0.0>

정보보호 관리체계 인증 신청서

※ [ ]에는 해당되는 곳에 √표를 하고, 어두운 부분은 신청인이 작성하지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명	사업자등록번호
	주소	전화번호
	대표자	

인증신청의 구분	[ ]최초심사 [ ]사후심사 [ ]갱신심사
정보보호 관리체계의 범위	
정보보호 관리체계의 범위에 포함되어 있는 종업원의 수	
정보보호 관리체계의 범위에 포함되어 있는 서버의 수	

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제11항, 같은 법 시행령 제47조에 따라 위와 같이 정보보호 관리체계의 인증을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

(한국인터넷진흥원 · 인증기관 또는 심사기관) 귀중

신청(신고)인 제출서류	정보보호 관리체계의 내역서 1부.	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

210㎜×297㎜[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제14호서식] <개정 2016.0.0> (제1쪽)

정보보호 관리체계 인증서

인증번호 :

업체명 :

대표자 :

주소 :

인증의 범위 :

유효기간 :

심사수행 기관 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제11항, 같은 법 시행령 제47조에 따라 위와 같이 정보보호 관리체계를 인증합니다.

년 월 일

한국인터넷진흥원 원장
또는 정보보호 관리체계
인증기관 장 직인

210mm×297mm[백상지(120g/㎡)]

(제2쪽)

CERTIFICATE
OF
Information Security Management System

Certificate Number :

Name of Organization :

Name of Representative :

Address :

Scope of Certification :

Period of Validity :

name of Audit Organization :

This is to certify that the abovementioned organization is compliant to the assessment standard for Information Security Management System certification in accordance with Article 47, Paragraph 1 and 11 of 「Act on Information Network Utilization and Data Protection, etc.」 and Article 47 of the Enforcement Decree of the same Act.

Date of Issuance :

Signed by the
President of Korea Internet & Security Agency or certification body

210㎜×297㎜[백상지(120g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제15호서식] <개정 2013.8.8>

정보보호 관리체계 인증서 추가발급 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명	사업자등록번호
	주소	전화번호
	대표자	

추가발급 사유	

위와 같이 정보보호 관리체계 인증서의 추가발급을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

한국인터넷진흥원 또는 정보보호 관리체계 인증기관명 귀중

제출서류	해당없음	수수료 없 음

210mm×297mm[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제16호서식] <개정 2013.8.8>

정보보호 관리체계 인증서 변경 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		

변경 내용	변경전	(국문)
		(영문)
	변경후	(국문)
		(영문)
변경사유		

위와 같이 정보보호 관리체계 인증서 변경을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

한국인터넷진흥원 또는 정보보호 관리체계 인증기관명 귀중

제출서류	해당없음	수수료 없 음

210mm×297mm[백상지(80g/㎡)]

정보보호 관리체계 인증 등에 관한 고시

[시행 2016.6.2] [고시 제2016 - 59호, 2016.6.2, 일부개정]

제1장 총 칙

제1조(목적) 이 고시는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) 제47조제3항ㆍ제4항, 같은 법 시행령(이하 "영"이라 한다) 제47조부터 제53조의2까지의 규정 및 같은 법 시행규칙(이하 "규칙"이라 한다) 제3조에 따라 정보보호 관리체계 인증에 관하여 필요한 사항에 대해 정하는 것을 목적으로 한다.

제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "정보보호 관리체계 인증기관(이하 ‘ 인증기관 ’ 이라 한다)"이란 법 제47조제6항에 따라 미래창조과학부가 인증에 관한 업무를 수행할 수 있도록 지정한 기관을 말한다.
2. "정보보호 관리체계 심사기관(이하 ‘ 심사기관 ’ 이라 한다)"이란 법 제47조제7항에 따라 미래창조과학부가 인증심사 업무를 수행할 수 있도록 지정한 기관을 말한다.
3. "업무수행 요건ㆍ능력 심사"란 인증기관 또는 심사기관으로 지정받고자 신청한 법인 또는 단체의 업무수행 요건ㆍ능력을 별표 2의 세부기준에 따라 심사하는 것을 말한다.
4. "인증"이란 신청기관이 수립하여 운영하고 있는 정보보호 관리체계가 별표 7의 정보보호 관리체계 인증기준(이하 "인증기준"이라 한다)에 적합함을 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다) 또는 인증기관이 증명하는 것을 말한다.
5. "인증심사"란 신청기관이 수립하여 운영하는 정보보호 관리체계가 인증기준에 적합한지의 여부를 인터넷진흥원ㆍ인증기관 또는 심사기관이 서면심사 및 현장심사의 방법으로 확인하는 것을 말한다.
6. "정보보호관리과정(이하 ‘ 관리과정 ’ 이라 한다)"이란 정보보호 관리체계를 수립ㆍ운영하기 위하여 유지ㆍ관리하여야 할 과정으로 다음 각 목의 5단계 활동을 말한다.
   가. 정보보호정책 수립 및 범위설정
   나. 경영진 책임 및 조직구성
   다. 위험관리
   라. 정보보호대책 구현
   마. 사후관리

7. "정보보호대책"이란 신청기관이 정보보호 관리체계를 수립·운영하기 위하여 별표 7에서 선택한 통제사항을 말한다.
8. "신청기관"이란 이 고시에 따라 정보보호 관리체계 인증을 취득하고자 신청한 자를 말한다.
9. "인증심사원"이란 별표 3의 자격요건을 갖춘 자를 말한다.
10. "최초심사"란 처음으로 인증을 신청하거나 인증의 범위에 중요한 변경이 있어서 다시 인증을 신청한 때 실시하는 인증심사를 말한다.
11. "사후심사"란 정보보호 관리체계 인증(인증이 갱신된 경우를 포함한다)을 받고난 후 매년 사후관리를 위하여 실시하는 인증심사를 말한다.
12. "갱신심사"란 유효기간 만료로 다시 인증을 신청한 때 실시하는 인증심사를 말한다.

제2장 정보보호 관리체계 인증기관 및 심사기관

제3조(인증기관 및 심사기관의 지정공고 등) ① 미래창조과학부는 법 제47조제6항·제7항 및 영 제53조의2에 따라 인증기관 또는 심사기관을 지정할 필요가 있는 때에는 지정대상 기관의 수, 업무의 범위 및 신청방법 등을 정하여 관보 및 인터넷 홈페이지에 20일 이상 공고하여야 한다.

② 제1항에 따라 인증기관으로 지정받으려는 자는 다음 각 호의 서류를 미래창조과학부에 제출하여야 한다.

1. 별지 1호 서식의 정보보호 관리체계 인증기관 지정 신청서
2. 영 제53조의2제1항제2호에 따른 별지 3호서식의 인증심사원 보유현황과 이를 증명할 수 있는 서류
3. 영 제53조의2제1항제3호에 따른 별표 1의 업무수행 요건·능력 심사를 위하여 필요한 서류

③ 제1항에 따라 심사기관으로 지정받으려는 자는 다음 각 호의 서류를 미래창조과학부에 제출하여야 한다.

1. 별지 2호서식의 정보보호 관리체계 심사기관 지정 신청서
2. 영 제53조의2제1항제2호에 따른 별지 제3호서식의 인증심사원 보유현황과 이를 증명할 수 있는 서류
3. 영 제53조의2제1항제3호에 따른 별표 1의 업무수행 요건·능력 심사를 위하여 필요한 서류

제4조(업무수행 요건·능력 심사 세부기준 등) ① 영 제53조제2항에 따른 업무수행 요건·능력 심사를 위한 세부기준은 별표 2와 같다.

② 미래창조과학부는 제3조제2항에 따라 인증기관 또는 심사기관의 지정 신청을 받은 때에는 제1항에 따라 업무수행 요건·능력을 심사하여 지정 대상기관의 순위를 정한다.

제5조(업무수행 능력의 적합성 인정) ① 미래창조과학부는 제4조제1항에 따라 업무수행 요건·능력을 심사하여 지정에 필요한 수만큼 점수의 합이 높은 순으로 선별한다.
② 미래창조과학부는 제1항에 따라 심사한 결과를 바탕으로 하여 인증기관 또는 심사기관으로의 지정 여부를 최종 결정한다.

제6조(인증기관 및 심사기관의 지정서) ① 영 제53조의2제3항에 따른 정보보호 관리체계 인증기관 지정서는 별지 제4호서식과 같다.
② 영 제53조의2제3항에 따른 정보보호 관리체계 심사기관 지정서는 별지 제5호서식과 같다.

제7조(인증기관 및 심사기관의 사후관리) ① 영 제53조의4제1항에 따른 인증기관의 전년도 인증실적 보고서는 별지 제6호서식과 같다.
② 영 제53조의4제1항에 따른 심사기관의 전년도 인증심사실적 보고서는 별지 제7호서식과 같다.

제8조(인증기관 및 심사기관의 재지정) ① 인증기관은 유효기간이 끝나기 전 6개월부터 끝나는 날까지 별지 제1호서식에 따라 미래창조과학부에 재지정 신청을 할 수 있다.
② 심사기관은 유효기간이 끝나기 전 6개월부터 끝나는 날까지 별지 제2호서식에 따라 미래창조과학부에 재지정 신청을 할 수 있다.
③ 제1항 또는 제2항에 따른 재지정의 심사, 재지정 결과 통지, 재지정서 발급 등에 관하여는 영 제53조의2제3항을 준용한다.

제3장 인증심사원의 자격 및 관리

제9조(인증심사원의 자격 요건 등) ① 인증심사원은 심사원보, 심사원, 선임심사원으로 구분하며, 인증심사원 등급별 자격 요건은 별표 3과 같다.
② 인증심사원이 되려는 자는 별표 3의 학력 및 경력 요건을 갖추고 인터넷진흥원이 지정하는 기관에서 인증심사원 양성교육 과정을 수료하여야 한다.

제10조(인증심사원 자격 신청) 인증심사원의 자격을 신청하고자 하는 자는 제9조제2항에 따라 인증심사원 양성교육 과정을 수료한 날로부터 1개월 이내에 인터넷진흥원에 다음 각 호의 모든 서류를 제출하여야 한다.
1. 별지 제8호서식 정보보호 관리체계 인증심사원 자격 신청서
2. 학위증명서, 자격증 사본(해당 시)
3. 별지 제9호서식 경력증명서
4. 별지 제10호서식 상세 재직증명서 등 경력증빙서류
5. 별지 제11호서식 기술실적증명서(해당 시)

제11조(인증심사원 자격 부여) ① 인터넷진흥원은 인증심사원 자격 신청서를 접수한 때에는 신청서류를 검토하여 서류 보완 및 추가제출을 요청할 수 있다.

② 서류 보완 및 추가제출을 요청받은 자격 신청자는 1개월 이내에 관련 서류 등을 제출하여야 한다.

③ 인터넷진흥원은 인증심사원 자격의 적합 여부를 확인하여 통과한 자에게 별지 제12호서식의 인증심사원 자격 증명서를 발급하여야 한다.

제12조(인증심사원 자격 유지) ① 인증심사원의 자격 유효기간은 자격 부여를 받은 날로부터 3년으로 한다.

② 인증심사원은 자격 유지를 위해 유효기간 내에 인터넷진흥원이 지정하는 기관에서 시행하는 인증심사원 보수교육을 이수해야 한다. 다만, 부득이한 사유로 보수교육을 받지 못한 경우에는 인터넷진흥원이 인정하는 대체교육을 받아야 한다.

③ 보수교육을 이수한 자에 한하여 자격 유효기간이 3년간 연장된다.

제13조(인증심사원 자격 취소) ① 인증심사원 자격 신청 시 제출한 서류가 허위이거나, 제12조에 따른 자격 유지 기준을 충족하지 못한 경우에는 자격을 취소한다.

② 인증심사원으로서 객관적이고 공정한 인증심사를 수행하지 않거나, 인증심사와 관련된 부당한 금전, 금품 등을 수수하거나 인증심사 수행 중 취득한 정보를 누설하는 경우에는 자격을 취소한다.

제4장 인증심사의 신청 및 계약

제14조(인증 의무대상자 범위) ① 인증 의무대상자란 법 제47조제2항, 영 제49조에 따라 정보보호 관리체계 인증을 받아야 하는 자를 말한다.

② 법 제47조제2항제2호에 따라 정보보호 관리체계 인증을 받아야 하는 자 중 집적정보통신시설 사업자가 마련한 시설의 일부를 임대하여 집적정보통신시설 사업을 하는 자에 대하여는 영 제49조제2항의 기준을 준용한다.

③ 인증 의무대상자는 매년 1월1일부터 12월31일까지 인증을 받아야 한다.

제15조(신청기관의 사전 준비사항) 신청기관은 정보보호 관리체계 인증을 신청하기 전에 인증기준에 따른 정보보호 관리체계를 구축하여 최소 2개월 이상 운영하여야 한다.

제16조(인증의 신청 등) ① 법 제47조제1항 또는 제2항에 따라 정보보호 관리체계 인증을 받으려는 자는 별지 제13호서식의 정보보호 관리체계 인증 신청서를 인터넷진흥원·인증기관 또는 심사기관에 제출하여야 한다.

② 신청기관은 인증의 범위 및 일정 등을 인터넷진흥원·인증기관 또는 심사기관과 사전 협의하여 신청하여야 한다.

③ 인터넷진흥원·인증기관 또는 심사기관은 제14조에 따른 인증 의무대상자가 사업자 등록일이 속한 분기가 끝나는 날의 1개월 전까지 인증 신청을 한 경우 인증심사를 우선적으로 처리할 수 있다.

제17조(인증심사의 일부 생략 신청 등) ① 규칙 제3조에 따른 인증을 받았거나 정보보호 조치를 취한 자가 정보보호 관리체계 인증심사의 일부 생략을 신청하는 경우 인터넷진흥원·인증기관 또는 심사기관은 별표 4의 범위 내에서 정보보호 관리체계 인증심사를 생략할 수 있다. 다만, 인증 또는 정보보호 조치의 항목이 별표 7의 항목과 동일하다는 것을 증명하는 서류를 별도로 제출하는 경우에는 별표 4의 범위 외의 항목에 대해서도 정보보호 관리체계 인증심사를 생략할 수 있다.

② 제1항 단서에 따라 신청자가 별도로 제출한 인증 또는 정보보호 조치 항목에 대한 인증심사 생략 여부는 제22조에 따른 인증위원회 심의, 인터넷진흥원과 인증기관간의 협의, 미래창조과학부 장관의 승인을 거쳐 확정하고, 미래창조과학부, 인터넷진흥원·인증기관 및 심사기관 홈페이지에 게시한다.

제18조(인증심사 계약 체결) 신청기관은 인터넷진흥원·인증기관 또는 심사기관과 협의한 후 심사기간, 심사인원, 인증 수수료, 인증의 범위 등을 포함하는 인증심사 계약을 체결한다.

제5장 인증심사의 기준과 방법

제19조(인증기준) 인증기준은 별표 7과 같다.

제20조(인증심사팀 구성) ① 인터넷진흥원·인증기관 또는 심사기관은 제18조에 따른 인증심사 계약을 체결한 때에는 지체 없이 인증심사원으로 인증심사팀을 구성하여야 한다.

② 인증심사팀 구성 시 심사팀장은 인터넷진흥원·인증기관 또는 심사기관 소속의 심사원 이상으로 선정하여야 한다.

③ 신청기관의 정보보호 관리체계 인증을 위한 컨설팅에 참여한 인증심사원 또는 신청기관의 소속직원은 인증심사팀의 구성원에서 배제하여야 한다.

제21조(인증심사 방법 및 보완조치) ① 인증심사는 신청기관을 방문하여 서면심사와 현장심사를 병행한다.

② 서면심사는 인증기준에 적합한지에 대하여 정보보호 관리체계 구축·운영 관련 정보보호 정책, 지침, 절차 및 이행의 증적자료 검토, 정보보호대책 적용 여부 확인 등의 방법으로 관리적 요소를 심사한다.

③ 현장심사는 서면심사의 결과와 기술적·물리적 보호대책 이행 여부를 확인하기 위하여 담당자 면담, 관련 시스템 확인 및 취약점 점검 등의 방법으로 기술적 요소를 심사한다.

④ 인터넷진흥원·인증기관 또는 심사기관은 인증심사에서 발견된 결함에 대해 최대 90일(재조치 요구 60일 포함) 이내에 보완조치를 완료하도록 신청기관에게 요청할 수 있다.

⑤ 인터넷진흥원 또는 인증기관은 인증위원회 심의결과에 따라 신청기관에 30일 이내에 보완조치를 요구할 수 있다. 심사기관은 인터넷진흥원 또는 인증기관으로부터 인증위원회 심의결과를 통보받아 신청기관에 30일 이내에 보완조치를 요구할 수 있다.

제6장 인증위원회 구성과 운영

제22조(인증위원회의 구성) ① 법 제47조제6항에 따라 인터넷진흥원 또는 인증기관의 장은 다음 각 호의 사항을 심의·의결하기 위하여 인증위원회를 설치·운영하여야 한다.

1. 최초심사 또는 갱신심사 결과가 인증기준에 적합한지 여부
2. 사후심사 결과 법 제47조제10항 각 호에 해당하는 사유를 발견한 경우에 그 결과의 적합성 여부
3. 그 밖에 정보보호 관리체계 인증과 관련하여 위원장이 필요하다고 인정하는 사항

② 인증위원회는 5인 이상 10인 이내의 위원으로 구성하되, 위원은 정보보호 전문가, 정보시스템감리사, 기술사, 교수 등 정보보호 분야에 학식과 경험이 있는 자 중에서 인터넷진흥원 또는 인증기관의 장이 위촉하며, 위원장은 위원 중에서 호선한다.

③ 위원장은 인증위원회의 업무를 통할하며 위원회를 대표한다.

제23조(인증위원회의 운영) ① 인터넷진흥원 또는 인증기관의 장은 인증위원회의 심의안건을 검토하여 위원회 개최 5일 전까지 인증위원회에 제출한다.

② 인증위원회 위원장은 제22조제1항 각 호의 사항에 대한 심의·의결 결과를 인터넷진흥원 또는 인증기관의 장에게 제출한다.

제7장 인증서의 발급·관리 및 홍보

제24조(인증서 발급) 인터넷진흥원 또는 인증기관의 장은 제23조제2항에 따라 인증위원회의 심의·의결 결과를 제출받은 때에는 신청기관의 정보보호 관리체계가 이 고시에서 정한 인증기준에 적합하다고 판단된 경우 별지 제14호서식의 정보보호 관리체계 인증서를 발급하여야 한다.

제25조(인증서 관리) ① 인터넷진흥원 또는 인증기관은 발급된 인증서의 인증번호, 발급일, 유효기간 등 인증서를 관리하여야 한다.

② 인증을 취득한 자는 인증서의 분실 등으로 인해 재발급을 받고자 할 경우 별지 제15호서식의 정보보호 관리체계 인증서 추가발급 신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

③ 인증을 취득한 자가 주소, 업체명 등 인증서 기재사항의 변경을 요청하고자 하는 경우 별지 제16호서식의 정보보호 관리체계 인증서 변경신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

제26조(인증의 표시 및 홍보) ① 영 제52조에 따른 인증의 표시는 별표 5와 같다.

② 제1항에 따른 인증의 표시를 사용하는 경우에는 영 제52조에 따라 인증의 범위와 유효기간을 함께 표시하여야 한다.

제8장 정보보호 관리체계 인증 수수료

제27조(수수료의 산정) ① 인증 수수료는 다음 각 호의 기준을 준용하되 별표 6의 정보보호 관리체계 인증 수수료 산정기준을 적용하여 산정한다.

1. 「엔지니어링산업 진흥법」 제31조제2항에 따른 엔지니어링사업의 대가 기준
2. 한국소프트웨어산업협회가 제공하는 「SW사업 대가산정 가이드」의 정보보안 컨설팅비

② 인터넷진흥원·인증기관 또는 심사기관은 제1항에 따라 산정된 인증 수수료를 공지하여야 한다. 다만, 「중소기업기본법」 제2조에 따른 중소기업이 인증을 신청하는 경우 수수료 감면 등 필요한 지원을 할 수 있다.

③ 인터넷진흥원·인증기관 또는 심사기관은 신청기관의 인증범위가 정보보호 관련 타 인증과 중복되거나 제17조에 따른 인증심사 일부를 생략하는 경우 신청기관과 협의하여 수수료를 조정할 수 있다.

제28조(수수료의 납부) ① 신청기관은 최초심사, 사후심사 및 갱신심사 신청 시 수수료를 납부한다. 다만, 수수료 납부 방법(일괄 또는 분할)은 인증심사 계약 시 신청기관과 협의하여 조정할 수 있다.

② 신청기관은 인증심사 계약을 체결한 날로부터 1개월 이내에 인증 수수료를 인터넷진흥원·인증기관 또는 심사기관에 납부하여야 한다.

제29조(인증업무 지침 등) ① 인터넷진흥원 또는 인증기관은 인증업무 수행을 위해 필요한 경우 인증업무에 관한 지침을 마련하여 시행할 수 있다.

② 심사기관은 인증심사업무 수행에 필요한 지침을 마련하여 시행할 수 있다.

제30조(재검토기한) 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제334호)에 따라 이 고시에 대하여 2017년 1월 1일 기준으로 매 3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2013-4호,2013.1.17>

제1조(시행일) 이 고시는 2013년 2월 18일부터 시행한다.

제2조(인증심사원에 관한 경과조치) 이 고시 시행 이전에 종전 고시에 따라 인증 심사업무를 전담하는 직원의 요건을 갖추고 인터넷진흥원으로부터 위촉된 자는 이 고시에 의한 인증심사원 자격을 취득한 것으로 본다.

부칙 <제2013-36호,2013.8.8>

제1조(시행일) 이 고시는 2013년 8월 8일부터 시행한다.

부칙 <제2016 - 38호,2016.4.8>

제1조(시행일) 이 고시는 공포한 날부터 시행한다.

부칙 <제2016 - 59호,2016.6.2>

제1조(시행일) 이 고시는 공포한 날부터 시행한다.

[별표 1]

업무수행 요건·능력 심사 규정에 따른 제출서류(제3조제2항·제3항 관련)

구 분	제 출 서 류
1. 정보보호 관리체계 인증심사 참여 실적을 확인하는 데 필요한 서류	가. 정보보호 관리체계 인증심사 참여실적 명세서 및 이를 증빙할 수 있는 자료 (인증심사 참여통지 문서 등) 나. 인증심사원 자격 증빙 자료
2. 업무수행 요건·능력 심사를 위하여 필요한 서류	가. 자본금 5억원 이상 내역(공인회계사 또는 회계담당자가 서명날인한 서류) 나. 부채비율 및 자기자본 이익률의 계산내역(회계결산내역 등 관련 증빙자료) 다. 인증업무 운영체계(인증기관에 해당) o 인증기관의 운영체계 및 인증의 품질관리 o 인증업무를 수행하는 직원에 대한 운영관리 등의 내부 규정 o 인증업무 수행 방법 및 절차 라. 심사업무 운영체계(심사기관에 해당) o 심사기관의 운영 체계 및 심사의 품질관리 o 심사업무를 수행하는 직원에 대한 운영관리 등의 내부 규정 o 심사업무 수행 방법 및 절차

[별표 2]

업무수행 요건·능력 심사 세부기준(제4조제1항 관련)

가. 업무수행 요건 심사 세부기준

평가항목	세부 평가 기준
1. 인증심사원 5명 이상 상시 고용 여부	o 인증심사원 5명 이상을 상시 고용하고 있어야 함 - 다만, 심사팀장급 심사원 1명 이상 확보해야 함
2. 인증기관 또는 심사기관 공정성 확보 여부	o 정보보호 관리체계 인증기관 또는 심사기관으로 지정을 받으려는 기관은 인증업무 또는 심사업무의 독립성, 객관성, 공정성, 신뢰성을 확보하기 위하여 정보보호 관리체계 구축과 관련된 컨설팅 업무를 수행하지 않아야 함

나. 인증기관 업무수행 능력 심사 세부기준

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td rowspan="5">1. 조직 및 직원들의 정보보호 전문성 (30)</td><td>전담조직</td><td>2</td><td>평가점수</td><td>o 인증에 관한 업무 전담조직 유무
<table><tr><th>전담조직 유무</th><th>점수</th></tr><tr><td>있음</td><td>2점</td></tr><tr><td>없음</td><td>0점</td></tr></table></td></tr>
<tr><td rowspan="4">정보보호 업무 전문성</td><td>10</td><td>평가점수</td><td>o 조직 내 인증심사원 상시 고용 인력 수
<table><tr><th>인증심사원 수</th><th>점수</th></tr><tr><td>10명 이상</td><td>배점의 100%</td></tr><tr><td>5명 이상 ~ 10명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (인증심사원 수/10명) × 100</td></tr></table></td></tr>
<tr><td>4</td><td>비율</td><td>o 정보보호 관련 박사학위 소지자·기술사 인력의 수
<table><tr><th>박사학위소지자기술사 수</th><th>점수</th></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (박사학위 소지자, 기술사 수/5명) × 100</td></tr></table></td></tr>
<tr><td>4</td><td>비율</td><td>o CISM, SIS, CISSP, CISA, CPPG, 정보보안기사/산업기사 자격증 소지자 수
<table><tr><th>자격증 소지자 수</th><th>점수</th></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (자격증 소지자 수/5명) × 100</td></tr></table></td></tr>
<tr><td>정보보호 관리체계 인증심사 참여실적</td><td>10</td><td>비율</td><td>o 상시 고용하고 있는 인증심사원이 최근 3년간 참여한 정보보호 관리체계 인증심사 참여 실적을 인정하고 평가점수는 개별 참여 실적을 합한 총 참여일수에 따라 산출
<table><tr><th>총 참여 일수(단위 : 일)</th><th>점수</th></tr><tr><td>200일 이상</td><td>배점의 100%</td></tr><tr><td>200일 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (총 참여일수/200일) × 100</td></tr></table></td></tr>
</table>

<table>
<tr><td>2. 시설(10)</td><td>사무공간·인증심사 서류 보관 창소 및 보안설비·시설 확보</td><td>10</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 인증심사의 상담, 인증심사 업무의 처리를 위해 필요한 사무실</td><td>2점</td></tr>
<tr><td>o 사무 관련 장비 확보</td><td>2점</td></tr>
<tr><td>o 사무실 출입자에 대한 신원확인 및 출입통제를 위한 설비</td><td>2점</td></tr>
<tr><td>o 기록물 및 자료의 안전한 관리를 위한 보관 창소</td><td>2점</td></tr>
<tr><td>o 인증심사 서류의 분실, 도난 등 예방을 위한 보안시설</td><td>2점</td></tr>
</table>
</td></tr>
<tr><td rowspan="2">3. 신뢰도 및 재정상태 건실도 (10)

※비영리기관 평가제외</td><td>부채비율</td><td>5</td><td>평가점수</td><td>o 지정 공고일 기준으로 직전년도 부채비율 (부채총계/자기자본)
<table>
<tr><th>비율</th><th>점수</th></tr>
<tr><td>50% 미만</td><td>5점</td></tr>
<tr><td>50% 이상 ~ 100% 미만</td><td>4점</td></tr>
<tr><td>100% 이상 ~ 150% 미만</td><td>3점</td></tr>
<tr><td>150% 이상 ~ 200% 미만</td><td>2점</td></tr>
<tr><td>200% 이상</td><td>1점</td></tr>
</table>
</td></tr>
<tr><td>자기자본 이익률</td><td>5</td><td>평가점수</td><td>o 지정 공고일 기준으로 직전년도 자기자본이익률 (당기순이익/자기자본)
<table>
<tr><th>비율</th><th>점수</th></tr>
<tr><td>20% 이상</td><td>5점</td></tr>
<tr><td>20% 미만 ~ 15% 이상</td><td>4점</td></tr>
<tr><td>15% 미만 ~ 10% 이상</td><td>3점</td></tr>
<tr><td>10% 미만 ~ 5% 이상</td><td>2점</td></tr>
<tr><td>5% 미만</td><td>1점</td></tr>
</table>
</td></tr>
<tr><td rowspan="3">4. 인증업무 운영 체계 (50)</td><td>인증기관의 운영 체계 및 인증의 품질관리</td><td>20</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 인증기관의 공정성·객관성·신뢰성·독립성 보증 방안</td><td>5점</td></tr>
<tr><td>o 인증기관의 내부감사 실시 및 검토 등에 대한 방안</td><td>5점</td></tr>
<tr><td>o 인증의 품질 보증 및 관리방안</td><td>5점</td></tr>
<tr><td>o 인증업무의 기록 및 문서화 관리체계의 적절성</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td>인증업무를 수행하는 직원에 대한 운영·관리 등의 내부 규정</td><td>10</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 인증업무를 수행하는 직원에 대한 규정 보유 및 그 규정의 타당성 및 실효성
- 인증업무를 수행하는 직원의 의무와 책임 등 준수사항
- 인증업무를 수행하는 직원의 자체 보안관리 및 감독 요령</td><td>5점</td></tr>
<tr><td>o 인증업무를 수행하는 직원의 교육 및 평가 등에 대한 방안 및 그 방안의 적절성 및 타당성</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td>인증업무 수행 방법 및 절차</td><td>10</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 심사업무 수행 방법 및 절차 등의 적절성 및 타당성</td><td>5점</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td></td><td>
<table>
<tr><td>- 인증심사의 절차 및 방법
- 인증수수료 및 그 징수방법
- 인증심사팀 구성 원칙
- 인증심사 사후관리방안 등</td><td></td></tr>
<tr><td>o 인증위원회 구성 및 운영
- 인증심사 결과의 공정성 확보를 위한 인증위원 구성 원칙
- 인증위원회 운영의 독립성·객관성이 확보 방안</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td></td><td>인증업무
지원체계</td><td>10</td><td>평가점수</td><td>
<table>
<tr><th>세부 평가요소</th><th>점수</th></tr>
<tr><td>o 운영자금 법인통장 보유 및 유지 수준</td><td>5점</td></tr>
<tr><td>o 지정취소, 부도·해산 등에 따른 신청기관 피해 보상 관련 대책마련 여부</td><td>5점</td></tr>
</table>
</td></tr>
<tr><td>5. 가점 및 감점</td><td>정보보호
관리체계
인증의 취득 및 유지</td><td>2
(가점)</td><td>인증
취득 및
유지</td><td>o 정보보호 관리체계 인증을 취득하고, 인증을 유지하고 있을 때</td></tr>
<tr><td></td><td>자격취소 사실</td><td>5
(감점)</td><td>취소사실
및
취소회수</td><td>o 지정 공고일 기준으로 10년 이내에 미래창조과학부가 부여한 정보보호 관련 수행자격이 취소된 경우
- 정보보호 관리체계 인증기관, 안전진단 수행기관 등
※ 취소 1회당 : 감점 5점</td></tr>
</table>

<비 고>

1. 평가항목에 대한 각 평가요소별 세부평가 점수는 소수점 이하 둘째 자리에서 반올림한다.
2. 평가항목에 대한 각 평가요소별 평가점수는 평가결과의 최저점과 최고점을 제외한 점수들의 평균점을 부여한다. 다만, 최저점 또는 최고점이 2개 이상일 경우 각 1개만 제외한다.
3. 가점을 합한 점수가 100점을 초과해도 만점 100점으로 표기한다.
4. '시설', '인증업무 운영체계'에 대한 각 평가요소별 세부평가 점수 부여기준은 각 평가요소의 평가결과에 평가등급(계수)를 곱하여 나온 점수를 합산한다.

평가요소별 세부평가 점수	평가등급(계수)
100점 이하 ~ 90점 이상	우수(1.0)
90점 미만 ~ 80점 이상	보통(0.6)
80점 미만 ~	미흡(0.2)
미 제출	점수없음(0)

다. 심사기관 업무수행 능력심사 세부기준

<table>
<tr><th>평가항목</th><th>평가요소</th><th>배점</th><th>평가지표</th><th>세부 평가방법</th></tr>
<tr><td rowspan="5">1. 조직 및 직원들의 정보보호 전문성 (30)</td><td>전담조직</td><td>2</td><td>평가점수</td><td>o 심사업무 전담조직 유무
<table><tr><th>전담조직 유무</th><th>점수</th></tr><tr><td>있음</td><td>2점</td></tr><tr><td>없음</td><td>0점</td></tr></table></td></tr>
<tr><td rowspan="3">정보보호 업무 전문성</td><td>10</td><td>평가점수</td><td>o 조직 내 인증심사원 상시 고용 인력 수
<table><tr><th>인증심사원 수</th><th>점수</th></tr><tr><td>10명 이상</td><td>배점의 100%</td></tr><tr><td>5명 이상 ~ 10명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (인증심사원 수/10명) × 100</td></tr></table></td></tr>
<tr><td>4</td><td>비율</td><td>o 정보보호 관련 박사학위 소지자 · 기술사 인력의 수
<table><tr><th>박사학위소지자·기술사 수</th><th>점수</th></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (박사학위 소지자, 기술사 수/5명) × 100</td></tr></table></td></tr>
<tr><td>4</td><td>비율</td><td>o CISM, SIS, CISSP, CISA, CPPG, 정보보안기사/산업기사 자격증 소지자 수
<table><tr><th>자격증 소지자 수</th><th>점수</th></tr><tr><td>5명 이상</td><td>배점의 100%</td></tr><tr><td>5명 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (자격증 소지자 수/5명) × 100</td></tr></table></td></tr>
<tr><td>정보보호 관리체계 인증심사 참여실적</td><td>10</td><td>비율</td><td>o 상시 고용하고 있는 인증심사원이 최근 3년간 참여한 정보보호 관리체계 인증심사 참여 실적을 인정하고 평가점수는 개별 참여 실적을 합한 총 참여일수에 따라 산출
<table><tr><th>총 참여 일수(단위 : 일)</th><th>점수</th></tr><tr><td>200일 이상</td><td>배점의 100%</td></tr><tr><td>200일 미만</td><td>배점의 X%</td></tr><tr><td colspan="2">※ X = (총 참여일수/200일) × 100</td></tr></table></td></tr>
<tr><td>2. 시설(10)</td><td>사무공간·인증심사 서류 보관 창소 및 보안설비·시설 확보</td><td>10</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 인증심사의 상담, 인증심사 업무의 처리를 위해 필요한 사무실</td><td>2점</td></tr><tr><td>o 사무 관련 장비 확보</td><td>2점</td></tr><tr><td>o 사무실 출입자에 대한 신원확인 및 출입통제를 위한 설비</td><td>2점</td></tr><tr><td>o 기록물 및 자료의 안전한 관리를 위한 보관 창소</td><td>2점</td></tr><tr><td>o 인증심사 서류의 분실, 도난 등 예방을 위한 보안시설</td><td>2점</td></tr></table></td></tr>
<tr><td>3. 신뢰도 및 재정상태 건실도 (10)</td><td>부채비율</td><td>5</td><td>평가점수</td><td>o 지정 공고일 기준으로 직전년도 부채비율
(부채총계/자기자본)</td></tr>
</table>

<table>
<tr><td>※비영리기관
평가제외</td><td></td><td></td><td></td><td><table><tr><th>비율</th><th>점수</th></tr><tr><td>50% 미만</td><td>5점</td></tr><tr><td>50% 이상 ~ 100% 미만</td><td>4점</td></tr><tr><td>100% 이상 ~ 150% 미만</td><td>3점</td></tr><tr><td>150% 이상 ~ 200% 미만</td><td>2점</td></tr><tr><td>200% 이상</td><td>1점</td></tr></table></td></tr>
<tr><td></td><td>자기자본
이익률</td><td>5</td><td>평가점수</td><td>o 지정 공고일 기준으로 직전년도 자기자본이익률
(당기순이익/자기자본)<table><tr><th>비율</th><th>점수</th></tr><tr><td>20% 이상</td><td>5점</td></tr><tr><td>20% 미만 ~ 15% 이상</td><td>4점</td></tr><tr><td>15% 미만 ~ 10% 이상</td><td>3점</td></tr><tr><td>10% 미만 ~ 5% 이상</td><td>2점</td></tr><tr><td>5% 미만</td><td>1점</td></tr></table></td></tr>
<tr><td>4. 심사업무
운영 체계
(50)</td><td>심사기관의
운영 체계 및
심사의
품질관리</td><td>20</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 심사기관의 공정성과 객관성 신뢰성 독립성 보증 방안</td><td>5점</td></tr><tr><td>o 심사기관의 내부감사 실시 및 검토 등에 대한 방안</td><td>5점</td></tr><tr><td>o 심사의 품질 보증 및 관리방안</td><td>5점</td></tr><tr><td>o 심사업무의 기록 및 문서화 관리체계의 적절성</td><td>5점</td></tr></table></td></tr>
<tr><td></td><td>심사업무를
수행하는
직원에 대한
운영관리
등의 내부
규정</td><td>10</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 심사업무를 수행하는 직원에 대한 규정 보유 및 그 규정의 타당성 및 실효성
- 심사업무를 수행하는 직원의 의무와 책임 등 준수사항
- 심사업무를 수행하는 직원의 자체 보안관리 및 감독 요령</td><td>5점</td></tr><tr><td>o 심사업무를 수행하는 직원의 교육 및 평가 등에 대한 방안 및 그 방안의 적절성 및 타당성</td><td>5점</td></tr></table></td></tr>
<tr><td></td><td>심사업무
수행 방법 및
절차</td><td>10</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 심사업무 수행 방법 및 절차 등의 적절성 및 타당성
- 인증심사의 절차 및 방법
- 인증수수료 및 그 징수방법
- 인증심사팀 구성 원칙
- 인증심사 사후관리방안 등</td><td>10점</td></tr></table></td></tr>
<tr><td></td><td>심사업무
지원체계</td><td>10</td><td>평가점수</td><td><table><tr><th>세부 평가요소</th><th>점수</th></tr><tr><td>o 운영자금 법인통장 보유 및 유지 수준</td><td>5점</td></tr><tr><td>o 지정취소, 부도·해산 등에 따른 신청기관 피해보상 관련 대책마련 여부</td><td>5점</td></tr></table></td></tr>
<tr><td>5. 가점 및 감점</td><td>정보보호
관리체계
인증의 취득
및 유지</td><td>2
(가점)</td><td>인증
취득 및
유지</td><td>o 정보보호 관리체계 인증을 취득하고, 인증을 유지하고 있을 때</td></tr>
<tr><td></td><td>자격취소 사실</td><td>5
(감점)</td><td>취소사실
및
취소회수</td><td>o 지정 공고일 기준으로 10년 이내에 미래창조과학부가 부여한 정보보호 관련 수행자격이 취소된 경우
- 정보보호 관리체계 인증기관, 안전진단 수행기관 등
※ 취소 1회당 : 감점 5점</td></tr>
</table>

<비 고>

1. 평가항목에 대한 각 평가요소별 세부평가 점수는 소수점 이하 둘째 자리에서 반올림한다.
2. 평가항목에 대한 각 평가요소별 평가점수는 평가결과의 최저점과 최고점을 제외한 점수들의 평균점을 부여한다. 다만, 최저점 또는 최고점이 2개 이상일 경우 각 1개만 제외한다.

3. 가점을 합한 점수가 100점을 초과해도 만점 100점으로 표기한다.
4. '시설', '심사업무 운영체계'에 대한 각 평가요소별 세부평가 점수 부여기준은 각 평가요소의 평가결과에 평가등급(계수)를 곱하여 나온 점수를 합산한다.

평가요소별 세부평가 점수	평가등급(계수)
100점 이하 ~ 90점 이상	우수(1.0)
90점 미만 ~ 80점 이상	보통(0.6)
80점 미만 ~	미흡(0.2)
미 제출	점수없음(0)

[별표 3]

인증심사원 자격 요건(제9조 관련)

1. 인증심사원 등급별 자격 요건

구 분	자격 요건
심사원보	o 인증심사원 학력 및 경력요건을 만족하는 자로서 인터넷진흥원이 지정하는 기관에서 인증심사원 양성교육 과정을 수료한 자
심사원	o 심사원보 자격 취득자로서 인증심사 4회 이상 참여하고 심사일수의 합이 20일 이상인 자
선임심사원	o 심사원 자격 취득자로서 3회 이상 심사 총괄업무를 수행하고 심사일수의 합이 15일 이상인 자

2. 인증심사원 학력 및 경력 요건

o 학사학위를 취득한 후 정보통신 또는 정보보호 유관경력 6년(전문학사의 경우 8년, 수업연한이 3년인 전문학사의 경우 7년, 고등학교 졸업자의 경우 10년을 말한다) 이상을 보유한 자(최근 10년 이내의 경력에 한함)

o 유관자격 소지자 또는 유관학력을 취득한 자로서 다음 각 목의 어느 하나에 해당하는 경우 정보통신 유관경력을 인정한다.
가. 기술사 자격 소지자 또는 박사 학위를 취득한 자의 경우 3년
나. 기사 자격 소지자 또는 석사 학위를 취득한 자의 경우 2년
다. 산업기사 자격 소지자 또는 학사 학위를 취득한 자의 경우 1년

o 다음 각 목의 어느 하나에 해당하는 자격을 취득한 자는 정보통신 또는 정보보호 유관경력 1년을 추가 인정한다.
가. 한국인터넷진흥원 정보보호전문가(SIS)
나. 전자정부법 제60조에 따른 감리원
다. 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 정보시스템감사사(CISA)
라. 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 정보시스템보호전문가(CISSP)

<비 고>
1. "정보통신 유관경력", "정보보호 유관경력", "유관자격" 및 "유관학력"은 영 별표 2 "정보보호 기술인력의 자격 기준"을 준용한다.

[별표 4]

정보보호 관리체계 인증심사 일부 생략의 범위(제17조 관련)

<table>
<tr><th>인증 또는 정보보호 조치</th><th>정보보호 관리체계 인증심사 생략범위</th></tr>
<tr><td>국제표준 정보보호경영시스템 인증</td><td>나. 정보보호대책
<table>
<tr><td>1.1 정책의 승인 및 공표</td><td>1.3 정책의 유지관리</td></tr>
<tr><td>2.2 역할 및 책임</td><td>3.1 보안 요구사항의 정의</td></tr>
<tr><td>3.2 외부자 보안 이행</td><td>4.1 정보자산 식별 및 책임</td></tr>
<tr><td>4.2 정보자산의 분류 및 취급</td><td>5.1 교육 프로그램 수립</td></tr>
<tr><td>6.1 정보보호 책임</td><td>6.2 인사규정</td></tr>
<tr><td>7.1 물리적 보호구역</td><td>7.2 시스템 보호</td></tr>
<tr><td>7.3 사무실 환경보안</td><td>8.1 분석 및 설계 보안관리</td></tr>
<tr><td>8.3 외부개발 보안</td><td>9.1 암호정책</td></tr>
<tr><td>9.2 암호키 관리</td><td>10.1 접근통제 정책</td></tr>
<tr><td>11.4 매체보안</td><td>11.6 로그관리 및 모니터링</td></tr>
<tr><td>12.1 절차 및 체계</td><td>12.2 대응 및 복구</td></tr>
<tr><td>13.1 체계구축</td><td>13.2 대책구현</td></tr>
</table></td></tr>
<tr><td>개인정보보호 관리체계 인증</td><td>나. 정보보호대책
<table>
<tr><td>1.1 정책의 승인 및 공표</td><td>1.3 정책의 유지관리</td></tr>
<tr><td>2.1 조직체계</td><td>2.2 역할 및 책임</td></tr>
<tr><td>5.1 교육프로그램 수립</td><td>5.2 교육시행 및 평가</td></tr>
<tr><td>6.1 정보보호 책임</td><td>7.1 물리적 보호구역</td></tr>
<tr><td>7.2 시스템 보호</td><td>7.3 사무실 환경보안</td></tr>
<tr><td>9.1 암호정책</td><td>9.2 암호키 관리</td></tr>
<tr><td>10.1 접근통제 정책</td><td>11.1 운영절차 및 변경관리</td></tr>
<tr><td>11.4 매체관리</td><td>11.6 로그관리 및 모니터링</td></tr>
<tr><td>12.1 절차 및 체계</td><td>12.2 대응 및 복구</td></tr>
</table></td></tr>
<tr><td>「정보통신기반 보호법」 제9조에 따른 취약점의 분석·평가</td><td>나. 정보보호대책
<table>
<tr><td>1.3 정책의 유지관리</td><td>2.1 조직체계</td></tr>
<tr><td>3.1 보안요구사항의 정의</td><td>3.2 외부자보안 이행</td></tr>
<tr><td>4.1 정보자산식별 및 책임</td><td>4.2 정보자산의 분류 및 취급</td></tr>
<tr><td>5.1 교육프로그램 수립</td><td>6.1 정보보호 책임</td></tr>
<tr><td>7.1 물리적 보호구역</td><td>7.2 시스템 보호</td></tr>
<tr><td>8.2 구현 및 이관보안</td><td>10.1 접근통제 정책</td></tr>
<tr><td>10.3 식별 및 인증</td><td>12.1 절차 및 체계</td></tr>
</table></td></tr>
</table>

[별표 5]

정보보호 관리체계 인증의 표시(제26조 관련)

□ 출입구 부착용

1. 도안모형



2. 인증명판 제작 유의사항

가. 소재는 가급적 동판으로 제작한다(전체 두께 1.0㎝, 바탕 0.4㎝, 테두리 폭 0.5㎝)

나. 바탕색은 가급적 연마하지 않은 황동색으로 한다

다. 도안 모형은 인증의 표시를 중앙에 둔다

라. 글씨 및 도형은 양각으로 한다.

마. 크기는 사각형으로 하며 인증마크는 중앙에 위치하도록 하며 가로와 세로 비율을 3 : 2로 하여 일정 비율로 조정할 수 있다

□ 서류 등 표시용

1. 도안모형



2. 도안 및 표시방법

가. 'Information Security Management System'은 검청색으로, '정보보호 관리체계 인증'은 군청색으로 한다. 게시장소의 칼라표시가 불합리한 경우에는 흑백으로 할 수 있다.

나. 마크의 크기는 제품과 그 제품의 포장 또는 용기의 크기에 따라 일정 비율로 조정할 수 있다.

[별표 6]

정보보호 관리체계 인증 수수료 산정기준(제27조 관련)

1. 인증 수수료 산정 방식

인증 수수료 = 직접인건비 + 직접경비 + 제경비 + 기술료

① 직접인건비는 인증심사에 투입되는 인증심사원에 대한 인건비로 산정한다. 인건비는 SW사업 대가 산정 가이드의 정보보안 컨설팅비를 준용한다

인증심사원 등급	컨설턴트 등급
선임심사원	선임 컨설턴트 이상
심사원	
심사원보	컨설턴트

② 직접경비는 인증심사업무의 수행에 따라 발생하는 교통비, 숙박비 및 식대 등 인증심사업무에 소요되는 직접적인 경비를 산정한다.

③ 제경비는 최대 (직접인건비×120%) 로 산정한다.

④ 기술료는 최대 {(직접인건비+제경비)×40% } 로 산정한다.

[별표 7]

정보보호 관리체계 인증기준(제19조 관련)

가. 정보보호관리과정

	관리과정		세부관리과정	관리과정 상세내용
1	정보보호정책 수립 및 범위설정	1.1	정보보호정책의 수립	조직이 수행하는 모든 정보보호 활동의 근거를 포함할 수 있도록 정보보호정책을 수립하고 동 정책은 국가나 관련 산업에서 정하는 정보보호 관련 법, 규제를 만족하여야 한다.
		1.2	범위설정	조직에 미치는 영향을 고려하여 중요한 업무, 서비스, 조직, 자산 등을 포함할 수 있도록 정보보호 관리체계 범위를 설정하고 범위 내 모든 자산을 식별하여 문서화하여야 한다.
2	경영진 책임 및 조직구성	2.1	경영진 참여	정보보호 관리체계 수립 및 운영 등 조직이 수행하는 정보보호 활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여야 한다.
		2.2	정보보호 조직 구성 및 자원 할당	최고경영자는 조직의 규모, 업무 중요도 분석을 통해 정보보호 관리체계의 지속적인 운영이 가능하도록 정보보호 최고책임자, 실무조직 등 정보보호 조직을 구성하고 정보보호 관리체계 운영 활동을 수행하는데 필요한 자원(예산 및 인력)을 확보하여야 한다.
3	위험관리	3.1	위험관리 방법 및 계획 수립	관리적, 기술적, 물리적, 법적 분야 등 조직의 정보보호 전 영역에 대한 위험식별 및 평가가 가능하도록 위험관리 방법을 선정하고 위험관리의 전문성을 보장할 수 있도록 수행인원, 기간, 대상, 방법 등을 구체적으로 포함한 위험관리계획을 사전에 수립하여야 한다.
		3.2	위험식별 및 평가	위험관리 방법 및 계획에 따라 정보보호 전 영역에 대한 위험 식별 및 평가를 연 1회 이상 수행하고 그 결과에 따라 조직에서 수용 가능한 위험수준을 설정하여 관리하여야 한다.

	관리과정		세부관리과정	관리과정 상세내용
3	위험관리	3.3	정보보호대책 선정 및 이행계획 수립	위험을 수용 가능한 수준으로 감소시키기 위해 정보보호대책을 선정하고 그 보호대책의 구현 우선순위, 일정, 담당부서 및 담당자 지정, 예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.
4	정보보호대책 구현	4.1	정보보호대책의 효과적 구현	정보보호대책 이행계획에 따라 보호대책을 구현하고 경영진은 이행결과의 정확성 및 효과성 여부를 확인하여야 한다.
		4.2	내부 공유 및 교육	구현된 정보보호대책을 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여야 한다.
5	사후관리	5.1	법적요구사항 준수검토	조직이 준수해야 할 정보보호 관련 법적요구사항을 지속적으로 파악하여 최신성을 유지하고 준수여부를 지속적으로 검토하여야 한다.
		5.2	정보보호 관리체계 운영현황 관리	정보보호 관리체계 범위 내에서 주기적 또는 상시적으로 수행해야 하는 활동을 문서화하고 그 운영현황을 지속적으로 관리하여야 한다.
		5.3	내부감사	조직은 정보보호 관리체계가 정해진 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는 지를 점검하기 위하여 연 1회 이상 내부감사를 수행하여야 한다. 이를 위해 감사기준, 범위, 주기, 방법 등을 구체적으로 정하고 내부감사를 통해 발견된 문제점은 보완조치를 완료하여 경영진 및 관련 책임자에게 보고하여야 한다. 또한 감사의 독립성 및 전문성을 확보할 수 있도록 감사인력에 대한 자격요건을 정의하여야 한다.

나. 정보보호대책

	통제분야		통제목적		통제사항	통제내용
1	정보보호 정책	1.1	정책의 승인 및 공표	1.1.1	정책의 승인	정보보호정책은 이해관련자의 검토와 최고경영자의 승인을 받아야 한다.
				1.1.2	정책의 공표	정보보호정책 문서는 모든 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.
		1.2	정책의 체계	1.2.1	상위 정책과의 연계성	정보보호정책은 상위조직 및 관련 기관의 정책과 연계성을 유지하여야 한다.
				1.2.2	정책시행 문서수립	정보보호정책의 구체적인 시행을 위한 정보보호지침, 절차를 수립하고 관련 문서간의 일관성을 유지하여야 한다.
		1.3	정책의 유지관리	1.3.1	정책의 검토	정기적으로 정보보호정책 및 정책 시행문서의 타당성을 검토하고, 중대한 보안사고 발생, 새로운 위협 또는 취약성의 발견, 정보보호 환경에 중대한 변화 등이 정보보호정책에 미치는 영향을 분석하여 필요한 경우 제·개정하여야 한다.
				1.3.2	정책문서 관리	정보보호정책 및 정책 시행문서의 이력관리를 위해 제정, 개정, 배포, 폐기 등의 관리절차를 수립하고 문서는 최신본으로 유지하여야 한다. 또한 정책문서 시행에 따른 운영기록을 생성하여 유지하여야 한다.
2	정보보호 조직	2.1	조직 체계	2.1.1	정보보호 최고 책임자 지정	최고경영자는 임원급의 정보보호 최고책임자를 지정하고 정보보호 최고책임자는 정보보호정책 수립, 정보보호 조직 구성, 위험관리, 정보보호위원회 운영 등의 정보보호에 관한 업무를 총괄 관리하여야 한다.

	통제분야		통제목적		통제사항	통제내용
2	정보보호 조직	2.1	조직의 체계	2.1.2	실무조직 구성	최고경영자는 정보보호 최고책임자의 역할을 지원하고 조직의 정보보호 활동을 체계적으로 이행하기 위해 실무조직을 구성하고 조직 구성원의 정보보호 전문성을 고려하여 구성한다.
				2.1.3	정보보호 위원회	정보보호 자원할당 등 조직 전반에 걸친 중요한 정보보호 관련사항에 대한 검토 및 의사결정을 할 수 있도록 정보보호위원회를 구성하여 운영하여야 한다.
		2.2	역할 및 책임	2.2.1	역할 및 책임	정보보호 최고책임자와 정보보호 관련 담당자에 대한 역할 및 책임을 정의하고 그 활동을 평가할 수 있는 체계를 마련하여야 한다.
3	외부자 보안	3.1	보안 요구사항 정의	3.1.1	외부자 계약 시 보안요구사항	조직의 정보처리 업무를 외부자에게 위탁하거나 정보자산에 대한 접근을 허용할 경우, 또는 업무를 위해 클라우드 서비스 등 외부 서비스를 이용하는 경우에는 보안요구사항을 식별하고 관련 내용을 계약서 및 협정서 등에 명시하여야 한다.
		3.2	외부자 보안 이행	3.2.1	외부자 보안 이행 관리	외부자가 계약서 및 협정서에 명시된 보안요구사항의 이행여부를 관리 감독하고 주기적인 점검 또는 감사를 수행하여야 한다.
				3.2.2	외부자 계약 만료 시 보안	외부자와의 계약 만료, 업무 종료, 담당자 변경 시 조직이 외부자에게 제공한 정보자산의 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 업무 수행 시 알게 된 정보의 비밀유지 확약서 등의 내용을 확인하여야 한다.

	통제분야		통제목적		통제사항	통제내용
4	정보자산 분류	4.1	정보자산 식별 및 책임	4.1.1	정보자산 식별	조직의 업무특성에 따라 정보자산 분류기준을 수립하고 정보보호 관리체계 범위 내 모든 정보자산을 식별하여야 한다. 또한 식별된 정보자산을 목록으로 관리하여야 한다.
				4.1.2	정보자산별 책임할당	식별된 정보자산에 대한 책임자 및 관리자를 지정하여 책임소재를 명확히 하여야 한다.
		4.2	정보자산의 분류 및 취급	4.2.1	보안등급과 취급	기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 정보자산이 조직에 미치는 중요도를 평가하고 그 중요도에 따라 보안등급을 부여하여야 한다. 또한 보안등급을 표시하고 등급 부여에 따른 취급절차를 정의하여 이행하여야 한다.
5	정보보호 교육	5.1	교육 프로그램 수립	5.1.1	교육 계획	교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 정보보호 교육 계획을 수립하여야 한다.
				5.1.2	교육 대상	교육 대상에는 정보보호 관리체계 범위 내 임직원 및 외부자를 모두 포함하여야 한다.
				5.1.3	교육 내용 및 방법	교육에는 정보보호 및 정보보호 관리체계 개요, 보안사고 사례, 내부 규정 및 절차, 법적 책임 등의 내용을 포함하고 일반 임직원, 책임자, IT 및 정보보호 담당자 등 각 직무별 전문성 제고에 적합한 교육내용 및 방법을 정하여야 한다.
		5.2	교육 시행 및 평가	5.2.1	교육 시행 및 평가	정보보호 관리체계 범위 내 임직원 및 외부자를 대상으로 연 1회 이상 교육을 시행하고 정보보호 정책 및 절차의 중대한 변경, 조직 내·외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생할 경우 추가 교육을 수행하여야 한다. 또한 교육 시행에 대한 기록을 남기고 평가하여야 한다.

	통제분야		통제목적		통제사항	통제내용
6	인적 보안	6.1	정보보호 책임	6.1.1	주요 직무자 지정 및 감독	인사정보, 영업비밀, 산업기밀, 개인정보 등 중요정보를 대량으로 취급하는 임직원의 경우 주요직무자로 지정하고 주요직무자 지정을 최소화 하는 등 관리할 수 있는 보호대책을 수립하여야 한다.
				6.1.2	직무 분리	권한 오남용 등 고의적인 행위로 인해 발생할 수 있는 잠재적인 피해를 줄이기 위하여 직무 분리 기준을 수립하고 적용하여야 한다. 다만 인적 자원 부족 등 불가피하게 직무분리가 어려운 경우 별도의 보완통제를 마련하여야 한다.
				6.1.3	비밀유지 서약서	임직원으로부터 비밀유지 서약서를 받아야 하고 임시직원이나 외부자에게 정보시스템에 대한 접근권한을 부여할 경우에도 비밀유지서약서를 받아야 한다.
		6.2	인사규정	6.2.1	퇴직 및 직무변경 관리	퇴직 및 직무변경 시 인사부서와 정보보호 및 시스템 운영 부서 등 관련 부서에서 이행해야 할 자산반납, 접근권한 회수·조정, 결과 확인 등의 절차를 수립하여야 한다.
				6.2.2	상벌규정	인사규정에 직원이 정보보호 책임과 의무를 충실히 이행했는지 여부 등 정보보호 활동 수행에 따른 상벌 규정을 포함하여야 한다.

	통제분야		통제목적		통제사항	통제내용
7	물리적 보안	7.1	물리적 보호구역	7.1.1	보호구역 지정	비인가자의 물리적 접근 및 각종 물리적, 환경적 재난으로부터 주요 설비 및 시스템을 보호하기 위하여 통제구역, 제한구역, 접견구역 등 물리적 보호구역을 지정하고 각 구역별 보호대책을 수립·이행하여야 한다.
				7.1.2	보호설비	각 보호구역의 중요도 및 특성에 따라 화재, 전력이상 등 인·재해에 대비하여 온습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 설비를 충분히 갖추고 운영절차를 수립하여 운영하여야 한다. 또한 주요 시스템을 외부 집적정보통신시설에 위탁운영하는 경우 관련 요구사항을 계약서에 반영하고 주기적으로 검토를 수행하여야 한다.
				7.1.3	보호구역 내 작업	유지보수 등 주요 설비 및 시스템이 위치한 보호구역 내에서의 작업 절차를 수립하고 작업에 대한 기록을 주기적으로 검토하여야 한다.
				7.1.4	출입통제	보호구역 및 보호구역 내 주요 설비 및 시스템은 인가된 사람만이 접근할 수 있도록 출입을 통제하고 책임추적성을 확보할 수 있도록 출입 및 접근 이력을 주기적으로 검토하여야 한다.
				7.1.5	모바일 기기 반출입	노트북 등 모바일 기기 미승인 반출입을 통한 중요정보 유출, 내부망 악성코드 감염 등의 보안사고 예방을 위하여 보호구역 내 임직원 및 외부자 모바일 기기 반출입 통제절차를 수립하고 기록·관리하여야 한다.
		7.2	시스템 보호	7.2.1	케이블 보안	데이터를 송수신하는 통신케이블이나 전력을 공급하는 전력 케이블은 손상을 입지 않도록 보호하여야 한다.
				7.2.2	시스템 배치 및 관리	시스템은 그 특성에 따라 분리하여 배치하고 장애 또는 보안사고 발생 시 주요 시스템의 위치를 즉시 확인할 수 있는 체계를 수립하여야 한다.

	통제분야		통제목적		통제사항	통제내용
		7.3	사무실 보안	7.3.1	개인업무 환경 보안	일정시간 동안 자리를 비울 경우에는 책상 위에 중요한 문서나 저장매체를 남겨놓지 않고 컴퓨터 화면에 중요정보가 노출되지 않도록 화면보호기 설정, 패스워드 노출 금지 등 보호대책을 수립하여야 한다.
				7.3.2	공용업무 환경 보안	사무실에서 공용으로 사용하는 사무처리 기기, 문서고, 공용 PC, 파일서버 등을 통해 중요정보 유출이 발생하지 않도록 보호대책을 마련하여야 한다.
8	시스템 개발보안	8.1	분석 및 설계 보안관리	8.1.1	보안 요구사항 정의	신규 정보시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안취약점, 정보보호 기본요소(기밀성, 무결성, 가용성) 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용하여야 한다.
				8.1.2	인증 및 암호화 기능	정보시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입·출력 및 송수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다.
				8.1.3	보안로그 기능	정보시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 하여야 한다.
				8.1.4	접근권한 기능	정보시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다.

	통제분야		통제목적		통제사항	통제내용
8	시스템 개발 보안	8.2	구현 및 이관 보안	8.2.1	구현 및 시험	안전한 코딩방법에 따라 정보시스템을 구현 하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다. 또한 알려진 기술적 보안 취약성에 대한 노출여부를 점검하고 이에 대한 보안대책을 수립하여야 한다.
				8.2.2	개발과 운영 환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다.
				8.2.3	운영환경 이관	운영환경으로의 이관은 통제된 절차에 따라 이루어져야 하고 실행코드는 시험과 사용자 인수 후 실행하여야 한다.
				8.2.4	시험 데이터 보안	시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다.
				8.2.5	소스 프로그램 보안	소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행하여야 한다. 또한 소스 프로그램은 운영환경에 보관하지 않는 것을 원칙으로 한다.
		8.3	외주개발 보안	8.3.1	외주개발 보안	정보시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독하여야 한다.

	통제분야		통제목적		통제사항	통제내용
9	암호통제	9.1	암호 정책	9.1.1	암호 정책 수립	조직의 중요정보 보호를 위하여 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 수립하고 이행하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.
		9.2	암호키 관리	9.2.1	암호키 생성 및 이용	암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고 필요 시 복구방안을 마련하여야 한다.
10	접근 통제	10.1	접근통제 정책	10.1.1	접근통제 정책 수립	비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다.
		10.2	접근권한 관리	10.2.1	사용자 등록 및 권한부여	정보시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다.
				10.2.2	관리자 및 특수 권한 관리	정보시스템 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.
				10.2.3	접근권한 검토	정보시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 점검하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.3	사용자 인증 및 식별	10.3.1	사용자 인증	정보시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제되어야 하고, 필요한 경우 법적요구사항 등을 고려하여 중요 정보시스템 접근 시 강화된 인증방식을 적용하여야 한다.
				10.3.2	사용자 식별	정보시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다. 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.
				10.3.3	사용자 패스워드 관리	법적요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경주기 등 사용자 패스워드 관리절차를 수립·이행하고 패스워드 관리 책임이 사용자에게 있음을 주지시켜야 한다. 특히 관리자 패스워드는 별도 보호대책을 수립하여 관리하여야 한다.
				10.3.4	이용자 패스워드 관리	고객, 회원 등 외부 이용자가 접근하는 정보시스템 또는 웹서비스의 안전한 이용을 위하여 계정 및 패스워드 등의 관리절차를 마련하고 관련 내용을 공지하여야 한다.
		10.4	접근통제 영역	10.4.1	네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 접근통제 리스트, 네트워크 식별자 등에 대한 관리절차를 수립하고 서비스, 사용자 그룹, 정보자산의 중요도에 따라 내·외부 네트워크를 분리하여야 한다.
				10.4.2	서버 접근	서버별로 접근이 허용되는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 적용하여야 한다.

	통제분야		통제목적		통제사항	통제내용
10	접근통제	10.4	접근통제 영역	10.4.3	응용 프로그램 접근	사용자의 업무 또는 직무에 따라 응용프로그램 접근권한을 제한하고 불필요한 중요정보 노출을 최소화해야 한다.
				10.4.4	데이터베이스 접근	데이터베이스 접근을 허용하는 응용프로그램 및 사용자 직무를 명확하게 정의하고 응용프로그램 및 직무별 접근통제 정책을 수립하여야 한다. 또한 중요정보를 저장하고 있는 데이터베이스의 경우 사용자 접근내역을 기록하고 접근의 타당성을 정기적으로 검토하여야 한다.
				10.4.5	모바일 기기 접근	모바일기기를 업무 목적으로 내·외부 네트워크에 연결하여 활용하는 경우 중요정보 유출 및 침해사고 예방을 위해 기기 인증 및 승인, 접근 범위, 기기 보안설정, 오남용 모니터링 등의 접근통제 대책을 수립하여야 한다.
				10.4.6	인터넷 접속	인사정보, 영업비밀, 산업기밀, 개인정보 등 중요정보를 대량으로 취급·운영하는 주요직무자의 경우 인터넷 접속 또는 서비스(P2P, 웹메일, 웹하드, 메신저 등)를 제한하고 인터넷 접속은 침입차단시스템을 통해 통제하여야 한다. 필요시 침입탐지시스템 등을 통해 인터넷 접속내역을 모니터링하여야 한다.
11	운영보안	11.1	운영 절차 및 변경 관리	11.1.1	운영절차 수립	정보시스템 동작, 문제 발생 시 재 동작 및 복구, 오류 및 예외사항 처리 등 시스템 운영을 위한 절차를 수립하여야 한다.
				11.1.2	변경관리	정보시스템 관련 자산의 모든 변경내역을 관리할 수 있도록 절차를 수립하고 변경 전 시스템의 전반적인 성능 및 보안에 미치는 영향을 분석하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영보안	11.2	시스템 및 서비스 운영 보안	11.2.1	정보 시스템 인수	새로운 정보시스템 도입 또는 개선 시 필수 보안요구사항을 포함한 인수 기준을 수립하고 인수 전 기준 적합성을 검토하여야 한다.
				11.2.2	보안 시스템 운영	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립하고 보안시스템 별 정책적용 현황을 관리하여야 한다.
				11.2.3	성능 및 용량관리	정보시스템 및 서비스 가용성 보장을 위해 성능 및 용량 요구사항을 정의하고 현황을 지속적으로 모니터링할 수 있는 방법 및 절차를 수립하여야 한다.
				11.2.4	장애관리	정보시스템 장애 발생 시 효과적으로 대응하기 위한 탐지, 기록, 분석, 복구, 보고 등의 절차를 수립하여야 한다.
				11.2.5	원격운영 관리	내부 네트워크를 통하여 정보시스템을 관리하는 경우 특정 단말에서만 접근을 할 수 있도록 제한하고, 원격지에서 인터넷 등 외부 네트워크를 통하여 정보시스템을 관리하는 것은 원칙적으로 금지하고 부득이한 사유로 인해 허용하는 경우에는 책임자 승인, 접속 단말 및 사용자 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등의 보호대책을 수립하여야 한다.
				11.2.6	스마트 워크 보안	재택근무, 원격협업 등과 같은 원격 업무 수행 시 이에 대한 관리적·기술적 보호대책을 수립하고 이행하여야 한다.
				11.2.7	무선네트워크 보안	무선랜 등을 통해 무선인터넷을 사용하는 경우 무선 네트워크 구간에 대한 보안을 강화하기 위해 사용자 인증, 송수신 데이터 암호화 등의 보호대책을 수립하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영보안			11.2.8	공개서버 보안	웹사이트 등에 정보를 공개하는 경우 정보 수집, 저장, 공개에 따른 허가 및 게시절차를 수립하고 공개서버에 대한 물리적, 기술적 보호대책을 수립하여야 한다.
				11.2.9	백업관리	데이터의 무결성 및 정보시스템의 가용성을 유지하기 위해 백업 대상, 주기, 방법 등의 절차를 수립하고 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다.
				11.2.10	취약점 점검	정보시스템이 알려진 취약점에 노출되어 있는 지 여부를 확인하기 위하여 정기적으로 기술적 취약점 점검을 수행하고 발견된 취약점들은 조치하여야 한다.
		11.3	전자거래 및 정보전송 보안	11.3.1	전자거래 보안	전자거래 서비스 제공 시 정보유출, 데이터 조작, 사기 등의 침해사고를 예방하기 위해 사용자 인증, 암호화, 부인방지 등의 보호대책을 수립하고 결제시스템 등 외부 시스템과의 연계가 필요한 경우 연계 안전성을 점검하여야 한다.
				11.3.2	정보전송 정책 수립 및 협약 체결	타 조직에 중요정보를 전송할 경우 안전한 전송을 위한 정책을 수립하고 조직 간 정보전송 합의를 통해 관리책임, 전송 기술 표준, 중요정보의 보호를 위한 기술적 보호조치 등을 포함한 협약서를 작성하여야 한다.
		11.4	매체 보안	11.4.1	정보 시스템 저장매체 관리	정보시스템 폐기 또는 재사용 시 중요정보를 담고 있는 하드디스크, 스토리지, 테잎 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제하여야 한다.
				11.4.2	휴대용 저장매체 관리	조직의 중요정보 유출을 예방하기 위해 외장하드, USB, CD 등 휴대용 저장매체 취급, 보관, 폐기, 재사용에 대한 절차를 수립하여야 한다. 또한 매체를 통한 악성코드 감염 방지 대책을 마련하여야 한다.

	통제분야		통제목적		통제사항	통제내용
11	운영보안	11.5	악성코드 관리	11.5.1	악성코드 통제	바이러스, 웜, 트로이목마 등의 악성코드로부터 정보시스템을 보호하기 위해 악성코드 예방, 탐지, 대응 등의 보호대책을 수립하여야 한다.
				11.5.2	패치관리	소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인해 발생할 수 있는 침해사고를 예방하기 위해 최신 패치를 정기적으로 적용하고 필요한 경우 시스템에 미치는 영향을 분석하여야 한다.
		11.6	로그관리 및 모니터링	11.6.1	시각 동기화	로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 정보시스템 시각을 공식 표준시각으로 정확하게 동기화 하여야 한다.
				11.6.2	로그 기록 및 보존	정보시스템, 응용프로그램, 보안시스템, 네트워크 장비 등 기록해야 할 로그 유형을 정의하여 일정기간 보존하고 주기적으로 검토하여야 한다. 보존기간 및 검토주기는 법적요구사항을 고려하여야 한다.
				11.6.3	접근 및 사용 모니터링	중요정보, 정보시스템, 응용프로그램, 네트워크 장비에 대한 사용자 접근이 업무상 허용된 범위에 있는 지 주기적으로 확인하여야 한다.
				11.6.4	침해시도 모니터링	외부로부터의 침해시도를 모니터링하기 위한 체계 및 절차를 수립하여야 한다.
12	침해사고 관리	12.1	절차 및 체계	12.1.1	침해사고 대응절차 수립	DDoS 등 침해사고 유형별 중요도 분류, 유형별 보고·대응·복구 절차, 비상연락체계, 훈련 시나리오 등을 포함한 침해사고 대응 절차를 수립하여야 한다.
				12.1.2	침해사고 대응체계 구축	침해사고 대응이 신속하게 이루어질 수 있도록 중앙 집중적인 대응체계를 구축하고 외부기관 및 전문가들과의 협조체계를 수립하여야 한다.
		12.2	대응 및 복구	12.2.1	침해사고 훈련	침해사고 대응 절차를 임직원들이 숙지할 수 있도록 시나리오에 따른 모의훈련을 실시하여야 한다.

	통제분야		통제목적		통제사항	통제내용
12	침해사고 관리	12.2	대응 및 복구	12.2.2	침해사고 보고	침해사고 징후 또는 사고 발생을 인지한 때에는 침해사고 유형별 보고 절차에 따라 신속히 보고하고 법적 통지 및 신고 의무를 준수하여야 한다.
				12.2.3	침해사고 처리 및 복구	침해사고 대응절차에 따라 처리와 복구를 신속하게 수행하여야 한다.
		12.3	사후관리	12.3.1	침해사고 분석 및 공유	침해사고가 처리되고 종결된 후 이에 대한 분석을 수행하고 그 결과를 보고하여야 한다. 또한 사고에 대한 정보와 발견된 취약점들을 관련 조직 및 임직원들과 공유하여야 한다.
				12.3.2	재발방지	침해사고로부터 얻은 정보를 활용하여, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하고 이를 위해 필요한 경우 정책, 절차, 조직 등의 대응체계를 변경하여야 한다.
13	IT 재해복구	13.1	체계 구축	13.1.1	IT 재해복구 체계 구축	자연재앙, 해킹, 통신장애, 전력중단 등의 요인으로 인해 IT 시스템 중단 또는 파손 등 피해가 발생할 경우를 대비하여 비상 시 복구조직, 비상연락체계, 복구절차 등 IT 재해복구 체계를 구축하여야 한다.
		13.2	대책 구현	13.2.1	영향분석에 따른 복구대책 수립	조직의 핵심 서비스 연속성을 위협할 수 있는 IT 재해 유형을 식별하고 유형별 예상 피해규모 및 영향을 분석하여야 한다. 또한 IT 서비스 및 시스템 복구목표시간, 복구시점을 정의하고 적절한 복구전략 및 대책을 수립·이행하여야 한다.
				13.2.2	시험 및 유지관리	IT 서비스 복구전략 및 대책에 따라 효과적인 복구가 가능한 지 시험을 실시하고 시험계획에는 시나리오, 일정, 방법, 절차 등을 포함하여야 한다. 또한 시험결과, IT 환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완하여야 한다.

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제1호서식] <개정 2016.0.0>

정보보호 관리체계 인증기관 지정 신청서

* 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	처리기간	3개월이내

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	총 직원 수	인증심사원 직원 수	
신청구분	☐ 신규	☐ 재지정	

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제6항 및 같은 법 시행령 제53조의2에 따라 정보보호 관리체계 인증기관 지정을 위와 같이 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

미래창조과학부 귀중

신청인 제출서류	1. 정관 또는 규약 1부. 2. 별지 제3호서식의 인증심사원의 보유현황과 이를 증명할 수 있는 서류 1부. 3. 별표 1에 따른 업무수행 요건·능력 심사를 위하여 필요한 서류 1부.	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

처 리 절 차

신청서 작성	→	접 수	→	심 사	→	지정여부 결정	→	지정서 교부
신청인		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)

210mm×297mm[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제2호서식] <개정 2016.0.0>

정보보호 관리체계 심사기관 지정 신청서

* 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	처리기간	3개월이내

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	총 직원 수	인증심사원 직원 수	
신청구분	☐ 신규	☐ 재지정	

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제7항 및 같은 법 시행령 제53조의2에 따라 정보보호 관리체계 심사기관 지정을 위와 같이 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

미래창조과학부 귀중

신청인 제출서류	1. 정관 또는 규약 1부. 2. 별지 제3호서식의 인증심사원의 보유현황과 이를 증명할 수 있는 서류 1부. 3. 별표 1에 따른 업무수행 요건·능력 심사를 위하여 필요한 서류 1부.	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

처 리 절 차

신청서 작성	→	접 수	→	심 사	→	지정여부 결정	→	지정서 교부
신청인		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)		처 리 기 관 (미래창조과학부)

210mm×297mm[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제3호서식] <개정 2016.0.0>

인증심사원의 보유현황

(제1쪽)

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		
	직원 수	인증심사원 직원 수	

일련번호	성명	주소		최종학력	해당요건
		생년월일	입사일	취득학위 및 학과	

유의사항

1. 「해당요건」란에는 선임심사원, 심사원, 심사원보 요건을 기재한다.
2. 기재된 최종학위를 증명할 수 있는 직원의 졸업 또는 학위증명서 사본을 제출하여야 한다.
3. 별표 3의 「인증 심사원 학력 및 경력 요건」을 충족하는 직원은 기술자격증 사본 등 자격을 취득하였음을 확인할 수 있는 서류를 함께 제출하여야 한다.
4. 정보통신유관경력 또는 정보보호유관경력을 증명할 수 있는 경력증명서(근무부서 또는 담당업무 등이 기재되어야 한다)와 해당 직원이 신청업체에 현재 근무하고 있음을 확인할 수 있는 재직증명서를 함께 제출하여야 한다.

210㎜×297㎜[백상지(80g/㎡)]

인증심사업무를 전담하는 직원의 보유현황

(제2쪽)

일련번호	성명	주소		최종학력	해당요건
		생년월일	입사일	취득학위 및 학과	

10㎜×297㎜[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제4호서식] <개정 2016.O.O> (제1쪽)

정보보호 관리체계 인증기관 지정서

등록번호 :

업체명 :

대표자 :

주소 :

지정의 유효기간 :

인증업무의 범위 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제6항 및 같은 법 시행령 제53조의2에 따라 위와 같이 정보보호 관리체계 인증기관으로 지정합니다.

년 월 일

미래창조과학부장관 직인

210mm×297mm[백상지(120g/㎡)]

(제2쪽)

CERTIFICATE OF DESIGNATION
AS
ISMS Certification Authority

Registry Number :

Name of Organization :

Name of Representative :

Address :

Period of Validity :

Scope of Certification work :

This is to certify that the abovementioned organization is designated Information Security Management System (ISMS) Certification Authority in accordance with Article 47, Paragraph 6 of 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」 and Article 53-2 of the Enforcement Decree of the same Act.

Date of Issuance:

Signed by the
Minister of Ministry of Science, ICT and Future Planning
Republic of Korea

210㎜×297㎜[백상지 120g/㎡]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제5호서식] <개정 2016.O.O> (제1쪽)

정보보호 관리체계 심사기관 지정서

등록번호 :

업체명 :

대표자 :

주소 :

지정의 유효기간 :

심사업무의 범위 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제7항 및 같은 법 시행령 제53조의2에 따라 위와 같이 정보보호 관리체계 심사기관으로 지정합니다.

년 월 일

미래창조과학부장관 직인

210mm×297mm[백상지(120g/㎡)]

(제2쪽)

CERTIFICATE OF DESIGNATION
AS
ISMS Audit Authority

Registry Number :

Name of Organization :

Name of Representative :

Address :

Period of Validity :

Scope of Audit work :

This is to certify that the abovementioned organization is designated Information Security Management System (ISMS) Audit Authority in accordance with Article 47, Paragraph 7 of 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」 and Article 53-2 of the Enforcement Decree of the same Act.

Date of Issuance:

Signed by the
Minister of Ministry of Science, ICT and Future Planning
Republic of Korea

210㎜×297㎜[백상지 120g/㎡]

■「정보보호 관리체계 인증 등에 관한 고시」 [별지 제6호서식] <개정 2013.8.8>

인증실적 보고서

정보보호 관리체계 인증기관	업체명		사업자등록번호
	주소		전화번호
	대표자		
	정보보호 관리체계 인증실적 총계		

일련번호	인증 번호	대상기관(기업)명	인증범위	유효기간

년 월 일

신청인(대표자) (서명 또는 인)

미래창조과학부 귀중

■「정보보호 관리체계 인증 등에 관한 고시」 [별지 제7호서식] <개정 2016.0.0>

인증심사실적 보고서

정보보호 관리체계 심사기관	업체명		사업자등록번호
	주소		전화번호
	대표자		
	정보보호 관리체계 인증심사 실적 총계	최초심사	건
		갱신심사	건
		사후심사	건

일련 번호	대상기관(기업)명	인증심사 범위	인증심사 기간	구분 (최초/갱신/사후)

년 월 일

신청인(대표자) (서명 또는 인)

미래창조과학부 귀중

■「정보보호 관리체계 인증 등에 관한 고시」 [별지 제8호서식] <개정 2013.8.8> (제1쪽)

정보보호 관리체계 인증심사원 자격 신청서

신청자 인적사항	성 명		생년월일		사진	
	주 소	(우: -)				
	회 사 명					
	회사주소	(우: -)				
	이 메 일					
	전화번호		휴대전화			
신청사항	신청 구분	□ 자격인증 □ 전문분야 변경				
학력사항	최종학력	□ 고졸	□ 전문학사	□ 학사	□ 석사	□ 박사
	학사	전공		기간		
	석사	전공		기간		
	박사	전공		기간		
인증심사원 교육이수	교육기간	년 월 일 ~ 년 월 일		수료증번호		

자격사항 ※해당자에 한함	자격증번호	자격증명/등급	취득일자	수여기관

경력사항 ※최근 10년 내 경력사항 기술	총 경력	정보기술	총 년 개월	정보보호	총 년 개월

No.	구분	기간	회사명	부서	직책
1	□정보기술 □정보보호	~ (년 개월)			
2	□정보기술 □정보보호	~ (년 개월)			
3	□정보기술 □정보보호	~ (년 개월)			
4	□정보기술 □정보보호	~ (년 개월)			
5	□정보기술 □정보보호	~ (년 개월)			

※ 칸이 부족할 경우 추가 작성

(제2쪽)

(1) 개인별 전문분야 (복수 선택 가능, 우선순위 표기요망)					
대분류	중분류	소분류	순위	실무경력	
관리적 정보 보호	정책, 조직 및 인적보안	정보보호정책수립 및 조직구성			년
		인적보안, 외부자 보안, 외부위탁관리			년
		정보보호교육 및 훈련			년
		국내외 표준 기준 및 법령			년
	위험관리	자산분류, 위험평가 수행, 대책 및 계획수립			년
	업무연속성관리	업무연속성 계획수립 및 시험, 유지관리			년
	침해사고대응	침해사고 대응계획 및 체계, 복구			년
	정보시스템 감사/감리	정보시스템 및 정보보호시스템 감사/감리			년
기술적 정보 보호	네트워크	네트워크 설계기술			년
		라우팅 제어, 프로토콜 제어, 접근통제, 암호화, NAT, 운용관리(로그, SNMP, 설정도구)등 통신기술			년
		라우터, 스위치(L2~L7), RAS, VPN, SSL, DHCP, 네트워크 감시 등 기기기술			년
		기타( )			년
	운영체제 및 시스템	OS 기본지식, 계정관리, 접근권한, 서비스관리, 로그관리, 패치, 보안 S/W 사용 등 유닉스/리눅스 시스템			년
		OS 기본지식, 계정관리, 접근권한, 서비스관리, 로그관리, 패치, 보안 S/W 사용 등 윈도우 시스템			년
		메인프레임 등 기타( )			년
	응용서비스	HTTP 프로토콜, 브라우저, SQL-Injection 등 Web 위협에 대한 대응책, SSL, CGI 보안 프로그래밍 등 Web 서비스			년
		부하분산, DNSSEC, 보안설정 등 DNS 서비스			년
		메일 프로토콜, 스팸대응, 웜/바이러스 필터링 등 메일 서비스			년
		DB 기본지식, 이중화, 데이터백업, 암호화 등 데이터베이스			년
		ERP, KMS, CRM 등 사내정보시스템			년
		분산시스템 등 기타( )			년
	정보보호 솔루션	FW 기본지식, 접근통제, 라우팅, 네트워크 정책설계, 구성(이중화, 망분리, 로드밸런싱 등) 등 침입차단시스템			년
		웜/바이러스 기본지식, 웜/바이러스별 감염 증상과 대책 등 바이러스 월			년
		IDS 기본지식, 방화벽 연동, 패턴 매칭 방법, 구성(에이전트 위치, 통합콘솔 등) 등 침입탐지시스템			년
		SecureOS 기본지식, 계정관리, 접근권한, 서비스관리, 로그관리, 패치 등 SecureOS			년
		기타( )			년

(제3쪽)

(1) 개인별 전문분야 (복수 선택 가능, 우선순위 표기요망) (계속)					
대분류	중분류	소분류	순위	실무경력	
기술적 정보 보호 (계속)	취약성분석	사회공학적 방법, 스캔, Sniffing, DOS, Buffer Overflow, 웜/바이러스, 백도어 등 취약성 분석 및 점검			년
	보안 운영	통합관제(ESM, NMS 등), 망관리, 백업, 로그 분석, 모니터링, 패치, 문제해결(원인규명)			년
	기반기술	IPSec, PPTP, L2TP, SSH, SSL/TLS, MPLS, IKE, S/MIME, PGP 등 보안 프로토콜			년
		패스워드인증, 생체인증, 인증디바이스, 인증프로토콜, WEB인증, RADIUS, SSO 등 인증기술			년
		증명서 인증 및 실효, 신뢰모델, 기술 및 데이터방식, 인증센터 구축과 운영, 법적구조 등 PKI			년
		암호알고리즘, Key 관리, 암호방식 등 암호기술			년
		디지털서명, 디지털 봉투, 코드 서명			년
물리적 정보 보호	접근보안	출입 및 접근통제, 모니터링 등			년
	시설관리	소방시설, 비상전원, 비상조명, 항온항습 등			년
개인정보보호		개인정보보호 책임자, 취급자, 컨설턴트, 법률 담당, 소비자 민원 및 상담 등			년
기타		( )			년

※ 경력 및 전문 분야에 대한 관련 내용을 상세히 기술
※ 칸이 부족할 경우 별지 사용

No.	상세내용
1	
2	
3	
4	
5	
6	

(제4쪽)

(2) 통제분야별 전문분야 (5순위까지 선택, 우선순위 표기요망)

통제분야	순위	실무경력		통제분야	순위	실무경력	
1. 정보보호정책			년	9. 암호통제			년
2. 정보보호조직			년	10. 접근통제			년
3. 외부자 보안			년	11. 운영관리			년
4. 정보자산분류			년	12. 전자거래보안			년
5. 정보보호교육 및 훈련			년	13. 보안사고관리			년
6. 인적 보안			년	14. 검토, 모니터링 및 감사			년
7. 물리적 보안			년	15. 업무연속성 관리			년
8. 시스템개발 보안			년	16. 개인정보보호			년

관련 경력기술

※ 5순위까지 선택한 전문분야 관련 실무경력, 전문기술, 인증심사실적 등 관련경력을 상세히 기술

<개인정보 수집·이용>

- 개인정보 수집 이용 목적 : 정보보호 관리체계(ISMS) 인증심사원 양성 교육, 자격부여 및 관리, 자문료 지급, 심사팀구성
- 수집하는 개인정보 항목 : 성명, 생년월일, 주소, 이메일, 전화번호, 학력, 자격경력, 발령사항, 기술실적사항
- 보유 및 이용기간 : 인증심사원 자격 종료시까지
- 개인정보의 수집·이용을 거부할 수 있으며, 이 경우 인증심사원 등록 및 위촉에 불이익이 발생할 수 있음을 알려드립니다.

▷ 개인정보 수집 · 이용 동의여부 **동의 □** **미동의 □**

<인증심사원 의무사항>

- 인증심사원은 객관적이고 공정한 인증심사를 수행한다.
- 인증심사원으로서의 성실한 직무수행 및 품위유지를 한다.
- 인증심사와 관련된 부당한 금전, 금품 등의 수수를 금지한다.
- 인증심사의 수행에서 취득한 정보를 관련 법령 또는 신청기관의 동의 없이 외부에 누설하여서는 안된다.
- 인증심사원은 인증업무지침을 성실히 준수한다.
- 인증심사원은 본인이 ISMS 인증 취득을 위한 컨설팅을 수행한 기업에 대하여는 인증심사에 참여할 수 없다.
- 인증심사원은 인증심사의 수행과 관련하여 상업적, 재정적 그리고 기타 모든 압력으로부터 배제되어야 한다.

1. 위의 인증심사원 의무사항을 읽고 이해하였으며, 성실히 준수하겠습니다.
2. 본 신청서의 기재사항은 사실과 틀림없으며, 만약 허위로 판명될 경우에는 자격취소 등 불이익을 감수하겠습니다.

※ 필요시 학력, 경력 등 증빙서류 제출을 요청받을 수 있으며 반드시 이에 응해야 함

위와 같이 인증심사원 자격을 신청합니다.

년 월 일

신청자		(서명 또는 인)

한국인터넷진흥원 귀중

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제9호서식] <개정 2013.8.8>

경력증명서

인적사항	성명		생년월일	
	주소		연락처	

경력사항	전 근무처 명				
	근무기간		부서	직위	담당업무
	부터	까지			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			

근무년수	년 개월	최종직위	
용도	정보보호 관리체계 인증심사원 자격 신청		

위와 같이 경력을 증명합니다.

년 월 일

회사명

대표자 (서명 또는 인)

확인자	성명	부서	연락처	비고

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제10호서식] <개정 2013.8.8>

상세 재직증명서

인적사항	성명		생년월일	
	주소		연락처	
소속사항	회사명			
	부서		직위	
	근속기간	~	근무년수	년 개월

발령사항	근무기간		부서	직위	담당업무
	부터	까지			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			

용도	정보보호 관리체계 인증심사원 자격 신청

위와 같이 재직하고 있음을 증명합니다.

년 월 일

회사명

대표자 (서명 또는 인)

확인자	성명	부서	연락처	비고

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제11호서식] <개정 2013.8.8>

기술실적증명서

인적사항	성명			생년월일	
	주소			연락처	
실적사항	소속				
	수행기간		참여사업명	발주처	담당업무
	부터	까지			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
	. .	. .			
용도	정보보호 관리체계 인증심사원 자격 신청				

위와 같이 기술실적을 증명합니다.

년 월 일

회사명

대표자 (서명 또는 인)

확인자	성명	부서	연락처	비고

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제12호서식] <개정 2013.8.8>

제 호

인증심사원 자격 증명서

성 명 : (. . .)

인증심사원 등급 :

유효기간 :

※ 인증심사원 유지조건을 만족하지 못할 경우 자격이 취소될 수 있습니다.

귀하에게 정보보호 관리체계 인증심사원 자격을 부여합니다.

년 월 일

한국인터넷진흥원 원장 직인

210mm×297mm[백상지(120g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제13호서식] <개정 2016.0.0>

정보보호 관리체계 인증 신청서

※ [ ]에는 해당되는 곳에 √표를 하고, 어두운 부분은 신청인이 작성하지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명	사업자등록번호
	주소	전화번호
	대표자	

인증신청의 구분	[ ]최초심사 [ ]사후심사 [ ]갱신심사
정보보호 관리체계의 범위	
정보보호 관리체계의 범위에 포함되어 있는 종업원의 수	
정보보호 관리체계의 범위에 포함되어 있는 서버의 수	

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제11항, 같은 법 시행령 제47조에 따라 위와 같이 정보보호 관리체계의 인증을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

(한국인터넷진흥원 · 인증기관 또는 심사기관) 귀중

신청(신고)인 제출서류	정보보호 관리체계의 내역서 1부.	수수료 없음
담당공무원 확인사항	법인등기사항증명서	

210㎜×297㎜[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제14호서식] <개정 2016.0.0> (제1쪽)

정보보호 관리체계 인증서

인증번호 :

업체명 :

대표자 :

주소 :

인증의 범위 :

유효기간 :

심사수행 기관 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제11항, 같은 법 시행령 제47조에 따라 위와 같이 정보보호 관리체계를 인증합니다.

년 월 일

한국인터넷진흥원 원장
또는 정보보호 관리체계
인증기관 장 직인

210mm×297mm[백상지(120g/㎡)]

(제2쪽)

CERTIFICATE
OF
Information Security Management System

Certificate Number :

Name of Organization :

Name of Representative :

Address :

Scope of Certification :

Period of Validity :

name of Audit Organization :

This is to certify that the abovementioned organization is compliant to the assessment standard for Information Security Management System certification in accordance with Article 47, Paragraph 1 and 11 of 「Act on Information Network Utilization and Data Protection, etc.」 and Article 47 of the Enforcement Decree of the same Act.

Date of Issuance :

Signed by the
President of Korea Internet & Security Agency or certification body

210㎜×297㎜[백상지(120g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제15호서식] <개정 2013.8.8>

정보보호 관리체계 인증서 추가발급 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명	사업자등록번호
	주소	전화번호
	대표자	

추가발급 사유	

위와 같이 정보보호 관리체계 인증서의 추가발급을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

한국인터넷진흥원 또는 정보보호 관리체계 인증기관명 귀중

제출서류	해당없음	수수료 없 음

210mm×297mm[백상지(80g/㎡)]

■ 「정보보호 관리체계 인증 등에 관한 고시」 [별지 제16호서식] <개정 2013.8.8>

정보보호 관리체계 인증서 변경 신청서

※ 색상이 어두운 곳은 신청인이 적지 않습니다.

접수번호	접수일자	발급일	처리기간

신청인	업체명		사업자등록번호
	주소		전화번호
	대표자		

변경 내용	변경전	(국문)
		(영문)
	변경후	(국문)
		(영문)
변경사유		

위와 같이 정보보호 관리체계 인증서 변경을 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

한국인터넷진흥원 또는 정보보호 관리체계 인증기관명 귀중

제출서류	해당없음	수수료 없 음

210㎜×297㎜[백상지(80g/㎡)]

개인정보법

1. 개인정보 보호법 시행규칙
2. 표준 개인정보 보호지침
3. 개인정보의 안전성 확보조치 기준
4. 개인정보 보호법
5. 개인정보 보호법 시행령

개인정보 보호법 시행규칙

[시행 2014.11.19] [행정자치부령 제00001호, 2014.11.19, 타법개정]

제1조(목적) 이 규칙은 「개인정보 보호법」 및 같은 법 시행령에서 위임된 사항과 그 시행에 필요한 사항을 규정함을 목적으로 한다.

제2조(공공기관에 의한 개인정보의 목적 외 이용 또는 제3자 제공의 공고) 공공기관은 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공(이하 "목적외이용등"이라 한다)하는 경우에는 「개인정보 보호법」(이하 "법"이라 한다) 제18조제4항에 따라 개인정보를 목적외이용등을 한 날부터 30일 이내에 다음 각 호의 사항을 관보 또는 인터넷 홈페이지에 게재하여야 한다. 이 경우 인터넷 홈페이지에 게재할 때에는 10일 이상 계속 게재하되, 게재를 시작하는 날은 목적외이용등을 한 날부터 30일 이내여야 한다.

1. 목적외이용등을 한 날짜
2. 목적외이용등의 법적 근거
3. 목적외이용등의 목적
4. 목적외이용등을 한 개인정보의 항목

제3조(개인정보 보호업무 관련 장부 및 문서 서식) ① 법 제18조제2항과 「개인정보 보호법 시행령」(이하 "영"이라 한다) 제15조에 따른 개인정보의 목적 외 이용 및 제3자 제공 대장은 별지 제1호서식과 같다.

② 법 제32조제1항과 영 제34조제1항에 따른 개인정보파일 등록 신청 및 변경등록 신청은 별지 제2호서식의 개인정보파일 등록·변경등록 신청서에 따른다.

③ 영 제37조제2항에 따라 개인정보 영향평가기관의 지정을 신청하려는 자는 별지 제3호서식의 개인정보 영향평가기관 지정신청서에 다음 각 호의 서류(전자문서를 포함한다)를 첨부하여 행정자치부장관에게 제출하여야 한다.<개정 2013.3.23, 2014.11.19>

1. 영 제37조제2항제1호부터 제3호까지의 규정에 따른 서류
2. 영 제37조제2항제4호에 따른 다음 각 목의 서류
   가. 별지 제4호서식의 개인정보 영향평가 수행인력 보유 현황
   나. 별지 제5호서식의 개인정보 영향평가 수행 관련 사무실 및 설비 보유 현황
   다. 영 제37조제1항제1호의 사실을 증명할 수 있는 서류 등 행정자치부장관이 정하는 서류
3. 「출입국관리법」 제88조제2항에 따른 외국인등록 사실증명(영 제37조제3항 각 호 외의 부분 단서에 해당하는 경우에만 첨부한다)

④ 법 제33조제1항과 영 제37조제4항에 따른 개인정보 영향평가기관 지정서는 별지 제6호서식과 같다.

⑤ 법 제33조제6항과 영 제37조제6항에 따른 신고는 별지 제7호서식의 개인정보 영향평가기관 변경사항 신고서에 따른다.

⑥ 법 제35조제1항·제2항과 영 제41조제1항에 따른 개인정보 열람의 요구, 법 제36조제1항과 영 제43조제1항에 따른 개인정보 정정·삭제 요구, 법 제37조제1항과 영 제44조제1항에 따른 개인정보 처리정지 요구는 별지 제8호서식의 개인정보 열람, 정정·삭제, 처리정지 요구서에 따른다.

⑦ 법 제35조제5항과 영 제41조제4항에 따른 개인정보 열람 및 일부열람의 통지, 법 제35조제3항 후단과 영 제42조제2항에 따른 개인정보 열람연기의 통지, 법 제35조제4항과 영 제42조제2항에 따른 열람거절의 통지는 별지 제9호서식의 개인정보 열람, 일부열람, 열람연기, 열람거절 통지서에 따른다.

⑧ 법 제36조제6항과 영 제43조제3항에 따른 개인정보 정정·삭제 요구에 대한 결과의 통지, 법 제37조제5항과 영 제44조제2항에 따른 개인정보 처리정지 요구에 대한 결과의 통지는 별지 제10호서식의 개인정보 정정·삭제, 처리정지 요구에 대한 결과 통지서에 따른다.

⑨ 영 제45조제2항에 따른 정보주체의 위임장은 별지 제11호서식과 같다.

부칙 <제241호,2011.9.29>

제1조(시행일) 이 규칙은 2011년 9월 30일부터 시행한다.

제2조(다른 법령의 폐지) 공공기관의 개인정보보호에 관한 법률 시행규칙은 폐지한다.

제3조(다른 법령과의 관계) 이 규칙 시행 당시 다른 법령에서 종전의 「공공기관의 개인정보보호에 관한 법률 시행규칙」 또는 그 규정을 인용하고 있는 경우 이 규칙 가운데 그에 해당하는 규정이 있을 때에는 종전의 규정을 갈음하여 이 규칙 또는 이 규칙의 해당 규정을 인용한 것으로 본다.

부칙 <제1호,2013.3.23>

제1조(시행일) 이 규칙은 공포한 날부터 시행한다.

제2조부터 제4조까지 생략

제5조(다른 법령의 개정) ① 개인정보 보호법 시행규칙 일부를 다음과 같이 개정한다.

제3조제3항 각 호 외의 부분 및 같은 항 제2호다목 중 "행정안전부장관"을 각각 "안전행정부장관"으로 한다.

별지 제2호서식, 별지 제3호서식, 별지 제6호서식 및 별지 제7호서식 중 "행정안전부장관"을 각각 "안전행정부장관"으로 한다.

별지 제3호서식의 처리절차란 중 "행정안전부"를 각각 "안전행정부"로 한다.

②부터 <51>까지 생략

부칙 <제1호,2014.11.19>

제1조(시행일) 이 규칙은 공포한 날부터 시행한다. 다만, 부칙 제6조에 따라 개정되는 시행규칙 중 이 규칙 시행 전에 공포되었으나 시행일이 도래하지 아니한 시행규칙을 개정한 부분은 각각 해당 시행규칙의 시행일부터 시행한다.

제2조부터 제5조까지 생략

제6조(다른 법령의 개정) ① 개인정보 보호법 시행규칙 일부를 다음과 같이 개정한다.

제3조제3항 각 호 외의 부분 및 같은 항 제2호다목 중 "안전행정부장관"을 각각 "행정자치부장관"으로 한다.

별지 제2호서식, 별지 제3호서식, 별지 제6호서식 및 별지 제7호서식 중 "안전행정부장관"을 각각 "행정자치부장관"으로 한다.

별지 제3호서식의 처리절차란 중 "안전행정부"를 각각 "행정자치부"로 한다.

②부터 <42>까지 생략

■ 개인정보 보호법 시행규칙 [별지 제1호서식]

개인정보의 목적 외 이용 및 제3자 제공 대장

<table>
<tr><td>개인정보 또는
개인정보파일 명칭</td><td colspan="3"></td></tr>
<tr><td>이용 또는 제공 구분</td><td colspan="3">[ ] 목적외 이용 [ ] 제3자 제공</td></tr>
<tr><td>목적 외 이용기관의 명칭
(목적 외 이용의 경우)</td><td></td><td rowspan="3">담당자</td><td>소 속
성 명
전화번호</td></tr>
<tr><td>제공받는 기관의 명칭
(제3자 제공의 경우)</td><td></td><td rowspan="3">담당자</td><td>성 명
소 속
전화번호</td></tr>
<tr><td>이용하거나 제공한 날짜,
주기 또는 기간</td><td colspan="3"></td></tr>
<tr><td>이용하거나 제공한 형태</td><td colspan="3"></td></tr>
<tr><td>이용 또는 제공의 법적
근거</td><td colspan="3"></td></tr>
<tr><td>이용 목적 또는
제공받는 목적</td><td colspan="3"></td></tr>
<tr><td>이용하거나 제공한
개인정보의 항목</td><td colspan="3"></td></tr>
<tr><td>「개인정보 보호법」
제18조제5항에 따라
제한을 하거나 필요한
조치를 마련할 것을
요청한 경우에는 그 내용</td><td colspan="3"></td></tr>
</table>

210㎜×297㎜[인쇄용지(특급) 34g/㎡]

■ 개인정보 보호법 시행규칙 [별지 제2호서식] <개정 2014.11.19.>

개인정보파일 ([ ] 등록 [ ] 변경등록) 신청서

※ '변경정보 및 변경사유' 란은 변경등록시에만 작성합니다.

접수번호	접수일	처리기간 7일

공공기관 명칭	주소	등록부서	전화번호

등록항목	등록정보	변경정보 및 변경사유
개인정보파일 명칭		
개인정보파일의 운영 근거 및 목적		
개인정보파일에 기록되는 개인정보의 항목		
개인정보의 처리방법		
개인정보의 보유기간		
개인정보를 통상적 또는 반복적으로 제공하는 경우 그 제공받는 자		
개인정보파일을 운용하는 공공기관의 명칭		
개인정보파일로 보유하고 있는 개인정보의 정보주체 수		
해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서		
개인정보의 열람 요구를 접수·처리하는 부서		
개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유		

「개인정보 보호법」 제32조제1항과 같은 법 시행령 제34조제1항에 따라 위와 같이 개인정보파일 ([ ] 등록 [ ] 변경등록)을 신청합니다.

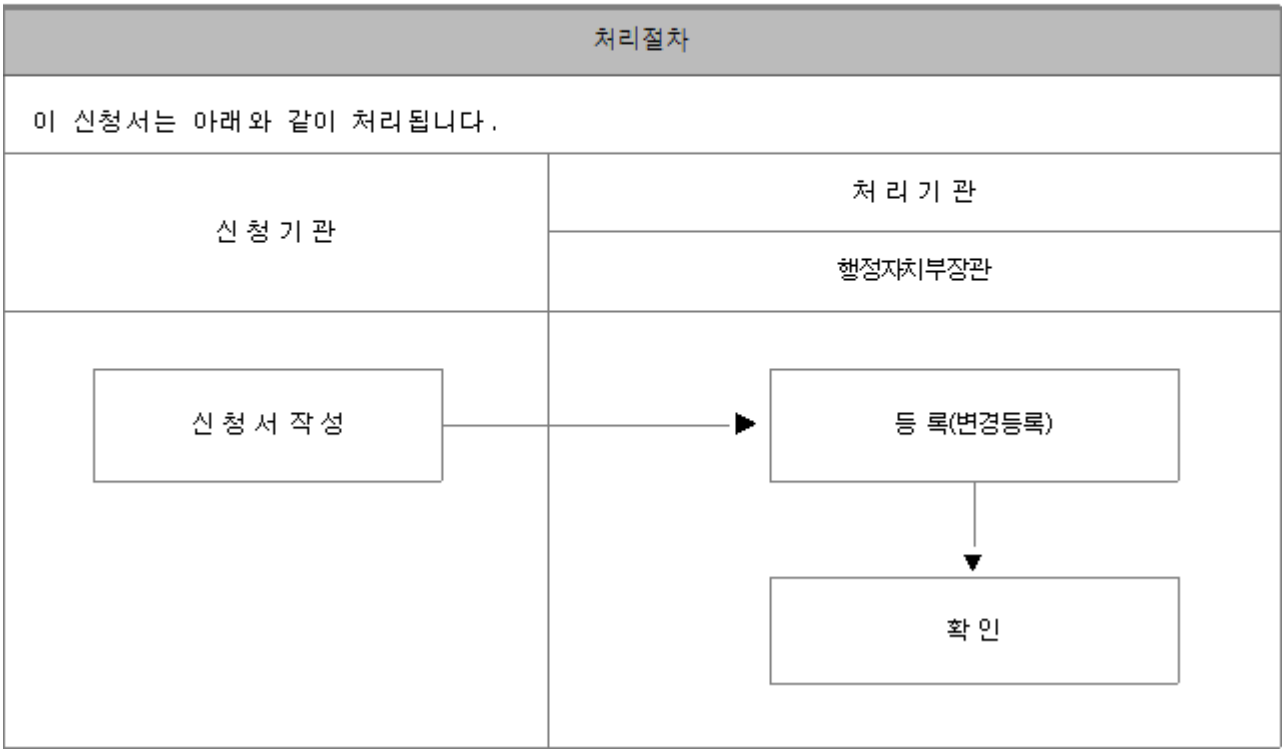
년 월 일

신청기관 (서명 또는 인)

행정자치부장관 귀하

210mm×297mm[일반용지 70g/㎡(재활용품)]

(뒤 쪽)



■ 개인정보 보호법 시행규칙 [별지 제3호서식] <개정 2014.11.19.>

개인정보 영향평가기관 지정신청서

접수번호	접수일	처리기간 2개월

신청인	법인명 및 대표자 성명	법인 설립일
	소재지	전화번호
개인정보 영향평가 수행인력의 수	명	

「개인정보 보호법 시행령」 제37조제2항에 따라 개인정보 영향평가기관 지정을 위와 같이 신청합니다.

년 월 일

신청인 (서명 또는 인)

행정자치부장관 귀하

첨부서류	1. 「개인정보 보호법 시행령」 제37조제2항제1호부터 제3호까지의 규정에 따른 서류 2. 「개인정보 보호법 시행령」 제37조제2항제4호에 따른 다음의 서류 가. 「개인정보보호법 시행규칙」 별지 제4호서식의 개인정보 영향평가 수행인력 보유 현황 나. 「개인정보보호법 시행규칙」 별지 제6호서식의 개인정보 영향평가 수행 관련 사무실 및 설비 보유 현황 다. 「개인정보 보호법 시행령」 제37조제1항제1호의 사실을 증명할 수 있는 서류 등 행정자치부장관이 정하는 서류 3. 「출입국관리법」 제88조제2항에 따른 외국인등록 사실증명(「개인정보보호법 시행령」 제37조제3항 각 호 외의 부분 단서에 해당하는 경우에만 첨부합니다)

처리절차

신청서 작성	→	접 수	→	검 토	→	결 재	→	지정서 발급
신청인		처리기관 (한국정보화진흥원)		처리기관 (행정자치부)		처리기관 (행정자치부)		

210mm×297mm[일반용지 70g/㎡(재활용품)]

■ 개인정보 보호법 시행규칙 [별지 제4호서식]

개인정보 영향평가 수행인력 보유현황

법인명 및 대표자 성명								
영향평가 수행인력 총수			명					
일련번호	성명	생년월일	입사일	보유자격증 (취득연월일)	자격증 취득 후 업무 수행 경력 (년 개월)	전문분야	학위 및 학과	비고

유의사항

전문분야는 「개인정보보호법 시행령」 제37조제1항제1호 각 목에 따른 업무 분야를 말합니다.

210mm×297mm[일반용지 60g/㎡(재활용품)]

■ 개인정보 보호법 시행규칙 [별지 제5호서식]

개인정보 영향평가 수행 관련 사무실 및 설비 보유 현황

※ 아래의 작성방법을 읽고 작성하시기 바랍니다.

법인명 및 대표자 성명	
소 재 지	

① 신원 확인 및 출입 통제를 위한 설비를 갖춘 사무실

[ ] 있음 [ ] 없음

② 신원 확인 및 출입 통제 설비

명 칭	설비 등의 세부사항	수 량	비고

③ 기록 및 자료의 안전관리 설비

명 칭	설비 등의 세부사항	수 량	비 고

작 성 방 법

①의 신원 확인 및 출입 통제를 위한 설비를 갖춘 사무실이 있는 경우에는 '있음'란에 [√] 표시를 하고, 없는 경우에는 '없음'란에 [√] 표시를 합니다.

210㎜×297㎜[일반용지 60g/㎡(재활용품)]

■ 개인정보 보호법 시행규칙 [별지 제6호서식] <개정 2014.11.19.>

제 호

개인정보 영향평가기관 지정서

1. 대 표 자:
2. 생년월일 또는 사업자등록번호:
3. 법 인 명:
4. 주 소:
5. 전화번호:
6. 지정요건:

「개인정보 보호법」 제33조제1항과 같은 법 시행령 제37조제4항에 따라 위의 법인을 개인정보 영향평가기관으로 지정하였으므로 개인정보 영향평가기관 지정서를 발급합니다.

년 월 일

행정자치부장관 직인

210㎜×297㎜[보존용지 120g/㎡]

■ 개인정보 보호법 시행규칙 [별지 제7호서식] <개정 2014.11.19.>

개인정보 영향평가기관 변경사항 신고서

접수번호	접수일자	처리기간 7일

신고인	법인명		
	대표자명	생년월일	
	주소 (주된 사무소의 소재지) (전화번호 :)		
변경일			
구분	종 전	변 경	
수행 인력			
사무실 및 설비			
평가 기관 양도·양수 또는 합병 등	종전 법인	법인명	
		대표자명	생년월일
		주소 (전화번호 :)	
	변경 법인	법인명	
		대표자명	생년월일
		주소 (전화번호 :)	
법인 명칭·주소·전화번호 및 대표자 변경			

「개인정보 보호법」 제33조제6항과 같은 법 시행령 제37조제6항에 따라 평가기관의 변경사항을 위와 같이 신고합니다.

년 월 일

신고인 대표 (서명 또는 인)

행정자치부장관 귀하

첨부서류	1. 양도·양수·합병 등의 경우 양도·양수 또는 합병 계약서 등 사본 1부 2. 그 밖의 변경사항 증명서류 각 1부

유의사항
위 변경사항과 관련하여 자세한 내용은 별지로 작성하거나 관련 서류를 첨부하여 제출할 수 있습니다.

210㎜×297㎜[일반용지 60g/㎡(재활용품)]

■ 개인정보 보호법 시행규칙 [별지 제8호서식]

개인정보([ ] 열람 [ ] 정정·삭제 [ ] 처리정지) 요구서

※ 아래 작성방법을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다. (앞 쪽)

접수번호	접수일	처리기간 10일 이내

정보주체	성 명	전 화 번 호
	생년월일	
	주 소	
대리인	성 명	전 화 번 호
	생년월일	정보주체와의 관계
	주 소	
요구내용	[ ] 열람	[ ] 개인정보의 항목 및 내용 [ ] 개인정보 수집·이용의 목적 [ ] 개인정보 보유 및 이용 기간 [ ] 개인정보의 제3자 제공 현황 [ ] 개인정보 처리에 동의한 사실 및 내용
	[ ] 정정·삭제	※ 정정·삭제하려는 개인정보의 항목과 그 사유를 적습니다.
	[ ] 처리정지	※ 개인정보의 처리정지를 원하는 대상·내용 및 그 사유를 적습니다.

「개인정보 보호법」 제35조제1항·제2항, 제36조제1항 또는 제37조제1항과 같은 법 시행령 제41조제1항, 제43조제1항 또는 제44조제1항에 따라 위와 같이 요구합니다.

년 월 일

요구인 (서명 또는 인)

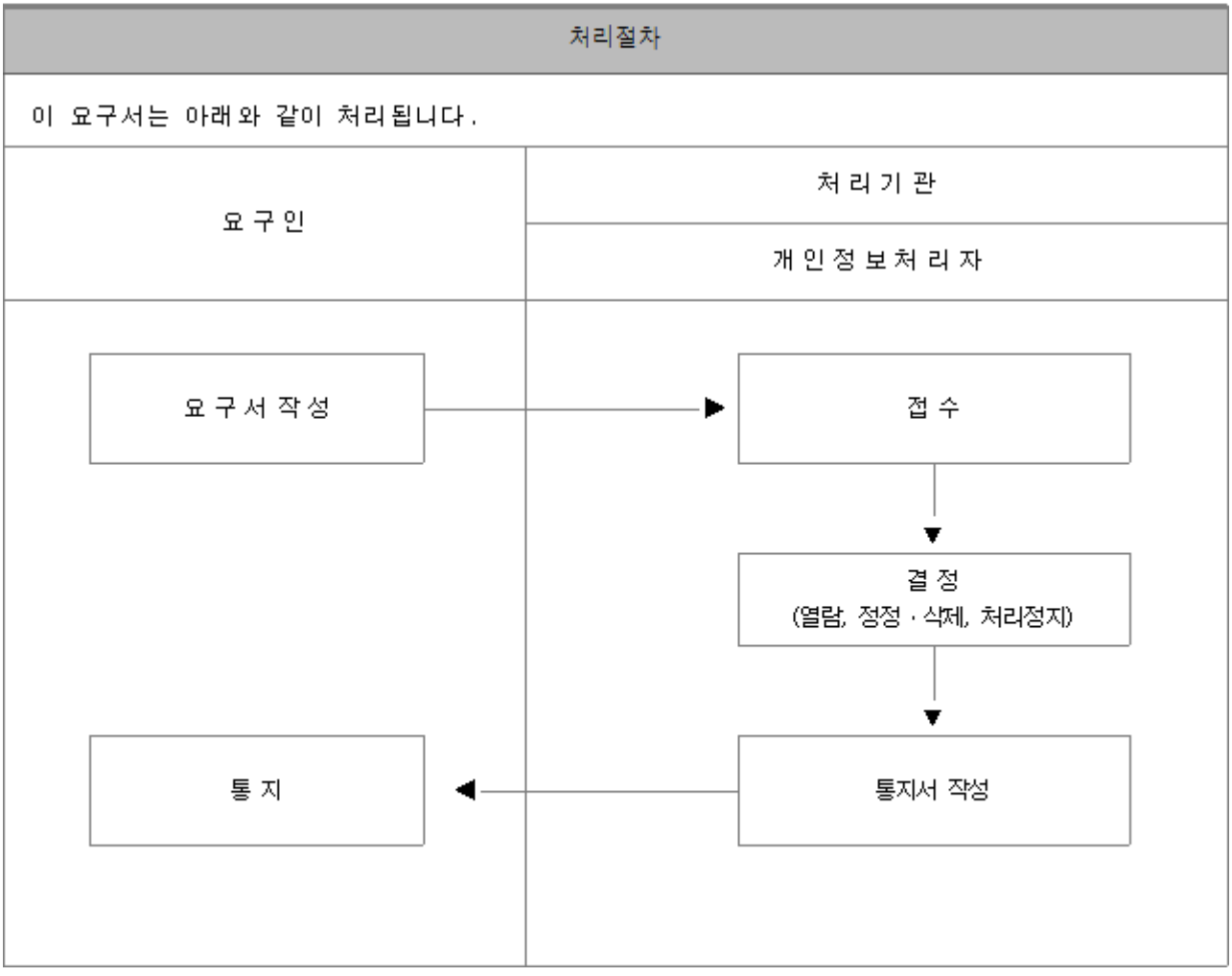
○○○○ 귀하

작 성 방 법

1. '대리인'란은 대리인이 요구인일 때에만 적습니다.
2. 개인정보의 열람을 요구하려는 경우에는 '열람' 란에 [√] 표시를 하고 열람하려는 사항을 선택하여 [√] 표시를 합니다. 표시를 하지 않은 경우에는 해당 항목의 열람을 요구하지 않은 것으로 처리됩니다.
3. 개인정보의 정정·삭제를 요구하려는 경우에는 '정정·삭제' 란에 [√] 표시를 하고 정정하거나 삭제하려는 개인정보의 항목과 그 사유를 적습니다.
4. 개인정보의 처리정지를 요구하려는 경우에는 '처리정지' 란에 [√] 표시를 하고 처리정지 요구의 대상·내용 및 그 사유를 적습니다.

210mm×297mm[일반용지 70g/㎡(재활용품)]

(뒤 쪽)


처리절차
이 요구서는 아래와 같이 처리됩니다.
요구인
처리기관
개인정보처리자
요구서 작성
접수
결정
(열람, 정정·삭제, 처리정지)
통지
통지서 작성

■ 개인정보 보호법 시행규칙 [별지 제9호서식]

개인정보 ([ ] 열람 [ ] 일부열람 [ ] 열람연기 [ ] 열람거절) 통지서

(앞 쪽)

수신자 (우편번호: , 주소:)

요구 내용					
열람 일시		열람 장소			
통지 내용 ([ ] 열람 [ ] 일부열람 [ ] 열람연기 [ ] 열람거절)					
열람 형태 및 방법	열람 형태	[ ]열람·시청	[ ]사본·출력물	[ ]전자파일	[ ]복제물·인화물	[ ]기타
	열람 방법	[ ]직접방문	[ ]우편	[ ]팩스	[ ]전자우편	[ ]기타
납부 금액	①수수료 원	②우송료 원	계(①+②) 원		
	수수료 산정 명세				
사 유					
이의제기방법	※ 개인정보처리자는 이의제기방법을 적습니다.				

「개인정보 보호법」 제35조제3항·제4항 또는 제5항과 같은 법 시행령 제41조제4항 또는 제42조제2항에 따라 귀하의 개인정보 열람 요구에 대하여 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

210㎜×297㎜[신문용지 54g/㎡]

(뒤 쪽)

유의사항

1. 개인정보 열람 장소에 오실 때에는 이 통지서를 지참하셔야 하며, 요구인 본인 또는 그 정당한 대리인임을 확인하기 위하여 다음의 구분에 따른 증명서를 지참하셔야 합니다.

가. 요구인 본인에게 공개할 때: 요구인의 신원을 확인할 수 있는 신분증명서(주민등록증 등)

나. 요구인의 대리인에게 공개할 때: 대리인임을 증명할 수 있는 서류와 대리인의 신원을 확인할 수 있는 신분증명서

2. 수수료 또는 우송료는 다음의 구분에 따른 방법으로 냅니다.

가. 국가기관인 개인정보처리자에게 내는 경우: 수입인지

나. 지방자치단체인 개인정보처리자에게 내는 경우: 수입증지

다. 국가기관 및 지방자치단체 외의 개인정보처리자에게 내는 경우: 해당 개인정보처리자가 정하는 방법

※ 국회, 법원, 헌법재판소, 중앙선거관리위원회, 중앙행정기관 및 그 소속 기관 또는 지방자치단체인 개인정보처리자에게 수수료 또는 우송료를 내는 경우에는 「전자금융거래법」 제2조제11호에 따른 전자지급수단 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제10호에 따른 통신과금서비스를 이용하여 수수료 또는 우송료를 낼 수 있습니다.

3. 열람제한, 열람연기 또는 열람거절의 통지를 받은 경우에는 개인정보처리자가 이의제기방법란에 적은 방법으로 이의제기를 할 수 있습니다.

210㎜×297㎜[신문용지 54g/㎡]

■ 개인정보 보호법 시행규칙 [별지 제10호서식]

개인정보 ([ ] 정정·삭제, [ ] 처리정지) 요구에 대한 결과 통지서

수신자 (우편번호: , 주소:)

요구 내용	
□ 정정·삭제 □ 처리정지 조치 내용	
□ 정정·삭제 □ 처리정지 결정 사유	
이의제기방법	※ 개인정보처리자는 이의제기방법을 기재합니다.

「개인정보 보호법」 제36조제6항 및 같은 법 시행령 제43조제3항 또는 같은 법 제37조제5항 및 같은 법 시행령 제44조제2항에 따라 귀하의 요구에 대한 결과를 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

유의사항

개인정보의 정정·삭제 또는 처리정지 요구에 대한 결정을 통지받은 경우에는 개인정보처리자가 '이의제기방법'란에 적은 방법으로 이의제기를 할 수 있습니다.

210㎜×297㎜[신문용지 54g/㎡]

■ 개인정보 보호법 시행규칙 [별지 제11호서식]

위 임 장

위임받는 자	성명	전 화 번 호
	생년월일	정보주체와의 관계
	주소	
위임자	성명	전화번호
	생년월일	
	주소	

「개인정보 보호법」 제38조제1항에 따라 위와 같이 개인정보의 (□ 열람, □ 정정·삭제, □ 처리정지)의 요구를 위의 자에게 위임합니다.

년 월 일

위임자

(서명 또는 인)

ㅇㅇㅇㅇ 귀하

210mm×297mm[인쇄용지(특급) 34g/㎡]

표준 개인정보 보호지침

[시행 2016.6.30] [고시 제2016 - 21호, 2016.6.30, 전부개정]

제1장 총칙

제1조(목적) 이 지침은 「개인정보 보호법」(이하 "법"이라 한다) 제12조제1항에 따른 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 세부적인 사항을 규정함을 목적으로 한다.

제2조(용어의 정의) 이 지침에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보 처리"란 개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
2. "개인정보처리자"란 업무를 목적으로 법 제2조제4호에 따른 개인정보파일을 운용하기 위하여 개인정보를 처리하는 모든 공공기관, 영리목적의 사업자, 협회·동창회 등 비영리기관·단체, 개인 등을 말한다.
3. "공공기관"이란 법 제2조제6호 및 「개인정보 보호법 시행령」(이하 "영"이라 한다) 제2조에 따른 기관을 말한다.
4. "친목단체"란 학교, 지역, 기업, 인터넷 커뮤니티 등을 단위로 구성되는 것으로서 자원봉사, 취미, 정치, 종교 등 공통의 관심사나 목표를 가진 사람간의 친목도모를 위한 각종 동창회, 동호회, 향우회, 반상회 및 동아리 등의 모임을 말한다.
5. "개인정보 보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.
6. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
7. "개인정보처리시스템"이란 데이터베이스 시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 응용시스템을 말한다.
8. "영상정보처리기기"란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 일체의 장치로서 영 제3조에 따른 폐쇄회로 텔레비전 및 네트워크 카메라를 말한다.
9. "개인영상정보"란 영상정보처리기기에 의하여 촬영·처리되는 영상정보 중 개인의 초상, 행동 등과 관련된 영상으로서 해당 개인을 식별할 수 있는 정보를 말한다.

10. "영상정보처리기기운영자"란 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자를 말한다.
11. "공개된 장소"란 공원, 도로, 지하철, 상가 내부, 주차장 등 불특정 또는 다수가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소를 말한다.

제3조(적용범위) 이 지침은 전자적 파일과 인쇄물, 서면 등 모든 형태의 개인정보파일을 운용하는 개인정보처리자에게 적용된다.

제4조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성과 최신성을 유지하도록 하여야 하고, 개인정보를 처리하는 과정에서 고의 또는 과실로 부당하게 변경 또는 훼손되지 않도록 하여야 한다.
④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 그에 상응하는 적절한 관리적·기술적 및 물리적 보호조치를 통하여 개인정보를 안전하게 관리하여야 한다.
⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리가 보장될 수 있도록 합리적인 절차와 방법 등을 마련하여야 한다.
⑥ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하는 경우에도 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
⑦ 개인정보처리자는 개인정보를 적법하게 수집한 경우에도 익명에 의하여 업무 목적을 달성할 수 있으면 개인정보를 익명에 의하여 처리될 수 있도록 하여야 한다.
⑧ 개인정보처리자는 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

제5조(다른 지침과의 관계) 중앙행정기관의 장이 소관 분야의 개인정보 처리와 관련한 개인정보 보호지침을 정하는 경우에는 이 지침에 부합되도록 하여야 한다.

제2장 개인정보 처리 기준
제1절 개인정보의 처리

제6조(개인정보의 수집·이용) ① 개인정보의 "수집"이란 정보주체로부터 직접 이름, 주소, 전화번호 등의 개인정보를 제공받는 것뿐만 아니라 정보주체에 관한 모든 형태의 개인정보를 취득하는 것을 말한다.

② 개인정보처리자는 다음 각 호의 경우에 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체로부터 사전에 동의를 받은 경우
2. 법률에서 개인정보를 수집·이용할 수 있음을 구체적으로 명시하거나 허용하고 있는 경우
3. 법령에서 개인정보처리자에게 구체적인 의무를 부과하고 있고, 개인정보처리자가 개인정보를 수집·이용하지 않고는 그 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우
4. 공공기관이 개인정보를 수집·이용하지 않고는 법령 등에서 정한 소관 업무를 수행하는 것이 불가능하거나 현저히 곤란한 경우
5. 개인정보를 수집·이용하지 않고는 정보주체와 계약을 체결하고, 체결된 계약의 내용에 따른 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우
6. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자(정보주체를 제외한 그 밖의 모든 자를 말한다)의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
7. 개인정보처리자가 법령 또는 정보주체와의 계약 등에 따른 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 다만, 이 경우 개인정보의 수집·이용은 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니한 경우에 한한다.

③ 개인정보처리자는 정보주체로부터 직접 명함 또는 그와 유사한 매체(이하 "명함등"이라 함)를 제공받음으로써 개인정보를 수집하는 경우 명함등을 제공하는 정황 등에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

④ 개인정보처리자는 인터넷 홈페이지 등 공개된 매체 또는 장소(이하 "인터넷 홈페이지등"이라 함)에서 개인정보를 수집하는 경우 정보주체의 동의 의사가 명확히 표시되거나 인터넷 홈페이지등의 표시 내용에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

⑤ 개인정보처리자는 계약 등의 상대방인 정보주체가 대리인을 통하여 법률행위 또는 의사표시를 하는 경우 대리인의 대리권 확인을 위한 목적으로만 대리인의 개인정보를 수집·이용할 수 있다.

⑥ 근로자와 사용자가 근로계약을 체결하는 경우 「근로기준법」에 따른 임금지급, 교육, 증명서 발급, 근로자 복지제공을 위하여 근로자의 동의 없이 개인정보를 수집·이용할 수 있다.

제7조(개인정보의 제공) ① 개인정보의 "제공"이란 개인정보의 저장 매체나 개인정보가 담긴 출력물·책자 등을 물리적으로 이전하거나 네트워크를 통한 개인정보의 전송, 개인정보에 대한 제3자의 접근권한 부여, 개인정보처리자와 제3자의 개인정보 공유 등 개인정보의 이전 또는 공동 이용 상태를 초래하는 모든 행위를 말한다.

② 법 제17조의 "제3자"란 정보주체와 정보주체에 관한 개인정보를 수집·보유하고 있는 개인정보처리자를 제외한 모든 자를 의미하며, 정보주체의 대리인(명백히 대리의 범위 내에 있는 것에 한한다)과 법 제26조제2항에 따른 수탁자는 제외한다(이하 같다).

③ 개인정보처리자가 법 제17조제2항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

제8조(개인정보의 목적 외 이용·제공) ① 개인정보처리자가 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 이용 기간, 이용 형태 등을 제한하거나, 개인정보의 안전성 확보를 위하여 필요한 구체적인 조치를 마련하도록 문서(전자문서를 포함한다. 이하 같다)로 요청하여야 한다. 이 경우 요청을 받은 자는 그에 따른 조치를 취하고 그 사실을 개인정보를 제공한 개인정보처리자에게 문서로 알려야 한다.

② 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 자는 해당 개인정보를 제공받는 자와 개인정보의 안전성 확보 조치에 관한 책임관계를 명확히 하여야 한다.

③ 개인정보처리자가 법 제18조제3항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

④ 개인정보처리자가 법 제18조제2항제4호에 따라 개인정보를 제3자에게 제공하는 경우에는 다른 정보와 결합하여서도 특정 개인을 알아볼 수 없는 형태로 제공하여야 한다.

제9조(개인정보 수집 출처 등 고지) ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정당한 사유가 없는 한 정보주체의 요구가 있은 날로부터 3일 이내에 법 제20조제1항 각 호의 모든 사항을 정보주체에게 알려야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니 하다.

1. 고지를 요구하는 대상이 되는 개인정보가 법 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우
2. 고지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

② 개인정보처리자는 제1항 단서에 따라 제1항 전문에 따른 정보주체의 요구를 거부하는 경우에는 정당한 사유가 없는 한 정보주체의 요구가 있은 날로부터 3일 이내에 그 거부의 근거와 사유를 정보주체에게 알려야 한다.

제10조(개인정보의 파기방법 및 절차) ① 개인정보처리자는 개인정보의 보유 기간이 경과하거나 개인정보의 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 그로부터 5일 이내에 그 개인정보를 파기하여야 한다.

② 영 제16조제1항제1호의 '복원이 불가능한 방법'이란 현재의 기술수준에서 사회통념상 적정한 비용으로 파기한 개인정보의 복원이 불가능하도록 조치하는 방법을 말한다.

③ 개인정보처리자는 개인정보의 파기에 관한 사항을 기록·관리하여야 한다.

④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하여야 한다.

⑤ 개인정보처리자 중 공공기관의 개인정보파일 파기에 관하여는 제55조 및 제56조를 적용한다.

제11조(법령에 따른 개인정보의 보존) ① 개인정보처리자가 법 제21조제1항 단서에 따라 법령에 근거하여 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 물리적 또는 기술적 방법으로 분리하여서 저장·관리하여야 한다.

② 제1항에 따라 개인정보를 분리하여 저장·관리하는 경우에는 개인정보 처리방침 등을 통하여 법령에 근거하여 해당 개인정보 또는 개인정보파일을 저장·관리한다는 점을 정보주체가 알 수 있도록 하여야 한다.

제12조(동의를 받는 방법) ① 개인정보처리자가 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 하며, 정보주체의 동의는 동의가 필요한 개인정보에 한한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.

② 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 법 제18조제3항 각 호의 사항을 알리고 동의를 받아야 한다.

1. 개인정보를 수집·이용하고자 하는 경우로서 법 제15조제1항제2호 내지 제6호에 해당하지 않은 경우
2. 법 제18조제2항에 따라 개인정보를 수집 목적 외의 용도로 이용하거나 제공하고자 하는 경우
3. 법 제22조제3항에 해당하여 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하고자 하는 경우
4. 주민등록번호 외의 고유식별정보 처리가 필요한 경우로서 법령에 고유식별정보 처리 근거가 없는 경우
5. 민감정보를 처리하고자 하는 경우로서 법령에 민감정보 처리 근거가 없는 경우

③ 개인정보처리자는 제2항 각 호에 해당하여 개인정보를 처리하고자 하는 경우에는 정보주체에게 동의 또는 동의 거부를 선택할 수 있음을 명시적으로 알려야 한다.

④ 개인정보처리자는 법 제15조제1항제2호 내지 제6호에 따라 정보주체의 동의 없이 개인정보를 수집하는 경우에는 개인정보를 수집할 수 있는 법적 근거 등을 정보주체에게 알리기 위해 노력하여야 한다.

⑤ 개인정보처리자가 영 제17조제1항제2호의 규정에 따라 전화에 의한 동의와 관련하여 통화내용을 녹취할 때에는 녹취사실을 정보주체에게 알려야 한다.

⑥ 개인정보처리자가 친목단체를 운영하기 위하여 다음 각 호의 어느 하나에 해당하는 개인정보를 수집하는 경우에는 정보주체의 동의 없이 개인정보를 수집·이용할 수 있다.

1. 친목단체의 가입을 위한 성명, 연락처 및 친목단체의 회칙으로 정한 공통의 관심사나 목표와 관련된 인적 사항
2. 친목단체의 회비 등 친목유지를 위해 필요한 비용의 납부현황에 관한 사항
3. 친목단체의 활동에 대한 구성원의 참석여부 및 활동내용에 관한 사항
4. 기타 친목단체의 구성원 상호 간의 친교와 화합을 위해 구성원이 다른 구성원에게 알리기를 원하는 생일, 취향 및 가족의 애경사 등에 관한 사항

⑦ 개인정보처리자가 정보주체의 동의를 받기 위하여 동의서를 작성하는 경우에는 「개인정보 수집·제공 동의서 작성 가이드라인」을 준수하여야 한다.

제13조(법정대리인의 동의) ① 영 제17조제3항에 따라 개인정보처리자가 법정대리인의 성명·연락처를 수집할 때에는 해당 아동에게 자신의 신분과 연락처, 법정대리인의 성명과 연락처를 수집하고자 하는 이유를 알려야 한다.

② 개인정보처리자는 법 제22조제5항에 따라 수집한 법정대리인의 개인정보를 법정대리인의 동의를 얻기 위한 목적으로만 이용하여야 하며, 법정대리인의 동의 거부가 있거나 법정대리인의 동의 의사가 확인되지 않는 경우 수집일로부터 5일 이내에 파기해야 한다.

제14조(정보주체의 사전 동의를 받을 수 없는 경우) 개인정보처리자가 법 제15조제1항제5호 및 법 제18조제2항제3호에 따라 정보주체의 사전 동의 없이 개인정보를 수집·이용 또는 제공한 경우 당해 사유가 해소된 때에는 개인정보의 처리를 즉시 중단하여야 하며, 정보주체에게 사전 동의 없이 개인정보를 수집·이용 또는 제공한 사실과 그 사유 및 이용내역을 알려야 한다.

제15조(개인정보취급자에 대한 감독) ① 개인정보처리자는 개인정보취급자를 업무상 필요한 한도 내에서 최소한으로 두어야 하며, 개인정보취급자의 개인정보 처리 범위를 업무상 필요한 한도 내에서 최소한으로 제한하여야 한다.

② 개인정보처리자는 개인정보 처리시스템에 대한 접근권한을 업무의 성격에 따라 당해 업무수행에 필요한 최소한의 범위로 업무담당자에게 차등 부여하고 접근권한을 관리하기 위한 조치를 취해야 한다.

③ 개인정보처리자는 개인정보취급자에게 보안서약서를 제출하도록 하는 등 적절한 관리·감독을 해야 하며, 인사이동 등에 따라 개인정보취급자의 업무가 변경되는 경우에는 개인정보에 대한 접근권한을 변경 또는 말소해야 한다.

제2절 개인정보 처리의 위탁

제16조(수탁자의 선정 시 고려사항) 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)가 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라 한다)를 선정할 때에는 인력과 물적 시설, 재정 부담능력, 기술 보유의 정도, 책임능력 등 개인정보 처리 및 보호 역량을 종합적으로 고려하여야 한다.

제17조(개인정보 보호 조치의무) 수탁자는 위탁받은 개인정보를 보호하기 위하여 「개인정보의 안전성 확보조치 기준 고시」에 따른 관리적·기술적·물리적 조치를 하여야 한다.

제3절 개인정보 처리방침 작성

제18조(개인정보 처리방침의 작성기준 등) ① 개인정보처리자가 개인정보 처리방침을 작성하는 때에는 법 제30조제1항 각 호 및 영 제31조제1항 각 호의 사항을 명시적으로 구분하되, 알기 쉬운 용어로 구체적이고 명확하게 표현하여야 한다.

② 개인정보처리자는 처리하는 개인정보가 개인정보의 처리 목적에 필요한 최소한이라는 점을 밝혀야 한다.

제19조(개인정보 처리방침의 기재사항) 개인정보처리자가 개인정보 처리방침을 작성할 때에는 법 제30조제1항에 따라 다음 각 호의 사항을 모두 포함하여야 한다.

1. 개인정보의 처리 목적
2. 처리하는 개인정보의 항목
3. 개인정보의 처리 및 보유 기간
4. 개인정보의 제3자 제공에 관한 사항(해당하는 경우에만 정한다)
5. 개인정보의 파기에 관한 사항
6. 개인정보 처리 수탁자 담당자 연락처, 수탁자의 관리 현황 점검 결과 등 개인정보처리 위탁에 관한 사항(해당하는 경우에만 정한다)
7. 영 제30조제1항에 따른 개인정보의 안전성 확보조치에 관한 사항
8. 개인정보의 열람, 정정·삭제, 처리정지 요구권 등 정보주체의 권리·의무 및 그 행사방법에 관한 사항
9. 개인정보 처리방침의 변경에 관한 사항
10. 개인정보 보호책임자에 관한 사항
11. 개인정보의 열람청구를 접수·처리하는 부서
12. 정보주체의 권익침해에 대한 구제방법

제20조(개인정보 처리방침의 공개) ① 개인정보처리자가 법 제30조제2항에 따라 개인정보 처리방침을 수립하는 경우에는 인터넷 홈페이지를 통해 지속적으로 게재하여야 하며, 이 경우 "개인정보 처리방침"이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.

② 개인정보처리자가 인터넷 홈페이지를 운영하지 않는 경우 또는 인터넷 홈페이지 관리상의 하자가 있는 경우에는 영 제31조제3항 각 호의 어느 하나 이상의 방법으로 개인정보 처리방침을 공개하여야 한다. 이 경우에도 "개인정보 처리방침"이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.

③ 개인정보처리자가 영 제31조제3항제3호의 방법으로 개인정보 처리방침을 공개하는 경우에는 간행물·소식지·홍보지·청구서 등이 발행될 때마다 계속하여 게재하여야 한다.

제21조(개인정보 처리방침의 변경) 개인정보처리자가 개인정보 처리방침을 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개하여야 한다.

제4절 개인정보 보호책임자

제22조(개인정보 보호책임자의 공개) ① 개인정보처리자가 개인정보 보호책임자를 지정하거나 변경하는 경우 개인정보 보호책임자의 지정 및 변경 사실, 성명과 부서의 명칭, 전화번호 등 연락처를 공개하여야 한다.

② 개인정보처리자는 개인정보 보호책임자를 공개하는 경우 개인정보 보호와 관련한 고충처리 및 상담을 실제로 처리할 수 있는 연락처를 공개하여야 한다. 이 경우 개인정보 보호책임자와 개인정보 보호 업무를 처리하는 담당자의 성명, 부서의 명칭, 전화번호 등 연락처를 함께 공개할 수 있다.

제23조(개인정보 보호책임자의 교육) 영 제32조제3항에 따라 행정자치부장관이 개설 운영할 수 있는 개인정보 보호책임자에 대한 교육의 내용은 다음 각 호와 같다.

1. 개인정보 보호 관련 법령 및 제도의 내용
2. 법 제31조제2항 및 영 제32조제1항 각 호의 업무수행에 필요한 사항
3. 그 밖에 개인정보처리자의 개인정보 보호를 위하여 필요한 사항

제24조(교육계획의 수립 및 시행) ① 행정자치부장관은 매년 초 당해 연도 개인정보 보호책임자 교육계획을 수립하여 시행한다.

② 행정자치부장관은 제1항의 교육계획에 따라 사단법인 한국개인정보보호협의회 등의 단체에 개인정보 보호책임자 교육을 실시하게 할 수 있다.

③ 행정자치부장관은 개인정보 보호책임자가 지리적·경제적 여건에 구애받지 않고 편리하게 교육을 받은 수 있는 여건 조성을 위해 노력하여야 한다.

제5절 개인정보 유출 통지 및 신고 등

제25조(개인정보의 유출) 개인정보의 유출은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용한 것으로서 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2. 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
3. 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장 매체가 권한이 없는 자에게 잘못 전달된 경우

4. 기타 권한이 없는 자에게 개인정보가 전달된 경우

제26조(유출 통지시기 및 항목) ① 개인정보처리자는 개인정보가 유출되었음을 알게 된 때에는 정당한 사유가 없는 한 5일 이내에 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 그로부터 5일 이내에 정보주체에게 알릴 수 있다.

1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 개인정보처리자는 제1항 각 호의 사항을 모두 확인하기 어려운 경우에는 정보주체에게 다음 각 호의 사실만을 우선 알리고, 추후 확인되는 즉시 알릴 수 있다.

1. 정보주체에게 유출이 발생한 사실
2. 제1항의 통지항목 중 확인된 사항

③ 개인정보처리자는 개인정보 유출 사고를 인지하지 못해 유출 사고가 발생한 시점으로부터 5일 이내에 해당 정보주체에게 개인정보 유출 통지를 하지 아니한 경우에는 실제 유출 사고를 알게 된 시점을 입증하여야 한다.

제27조(유출 통지방법) ① 개인정보처리자는 정보주체에게 제26조제1항 각 호의 사항을 통지할 때에는 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 지체 없이 정보주체에게 알려야 한다.

② 개인정보처리자는 제1항의 통지방법과 동시에, 홈페이지 등을 통하여 제26조제1항 각 호의 사항을 공개할 수 있다.

제28조(개인정보 유출신고 등) ① 개인정보처리자는 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 정보주체에 대한 통지 및 조치결과를 5일 이내에 행정자치부장관 또는 영 제39조제2항의 전문기관에게 신고하여야 한다.

② 제1항에 따른 신고는 별지 제1호서식에 따른 개인정보 유출신고서를 통하여 하여야 한다.

③ 개인정보처리자는 전자우편, 팩스 또는 영 제39조제2항에 따른 전문기관의 인터넷 사이트를 통하여 유출신고를 할 시간적 여유가 없거나 그밖에 특별한 사정이 있는 때에는 먼저 전화를 통하여 제26조제1항의 사항을 신고한 후, 별지 제1호서식에 따른 개인정보 유출신고서를 제출할 수 있다.

④ 개인정보처리자는 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 제26조제1항에 따른 통지와 함께 인터넷 홈페이지 등에 정보주체가 알아보기 쉽도록 제26조제1항 각 호의 사항을 7일 이상 게재하여야 한다.

제29조(개인정보 유출 사고 대응 매뉴얼 등) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리자는 유출 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 「개인정보 유출 사고 대응 매뉴얼」을 마련하여야 한다.

1. 법 제2조제6호에 따른 공공기관
2. 그 밖에 1만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리자

② 제1항에 따른 개인정보 유출 사고 대응 매뉴얼에는 유출 통지·조회 절차, 영업점·인터넷 회선 확충 등 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다.

③ 개인정보처리자는 개인정보 유출에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

제30조(개인정보 침해 사실의 신고 처리 등) ① 개인정보처리자의 개인정보 처리로 인하여 개인정보에 관한 권리 또는 이익을 침해받은 사람은 법 제62조제2항에 따른 개인정보침해 신고센터에 침해 사실을 신고할 수 있다.

② 제1항에 따른 개인정보침해 신고센터는 다음 각 호의 업무를 수행한다.

1. 개인정보 처리와 관련한 신고의 접수·상담
2. 개인정보 침해 신고에 대한 사실 조사·확인 및 관계자의 의견 청취
3. 개인정보처리자에 대한 개인정보 침해 사실 안내 및 시정 유도
4. 사실 조사 결과가 정보주체의 권리 또는 이익 침해 사실이 없는 것으로 판단되는 경우 신고의 종결 처리
5. 법 제43조에 따른 개인정보 분쟁조정위원회 조정 안내 등을 통한 고충 해소 지원

제6절 정보주체의 권리 보장

제31조(개인정보 열람 연기 사유의 소멸) ① 개인정보처리자가 법 제35조제3항 후문에 따라 개인정보의 열람을 연기한 후 그 사유가 소멸한 경우에는 정당한 사유가 없는 한 사유가 소멸한 날로부터 10일 이내에 열람하도록 하여야 한다.

② 정보주체로부터 영 제41조제1항제4호의 규정에 따른 개인정보의 제3자 제공 현황의 열람청구를 받은 개인정보처리자는 국가안보에 긴요한 사안으로 법 제35조제4항제3호마목의 규정에 따른 업무를 수행하는데 중대한 지장을 초래하는 경우, 제3자에게 열람청구의 허용 또는 제한, 거부와 관련한 의견을 조회하여 결정할 수 있다.

제32조(개인정보의 정정·삭제) ① 개인정보처리자가 법 제36조제1항에 따른 개인정보의 정정·삭제 요구를 받았을 때는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

② 정보주체의 정정·삭제 요구가 법 제36조제1항 단서에 해당하는 경우에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 삭제를 요구할 수 없는 근거법령의 내용을 정보주체에게 알려야 한다.

제33조(개인정보의 처리정지) ① 개인정보처리자가 정보주체로부터 법 제37조제1항에 따라 개인정보처리를 정지하도록 요구받은 때에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 개인정보 처리의 일부 또는 전부를 정지하여야 한다. 다만, 법 제37조제2항 단서에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.

② 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 정당한 사유가 없는 한 처리정지의 요구를 받은 날로부터 10일 이내에 해당 개인정보의 파기 등 정보주체의 요구에 상응하는 조치를 취하고 그 결과를 정보주체에게 알려야 한다.

제34조(권리행사의 방법 및 절차) ① 개인정보처리자는 정보주체가 법 제38조제1항에 따른 열람등요구를 하는 경우에는 개인정보를 수집하는 방법과 동일하거나 보다 쉽게 정보주체가 열람요구 등 권리를 행사할 수 있도록 간편한 방법을 제공하여야 하며, 개인정보의 수집시에 요구되지 않았던 증빙서류 등을 요구하거나 추가적인 절차를 요구할 수 없다.

② 제1항의 규정은 영 제46조에 따라 본인 또는 정당한 대리인임을 확인하고자 하는 경우와 영 제47조에 따른 수수료와 우송료의 정산에도 준용한다.

제3장 영상정보처리기기 설치·운영
제1절 영상정보처리기기의 설치

제35조(적용범위) 이 장은 영상정보처리기기운영자가 공개된 장소에 설치·운영하는 영상정보처리기기와 이 기기를 통하여 처리되는 개인영상정보를 대상으로 한다.

제36조(영상정보처리기기 운영·관리 지침) ① 영상정보처리기기 운영·관리 지침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.

② 영상정보처리기기 운영·관리 지침을 마련한 경우에는 법 제30조에 따른 개인정보 처리방침을 정하지 아니하거나, 영상정보처리기기 설치·운영에 관한 사항을 법 제30조에 따른 개인정보 처리방침에 포함하여 정할 수 있다.

제37조(관리책임자의 지정) ① 영상정보처리기기운영자는 개인영상정보의 처리에 관한 업무를 총괄해서 책임질 관리책임자를 지정하여야 한다.

② 제1항의 관리책임자는 법 제31조제2항에 따른 개인정보 보호책임자의 업무에 준하여 다음 각 호의 업무를 수행한다.

1. 개인영상정보 보호 계획의 수립 및 시행
2. 개인영상정보 처리 실태 및 관행의 정기적인 조사 및 개선

3. 개인영상정보 처리와 관련한 불만의 처리 및 피해구제
4. 개인영상정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인영상정보 보호 교육 계획 수립 및 시행
6. 개인영상정보 파일의 보호 및 파기에 대한 관리·감독
7. 그 밖에 개인영상정보의 보호를 위하여 필요한 업무

③ 법 제31조에 따른 개인정보 보호책임자가 지정되어 있는 경우에는 그 개인정보 보호책임자가 관리책임자의 업무를 수행할 수 있다.

제38조(사전의견 수렴) 영상정보처리기기의 설치 목적 변경에 따른 추가 설치 등의 경우에도 영 제23조제1항에 따라 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

제39조(안내판의 설치) ① 영상정보처리기기운영자는 정보주체가 영상정보처리기기가 설치·운영 중임을 쉽게 알아볼 수 있도록 법 제25조제4항 본문에 따라 다음 각 호의 사항을 기재한 안내판 설치 등 필요한 조치를 하여야 한다.

1. 설치목적 및 장소
2. 촬영범위 및 시간
3. 관리책임자의 성명 또는 직책 및 연락처
4. 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 수탁자의 명칭 및 연락처

② 제1항에 따른 안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 누구라도 용이하게 판독할 수 있게 설치되어야 하며, 이 범위 내에서 영상정보처리기기운영자가 안내판의 크기, 설치위치 등을 자율적으로 정할 수 있다.

③ 공공기관의 장이 기관 내 또는 기관 간에 영상정보처리기기의 효율적 관리 및 정보 연계 등을 위해 용도별·지역별 영상정보처리기기를 물리적·관리적으로 통합하여 설치·운영(이하 '통합관리'라 한다)하는 경우에는 설치목적 등 통합관리에 관한 내용을 정보주체가 쉽게 알아볼 수 있도록 제1항에 따른 안내판에 기재하여야 한다.

제2절 개인영상정보의 처리

제40조(개인영상정보 이용·제3자 제공 등 제한 등) ① 영상정보처리기기운영자는 다음 각 호의 경우를 제외하고는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하여서는 아니 된다. 다만 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

1. 정보주체에게 동의를 얻은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우

4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인영상정보를 제공하는 경우
5. 개인영상정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

제41조(보관 및 파기) ① 영상정보처리기기운영자는 수집한 개인영상정보를 영상정보처리기기 운영·관리 방침에 명시한 보관 기간이 만료한 때에는 지체 없이 파기하여야 한다. 다만, 다른 법령에 특별한 규정이 있는 경우에는 그러하지 아니하다.

② 영상정보처리기기운영자가 그 사정에 따라 보유 목적의 달성을 위한 최소한의 기간을 산정하기 곤란한 때에는 보관 기간을 개인영상정보 수집 후 30일 이내로 한다.

③ 개인영상정보의 파기 방법은 다음 각 호의 어느 하나와 같다.

1. 개인영상정보가 기록된 출력물(사진 등) 등은 파쇄 또는 소각
2. 전자기적(電磁氣的) 파일 형태의 개인영상정보는 복원이 불가능한 기술적 방법으로 영구 삭제

제42조(이용·제3자 제공·파기의 기록 및 관리) ① 영상정보처리기기운영자는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하는 경우에는 다음 각 호의 사항을 기록하고 이를 관리하여야 한다.

1. 개인영상정보 파일의 명칭
2. 이용하거나 제공받은 자(공공기관 또는 개인)의 명칭
3. 이용 또는 제공의 목적
4. 법령상 이용 또는 제공근거가 있는 경우 그 근거
5. 이용 또는 제공의 기간이 정하여져 있는 경우에는 그 기간
6. 이용 또는 제공의 형태

② 영상정보처리기기운영자가 개인영상정보를 파기하는 경우에는 다음 사항을 기록하고 관리하여야 한다.

1. 파기하는 개인영상정보 파일의 명칭
2. 개인영상정보 파기 일시 (사전에 파기 시기 등을 정한 자동 삭제의 경우에는 파기 주기 및 자동 삭제 여부에 관한 확인 시기)
3. 개인영상정보 파기 담당자

제43조(영상정보처리기기 설치 및 관리 등의 위탁) ① 영상정보처리기기운영자가 영 제26조제1항에 따라 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁하는 경우에는 그

내용을 정보주체가 언제든지 쉽게 확인할 수 있도록 영 제24조에 따른 안내판 및 영 제27조에 따른 영상정보처리기기 운영·관리 방침에 수탁자의 명칭 등을 공개하여야 한다.

② 영상정보처리기기운영자가 영 제26조제1항에 따라 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁할 경우에는 그 사무를 위탁받은 자가 개인영상정보를 안전하게 처리하고 있는지를 관리·감독하여야 한다.

제3절 개인영상정보의 열람등 요구

제44조(정보주체의 열람등 요구) ① 정보주체는 영상정보처리기기운영자가 처리하는 개인영상정보에 대하여 열람 또는 존재확인(이하 "열람등"이라 한다)을 해당 영상정보처리기기운영자에게 요구할 수 있다. 이 경우 정보주체가 열람등을 요구할 수 있는 개인영상정보는 정보주체 자신이 촬영된 개인영상정보 및 명백히 정보주체의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 개인영상정보에 한한다.

② 영상정보처리기기운영자가 공공기관인 경우에는 해당 기관의 장에게 별지 제2호서식에 따른 개인영상정보 열람·존재확인 청구서(전자문서를 포함한다)로 하여야 한다.

③ 영상정보처리기기운영자는 제1항에 따른 요구를 받았을 때에는 지체 없이 필요한 조치를 취하여야 한다. 이때에 영상정보처리기기운영자는 열람등 요구를 한 자가 본인이거나 정당한 대리인인지를 주민등록증·운전면허증·여권 등의 신분증명서를 제출받아 확인하여야 한다.

④ 제3항의 규정에도 불구하고 다음 각 호에 해당하는 경우에는 영상정보처리기기운영자는 정보주체의 개인영상정보 열람등 요구를 거부할 수 있다. 이 경우 영상정보처리기기운영자는 10일 이내에 서면 등으로 거부 사유를 정보주체에게 통지하여야 한다.

1. 범죄수사·공소유지·재판수행에 중대한 지장을 초래하는 경우(공공기관에 한함)
2. 개인영상정보의 보관기간이 경과하여 파기한 경우
3. 기타 정보주체의 열람등 요구를 거부할 만한 정당한 사유가 존재하는 경우

⑤ 영상정보처리기기운영자는 제3항 및 제4항에 따른 조치를 취하는 경우 다음 각 호의 사항을 기록하고 관리하여야 한다.

1. 개인영상정보 열람등을 요구한 정보주체의 성명 및 연락처
2. 정보주체가 열람등을 요구한 개인영상정보 파일의 명칭 및 내용
3. 개인영상정보 열람등의 목적
4. 개인영상정보 열람등을 거부한 경우 그 거부의 구체적 사유
5. 정보주체에게 개인영상정보 사본을 제공한 경우 해당 영상정보의 내용과 제공한 사유

⑥ 정보주체는 영상정보처리기기운영자에게 정보주체 자신의 개인영상정보에 대한 파기를 요구하는 때에는 제1항에 의하여 보존을 요구하였던 개인영상정보에 대하여만 그 파기를 요구할 수 있다. 영상정보처리기기운영자가 해당 파기조치를 취한 경우에는 그 내용을 기록하고 관리하여야 한다.

제45조(개인영상정보 관리대장) 제42조제1항 및 제2항, 제44조제5항 및 제6항에 따른 기록 및 관리는 별지 제3호서식에 따른 ‘ 개인영상정보 관리대장 ’ 을 활용할 수 있다.

제46조(정보주체 이외의 자의 개인영상정보 보호) 영상정보처리기기운영자는 제44조제2항에 따른 열람등 조치를 취하는 경우, 만일 정보주체 이외의 자를 명백히 알아볼 수 있거나 정보주체 이외의 자의 사생활 침해의 우려가 있는 경우에는 해당되는 정보주체 이외의 자의 개인영상정보를 알아볼 수 없도록 보호조치를 취하여야 한다.

제4절 개인영상정보 보호 조치

제47조(개인영상정보의 안전성 확보를 위한 조치) 영상정보처리기기운영자는 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 법 제29조 및 영 제30조제1항에 따라 안전성 확보를 위하여 다음 각 호의 조치를 하여야 한다.

1. 개인영상정보의 안전한 처리를 위한 내부 관리계획의 수립·시행, 다만 「개인정보의 안전성 확보조치 기준 고시」 제2조제4호에 따른 ‘ 소상공인 ’ 은 내부관리계획을 수립하지 아니할 수 있다.
2. 개인영상정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용 (네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일 저장시 비밀번호 설정 등)
4. 처리기록의 보관 및 위조·변조 방지를 위한 조치 (개인영상정보의 생성 일시 및 열람할 경우에 열람 목적·열람자·열람 일시 등 기록·관리 조치 등)
5. 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치

제48조(개인영상정보처리기기의 설치·운영에 대한 점검) ① 공공기관의 장이 영상정보처리기기를 설치·운영하는 경우에는 이 지침의 준수 여부에 대한 자체점검을 실시하여 다음 해 3월 31일까지 그 결과를 행정자치부장관에게 통보하고 영 제34조제3항에 따른 시스템에 등록하여야 한다. 이 경우 다음 각 호의 사항을 고려하여야 한다.

1. 영상정보처리기기의 운영·관리 방침에 열거된 사항
2. 관리책임자의 업무 수행 현황
3. 영상정보처리기기의 설치 및 운영 현황
4. 개인영상정보 수집 및 이용·제공·파기 현황
5. 위탁 및 수탁자에 대한 관리·감독 현황
6. 정보주체의 권리행사에 대한 조치 현황
7. 기술적·관리적·물리적 조치 현황
8. 영상정보처리기 설치·운영의 필요성 지속 여부 등

② 공공기관의 장은 제1항과 제3항에 따른 영상정보처리기기 설치·운영에 대한 자체점검을 완료한 후에는 그 결과를 홈페이지 등에 공개하여야 한다.

③ 공공기관 외의 영상정보처리기기운영자는 영상정보처리기기 설치·운영으로 인하여 정보주체의 개인영상정보의 침해가 우려되는 경우에는 자체점검 등 개인영상정보의 침해 방지를 위해 적극 노력하여야 한다.

제4장 공공기관 개인정보파일 등록·공개

제1절 총칙

제49조(적용대상) 이 장의 적용대상은 다음과 같다.

1. 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체
2. 「국가인권위원회법」에 따른 국가인권위원회
3. 「공공기관의 운영에 관한 법률」에 따른 공공기관
4. 「지방공기업법」에 따른 지방공사 및 지방공단
5. 특별법에 의하여 설립된 특수법인
6. 「초·중등교육법」,「고등교육법」및 그 밖의 다른 법률에 따라 설치된 각급 학교

제50조(적용제외) 이 장은 다음 각 호의 어느 하나에 해당하는 개인정보파일에 관하여는 적용하지 아니한다.

1. 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속기관을 포함한다)에서 관리하는 개인정보파일
2. 법 제32조제2항에 따라 적용이 제외되는 다음 각목의 개인정보파일
   가. 국가안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
   나. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국 관리에 관한 사항을 기록한 개인정보파일
   다. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
   라. 공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일
   마. 다른 법령에 따라 비밀로 분류된 개인정보파일
3. 법 제58조제1항에 따라 적용이 제외되는 다음 각목의 개인정보파일
   가. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보파일
   나. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보파일
   다. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일
4. 영상정보처리기기를 통하여 처리되는 개인영상정보파일
5. 자료·물품 또는 금전의 송부, 1회성 행사 수행 등의 목적만을 위하여 운용하는 경우로서 저장하거나 기록하지 않고 폐기할 목적으로 수집된 개인정보파일

6.「금융실명거래 및 비밀보장에 관한 법률」에 따른 금융기관이 금융업무 취급을 위해 보유하는 개인정보파일

제2절 개인정보파일의 등록주체와 절차

제51조(개인정보파일 등록 주체) ① 개인정보파일을 운용하는 공공기관의 개인정보 보호책임자는 그 현황을 행정자치부에 등록하여야 한다.

② 중앙행정기관, 광역자치단체, 특별자치시도, 기초자치단체는 행정자치부에 직접 등록하여야 한다.

③ 교육청 및 각급 학교 등은 교육부를 통하여 행정자치부에 등록하여야 한다.

④ 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관을 통하여 행정자치부에 등록하여야 한다.

제52조(개인정보파일 등록 및 변경 신청) ① 개인정보파일을 운용하는 공공기관의 개인정보취급자는 해당 공공기관의 개인정보 보호책임자에게 개인정보파일 등록을 신청하여야 한다.

② 개인정보파일 등록 신청 사항은 다음의 각 호와 같다. 신청은 「개인정보 보호법 시행규칙」(이하 "시행규칙"이라 한다) 제3조제2항에 따른 별지 제2호서식의 ‘개인정보파일 등록·변경등록 신청서‘를 활용할 수 있다.

1. 개인정보파일을 운용하는 공공기관의 명칭
2. 개인정보파일의 명칭
3. 개인정보파일의 운영 근거 및 목적
4. 개인정보파일에 기록되는 개인정보의 항목
5. 개인정보파일로 보유하고 있는 개인정보의 정보주체 수
6. 개인정보의 처리 방법
7. 개인정보의 보유 기간
8. 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
9. 해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서
10. 개인정보의 열람 요구를 접수·처리하는 부서
11. 개인정보파일의 개인정보 중 법 제35조제4항에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유
12. 법 제33조제1항에 따른 개인정보 영향평가를 받은 개인정보파일의 경우에는 그 영향평가의 결과

③ 개인정보취급자는 등록한 사항이 변경된 경우에는 시행규칙 제3조제2항에 따른 별지 제2호서식의 ‘개인정보파일 등록·변경등록 신청서‘를 활용하여 개인정보 보호책임자에게 변경을 신청하여야 한다.

제53조(개인정보파일 등록 및 변경 확인) ① 개인정보파일 등록 또는 변경 신청을 받은 개인정보 보호책임자는 등록·변경 사항을 검토하고 그 적정성을 판단한 후 행정자치부에 등록하여야 한다.

② 교육청 및 각급 학교 등의 개인정보 보호책임자는 교육부에 제1항에 따른 등록·변경 사항의 검토 및 적정성 판단을 요청한 후, 교육부의 확인을 받아 행정자치부에 등록하여야 한다.

③ 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관에 제1항에 따른 등록·변경 사항의 검토 및 적정성 판단을 요청한 후, 상위 관리기관의 확인을 받아 행정자치부에 등록하여야 한다.

④ 제1항부터 제3항의 등록은 60일 이내에 하여야 한다.

제54조(개인정보파일 표준목록 등록과 관리) ① 특별지방행정기관, 지방자치단체, 교육기관(학교 포함) 등 전국적으로 단일한 공통업무를 집행하고 있는 기관은 각 중앙행정기관에서 제공하는 '개인정보파일 표준목록'에 따라 등록해야 한다.

② 전국 단일의 공통업무와 관련된 개인정보파일 표준목록은 해당 중앙부처에서 등록·관리해야 한다.

제55조(개인정보파일의 파기) ① 공공기관은 개인정보파일의 보유기간 경과, 처리 목적 달성 등 개인정보파일이 불필요하게 되었을 때에는 지체 없이 그 개인정보파일을 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 공공기관은 개인정보파일의 보유기간, 처리 목적 등을 반영한 개인정보 파기계획을 수립·시행하여야 한다. 다만, 영 제30조제1항제1호에 따른 내부 관리계획이 수립되어 있는 경우에는 내부 관리계획에 개인정보 파기계획을 포함하여 시행할 수 있다.

③ 개인정보취급자는 보유기간 경과, 처리 목적 달성 등 파기 사유가 발생한 개인정보파일을 선정하고, 별지 제4호서식에 따른 개인정보파일 파기요청서에 파기 대상 개인정보파일의 명칭, 파기방법 등을 기재하여 개인정보 보호책임자의 승인을 받아 개인정보를 파기하여야 한다.

④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하고 별지 제5호서식에 따른 개인정보파일 파기 관리대장을 작성하여야 한다.

제56조(개인정보파일 등록 사실의 삭제) ① 개인정보취급자는 제55조에 따라 개인정보파일을 파기한 경우, 법 제32조에 따른 개인정보파일의 등록사실에 대한 삭제를 개인정보 보호책임자에게 요청해야 한다.

② 개인정보파일 등록의 삭제를 요청받은 개인정보 보호책임자는 그 사실을 확인하고, 지체 없이 등록 사실을 삭제한 후 그 사실을 행정자치부에 통보한다.

제57조(등록·파기에 대한 개선권고) ① 공공기관의 개인정보 보호책임자는 제53조제1항에 따라 검토한 개인정보파일이 과다하게 운용되고 있다고 판단되는 경우에는 개선을 권고할 수 있다.

② 교육청 및 각급 학교, 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관의 개인정보 보호책임자는 제53조제2항 및 제53조제3항에 따라 검토한 개인정보파일이 과다하게 운용된다고 판단되거나, 등록되지 않은 파일이 있는 것으로 확인되는 경우에는 개선을 권고할 수 있다.

③ 행정자치부장관은 개인정보파일의 등록사항과 그 내용을 검토하고 다음 각 호의 어느 하나에 해당되는 경우에는 법 제32조제3항에 따라 해당 공공기관의 개인정보 보호책임자에게 개선을 권고할 수 있다.

1. 개인정보파일이 과다하게 운용된다고 판단되는 경우
2. 등록하지 않은 개인정보파일이 있는 경우
3. 개인정보파일 등록 사실이 삭제되었음에도 불구하고 개인정보파일을 계속 보유하고 있는 경우
4. 개인정보 영향평가를 받은 개인정보파일을 보유하고 있음에도 그 결과를 등록사항에 포함하지 않은 경우
5. 기타 법 제32조에 따른 개인정보파일의 등록 및 공개에 위반되는 사항이 있다고 판단되는 경우

④ 행정자치부장관은 제3항에 따라 개선을 권고한 경우에는 그 내용 및 결과에 대하여 개인정보 보호위원회의 심의·의결을 거쳐 공표할 수 있다.

⑤ 행정자치부장관은 공공기관의 개인정보파일 등록·파기 현황에 대한 점검을 실시할 수 있다.

제3절 개인정보파일의 관리 및 공개

제58조(개인정보파일대장 작성) 공공기관은 1개의 개인정보파일에 1개의 개인정보파일대장을 작성해야 한다.

제59조(개인정보파일 이용·제공 관리) 공공기관은 법 제18조제2항 각 호에 따라 제3자가 개인정보파일의 이용·제공을 요청한 경우에는 각각의 이용·제공 가능 여부를 확인하고 별지 제6호서식의 '개인정보 목적 외 이용·제공대장'에 기록하여 관리해야 한다.

제60조(개인정보파일 보유기간의 산정) ① 보유기간은 전체 개인정보가 아닌 개별 개인정보의 수집부터 삭제까지의 생애주기로서 보유목적에 부합된 최소기간으로 산정하되, 개별 법령의 규정에 명시된 자료의 보존기간에 따라 산정해야 한다.

② 개별 법령에 구체적인 보유기간이 명시되어 있지 않은 경우에는 개인정보 보호책임자의 협의를 거쳐 기관장의 결재를 통하여 산정해야 한다. 다만, 보유기간은 별표 1의 개인정보파일 보유기간 책정 기준표에서 제시한 기준과 「공공기록물 관리에 관한 법률 영」에 따른 기록관리기준표를 상회할 수 없다.

③ 정책고객, 홈페이지회원 등의 홍보 및 대국민서비스 목적의 외부고객 명부는 특별한 경우를 제외하고는 2년을 주기로 정보주체의 재동의 절차를 거쳐 동의한 경우에만 계속하여 보유할 수 있다.

제61조(개인정보파일 현황 공개 및 방법) ① 공공기관의 개인정보 보호책임자는 개인정보파일의 보유·파기현황을 주기적으로 조사하여 그 결과를 해당 공공기관의 개인정보 처리방침에 포함하여 관리해야 한다.

② 행정자치부장관은 개인정보파일 등록 현황을 누구든지 쉽게 열람할 수 있도록 공개하여야 한다.

③ 행정자치부는 전 공공기관의 개인정보파일 등록 및 삭제 현황을 종합하여 매년 공개해야 하며, 개인정보파일 현황 공개에 관한 업무를 전자적으로 처리하기 위하여 정보시스템을 구축·운영할 수 있다.

제5장 보칙

제62조(친목단체에 대한 벌칙조항의 적용배제) ① 친목단체의 개인정보처리자에 대하여는 법 제75조제1항제1호, 법 제75조제2항제1호, 법 제75조제3항제7호 및 법 제75조제3항제8호의 벌칙을 적용하지 아니한다.

② 제1항에서 규정한 사항을 제외한 벌칙규정은 친목단체의 개인정보처리자에 대하여도 적용한다.

제63조(처리 중인 개인정보에 관한 경과조치) ① 법 시행 전에 근거법령 없이 개인정보를 수집한 경우 당해 개인정보를 보유하는 것은 적법한 처리로 본다. 다만, 이 법 시행 이후 기존의 수집목적 범위 내에서 이용하는 경우를 제외하고 개인정보를 새롭게 처리하는 경우에는 법, 영, 시행규칙 및 이 지침에 따라야 한다.

② 법 시행 전에 법률의 근거 또는 정보주체의 동의 없이 제3자로부터 개인정보를 제공받아 목적 외의 용도로 이용하고 있는 개인정보처리자는 정보주체의 동의를 받아야 한다.

③ 법 시행 전에 개인정보를 수집한 개인정보처리자는 기존의 수집목적 범위에도 불구하고 제1항 단서 및 제2항을 준수하기 위하여 새롭게 정보주체의 동의를 받을 목적으로 법 시행 전에 수집한 개인정보를 이용할 수 있다.

부칙 <제2016 - 21호,2016.6.30>

이 규정은 발령한 날부터 시행한다.

[별표 1호]

개인정보파일 보유기간 책정 기준표

보유기간	대상 개인정보파일
영구	1. 국민의 지위, 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일 2. 국민의 건강증진과 관련된 업무를 수행하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일
준영구	1. 국민의 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 개인이 사망, 폐지 그 밖의 사유로 소멸되기 때문에 영구 보존할 필요가 없는 개인정보파일 2. 국민의 신분증명 및 의무부과, 특정대상 관리 등을 위하여 행정기관이 구축하여 운영하는 행정정보시스템의 데이터 셋으로 구성된 개인정보파일
30년	1. 관계 법령에 따라 10년 이상 30년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
10년	1. 관계 법령에 따라 5년 이상 10년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
5년	1. 관계 법령에 따라 3년 이상 5년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
3년	1. 행정업무의 참고 또는 사실 증명을 위하여 1년 이상 3년 미만의 기간 동안 보존할 필요가 있는 개인정보파일 2. 관계 법령에 따라 1년 이상 3년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 3. 각종 증명서 발급과 관련된 개인정보파일(단 다른 법령에서 증명서 발급 관련 보유기간이 별도로 규정된 경우 해당 법령에 따름)
1년	1. 상급기관(부서)의 요구에 따라 단순 보고를 위해 생성한 개인정보파일

[별지 제1호서식]

개인정보 유출신고서

기관명					
정보주체에의 통지 여부					
유출된 개인정보의 항목 및 규모					
유출된 시점과 그 경위					
유출피해 최소화 대책·조치 및 결과					
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차					
담당부서·담당자 및 연락처		성명	부서	직위	연락처
	개인정보 보호책임자				
	개인정보 취급자				

유출신고접수기관	기관명	담당자명	연락처

[별지 제2호서식] (앞 쪽)

개인영상정보(□ 존재확인 □ 열람) 청구서	처리기한
※ 아래 유의사항을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다.	10일 이내

청 구 인	성 명		전 화 번 호	
	생년월일		정보주체와의 관계	
	주 소			
정보주체의 인적사항	성 명		전 화 번 호	
	생년월일			
	주 소			
청구내용 (구체적으로 요청하지 않으면 처리가 곤란할 수 있음)	영상정보 기록기간	(예 : 2011.01.01 18:30 ~ 2011.01.01 19:00)		
	영상정보 처리기기 설치장소	(예 : 00시 00구 00대로 0 인근 CCTV)		
	청구 목적 및 사유			

「표준 개인정보 보호지침」 제44조에 따라 위와 같이 개인영상정보의 존재확인, 열람을 청구합니다.

년 월 일

청구인 (서명 또는 인)

○ ○ ○ ○ 귀하

담당자의 청구인에 대한 확인 서명	

[별지 제3호서식]

개인영상정보 관리대장

번호	구분	일시	파일 명/ 형태	담당자	목적/ 사유	이용 · 제공받는 제3자 /열람등 요구자	이용 · 제공 근거	이용 · 제공 형태	기간
1	□ 이용 □ 제공 □ 열람 □ 파기								
2	□ 이용 □ 제공 □ 열람 □ 파기								
3	□ 이용 □ 제공 □ 열람 □ 파기								
4	□ 이용 □ 제공 □ 열람 □ 파기								
5	□ 이용 □ 제공 □ 열람 □ 파기								
6	□ 이용 □ 제공 □ 열람 □ 파기								
7	□ 이용 □ 제공 □ 열람 □ 파기								

[별지 제4호서식]

개인정보파일 파기 요청서

작성일		작성자	
파기 대상 개인정보파일			
생성일자		개인정보취급자	
주요 대상업무		현재 보관건수	
파기 사유			
파기 일정			
특기사항			
파기 승인일		승인자 (개인정보 보호책임자)	
파기 장소			
파기 방법			
파기 수행자		입회자	
폐기 확인 방법			
백업 조치 유무			
매체 폐기 여부			

[별지 제5호서식]

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장

[별지 제6호서식]

개인정보 목적 외 이용·제공 대장

구분	주요내용
① 개인정보파일명	
② 이용 · 제공받는 기관	
③ 이용 · 제공일자	
④ 이용 · 제공주기	
⑤ 이용 · 제공형태	
⑥ 이용 · 제공목적	
⑦ 이용 · 제공근거	
⑧ 이용 · 제공항목	
⑨ 비고	

개인정보의 안전성 확보조치 기준

[시행 2016.9.1] [고시 제2016 - 35호, 2016.9.1, 전부개정]

제1조(목적) 이 기준은 「개인정보 보호법」(이하 “ 법 ”이라 한다) 제23조제2항, 제24조제3항 및 제29조와 같은 법 시행령(이하 “ 영 ”이라 한다) 제21조 및 제30조에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실、도난、유출、위조、변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적、관리적 및 물리적 안전조치에 관한 최소한의 기준을 정하는 것을 목적으로 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. “ 정보주체 ”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
2. “ 개인정보파일 ”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
3. “ 개인정보처리자 ”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
4. “ 대기업 ”이란 「독점규제 및 공정거래에 관한 법률」제14조에 따라 공정거래위원회가 지정한 기업집단을 말한다.
5. “ 중견기업 ”이란「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」제2조에 해당하는 기업을 말한다.
6. “ 중소기업 ”이란 「중소기업기본법」제2조 및 동법 시행령 제3조에 해당하는 기업을 말한다.
7. “ 소상공인 ”이란 「소상공인 보호 및 지원에 관한 법률」제2조에 해당하는 자를 말한다.
8. “ 개인정보 보호책임자 ”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.
9. “ 개인정보취급자 ”란 개인정보처리자의 지휘、감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
10. “ 개인정보처리시스템 ”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
11. “ 위험도 분석 ”이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별、평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행

위를 말한다.

12. “비밀번호”란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
13. “정보통신망”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
14. “공개된 무선망”이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
15. “모바일 기기”란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
16. “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
17. “보조저장매체”란 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.
18. “내부망”이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
19. “접속기록”이란 개인정보취급자 등이 개인정보처리시스템에 접속한 사실을 알 수 있는 계정, 접속일시, 접속자 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
20. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

제3조(안전조치 기준 적용) 개인정보처리자가 개인정보의 안전성 확보에 필요한 조치를 하는 경우에는 [별표] 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준을 적용하여야 한다. 이 경우 개인정보처리자가 어느 유형에 해당하는지에 대한 입증책임은 당해 개인정보처리자가 부담한다.

제4조(내부 관리계획의 수립·시행) ① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다.

1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보취급자에 대한 교육에 관한 사항

4. 접근 권한의 관리에 관한 사항
5. 접근 통제에 관한 사항
6. 개인정보의 암호화 조치에 관한 사항
7. 접속기록 보관 및 점검에 관한 사항
8. 악성프로그램 등 방지에 관한 사항
9. 물리적 안전조치에 관한 사항
10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항
11. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
12. 위험도 분석 및 대응방안 마련에 관한 사항
13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항
14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
15. 그 밖에 개인정보 보호를 위하여 필요한 사항

② [별표]의 유형1에 해당하는 개인정보처리자는 제1항에 따른 내부 관리계획을 수립하지 아니할 수 있고, [별표]의 유형2에 해당하는 개인정보처리자는 제1항제12호부터 제14호까지를 내부 관리계획에 포함하지 아니할 수 있다.

③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

④ 개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리하여야 한다.

제5조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

⑥개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

⑦ [별표]의 유형1에 해당하는 개인정보처리자는 제1항 및 제6항을 아니할 수 있다.

제6조(접근통제) ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP (Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

③ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.

④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.

⑤ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.

⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근 통제 기능을 이용할 수 있다.

⑦ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

⑧ [별표]의 유형1에 해당하는 개인정보처리자는 제2항, 제4항부터 제5항까지의 조치를 아니할 수 있다.

제7조(개인정보의 암호화) ① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과

2. 암호화 미적용시 위험도 분석에 따른 결과

⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.

제8조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관·관리하여야 한다.

② 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.

③ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제9조(악성프로그램 등 방지) 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시
3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

제10조(관리용 단말기의 안전조치) 개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.

1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
2. 본래 목적 외로 사용되지 않도록 조치
3. 악성프로그램 감염 방지 등을 위한 보안조치 적용

제11조(물리적 안전조치) ① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제12조(재해·재난 대비 안전조치) ① 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

② 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

③ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제1항부터 제2항까지 조치를 이행하지 아니할 수 있다.

제13조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

부칙 <제2016-35호,2016.9.1>

제1조(시행일) 이 고시는 2016년 9월 1일부터 시행한다.

제2조(적용례) 영 제21조의2제2항에 따른 주민등록번호의 암호화 적용시기 이후에는 고유식별정보 중 주민등록번호는 제7조제4항을 적용하지 아니한다.

[별표]

개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준

유형	적용 대상	안전조치 기준
유형1 (완화)	· 1만명 미만의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인	· 제5조 : 제2항부터 제5항까지 · 제6조 : 제1항, 제3항, 제6항 및 제7항 · 제7조 : 제1항부터 제5항까지, 제7항 · 제8조 · 제9조 · 제10조 · 제11조 · 제13조
유형2 (표준)	· 100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업 · 10만명 미만의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 · 1만명 이상의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인	· 제4조 : 제1항제1호부터 제11호까지 및 제 15호, 제3항부터 제4항까지 · 제5조 · 제6조 : 제1항부터 제7항까지 · 제7조 : 제1항부터 제5항까지, 제7항 · 제8조 · 제9조 · 제10조 · 제11조 · 제13조
유형3 (강화)	· 10만명 이상의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 · 100만명 이상의 정보주체에 관한 개인정보를 보유한 중소기업, 단체	· 제4조부터 제13조까지

개인정보 보호법

[시행 2016.9.30] [법률 제14107호, 2016.3.29, 일부개정]

제1장 총칙

제1조(목적) 이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다. <개정 2014.3.24>

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014.3.24>

1. "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
2. "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
3. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
5. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
6. "공공기관"이란 다음 각 목의 기관을 말한다.
   가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체
   나. 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관
7. "영상정보처리기기"란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.

제3조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.
⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
⑦ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.
⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.
1. 개인정보의 처리에 관한 정보를 제공받을 권리
2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
3. 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급을 포함한다. 이하 같다)을 요구할 권리
4. 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

제5조(국가 등의 책무) ① 국가와 지방자치단체는 개인정보의 목적 외 수집, 오용·남용 및 무분별한 감시·추적 등에 따른 폐해를 방지하여 인간의 존엄과 개인의 사생활 보호를 도모하기 위한 시책을 강구하여야 한다.
② 국가와 지방자치단체는 제4조에 따른 정보주체의 권리를 보호하기 위하여 법령의 개선 등 필요한 시책을 마련하여야 한다.
③ 국가와 지방자치단체는 개인정보의 처리에 관한 불합리한 사회적 관행을 개선하기 위하여 개인정보처리자의 자율적인 개인정보 보호활동을 존중하고 촉진·지원하여야 한다.
④ 국가와 지방자치단체는 개인정보의 처리에 관한 법령 또는 조례를 제정하거나 개정하는 경우에는 이 법의 목적에 부합되도록 하여야 한다.

제6조(다른 법률과의 관계) 개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다. <개정 2014.3.24>

제2장 개인정보 보호정책의 수립 등

제7조(개인정보 보호위원회) ① 개인정보 보호에 관한 사항을 심의·의결하기 위하여 대통령 소속으로 개인정보 보호위원회(이하 "보호위원회"라 한다)를 둔다. 보호위원회는 그 권한에 속하는 업무를 독립하여 수행한다.

② 보호위원회는 위원장 1명, 상임위원 1명을 포함한 15명 이내의 위원으로 구성하되, 상임위원은 정무직 공무원으로 임명한다.

③ 위원장은 위원 중에서 공무원이 아닌 사람으로 대통령이 위촉한다.

④ 위원은 다음 각 호의 어느 하나에 해당하는 사람을 대통령이 임명하거나 위촉한다. 이 경우 위원 중 5명은 국회가 선출하는 자를, 5명은 대법원장이 지명하는 자를 각각 임명하거나 위촉한다.

1. 개인정보 보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람
2. 개인정보처리자로 구성된 사업자단체로부터 추천을 받은 사람
3. 그 밖에 개인정보에 관한 학식과 경험이 풍부한 사람

⑤ 위원장과 위원의 임기는 3년으로 하되, 1차에 한하여 연임할 수 있다.

⑥ 보호위원회의 회의는 위원장이 필요하다고 인정하거나 재적위원 4분의 1 이상의 요구가 있는 경우에 위원장이 소집한다.

⑦ 보호위원회는 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 의결한다.

⑧ 보호위원회의 사무를 지원하기 위하여 보호위원회에 사무국을 둔다.

⑨ 제1항부터 제8항까지에서 규정한 사항 외에 보호위원회의 조직과 운영에 필요한 사항은 대통령령으로 정한다.

제8조(보호위원회의 기능 등) ① 보호위원회는 다음 각 호의 사항을 심의·의결한다. <개정 2015.7.24>

1. 제8조의2에 따른 개인정보 침해요인 평가에 관한 사항
1의2. 제9조에 따른 기본계획 및 제10조에 따른 시행계획
2. 개인정보 보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항
3. 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항
4. 개인정보 보호에 관한 법령의 해석·운용에 관한 사항
5. 제18조제2항제5호에 따른 개인정보의 이용·제공에 관한 사항
6. 제33조제3항에 따른 영향평가 결과에 관한 사항
7. 제61조제1항에 따른 의견제시에 관한 사항
8. 제64조제4항에 따른 조치의 권고에 관한 사항
9. 제66조에 따른 처리 결과의 공표에 관한 사항
10. 제67조제1항에 따른 연차보고서의 작성·제출에 관한 사항
11. 개인정보 보호와 관련하여 대통령, 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항

12. 그 밖에 이 법 또는 다른 법령에 따라 보호위원회가 심의·의결하는 사항

② 보호위원회는 제1항 각 호의 사항을 심의·의결하기 위하여 필요한 경우 다음 각 호의 조치를 할 수 있다.<개정 2015.7.24>

1. 관계 공무원, 개인정보 보호에 관한 전문 지식이 있는 사람이나 시민사회단체 및 관련 사업자로부터의 의견 청취
2. 관계 기관 등에 대한 자료제출이나 사실조회 요구

③ 제2항제2호에 따른 요구를 받은 관계 기관 등은 특별한 사정이 없으면 이에 응하여야 한다. <신설 2015.7.24>

④ 보호위원회는 제1항제2호의 사항을 심의·의결한 경우에는 관계 기관에 그 개선을 권고할 수 있다.<신설 2015.7.24>

⑤ 보호위원회는 제4항에 따른 권고 내용의 이행 여부를 점검할 수 있다.<신설 2015.7.24>

제8조의2(개인정보 침해요인 평가) ① 중앙행정기관의 장은 소관 법령의 제정 또는 개정을 통하여 개인정보 처리를 수반하는 정책이나 제도를 도입·변경하는 경우에는 보호위원회에 개인정보 침해요인 평가를 요청하여야 한다.

② 보호위원회가 제1항에 따른 요청을 받은 때에는 해당 법령의 개인정보 침해요인을 분석·검토하여 그 법령의 소관기관의 장에게 그 개선을 위하여 필요한 사항을 권고할 수 있다.

③ 제1항에 따른 개인정보 침해요인 평가의 절차와 방법에 관하여 필요한 사항은 대통령령으로 정한다.

[본조신설 2015.7.24]

제9조(기본계획) ① 보호위원회는 개인정보의 보호와 정보주체의 권익 보장을 위하여 3년마다 개인정보 보호 기본계획(이하 "기본계획"이라 한다)을 관계 중앙행정기관의 장과 협의하여 수립한다. <개정 2013.3.23, 2014.11.19, 2015.7.24>

② 기본계획에는 다음 각 호의 사항이 포함되어야 한다.

1. 개인정보 보호의 기본목표와 추진방향
2. 개인정보 보호와 관련된 제도 및 법령의 개선
3. 개인정보 침해 방지를 위한 대책
4. 개인정보 보호 자율규제의 활성화
5. 개인정보 보호 교육·홍보의 활성화
6. 개인정보 보호를 위한 전문인력의 양성
7. 그 밖에 개인정보 보호를 위하여 필요한 사항

③ 국회, 법원, 헌법재판소, 중앙선거관리위원회는 해당 기관(그 소속 기관을 포함한다)의 개인정보 보호를 위한 기본계획을 수립·시행할 수 있다.

제10조(시행계획) ① 중앙행정기관의 장은 기본계획에 따라 매년 개인정보 보호를 위한 시행계획을 작성하여 보호위원회에 제출하고, 보호위원회의 심의·의결을 거쳐 시행하여야 한다.

② 시행계획의 수립·시행에 필요한 사항은 대통령령으로 정한다.

제11조(자료제출 요구 등) ① 보호위원회는 기본계획을 효율적으로 수립하기 위하여 개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관·단체 등에 개인정보처리자의 법규 준수 현황과 개인정보 관리 실태 등에 관한 자료의 제출이나 의견의 진술 등을 요구할 수 있다. <개정 2013.3.23, 2014.11.19, 2015.7.24>

② 행정자치부장관은 개인정보 보호 정책 추진, 성과평가 등을 위하여 필요한 경우 개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관·단체 등을 대상으로 개인정보관리 수준 및 실태파악 등을 위한 조사를 실시할 수 있다.<신설 2015.7.24>

③ 중앙행정기관의 장은 시행계획을 효율적으로 수립·추진하기 위하여 소관 분야의 개인정보처리자에게 제1항에 따른 자료제출 등을 요구할 수 있다.<개정 2015.7.24>

④ 제1항부터 제3항까지에 따른 자료제출 등을 요구받은 자는 특별한 사정이 없으면 이에 따라야 한다.<개정 2015.7.24>

⑤ 제1항부터 제3항까지에 따른 자료제출 등의 범위와 방법 등 필요한 사항은 대통령령으로 정한다.<개정 2015.7.24>

제12조(개인정보 보호지침) ① 행정자치부장관은 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 표준 개인정보 보호지침(이하 "표준지침"이라 한다)을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다. <개정 2013.3.23, 2014.11.19>

② 중앙행정기관의 장은 표준지침에 따라 소관 분야의 개인정보 처리와 관련한 개인정보 보호지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.

③ 국회, 법원, 헌법재판소 및 중앙선거관리위원회는 해당 기관(그 소속 기관을 포함한다)의 개인정보 보호지침을 정하여 시행할 수 있다.

제13조(자율규제의 촉진 및 지원) 행정자치부장관은 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하고 지원하기 위하여 다음 각 호의 필요한 시책을 마련하여야 한다. <개정 2013.3.23, 2014.11.19>

1. 개인정보 보호에 관한 교육·홍보
2. 개인정보 보호와 관련된 기관·단체의 육성 및 지원
3. 개인정보 보호 인증마크의 도입·시행 지원
4. 개인정보처리자의 자율적인 규약의 제정·시행 지원
5. 그 밖에 개인정보처리자의 자율적 개인정보 보호활동을 지원하기 위하여 필요한 사항

제14조(국제협력) ① 정부는 국제적 환경에서의 개인정보 보호 수준을 향상시키기 위하여 필요한 시책을 마련하여야 한다.

② 정부는 개인정보 국외 이전으로 인하여 정보주체의 권리가 침해되지 아니하도록 관련 시책을 마련하여야 한다.

제3장 개인정보의 처리

제1절 개인정보의 수집, 이용, 제공 등

제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보의 수집·이용 목적
2. 수집하려는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

제16조(개인정보의 수집 제한) ① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.

② 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다.<신설 2013.8.6>

③ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.<개정 2013.8.6>

제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 제15조제1항제2호·제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

제18조(개인정보의 목적 외 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.

② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우

9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

③ 개인정보처리자는 제2항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보를 제공받는 자
2. 개인정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적을 말한다)
3. 이용 또는 제공하는 개인정보의 항목
4. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

④ 공공기관은 제2항제2호부터 제6호까지, 제8호 및 제9호에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 행정자치부령으로 정하는 바에 따라 관보 또는 인터넷 홈페이지 등에 게재하여야 한다.<개정 2013.3.23, 2014.11.19>

⑤ 개인정보처리자는 제2항 각 호의 어느 하나의 경우에 해당하여 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다. 이 경우 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다.

[제목개정 2013.8.6]

제19조(개인정보를 제공받은 자의 이용·제공 제한) 개인정보처리자로부터 개인정보를 제공받은 자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 개인정보를 제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공하여서는 아니 된다.

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우

제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지) ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.

1. 개인정보의 수집 출처
2. 개인정보의 처리 목적
3. 제37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실

② 제1항에도 불구하고 처리하는 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 제17조제1항제1호에 따라 정보주체 이외로부터 개인정보를 수집하여 처리하는 때에는 제1항 각 호의 모든 사항을 정보주체에게 알려야 한다. 다만, 개인정보처리자가 수집한 정보에 연락처 등 정보주체에게 알릴 수

있는 개인정보가 포함되지 아니한 경우에는 그러하지 아니하다.<신설 2016.3.29>

③ 제2항 본문에 따라 알리는 경우 정보주체에게 알리는 시기ㆍ방법 및 절차 등 필요한 사항은 대통령령으로 정한다.<신설 2016.3.29>

④ 제1항과 제2항 본문은 다음 각 호의 어느 하나에 해당하는 경우에는 적용하지 아니한다. 다만, 이 법에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한한다.<개정 2016.3.29>

1. 고지를 요구하는 대상이 되는 개인정보가 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우
2. 고지로 인하여 다른 사람의 생명ㆍ신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

제21조(개인정보의 파기) ① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

③ 개인정보처리자가 제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장ㆍ관리하여야 한다.

④ 개인정보의 파기방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

제22조(동의를 받는 방법) ① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제5항에 따른 법정대리인을 포함한다. 이하 이 조에서 같다)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다.

② 개인정보처리자는 제15조제1항제1호, 제17조제1항제1호, 제23조제1항제1호 및 제24조제1항제1호에 따라 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체와의 계약 체결 등을 위하여 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.<개정 2016.3.29>

③ 개인정보처리자는 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.

④ 개인정보처리자는 정보주체가 제2항에 따라 선택적으로 동의할 수 있는 사항을 동의하지 아니하거나 제3항 및 제18조제2항제1호에 따른 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.

⑤ 개인정보처리자는 만 14세 미만 아동의 개인정보를 처리하기 위하여 이 법에 따른 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 한다. 이 경우 법정대리인의 동의를 받기 위

하여 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.

⑥ 제1항부터 제5항까지에서 규정한 사항 외에 정보주체의 동의를 받는 세부적인 방법 및 제5항에 따른 최소한의 정보의 내용에 관하여 필요한 사항은 개인정보의 수집매체 등을 고려하여 대통령령으로 정한다.

제2절 개인정보의 처리 제한

제23조(민감정보의 처리 제한) ①개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. <개정 2016.3.29>

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다.<신설 2016.3.29>

제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 "고유식별정보"라 한다)를 처리할 수 없다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우

② 삭제 <2013.8.6>

③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.<개정 2015.7.24>

④ 행정자치부장관은 처리하는 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 제3항에 따라 안전성 확보에 필요한 조치를 하였는지에 관하여 대통령령으로 정하는 바에 따라 정기적으로 조사하여야 한다.<신설 2016.3.29>

⑤ 행정자치부장관은 대통령령으로 정하는 전문기관으로 하여금 제4항에 따른 조사를 수행하게 할 수 있다.<신설 2016.3.29>

제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 안전행정부령으로 정하는 경우

② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.<신설 2014.3.24, 2015.7.24>

③ 개인정보처리자는 제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.<개정 2014.3.24>

④ 안전행정부장관은 개인정보처리자가 제3항에 따른 방법을 제공할 수 있도록 관계 법령의 정비, 계획의 수립, 필요한 시설 및 시스템의 구축 등 제반 조치를 마련·지원할 수 있다.<개정 2014.3.24>

[본조신설 2013.8.6]

제25조(영상정보처리기기의 설치·운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영하여서는 아니 된다. 다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.

③ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하려는 공공기관의 장과 제2항 단서에 따라 영상정보처리기기를 설치·운영하려는 자는 공청회·설명회의 개최 등 대통령령으로 정하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

④ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자(이하 "영상정보처리기기운영자"라 한다)는 정보주체가 쉽게 인식할 수 있도록 다음 각 호의 사항이 포함된 안내판을 설치하는 등 필요한 조치를 하여야 한다. 다만, 「군사기지 및 군사시설 보호법」 제2조제2호에 따른 군사시설, 「통합방위법」 제2조제13호에 따른 국가중요시설, 그 밖에 대통령령으로 정하

는 시설에 대하여는 그러하지 아니하다.<개정 2016.3.29>

1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자 성명 및 연락처
4. 그 밖에 대통령령으로 정하는 사항

⑤ 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.

⑥ 영상정보처리기기운영자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따라 안전성 확보에 필요한 조치를 하여야 한다.<개정 2015.7.24>

⑦ 영상정보처리기기운영자는 대통령령으로 정하는 바에 따라 영상정보처리기기 운영·관리 방침을 마련하여야 한다. 이 경우 제30조에 따른 개인정보 처리방침을 정하지 아니할 수 있다.

⑧ 영상정보처리기기운영자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다. 다만, 공공기관이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 대통령령으로 정하는 절차 및 요건에 따라야 한다.

제26조(업무위탁에 따른 개인정보의 처리 제한) ① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적·관리적 보호조치에 관한 사항
3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항

② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.

④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.<개정 2015.7.24>

⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.

⑥ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다.

⑦ 수탁자에 관하여는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.

제27조(영업양도 등에 따른 개인정보의 이전 제한) ① 개인정보처리자는 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 다음 각 호의 사항을 대통령령으로 정하는 방법에 따라 해당 정보주체에게 알려야 한다.

1. 개인정보를 이전하려는 사실
2. 개인정보를 이전받는 자(이하 "영업양수자등"이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처
3. 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차

② 영업양수자등은 개인정보를 이전받았을 때에는 지체 없이 그 사실을 대통령령으로 정하는 방법에 따라 정보주체에게 알려야 한다. 다만, 개인정보처리자가 제1항에 따라 그 이전 사실을 이미 알린 경우에는 그러하지 아니하다.

③ 영업양수자등은 영업의 양도·합병 등으로 개인정보를 이전받은 경우에는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공할 수 있다. 이 경우 영업양수자등은 개인정보처리자로 본다.

제28조(개인정보취급자에 대한 감독) ① 개인정보처리자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자(이하 "개인정보취급자"라 한다)에 대하여 적절한 관리·감독을 행하여야 한다.

② 개인정보처리자는 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다.

제4장 개인정보의 안전한 관리

제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다. <개정 2015.7.24>

제30조(개인정보 처리방침의 수립 및 공개) ① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 "개인정보 처리방침"이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다. <개정 2016.3.29>

1. 개인정보의 처리 목적
2. 개인정보의 처리 및 보유 기간
3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
5. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항

6. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
7. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)
8. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항

② 개인정보처리자가 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

③ 개인정보 처리방침의 내용과 개인정보처리자와 정보주체 간에 체결한 계약의 내용이 다른 경우에는 정보주체에게 유리한 것을 적용한다.

④ 행정자치부장관은 개인정보 처리방침의 작성지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.<개정 2013.3.23, 2014.11.19>

제31조(개인정보 보호책임자의 지정) ① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다.

② 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독
7. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무

③ 개인정보 보호책임자는 제2항 각 호의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.

④ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다.

⑤ 개인정보처리자는 개인정보 보호책임자가 제2항 각 호의 업무를 수행함에 있어서 정당한 이유 없이 불이익을 주거나 받게 하여서는 아니 된다.

⑥ 개인정보 보호책임자의 지정요건, 업무, 자격요건, 그 밖에 필요한 사항은 대통령령으로 정한다.

제32조(개인정보파일의 등록 및 공개) ① 공공기관의 장이 개인정보파일을 운용하는 경우에는 다음 각 호의 사항을 행정자치부장관에게 등록하여야 한다. 등록한 사항이 변경된 경우에도 또한 같다. <개정 2013.3.23, 2014.11.19>

1. 개인정보파일의 명칭

2. 개인정보파일의 운영 근거 및 목적
3. 개인정보파일에 기록되는 개인정보의 항목
4. 개인정보의 처리방법
5. 개인정보의 보유기간
6. 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
7. 그 밖에 대통령령으로 정하는 사항

② 다음 각 호의 어느 하나에 해당하는 개인정보파일에 대하여는 제1항을 적용하지 아니한다.

1. 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
2. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일
3. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
4. 공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일
5. 다른 법령에 따라 비밀로 분류된 개인정보파일

③ 행정자치부장관은 필요하면 제1항에 따른 개인정보파일의 등록사항과 그 내용을 검토하여 해당 공공기관의 장에게 개선을 권고할 수 있다.<개정 2013.3.23, 2014.11.19>

④ 행정자치부장관은 제1항에 따른 개인정보파일의 등록 현황을 누구든지 쉽게 열람할 수 있도록 공개하여야 한다.<개정 2013.3.23, 2014.11.19>

⑤ 제1항에 따른 등록과 제4항에 따른 공개의 방법, 범위 및 절차에 관하여 필요한 사항은 대통령령으로 정한다.

⑥ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 개인정보파일 등록 및 공개에 관하여는 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정한다.

제32조의2(개인정보 보호 인증) ① 행정자치부장관은 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 이 법에 부합하는지 등에 관하여 인증할 수 있다.

② 제1항에 따른 인증의 유효기간은 3년으로 한다.

③ 행정자치부장관은 다음 각 호의 어느 하나에 해당하는 경우에는 대통령령으로 정하는 바에 따라 제1항에 따른 인증을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 취소하여야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 개인정보 보호 인증을 받은 경우
2. 제4항에 따른 사후관리를 거부 또는 방해한 경우
3. 제8항에 따른 인증기준에 미달하게 된 경우
4. 개인정보 보호 관련 법령을 위반하고 그 위반사유가 중대한 경우

④ 행정자치부장관은 개인정보 보호 인증의 실효성 유지를 위하여 연 1회 이상 사후관리를 실시하여야 한다.

⑤ 행정자치부장관은 대통령령으로 정하는 전문기관으로 하여금 제1항에 따른 인증, 제3항에 따른 인증 취소, 제4항에 따른 사후관리 및 제7항에 따른 인증 심사원 관리 업무를 수행하게 할 수 있다.
⑥ 제1항에 따른 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다.
⑦ 제1항에 따른 인증을 위하여 필요한 심사를 수행할 심사원의 자격 및 자격 취소 요건 등에 관하여는 전문성과 경력 및 그 밖에 필요한 사항을 고려하여 대통령령으로 정한다.
⑧ 그 밖에 개인정보 관리체계, 정보주체 권리보장, 안전성 확보조치가 이 법에 부합하는지 여부 등 제1항에 따른 인증의 기준·방법·절차 등 필요한 사항은 대통령령으로 정한다.
[본조신설 2015.7.24]

제33조(개인정보 영향평가) ① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 "영향평가"라 한다)를 하고 그 결과를 행정자치부장관에게 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 행정자치부장관이 지정하는 기관(이하 "평가기관"이라 한다) 중에서 의뢰하여야 한다. <개정 2013.3.23, 2014.11.19>
② 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다.
1. 처리하는 개인정보의 수
2. 개인정보의 제3자 제공 여부
3. 정보주체의 권리를 해할 가능성 및 그 위험 정도
4. 그 밖에 대통령령으로 정한 사항
③ 행정자치부장관은 제1항에 따라 제출받은 영향평가 결과에 대하여 보호위원회의 심의·의결을 거쳐 의견을 제시할 수 있다.<개정 2013.3.23, 2014.11.19>
④ 공공기관의 장은 제1항에 따라 영향평가를 한 개인정보파일을 제32조제1항에 따라 등록할 때에는 영향평가 결과를 함께 첨부하여야 한다.
⑤ 행정자치부장관은 영향평가의 활성화를 위하여 관계 전문가의 육성, 영향평가 기준의 개발·보급 등 필요한 조치를 마련하여야 한다.<개정 2013.3.23, 2014.11.19>
⑥ 제1항에 따른 평가기관의 지정기준 및 지정취소, 평가기준, 영향평가의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다.
⑦ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 영향평가에 관한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따른다.
⑧ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다.

제34조(개인정보 유출 통지 등) ① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.

1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

③ 개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제1항에 따른 통지 및 제2항에 따른 조치 결과를 지체 없이 행정자치부장관 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 행정자치부장관 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.<개정 2013.3.23, 2014.11.19>

④ 제1항에 따른 통지의 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제34조의2(과징금의 부과 등) ① 행정자치부장관은 개인정보처리자가 처리하는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 5억원 이하의 과징금을 부과·징수할 수 있다. 다만, 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보처리자가 제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다. <개정 2014.11.19, 2015.7.24>

② 행정자치부장관은 제1항에 따른 과징금을 부과하는 경우에는 다음 각 호의 사항을 고려하여야 한다.<개정 2014.11.19, 2015.7.24>

1. 제24조제3항에 따른 안전성 확보에 필요한 조치 이행 노력 정도
2. 분실·도난·유출·위조·변조 또는 훼손된 주민등록번호의 정도
3. 피해확산 방지를 위한 후속조치 이행 여부

③ 행정자치부장관은 제1항에 따른 과징금을 내야 할 자가 납부기한까지 내지 아니하면 납부기한의 다음 날부터 과징금을 낸 날의 전날까지의 기간에 대하여 내지 아니한 과징금의 연 100분의 6의 범위에서 대통령령으로 정하는 가산금을 징수한다. 이 경우 가산금을 징수하는 기간은 60개월을 초과하지 못한다.<개정 2014.11.19>

④ 행정자치부장관은 제1항에 따른 과징금을 내야 할 자가 납부기한까지 내지 아니하면 기간을 정하여 독촉을 하고, 그 지정한 기간 내에 과징금 및 제2항에 따른 가산금을 내지 아니하면 국세 체납처분의 예에 따라 징수한다.<개정 2014.11.19>

⑤ 과징금의 부과·징수에 관하여 그 밖에 필요한 사항은 대통령령으로 정한다.

[본조신설 2013.8.6]

제5장 정보주체의 권리 보장

제35조(개인정보의 열람) ① 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다.

② 제1항에도 불구하고 정보주체가 자신의 개인정보에 대한 열람을 공공기관에 요구하고자 할 때에는 공공기관에 직접 열람을 요구하거나 대통령령으로 정하는 바에 따라 행정자치부장관을 통하여 열람을 요구할 수 있다.<개정 2013.3.23, 2014.11.19>

③ 개인정보처리자는 제1항 및 제2항에 따른 열람을 요구받았을 때에는 대통령령으로 정하는 기간 내에 정보주체가 해당 개인정보를 열람할 수 있도록 하여야 한다. 이 경우 해당 기간 내에 열람할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리고 열람을 연기할 수 있으며, 그 사유가 소멸하면 지체 없이 열람하게 하여야 한다.

④ 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다.

1. 법률에 따라 열람이 금지되거나 제한되는 경우
2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 공공기관이 다음 각 목의 어느 하나에 해당하는 업무를 수행할 때 중대한 지장을 초래하는 경우
   가. 조세의 부과·징수 또는 환급에 관한 업무
   나. 「초·중등교육법」 및 「고등교육법」에 따른 각급 학교, 「평생교육법」에 따른 평생교육시설, 그 밖의 다른 법률에 따라 설치된 고등교육기관에서의 성적 평가 또는 입학자 선발에 관한 업무
   다. 학력·기능 및 채용에 관한 시험, 자격 심사에 관한 업무
   라. 보상금·급부금 산정 등에 대하여 진행 중인 평가 또는 판단에 관한 업무
   마. 다른 법률에 따라 진행 중인 감사 및 조사에 관한 업무

⑤ 제1항부터 제4항까지의 규정에 따른 열람 요구, 열람 제한, 통지 등의 방법 및 절차에 관하여 필요한 사항은 대통령령으로 정한다.

제36조(개인정보의 정정·삭제) ① 제35조에 따라 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다.

② 개인정보처리자는 제1항에 따른 정보주체의 요구를 받았을 때에는 개인정보의 정정 또는 삭제에 관하여 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

③ 개인정보처리자가 제2항에 따라 개인정보를 삭제할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

④ 개인정보처리자는 정보주체의 요구가 제1항 단서에 해당될 때에는 지체 없이 그 내용을 정보주체에게 알려야 한다.
⑤ 개인정보처리자는 제2항에 따른 조사를 할 때 필요하면 해당 정보주체에게 정정·삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있다.
⑥ 제1항·제2항 및 제4항에 따른 정정 또는 삭제 요구, 통지 방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

제37조(개인정보의 처리정지 등) ① 정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있다. 이 경우 공공기관에 대하여는 제32조에 따라 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구할 수 있다.
② 개인정보처리자는 제1항에 따른 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.
1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우
4. 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우
③ 개인정보처리자는 제2항 단서에 따라 처리정지 요구를 거절하였을 때에는 정보주체에게 지체 없이 그 사유를 알려야 한다.
④ 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다.
⑤ 제1항부터 제3항까지의 규정에 따른 처리정지의 요구, 처리정지의 거절, 통지 등의 방법 및 절차에 필요한 사항은 대통령령으로 정한다.

제38조(권리행사의 방법 및 절차) ① 정보주체는 제35조에 따른 열람, 제36조에 따른 정정·삭제, 제37조에 따른 처리정지 등의 요구(이하 "열람등요구"라 한다)를 문서 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다.
② 만 14세 미만 아동의 법정대리인은 개인정보처리자에게 그 아동의 개인정보 열람등요구를 할 수 있다.
③ 개인정보처리자는 열람등요구를 하는 자에게 대통령령으로 정하는 바에 따라 수수료와 우송료(사본의 우송을 청구하는 경우에 한한다)를 청구할 수 있다.
④ 개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다.

⑤ 개인정보처리자는 정보주체가 열람등요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.

제39조(손해배상책임) ① 정보주체는 개인정보처리자가 이 법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있다. 이 경우 그 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

② 삭제 <2015.7.24>

③ 개인정보처리자의 고의 또는 중대한 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우로서 정보주체에게 손해가 발생한 때에는 법원은 그 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다. 다만, 개인정보처리자가 고의 또는 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다.<신설 2015.7.24>

④ 법원은 제3항의 배상액을 정할 때에는 다음 각 호의 사항을 고려하여야 한다.<신설 2015.7.24>

1. 고의 또는 손해 발생의 우려를 인식한 정도
2. 위반행위로 인하여 입은 피해 규모
3. 위법행위로 인하여 개인정보처리자가 취득한 경제적 이익
4. 위반행위에 따른 벌금 및 과징금
5. 위반행위의 기간·횟수 등
6. 개인정보처리자의 재산상태
7. 개인정보처리자가 정보주체의 개인정보 분실·도난·유출 후 해당 개인정보를 회수하기 위하여 노력한 정도
8. 개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도

제39조의2(법정손해배상의 청구) ① 제39조제1항에도 불구하고 정보주체는 개인정보처리자의 고의 또는 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

② 법원은 제1항에 따른 청구가 있는 경우에 변론 전체의 취지와 증거조사의 결과를 고려하여 제1항의 범위에서 상당한 손해액을 인정할 수 있다.

③ 제39조에 따라 손해배상을 청구한 정보주체는 사실심(事實審)의 변론이 종결되기 전까지 그 청구를 제1항에 따른 청구로 변경할 수 있다.

[본조신설 2015.7.24]

제6장 개인정보 분쟁조정위원회

제40조(설치 및 구성) ① 개인정보에 관한 분쟁의 조정(調停)을 위하여 개인정보 분쟁조정위원회(이하 "분쟁조정위원회"라 한다)를 둔다.

② 분쟁조정위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성하며, 위원은 당연직위원과 위촉위원으로 구성한다.<개정 2015.7.24>

③ 위촉위원은 다음 각 호의 어느 하나에 해당하는 사람 중에서 보호위원회 위원장이 위촉하고, 대통령령으로 정하는 국가기관 소속 공무원은 당연직위원이 된다.<개정 2013.3.23, 2014.11.19, 2015.7.24>

1. 개인정보 보호업무를 관장하는 중앙행정기관의 고위공무원단에 속하는 공무원으로 재직하였던 사람 또는 이에 상당하는 공공부문 및 관련 단체의 직에 재직하고 있거나 재직하였던 사람으로서 개인정보 보호업무의 경험이 있는 사람
2. 대학이나 공인된 연구기관에서 부교수 이상 또는 이에 상당하는 직에 재직하고 있거나 재직하였던 사람
3. 판사·검사 또는 변호사로 재직하고 있거나 재직하였던 사람
4. 개인정보 보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람
5. 개인정보처리자로 구성된 사업자단체의 임원으로 재직하고 있거나 재직하였던 사람

④ 위원장은 위원 중에서 공무원이 아닌 사람으로 보호위원회 위원장이 위촉한다.<개정 2013.3.23, 2014.11.19, 2015.7.24>

⑤ 위원장과 위촉위원의 임기는 2년으로 하되, 1차에 한하여 연임할 수 있다.<개정 2015.7.24>

⑥ 분쟁조정위원회는 분쟁조정 업무를 효율적으로 수행하기 위하여 필요하면 대통령령으로 정하는 바에 따라 조정사건의 분야별로 5명 이내의 위원으로 구성되는 조정부를 둘 수 있다. 이 경우 조정부가 분쟁조정위원회에서 위임받아 의결한 사항은 분쟁조정위원회에서 의결한 것으로 본다.

⑦ 분쟁조정위원회 또는 조정부는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.

⑧ 보호위원회는 분쟁조정 접수, 사실 확인 등 분쟁조정에 필요한 사무를 처리할 수 있다.<개정 2015.7.24>

⑨ 이 법에서 정한 사항 외에 분쟁조정위원회 운영에 필요한 사항은 대통령령으로 정한다.

제41조(위원의 신분보장) 위원은 자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직되거나 해촉되지 아니한다.

제42조(위원의 제척·기피·회피) ① 분쟁조정위원회의 위원은 다음 각 호의 어느 하나에 해당하는 경우에는 제43조제1항에 따라 분쟁조정위원회에 신청된 분쟁조정사건(이하 이 조에서 "사건"이라 한다)의 심의·의결에서 제척(除斥)된다.

1. 위원 또는 그 배우자나 배우자였던 자가 그 사건의 당사자가 되거나 그 사건에 관하여 공동의 권리자 또는 의무자의 관계에 있는 경우
2. 위원이 그 사건의 당사자와 친족이거나 친족이었던 경우
3. 위원이 그 사건에 관하여 증언, 감정, 법률자문을 한 경우

4. 위원이 그 사건에 관하여 당사자의 대리인으로서 관여하거나 관여하였던 경우

② 당사자는 위원에게 공정한 심의·의결을 기대하기 어려운 사정이 있으면 위원장에게 기피신청을 할 수 있다. 이 경우 위원장은 기피신청에 대하여 분쟁조정위원회의 의결을 거치지 아니하고 결정한다.

③ 위원이 제1항 또는 제2항의 사유에 해당하는 경우에는 스스로 그 사건의 심의·의결에서 회피할 수 있다.

제43조(조정의 신청 등) ① 개인정보와 관련한 분쟁의 조정을 원하는 자는 분쟁조정위원회에 분쟁조정을 신청할 수 있다.

② 분쟁조정위원회는 당사자 일방으로부터 분쟁조정 신청을 받았을 때에는 그 신청내용을 상대방에게 알려야 한다.

③ 공공기관이 제2항에 따른 분쟁조정의 통지를 받은 경우에는 특별한 사유가 없으면 분쟁조정에 응하여야 한다.

제44조(처리기간) ① 분쟁조정위원회는 제43조제1항에 따른 분쟁조정 신청을 받은 날부터 60일 이내에 이를 심사하여 조정안을 작성하여야 한다. 다만, 부득이한 사정이 있는 경우에는 분쟁조정위원회의 의결로 처리기간을 연장할 수 있다.

② 분쟁조정위원회는 제1항 단서에 따라 처리기간을 연장한 경우에는 기간연장의 사유와 그 밖의 기간연장에 관한 사항을 신청인에게 알려야 한다.

제45조(자료의 요청 등) ① 분쟁조정위원회는 제43조제1항에 따라 분쟁조정 신청을 받았을 때에는 해당 분쟁의 조정을 위하여 필요한 자료를 분쟁당사자에게 요청할 수 있다. 이 경우 분쟁당사자는 정당한 사유가 없으면 요청에 따라야 한다.

② 분쟁조정위원회는 필요하다고 인정하면 분쟁당사자나 참고인을 위원회에 출석하도록 하여 그 의견을 들을 수 있다.

제46조(조정 전 합의 권고) 분쟁조정위원회는 제43조제1항에 따라 분쟁조정 신청을 받았을 때에는 당사자에게 그 내용을 제시하고 조정 전 합의를 권고할 수 있다.

제47조(분쟁의 조정) ① 분쟁조정위원회는 다음 각 호의 어느 하나의 사항을 포함하여 조정안을 작성할 수 있다.

1. 조사 대상 침해행위의 중지
2. 원상회복, 손해배상, 그 밖에 필요한 구제조치
3. 같거나 비슷한 침해의 재발을 방지하기 위하여 필요한 조치

② 분쟁조정위원회는 제1항에 따라 조정안을 작성하면 지체 없이 각 당사자에게 제시하여야 한다.

③ 제1항에 따라 조정안을 제시받은 당사자가 제시받은 날부터 15일 이내에 수락 여부를 알리지 아니하면 조정을 거부한 것으로 본다.

④ 당사자가 조정내용을 수락한 경우 분쟁조정위원회는 조정서를 작성하고, 분쟁조정위원회의 위원장과 각 당사자가 기명날인하여야 한다.
⑤ 제4항에 따른 조정의 내용은 재판상 화해와 동일한 효력을 갖는다.

제48조(조정의 거부 및 중지) ① 분쟁조정위원회는 분쟁의 성질상 분쟁조정위원회에서 조정하는 것이 적합하지 아니하다고 인정하거나 부정한 목적으로 조정이 신청되었다고 인정하는 경우에는 그 조정을 거부할 수 있다. 이 경우 조정거부의 사유 등을 신청인에게 알려야 한다.
② 분쟁조정위원회는 신청된 조정사건에 대한 처리절차를 진행하던 중에 한 쪽 당사자가 소를 제기하면 그 조정의 처리를 중지하고 이를 당사자에게 알려야 한다.

제49조(집단분쟁조정) ① 국가 및 지방자치단체, 개인정보 보호단체 및 기관, 정보주체, 개인정보처리자는 정보주체의 피해 또는 권리침해가 다수의 정보주체에게 같거나 비슷한 유형으로 발생하는 경우로서 대통령령으로 정하는 사건에 대하여는 분쟁조정위원회에 일괄적인 분쟁조정(이하 "집단분쟁조정"이라 한다)을 의뢰 또는 신청할 수 있다.
② 제1항에 따라 집단분쟁조정을 의뢰받거나 신청받은 분쟁조정위원회는 그 의결로써 제3항부터 제7항까지의 규정에 따른 집단분쟁조정의 절차를 개시할 수 있다. 이 경우 분쟁조정위원회는 대통령령으로 정하는 기간 동안 그 절차의 개시를 공고하여야 한다.
③ 분쟁조정위원회는 집단분쟁조정의 당사자가 아닌 정보주체 또는 개인정보처리자로부터 그 분쟁조정의 당사자에 추가로 포함될 수 있도록 하는 신청을 받을 수 있다.
④ 분쟁조정위원회는 그 의결로써 제1항 및 제3항에 따른 집단분쟁조정의 당사자 중에서 공동의 이익을 대표하기에 가장 적합한 1인 또는 수인을 대표당사자로 선임할 수 있다.
⑤ 분쟁조정위원회는 개인정보처리자가 분쟁조정위원회의 집단분쟁조정의 내용을 수락한 경우에는 집단분쟁조정의 당사자가 아닌 자로서 피해를 입은 정보주체에 대한 보상계획서를 작성하여 분쟁조정위원회에 제출하도록 권고할 수 있다.
⑥ 제48조제2항에도 불구하고 분쟁조정위원회는 집단분쟁조정의 당사자인 다수의 정보주체 중 일부의 정보주체가 법원에 소를 제기한 경우에는 그 절차를 중지하지 아니하고, 소를 제기한 일부의 정보주체를 그 절차에서 제외한다.
⑦ 집단분쟁조정의 기간은 제2항에 따른 공고가 종료된 날의 다음 날부터 60일 이내로 한다. 다만, 부득이한 사정이 있는 경우에는 분쟁조정위원회의 의결로 처리기간을 연장할 수 있다.
⑧ 집단분쟁조정의 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제50조(조정절차 등) ① 제43조부터 제49조까지의 규정에서 정한 것 외에 분쟁의 조정방법, 조정절차 및 조정업무의 처리 등에 필요한 사항은 대통령령으로 정한다.
② 분쟁조정위원회의 운영 및 분쟁조정 절차에 관하여 이 법에서 규정하지 아니한 사항에 대하여는 「민사조정법」을 준용한다.

제7장 개인정보 단체소송

제51조(단체소송의 대상 등) 다음 각 호의 어느 하나에 해당하는 단체는 개인정보처리자가 제49조에 따른 집단분쟁조정을 거부하거나 집단분쟁조정의 결과를 수락하지 아니한 경우에는 법원에 권리침해 행위의 금지·중지를 구하는 소송(이하 "단체소송"이라 한다)을 제기할 수 있다.

1. 「소비자기본법」 제29조에 따라 공정거래위원회에 등록한 소비자단체로서 다음 각 목의 요건을 모두 갖춘 단체
   가. 정관에 따라 상시적으로 정보주체의 권익증진을 주된 목적으로 하는 단체일 것
   나. 단체의 정회원수가 1천명 이상일 것
   다. 「소비자기본법」 제29조에 따른 등록 후 3년이 경과하였을 것
2. 「비영리민간단체 지원법」 제2조에 따른 비영리민간단체로서 다음 각 목의 요건을 모두 갖춘 단체
   가. 법률상 또는 사실상 동일한 침해를 입은 100명 이상의 정보주체로부터 단체소송의 제기를 요청받을 것
   나. 정관에 개인정보 보호를 단체의 목적으로 명시한 후 최근 3년 이상 이를 위한 활동실적이 있을 것
   다. 단체의 상시 구성원수가 5천명 이상일 것
   라. 중앙행정기관에 등록되어 있을 것

제52조(전속관할) ① 단체소송의 소는 피고의 주된 사무소 또는 영업소가 있는 곳, 주된 사무소나 영업소가 없는 경우에는 주된 업무담당자의 주소가 있는 곳의 지방법원 본원 합의부의 관할에 전속한다.

② 제1항을 외국사업자에 적용하는 경우 대한민국에 있는 이들의 주된 사무소·영업소 또는 업무담당자의 주소에 따라 정한다.

제53조(소송대리인의 선임) 단체소송의 원고는 변호사를 소송대리인으로 선임하여야 한다.

제54조(소송허가신청) ① 단체소송을 제기하는 단체는 소장과 함께 다음 각 호의 사항을 기재한 소송허가신청서를 법원에 제출하여야 한다.

1. 원고 및 그 소송대리인
2. 피고
3. 정보주체의 침해된 권리의 내용

② 제1항에 따른 소송허가신청서에는 다음 각 호의 자료를 첨부하여야 한다.

1. 소제기단체가 제51조 각 호의 어느 하나에 해당하는 요건을 갖추고 있음을 소명하는 자료
2. 개인정보처리자가 조정을 거부하였거나 조정결과를 수락하지 아니하였음을 증명하는 서류

제55조(소송허가요건 등) ① 법원은 다음 각 호의 요건을 모두 갖춘 경우에 한하여 결정으로 단체소송을 허가한다.

1. 개인정보처리자가 분쟁조정위원회의 조정을 거부하거나 조정결과를 수락하지 아니하였을 것
2. 제54조에 따른 소송허가신청서의 기재사항에 흠결이 없을 것

② 단체소송을 허가하거나 불허가하는 결정에 대하여는 즉시항고할 수 있다.

제56조(확정판결의 효력) 원고의 청구를 기각하는 판결이 확정된 경우 이와 동일한 사안에 관하여는 제51조에 따른 다른 단체는 단체소송을 제기할 수 없다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 판결이 확정된 후 그 사안과 관련하여 국가·지방자치단체 또는 국가·지방자치단체가 설립한 기관에 의하여 새로운 증거가 나타난 경우
2. 기각판결이 원고의 고의로 인한 것임이 밝혀진 경우

제57조(「민사소송법」의 적용 등) ① 단체소송에 관하여 이 법에 특별한 규정이 없는 경우에는 「민사소송법」을 적용한다.

② 제55조에 따른 단체소송의 허가결정이 있는 경우에는 「민사집행법」 제4편에 따른 보전처분을 할 수 있다.

③ 단체소송의 절차에 관하여 필요한 사항은 대법원규칙으로 정한다.

제8장 보칙

제58조(적용의 일부 제외) ① 다음 각 호의 어느 하나에 해당하는 개인정보에 관하여는 제3장부터 제7장까지를 적용하지 아니한다.

1. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보
2. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보
3. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보
4. 언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보

② 제25조제1항 각 호에 따라 공개된 장소에 영상정보처리기기를 설치·운영하여 처리되는 개인정보에 대하여는 제15조, 제22조, 제27조제1항·제2항, 제34조 및 제37조를 적용하지 아니한다.

③ 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 제15조, 제30조 및 제31조를 적용하지 아니한다.

④ 개인정보처리자는 제1항 각 호에 따라 개인정보를 처리하는 경우에도 그 목적을 위하여 필요한 범위에서 최소한의 기간에 최소한의 개인정보만을 처리하여야 하며, 개인정보의 안전한 관리를 위하여 필요한 기술적·관리적 및 물리적 보호조치, 개인정보의 처리에 관한 고충처리, 그 밖에 개인정보의 적절한 처리를 위하여 필요한 조치를 마련하여야 한다.

제59조(금지행위) 개인정보를 처리하거나 처리하였던 자는 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.

1. 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 처리에 관한 동의를 받는 행위
2. 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위
3. 정당한 권한 없이 또는 허용된 권한을 초과하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출하는 행위

제60조(비밀유지 등) 다음 각 호의 업무에 종사하거나 종사하였던 자는 직무상 알게 된 비밀을 다른 사람에게 누설하거나 직무상 목적 외의 용도로 이용하여서는 아니 된다. 다만, 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다.

1. 제8조에 따른 보호위원회의 업무
2. 제33조에 따른 영향평가 업무
3. 제40조에 따른 분쟁조정위원회의 분쟁조정 업무

제61조(의견제시 및 개선권고) ① 행정자치부장관은 개인정보 보호에 영향을 미치는 내용이 포함된 법령이나 조례에 대하여 필요하다고 인정하면 보호위원회의 심의·의결을 거쳐 관계 기관에 의견을 제시할 수 있다. <개정 2013.3.23, 2014.11.19>

② 행정자치부장관은 개인정보 보호를 위하여 필요하다고 인정하면 개인정보처리자에게 개인정보 처리 실태의 개선을 권고할 수 있다. 이 경우 권고를 받은 개인정보처리자는 이를 이행하기 위하여 성실하게 노력하여야 하며, 그 조치 결과를 행정자치부장관에게 알려야 한다.<개정 2013.3.23, 2014.11.19>

③ 관계 중앙행정기관의 장은 개인정보 보호를 위하여 필요하다고 인정하면 소관 법률에 따라 개인정보처리자에게 개인정보 처리 실태의 개선을 권고할 수 있다. 이 경우 권고를 받은 개인정보처리자는 이를 이행하기 위하여 성실하게 노력하여야 하며, 그 조치 결과를 관계 중앙행정기관의 장에게 알려야 한다.

④ 중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 그 소속 기관 및 소관 공공기관에 대하여 개인정보 보호에 관한 의견을 제시하거나 지도·점검을 할 수 있다.

제62조(침해 사실의 신고 등) ① 개인정보처리자가 개인정보를 처리할 때 개인정보에 관한 권리 또는 이익을 침해받은 사람은 행정자치부장관에게 그 침해 사실을 신고할 수 있다. <개정 2013.3.23, 2014.11.19>

② 행정자치부장관은 제1항에 따른 신고의 접수·처리 등에 관한 업무를 효율적으로 수행하기 위하여 대통령령으로 정하는 바에 따라 전문기관을 지정할 수 있다. 이 경우 전문기관은 개인정보침해 신고센터(이하 "신고센터"라 한다)를 설치·운영하여야 한다.<개정 2013.3.23, 2014.11.19>

③ 신고센터는 다음 각 호의 업무를 수행한다.

1. 개인정보 처리와 관련한 신고의 접수·상담
2. 사실의 조사·확인 및 관계자의 의견 청취
3. 제1호 및 제2호에 따른 업무에 딸린 업무

④ 행정자치부장관은 제3항제2호의 사실 조사·확인 등의 업무를 효율적으로 하기 위하여 필요하면 「국가공무원법」 제32조의4에 따라 소속 공무원을 제2항에 따른 전문기관에 파견할 수 있다.<개정 2013.3.23, 2014.11.19>

제63조(자료제출 요구 및 검사) ① 행정자치부장관은 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보처리자에게 관계 물품·서류 등 자료를 제출하게 할 수 있다. <개정 2013.3.23, 2014.11.19>

1. 이 법을 위반하는 사항을 발견하거나 혐의가 있음을 알게 된 경우
2. 이 법 위반에 대한 신고를 받거나 민원이 접수된 경우
3. 그 밖에 정보주체의 개인정보 보호를 위하여 필요한 경우로서 대통령령으로 정하는 경우

② 행정자치부장관은 개인정보처리자가 제1항에 따른 자료를 제출하지 아니하거나 이 법을 위반한 사실이 있다고 인정되면 소속 공무원으로 하여금 개인정보처리자 및 해당 법 위반사실과 관련한 관계인의 사무소나 사업장에 출입하여 업무 상황, 장부 또는 서류 등을 검사하게 할 수 있다. 이 경우 검사를 하는 공무원은 그 권한을 나타내는 증표를 지니고 이를 관계인에게 내보여야 한다.<개정 2013.3.23, 2014.11.19, 2015.7.24>

③ 관계 중앙행정기관의 장은 소관 법률에 따라 개인정보처리자에게 제1항에 따른 자료제출을 요구하거나 개인정보처리자 및 해당 법 위반사실과 관련한 관계인에 대하여 제2항에 따른 검사를 할 수 있다.<개정 2015.7.24>

④ 보호위원회는 이 법을 위반하는 사항을 발견하거나 혐의가 있음을 알게 된 경우에는 행정자치부장관 또는 관계 중앙행정기관의 장에게 제1항 각 호 외의 부분 또는 제3항에 따른 조치를 하도록 요구할 수 있다. 이 경우 그 요구를 받은 행정자치부장관 또는 관계 중앙행정기관의 장은 특별한 사정이 없으면 이에 응하여야 한다.<신설 2015.7.24>

⑤ 행정자치부장관과 관계 중앙행정기관의 장은 제1항 및 제2항에 따라 제출받거나 수집한 서류·자료 등을 이 법에 따른 경우를 제외하고는 제3자에게 제공하거나 일반에게 공개하여서는 아니 된다.<개정 2013.3.23, 2014.11.19, 2015.7.24>

⑥ 행정자치부장관과 관계 중앙행정기관의 장은 정보통신망을 통하여 자료의 제출 등을 받은 경우나 수집한 자료 등을 전자화한 경우에는 개인정보·영업비밀 등이 유출되지 아니하도록 제도적·기술적 보완조치를 하여야 한다.<개정 2013.3.23, 2014.11.19, 2015.7.24>

⑦ 행정자치부장관은 개인정보 침해사고의 예방과 효과적인 대응을 위하여 관계 중앙행정기관의 장과 합동으로 개인정보 보호실태를 점검할 수 있다.<신설 2015.7.24>

제64조(시정조치 등) ① 행정자치부장관은 개인정보가 침해되었다고 판단할 상당한 근거가 있고 이를 방치할 경우 회복하기 어려운 피해가 발생할 우려가 있다고 인정되면 이 법을 위반한

자(중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 제외한다)에 대하여 다음 각 호에 해당하는 조치를 명할 수 있다. <개정 2013.3.23, 2014.11.19>

1. 개인정보 침해행위의 중지
2. 개인정보 처리의 일시적인 정지
3. 그 밖에 개인정보의 보호 및 침해 방지를 위하여 필요한 조치

② 관계 중앙행정기관의 장은 개인정보가 침해되었다고 판단할 상당한 근거가 있고 이를 방치할 경우 회복하기 어려운 피해가 발생할 우려가 있다고 인정되면 소관 법률에 따라 개인정보처리자에 대하여 제1항 각 호에 해당하는 조치를 명할 수 있다.

③ 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 그 소속 기관 및 소관 공공기관이 이 법을 위반하였을 때에는 제1항 각 호에 해당하는 조치를 명할 수 있다.

④ 보호위원회는 중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회가 이 법을 위반하였을 때에는 해당 기관의 장에게 제1항 각 호에 해당하는 조치를 하도록 권고할 수 있다. 이 경우 권고를 받은 기관은 특별한 사유가 없으면 이를 존중하여야 한다.

제65조(고발 및 징계권고) ① 행정자치부장관은 개인정보처리자에게 이 법 등 개인정보 보호와 관련된 법규의 위반에 따른 범죄혐의가 있다고 인정될 만한 상당한 이유가 있을 때에는 관할 수사기관에 그 내용을 고발할 수 있다. <개정 2013.3.23, 2014.11.19>

② 행정자치부장관은 이 법 등 개인정보 보호와 관련된 법규의 위반행위가 있다고 인정될 만한 상당한 이유가 있을 때에는 책임이 있는 자(대표자 및 책임있는 임원을 포함한다)를 징계할 것을 해당 개인정보처리자에게 권고할 수 있다. 이 경우 권고를 받은 사람은 이를 존중하여야 하며 그 결과를 행정자치부장관에게 통보하여야 한다.<개정 2013.3.23, 2013.8.6, 2014.11.19>

③ 관계 중앙행정기관의 장은 소관 법률에 따라 개인정보처리자에 대하여 제1항에 따른 고발을 하거나 소속 기관·단체 등의 장에게 제2항에 따른 징계권고를 할 수 있다. 이 경우 제2항에 따른 권고를 받은 사람은 이를 존중하여야 하며 그 결과를 관계 중앙행정기관의 장에게 통보하여야 한다.

제66조(결과의 공표) ① 행정자치부장관은 제61조에 따른 개선권고, 제64조에 따른 시정조치 명령, 제65조에 따른 고발 또는 징계권고 및 제75조에 따른 과태료 부과의 내용 및 결과에 대하여 보호위원회의 심의·의결을 거쳐 공표할 수 있다. <개정 2013.3.23, 2014.11.19>

② 관계 중앙행정기관의 장은 소관 법률에 따라 제1항에 따른 공표를 할 수 있다.

③ 제1항 및 제2항에 따른 공표의 방법, 기준 및 절차 등은 대통령령으로 정한다.

제67조(연차보고) ① 보호위원회는 관계 기관 등으로부터 필요한 자료를 제출받아 매년 개인정보 보호시책의 수립 및 시행에 관한 보고서를 작성하여 정기국회 개회 전까지 국회에 제출(정보통신망에 의한 제출을 포함한다)하여야 한다.

② 제1항에 따른 보고서에는 다음 각 호의 내용이 포함되어야 한다.

1. 정보주체의 권리침해 및 그 구제현황
2. 개인정보 처리에 관한 실태조사 등의 결과
3. 개인정보 보호시책의 추진현황 및 실적
4. 개인정보 관련 해외의 입법 및 정책 동향
5. 그 밖에 개인정보 보호시책에 관하여 공개 또는 보고하여야 할 사항

제68조(권한의 위임·위탁) ① 이 법에 따른 행정자치부장관 또는 관계 중앙행정기관의 장의 권한은 그 일부를 대통령령으로 정하는 바에 따라 특별시장, 광역시장, 도지사, 특별자치도지사 또는 대통령령으로 정하는 전문기관에 위임하거나 위탁할 수 있다. <개정 2013.3.23, 2014.11.19>

② 제1항에 따라 행정자치부장관 또는 관계 중앙행정기관의 장의 권한을 위임 또는 위탁받은 기관은 위임 또는 위탁받은 업무의 처리 결과를 행정자치부장관 또는 관계 중앙행정기관의 장에게 통보하여야 한다.<개정 2013.3.23, 2014.11.19>

③ 행정자치부장관은 제1항에 따른 전문기관에 권한의 일부를 위임하거나 위탁하는 경우 해당 전문기관의 업무 수행을 위하여 필요한 경비를 출연할 수 있다.<개정 2013.3.23, 2014.11.19>

제69조(벌칙 적용 시의 공무원 의제) 행정자치부장관 또는 관계 중앙행정기관의 장의 권한을 위탁한 업무에 종사하는 관계 기관의 임직원은 「형법」 제129조부터 제132조까지의 규정을 적용할 때에는 공무원으로 본다. <개정 2013.3.23, 2014.11.19>

제9장 벌칙

제70조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다. <개정 2015.7.24>

1. 공공기관의 개인정보 처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경하거나 말소하여 공공기관의 업무 수행의 중단·마비 등 심각한 지장을 초래한 자
2. 거짓이나 그 밖의 부정한 수단이나 방법으로 다른 사람이 처리하고 있는 개인정보를 취득한 후 이를 영리 또는 부정한 목적으로 제3자에게 제공한 자와 이를 교사·알선한 자

제71조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. <개정 2016.3.29>

1. 제17조제1항제2호에 해당하지 아니함에도 같은 항 제1호를 위반하여 정보주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 자 및 그 사정을 알고 개인정보를 제공받은 자
2. 제18조제1항·제2항, 제19조, 제26조제5항 또는 제27조제3항을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자

3. 제23조제1항을 위반하여 민감정보를 처리한 자
4. 제24조제1항을 위반하여 고유식별정보를 처리한 자
5. 제59조제2호를 위반하여 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
6. 제59조제3호를 위반하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출한 자

제72조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

1. 제25조제5항을 위반하여 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자
2. 제59조제1호를 위반하여 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 개인정보 처리에 관한 동의를 받는 행위를 한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
3. 제60조를 위반하여 직무상 알게 된 비밀을 누설하거나 직무상 목적 외에 이용한 자

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. <개정 2015.7.24, 2016.3.29>

1. 제23조제2항, 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자
2. 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 자
3. 제37조제2항을 위반하여 개인정보의 처리를 정지하지 아니하고 계속 이용하거나 제3자에게 제공한 자

제74조(양벌규정) ① 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제70조에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인을 7천만원 이하의 벌금에 처한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.

② 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제71조부터 제73조까지의 어느 하나에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형을 과(科)한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.

제74조의2(몰수·추징 등) 제70조부터 제73조까지의 어느 하나에 해당하는 죄를 지은 자가 해당 위반행위와 관련하여 취득한 금품이나 그 밖의 이익은 몰수할 수 있으며, 이를 몰수할 수

없을 때에는 그 가액을 추징할 수 있다. 이 경우 몰수 또는 추징은 다른 벌칙에 부가하여 과할 수 있다.

[본조신설 2015.7.24]

제75조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다.

1. 제15조제1항을 위반하여 개인정보를 수집한 자
2. 제22조제5항을 위반하여 법정대리인의 동의를 받지 아니한 자
3. 제25조제2항을 위반하여 영상정보처리기기를 설치·운영한 자

② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.<개정 2013.8.6, 2014.3.24, 2015.7.24, 2016.3.29>

1. 제15조제2항, 제17조제2항, 제18조제3항 또는 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자
2. 제16조제3항 또는 제22조제4항을 위반하여 재화 또는 서비스의 제공을 거부한 자
3. 제20조제1항 또는 제2항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자
4. 제21조제1항을 위반하여 개인정보를 파기하지 아니한 자

4의2. 제24조의2제1항을 위반하여 주민등록번호를 처리한 자

4의3. 제24조의2제2항을 위반하여 암호화 조치를 하지 아니한 자

5. 제24조의2제3항을 위반하여 정보주체가 주민등록번호를 사용하지 아니할 수 있는 방법을 제공하지 아니한 자
6. 제23조제2항, 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자
7. 제25조제1항을 위반하여 영상정보처리기기를 설치·운영한 자

7의2. 제32조의2제6항을 위반하여 인증을 받지 아니하였음에도 거짓으로 인증의 내용을 표시하거나 홍보한 자

8. 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자
9. 제34조제3항을 위반하여 조치 결과를 신고하지 아니한 자
10. 제35조제3항을 위반하여 열람을 제한하거나 거절한 자
11. 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니한 자
12. 제37조제4항을 위반하여 처리가 정지된 개인정보에 대하여 파기 등 필요한 조치를 하지 아니한 자
13. 제64조제1항에 따른 시정명령에 따르지 아니한 자

③ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.

1. 제21조제3항을 위반하여 개인정보를 분리하여 저장·관리하지 아니한 자
2. 제22조제1항부터 제3항까지의 규정을 위반하여 동의를 받은 자

3. 제25조제4항을 위반하여 안내판 설치 등 필요한 조치를 하지 아니한 자
4. 제26조제1항을 위반하여 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서에 의하지 아니한 자
5. 제26조제2항을 위반하여 위탁하는 업무의 내용과 수탁자를 공개하지 아니한 자
6. 제27조제1항 또는 제2항을 위반하여 정보주체에게 개인정보의 이전 사실을 알리지 아니한 자
7. 제30조제1항 또는 제2항을 위반하여 개인정보 처리방침을 정하지 아니하거나 이를 공개하지 아니한 자
8. 제31조제1항을 위반하여 개인정보 보호책임자를 지정하지 아니한 자
9. 제35조제3항·제4항, 제36조제2항·제4항 또는 제37조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자
10. 제63조제1항에 따른 관계 물품·서류 등 자료를 제출하지 아니하거나 거짓으로 제출한 자
11. 제63조제2항에 따른 출입·검사를 거부·방해 또는 기피한 자

④ 제1항부터 제3항까지의 규정에 따른 과태료는 대통령령으로 정하는 바에 따라 행정자치부장관과 관계 중앙행정기관의 장이 부과·징수한다. 이 경우 관계 중앙행정기관의 장은 소관 분야의 개인정보처리자에게 과태료를 부과·징수한다.<개정 2013.3.23, 2014.11.19>

제76조(과태료에 관한 규정 적용의 특례) 제75조의 과태료에 관한 규정을 적용할 때 제34조의2에 따라 과징금을 부과한 행위에 대하여는 과태료를 부과할 수 없다.

[본조신설 2013.8.6]

부칙 <제10465호,2011.3.29>

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다. 다만, 제24조제2항 및 제75조제2항제5호는 공포 후 1년이 경과한 날부터 시행한다.

제2조(다른 법률의 폐지) 공공기관의 개인정보보호에 관한 법률은 폐지한다.

제3조(개인정보분쟁조정위원회에 관한 경과조치) 이 법 시행 당시 종전의 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따른 개인정보분쟁조정위원회의 행위나 개인정보분쟁조정위원회에 대한 행위는 그에 해당하는 이 법에 따른 개인정보 분쟁조정위원회의 행위나 개인정보 분쟁조정위원회에 대한 행위로 본다.

제4조(처리 중인 개인정보에 관한 경과조치) 이 법 시행 전에 다른 법령에 따라 적법하게 처리된 개인정보는 이 법에 따라 처리된 것으로 본다.

제5조(벌칙의 적용에 관한 경과조치) ① 이 법 시행 전에 종전의 「공공기관의 개인정보보호에 관한 법률」을 위반한 행위에 대하여 벌칙을 적용할 때에는 종전의 「공공기관의 개인정보보호에 관한 법률」에 따른다.

② 이 법 시행 전에 종전의 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 위반한 행위에 대하여 벌칙을 적용할 때에는 종전의 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따른다.

제6조(다른 법률의 개정) ① 6·25 전사자유해의 발굴 등에 관한 법률 일부를 다음과 같이 개정한다.

제14조제1항제2호 중 "「공공기관의 개인정보보호에 관한 법률」 제2조제2호"를 "「개인정보 보호법」 제2조제1호"로 한다.

② 공직자윤리법 일부를 다음과 같이 개정한다.

제6조제6항 및 제9항 중 "「공공기관의 개인정보보호에 관한 법률」 제10조"를 각각 "「개인정보 보호법」 제18조"로 한다.

③ 국가공무원법 일부를 다음과 같이 개정한다.

제19조의3제3항 중 "「공공기관의 개인정보보호에 관한 법률」 제2조제1호"를 "「개인정보 보호법」 제2조제6호"로 하고, 같은 조 제4항 중 "「공공기관의 개인정보보호에 관한 법률」"을 "「개인정보 보호법」"으로 한다.

④ 발명진흥법 일부를 다음과 같이 개정한다.

제20조의2제1항 중 "「공공기관의 개인정보보호에 관한 법률」"을 "「개인정보 보호법」"으로 한다.

⑤ 신용정보의 이용 및 보호에 관한 법률 일부를 다음과 같이 개정한다.

제23조제2항제2호를 다음과 같이 한다.

2. 「개인정보 보호법」

⑥ 아동복지법 일부를 다음과 같이 개정한다.

제9조의2제3항 중 "「공공기관의 개인정보보호에 관한 법률」"을 "「개인정보 보호법」"으로 한다.

⑦ 법률 제10333호 암관리법 전부개정법률 일부를 다음과 같이 개정한다.

제14조제1항 후단 중 "「공공기관의 개인정보보호에 관한 법률」 제3조제2항"을 "「개인정보 보호법」 제58조제1항"으로 한다.

제49조 중 "「공공기관의 개인정보보호에 관한 법률」 제10조제3항"을 "「개인정보 보호법」 제18조제2항"으로 한다.

⑧ 장애인차별금지 및 권리구제 등에 관한 법률 일부를 다음과 같이 개정한다.

제3조제8호다목 중 "「공공기관의 개인정보보호에 관한 법률」 제2조제2호"를 "「개인정보 보호법」 제2조제1호"로 한다.

제22조제2항 중 "「공공기관의 개인정보보호에 관한 법률」"을 "「개인정보 보호법」"으로 한다.

⑨ 전자서명법 일부를 다음과 같이 개정한다.

제24조제2항을 삭제한다.

⑩ 전자정부법 일부를 다음과 같이 개정한다.

제21조제2항 중 "「공공기관의 개인정보보호에 관한 법률」 제2조제2호"를 "「개인정보 보호법」 제2조제1호"로 한다.

제39조제4항 중 "「공공기관의 개인정보보호에 관한 법률」 제5조"를 "「개인정보 보호법」 제32조"로, "같은 법 제20조제1항에 따른 공공기관개인정보보호심의위원회의 심의를 거쳐"를 "「개인정보 보호법」 제7조에 따른 개인정보 보호위원회의 심의·의결을 거쳐"로 한다.

제42조제1항 중 "「공공기관의 개인정보보호에 관한 법률」 제2조제8호"를 "「개인정보 보호법」 제2조제3호"로, "「공공기관의 개인정보보호에 관한 법률」 제10조제3항제1호 및 같은 조 제5항은"을 "「개인정보 보호법」 제18조제2항제1호 및 제19조제1호는"으로 한다.

⑪ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부를 다음과 같이 개정한다.

제4장제4절(제33조, 제33조의2, 제34조부터 제40조까지), 제66조제1호 및 제67조를 각각 삭제한다.

제4조제1항·제3항, 제64조의2제3항 후단, 제65조제1항 및 제69조 중 "행정안전부장관, 지식경제부장관 또는 방송통신위원회"를 각각 "지식경제부장관 또는 방송통신위원회"로 한다.

제64조제1항 각 호 외의 부분·제3항·제4항 전단·제5항 전단·제6항·제9항·제10항, 제64조의2제1항·제2항·제3항 각 호 외의 부분 전단, 제65조제3항, 제76조제1항제12호 및 제4항부터 제6항까지 중 "행정안전부장관 또는 방송통신위원회"를 각각 "방송통신위원회"로 한다.

⑫ 채권의 공정한 추심에 관한 법률 일부를 다음과 같이 개정한다.

제2조제5호 중 "「공공기관의 개인정보보호에 관한 법률」 제2조제2호"를 "「개인정보 보호법」 제2조제1호"로 한다.

⑬ 출입국관리법 일부를 다음과 같이 개정한다.

제12조의2제6항 및 제38조제3항 중 "「공공기관의 개인정보보호에 관한 법률」"을 각각 "「개인정보 보호법」"으로 한다.

⑭ 한국장학재단 설립 등에 관한 법률 일부를 다음과 같이 개정한다.

제50조제3항 중 "「공공기관의 개인정보보호에 관한 법률」"을 "「개인정보 보호법」"으로 한다.

제7조(다른 법령과의 관계) 이 법 시행 당시 다른 법령에서 종전의 「공공기관의 개인정보보호에 관한 법률」 또는 그 규정을 인용하고 있는 경우 이 법 중 그에 해당하는 규정이 있을 때에는 종전의 규정을 갈음하여 이 법 또는 이 법의 해당 규정을 인용한 것으로 본다.

부칙 <제11690호,2013.3.23>

제1조(시행일) ① 이 법은 공포한 날부터 시행한다.

②생략

제2조부터 제5조까지 생략

제6조(다른 법률의 개정) ①부터 <149>까지 생략

<150> 개인정보 보호법 일부를 다음과 같이 개정한다.

제9조제1항, 제11조제1항, 제12조제1항, 제13조 각 호 외의 부분, 제24조제4항, 제30조제4항, 제32조제1항 각 호 외의 부분 전단, 같은 조 제3항ㆍ제4항, 제33조제1항 전단ㆍ후단, 같은 조 제3항ㆍ제5항, 제34조제3항 전단ㆍ후단, 제35조제2항, 제40조제3항 각 호 외의 부분, 같은 조 제4항ㆍ제8항, 제61조제1항, 같은 조 제2항 전단ㆍ후단, 제62조제1항, 같은 조 제2항 전단, 같은 조 제4항, 제63조제1항 각 호 외의 부분, 같은 조 제2항 전단, 같은 조 제4항ㆍ제5항, 제64조제1항 각 호 외의 부분, 제65조제1항, 같은 조 제2항 전단ㆍ후단, 제66조제1항, 제68조제1항부터 제3항까지, 제69조 및 제75조제4항 전단 중 "행정안전부장관"을 각각 "안전행정부장관"으로 한다.

제18조제4항 중 "행정안전부령"을 "안전행정부령"으로 한다.

<151>부터 <710>까지 생략

제7조 생략

부칙 <제11990호,2013.8.6>

제1조(시행일) 이 법은 공포 후 1년이 경과한 날부터 시행한다.

제2조(주민등록번호 처리 제한에 관한 경과조치) ① 이 법 시행 당시 주민등록번호를 처리하고 있는 개인정보처리자는 이 법 시행일부터 2년 이내에 보유하고 있는 주민등록번호를 파기하여야 한다. 다만, 제24조의2제1항 각 호의 개정규정의 어느 하나에 해당하는 경우는 제외한다.

② 제1항에 따른 기간 이내에 보유하고 있는 주민등록번호를 파기하지 아니한 경우에는 제24조의2제1항의 개정규정을 위반한 것으로 본다.

부칙 <제12504호,2014.3.24>

이 법은 공포한 날부터 시행한다. 다만, 법률 제11990호 개인정보 보호법 일부개정법률 제24조의2 및 제75조제2항제5호의 개정규정은 2016년 1월 1일부터 시행한다.

부칙 <제12844호,2014.11.19>

제1조(시행일) 이 법은 공포한 날부터 시행한다. 다만, 부칙 제6조에 따라 개정되는 법률 중 이 법 시행 전에 공포되었으나 시행일이 도래하지 아니한 법률을 개정한 부분은 각각 해당 법률의 시행일부터 시행한다.

제2조부터 제5조까지 생략

제6조(다른 법률의 개정) ①부터 <55>까지 생략

<56> 개인정보 보호법 일부를 다음과 같이 개정한다.

제9조제1항, 제11조제1항, 제12조제1항, 제13조 각 호 외의 부분, 제24조의2제1항제3호, 제30조제4항, 제32조제1항 각 호 외의 부분 전단, 같은 조 제3항ㆍ제4항, 제33조제1항 전단ㆍ후단, 같은 조 제3항ㆍ제5항, 제34조제3항 전단ㆍ후단, 제34조의2제1항 본문, 같은 조 제2항 각 호 외의 부분, 같은 조 제3항 전단, 같은 조 제4항, 제35조제2항, 제40조제3항 각 호 외의 부분, 같은 조 제4항ㆍ제8항, 제61조제1항, 같은 조 제2항 전단ㆍ후단, 제62조제1항, 같은 조 제2항 전단, 같은 조 제4항, 제63조제1항 각 호 외의 부분, 같은 조 제2항 전단, 같은 조 제4항ㆍ제5항, 제64조제1항 각 호 외의 부분, 제65조제1항, 같은 조 제2항 전단ㆍ후단, 제66조제1항, 제68조제1항부터 제3항까지, 제69조 및 제75조제4항 전단 중 "안전행정부장관"을 각각 "행정자치부장관"으로 한다.

제18조제4항 중 "안전행정부령"을 "행정자치부령"으로 한다.

<57>부터 <258>까지 생략

제7조 생략

부칙 <제13423호,2015.7.24>

제1조(시행일) 이 법은 공포한 날부터 시행한다. 다만, 제8조제1항, 제8조의2, 제9조, 제11조제1항, 제32조의2, 제39조제3항ㆍ제4항, 제39조의2, 제40조, 제75조제2항제7호의2의 개정규정은 공포 후 1년이 경과한 날부터, 법률 제12504호 개인정보 보호법 일부개정법률 제24조의2제2항 전단 및 제75조제2항제4호의3의 개정규정은 2016년 1월 1일부터 각각 시행한다.

제2조(손해배상에 관한 적용례) 제39조제3항ㆍ제4항 및 제39조의2의 개정규정은 이 법 시행 후에 분실ㆍ도난ㆍ유출ㆍ위조ㆍ변조 또는 훼손된 개인정보에 관한 손해배상 청구분부터 적용한다.

제3조(개인정보 보호 인증에 관한 경과조치) 이 법 시행 전에 행정자치부장관으로부터 개인정보 보호 인증을 받은 자는 제32조의2의 개정규정에 따른 개인정보 보호 인증을 받은 것으로 본다.

제4조(개인정보 인증 심사원 자격에 관한 경과조치) 이 법 시행 전에 개인정보 보호 인증 심사원의 자격을 취득한 자는 이 법에 따른 개인정보 보호 인증 심사원의 자격을 취득한 것으로 본다.

제5조(개인정보 분쟁조정위원회 위원의 임기에 관한 경과조치) 이 법 시행 전에 행정자치부장관이 임명하거나 위촉한 분쟁조정위원회 위원은 제40조의 개정규정에 따른 보호위원회가 위촉한 분쟁조정위원회 위원으로 본다.

제6조(벌칙 등에 관한 경과조치) 이 법 시행 전의 위반행위에 대하여 벌칙 또는 과태료를 적용할 때에는 종전의 규정에 따른다.

부칙 <제14107호,2016.3.29>

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다. 다만, 제24조의2제1항제1호 및 제67조제2항제5호의 개정규정은 공포 후 1년이 경과한 날부터 시행한다.

제2조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지에 관한 적용례) 제20조제2항 및 제3항의 개정규정은 이 법 시행 후 최초로 정보주체 이외로부터 개인정보를 수집하는 경우부터 적용한다.

제3조(개인정보 처리방침에 관한 경과조치) ① 이 법 시행 당시 종전의 규정에 따른 개인정보 처리방침은 제30조제1항의 개정규정에 따른 개인정보 처리방침으로 본다.

② 개인정보처리자는 이 법 시행 후 6개월 이내에 제1항에 따른 개인정보 처리방침을 제30조제1항의 개정취지에 맞도록 개정하여야 한다.

개인정보 보호법 시행령

[시행 2016.9.30] [대통령령 제27522호, 2016.9.29, 일부개정]

제1장 총칙

제1조(목적) 이 영은 「개인정보 보호법」에서 위임된 사항과 그 시행에 필요한 사항을 규정함을 목적으로 한다.

제2조(공공기관의 범위) 「개인정보 보호법」(이하 "법"이라 한다) 제2조제6호나목에서 "대통령령으로 정하는 기관"이란 다음 각 호의 기관을 말한다.

1. 「국가인권위원회법」 제3조에 따른 국가인권위원회
2. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관
3. 「지방공기업법」에 따른 지방공사와 지방공단
4. 특별법에 따라 설립된 특수법인
5. 「초·중등교육법」, 「고등교육법」, 그 밖의 다른 법률에 따라 설치된 각급 학교

제3조(영상정보처리기기의 범위) 법 제2조제7호에서 "대통령령으로 정하는 장치"란 다음 각 호의 장치를 말한다.

1. 폐쇄회로 텔레비전: 다음 각 목의 어느 하나에 해당하는 장치
   가. 일정한 공간에 지속적으로 설치된 카메라를 통하여 영상 등을 촬영하거나 촬영한 영상정보를 유무선 폐쇄회로 등의 전송로를 통하여 특정 장소에 전송하는 장치
   나. 가목에 따라 촬영되거나 전송된 영상정보를 녹화·기록할 수 있도록 하는 장치
2. 네트워크 카메라: 일정한 공간에 지속적으로 설치된 기기로 촬영한 영상정보를 그 기기를 설치·관리하는 자가 유무선 인터넷을 통하여 어느 곳에서나 수집·저장 등의 처리를 할 수 있도록 하는 장치

제2장 개인정보 보호위원회

제4조(위원의 제척·기피·회피) ① 법 제7조제2항에 따른 개인정보 보호위원회(이하 "보호위원회"라 한다)의 위원은 다음 각 호의 어느 하나에 해당하는 사항에 대한 심의·의결에 관여하지 못한다.

1. 위원 또는 위원의 배우자, 4촌 이내의 혈족, 2촌 이내의 인척인 사람이나 그 사람이 속한 기관·단체와 이해관계가 있는 사항

2. 위원이 증언, 진술 또는 감정(鑑定)을 하거나 대리인으로 관여한 사항
3. 위원이나 위원이 속한 공공기관ㆍ법인 또는 단체 등이 조언 등 지원을 하고 있는 자와 이해관계가 있는 사항

② 보호위원회가 심의ㆍ의결하는 사항과 직접적인 이해관계가 있는 자는 제1항에 따른 제척 사유가 있거나 심의ㆍ의결의 공정을 기대하기 어려운 사유가 있는 위원에 대해서는 그 사유를 밝혀 보호위원회에 그 위원의 기피를 신청할 수 있다. 이 경우 위원장이 기피 여부를 결정한다.

③ 위원은 제1항 또는 제2항에 해당하는 경우에는 스스로 심의ㆍ의결을 회피할 수 있다.

제5조(전문위원회) ① 보호위원회는 법 제8조제1항에 따른 심의ㆍ의결 사항에 대하여 사전에 전문적으로 검토하기 위하여 보호위원회에 분야별 전문위원회(이하 "전문위원회"라 한다)를 둘 수 있다.

② 제1항에 따라 전문위원회를 두는 경우 각 전문위원회는 위원장 1명을 포함한 10명 이내의 위원으로 구성하되, 전문위원회 위원은 다음 각 호의 사람 중에서 보호위원회의 동의를 받아 보호위원회 위원장이 임명하거나 위촉하고, 전문위원회 위원장은 보호위원회 위원장이 전문위원회 위원 중에서 지명한다.<개정 2016.7.22>

1. 보호위원회 위원
2. 개인정보 보호 관련 업무를 담당하는 중앙행정기관의 관계 공무원
3. 개인정보 보호에 관한 전문지식과 경험이 풍부한 사람
4. 개인정보 보호와 관련된 단체 또는 사업자단체에 속하거나 그 단체의 추천을 받은 사람

③ 전문위원회의 회의는 재적위원 과반수의 출석으로 개의(開議)하고, 출석위원 과반수의 찬성으로 의결한다.

제6조(의사의 공개) 보호위원회의 의사(議事)는 공개한다. 다만, 보호위원회 위원장이 필요하다고 인정하는 경우에는 공개하지 아니할 수 있다.

제7조(공무원 등의 파견) 보호위원회는 그 업무 수행을 위하여 필요하다고 인정하는 경우에는 공공기관에 그 소속 공무원 또는 임직원의 파견을 요청할 수 있다.

제8조(조직 및 정원 등) 이 영에서 규정한 사항 외에 보호위원회의 조직 및 정원 등에 관하여 필요한 사항은 따로 대통령령으로 정한다.

제9조(출석수당 등) 보호위원회 또는 전문위원회의 회의에 출석한 위원, 법 제8조제2항에 따라 보호위원회에 출석한 사람 및 전문위원회에 출석한 사람에게는 예산의 범위에서 수당ㆍ여비, 그 밖에 필요한 경비를 지급할 수 있다. 다만, 공무원이 그 소관 업무와 직접 관련되어 출석하는 경우에는 그러하지 아니하다.

제9조의2(정책ㆍ제도ㆍ법령 개선 권고의 절차 등) ① 보호위원회는 법 제8조제4항에 따라 관계 기관에 정책ㆍ제도 및 법령의 개선을 권고하는 경우에는 그 내용과 사유 등을 함께 통보하여야 한다.

② 보호위원회는 법 제8조제5항에 따른 권고내용의 이행여부를 점검하기 위하여 관계 기관에 권고사항의 이행결과에 대한 자료 제출을 요청할 수 있다.

[본조신설 2016.7.22]

제9조의3(개인정보 침해요인 평가 절차 등) ① 중앙행정기관의 장은 법 제8조의2제1항에 따라 개인정보 침해요인 평가(이하 "침해요인 평가"라 한다)를 요청하는 경우 다음 각 호의 사항을 포함하는 개인정보 침해요인 평가 요청서(전자문서를 포함한다)를 보호위원회에 제출하여야 한다.

1. 법령(법령안을 포함한다)을 통하여 도입되거나 변경되는 개인정보 처리를 수반하는 정책·제도의 목적과 주요 내용
2. 개인정보 처리를 수반하는 정책·제도의 도입·변경에 따른 제2항 각 호의 사항에 대한 개인정보 침해요인 자체 분석
3. 개인정보 처리를 수반하는 정책·제도의 도입·변경에 따른 개인정보 보호 대책

② 보호위원회는 제1항에 따른 요청서를 받은 경우에는 다음 각 호의 사항을 고려하여 침해요인 평가를 하고, 그 결과를 해당 중앙행정기관의 장에게 통보하여야 한다.

1. 개인정보 처리의 필요성
2. 개인정보 주체의 권리보장의 적정성
3. 개인정보 관리의 안전성
4. 그 밖에 침해요인 평가에 필요한 사항

③ 중앙행정기관의 장은 법 제8조의2제2항에 따른 권고를 받은 경우에는 그 내용을 해당 법령안에 반영하는 등 권고내용을 이행하도록 노력하여야 한다. 다만, 보호위원회의 권고대로 이행하기 곤란한 경우에는 그 사유를 보호위원회에 통보하여야 한다.

④ 보호위원회는 침해요인 평가를 하는 경우에는 침해요인 평가에 필요한 자료 등을 해당 중앙행정기관의 장에게 요청할 수 있다.

⑤ 보호위원회는 침해요인 평가의 세부기준 및 방법 등 침해요인 평가에 필요한 지침을 수립하여 중앙행정기관의 장에게 통보할 수 있다.

⑥ 보호위원회는 침해요인 평가를 실시하기 위하여 필요하면 관계 전문가에게 자문 등을 할 수 있다.

[본조신설 2016.7.22]

제10조(보호위원회 등의 운영 세칙) 법과 이 영에서 규정한 사항 외에 보호위원회 및 전문위원회의 구성 및 운영 등에 필요한 사항은 보호위원회의 의결을 거쳐 보호위원회의 규칙으로 정한다.

제3장 기본계획 및 시행계획의 수립절차

제11조(기본계획의 수립절차 등) ① 보호위원회는 3년마다 법 제9조에 따른 개인정보 보호 기본계획(이하 "기본계획"이라 한다)을 그 3년이 시작되는 해의 전전년도 12월 31일까지 수립하여야 한다. <개정 2013.3.23, 2014.11.19, 2016.7.22>

② 보호위원회는 제1항에 따라 기본계획을 작성하는 경우에는 관계 중앙행정기관의 장으로부터 개인정보 보호 관련 중장기 계획과 시책 등을 반영한 부문별 계획을 제출받아 기본계획에 반영할 수 있다. 이 경우 보호위원회는 기본계획의 목표, 추진방향 및 부문별 계획의 작성 지침 등에 관하여 관계 중앙행정기관의 장과 협의하여야 한다.<개정 2013.3.23, 2014.11.19, 2016.7.22>

③ 보호위원회는 기본계획이 확정되면 지체 없이 관계 중앙행정기관의 장에게 통보하여야 한다.<개정 2013.3.23, 2014.11.19, 2016.7.22>

제12조(시행계획의 수립절차 등) ① 보호위원회는 매년 12월 31일까지 다음다음 해 시행계획의 작성방법 등에 관한 지침을 마련하여 관계 중앙행정기관의 장에게 통보하여야 한다. <개정 2013.3.23, 2014.11.19, 2016.7.22>

② 관계 중앙행정기관의 장은 제1항의 지침에 따라 기본계획 중 다음 해에 시행할 소관 분야의 시행계획을 작성하여 매년 2월 말일까지 보호위원회에 제출하여야 한다.

③ 보호위원회는 제2항에 따라 제출된 시행계획을 그 해 4월 30일까지 심의·의결하여야 한다.

제13조(자료제출 요구 등의 범위와 방법) ① 보호위원회는 법 제11조제1항에 따라 개인정보처리자에게 다음 각 호의 사항에 관한 자료의 제출이나 의견의 진술 등을 요구할 수 있다. <개정 2013.3.23, 2014.11.19, 2016.7.22>

1. 해당 개인정보처리자가 처리하는 개인정보 및 개인정보파일의 관리와 영상정보처리기기의 설치·운영에 관한 사항
2. 법 제31조에 따른 개인정보 보호책임자의 지정 여부에 관한 사항
3. 개인정보의 안전성 확보를 위한 기술적·관리적·물리적 조치에 관한 사항
4. 정보주체의 열람, 개인정보의 정정·삭제·처리정지의 요구 및 조치 현황에 관한 사항
5. 그 밖에 법 및 이 영의 준수에 관한 사항 등 기본계획의 수립·추진을 위하여 필요한 사항

② 보호위원회는 제1항에 따라 자료의 제출이나 의견의 진술 등을 요구할 때에는 기본계획을 효율적으로 수립·추진하기 위하여 필요한 최소한의 범위로 한정하여 요구하여야 한다.<개정 2013.3.23, 2014.11.19, 2016.7.22>

③ 법 제11조제3항에 따라 중앙행정기관의 장이 소관 분야의 개인정보처리자에게 자료의 제출 등을 요구하는 경우에는 제1항과 제2항을 준용한다. 이 경우 "보호위원회"는 "중앙행정기관의 장"으로, "법 제11조제1항"은 "법 제11조제3항"으로 본다.<개정 2013.3.23, 2014.11.19, 2016.7.22>

제14조(자율규제의 촉진 및 지원) 행정자치부장관은 법 제13조제2호에 따라 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하기 위하여 예산의 범위에서 개인정보 보호와 관련된 기

관 또는 단체에 필요한 지원을 할 수 있다. <개정 2013.3.23, 2014.11.19>

제4장 개인정보의 처리

제15조(개인정보의 목적 외 이용 또는 제3자 제공의 관리) 공공기관은 법 제18조제2항 각 호에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 다음 각 호의 사항을 행정자치부령으로 정하는 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록하고 관리하여야 한다. <개정 2013.3.23, 2014.11.19>

1. 이용하거나 제공하는 개인정보 또는 개인정보파일의 명칭
2. 이용기관 또는 제공받는 기관의 명칭
3. 이용 목적 또는 제공받는 목적
4. 이용 또는 제공의 법적 근거
5. 이용하거나 제공하는 개인정보의 항목
6. 이용 또는 제공의 날짜, 주기 또는 기간
7. 이용하거나 제공하는 형태
8. 법 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용

제15조의2(개인정보 수집 출처 등 고지 대상、방법、절차) ① 법 제20조제2항 본문에서 "대통령령으로 정하는 기준에 해당하는 개인정보처리자"란 다음 각 호의 어느 하나에 해당하는 개인정보처리자를 말한다.

1. 5만명 이상의 정보주체에 관하여 법 제23조에 따른 민감정보(이하 "민감정보"라 한다) 또는 법 제24조제1항에 따른 고유식별정보(이하 "고유식별정보"라 한다)를 처리하는 자
2. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자

② 제1항 각 호의 어느 하나에 해당하는 개인정보처리자는 법 제20조제1항 각 호의 사항을 서면、전화、문자전송、전자우편 등 정보주체가 쉽게 알 수 있는 방법으로 개인정보를 제공받은 날부터 3개월 이내에 정보주체에게 알려야 한다. 다만, 법 제17조제2항제1호부터 제4호까지의 사항에 대하여 같은 조 제1항제1호에 따라 정보주체의 동의를 받은 범위에서 연 2회 이상 주기적으로 개인정보를 제공받아 처리하는 경우에는 개인정보를 제공받은 날부터 3개월 이내에 정보주체에게 알리거나 그 동의를 받은 날부터 기산하여 연 1회 이상 정보주체에게 알려야 한다.

③ 제1항 각 호의 어느 하나에 해당하는 개인정보처리자는 제2항에 따라 알린 경우 다음 각 호의 사항을 법 제21조 또는 제37조제4항에 따라 해당 개인정보를 파기할 때까지 보관、관리하여야 한다.

1. 정보주체에게 알린 사실
2. 알린 시기

3. 알린 방법

[본조신설 2016.9.29]

제16조(개인정보의 파기방법) ①개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 하여야 한다. <개정 2014.8.6>

1. 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 파쇄 또는 소각

② 제1항에 따른 개인정보의 안전한 파기에 관한 세부 사항은 행정자치부장관이 정하여 고시한다.<신설 2014.8.6, 2014.11.19>

제17조(동의를 받는 방법) ① 개인정보처리자는 법 제22조에 따라 개인정보의 처리에 대하여 다음 각 호의 어느 하나에 해당하는 방법으로 정보주체의 동의를 받아야 한다.

1. 동의 내용이 적힌 서면을 정보주체에게 직접 발급하거나 우편 또는 팩스 등의 방법으로 전달하고, 정보주체가 서명하거나 날인한 동의서를 받는 방법
2. 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하는 방법
3. 전화를 통하여 동의 내용을 정보주체에게 알리고 정보주체에게 인터넷주소 등을 통하여 동의 사항을 확인하도록 한 후 다시 전화를 통하여 그 동의 사항에 대한 동의의 의사표시를 확인하는 방법
4. 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법
5. 동의 내용이 적힌 전자우편을 발송하여 정보주체로부터 동의의 의사표시가 적힌 전자우편을 받는 방법
6. 그 밖에 제1호부터 제5호까지의 규정에 따른 방법에 준하는 방법으로 동의 내용을 알리고 동의의 의사표시를 확인하는 방법

② 개인정보처리자가 정보주체로부터 법 제18조제2항제1호 및 제22조제3항에 따른 동의를 받거나 법 제22조제2항에 따라 선택적으로 동의할 수 있는 사항에 대한 동의를 받으려는 때에는 정보주체가 동의 여부를 선택할 수 있다는 사실을 명확하게 확인할 수 있도록 선택적으로 동의할 수 있는 사항 외의 사항과 구분하여 표시하여야 한다.<신설 2015.12.30>

③ 개인정보처리자는 법 제22조제5항에 따라 만 14세 미만 아동의 법정대리인의 동의를 받기 위하여 해당 아동으로부터 직접 법정대리인의 성명·연락처에 관한 정보를 수집할 수 있다. <개정 2015.12.30>

④ 중앙행정기관의 장은 제1항에 따른 동의방법 중 소관 분야의 개인정보처리자별 업무, 업종의 특성 및 정보주체의 수 등을 고려하여 적절한 동의방법에 관한 기준을 법 제12조제2항에 따른 개인정보 보호지침(이하 "개인정보 보호지침"이라 한다)으로 정하여 그 기준에 따라 동의를 받도록 개인정보처리자에게 권장할 수 있다.<개정 2015.12.30>

제18조(민감정보의 범위) 법 제23조제1항 각 호 외의 부분 본문에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우

의 해당 정보는 제외한다. <개정 2016.9.29>

1. 유전자검사 등의 결과로 얻어진 유전정보
2. 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보

제19조(고유식별정보의 범위) 법 제24조제1항 각 호 외의 부분에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다. <개정 2016.9.29>

1. 「주민등록법」 제7조제3항에 따른 주민등록번호
2. 「여권법」 제7조제1항제1호에 따른 여권번호
3. 「도로교통법」 제80조에 따른 운전면허의 면허번호
4. 「출입국관리법」 제31조제4항에 따른 외국인등록번호

제20조 삭제 <2014.8.6>

제21조(고유식별정보의 안전성 확보 조치) ① 법 제24조제3항에 따른 고유식별정보의 안전성 확보 조치에 관하여는 제30조를 준용한다. 이 경우 "법 제29조"는 "법 제24조제3항"으로, "개인정보"는 "고유식별정보"로 본다.

② 법 제24조제4항에서 "대통령령으로 정하는 기준에 해당하는 개인정보처리자"란 다음 각 호의 어느 하나에 해당하는 개인정보처리자를 말한다.

1. 공공기관
2. 5만명 이상의 정보주체에 관하여 고유식별정보를 처리하는 자

③ 행정자치부장관은 제2항 각 호의 어느 하나에 해당하는 개인정보처리자에 대하여 법 제24조제4항에 따라 안전성 확보에 필요한 조치를 하였는지를 2년마다 1회 이상 조사하여야 한다.

④ 제3항에 따른 조사는 제2항 각 호의 어느 하나에 해당하는 개인정보처리자에게 온라인 또는 서면을 통하여 필요한 자료를 제출하게 하는 방법으로 한다.

⑤ 법 제24조제5항에서 "대통령령으로 정하는 전문기관"이란 다음 각 호의 기관을 말한다.

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원 (이하 "한국인터넷진흥원"이라 한다)
2. 법 제24조제4항에 따른 조사를 수행할 수 있는 기술적·재정적 능력과 설비를 보유한 것으로 인정되어 행정자치부장관이 정하여 고시하는 법인, 단체 또는 기관

[전문개정 2016.9.29]

제21조의2(주민등록번호 암호화 적용 대상 등) ① 법 제24조의2제2항에 따라 암호화 조치를 하여야 하는 암호화 적용 대상은 주민등록번호를 전자적인 방법으로 보관하는 개인정보처리자로 한다.

② 제1항의 개인정보처리자에 대한 암호화 적용 시기는 다음 각 호와 같다.

1. 100만명 미만의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2017년 1월 1일
2. 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2018년 1월 1일

③ 행정자치부장관은 기술적ㆍ 경제적 타당성 등을 고려하여 제1항에 따른 암호화 조치의 세부적인 사항을 정하여 고시할 수 있다.

[본조신설 2015.12.30]

제22조(영상정보처리기기 설치ㆍ운영 제한의 예외) ① 법 제25조제2항 단서에서 "대통령령으로 정하는 시설"이란 다음 각 호의 시설을 말한다.

1. 「형의 집행 및 수용자의 처우에 관한 법률」 제2조제4호에 따른 교정시설
2. 「정신보건법」 제3조제3호부터 제5호까지의 규정에 따른 정신의료기관(수용시설을 갖추고 있는 것만 해당한다), 정신질환자사회복귀시설 및 정신요양시설

② 중앙행정기관의 장은 소관 분야의 개인정보처리자가 법 제25조제2항 단서에 따라 제1항 각 호의 시설에 영상정보처리기기를 설치ㆍ운영하는 경우 정보주체의 사생활 침해를 최소화하기 위하여 필요한 세부 사항을 개인정보 보호지침으로 정하여 그 준수를 권장할 수 있다.

제23조(영상정보처리기기 설치 시 의견 수렴) ① 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치ㆍ운영하려는 공공기관의 장은 다음 각 호의 어느 하나에 해당하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

1. 「행정절차법」에 따른 행정예고의 실시 또는 의견청취
2. 해당 영상정보처리기기의 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회ㆍ설문조사 또는 여론조사

② 법 제25조제2항 단서에 따른 시설에 영상정보처리기기를 설치ㆍ운영하려는 자는 다음 각 호의 사람으로부터 의견을 수렴하여야 한다.

1. 관계 전문가
2. 해당 시설에 종사하는 사람, 해당 시설에 구금되어 있거나 보호받고 있는 사람 또는 그 사람의 보호자 등 이해관계인

제24조(안내판의 설치 등) ① 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치ㆍ운영하는 자(이하 "영상정보처리기기운영자"라 한다)는 영상정보처리기기가 설치ㆍ운영되고 있음을 정보주체가 쉽게 알아볼 수 있도록 같은 조 제4항 각 호의 사항이 포함된 안내판을 설치하여야 한다. 다만, 건물 안에 여러 개의 영상정보처리기기를 설치하는 경우에는 출입구 등 잘 보이는 곳에 해당 시설 또는 장소 전체가 영상정보처리기기 설치지역임을 표시하는 안내판을 설치할 수 있다. <개정 2016.9.29>

1. 삭제 <2016.9.29>

2. 삭제 <2016.9.29>
3. 삭제 <2016.9.29>

② 제1항에도 불구하고 영상정보처리기기운영자가 설치·운영하는 영상정보처리기기가 다음 각 호의 어느 하나에 해당하는 경우에는 안내판 설치를 갈음하여 영상정보처리기기운영자의 인터넷 홈페이지에 법 제25조제4항 각 호의 사항을 게재할 수 있다.<개정 2016.9.29>

1. 공공기관이 원거리 촬영, 과속·신호위반 단속 또는 교통흐름조사 등의 목적으로 영상정보처리기기를 설치하는 경우로서 개인정보 침해의 우려가 적은 경우
2. 산불감시용 영상정보처리기기를 설치하는 경우 등 장소적 특성으로 인하여 안내판을 설치하는 것이 불가능하거나 안내판을 설치하더라도 정보주체가 쉽게 알아볼 수 없는 경우

③ 제2항에 따라 인터넷 홈페이지에 법 제25조제4항 각 호의 사항을 게재할 수 없으면 영상정보처리기기운영자는 다음 각 호의 어느 하나 이상의 방법으로 법 제25조제4항 각 호의 사항을 공개하여야 한다.<개정 2016.9.29>

1. 영상정보처리기기운영자의 사업장·영업소·사무소·점포 등(이하 "사업장등"이라 한다)의 보기 쉬운 장소에 게시하는 방법
2. 관보(영상정보처리기기운영자가 공공기관인 경우만 해당한다)나 영상정보처리기기운영자의 사업장등이 있는 특별시·광역시·도 또는 특별자치도(이하 "시·도"라 한다) 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법

④ 법 제25조제4항 각 호 외의 부분 단서에서 "대통령령으로 정하는 시설"이란 「보안업무규정」 제32조에 따른 국가보안시설을 말한다.<개정 2016.9.29>

제25조(영상정보처리기기 운영·관리 방침) ① 영상정보처리기기운영자는 법 제25조제7항에 따라 다음 각 호의 사항이 포함된 영상정보처리기기 운영·관리 방침을 마련하여야 한다.

1. 영상정보처리기기의 설치 근거 및 설치 목적
2. 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위
3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람
4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법
5. 영상정보처리기기운영자의 영상정보 확인 방법 및 장소
6. 정보주체의 영상정보 열람 등 요구에 대한 조치
7. 영상정보 보호를 위한 기술적·관리적 및 물리적 조치
8. 그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항

② 제1항에 따라 마련한 영상정보처리기기 운영·관리 방침의 공개에 관하여는 제31조제2항 및 제3항을 준용한다. 이 경우 "개인정보처리자"는 "영상정보처리기기운영자"로, "법 제30조제2항"은 "법 제25조제7항"으로, "개인정보 처리방침"은 "영상정보처리기기 운영·관리 방침"으로 본다.<개정 2016.9.29>

제26조(공공기관의 영상정보처리기기 설치·운영 사무의 위탁) ① 법 제25조제8항 단서에 따라 공공기관이 영상정보처리기기의 설치·운영에 관한 사무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서로 하여야 한다.

1. 위탁하는 사무의 목적 및 범위
2. 재위탁 제한에 관한 사항
3. 영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
4. 영상정보의 관리 현황 점검에 관한 사항
5. 위탁받는 자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

② 제1항에 따라 사무를 위탁한 경우에는 제24조제1항부터 제3항까지의 규정에 따른 안내판 등에 위탁받는 자의 명칭 및 연락처를 포함시켜야 한다.

제27조(영상정보처리기기 설치·운영 지침) 행정자치부장관은 법 및 이 영에서 규정한 사항 외에 영상정보처리기기의 설치·운영에 관한 기준, 설치·운영 사무의 위탁 등에 관하여 법 제12조제1항에 따른 표준 개인정보 보호지침을 정하여 영상정보처리기기운영자에게 그 준수를 권장할 수 있다. <개정 2013.3.23, 2014.11.19>

제28조(개인정보의 처리 업무 위탁 시 조치) ① 법 제26조제1항제3호에서 "대통령령으로 정한 사항"이란 다음 각 호의 사항을 말한다.

1. 위탁업무의 목적 및 범위
2. 재위탁 제한에 관한 사항
3. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
4. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
5. 법 제26조제2항에 따른 수탁자(이하 "수탁자"라 한다)가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

② 법 제26조제2항에서 "대통령령으로 정하는 방법"이란 개인정보 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)가 위탁자의 인터넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 게재하는 방법을 말한다.

③ 제2항에 따라 인터넷 홈페이지에 게재할 수 없는 경우에는 다음 각 호의 어느 하나 이상의 방법으로 위탁하는 업무의 내용과 수탁자를 공개하여야 한다.

1. 위탁자의 사업장등의 보기 쉬운 장소에 게시하는 방법
2. 관보(위탁자가 공공기관인 경우만 해당한다)나 위탁자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법
3. 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 싣는 방법
4. 재화나 용역을 제공하기 위하여 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

④ 법 제26조제3항 전단에서 "대통령령으로 정하는 방법"이란 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(이하 "서면등의 방법"이라 한다)을 말한다.
⑤ 위탁자가 과실 없이 제4항에 따른 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다. 다만, 인터넷 홈페이지를 운영하지 아니하는 위탁자의 경우에는 사업장등의 보기 쉬운 장소에 30일 이상 게시하여야 한다.
⑥ 위탁자는 수탁자가 개인정보 처리 업무를 수행하는 경우에 법 또는 이 영에 따라 개인정보처리자가 준수하여야 할 사항과 법 제26조제1항 각 호의 사항을 준수하는지를 같은 조 제4항에 따라 감독하여야 한다.

제29조(영업양도 등에 따른 개인정보 이전의 통지) ① 법 제27조제1항 각 호 외의 부분과 같은 조 제2항 본문에서 "대통령령으로 정하는 방법"이란 서면등의 방법을 말한다.
② 법 제27조제1항에 따라 개인정보를 이전하려는 자(이하 이 항에서 "영업양도자등"이라 한다)가 과실 없이 제1항에 따른 방법으로 법 제27조제1항 각 호의 사항을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다. 다만, 인터넷 홈페이지를 운영하지 아니하는 영업양도자등의 경우에는 사업장등의 보기 쉬운 장소에 30일 이상 게시하여야 한다.

제5장 개인정보의 안전한 관리

제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.
1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
5. 개인정보에 대한 보안프로그램의 설치 및 갱신
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치
② 행정자치부장관은 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.<개정 2013.3.23, 2014.11.19>
③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 행정자치부장관이 정하여 고시한다. <개정 2013.3.23, 2014.11.19>

제31조(개인정보 처리방침의 내용 및 공개방법 등) ① 법 제30조제1항제8호에서 "대통령령으로 정한 사항"이란 다음 각 호의 사항을 말한다. <개정 2016.9.29>
1. 처리하는 개인정보의 항목

2. 개인정보의 파기에 관한 사항
3. 제30조에 따른 개인정보의 안전성 확보 조치에 관한 사항

② 개인정보처리자는 법 제30조제2항에 따라 수립하거나 변경한 개인정보 처리방침을 개인정보처리자의 인터넷 홈페이지에 지속적으로 게재하여야 한다.

③ 제2항에 따라 인터넷 홈페이지에 게재할 수 없는 경우에는 다음 각 호의 어느 하나 이상의 방법으로 수립하거나 변경한 개인정보 처리방침을 공개하여야 한다.

1. 개인정보처리자의 사업장등의 보기 쉬운 장소에 게시하는 방법
2. 관보(개인정보처리자가 공공기관인 경우만 해당한다)나 개인정보처리자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 싣는 방법
3. 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 싣는 방법
4. 재화나 용역을 제공하기 위하여 개인정보처리자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

제32조(개인정보 보호책임자의 업무 및 지정요건 등) ① 법 제31조제2항제7호에서 "대통령령으로 정한 업무"란 다음 각 호와 같다.

1. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
2. 개인정보 보호 관련 자료의 관리
3. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

② 개인정보처리자는 법 제31조제1항에 따라 개인정보 보호책임자를 지정하려는 경우에는 다음 각 호의 구분에 따라 지정한다.<개정 2016.7.22>

1. 공공기관: 다음 각 목의 구분에 따른 기준에 해당하는 공무원 등
   가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관: 고위공무원단에 속하는 공무원(이하 "고위공무원"이라 한다) 또는 그에 상당하는 공무원
   나. 가목 외에 정무직공무원을 장(長)으로 하는 국가기관: 3급 이상 공무원(고위공무원을 포함한다) 또는 그에 상당하는 공무원
   다. 가목 및 나목 외에 고위공무원, 3급 공무원 또는 그에 상당하는 공무원 이상의 공무원을 장으로 하는 국가기관: 4급 이상 공무원 또는 그에 상당하는 공무원
   라. 가목부터 다목까지의 규정에 따른 국가기관 외의 국가기관(소속 기관을 포함한다): 해당 기관의 개인정보 처리 관련 업무를 담당하는 부서의 장
   마. 시·도 및 시·도 교육청: 3급 이상 공무원 또는 그에 상당하는 공무원
   바. 시·군 및 자치구: 4급 공무원 또는 그에 상당하는 공무원
   사. 제2조제5호에 따른 각급 학교: 해당 학교의 행정사무를 총괄하는 사람

아. 가목부터 사목까지의 규정에 따른 기관 외의 공공기관: 개인정보 처리 관련 업무를 담당하는 부서의 장. 다만, 개인정보 처리 관련 업무를 담당하는 부서의 장이 2명 이상인 경우에는 해당 공공기관의 장이 지명하는 부서의 장이 된다.

2. 공공기관 외의 개인정보처리자: 다음 각 목의 어느 하나에 해당하는 사람

가. 사업주 또는 대표자

나. 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장)

③ 행정자치부장관은 개인정보 보호책임자가 법 제31조제2항의 업무를 원활히 수행할 수 있도록 개인정보 보호책임자에 대한 교육과정을 개설·운영하는 등 지원을 할 수 있다.<개정 2013.3.23, 2014.11.19>

제33조(개인정보파일의 등록사항) 법 제32조제1항제7호에서 "대통령령으로 정하는 사항"이란 다음 각 호의 사항을 말한다.

1. 개인정보파일을 운용하는 공공기관의 명칭
2. 개인정보파일로 보유하고 있는 개인정보의 정보주체 수
3. 해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서
4. 제41조에 따른 개인정보의 열람 요구를 접수·처리하는 부서
5. 개인정보파일의 개인정보 중 법 제35조제4항에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유

제34조(개인정보파일의 등록 및 공개 등) ① 개인정보파일을 운용하는 공공기관의 장은 그 운용을 시작한 날부터 60일 이내에 행정자치부령으로 정하는 바에 따라 행정자치부장관에게 법 제32조제1항 및 이 영 제33조에 따른 등록사항(이하 "등록사항"이라 한다)의 등록을 신청하여야 한다. 등록 후 등록한 사항이 변경된 경우에도 또한 같다. <개정 2013.3.23, 2014.11.19>

② 행정자치부장관은 법 제32조제4항에 따라 개인정보파일의 등록 현황을 인터넷 홈페이지에 게재하여야 한다.<개정 2013.3.23, 2014.11.19>

③ 행정자치부장관은 제1항에 따른 개인정보파일의 등록사항을 등록하거나 변경하는 업무를 전자적으로 처리할 수 있도록 시스템을 구축·운영할 수 있다.<개정 2013.3.23, 2014.11.19>

제34조의2(개인정보 보호 인증의 기준·방법·절차 등) ① 행정자치부장관은 제30조제1항 각 호의 사항을 고려하여 개인정보 보호의 관리적·기술적·물리적 보호대책의 수립 등을 포함한 법 제32조의2제1항에 따른 인증의 기준을 정하여 고시한다.

② 법 제32조의2제1항 따라 개인정보 보호의 인증을 받으려는 자(이하 이 조 및 제34조의3에서 "신청인"이라 한다)는 다음 각 호의 사항이 포함된 개인정보 보호 인증신청서(전자문서로 된 신청서를 포함한다)를 제34조의6에 따른 개인정보 보호 인증 전문기관(이하 "인증기관"이라 한다)에 제출하여야 한다.

1. 인증 대상 개인정보 처리시스템의 목록
2. 개인정보 보호 관리체계를 수립·운영하는 방법과 절차

3. 개인정보 보호 관리체계 및 보호대책 구현과 관련되는 문서 목록

③ 인증기관은 제2항에 따른 인증신청서를 받은 경우에는 신청인과 인증의 범위 및 일정 등에 관하여 협의하여야 한다.

④ 법 제32조의2제1항에 따른 개인정보 보호 인증심사는 제34조의8에 따른 개인정보 보호 인증심사원이 서면심사 또는 현장심사의 방법으로 실시한다.

⑤ 인증기관은 제4항에 따른 인증심사의 결과를 심의하기 위하여 정보보호에 관한 학식과 경험이 풍부한 사람을 위원으로 하는 인증위원회를 설치·운영하여야 한다.

⑥ 제1항부터 제5항까지에서 규정한 사항 외에 인증신청, 인증심사, 인증위원회의 설치·운영 및 인증서의 발급 등 개인정보 보호 인증에 필요한 세부사항은 행정자치부장관이 정하여 고시한다.

[본조신설 2016.7.22]

제34조의3(개인정보 보호 인증의 수수료) ① 신청인은 인증기관에 개인정보 보호 인증 심사에 소요되는 수수료를 납부하여야 한다.

② 행정자치부장관은 개인정보 보호 인증 심사에 투입되는 인증 심사원의 수 및 인증심사에 필요한 일수 등을 고려하여 제1항에 따른 수수료 산정을 위한 구체적인 기준을 정하여 고시한다.

[본조신설 2016.7.22]

제34조의4(인증취소) ① 인증기관은 법 제32조의2제3항에 따라 개인정보 보호 인증을 취소하려는 경우에는 제34조의2제5항에 따른 인증위원회의 심의·의결을 거쳐야 한다.

② 행정자치부장관 또는 인증기관은 법 제32조의2제3항에 따라 인증을 취소한 경우에는 그 사실을 당사자에게 통보하고, 관보 또는 인증기관의 홈페이지에 공고하거나 게시하여야 한다.

[본조신설 2016.7.22]

제34조의5(인증의 사후관리) ① 법 제32조의2제4항에 따른 사후관리 심사는 서면심사 또는 현장심사의 방법으로 실시한다.

② 인증기관은 제1항에 따른 사후관리를 실시한 결과 법 제32조의2제3항 각 호의 사유를 발견한 경우에는 제34조의2제5항에 따른 인증위원회의 심의를 거쳐 그 결과를 행정자치부장관에게 제출하여야 한다.

[본조신설 2016.7.22]

제34조의6(개인정보 보호 인증 전문기관) ① 법 제32조의2제5항에서 "대통령령으로 정하는 전문기관"이란 다음 각 호의 기관을 말한다. <개정 2016.9.29>

1. 한국인터넷진흥원
2. 다음 각 목의 요건을 모두 충족하는 법인, 단체 또는 기관 중에서 행정자치부장관이 지정·고시하는 법인, 단체 또는 기관

가. 제34조의8에 따른 개인정보 보호 인증심사원 5명 이상을 보유할 것

나. 행정자치부장관이 실시하는 업무수행 요건·능력 심사에서 적합하다고 인정받을 것

② 제1항제2호에 해당하는 법인, 단체 또는 기관의 지정과 그 지정의 취소에 필요한 세부기준 등은 행정자치부장관이 정하여 고시한다.

[본조신설 2016.7.22]

제34조의7(인증의 표시 및 홍보) 법 제32조의2제6항에 따라 인증을 받은 자가 인증 받은 내용을 표시하거나 홍보하려는 경우에는 행정자치부장관이 정하여 고시하는 개인정보 보호 인증 표시를 사용할 수 있다. 이 경우 인증의 범위와 유효기간을 함께 표시하여야 한다.

[본조신설 2016.7.22]

제34조의8(개인정보 보호 인증심사원의 자격 및 자격 취소 요건) ① 인증기관은 법 제32조의2제7항에 따라 개인정보 보호에 관한 전문지식을 갖춘 사람으로서 인증심사에 필요한 전문 교육과정을 이수하고 시험에 합격한 사람에게 개인정보 보호 인증심사원(이하 "인증심사원"이라 한다)의 자격을 부여한다.

② 인증기관은 법 제32조의2제7항에 따라 인증심사원이 다음 각 호의 어느 하나에 해당하는 경우 그 자격을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 자격을 취소하여야 한다.

1. 거짓이나 부정한 방법으로 인증심사원 자격을 취득한 경우
2. 개인정보 보호 인증 심사와 관련하여 금전, 금품, 이익 등을 부당하게 수수한 경우
3. 개인정보 보호 인증 심사 과정에서 취득한 정보를 누설하거나 정당한 사유 없이 업무상 목적 외의 용도로 사용한 경우

③ 제1항 및 제2항에 따른 전문 교육과정의 이수, 인증심사원 자격의 부여 및 취소 등에 관한 세부 사항은 행정자치부장관이 정하여 고시한다.

[본조신설 2016.7.22]

제35조(개인정보 영향평가의 대상) 법 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다. <개정 2016.9.29>

1. 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
4. 법 제33조제1항에 따른 개인정보 영향평가(이하 "영향평가"라 한다)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.

제36조(영향평가 시 고려사항) 법 제33조제2항제4호에서 "대통령령으로 정한 사항"이란 다음 각 호의 사항을 말한다.

1. 민감정보 또는 고유식별정보의 처리 여부
2. 개인정보 보유기간

제37조(평가기관의 지정 및 지정취소) ① 행정자치부장관은 법 제33조제1항 후단에 따라 다음 각 호의 요건을 모두 갖춘 법인을 개인정보 영향평가기관(이하 "평가기관"이라 한다)으로 지정할 수 있다. <개정 2013.3.23, 2014.11.19, 2015.12.22>

1. 최근 5년간 다음 각 목의 어느 하나에 해당하는 업무 수행의 대가로 받은 금액의 합계액이 2억원 이상인 법인
   가. 영향평가 업무 또는 이와 유사한 업무
   나. 「전자정부법」 제2조제13호에 따른 정보시스템(정보보호시스템을 포함한다)의 구축 업무 중 정보보호컨설팅 업무(전자적 침해행위에 대비하기 위한 정보시스템의 분석·평가와 이에 기초한 정보 보호 대책의 제시 업무를 말한다. 이하 같다)
   다. 「전자정부법」 제2조제14호에 따른 정보시스템 감리 업무 중 정보보호컨설팅 업무
   라. 「정보보호산업의 진흥에 관한 법률」 제23조제1항제1호 및 제2호에 따른 업무
   마. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제8호에 따른 정보보호산업에 해당하는 업무 중 정보보호컨설팅 업무
2. 별표 1에 따른 전문인력을 10명 이상 상시 고용하고 있는 법인
3. 다음 각 목의 사무실 및 설비를 갖춘 법인
   가. 신원 확인 및 출입 통제를 위한 설비를 갖춘 사무실
   나. 기록 및 자료의 안전한 관리를 위한 설비

② 평가기관으로 지정받으려는 자는 행정자치부령으로 정하는 평가기관 지정신청서에 다음 각 호의 서류(전자문서를 포함한다. 이하 같다)를 첨부하여 행정자치부장관에게 제출하여야 한다.<개정 2013.3.23, 2014.11.19>

1. 정관
2. 대표자 및 임원의 성명
3. 제1항제2호에 따른 전문인력의 자격을 증명할 수 있는 서류
4. 그 밖에 행정자치부령으로 정하는 서류

③ 제2항에 따라 평가기관 지정신청서를 제출받은 행정자치부장관은 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 다음 각 호의 서류를 확인하여야 한다. 다만, 신청인이 제2호의 확인에 동의하지 아니하는 경우에는 신청인에게 그 서류를 첨부하게 하여야 한다.<개정 2013.3.23, 2014.11.19>

1. 법인 등기사항증명서
2. 「출입국관리법」 제88조제2항에 따른 외국인등록 사실증명(외국인인 경우만 해당한다)

④ 행정자치부장관은 제1항에 따라 평가기관을 지정한 경우에는 지체 없이 평가기관 지정서를 발급하고, 다음 각 호의 사항을 관보에 고시하여야 한다. 고시된 사항이 변경된 경우에도 또

한 같다.<개정 2013.3.23, 2014.11.19>

1. 평가기관의 명칭·주소 및 전화번호와 대표자의 성명
2. 지정 시 조건을 붙이는 경우 그 조건의 내용

⑤ 행정자치부장관은 제1항에 따라 지정된 평가기관이 다음 각 호의 어느 하나에 해당하는 경우에는 평가기관의 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 경우에는 평가기관의 지정을 취소하여야 한다.<개정 2013.3.23, 2014.11.19>

1. 거짓이나 그 밖의 부정한 방법으로 평가기관의 지정을 받은 경우
2. 지정된 평가기관 스스로 지정취소를 원하는 경우나 폐업한 경우
3. 제1항에 따른 지정요건을 충족하지 못하게 된 경우
4. 제6항에 따른 신고의무를 이행하지 아니한 경우
5. 고의 또는 중대한 과실로 영향평가 업무를 부실하게 수행하여 그 업무를 적정하게 수행할 수 없다고 인정되는 경우
6. 그 밖에 법 또는 이 영에 따른 의무를 위반한 경우

⑥ 제1항에 따라 지정된 평가기관은 지정된 후 다음 각 호의 어느 하나에 해당하는 사유가 발생한 경우에는 행정자치부령으로 정하는 바에 따라 그 사유가 발생한 날부터 7일 이내에 행정자치부장관에게 신고하여야 한다. 다만, 제3호에 해당하는 경우에는 그 사유가 발생한 날부터 30일 이내에 신고하여야 한다.<개정 2013.3.23, 2014.11.19>

1. 제1항 각 호의 어느 하나에 해당하는 사항이 변경된 경우
2. 제4항제1호에 해당하는 사항이 변경된 경우
3. 평가기관을 양도·양수하거나 합병하는 등의 사유가 발생한 경우

⑦ 행정자치부장관은 제5항에 따라 평가기관의 지정을 취소하려는 경우에는 청문을 하여야 한다.<개정 2013.3.23, 2014.11.19>

제38조(영향평가의 평가기준 등) ① 법 제33조제6항에 따른 영향평가의 평가기준은 다음 각 호와 같다. <개정 2016.7.22>

1. 해당 개인정보파일에 포함되는 개인정보의 종류·성질, 정보주체의 수 및 그에 따른 개인정보 침해의 가능성
2. 법 제24조제3항, 제25조제6항 및 제29조에 따른 안전성 확보 조치의 수준 및 이에 따른 개인정보 침해의 가능성
3. 개인정보 침해의 위험요인별 조치 여부
4. 그 밖에 법 및 이 영에 따라 필요한 조치 또는 의무 위반 요소에 관한 사항

② 법 제33조제1항에 따라 영향평가를 의뢰받은 평가기관은 제1항의 평가기준에 따라 개인정보파일의 운용으로 인한 개인정보 침해의 위험요인을 분석·평가한 후 다음 각 호의 사항이 포함된 평가 결과를 영향평가서로 작성하여 해당 공공기관의 장에게 보내야 하며, 공공기관의 장은 제35조 각 호에 해당하는 개인정보파일을 구축·운용 또는 변경하기 전에 그 영향평가서를 행정자치부장관에게 제출(영향평가서에 제3호에 따른 개선 필요 사항이 포함된 경우에는 그에 대한 조치 내용을 포함한다)하여야 한다.<개정 2013.3.23, 2014.11.19, 2016.7.22>

1. 개인정보파일 운용과 관련된 사업의 개요 및 개인정보파일 운용의 목적
2. 영향평가 대상 개인정보파일의 개요
3. 평가기준에 따른 개인정보 침해의 위험요인에 대한 분석·평가 및 개선이 필요한 사항
4. 영향평가 수행 인력 및 비용

③ 행정자치부장관은 법 및 이 영에서 정한 사항 외에 평가기관의 지정 및 영향평가의 절차 등에 관한 세부 기준을 정하여 고시할 수 있다.<개정 2013.3.23, 2014.11.19>

제39조(개인정보 유출 신고의 범위 및 기관) ① 법 제34조제3항 전단에서 "대통령령으로 정한 규모 이상의 개인정보"란 1만명 이상의 정보주체에 관한 개인정보를 말한다.

② 법 제34조제3항 전단 및 후단에서 "대통령령으로 정하는 전문기관"이란 각각 한국인터넷진흥원을 말한다.<개정 2015.12.30, 2016.7.22>

제40조(개인정보 유출 통지의 방법 및 절차) ① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 서면등의 방법으로 지체 없이 법 제34조제1항 각 호의 사항을 정보주체에게 알려야 한다. 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없이 정보주체에게 알릴 수 있다.

② 제1항에도 불구하고 개인정보처리자는 같은 항 본문에 따라 개인정보가 유출되었음을 알게 되었을 때나 같은 항 단서에 따라 유출 사실을 알고 긴급한 조치를 한 후에도 법 제34조제1항제1호 및 제2호의 구체적인 유출 내용을 확인하지 못한 경우에는 먼저 개인정보가 유출된 사실과 유출이 확인된 사항만을 서면등의 방법으로 먼저 알리고 나중에 확인되는 사항을 추가로 알릴 수 있다.

③ 제1항과 제2항에도 불구하고 법 제34조제3항 및 이 영 제39조제1항에 따라 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 법 제34조제1항 각 호의 사항을 7일 이상 게재하여야 한다. 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 서면등의 방법과 함께 사업장등의 보기 쉬운 장소에 법 제34조제1항 각 호의 사항을 7일 이상 게시하여야 한다.

제40조의2(과징금의 부과기준 등) ① 법 제34조의2제1항에 따른 과징금의 부과기준은 별표 1의2와 같다.

② 행정자치부장관은 법 제34조의2제1항에 따라 과징금을 부과하려는 경우에는 위반사실, 부과금액, 이의제기 방법 및 이의제기 기간 등을 명시하여 이를 납부할 것을 과징금 부과대상자에게 서면으로 통지하여야 한다.<개정 2014.11.19>

③ 제2항에 따라 통지를 받은 자는 통지를 받은 날부터 30일 이내에 행정자치부장관이 정하는 수납기관에 과징금을 납부하여야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 그 기간 내에 과징금을 납부할 수 없는 경우에는 그 사유가 없어진 날부터 7일 이내에 납부하여야 한다.<개정 2014.11.19>

④ 법 제34조의2제3항 전단에서 "대통령령으로 정하는 가산금"이란 납부기한의 다음 날부터 과징금을 낸 날의 전날까지의 기간에 대하여 매 1개월이 지날 때마다 내지 아니한 과징금의 1천분의 5에 상당하는 금액을 가산한 금액을 말한다.

[본조신설 2014.8.6]

제6장 정보주체의 권리 보장

제41조(개인정보의 열람절차 등) ① 정보주체는 법 제35조제1항 및 제2항에 따라 자신의 개인정보에 대한 열람을 요구하려는 경우에는 행정자치부령으로 정하는 바에 따라 다음 각 호의 사항 중 열람하려는 사항을 표시한 개인정보 열람요구서를 개인정보처리자에게 제출하여야 한다. <개정 2013.3.23, 2014.11.19>

1. 개인정보의 항목 및 내용
2. 개인정보의 수집·이용의 목적
3. 개인정보 보유 및 이용 기간
4. 개인정보의 제3자 제공 현황
5. 개인정보 처리에 동의한 사실 및 내용

② 정보주체가 법 제35조제2항에 따라 행정자치부장관을 통하여 자신의 개인정보에 대한 열람을 요구하려는 경우에는 제1항에 따른 개인정보 열람요구서를 행정자치부장관에게 제출하여야 한다. 이 경우 행정자치부장관은 지체 없이 그 개인정보 열람요구서를 해당 공공기관에 이송하여야 한다.<개정 2013.3.23, 2014.11.19>

③ 법 제35조제3항 전단에서 "대통령령으로 정하는 기간"이란 10일을 말한다.

④ 개인정보처리자는 제1항에 따른 개인정보 열람요구서를 받은 날부터 10일 이내에 정보주체에게 해당 개인정보를 열람할 수 있도록 하는 경우와 제42조제1항에 따라 열람 요구 사항 중 일부를 열람하게 하는 경우에는 열람할 개인정보와 열람이 가능한 날짜·시간 및 장소 등(제42조제1항에 따라 열람 요구 사항 중 일부만을 열람하게 하는 경우에는 그 사유와 이의제기방법을 포함한다)을 행정자치부령으로 정하는 열람통지서로 해당 정보주체에게 알려야 한다.<개정 2013.3.23, 2014.11.19>

제42조(개인정보 열람의 제한·연기 및 거절) ① 개인정보처리자는 제41조제1항에 따른 열람 요구 사항 중 일부가 법 제35조제4항 각 호의 어느 하나에 해당하는 경우에는 그 일부에 대하여 열람을 제한할 수 있으며, 열람이 제한되는 사항을 제외한 부분은 열람할 수 있도록 하여야 한다.

② 개인정보처리자가 법 제35조제3항 후단에 따라 정보주체의 열람을 연기하거나 같은 조 제4항에 따라 열람을 거절하려는 경우에는 열람 요구를 받은 날부터 10일 이내에 연기 또는 거절의 사유 및 이의제기방법을 행정자치부령으로 정하는 열람의 연기·거절 통지서로 해당 정보주체에게 알려야 한다.<개정 2013.3.23, 2014.11.19>

제43조(개인정보의 정정·삭제 등) ① 정보주체는 법 제36조제1항에 따라 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구하려는 경우에 행정자치부령으로 정하는 개인정보 정정·삭제 요구서를 해당 개인정보처리자에게 제출하여야 한다. <개정 2013.3.23, 2014.11.19>

② 다른 개인정보처리자로부터 개인정보를 제공받아 개인정보파일을 처리하는 개인정보처리자는 법 제36조제1항에 따른 개인정보의 정정 또는 삭제 요구를 받으면 그 요구에 따라 해당 개인정보를 정정·삭제하거나 그 개인정보 정정·삭제 요구서를 해당 개인정보를 제공한 기관의 장에게 지체 없이 보내고 그 처리 결과에 따라 필요한 조치를 하여야 한다.

③ 개인정보처리자는 제1항과 제2항에 따른 개인정보 정정·삭제 요구서를 받은 날부터 10일 이내에 법 제36조제2항에 따라 해당 개인정보의 정정·삭제 등의 조치를 한 경우에는 그 조치를 한 사실을, 법 제36조제1항 단서에 해당하여 삭제 요구에 따르지 아니한 경우에는 그 사실 및 이유와 이의제기방법을 행정자치부령으로 정하는 개인정보 정정·삭제 결과 통지서로 해당 정보주체에게 알려야 한다.<개정 2013.3.23, 2014.11.19>

제44조(개인정보의 처리정지 등) ① 정보주체는 법 제37조제1항에 따라 개인정보처리자에게 자신의 개인정보 처리의 정지를 요구하려는 경우에 행정자치부령으로 정하는 개인정보 처리정지 요구서를 그 개인정보처리자에게 제출하여야 한다. <개정 2013.3.23, 2014.11.19>

② 개인정보처리자는 제1항에 따른 개인정보 처리정지 요구서를 받은 날부터 10일 이내에 법 제37조제2항 본문에 따라 해당 개인정보의 처리정지 조치를 한 경우에는 그 조치를 한 사실을, 같은 항 단서에 해당하여 처리정지 요구에 따르지 아니한 경우에는 그 사실 및 이유와 이의제기방법을 행정자치부령으로 정하는 개인정보 처리정지 요구에 대한 결과 통지서로 해당 정보주체에게 알려야 한다.<개정 2013.3.23, 2014.11.19>

제45조(대리인의 범위 등) ① 법 제38조에 따라 정보주체를 대리할 수 있는 자는 다음 각 호와 같다.

1. 정보주체의 법정대리인
2. 정보주체로부터 위임을 받은 자

② 제1항에 따른 대리인이 법 제38조에 따라 정보주체를 대리할 때에는 개인정보처리자에게 행정자치부령으로 정하는 정보주체의 위임장을 제출하여야 한다.<개정 2013.3.23, 2014.11.19>

제46조(정보주체 또는 대리인의 확인) ① 개인정보처리자는 제41조제1항에 따른 열람의 요구, 제43조제1항에 따른 정정·삭제의 요구 또는 제44조제1항에 따른 처리정지의 요구(이하 이 조, 제47조 및 제48조에서 "열람등요구"라 한다)를 받았을 때에는 열람등요구를 한 자가 본인이거나 정당한 대리인인지를 확인하여야 한다.

② 공공기관인 개인정보처리자가 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 제1항에 따른 확인을 할 수 있는 경우에는 행정정보의 공동이용을 통하여 확인하여야 한다. 다만, 해당 공공기관이 행정정보의 공동이용을 할 수 없거나 정보주체가 확인에 동의하지 아니하는 경우에는 그러하지 아니하다.

제47조(수수료 등의 금액 등) ① 법 제38조제3항에 따른 수수료와 우송료의 금액은 열람등요구에 필요한 실비의 범위에서 해당 개인정보처리자가 정하는 바에 따른다. 다만, 개인정보처리자가 지방자치단체인 경우에는 그 지방자치단체의 조례로 정하는 바에 따른다.

② 개인정보처리자는 열람등요구를 하게 된 사유가 그 개인정보처리자에게 있는 경우에는 수수료와 우송료를 청구해서는 아니 된다.

③ 법 제38조제3항에 따른 수수료 또는 우송료는 다음 각 호의 구분에 따른 방법으로 낸다. 다만, 국회, 법원, 헌법재판소, 중앙선거관리위원회, 중앙행정기관 및 그 소속 기관(이하 이 조에서 "국가기관"이라 한다) 또는 지방자치단체인 개인정보처리자는 「전자금융거래법」 제2조제11호에 따른 전자지급수단 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제10호에 따른 통신과금서비스를 이용하여 수수료 또는 우송료를 내게 할 수 있다.

1. 국가기관인 개인정보처리자에게 내는 경우: 수입인지
2. 지방자치단체인 개인정보처리자에게 내는 경우: 수입증지
3. 국가기관 및 지방자치단체 외의 개인정보처리자에게 내는 경우: 해당 개인정보처리자가 정하는 방법

제48조(열람 요구 지원시스템의 구축 등) ① 개인정보처리자는 열람등요구 및 그에 대한 통지를 갈음하여 해당 업무를 전자적으로 처리할 수 있도록 시스템을 구축·운영하거나 그 밖의 절차를 정하여 해당 업무를 처리할 수 있다.

② 행정자치부장관은 개인정보처리자 중 공공기관이 보유하고 있는 개인정보에 관한 열람등요구 및 그에 대한 통지에 관한 공공기관의 업무 수행을 효율적으로 지원하기 위하여 시스템을 구축·운영할 수 있다.<개정 2013.3.23, 2014.11.19>

제7장 개인정보 분쟁조정

제48조의2(당연직위원) 법 제40조제1항에 따른 개인정보 분쟁조정위원회(이하 "분쟁조정위원회"라 한다)의 당연직위원은 행정자치부·방송통신위원회·금융위원회 및 보호위원회의 고위공무원단에 속하는 일반직공무원으로서 개인정보 보호에 관한 업무를 담당하는 사람 중 소속 기관의 장이 지명하는 사람으로 한다.

[본조신설 2016.7.22]

제49조(조정부의 구성 및 운영) ① 법 제40조제6항에 따른 조정부(이하 "조정부"라 한다)는 분쟁조정위원회 위원장이 지명하는 5명 이내의 위원으로 구성하되, 그 중 1명은 변호사 자격이 있는 위원으로 한다. <개정 2016.7.22>

② 분쟁조정위원회 위원장은 조정부의 회의를 소집한다.

③ 분쟁조정위원회의 위원장은 조정부의 회의를 소집하려면 회의 날짜·시간·장소 및 안건을 정하여 회의 개최 7일 전까지 조정부의 각 위원에게 알려야 한다. 다만, 긴급한 사정이 있는 경우에는 그러하지 아니하다.

④ 조정부의 장은 조정부 위원 중에서 호선(互選)한다.

⑤ 제1항부터 제4항까지의 규정에서 정한 사항 외에 조정부의 구성 및 운영 등에 필요한 사항은 분쟁조정위원회의 의결을 거쳐 분쟁조정위원회의 위원장이 정한다.

제50조(사무기구) 법 제40조제8항에 따른 분쟁조정 접수 및 사실 확인 등 분쟁조정에 필요한 사무처리는 보호위원회의 사무기구가 수행한다.

[전문개정 2016.7.22]

제51조(분쟁조정위원회 등의 운영) ① 분쟁조정위원회 위원장은 분쟁조정위원회의 회의를 소집하며, 그 의장이 된다.

② 분쟁조정위원회 위원장이 분쟁조정위원회의 회의를 소집하려면 회의 날짜·시간·장소 및 안건을 정하여 회의 개최 7일 전까지 각 위원에게 알려야 한다. 다만, 긴급한 사정이 있는 경우에는 그러하지 아니하다.

③ 분쟁조정위원회 및 조정부의 회의는 공개하지 아니한다. 다만, 필요하다고 인정되는 경우에는 분쟁조정위원회의 의결로 당사자 또는 이해관계인에게 방청을 하게 할 수 있다.

제52조(집단분쟁조정의 신청 대상) 법 제49조제1항에서 "대통령령으로 정하는 사건"이란 다음 각 호의 요건을 모두 갖춘 사건을 말한다.

1. 피해 또는 권리침해를 입은 정보주체의 수가 다음 각 목의 정보주체를 제외하고 50명 이상일 것
   가. 개인정보처리자와 분쟁해결이나 피해보상에 관한 합의가 이루어진 정보주체
   나. 같은 사안으로 다른 법령에 따라 설치된 분쟁조정기구에서 분쟁조정 절차가 진행 중인 정보주체
   다. 해당 개인정보 침해로 인한 피해에 대하여 법원에 소(訴)를 제기한 정보주체
2. 사건의 중요한 쟁점이 사실상 또는 법률상 공통될 것

제53조(집단분쟁조정 절차의 개시) ① 법 제49조제2항 후단에서 "대통령령으로 정하는 기간"이란 14일 이상의 기간을 말한다.

② 법 제49조제2항 후단에 따른 집단분쟁조정 절차의 개시 공고는 분쟁조정위원회의 인터넷 홈페이지 또는 「신문 등의 진흥에 관한 법률」에 따라 전국을 보급지역으로 하는 일반일간신문에 게재하는 방법으로 한다.<개정 2015.12.30>

제54조(집단분쟁조정 절차에 대한 참가 신청) ① 법 제49조에 따른 집단분쟁조정(이하 "집단분쟁조정"이라 한다)의 당사자가 아닌 정보주체 또는 개인정보처리자가 법 제49조제3항에 따라 추가로 집단분쟁조정의 당사자로 참가하려면 법 제49조제2항 후단의 공고기간에 문서로 참가 신청을 하여야 한다.

② 분쟁조정위원회는 제1항에 따라 집단분쟁조정 당사자 참가 신청을 받으면 제1항의 신청기간이 끝난 후 10일 이내에 참가 인정 여부를 문서로 알려야 한다.

제55조(집단분쟁조정 절차의 진행) ① 집단분쟁조정 절차가 개시된 후 제52조제1호가목부터 다목까지의 어느 하나에 해당하게 된 정보주체는 당사자에서 제외된다.
② 분쟁조정위원회는 제52조 각 호의 요건을 모두 갖춘 사건에 대하여 집단분쟁조정 절차가 개시되고 나면 그 후 집단분쟁조정 당사자 중 일부가 같은 조 제1호가목부터 다목까지의 어느 하나에 해당하게 되어 같은 조 제1호의 요건을 갖추지 못하게 되더라도 집단분쟁조정 절차를 중지하지 아니한다.

제56조(수당과 여비) 분쟁조정위원회 및 조정부의 회의에 출석한 위원 등에게는 예산의 범위에서 수당과 여비를 지급할 수 있다. 다만, 공무원인 위원이 그 소관 업무와 직접적으로 관련되어 출석하는 경우에는 그러하지 아니하다.

제57조(분쟁조정 세칙) 법 및 이 영에서 규정한 사항 외에 분쟁조정위원회의 운영 및 집단분쟁조정을 위하여 필요한 사항은 분쟁조정위원회의 의결을 거쳐 분쟁조정위원회의 위원장이 정한다.

제8장 보칙 및 벌칙

제58조(개선권고 및 징계권고) ① 법 제61조제2항·제3항에 따른 개선권고 및 법 제65조제2항·제3항에 따른 징계권고는 권고 사항, 권고 사유 및 조치 결과 회신기간 등을 분명하게 밝힌 문서로 하여야 한다.
② 제1항에 따른 권고를 받은 자는 권고 내용에 따라 필요한 조치를 하고, 그 결과를 행정자치부장관 또는 관계 중앙행정기관의 장에게 문서로 통보하여야 한다. 다만, 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 통보하여야 한다.<개정 2013.3.23, 2014.11.19>

제59조(침해 사실의 신고 등) 행정자치부장관은 법 제62조제2항에 따라 개인정보에 관한 권리 또는 이익 침해 사실 신고의 접수·처리 등에 관한 업무를 효율적으로 수행하기 위한 전문기관으로 한국인터넷진흥원을 지정한다. <개정 2013.3.23, 2014.11.19>

제60조(자료제출 요구 및 검사) ① 법 제63조제1항제3호에서 "대통령령으로 정하는 경우"란 개인정보 유출 등 정보주체의 개인정보에 관한 권리 또는 이익을 침해하는 사건·사고 등이 발생하였거나 발생할 가능성이 상당히 있는 경우를 말한다.
② 행정자치부장관은 법 제63조제1항 및 제2항에 따른 자료의 제출 요구 및 검사 등을 위하여 한국인터넷진흥원의 장에게 기술적인 사항을 자문하는 등 필요한 지원을 요청할 수 있다.<개정 2013.3.23, 2014.11.19, 2015.12.30>

제61조(결과의 공표) ① 행정자치부장관 및 관계 중앙행정기관의 장은 법 제66조제1항 및 제2항에 따라 다음 각 호의 사항을 인터넷 홈페이지 또는 「신문 등의 진흥에 관한 법률」에 따라 전국을 보급지역으로 하는 일반일간신문 등에 게재하여 공표할 수 있다. <개정 2013.3.23,

2014.11.19>

1. 위반행위의 내용
2. 위반행위를 한 자
3. 개선권고, 시정조치 명령, 고발, 징계권고 및 과태료 부과의 내용 및 결과

② 행정자치부장관 및 관계 중앙행정기관의 장은 법 제66조제1항 및 제2항에 따라 제1항 각 호의 사항을 공표하려는 경우에는 위반행위의 내용 및 정도, 위반 기간 및 횟수, 위반행위로 인하여 발생한 피해의 범위 및 결과 등을 고려하여야 한다.<개정 2013.3.23, 2014.11.19>

③ 행정자치부장관 및 관계 중앙행정기관의 장은 법 제66조제1항에 따른 보호위원회에 심의·의결을 요청하기 전에 공표대상자에게 공표대상자라는 사실을 알려 소명자료를 제출하거나 의견을 진술할 수 있는 기회를 주어야 한다.<개정 2013.3.23, 2014.11.19>

제62조(권한의 위탁) ① 삭제 <2015.12.30>

② 행정자치부장관은 법 제24조의2제4항에 따른 대체가입수단 제공의 지원에 관한 권한을 다음 각 호의 어느 하나의 기관에 위탁할 수 있다.<개정 2013.3.23, 2014.11.19, 2015.12.30>

1. 「전자정부법」 제72조제1항에 따른 한국지역정보개발원
2. 한국인터넷진흥원
3. 대체가입수단의 개발·제공·관리 업무를 안전하게 수행할 수 있는 기술적·재정적 능력과 설비를 보유한 것으로 인정되어 행정자치부장관이 고시하는 법인·기관·단체

③ 행정자치부장관은 다음 각 호의 권한을 한국인터넷진흥원에 위탁한다.<개정 2013.3.23, 2014.11.19, 2015.12.30>

1. 법 제13조제1호에 따른 개인정보 보호에 관한 교육·홍보
2. 법 제33조제5항에 따른 관계 전문가의 육성 및 영향평가 기준의 개발
3. 법 제35조제2항에 따른 열람 요구의 접수 및 처리
4. 법 제63조에 따른 자료제출 요구 및 검사(법 제62조에 따라 개인정보침해 신고센터에 접수된 신고의 접수·처리 및 상담과 관련된 사항만 해당한다)
5. 제37조제2항에 따른 평가기관 지정신청서의 접수 및 같은 조 제6항에 따른 신고 사항의 접수

④ 행정자치부장관은 제2항에 따라 권한을 위탁하는 경우에는 그 수탁자 및 위탁업무를 고시하여야 한다.<신설 2015.12.30>

제62조의2(고유식별정보의 처리) ① 행정자치부장관(제62조제3항에 따라 행정자치부장관의 권한을 위탁받은 자를 포함한다)은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다. <개정 2014.11.19, 2015.12.30>

1. 법 제24조의2제4항에 따른 주민등록번호 대체 방법 제공을 위한 시스템 구축 등 제반 조치 마련 및 지원에 관한 사무

2. 법 제34조의2에 따른 과징금의 부과 및 징수에 관한 사무
3. 법 제62조제3항에 따른 개인정보침해 신고센터의 업무에 관한 사무

② 분쟁조정위원회는 법 제45조 및 제47조에 따른 개인정보 분쟁 조정에 관한 사무를 수행하기 위하여 불가피한 경우 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

[본조신설 2014.8.6]

제62조의3(규제의 재검토) ① 행정자치부장관은 제40조의2 및 별표 1의2에 따른 과징금의 부과기준 등에 대하여 2014년 1월 1일을 기준으로 3년마다(매 3년이 되는 해의 1월 1일 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

② 행정자치부장관은 다음 각 호의 사항에 대하여 다음 각 호의 기준일을 기준으로 2년마다(매 2년이 되는 해의 기준일과 같은 날 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.<개정 2015.12.30>

1. 제23조에 따른 영상정보처리기기 설치 시 의견 수렴: 2015년 1월 1일
2. 제31조에 따른 개인정보 처리방침의 내용 및 공개방법 등: 2015년 1월 1일

2의2. 제37조에 따른 평가기관의 지정 및 지정 취소의 요건 등: 2016년 1월 1일

3. 제41조에 따른 개인정보의 열람절차 등: 2015년 1월 1일
4. 제52조에 따른 집단분쟁조정의 신청 대상: 2015년 1월 1일
5. 제63조 및 별표 2에 따른 과태료의 부과기준: 2015년 1월 1일

[전문개정 2014.12.9]

제63조(과태료의 부과기준) 법 제75조제1항부터 제3항까지의 규정에 따른 과태료의 부과기준은 별표 2와 같다.

부칙 <제23169호,2011.9.29>

제1조(시행일) 이 영은 2011년 9월 30일부터 시행한다. 다만, 제20조 및 별표 2 제2호자목은 2012년 3월 30일부터 시행한다.

제2조(다른 법령의 폐지) 공공기관의 개인정보보호에 관한 법률 시행령을 폐지한다.

제3조(기본계획 및 시행계획의 수립에 관한 경과조치) ① 행정안전부장관은 제11조에도 불구하고 2012년부터 제2014년까지의 기간에 대한 기본계획을 2011년 12월 31일까지 보호위원회의 심의·의결을 거쳐 수립하여야 한다.

② 중앙행정기관의 장은 제12조에도 불구하고 2012년 및 2013년에 시행할 시행계획을 제1항의 기본계획에 따라 2012년 2월 28일까지 보호위원회에 제출하여 2012년 4월 30일까지 보호위원회의 심의·의결을 거쳐 수립하여야 한다.

제4조(개인정보처리자가 수집·보유하고 있는 개인정보의 암호화에 관한 경과조치) 이 영 시행 당시 개인정보를 수집·보유하고 있는 개인정보처리자는 전자매체에 저장하는 개인정보에 대

하여 2012년 12월 31일까지 제30조제1항제3호에 따른 암호화 조치(제21조에 따라 준용되는 고유식별정보에 관한 암호화 조치를 포함한다)를 마쳐야 한다.

제5조(개인정보파일의 등록에 관한 경과조치) 이 영 시행 당시 개인정보파일을 운용하고 있는 공공기관(이 영 시행 전에 개인정보파일을 등록한 기관은 제외한다)의 장은 이 영 시행일부터 60일 이내에 제34조에 따라 행정안전부장관에게 등록을 신청하여야 한다.

제6조(개인정보 영향평가에 관한 경과조치) 이 영 시행 당시 제35조 각 호에 따른 개인정보파일을 운용하고 있거나, 운용할 목적으로 제35조 각 호에 따른 개인정보파일을 구축하고 있는 공공기관의 장은 이 영 시행일부터 5년 이내에 해당 개인정보파일에 대한 영향평가를 실시하고 그 결과를 행정안전부장관에게 제출하여야 한다.

제7조(다른 법령의 개정) ① 가맹사업거래의 공정화에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제5조의4제1항 중 "「공공기관의 개인정보보호에 관한 법률」 제2조제2호"를 "「개인정보 보호법」 제2조제1호"로 한다.

② 민주화운동관련자 명예회복 및 보상 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제19조의2 중 "「공공기관의 개인정보보호에 관한 법률」"을 "「개인정보 보호법」"으로 한다.

③ 발명진흥법 시행령 일부를 다음과 같이 개정한다.

제8조의2제2항 중 "「공공기관의 개인정보보호에 관한 법률」"을 "「개인정보 보호법」"으로 한다.

④ 소비자기본법 시행령 일부를 다음과 같이 개정한다.

제25조제7호를 다음과 같이 한다.

7. 「개인정보 보호법」 제40조에 따라 설치된 개인정보 분쟁조정위원회

⑤ 전자정부법 시행령 일부를 다음과 같이 개정한다.

제49조제1항 중 "「공공기관의 개인정보보호에 관한 법률」 제2조제8호"를 "「개인정보 보호법」 제2조제3호"로 한다.

⑥ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제3조제1항 중 "정보통신서비스 제공자 및 제71조에 따른 정보통신서비스 제공자 외의 자"를 "정보통신서비스 제공자"로 한다.

제16조부터 제22조까지를 각각 삭제한다.

제36조제6항을 삭제한다.

제66조제2항 중 "정보통신서비스 제공자등(법 제67조에 따라 준용되는 경우에 해당되는 자를 포함한다)"을 "정보통신서비스 제공자등"으로 한다.

제71조를 삭제한다.

제3조제1항ㆍ제2항, 제66조제2항, 제68조의2제1항 각 호 외의 부분, 같은 조 제2항, 제69조제1항 각 호 외의 부분 후단, 제70조제2항 각 호 외의 부분, 같은 조 제3항 각 호 외의 부분 및 별표 9 위반행위란의 제12호 각 목 외의 부분 중 "행정안전부장관 또는 방송통신위원회"를 각

각 "방송통신위원회"로 한다.

제8조(다른 법령과의 관계) 이 영 시행 당시 다른 법령에서 종전의 「공공기관의 개인정보보호에 관한 법률 시행령」 또는 그 규정을 인용하고 있는 경우 이 영 가운데 그에 해당하는 규정이 있을 때에는 종전의 규정을 갈음하여 이 영 또는 이 영의 해당 규정을 인용한 것으로 본다.

부칙 <제24425호,2013.3.23>

제1조(시행일) 이 영은 공포한 날부터 시행한다. 다만, 부칙 제6조에 따라 개정되는 대통령령 중 이 영 시행 전에 공포되었으나 시행일이 도래하지 아니한 대통령령을 개정한 부분은 각각 해당 대통령령의 시행일부터 시행한다.

제2조부터 제5조까지 생략

제6조(다른 법령의 개정) ①부터 ④까지 생략

⑤ 개인정보 보호법 시행령 일부를 다음과 같이 개정한다.

제11조제1항, 같은 조 제2항 전단·후단, 같은 조 제3항, 제12조제1항, 제13조제1항 각 호 외의 부분, 같은 조 제2항, 제14조, 제20조제2항 각 호 외의 부분, 제27조, 제30조제2항·제3항, 제32조제3항, 제34조제1항 전단, 같은 조 제2항·제3항, 제37조제1항 각 호 외의 부분, 제2항 각 호 외의 부분, 같은 조 제3항 각 호 외의 부분 본문, 같은 조 제4항 각 호 외의 부분 전단, 같은 조 제5항 각 호 외의 부분 본문, 같은 조 제6항 각 호 외의 부분 본문, 같은 조 제7항, 제38조제2항 각 호 외의 부분, 같은 조 제3항, 제41조제2항 전단·후단, 제48조제2항, 제50조제2항, 제58조제2항 본문, 제59조, 제60조제2항, 제61조제1항 각 호 외의 부분, 같은 조 제2항·제3항, 제62조제1항 각 호 외의 부분, 같은 조 제2항 및 제3항 중 "행정안전부장관"을 각각 "안전행정부장관"으로 한다.

제13조제3항 후단 중 ""행정안전부장관""을 ""안전행정부장관""으로 한다.

제15조 각 호 외의 부분, 제34조제1항 전단, 제37조제2항 각 호 외의 부분, 같은 항 제4호, 같은 조 제6항 각 호 외의 부분 본문, 제41조제1항 각 호 외의 부분, 같은 조 제4항, 제42조제2항, 제43조제1항·제3항, 제44조제1항·제2항 및 제45조제2항 중 "행정안전부령"을 각각 "안전행정부령"으로 한다.

별표 1의 제6호 중 "행정안전부장관"을 "안전행정부장관"으로 한다.

별표 2의 제1호나목1)부터 4)까지 외의 부분 본문 및 같은 호 다목1)부터 3)까지 외의 부분 본문 중 "행정안전부장관"을 각각 "안전행정부장관"으로 한다.

⑥부터 <129>까지 생략

부칙 <제25531호,2014.8.6>

이 영은 2014년 8월 7일부터 시행한다.

부칙 <제25751호,2014.11.19>

제1조(시행일) 이 영은 공포한 날부터 시행한다. 다만, 부칙 제5조에 따라 개정되는 대통령령 중 이 영 시행 전에 공포되었으나 시행일이 도래하지 아니한 대통령령을 개정한 부분은 각각 해당 대통령령의 시행일부터 시행한다.

제2조부터 제4조까지 생략

제5조(다른 법령의 개정) ①부터 <104>까지 생략

<105> 개인정보 보호법 시행령 일부를 다음과 같이 개정한다.

제11조제1항, 같은 조 제2항 전단·후단, 같은 조 제3항, 제12조제1항, 제13조제1항 각 호 외의 부분, 같은 조 제2항, 같은 조 제3항 후단, 제14조, 제16조제2항, 제27조, 제30조제2항·제3항, 제32조제3항, 제34조제1항 전단, 같은 조 제2항·제3항, 제37조제1항 각 호 외의 부분, 같은 조 제2항 각 호 외의 부분, 같은 조 제3항 각 호 외의 부분 본문, 같은 조 제4항 각 호 외의 부분 전단, 같은 조 제5항 각 호 외의 부분 본문, 같은 조 제6항 각 호 외의 부분 본문, 같은 조 제7항, 제38조제2항 각 호 외의 부분, 같은 조 제3항, 제40조의2제2항, 같은 조 제3항 본문, 제41조제2항 전단·후단, 제48조제2항, 제50조제2항, 제58조제2항 본문, 제59조, 제60조제2항, 제61조제1항 각 호 외의 부분, 같은 조 제2항·제3항, 제62조제1항 각 호 외의 부분, 같은 조 제2항·제3항, 제62조의2제1항 각 호 외의 부분 및 제62조의3 중 "안전행정부장관"을 각각 "행정자치부장관"으로 한다.

제15조 각 호 외의 부분, 제34조제1항 전단, 제37조제2항 각 호 외의 부분, 같은 항 제4호, 같은 조 제6항 각 호 외의 부분 본문, 제41조제1항 각 호 외의 부분, 같은 조 제4항, 제42조제2항, 제43조제1항·제3항, 제44조제1항·제2항 및 제45조제2항 중 "안전행정부령"을 각각 "행정자치부령"으로 한다.

별표 1 제6호 중 "안전행정부장관"을 "행정자치부장관"으로 한다.

별표 2 제1호나목1)부터 4)까지 외의 부분 본문 및 같은 호 다목1)부터 3)까지 외의 부분 본문 중 "안전행정부장관"을 각각 "행정자치부장관"으로 한다.

<106>부터 <418>까지 생략

부칙 <제25840호,2014.12.9>

제1조(시행일) 이 영은 2015년 1월 1일부터 시행한다.

제2조부터 제16조까지 생략

부칙 <제26140호,2015.3.11>

제1조(시행일) 이 영은 공포한 날부터 시행한다.

제2조 생략

제3조(다른 법령의 개정) ① 개인정보 보호법 시행령 일부를 다음과 같이 개정한다.

제24조제4항제3호 중 "보안목표시설"을 "국가보안시설"로 한다.

②부터 ⑤까지 생략

부칙 <제26728호,2015.12.22>

제1조(시행일) 이 영은 2015년 12월 23일부터 시행한다.

제2조 생략

제3조(다른 법령의 개정) ① 개인정보 보호법 시행령 일부를 다음과 같이 개정한다.

제37조제1항제1호라목을 다음과 같이 한다.

라. 「정보보호산업의 진흥에 관한 법률」 제23조제1항제1호 및 제2호에 따른 업무

② 및 ③ 생략

부칙 <제26776호,2015.12.30>

이 영은 공포한 날부터 시행한다. 다만, 제21조의2, 제62조제2항, 제62조의2제1항제1호 및 별표 2의 개정규정은 2016년 1월 1일부터 시행한다.

부칙 <제27370호,2016.7.22>

제1조(시행일) 이 영은 2016년 7월 25일부터 시행한다.

제2조(기본계획 및 시행계획의 수립에 관한 경과조치) ① 종전의 제11조에 따라 수립된 2015년부터 2017년까지의 기간에 대한 기본계획은 제11조의 개정규정에 따라 수립된 기본계획으로 본다.

② 종전의 제12조에 따라 수립된 2016년 및 2017년에 대한 시행계획은 각각 제12조의 개정규정에 따라 수립된 시행계획으로 본다.

부칙 <제27522호,2016.9.29>

이 영은 2016년 9월 30일부터 시행한다.

[별표 1] <개정 2014.11.19.>

전문인력의 자격기준(제37조제1항제2호 관련)

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원이 시행하는 정보보호전문가(SIS) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
2. 「전자정부법」 제60조에 따른 감리원(ISA) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
3. 「국가기술자격법」에 따른 정보통신 직무분야의 국가기술자격 중 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 전자계산기조직응용기사, 정보처리기사 또는 정보통신기사 기술자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
4. 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 공인정보시스템감사사(CISA) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
5. 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 공인정보시스템보호전문가(CISSP) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람
6. 그 밖에 개인정보 보호와 관련된 자격으로서 행정자치부장관이 정하는 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람

비고

"개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람"이란 공공기관, 법인 및 단체 등의 임직원으로 개인정보 보호를 위한 공통기반기술(암호기술, 인증기술 등을 말한다), 시스템·네트워크 보호(시스템 보호, 해킹·바이러스 대응, 네트워크 보호 등을 말한다) 또는 응용서비스 보호(전자거래 보호, 응용서비스 보호, 정보보호 표준화 등을 말한다)에 해당하는 분야에서 계획, 분석, 설계, 개발, 운영, 유지·보수, 감리, 컨설팅 또는 연구·개발 업무 등을 수행한 경력이 있는 사람을 말한다.

[별표 1의2] <신설 2014.8.6>

과징금의 부과기준(제40조의2제1항 관련)

1. 과징금 부과 여부의 결정

과징금은 법 제34조의2제2항 각 호의 사항과 위반행위의 내용 등을 종합적으로 고려하여 그 부과 여부를 결정한다. 다만, 법 제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 과징금을 부과하지 아니한다.

2. 과징금의 산정기준

과징금은 법 제34조의2제2항 각 호의 사항과 이에 영향을 미치는 사항을 종합적으로 고려하여 산정하되, 가목의 위반 정도에 따른 산정기준액에 나목의 안전성 확보에 필요한 조치 이행 노력 정도 등에 따른 조정(이하 "1차 조정"이라 한다), 다목의 위반행위의 기간 및 횟수 등에 따른 조정(이하 "2차 조정"이라 한다)을 거쳐 라목에 따라 부과과징금을 산정한다. 다만, 산정된 과징금이 5억원을 초과하는 경우에는 5억원으로 한다.

가. 기본 산정기준

위반 정도	산정기준액	비 고
매우 중대한 위반행위	3억 5천만원	고의 또는 중과실로 인하여 10만건 이상의 주민등록번호가 분실·도난·유출·변조 또는 훼손(이하 "분실등"이라 한다)된 경우를 말한다.
중대한 위반행위	2억 3천만원	고의 또는 중과실로 인하여 10만건 미만의 주민등록번호가 분실등이 된 경우 및 경과실로 인하여 10만건 이상의 주민등록번호가 분실등이 된 경우를 말한다.
일반 위반행위	1억원	경과실로 인하여 10만건 미만의 주민등록번호가 분실등이 된 경우를 말한다.

나. 1차 조정

법 제24조제3항에 따른 안전성 확보에 필요한 조치 이행 노력 정도, 피해를 최소화하기 위한 대책 마련 등 피해확산 방지를 위한 후속조치 이행 여부를 고려하여 산정기준액의 100분의 50의 범위에서 가중하거나 감경한다.

다. 2차 조정

위반행위의 기간 및 횟수, 위반 행위에 대한 조사 협조 여부, 위반행위에 따른 추가적 피해 발생 여부, 평소 개인정보 보호를 위한 노력 정도 등을 종합적으로 고려하여 1차 조정된 금액의 100분의 50의 범위에서 가중하거나 감경한다.

라. 부과과징금의 산정

개인정보처리자의 현실적 부담능력이나 그 위반행위가 미치는 효과, 위반행위로 인하여 취득한 이익의 규모 등을 고려하여 볼 때 과중하다고 인정되는 경우에는 2차 조정된 금액의 100분의 50의 범위에서 감액하여 부과과징금으로 정할 수 있다.

[별표 2] <개정 2016. 9. 29.>

과태료의 부과기준(제63조 관련)

1. 일반기준

가. 위반행위의 횟수에 따른 과태료 부과기준은 최근 3년간 같은 위반행위로 과태료를 부과받은 경우에 적용한다. 이 경우 위반행위에 대하여 과태료 부과처분을 한 날과 다시 같은 위반행위를 적발한 날을 각각 기준으로 하여 위반 횟수를 계산한다.

나. 행정자치부장관 또는 관계 중앙행정기관의 장은 다음의 어느 하나에 해당하는 경우에는 제2호에 따른 과태료 부과금액의 2분의 1의 범위에서 그 금액을 감경할 수 있다. 다만, 과태료를 체납하고 있는 위반행위자의 경우에는 그러하지 아니하다.

1) 위반행위자가 「질서위반행위규제법 시행령」 제2조의2제1항 각 호의 어느 하나에 해당하는 경우

2) 위반행위가 사소한 부주의나 오류로 인한 것으로 인정되는 경우

3) 위반행위자가 위법행위로 인한 결과를 시정하였거나 해소한 경우

4) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 과태료를 감경할 필요가 있다고 인정되는 경우

다. 행정자치부장관 또는 관계 중앙행정기관의 장은 다음의 어느 하나에 해당하는 경우에는 제2호에 따른 과태료 부과금액의 2분의 1의 범위에서 그 금액을 가중할 수 있다. 다만, 가중할 사유가 여러 개인 경우라도 법 제75조제1항부터 제3항까지의 규정에 따른 과태료 금액의 상한을 넘을 수 없다.

1) 위반의 내용 및 정도가 중대하여 소비자 등에게 미치는 피해가 크다고 인정되는 경우

2) 법 위반상태의 기간이 3개월 이상인 경우

3) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 과태료를 가중할 필요가 있다고 인정되는 경우

2. 개별기준

(단위: 만원)

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
가. 법 제15조제1항을 위반하여 개인정보를 수집한 경우	법 제75조제1항제1호	1000	2000	4000
나. 법 제15조제2항, 제17조제2항, 제18조제3항 또는 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 않은 경우	법 제75조제2항제1호	600	1200	2400

다. 법 제16조제3항 또는 제22조제4항을 위반하여 재화 또는 서비스의 제공을 거부한 경우	법 제75조 제2항제2호	600	1200	2400
라. 법 제20조제1항 또는 제2항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제75조 제2항제3호	600	1200	2400
마. 법 제21조제1항을 위반하여 개인정보를 파기하지 않은 경우	법 제75조 제2항제4호	600	1200	2400
바. 법 제21조제3항을 위반하여 개인정보를 분리하여 저장·관리하지 않은 경우	법 제75조 제3항제1호	200	400	800
사. 법 제22조제1항부터 제3항까지의 규정을 위반하여 동의를 받은 경우	법 제75조 제3항제2호	200	400	800
아. 법 제22조제5항을 위반하여 법정대리인의 동의를 받지 않은 경우	법 제75조 제1항제2호	1000	2000	4000
자. 법 제24조의2제1항을 위반하여 주민등록번호를 처리한 경우	법 제75조 제2항제4호의2	600	1200	2400
차. 법 제24조의2제2항을 위반하여 암호화 조치를 하지 않은 경우	법 제75조 제2항제4호의3	600	1200	2400
카. 법 제24조의2제3항을 위반하여 정보주체가 주민등록번호를 사용하지 않을 수 있는 방법을 제공하지 않은 경우	법 제75조 제2항제5호	600	1200	2400
타. 법 제23조제2항, 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1200	2400
파. 법 제25조제1항을 위반하여 영상정보처리기기를 설치·운영한 경우	법 제75조 제2항제7호	600	1200	2400
하. 법 제25조제2항을 위반하여 영상정보처리기기를 설치·운영한 경우	법 제75조 제1항제3호	1000	2000	4000
거. 법 제25조제4항을 위반하여 안내판 설치 등 필요한 조치를 하지 않은 경우	법 제75조 제3항제3호	200	400	800
너. 법 제26조제1항을 위반하여 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서에 의하지 않은 경우	법 제75조 제3항제4호	200	400	800
더. 법 제26조제2항을 위반하여 위탁하는 업무의 내용과 수탁자를 공개하지 않은 경우	법 제75조 제3항제5호	200	400	800
러. 법 제27조제1항 또는 제2항을 위반하여 정보주체에게 개인정보의 이전 사실을 알리지 않은	법 제75조 제3항제6호	200	400	800

경우				
머. 법 제30조제1항 또는 제2항을 위반하여 개인정보 처리방침을 정하지 않거나 이를 공개하지 않은 경우	법 제75조제3항제7호	200	400	800
버. 법 제31조제1항을 위반하여 개인정보 보호책임자를 지정하지 않은 경우	법 제75조제3항제8호	500		
서. 법 제32조의2제6항을 위반하여 인증을 받지 않았음에도 거짓으로 인증의 내용을 표시하거나 홍보한 경우	법 제75조제2항제7호의2	600	1200	2400
어. 법 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제75조제2항제8호	600	1200	2400
저. 법 제34조제3항을 위반하여 조치 결과를 신고하지 않은 경우	법 제75조제2항제9호	600	1200	2400
처. 법 제35조제3항을 위반하여 열람을 제한하거나 거절한 경우	법 제75조제2항제10호	600	1200	2400
커. 법 제35조제3항·제4항, 제36조제2항·제4항 또는 제37조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 않은 경우	법 제75조제3항제9호	200	400	800
터. 법 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 않은 경우	법 제75조제2항제11호	600	1200	2400
퍼. 법 제37조제4항을 위반하여 처리가 정지된 개인정보에 대하여 파기 등 필요한 조치를 하지 않은 경우	법 제75조제2항제12호	600	1200	2400
허. 법 제63조제1항에 따른 관계 물품·서류 등 자료를 제출하지 않거나 거짓으로 제출한 경우	법 제75조제3항제10호			
1) 자료를 제출하지 않은 경우		100	200	400
2) 자료를 거짓으로 제출한 경우		200	400	800
고. 법 제63조제2항에 따른 출입·검사를 거부·방해 또는 기피한 경우	법 제75조제3항제11호	200	400	800
노. 법 제64조제1항에 따른 시정명령에 따르지 않은 경우	법 제75조제2항제13호	600	1200	2400

기반보호법

1. 주요정보통신기반시설 취약점 분석 · 평가 기준
2. 미래창조과학부 소관 주요정보통신기반시설 보호지침
3. 정보통신기반 보호법
4. 정보통신기반 보호법 시행령
5. 정보통신기반 보호법 시행규칙

주요정보통신기반시설 취약점 분석 · 평가 기준

[시행 2013.8.8] [고시 제2013 - 37호, 2013.8.8, 일부개정]

1. 취약점 분석 · 평가 개요

o 취약점 분석 · 평가란, 악성코드 유포, 해킹 등 사이버 위협에 대한 주요정보통신기반시설의 취약점을 종합적으로 분석 및 평가?개선하는 일련의 과정을 말함

- 주요정보통신기반시설의 안정적 운영을 위협하는 사이버보안 점검항목과 항목별 세부 점검항목을 도출하여 취약점 분석을 실시

- 발견된 취약점에 대한 위험등급 부여, 개선방향 수립 등의 유기적인 평가 수행

<img id="14797192">

< 관련 근거 >

┌──
──┐
│ │
│ │
│ 정보통신기반 보호법 제9조(취약점의 분석 · 평가) │
│ ①관리기관의 장은 대통령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석 · │
│ 평가하여야 한다. │
│ - - - - - - - - - - - - - - - - - - (중략) - │
│ ④미래창조과학부장관은 관계중앙행정기관의 장 및 국가정보원장과 협의하여 제1항의 규정에 의한 취 │
│ 약점 분석 · 평가에 관한 기준을 정하고 이를 관계중앙행정기관의 장에게 통보하여야 한다. │
└──
──┘

</img>

2. 취약점 분석 · 평가 수행 주체 및 주기

□ 수행 주체

o 주요정보통신기반시설의 관리기관이 직접 수행할 경우 자체 전담반을 구성하여 운영

- 정보통신기반 보호법 시행령[별표1 : 취약점 분석 · 평가 전담반 구성 기준] [붙임1]

o 관리기관이 외부기관에게 위탁할 경우, 지식정보보안 컨설팅전문업체 등 전문기관에 위탁 수행

- 전문기관 : 한국인터넷진흥원, 정보공유 · 분석센터, 한국전자통신연구원, 지식정보보안 컨설팅전문업체 등 (정보통신기반 보호법 제9조)

※ 지식정보보안 컨설팅전문업체(정보통신산업진흥법 제33조) : 롯데정보통신, 시큐아이닷컴, 싸이버원, 안랩, 에스티지시큐리티, 에이쓰리시큐리티, 인포섹 이상 7개(2012년 11월 기준)

□ 수행 주기

o 주요정보통신기반시설로 지정된 첫 회는 지정 후 6개월 이내에 취약점 분석 · 평가를 실시

- 6개월 이내 취약점 분석 · 평가를 수행치 못할 경우 관할 중앙행정기관의 장의 승인을 얻어 3개월 연장가능(총9개월)

- 주요정보통신기반시설로 최초 지정일로 부터 6개월 이전 취약점 분석 · 평가를 하였을 경우 수행한 것으로 간주

※ 단, 6개월 이내의 취약점 분석 · 평가 수행 내용이 본 기준에 부합할 경우에 한하여 인정

o 매년 정기적으로 취약점 분석 · 평가 실시

- 취약점 분석 · 평가는 가용자원과 대상시설 식별, 자산 중요도 산정 및 해당 시스템 대한 정밀 분석 실시

- 취약점 분석 · 평가 대상시설에 중대한 변화가 있거나, 관리기관의 장이 필요하다고 판단하는 경우에는 1년이 되지않아도 취약점 분석 · 평가를 실시할 수 있음

3. 취약점 분석 평가의 범위 및 항목

o 취약점 분석?평가의 범위는 주요정보통신기반시설의 세부시설로 정의된 정보시스템 자산, 제어시스템 자산, 의료시스템 자산 등

- 정보시스템 자산에 직?간접적으로 관여하는 물리적?관리적?기술적 분야를 포함

o 정보통신기반시설과 연계된 타 시스템이 있을 경우는 연계 시스템이 기반시설에 미치는 영향을 포함

※ 연계된 타 시스템이란 내부 시스템과 외부 기관과의 연계전용망, 원격 접속을 위한 VPN 망, 인터넷 연결망 등의 접속구간과 정보시스템을 의미

o 취약점 분석?평가 기본항목은 ①관리적, ②물리적, ③기술적으로 구분

- 기본 항목은 3단계(상?중?하)로 중요도를 분리

- 기본 항목의 중요도 “상”인 점검항목은 필수적으로 점검[붙임2]

- 기본 항목의 “중”, “하” 항목은 기관의 사정에 따라 선택점검[붙임3]

※ 점검결과 사용되지 않거나, 불필요한 항목은 안전한 설정값 변환 등 보호대책 마련

4. 수행 절차 및 방법

□ 수행절차 : 4단계 구성
<img id="14797174">

</img>
□ 1단계 : 취약점 분석·평가 계획 수립

o 평가계획은 수행주체(자체?외부위탁), 수행절차, 소요예산, 산출물 등 취약점 분석?평가를 위한 세부계획을 수립

□ 2단계 : 취약점 분석·평가 대상 선별

o 기반시설의 IT자산, 제어시스템자산, 의료장비 등 자산을 식별하고, 유형별로 그룹화하여, 취약점 분석?평가 대상목록 작성

<img id="14797193">

</img>

o 식별된 대상목록의 각 자산에 대하여 중요도를 산정

※ 주요정보통신기반시설의 특성을 고려하여 상 · 중 · 하, 1~3등급 등으로 구분

□ 3단계 : 취약점 분석 수행

o 취약점 분석?평가를 위한 관리적/물리적/기술적 세부 점검항목표 수립

- [붙임2]로 제시된 취약점 점검항목을 기본으로 하며, 기관별 특성에 따라 추가 보완하여 점검표를 작성

- 특정 시스템(특정OS, 특정DB 등)에 대해서는 [붙임2]의 점검항목을 기반으로 일부 항목을 조정하여 점검표 마련

※ 예) VMS, OS/2 등의 특정OS 시스템은 붙임2의 유닉스 점검항목을 기반으로 점검을 수행하고 시스템 상황에 따라 일부 항목을 가감

<img id="14797195">

</img>

o 취약점 분석요령은 관리적/물리적/기술적으로 구분하여 확인

- 관리적 점검 요령은 정보보호 정책/지침 등 관련 문서 확인과 정보보호 담당자, 시스템 관리자, 사용자 등과의 면담으로 확인

- 물리적 점검 요령은 전산실, 현관, 발전실 등의 통제구역을 실사하여 확인

- 기술적 점검 요령은 점검도구(툴), 수동점검, 모의해킹 등을 통해 확인

※ 직전년도에 발견된 취약점에 대해서는 중점적인 확인 수행

□ 4단계 : 취약점 평가 수행

o 취약점 분석 결과에 대해 세부내용을 서술하고 발견된 취약점별 위험등급 표시 및 개선방향 수립을 원칙으로 함

- 위험등급은 상 · 중 · 하 등 3단계로 표시

※ 비밀성, 무결성, 가용성을 고려하여 위험등급(상?중?하)을 정의하고 구분

- 위험등급 “상”은 조기개선, “중”, “하”는 중기 또는 장기개선으로 구분하여 개선방향 수립

o 다만, 취약점 분석 · 평가 결과에 대해 정량적인 점수(100점 만점)로 산출 · 관리를 희망하는 관리기관은 [붙임4]의 산출식 예시를 참고하여 수행

※ 취약점 분석 · 평가 결과에 대한 정량적인 점수 산출은 관리기관의 시범적용 사례를 토대로 유효성, 적정성을 분석 후 필요시 향후 전면시행 검토 예정

5. 기타사항

o 취약점 분석?평가에서 발견된 위험요소(취약점)는 보호대책에 반영

- 차년도 보호대책의 추진 과제중 “예방계획” 또는 “대응복구계획”항목에 기재

o 취약점 분석?평가 결과 오용 방지를 위한 관리강화

- 취약점 분석?평가 결과는 해당 기관에서만 관리하고, 수행업체의 노트북, USB 등에 저장된 자료는 폐기

- 수행업체로 인한 외부유출 방지를 위하여 벌칙조항이 포함된 서약서 징구

[붙임1] 취약점 분석 · 평가 전담반 구성 기준

구성원	역할 또는 경력 · 자격 기준
반장 (정보보호책임자)	취약점 분석·평가 시행의 총괄
관리기술 담당	관리적·물리적 정보보호 등 조직의 정보보호관리체계의 관리·운영경력 소유자, 정보시스템 감리 경력자
응용프로그램 담당	해당기관의 주요정보통신기반시설에 대한 핵심 프로그램 개발·유지보수 경력자
서버 담당	유닉스, 리눅스, 윈도우 등 각종 서버관련 기술 보유자
정보보호 담당	정보보호시스템 평가 및 운영자, 정보보호정책·위험분석 또는 취약점 점검·평가 등의 보안관리기술 경력자
네트워크 담당	WAN, LAN, NMS 및 무선통신 등에 관한 기술 및 각종 통신 프로토콜 기술 보유자

※ 비고 : 관리기관은 소관 주요정보통신기반시설의 특성에 따라 전담반 구성요건을 고려하여 취약점 분석 · 평가를 수행할 수 있는 적정인원의 전문인력을 확보하여야 한다.

[붙임2]

취약점 분석·평가 기본항목

□ 관리적 분야

분류	번호	취약점 점검 항목	등급
정보 보호정책	A-1	조직 전반에 적용하고 있는 정보보호 정책/지침 또는 규정이 수립되었는가?	상
	A-2	정기적으로 정보보호정책의 타당성을 검토, 평가하여 수정 보완하고 있는가?	상
	A-3	연도별 정보보안업무 세부추진 계획을 수립·시행하고 그 추진결과에 대한 심사분석·평가를 실시하는가	상
	A-4	최근 1년간 기관장에게 연간 보호대책 등의 주요 정보보안 관련 사항을 보고하였는가?	상
정보 보호조직	A-5	보안활동을 계획, 실행, 검토하는 보안 전담조직 및 전담 보안 담당자가 구성되어 있는가?	상
인적 보안	A-6	신원조회(민간기관 제외)가 수행되고 비밀유지서약서를 작성하고 있으며 주기적으로 갱신되고 있는가?	상
	A-7	계약직 및 임시직원은 물론 정식직원 채용 시 신원, 업무능력, 교육정도, 경력 등에 대한 적격심사가 이루어지고 있는가?	상
외부자 보안	A-8	제3자(외부유지보수직원, 외부용역자포함)에 의한 정보자산 접근과 관련한 보안요구사항을 계약에 포함하고 있는가?	상
	A-9	위탁 기관(업체) 또는 용역사업 참여 업체의 보안관련사항 위반이나 침해사고 발생 시 조치를 수행하는가?	상
자산 분류	A-10	조직의 중요한 자산(인력, 시설, 장비 등)에 대한 자산분류기준이 있는가?	상
	A-11	정보자산을 보안등급과 중요도 등에 따라 분류하여 관리하고 있는가?	상
	A-12	정보자산별로 책임자가 지정되어 있으며 소유자, 관리자, 사용자들이 확인되고 있는가?	상
매체 관리	A-13	미디어 장치의 사용 및 반출입에 대한 관리절차나 문서가 있는가?	상
	A-14	정보나 매체가 용도 폐기되기 위한 폐기 방법이 수립되고 적절하게 이행되는가?	상
교육 및 훈련	A-15	교육 훈련 대상은 관련된 모든 내외 임직원 및 외부 인력을 포함하고 있으며 정보자산에 간접적으로 접근하는 일반 외부 용역 직원에 대해서도 정보보호교육훈련을 수행하는가?	상
접근 통제	A-16	업무 요구사항에 따라 접근통제의 방법과 범위 등을 정의하고 문서화하고 있는가?	상
	A-17	허가된 원격작업내용, 작업시간, 접근 허가된 내부 시스템 및 서비스 등의 내용을 포함한 재택근무 등의 원격작업에 대한 정책, 절차가 존재하는가?	상
	A-18	스마트폰·개인휴대단말기(PDA)·전자제어장비 등 첨단 정보통신기기를 활용하는 경우, 업무자료 등 중요정보 보호 및 안전한 전송을 위한 방안이 마련되어 있는가?	상
	A-19	정보통신망에 비인가 PC · 노트북 등을 연결시 차단하는가?	상
	A-20	정보시스템 및 정보보호시스템 접근기록의 비인가 열람, 훼손 등을 방지하기 위한 대책이 있는가?	상
	A-21	무선랜(Wi-Fi 등)은 국가정보원장의 보안성 검토를 필하거나 암호키 설정 등의 적절한 보안조치를 적용하였는가?	상
	A-22	무선랜 무단 사용 여부, 비인가 무선 중계기(AP) 설치 여부, 우회 정보통신망 사용 차단 여부 등을 주기적으로 점검하는가?	상

운영관리	A-23	개발 테스트 설비는 실제 운영설비와 분리되어 있는가?	상
	A-24	시스템을 도입하기 전에 보안성 검토 및 호환성 검토를 실시하는가?	상
	A-25	시스템 및 사용 장비에 대한 보안 취약점에 대한 주기적 검토 및 보완 프로세스가 있는가?	상
	A-26	바이러스, 악성코드 등에 대한 대비책을 가지고 있는가?	상
	A-27	보안규정의 이행여부를 확인하는 주기적인 보안점검 및 불시 보안점검이 이루어지고 있는가?	상
	A-28	시스템 및 패스워드 관리지침을 제공하고 시스템 및 패스워드 관리책임을 주지시키고 있는가?	상
	A-29	전자기록 보관을 위한 별도의 방법(아카이빙)이 존재하고, 이를 통한 관리를 하고 있는가?	상
	A-30	'사이버보안진단의 날' 등과 같이 월별 보안 중점점검사항에 대해 매월 점검하고 조치하는가?	상
	A-31	비밀(대외비 포함)을 비밀관리기록부에 등재하여 관리하는가?	상
	A-32	출력된 비밀문서의 경우 비밀함등 보관소 등에 안전하게 보관되어 있는가?	상
	A-33	비밀 등 중요 정보의 안전한 처리를 위한 시스템을 도입하여 사용하고 있거나 이를 계획하고 있는가?	상
	A-34	정보통신망 세부 구성현황 등을 대외비 이상으로 관리하는가?	상
	A-35	정보보호시스템은 국내용 CC인증을 받았거나, 보안적합성 검증을 받았는가?	상
업무연속성	A-36	업무복구목표와 요구사항에 적합한 업무연속성 전략을 수립하였는가?	상
사고대응	A-37	침해사고 발생시 신속한 보안사고 보고를 위한 절차가 문서화되어 있고 이에 따라 신속한 보고가 이루어지고 있는가?	상
	A-38	DDoS 대응체계를 수립하고 주기적인 훈련을 실시하고 있는가?	상
	A-39	개인정보보호를 위해 DB암호화등 개인정보유출에 대한 방안이 마련 되어 있는가?	상

□ 물리적 분야

분류	번호	취약점 점검 항목	등급
접근통제	P-1	주요 시스템에 대한 별도의 출입통제를 실시하거나 이중의 보호장치를 설치하고 있는가?	상
	P-2	보호구역의 출입에 관한 정책과 절차가 수립되어 있으며 이에 따라 출입통제가 되고 있는가?	상
감시통제	P-3	주요시설의 출입구와 전산실 및 통신장비실 내부에 CCTV를 설치하고 있는가?	상
	P-4	CCTV 운용 시 중계·관제서버, 관리용 PC, 정보통신망 등에 대해 보안대책을 수립하는가?	상
	P-5	주요시설에 대한 출입기록은 출입일로부터 일정기간 이상 보관하고 있는가?	상
	P-6	외부인에 대해서 출입증을 발급하고, 출입권한은 출입목적이 필요한 구역내로 한정하는가?	상
전력보호	P-7	전원공급 이상이나 기타 전기관련 사고로부터 장비가 보호되고 있는가? (UPS, 비상발전기, 이중전원선 등의 설비)	상

□ 기술적 분야

가. 유닉스

분류	번호	취약점 점검 항목	등급
계정 관리	U-1	root 계정 원격 접속 제한	상
	U-2	패스워드 복잡성 설정	상
	U-3	계정 잠금 임계값 설정	상
	U-4	패스워드 파일 보호	상
파일 및 디렉토리 관리	U-5	root 홈, 패스 디렉터리 권한 및 패스 설정	상
	U-6	파일 및 디렉터리 소유자 설정	상
	U-7	/etc/passwd 파일 소유자 및 권한 설정	상
	U-8	/etc/shadow 파일 소유자 및 권한 설정	상
	U-9	/etc/hosts 파일 소유자 및 권한 설정	상
	U-10	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상
	U-11	/etc/syslog.conf 파일 소유자 및 권한 설정	상
	U-12	/etc/services 파일 소유자 및 권한 설정	상
	U-13	SUID, SGID, Sticky bit 설정 파일 점검	상
	U-14	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상
	U-15	world writable 파일 점검	상
	U-16	/dev에 존재하지 않는 device 파일 점검	상
	U-17	$HOME/.rhosts, hosts.equiv 사용 금지	상
	U-18	접속 IP 및 포트 제한	상
서비스 관리	U-19	Finger 서비스 비활성화	상
	U-20	Anonymous FTP 비활성화	상
	U-21	r 계열 서비스 비활성화	상
	U-22	cron 파일 소유자 및 권한 설정	상
	U-23	DoS 공격에 취약한 서비스 비활성화	상
	U-24	NFS 서비스 비활성화	상
	U-25	NFS 접근통제	상
	U-26	automountd 제거	상
	U-27	RPC 서비스 확인	상
	U-28	NIS, NIS+ 점검	상

	U-29	tftp, talk 서비스 비활성화	상
	U-30	Sendmail 버전 점검	상
	U-31	스팸 메일 릴레이 제한	상
	U-32	일반사용자의 Sendmail 실행 방지	상
	U-33	DNS 보안 버전 패치	상
	U-34	DNS ZoneTransfer 설정	상
	U-35	Apache 디렉토리 리스팅 제거	상
	U-36	Apache 웹 프로세스 권한 제한	상
	U-37	Apache 상위 디렉토리 접근 금지	상
	U-38	Apache 불필요한 파일 제거	상
	U-39	Apache 링크 사용금지	상
	U-40	Apache 파일 업로드 및 다운로드 제한	상
	U-41	Apache 웹 서비스 영역의 분리	상
패치관리	U-42	최신 보안패치 및 벤더 권고사항 적용	상
로그관리	U-43	로그의 정기적 검토 및 보고	상

나. 윈도우즈

점검분류	번호	취약점 점검 항목	등급
계정 관리	W-1	Administrator 계정 이름 바꾸기	상
	W-2	Guest 계정 상태	상
	W-3	불필요한 계정 제거	상
	W-4	계정 잠금 임계값 설정	상
	W-5	해독 가능한 암호화를 사용하여 암호 저장	상
	W-6	관리자 그룹에 최소한의 사용자 포함	상
서비스 관리	W-7	공유 권한 및 사용자 그룹 설정	상
	W-8	하드디스크 기본 공유 제거	상
	W-9	불필요한 서비스 제거	상
	W-10	IIS 서비스 구동 점검	상
	W-11	IIS 디렉토리 리스팅 제거	상
	W-12	IIS CGI 실행 제한	상
	W-13	IIS 상위 디렉토리 접근 금지	상
	W-14	IIS 불필요한 파일 제거	상
	W-15	IIS 웹 프로세스 권한 제한	상
	W-16	IIS 링크 사용금지	상
	W-17	IIS 파일 업로드 및 다운로드 제한	상
	W-18	IIS DB 연결 취약점 점검	상
	W-19	IIS 가상 디렉토리 삭제	상
	W-20	IIS 데이터 파일 ACL 적용	상
	W-21	IIS 미사용 스크립트 매핑 제거	상
	W-22	IIS Exec 명령어 쉘 호출 진단	상
	W-23	IIS WebDAV 비활성화	상
	W-24	NetBIOS 바인딩 서비스 구동 점검	상
	W-25	FTP 서비스 구동 점검	상
	W-26	FTP 디렉토리 접근권한 설정	상
	W-27	Anonymouse FTP 금지	상
	W-28	FTP 접근 제어 설정	상
	W-29	DNS Zone Transfer 설정	상
	W-30	RDS(RemoteDataServices)제거	상
	W-31	최신 서비스팩 적용	상
패치 관리	W-32	최신 HOT FIX 적용	상
	W-33	백신 프로그램 업데이트	상
로그 관리	W-34	로그의 정기적 검토 및 보고	상
	W-35	원격으로 액세스할 수 있는 레지스트리 경로	상
보안 관리	W-36	백신 프로그램 설치	상
	W-37	SAM 파일 접근 통제 설정	상

	W-38	화면보호기 설정	상
	W-39	로그온하지 않고 시스템 종료 허용	상
	W-40	원격 시스템에서 강제로 시스템 종료	상
	W-41	보안 감사를 로그할 수 없는 경우 즉시 시스템 종료	상
	W-42	SAM 계정과 공유의 익명 열거 허용 안 함	상
	W-43	Autologon 기능 제어	상
	W-44	이동식 미디어 포맷 및 꺼내기 허용	상
	W-45	디스크볼륨 암호화 설정	상

다. 보안 장비

점검분류	번호	취약점 점검 항목	등급
계정 관리	S-1	보안장비 Default 계정 변경	상
	S-2	보안장비 Default 패스워드 변경	상
	S-3	보안장비 계정별 권한 설정	상
	S-4	보안장비 계정 관리	상
접근 관리	S-5	보안장비 원격 관리 접근 통제	상
	S-6	보안장비 보안 접속	상
	S-7	Session timeout 설정	상
패치관리	S-8	벤더에서 제공하는 최신 업데이트 적용	상
기능 관리	S-9	정책 관리	상
	S-10	NAT 설정	상
	S-11	DMZ 설정	상
	S-12	최소한의 서비스만 제공	상
	S-13	이상징후 탐지 경고 기능 설정	상
	S-14	장비 사용량 검토	상
	S-15	SNMP 서비스 확인	상
	S-16	SNMP community string 복잡성 설정	상

라. 네트워크 장비

점검분류	번호	취약점 점검 항목	등급

계정 관리	N-1	패스워드 설정	상
	N-2	패스워드 복잡성 설정	상
	N-3	암호화된 패스워드 사용	상
접근 관리	N-4	VTY 접근(ACL) 설정	상
	N-5	Session Timeout 설정	상
패치관리	N-6	최신 보안 패치 및 벤더 권고사항 적용	상
기능 관리	N-7	SNMP 서비스 확인	상
	N-8	SNMP community string 복잡성 설정	상
	N-9	SNMP ACL 설정	상
	N-10	SNMP 커뮤니티 권한 설정	상
	N-11	TFTP 서비스 차단	상
	N-12	Spoofing 방지 필터링 적용	상
	N-13	DDoS 공격 방어 설정	상
	N-14	사용하지 않는 인터페이스의 shutdown 설정	상

마. 제어시스템

점검분류	번호	취약점 점검 항목	등급
계정 관리	C-1	제어시스템 운영, 관리를 위한 계정이 타 사용자와 공유되지 않음	상
	C-2	ID/PW, 접속경로, 인증서 등이 하드코딩되지 않음	상
	C-3	제어시스템 운영, 관리를 위한 계정의 로그인, 사용 기록 저장	상
패치 관리	C-4	제어시스템에 대한 최신 업데이트, 보안패치를 안전하게 적용하기 위한 테스트 등의 절차 수립	상
접근 통제	C-5	제어시스템 운영자의 운영 권한은 제한된 범위 및 명령으로 제한	상
	C-6	제어시스템은 업무망, 인터넷 망과 물리적으로 분리	상
	C-7	제어 네트워크 외부와 자료연계시 물리적 일방향 환경을 구축하여 제어 네트워크로의 침입을 근본적으로 차단	상
	C-8	제어 네트워크에 무선인터넷, 테더링, 외부 유선망 연결 등의 외부망 연결을 제한하고 점검	상
	C-9	제어 네트워크에 비인가된 시스템에 대한 연결 및 접속 차단	상
보안 관리	C-10	제어시스템 구성도, 운용 매뉴얼, 비상조치 절차서 등을 작성하고 최신으로 관리	상
	C-11	제어시스템에서의 USB 사용을 금지하고, 사용시 USB 등의 이동형 저장매체 사용 통제	상

	C-12	제어명령에 대한 위변조 방지 대책 적용	상
	C-13	제어명령 replay 공격에 대한 방지 대책 적용	상
	C-14	제어시스템 개발자, 운영자, 관리자에 대한 접근권한 분리	상
	C-15	제어시스템, 제어기기에 (vendor default) 은닉서비스 및 취약한서비스가 없도록 설정	상
	C-16	제어프로그램의 입력창에 비정상적인 특정값을 입력할 시 사전에 정의한 에러 메시지가 출력되도록 하여 시스템 중요정보가 노출되지 않도록 설정	상

바. PC

점검분류	번호	취약점 점검 항목	등급
계정 관리	PC-1	패스워드의 주기적 변경	상
	PC-2	패스워드 정책이 해당기관의 보안정책에 적합하게 설정	상
서비스 관리	PC-3	공유폴더 제거	상
	PC-4	불필요한 서비스 제거	상
	PC-5	Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 금지	상
패치 관리	PC-6	HOT FIX 등 최신 보안패치 적용	상
	PC-7	최신 서비스팩 적용	상
	PC-8	MS-Office, 호글, 어도브 아크로뱃 등의 응용 프로그램에 대한 최신 보안 패치 및 벤더 권고사항 적용	상
보안 관리	PC-9	바이러스 백신 프로그램 설치 및 주기적 업데이트	상
	PC-10	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화	상
	PC-11	OS에서 제공하는 침입차단 기능 활성화	상
	PC-12	화면보호기 대기 시간을 5~10분으로 설정 및 재시작시 암호로 보호하도록 설정	상
	PC-13	CD, DVD, USB메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안대책 수립	상
	PC-14	PC 내부의 미사용(3개월) ActiveX 제거	상

사. 데이터베이스

점검분류	번호	취약점 점검 항목	등급
계정	D-1	기본 계정의 패스워드, 정책 등을 변경하여 사용	상

관리	D-2	scott 등 Demonstration 및 불필요 계정을 제거하거나 잠금설정 후 사용	상
	D-3	패스워드의 사용기간 및 복잡도를 기관의 정책에 맞도록 설정	상
	D-4	데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 대해서만 허용	상
접근 관리	D-5	원격에서 DB 서버로의 접속 제한	상
	D-6	DBA이외의 인가되지 않은 사용자가 시스템 테이블에 접근할 수 없도록 설정	상
	D-7	오라클 데이터베이스의 경우 리스너의 패스워드를 설정하여 사용	상
옵션 관리	D-8	응용프로그램 또는 DBA 계정의 Role이 Public으로 설정되지 않도록 조정	상
	D-9	OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES를 FALSE로 설정	상
패치 관리	D-10	데이터베이스에 대해 최신 보안패치와 밴더 권고사항을 모두 적용	상
	D-11	데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에 적합하도록 설정	상

아. 웹(Web)

코드	취약점명	설 명	등급
BO	버퍼오버플로우	메모리나 버퍼의 블록 크기보다 더 많은 데이터를 넣음으로써 결함을 발생시키는 취약점	상
FS	포맷스트링	스트링을 처리하는 부분에서 메모리 공간에 접근할 수 있는 문제를 이용하는 취약점	상
LI	LDAP인젝션	LDAP(Lightweight Directory Access Protocol) 쿼리를 주입함으로서 개인정보 등의 내용이 유출될 수 있는 문제를 이용하는 취약점	상
OC	운영체제명령실행	웹사이트의 인터페이스를 통해 웹서버를 운영하는 운영체제 명령을 실행하는 취약점	상
SI	SQL인젝션	SQL문으로 해석될 수 있는 입력을 시도하여 데이터베이스에 접근할 수 있는 취약점	상
SS	SSI인젝션	SSI(Server-side Include)는 "Last modified"와 같이 서버가 HTML 문서에 입력하는 변수 값으로, 웹서버상에 있는 파일을 include 시키고, 명령문이 실행되게 하여 데이터에 접근할 수 있는 취약점	상
XI	XPath인젝션	조작된 XPath(XML Path Language) 쿼리를 보냄으로써 비정상적인 데이터를 쿼리해 올 수 있는 취약점	상
DI	디렉토리인덱싱	요청 파일이 존재하지 않을 때 자동적으로 디렉토리 리스트를 출력하는 취약점	상
IL	정보누출	웹 사이트 데이터가 노출되는 것으로 개발과정의 코멘트나 오류 메시지 등에서 중요한 정보가 노출되어 공격자에게 2차 공격을 하기 위한 중요한 정보를 제공할 수 있는 취약점	상
CS	악성콘텐츠	웹애플리케이션에 정상적인 컨텐츠 대신에 악성 컨텐츠를 주입하여 사용자에게 악의적인 영향을 미치는 취약점	상
XS	크로스사이트스크립팅	웹애플리케이션을 사용해서 다른 최종 사용자의 클라이언트에서 임의의 스크립트가 실행되는 취약점	상
BF	약한문자열강도	사용자의 이름이나 패스워드, 신용카드 정보나 암호화 키 등을 자동으로 대입하여 여러 시행착오 후에 맞는 값이 발견되는 취약점	상

IA	불충분한 인증	민감한 데이터에 접근할 수 있는 곳에 취약한 인증 메커니즘으로 구현된 취약점	상
PR	취약한 패스워드 복구	취약한 패스워드 복구 메커니즘(패스워드 찾기 등)에 대해 공격자가 불법적으로 다른 사용자의 패스워드를 획득, 변경, 복구할 수 있는 취약점	상
CF	크로스사이트 리퀘스트변조(CSRF)	CSRF 공격은 로그온한 사용자 브라우저로 하여금 사용자의 세션 쿠키와 기타 인증 정보를 포함하는 위조된 HTTP 요청을 취약한 웹애플리케이션에 전송하는 취약점	상
SE	세션 예측	단순히 숫자가 증가하는 방법 등의 취약한 특정 세션의 식별자(ID)를 예측하여 세션을 가로챌 수 있는 취약점	상
IN	불충분한 인가	민감한 데이터 또는 기능에 대한 접근권한 제한을 두지 않은 취약점	상
SC	불충분한 세션만료	세션의 만료 기간을 정하지 않거나, 만료일자를 너무 길게 설정하여 공격자가 만료되지 않은 세션 활용이 가능하게 되는 취약점	상
SF	세션고정	세션값을 고정하여 명확한 세션 식별자(ID) 값으로 사용자가 로그인하여 정의된 세션 식별자(ID)가 사용 가능하게 되는 취약점	상
AU	자동화공격	웹애플리케이션에 정해진 프로세스에 자동화된 공격을 수행함으로써 자동으로 수많은 프로세스가 진행되는 취약점	상
PV	프로세스검증누락	공격자가 응용의 계획된 플로우 통제를 우회하는 것을 허가하는 취약점	상
FU	파일업로드	파일을 업로드 할 수 있는 기능을 이용하여 시스템 명령어를 실행할 수 있는 웹 프로그램을 업로드 할 수 있는 취약점	상
FD	파일다운로드	파일 다운로드 스크립트를 이용하여 첨부된 주요 파일을 다운로드 할 수 있는 취약점	상
AE	관리자페이지 노출	단순한 관리자 페이지 이름(admin, manager 등)이나 설정, 프로그램 설계상의 오류로 인해 관리자 메뉴에 직접 접근할 수 있는 취약점	상
PT	경로추적	공격자에게 외부에서 디렉터리에 접근할 수 있는 것이 허가되는 문제점으로 웹 루트 디렉터리에서 외부의 파일까지 접근하고 실행할 수 있는 취약점	상
PL	위치공개	예측 가능한 디렉토리나 파일명을 사용하여 해당 위치가 쉽게 노출되어 공격자가 이를 악용하여 대상에 대한 정보와 민감한 정보가 담긴 데이터에 접근이 가능하게 되는 취약점	상
SN	데이터평문전송	서버와 클라이언트간 통신 시 암호화하여 전송을 하지 않아 중요 정보 등이 평문으로 전송되는 취약점	상
CC	쿠키변조	적절히 보호되지 않은 쿠키를 사용하여 쿠키 인젝션 등과 같은 쿠키 값 변조를 통한 다른 사용자로의 위장 및 권한 상승 등이 가능한 취약점	상

※ 중요도 등급 "중", "하"는 참고자료[취약점 분석·평가 선택점검 항목]를 활용

[붙임3]

취약점 분석·평가 선택 점검항목

□ 관리적 분야

분류	번호	취약점 점검 항목	등급
정보보호정책	A-40	정보보호정책이 문서화되어 있으며 경영자층의 승인을 받고 있는가?	중
	A-41	정보보호정책서가 모든 임직원 및 관련자에게 배포되고 모든 임직원 및 관련자가 정보보호정책을 이해하고 있는가?	중
	A-42	정보보호정책의 내용과 기관의 사업 목표 및 전략 등과의 일관성이 검토되었는가?	하
	A-43	기관의 정보보안 강화를 위한 중장기(3년 이상) 계획이 있는가?	중
정보보호조직	A-44	보안관련 전문가 집단으로부터 조언을 받고 해당 내용을 반영하고 있는가?	중
	A-45	정보보호 관련 주요 의사결정을 수행하는 정보보호위원회가 구성되어 있으며 위원회의 역할 및 책임이 명확히 기술되어 있는가?	하
	A-46	정보보호관리자의 역할 및 책임이 규명되어 있는가?	하
인적보안	A-47	민감한 직무담당자에 대해 강화된 적격심사가 수행되고 있는가?	하
	A-48	모든 인력에 대하여 정보보호의 책임과 역할을 기술하는 직무기술서가 존재하는가?	중
	A-49	정보보안정책을 불이행할 경우 이에 대한 징계가 규정에 명시되어 있는가?	중
	A-50	고용계약 만료시 자산 반납 및 접근권한을 삭제하는 절차가 있는가?	중
외부자보안	A-51	제3자의 보안요구사항 준수 검토를 위해 제3자 관리책임자로부터 보안관리 상황에 대한 주기적인 보고를 받고 수시 점검을 수행하는가?	하
	A-52	외부 관계자에게 정보나 자산에 접근할 수 있는 보안 규정을 사전 통보하고 있는가?	하
	A-53	제3자(외부유지보수직원, 외부용역자포함)에 대한 보안서약서를 가지고 있는가?	하
자산분류	A-54	조직의 주요 자산 목록을 작성하고 변경사항을 유지 관리하고 있는가?	하
	A-55	자산에 대한 등급별 보호절차, 접근제한을 실시하고 있는가?	하
매체관리	A-56	안전을 요하는 매체가 운반될 때 접근 통제가 이루어지고 있는가?	하
	A-57	노트북, USB 메모리 등 이동형 장치의 분실을 통한 자료 유출 대비책이 있는가?	중
	A-58	보조기억매체의 사용을 주기적 점검을 통해 최신자료를 유지하는가?	중
교육및훈련	A-59	정보보호 인식제고를 위한 교육 및 훈련 계획을 종합적으로 수립하여 정기적으로 실시하고 있는가?	중
	A-60	교육 및 훈련은 대상자의 직위 및 업무 특성에 따라 구분하여 실시하고 있는가?	하
	A-61	교육 훈련의 효과가 측정, 분석되어 차기 교육에 반영되는가?	하
	A-62	직원을 대상으로 사이버안전센터 보안권고문·해킹메일주의공지, 윈도우 보안업데이트 사항, 보안취약점 조치요령 등을 공지하는가?	중

접근 통제	A-63	접근통제에 대한 주기적 검토를 통해 접근통제 정책이 적합한지를 확인하고 있는가?	중
	A-64	보안상 중요한 접근통제 규칙은 관리자의 승인을 거쳐서 설정 또는 변경하도록 하고 있는가?	하
	A-65	접근통제 방법은 내부 관련 정책 및 절차에 따라 결정되어 반영되는가?	하
	A-66	안전한 로그온 절차, 식별 및 인증관리 등과 같은 시스템 운영체제 접근통제 방법이 존재하고 이에 따라 이행하고 있는가?	중
	A-67	외부에서의 사용자 접근에 대한 안전한 인증방식을 사용하고 있는가?	하
	A-68	외부에서 내부 시스템의 기능을 사용할 수 있다면 VPN 등 안전한 접속방법을 제공하고 있는가?	하
	A-69	제3자가 원격에서 진단, 관리 등을 위한 서비스를 제공할때 필요할 때만 연결을 허용하고 있는가?	하
	A-70	제3자와의 정보 공유, 네트워크 공유 등에 대한 보안위협에 대한 대책이 있는가?	하
	A-71	민감한 시스템에 따라 네트워크를 분리 운영하여 서로간의 접근을 막고 있는가?	하
	A-72	방화벽, 침입탐지 등 안전한 네트워크를 위한 대책을 마련하고 있는가?	중
	A-73	내부망(업무망)과 인터넷망을 분리하여 사용하는가?	중
	A-74	망분리 후 안전한 자료전송을 위한 시스템을 도입하여 사용하고 있는가?	중
	A-75	인터넷 전화망과 일반 전산망은 분리하여 운용하는가?	하
	A-76	제3자의 내부 상주 인력에 대한 네트워크를 분리 운영하고 있는가?	하
운영 관리	A-77	보안책임자는 정보자산 도입 시 보안 정책에 부합하는지 확인하고 승인하는가?	하
	A-78	보안정책에 의해 정의된 운영지침과 절차는 문서화되어 관리되고 있는가?	중
	A-79	정보시스템의 변경관리 절차가 존재하며 이에 따라 변경관리가 수행되는가?	중
	A-80	중요 시스템 및 정보보호제품의 설정관리가 승인과정을 통해 이행되는가?	중
	A-81	개발자와 운영자의 접근 권한은 분리되어 있는가?	중
	A-82	중요 데이터와 일반데이터가 다른 서버에 분리되어 보관되는가?	하
	A-83	장애탐지, 장애기록, 장애분석, 장애복구, 장애보고 등의 사항을 포함하는 시스템의 장애관리 지침이 존재하는가?	하
	A-84	네트워크 운영 보안 유지를 위해 접근권한 통제, 원격접속 관리, 네트워크 분리 등의 내용을 포함한 네트워크 운영 보안정책이 수립되어 이행되는가?	하
	A-85	시스템과 네트워크의 사용 및 접근에 대한 모니터링 절차와 책임이 정의되어 있고 이에 따라 이행하고 있는가?	하
	A-86	네트워크를 통해 시스템을 운영하는 경우 원칙적으로 시스템 관리는 내부의 특정 터미널에서만 할 수 있도록 제한하고 있는가?	중
	A-87	네트워크, 메신저 등으로부터의 허가되지 않았거나 불분명한 파일의 다운로드를 금지하고, 부득이 다운로드받을 경우 바이러스 검사를 받는가?	중
	A-88	유지보수 도구를 사용하기 위한 사용 승인 및 통제, 감독이 이루어지는가?	하
	A-89	원격 유지보수 및 진단 활동에 대한 감시가 이루어지는가?	하
	A-90	암호키에 대한 관리지침이 마련되어 있고 이에 따라 관리되고 있는가?	중
	A-91	암호키를 복구하기 위한 복구 절차가 수립되고 복구 내역이 확인되는가?	하
	A-92	침입차단 및 탐지 도구는 조직의 보안 정책과 규칙에 적합하게 설치되어 있는가?	하
	A-93	공중망 및 사설망 통신경로에 대한 신뢰성을 평가하고 있는가?	하
	A-94	스팸 메일 수신을 줄이기 위한 방안(스팸차단 솔루션)이 마련되어 있는가?	하
	A-95	홈페이지 게시 자료에 대해 게시 절차를 마련하고 시행하고 있는가?	중
	A-96	업무용 시스템 및 홈페이지 등 정보시스템의 소스코드를 관리하는가?	중

업무 연속성 관리	A-97	모의 훈련 등을 통한 업무 연속성 관리가 지속적으로 검토되고 있으며 조직내의 변경이 있을 경우 이에 대한 사항이 반영되고 있는가?	중
	A-98	보안중요성이 높은 등급의 시스템들은 이중화하여 관리하고 있는가?	중
	A-99	백업은 정기적으로 수행하고 물리적으로 분리된 지역에 보관하는가?	중
사고 대응	A-100	부정접근 사례나 보안사고 내역을 지속적으로 모니터링 하고 있는가?	하
	A-101	보안사고 유형, 범위, 영향 등을 포함한 보안사고 분석이 기록되어 관리 되는가?	중
	A-102	보안 취약점 및 사고 발생시 이에 대한 보완작업 절차를 마련하고 있는가?	중
	A-103	사이버침해사고 발생 후 재발방지 대책을 수립하고 시행하였는가?	중
	A-104	침해사고 대응계획 즉 대응범위, 역할, 임무, 대응절차 등이 문서화되어 있는가?	하
	A-105	사이버위기 '주의'이상 경보 발령 및 피해발생 등 필요시 대응할 수 있는 '긴급대응반'이 구성되어 있는가?	중
	A-106	침해사고시 외부기관 및 전문가들과의 대응협조체계가 구축되어 있는가?	중
	A-107	침해사고 대응절차 및 방법 숙지를 위해 정기적인 교육을 실시하는가?	중
	A-108	서비스 거부 공격에 대해 공격 정도에 따른 대응 방안이 수립되어 있는가?	하
	A-109	내부의 DDoS공격방지(그린DDoSZone)를 위한 대응방안이 있는가?	중
감사	A-110	정보시스템 관련 법, 규제, 계약상의 요구사항을 정의하고 문서화하고 있는가?	하
	A-111	특허권 및 저작권법, 컴퓨터프로그램보호법 등 관련 법규를 준수하고 있는가? (불법 복제 및 해적판 소프트웨어의 사용 금지 등)	하
	A-112	보안사고 처리, 계약증빙 및 소송 등을 위한 적정한 증거자료 확보에 관한 지침이 존재하고, 이에 따라 이행되고 있는가?	하
	A-113	주기적으로 보안감사계획을 수립하고 시행하고 있는가?	하
	A-114	감사결과를 관리책임자에게 보고하여 적정한 사후관리를 시행하고 있는가?	하

□ 물리적 분야

분류	번호	취약점 점검 항목	등급
접근 통제	P-8	민감한 시설에 대해 물리적으로 접근하는 사람들의 출입기록 및 허가의 타당성을 주기적으로 검토하는가?	중
감시 통제	P-9	제한구역에서의 작업에 대한 추가적인 통제 수단 및 안내 지침이 존재하는가?	중
	P-10	전산 장비실에 외부협력업체 출입 시 내부 임직원이 상시 동행하는가?	중
	P-11	시각적으로 구분이 가능한 신분증을 가지고 있으며 패용하고 있는가?	하
	P-12	유리창 내 파손감지기, 진동감지기 등 침입감지와 관련된 장비를 설치하여 감시하고 있는가?	하
전력 보호	P-13	전원공급 이상이나 기타 전기관련 사고로부터 장비를 보호하기 위해 설비 상태에 대해 정기적으로 검토하는가?	하
	P-14	전원선 및 통신선은 도청이나 손상으로부터 보호되고 있는가?	중
	P-15	누전이 발생하였을 때 이를 차단할 수 있도록 누전차단기 또는 누전경보기가 설치되어 있는가?	중
환경 통제	P-16	소방훈련과 같은 재해훈련 시 비상탈출 및 복귀절차가 확립되어 있는가?	하
	P-17	물리적 중요도에 따라 제한구역, 통제구역 등으로 분류하는 다단계 보호대책이 있는가?	중
	P-18	제한구역의 선택, 설계시 화재, 홍수, 폭발, 폭동 혹은 다른 형태의 자연재해 또는 인재로 인한 피해가능성을 고려하였는가?	하
	P-19	데이터센터는 물리적, 환경적 위협이 적은 곳에 위치하고 건물구조가 안정성을 확보하고 있는가?	하
	P-20	주요장비, 대체시스템 및 자료들이 화재, 습도 등의 환경재해로부터 보호되는 적절한 곳에 배치되어 보호되고 있는가?	중
	P-21	전산실에 24시간 항온, 항습을 유지하기 위하여 온습도 측정이 가능하도록 항온항습기가 설치되어 있는가?	하
	P-22	전산실은 천장을 통하여 외부와의 왕래가 불가능하도록 전산실의 벽면과 접한 천장을 차단하는 조치가 되어 있는가?	하
	P-23	방재센터는 화재감지센서의 작동상황이 실시간으로 파악되도록 하고, 화재발생시에 경보신호를 통해 상황을 알 수 있도록 화재감지센서와 연동된 경보장치가 설치되어 있는가?	하
	P-24	주요시설(중앙감시실, 전산실, 전력관련시설, 통신장비실, 방재센터 등)에는 기존 조명설비의 작동이 멈추는 경우에도 작업이 가능하도록 비상조명이 설치되어 있는가?	중
	P-25	배달 및 하역구역은 비인가 지역과 격리되어 보호되고 있는가?	하
	P-26	단위면적당 규정하중을 견딜 수 있도록 설계되어 있는가?	하

□ 기술적 분야

가. 유닉스

분류	번호	취약점 점검 항목	등급
계정 관리	U-44	root 이외의 UID가 '0' 금지	중
	U-45	root 계정 su 제한	하
	U-46	패스워드 최소 길이 설정	중
	U-47	패스워드 최대 사용 기간 설정	중
	U-48	패스워드 최소 사용기간 설정	중
	U-49	불필요한 계정 제거	하
	U-50	관리자 그룹에 최소한의 계정 포함	하
	U-51	계정이 존재하지 않는 GID 금지	하
	U-52	동일한 UID 금지	중
	U-53	사용자 shell 점검	하
	U-54	Session Timeout 설정	하
파일 및 디렉토리 관리	U-55	hosts.lpd 파일 소유자 및 권한 설정	하
	U-56	NIS 서비스 비활성화	중
	U-57	UMASK 설정 관리	중
	U-58	홈디렉토리 소유자 및 권한 설정	중
	U-59	홈디렉토리로 지정한 디렉토리의 존재 관리	중
	U-60	숨겨진 파일 및 디렉토리 검색 및 제거	하
서비스 관리	U-61	ssh 원격접속 허용	중
	U-62	ftp 서비스 확인	하
	U-63	ftp 계정 shell 제한	중
	U-64	Ftpusers 파일 소유자 및 권한 설정	하
	U-65	Ftpusers 파일 설정	중
	U-66	at 파일 소유자 및 권한 설정	중
	U-67	SNMP 서비스 구동 점검	중
	U-68	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중
	U-69	로그온 시 경고 메시지 제공	하
	U-70	NFS 설정 파일 접근 권한	중
	U-71	expn, vrfy 명령어 제한	중
	U-72	Apache 웹서비스 정보 숨김	중
로그 관리	U-73	정책에 따른 시스템 로깅 설정	하

나. 윈도우즈

분류	번호	취약점 점검 항목	등급
계정 관리	W-46	Everyone 사용 권한을 익명 사용자에게 적용	중
	W-47	계정 잠금 기간 설정	중
	W-48	패스워드 복잡성 설정	중
	W-49	패스워드 최소 암호 길이	중
	W-50	패스워드 최대 사용 기간	중
	W-51	패스워드 최소 사용 기간	중
	W-52	마지막 사용자 이름 표시 안함	중
	W-53	로컬 로그온 허용	중
	W-54	익명 SID/이름 변환 허용	중
	W-55	최근 암호 기억	중
	W-56	콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한	중
	W-57	원격터미널 접속 가능한 사용자 그룹 제한	중
서비스 관리	W-58	터미널 서비스 암호화 수준 설정	중
	W-59	IIS 웹서비스 정보 숨김	중
	W-60	SNMP 서비스 구동 점검	중
	W-61	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중
	W-62	SNMP Access control 설정	중
	W-63	DNS 서비스 구동 점검	중
	W-64	HTTP/FTP/SMTP 배너 차단	하
	W-65	Telnet 보안 설정	중
	W-66	불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거	중
	W-67	원격터미널 접속 타임아웃 설정	중
	W-68	예약된 작업에 의심스러운 명령이 등록되어 있는지 점검	중
패치 관리	W-69	정책에 따른 시스템 로깅 설정	중
로그 관리	W-70	이벤트 로그 관리 설정	하
	W-71	원격에서 이벤트 로그 파일 접근 차단	중
보안 관리	W-72	Dos공격 방어 레지스트리 설정	중
	W-73	사용자가 프린터 드라이버를 설치할 수 없게 함	중
	W-74	세션 연결을 중단하기 전에 필요한 유휴시간	중
	W-75	경고 메시지 설정	하
	W-76	사용자별 홈 디렉터리 권한 설정	중
	W-77	LAN Manager 인증 수준	중
	W-78	보안 채널 데이터 디지털 암호화 또는 서명	중
	W-79	파일 및 디렉토리 보호	중
	W-80	컴퓨터 계정 암호 최대 사용 기간	중
	W-81	시작프로그램 목록 분석	중
DB 관리	W-82	Windows 인증 모드 사용	중

다. 보안 장비

분류	번호	취약점 점검 항목	등급
계정 관리	S-17	로그인 실패횟수 제한	중
로그 관리	S-18	보안장비 로그 설정	중
	S-19	보안장비 로그 정기적 검토	중
	S-20	보안장비 로그 보관	중
	S-21	보안장비 정책 백업 설정	중
	S-22	원격 로그 서버 사용	중
	S-23	로그 서버 설정 관리	하
	S-24	NTP 서버 연동	중
기능 관리	S-25	부가 기능 설정	중
	S-26	유해 트래픽 차단 정책 설정	중

라. 네트워크 장비

분류	번호	취약점 점검 항목	등급
계정 관리	N-15	사용자 · 명령어별 권한 수준 설정	중
접근 관리	N-16	VTY 접속 시 안전한 프로토콜 사용	중
	N-17	불필요한 보조 입출력 포트 사용 금지	중
	N-18	로그온 시 경고 메시지 설정	중
로그 관리	N-19	원격 로그서버 사용	하
	N-20	로깅 버퍼 크기 설정	중
	N-21	정책에 따른 로깅 설정	중
	N-22	NTP 서버 연동	중
	N-23	timestamp 로그 설정	하
기능 관리	N-24	TCP keepalive 서비스 설정	중
	N-25	Finger 서비스 차단	중
	N-26	웹 서비스 차단	중
	N-27	TCP/UDP small 서비스 차단	중
	N-28	Bootp 서비스 차단	중
	N-29	CDP 서비스 차단	중
	N-30	Directed-broadcast 차단	중
	N-31	Source 라우팅 차단	중
	N-32	Proxy ARP 차단	중
	N-33	ICMP unreachable, Redirect 차단	중
	N-34	identd 서비스 차단	중
	N-35	Domain lookup 차단	중
	N-36	pad 차단	중
	N-37	mask-rely 차단	중
	N-38	스위치 허브 보안 강화	하

마. 제어시스템

점검분류	번호	취약점 점검 항목	등급
보안 관리	CS-17	정보시스템에 대한 정책과 별도로 제어시스템에 대한 정보보안 정책, 지침이 수립되어 있는가?	중
	CS-18	비인가자 또는 인증과정이 없이 제어시스템, 제어기기에 대한 환경 설정이 가능하지 않도록 되어있는가?	중
	CS-19	제어시스템 및 운영시스템은 제어를 위한 목적으로만 사용되도록 다른 기능 및 서비스를 제거하였는가?	중
	CS-20	운영에 있어 사용가능한 제어명령 및 안전한 제어를 위한 파라미터의 범위를 제한하고 있는가?	중
	CS-21	제어시스템 개선, 신규 시스템 도입, 패치 및 수정 시, 안전성을 테스트하기 위한 테스트베드 또는 시험환경을 구축하였는가?	중
	CS-22	제어 네트워크는 각각의 세부망으로 세분화하고 제어시스템 운영에 필요한 네트워크, 시스템간으로 통신을 제한하고 있는가?	중

바. PC

점검분류	번호	취약점 점검 항목	등급
계정 관리	PC-15	복구 콘솔에서 자동 로그온을 금지하도록 설정하여 사용하고 있는가?	중
서비스 관리	PC-16	파일 시스템이 NTFS 포맷으로 되어 있는가?	중
	PC-17	대상 시스템이 windows 서버를 제외한 다른 OS로 멀티 부팅이 가능하지 않도록 설정하여 사용하는가?	중
	PC-18	브라우저 종료 시 임시 인터넷 파일 폴더의 내용을 삭제하도록 설정하여 사용하는가?	하
보안 관리	PC-19	시스템 부팅 시 Windows Messenger가 자동으로 시작되지 않도록 설정되어 있는가?	중
	PC-20	원격 지원을 금지하도록 정책이 설정되어 사용되는가?	중

사. 데이터베이스

점검분류	번호	취약점 점검 항목	등급
계정 관리	D-12	패스워드 재사용에 대한 제약이 설정되어 있는가?	중
	D-13	DB 사용자 계정을 개별적으로 부여하여 사용하고 있는가?	중
접근 관리	D-14	불필요한 ODBC/OLE-DB 데이터 소스와 드라이브를 제거하고 사용하는가?	중
	D-15	일정 횟수의 로그인 실패 시 이에 대한 잠금정책이 설정되어 있는가?	중
	D-16	데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask를 022 이상으로 설정하여 사용하는가?	하
	D-17	데이터베이스의 주요 설정파일, 패스워드 파일 등과 같은 주요 파일들의 접근 권한이 적절하게 설정되어 있는가?	중
	D-18	관리자 이외의 사용자가 오라클 리스너의 접속을 통해 리스너 로그 및 trace 파일에 대한 변경이 가능하지 않는가?	하
옵션 관리	D-19	패스워드 확인함수가 설정되어 적용되는가?	중
	D-20	인가되지 않은 Object Owner가 존재하지 않는가?	하
	D-21	grant option이 role에 의해 부여되도록 설정되어 있는가?	중
	D-22	데이터베이스의 자원 제한 기능을 TRUE로 설정하고 사용하는가?	하
패치 관리	D-23	보안에 취약하지 않은 버전의 데이터베이스를 사용하고 있는가?	중
로그관리	D-24	Audit Table은 데이터베이스 관리자 계정에 속해 있도록 설정되어 있는가?	하

[붙임4] 취약점 분석·평가 점수 산출식 예시

□ 개요

- o 각 취약점 점검항목에 대한 **취약점 점수 지정 및 진단결과값 산출**
- o 관리적 · 물리적·기술적 **취약점 점수 계산**
  - 단, 기술적 취약점 점수는 각 자산별 점수의 평균으로 계산
- o 관리적 · 물리적·기술적 **취약점 점수를 합산**
- o **망분리** 현황에 따른 **비율 지정**
- o 합산된 관리적 · 물리적·기술적 취약점 점수에 망분리 비율을 적용하여 **종합점수 산출**

□ 취약점 점수 지정 및 진단결과값 산출

- o 각 취약점 점검항목에 대해 중요도에 따라 점수 지정
  - '상'(필수항목): 10점, '중'(추가항목): 8점, '하'(추가항목): 6점
- o 각 취약점 점검항목에 대해 진단결과값 산출

진단결과	평가항목의 중요도		
	상	중	하
○ (취약점 발견)	10점	8점	6점
× (취약점 제거)	0점	0점	0점
P (일부 취약점만 제거)	5점	4점	3점

□ 관리적·물리적 취약점 점수 계산

- o 관리적 · 물리적 취약점 점검항목에 따라 취약점 점수를 각각 계산
- o 점수 계산 방법
  - 모든 취약점이 식별되었을 경우의 점수합: A
  - 식별된 취약점들의 점수합: B
  - 계산식: $\frac{A-B}{A} \times 100$

□ 기술적 취약점 점수 계산

o 기술적 취약점 점검항목에 따라 자산별로 취약점 점수를 계산

- 모든 취약점이 식별되었을 경우의 점수합: A
- 식별된 취약점들의 점수합: B
- 계산식: $\frac{A-B}{A} \times 100$

o 자산별 점수를 합산하여 전체 자산 점수의 평균을 계산

- 자산의 수: N
- 자산별 점수: S1, S2, ..., Sn
- 계산식: $\sum_{n=1}^{N} S_n \div N$

□ 취약점 점수 합산

o 관리적 · 물리적·기술적 취약점 점검항목수의 비율을 고려하여 점수 합산

< 계 산 식 >

·A : (관리적 취약점 점수 X 관리적 취약점 점검항목수)
·B : (물리적 취약점 점수 X 물리적 취약점 점검항목수)
·C : (기술적 취약점 점수 X 기술적 취약점 점검항목수)

$$\Rightarrow \frac{A+B+C}{\text{전체취약점점검항목수}}$$

□ 망분리 비율 지정

o 망분리의 종류에 따라 비율을 지정

구분	설명	적용 비율
물리적 분리	내부 네트워크와 외부 네트워크를 별도로 구축하였으며, 접점이 존재하지 않음	100%
논리적 분리	가상화 기술 등을 이용해 소프트웨어적으로 망 분리 또는 내부 네트워크와 외부 네트워크가 분리되어 있으나 접점이 존재하는 경우	95%
미분리	내부 네트워크와 외부 네트워크가 분리되지 않음	90%

※ 해당시설이 인터넷 연결이 반드시 필요한 경우에는 망 분리 비율을 적용하지 않음

□ 종합점수 산출

o 취약점 점수 합산값에 망분리 비율을 적용하여 최종 계산

- 전체 취약점 점수: A
- 지정된 망분리 비율: B
- 종합점수 계산식: A × B

□ 점수 계산 예제

o 가정사항

- 관리적 취약점 점수 : 80점(점검항목수 10개)
- 물리적 취약점 점수 : 70점(점검항목수 5개)

※ 관리적, 물리적 취약점 점수 계산과정은 18페이지에 기술되어 있으므로 생략하고 기술적 취약점 점수 계산과정을 중심으로 설명

- 대상자산 : 서버 1, 서버 2, 서버 3
- 정의된 취약점과 점수(점검항목 등급을 반영)

번호	취약점명	취약점 등급	점수
#1	시스템 정보 노출	상	10
#2	추측가능한 패스워드 사용	상	10
#3	패스워드가 없는 계정 존재	상	10
#4	Guest 계정 존재	상	10
#5	불필요한 서비스 활성화	상	10
#6	Anonymous FTP 활성화	상	10
#7	쓰기 가능한 Anonymous FTP 활성화	중	8
#8	SMTP expn/vrfy 명령을 통한 시스템 정보 획득 가능	중	8
#9	구 버전의 SNMP 사용	하	6
#10	쓰기 가능한 공유 폴더 존재	중	8
합 계			90

- 자산별로 식별된 취약점

번호	서버 1	서버 2	서버 3
#1	○		
#2	○	○	○
#3			○
#4			○
#5		○	○
#6			○
#7			
#8			
#9	○		
#10			

- 망분리 현황: 논리적 분리

o 점수 계산 절차

- 자산별로 기술적 취약점 식별 후, 점수를 계산(서버 3대 × 10개 점검 항목)

번호	서버 1	서버 2	서버 3	점수
#1	○			10
#2	○	○	○	10
#3			○	10
#4			○	10
#5		○	○	10
#6			○	10
#7				8
#8				8
#9	○			6
#10				8
장비별 점수	71 $\frac{90-26}{90}\times 100$	78 $\frac{90-20}{90}\times 100$	44 $\frac{90-60}{90}\times 100$	
	※ 모든 취약점 점수의 합 : 90점			

- 기술적 취약점 점수 : (71 + 78 + 44) / 3 = 64점
  (3개 자산의 점수를 합산하여 평균을 계산)

- 관리적 · 물리적·기술적 취약점 점수 합산 : (80점X10개) + (70점X5개) + (64점X10개) / (10개+5개+10개) = 71점

< 계 산 식 >

·A : (관리적 취약점 점수 X 관리적 취약점 점검항목수)
·B : (물리적 취약점 점수 X 물리적 취약점 점검항목수)
·C : (기술적 취약점 점수 X 기술적 취약점 점검항목수)

$$\Rightarrow \frac{A+B+C}{\text{전체취약점점검항목수}}$$

- 망분리 비율: 95%

(논리적 분리이므로 95%를 부여)

- 종합점수 계산: 71점 × 95% = 67점

(망분리 비율을 곱셈하여 종합점수를 계산)

미래창조과학부 소관 주요정보통신기반시설 보호지침

[시행 2013.10.29] [훈령 제82호, 2013.10.29, 일부개정]

제1장 총칙

제1조(목적) 이 지침은 「정보통신기반 보호법」(이하 "법"이라 한다) 제10조에 따라 미래창조과학부장관(이하 "장관"이라 한다)이 관할하는 주요정보통신기반시설을 각종 전자적 침해행위로부터 보호하기 위하여 해당 주요정보통신기반시설 관리기관의 장(이하 "관리기관의 장"이라 한다)이 준수하여야 할 정보보호에 관한 구체적 사항을 정함을 목적으로 한다.

제2조(적용범위) 이 지침은 법 제8조에 따라 장관이 관할하는 주요정보통신기반시설 관리기관의 장 및 해당 시설을 관리·운용하는 업무종사자에게 적용한다.

제3조(보호대책의 수립) ① 관리기관의 장은 법 제5조제1항에 따라 수립한 소관 주요정보통신기반시설 보호대책(이하 "보호대책"이라 한다)을 매년 8월말까지 장관에게 제출하여야 한다.

② 보호대책에는 다음 각 호의 사항이 포함되어야 한다.

1. 소관 주요정보통신기반시설 보호의 목적 및 대상시설
2. 정보보호체계 및 관리 대책
3. 취약점 분석·평가 및 점검 대책
4. 침해사고 예방 대책
5. 침해사고 대응 및 복구 대책
6. 그 밖에 소관 주요정보통신기반시설의 보호를 위하여 필요한 사항

③ 관리기관의 장은 법 제9조에 따라 실시한 취약점 분석·평가의 결과를 반영하여 보호대책을 수립하여야 한다. 다만, 관리기관의 장은 제14조제1항에 따른 자체 점검을 실시한 경우에는 그 실시한 결과를 함께 반영할 수 있다.

제4조(보호대책 이행점검) ① 장관은 소관 보호대책에 대한 이행점검을 실시하거나, 관리기관의 장에게 보호대책의 이행점검을 실시하도록 할 수 있다.

② 관리기관의 장은 제1항에 따라 보호대책 이행점검을 실시한 때에는 그 이행점검 결과를 장관에게 제출하여야 한다.

제2장 정보보호체계 및 관리

제5조(정보보호책임관 등) ① 법 제6조제5항에 따른 미래창조과학부 정보보호책임관은 미래창조과학부 정보화전략국의 정보보호에 관한 사무를 담당하는 과장으로 한다.

② 정보보호책임관은 장관이 관할하는 소관분야의 모든 주요정보통신기반시설의 보호에 관한 업무를 총괄한다.

③ 정보보호책임관은 다음 각 호의 업무를 수행한다.

1. 주요정보통신기반시설의 지정 및 지정취소에 관한 업무
2. 주요정보통신기반시설 보호계획의 수립에 관한 업무
3. 주요정보통신기반시설 보호지침의 작성·수정 및 보완에 관한 업무
4. 정보보호 조직·체계의 구축·운영에 관한 업무
5. 취약점 분석·평가 및 침해사고 예방·지원 업무
6. 소요 예산 및 시설·장비 등 자산의 확보에 관한 업무
7. 그 밖에 소관분야 주요정보통신기반시설의 보호를 위하여 장관이 지시하는 사항

제6조(정보보호추진체계) ① 정보보호책임관은 제5조제2항에 따른 정보보호업무의 총괄 수행을 위해 「정보통신기반 보호법 시행령」(이하 "영"이라 한다) 제15조제2항에 따른 협의회를 구성·운영할 수 있다.

② 제1항에 따른 협의회의 장은 미래창조과학부 소속 공무원으로 하고, 간사는 제5조에 따른 정보보호책임관으로 하며, 한국인터넷진흥원의 팀장급 담당자, 관계 전문가 등을 위원으로 구성한다.

③ 제1항에 따른 협의회는 다음 각 호의 업무를 수행한다.

1. 주요정보통신기반시설의 지정 심의·조정
2. 법 제5조제2항에 따라 제출받은 보호대책 분석, 이행점검 및 필요한 조치사항 권고
3. 제5조제3항 각 호의 업무 수행 지원

④ 장관은 원활한 업무 수행을 위하여 필요한 경우에는 영 제12조제1호에 따른 한국인터넷진흥원장에게 제3항의 업무 중 일부를 위임할 수 있으며, 필요한 행정적·기술적 지원을 요청할 수 있다.

⑤ 한국인터넷진흥원장은 제4항에 따라 위임받은 업무를 수행하기 위하여 필요한 경우에는 실무조정반을 구성·운영할 수 있다.

제7조(정보보호책임자) ① 법 제5조제4항에 따라 관리기관의 장의 지정을 받은 정보보호책임자는 관리기관의 장이 관할하는 주요정보통신기반시설의 보호에 관한 업무를 총괄한다.

② 정보보호책임자는 다음 각 호의 업무를 수행한다.

1. 소관 주요정보통신기반시설 보호대책의 수립에 관한 업무

2. 소관 주요정보통신기반시설의 설치 및 관리·운영에 대한 보호측면의 지도·감독에 관한 업무
3. 취약점 분석·평가 및 침해사고 예방에 관한 업무
4. 침해사고 대응 및 복구에 관한 업무
5. 소요 예산 및 시설·장비 등 자산의 확보에 관한 업무
6. 그 밖에 소관 주요정보통신기반시설의 보호를 위하여 관리기관의 장이 지시하는 업무

③ 관리기관의 장은 정보보호책임자를 지정한 때에는 그 사실을 장관에게 통지하여야 한다.

④ 정보보호책임자는 소관 주요정보통신기반시설과 다른 주요정보통신기반시설의 보호를 위하여 정보보호책임관과 긴밀히 협조하여야 한다.

제8조(전담 조직의 구성) ① 관리기관의 장은 정보보호에 관한 다음 각 호의 업무를 수행하기 위하여 필요하다고 인정하는 때에는 정보보호책임자 소속 하에 별도의 전담 조직을 구성·운영할 수 있다.

1. 제14조에 따른 점검
2. 제19조 및 제20조에 따른 침해사고의 대응 및 복구

② 관리기관의 장은 관리기관에 소속되지 아니한 자로서 정보보호에 관한 전문지식이 있는 인력을 전담 조직에 참여하게 할 수 있다.

③ 관리기관의 장은 제1항에 따른 전담 조직의 구성 및 운영에 필요한 사항을 정하여야 한다.

제9조(업무종사자의 준수사항) ① 관리기관의 장은 소관 주요정보통신기반시설을 관리·운용하는 업무종사자(계약직을 포함한다)로 하여금 다음 각 호의 사항을 준수하도록 하여야 한다.

1. 주요정보통신기반시설의 보호책임에 관한 사항
2. 비밀유지 및 비밀서약에 관한 사항
3. 주요정보통신기반시설 보호관련 법령 및 지침 등의 준수에 관한 사항
4. 보호관련 지침 및 보호조치 위반에 따른 징계에 관한 사항

② 관리기관의 장은 해당 시설을 관리·운용하는 업무종사자가 보직이 변경되거나 퇴사하는 경우 법 제27조에 따라 소관 주요정보통신기반시설의 관리·운용에 관하여 취득한 비밀을 외부에 유출하지 않도록 주지시켜야 한다. 이 경우 관리기관의 장은 보직이 변경되거나 퇴사하는 자에 대하여 비밀유지에 관한 서약서를 작성하도록 요구할 수 있다.

제10조(보호업무등의 위탁) 관리기관의 장은 소관 주요정보통신기반시설의 관리·운용 또는 제14조에 따른 점검 등 보호에 관한 업무 일부와 법 제9조제3항에 따른 취약점 분석·평가 업무를 다음 각 호의 기관 또는 업체에 위탁하는 때에는 해당 기관 또는 업체의 위탁업무 수행에 참여하는 종사자에게 법 제27조에 따른 비밀유지의무를 준수하도록 비밀유지 서약서의 작성 요구, 업무관련 기록·자료의 안전한 보존 및 폐기 등 필요한 조치를 하여야 한다.

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원
2. 법 제16조에 따른 정보공유·분석센터

3. 「정보통신산업 진흥법」 제33조에 따라 지정된 지식정보보안 컨설팅전문업체
4. 「정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조에 따른 한국전자통신연구원
5. 그 밖에 주요정보통신기반시설의 관리·운영 또는 보호 관련 업무(취약점 분석·평가에 관한 업무를 제외한다)를 영위하는 기관 또는 업체

제11조(유관기관과의 협조) 관리기관의 장은 소관 주요정보통신기반시설의 보호를 위하여 미래창조과학부, 한국인터넷진흥원 또는 다른 관리기관과 다음 각 호의 사항에 관하여 상호 협조할 수 있다.

1. 주요정보통신기반시설의 보호와 관련된 정보의 공유
2. 침해사고 예방·대응 및 복구를 위한 상호협력 및 지원
3. 그 밖에 소관 주요정보통신기반시설의 보호를 위하여 상호협력이 필요한 사항

제12조(정보보호 교육·훈련의 실시) ① 관리기관의 장은 소관 주요정보통신기반시설을 관리·운용하는 업무종사자를 대상으로 해당 시설의 보호를 위하여 필요한 교육·훈련을 매년 1회 이상 실시하여야 한다. 다만, 소관 주요정보통신기반시설의 보호를 위한 중요한 절차 및 방법 등의 변경이 있거나 신규로 직원을 채용한 때에는 지체 없이 필요한 교육·훈련을 실시하여야 한다.

② 관리기관의 장은 제1항에 따른 훈련을 실시하는 때에는 외부의 정보보호관련 전문기관에 이를 위탁하여 실시할 수 있다.

③ 관리기관의 장은 제1항에 따른 교육·훈련을 실시하기 위하여 다음 각 호의 사항을 정하여야 한다.

1. 교육·훈련의 내용 및 방법
2. 교육·훈련에 관한 기록유지 및 인사관리에 관한 사항
3. 그 밖에 교육·훈련을 위하여 필요한 사항

제3장 취약점 분석·평가 및 침해사고 예방

제13조(취약점 분석·평가) ① 관리기관의 장은 법 제9조에 따라 소관 주요정보통신기반시설에 대한 최초 취약점 분석·평가를 실시한 때에는 1년을 주기로 실시하여야 한다.

② 관리기관의 장은 제1항에도 불구하고 소관 정보통신기반시설이 주요정보통신기반시설로 새로이 지정된 경우에는 6개월 이내에 취약점 분석·평가를 실시하여야 한다. 다만, 관리기관의 장은 취약점 분석·평가를 지정 후 6개월 이내에 시행하지 못할 특별한 사유가 있는 경우에는 장관의 승인을 받아 지정 후 9개월 이내에 실시하여야 한다.

③ 관리기관의 장은 법 제9조제4항에 따른 취약점 분석·평가에 관한 기준을 고려하여 취약점 분석·평가의 대상, 기간, 절차, 방법, 소요예산 편성 및 집행 등 취약점 분석·평가를 구체적으로 시행하기 위하여 필요한 계획을 수립·시행하여야 한다.

④ 관리기관의 장은 법 제9조제2항에 따른 전담반을 구성하는 때에는 정보보호책임자를 반장으로 하고, 취약점 분석·평가의 실효성 및 객관성을 확보할 수 있도록 주요정보통신기반시설 관리·운용 업무종사자와 정보보호에 관한 전문성을 가진 자로 구성하여야 한다. 이 경우 관리기관의 장은 소관 주요정보통신기반시설의 특성 및 취약점 분석·평가 기준을 고려하여 필요한 전문인력을 미리 확보하여야 한다.

⑤ 관리기관의 장은 법 제9조제3항에 따라 취약점 분석·평가를 외부에 위탁하여 실시하는 때에는 소속 전담반이 함께 참여하도록 할 수 있다.

제14조(자체점검 및 수시점검) ① 관리기관의 장은 영 제17조에 따라 취약점 분석·평가가 필요하다고 판단되는 경우에는 1년이 되지 아니한 때에도 소관 주요정보통신기반시설에 대한 자체 점검을 실시할 수 있다.

② 관리기관의 장은 제1항에 따른 자체 점검을 실시하는 때에는 다음 각 호의 사항을 고려하여 실시하여야 한다.

1. 법 제9조에 따른 취약점 분석·평가의 기준, 절차 및 방법
2. 이전에 실시한 취약점 분석·평가의 결과
3. 점검 기간 및 소요예산

③ 관리기관의 장은 다음 각 호의 어느 하나에 해당하는 경우에는 수시로 점검(이하 "수시점검"이라 한다)을 실시할 수 있다.

1. 침해사고의 징후가 있는 경우
2. 시설·장비의 교체 및 보수를 한 경우
3. 침해사고에 따른 복구조치를 한 경우
4. 소관 주요정보통신기반시설의 보호에 관한 절차·방법 및 담당 인력의 변경이 있는 경우

④ 관리기관의 장은 제1항부터 제3항까지의 규정에 따른 점검을 실시한 때에는 점검 기간, 대상, 방법 및 결과 등 점검에 관한 제반사항을 기록·관리하여야 한다.

제15조(보완조치) ① 관리기관의 장은 제13조에 따른 취약점 분석·평가 및 제14조에 따른 점검을 실시한 결과를 반영하여 다음 각 호의 조치(이하 "보완조치"라 한다)를 하여야 한다.

1. 이 지침에 따라 수립된 각종 보호조치, 절차 및 방법 등의 재검토 및 수정·보완
2. 시설·장비의 개축·보수 또는 설치
3. 그 밖에 분석·평가 또는 점검 결과를 반영한 보완 조치

② 관리기관의 장은 보완조치를 하는 때에는 정보화관련 예산 또는 기본사업비 예산을 활용하여 보완조치에 필요한 경비를 우선 집행하여야 한다.

③ 관리기관의 장은 보완조치가 미흡하거나 추가적으로 보완조치가 필요한 때에는 해당 보완조치에 소요되는 비용을 다음 연도 예산에 반영하여야 한다.

제16조(침해사고 예방조치) ① 관리기관의 장은 소관 주요정보통신기반시설을 보호하기 위하여 다음 각 호의 사항을 포함하는 예방조치를 하여야 한다.

1. 관리·운영절차의 수립
2. 제한구역의 설정
3. 장비·시설의 설치·유지 및 보수
4. 기타 소관 주요정보통신기반시설의 보호에 필요한 사항

② 관리기관의 장은 소관 주요정보통신기반시설을 보호하기 위하여 정보보호시스템 및 정보보호용 컴퓨터프로그램의 설치·운용에 관하여 필요한 조치를 하여야 한다.

③ 관리기관의 장은 컴퓨터바이러스의 유입으로 인한 소관 주요정보통신기반시설의 피해를 방지하기 위하여 컴퓨터바이러스 백신프로그램의 배포·갱신 등 필요한 조치를 하여야 한다.

④ 관리기관의 장은 안전한 정보유통을 위하여「전자서명법」에 의한 전자서명 인증서를 이용할 수 있도록 관련 시스템의 구축 등 필요한 조치를 하고 소관 주요정보통신기반시설 관리·운용 업무종사자로 하여금 전자서명 인증서를 이용하도록 하여야 한다. 이 경우 관리기관의 장은 소관 주요정보통신기반시설을 이용하여 정보를 유통하는 자가 있는 경우에는 해당 이용자에게 전자서명 인증서의 이용을 권고하여야 한다.

⑤ 관리기관의 장은 소관 주요정보통신기반시설에 대한 권한 없는 자의 부당한 접근 및 이용을 방지하기 위하여 필요한 조치를 하여야 한다.

⑥ 관리기관의 장은 제1항부터 제5항까지의 규정에 따른 조치를 하는 때에는 별표 1에서 정하는 사항을 고려하여야 한다.

제17조(외부 정보통신망 연결에 따른 보호조치) 관리기관의 장은 소관 주요정보통신기반시설을 다른 기관 또는 업체와 정보통신망으로 연결하는 경우에는 해당 업체 또는 기관이 관리기관의 다음 각 호에 해당하는 조치, 절차 및 방법을 준수·협조하도록 필요한 약정을 체결하여야 한다.

1. 제16조에 따른 침해사고 예방을 위한 조치, 절차 및 방법
2. 제18조부터 제20조까지의 규정에 따른 침해사고 대응 및 복구를 위한 조치, 절차 및 방법

제4장 침해사고 대응 및 복구

제18조(연락체계의 구축) ① 관리기관의 장은 소관 주요정보통신기반시설에 대한 전자적 침해사고가 발생한 경우 신속히 대응하고 관계기관에 알리기 위하여 필요한 연락체계를 구축하여야 한다.

② 관리기관의 장은 제1항에 따른 연락체계에 있어 미래창조과학부와 한국인터넷진흥원이 포함되도록 하여야 한다.

제19조(침해사고 대응조치) ① 관리기관의 임직원과 제10조에 따른 위탁기관·업체의 위탁업무 수행에 참여하는 종사자는 전자적 침해사고의 징후가 있거나 전자적 침해사고의 발생을 인지한 때에는 이를 즉시 정보보호책임자에게 보고하여야 한다.

② 정보보호책임자는 소관 주요정보통신기반시설에 대한 중대한 전자적 침해사고의 발생·징후를 보고 받거나 인지한 때에는 이를 미래창조과학부에 즉시 보고하고 필요한 응급조치를 하여야 한다. 다만, 관리기관의 장은 소관 주요정보통신기반시설의 교란, 마비 또는 파괴가 일어나지 아니하는 등 경미한 침해사고의 발생·징후는 보고하지 아니할 수 있다.

③ 관리기관의 장은 제1항 및 제2항에 따른 사항을 포함하여 전자적 침해사고 발생에 따른 대응절차 및 방법에 관하여 필요한 사항을 정하여야 한다. 이 경우 별표 2에서 정하는 사항을 고려하여야 한다.

④ 관리기관의 장은 미래창조과학부가 권고하는 침해사고 대응요령에 따라 피해사실의 보고 및 긴급대응조치 등을 하여야 한다.

제20조(복구조치) ① 관리기관의 장은 전자적 침해사고로 인하여 소관 주요정보통신기반시설이 파괴되거나 기능이 제대로 수행되지 아니하는 때에는 해당 시설이 정상적으로 가동될 수 있도록 필요한 복구조치를 신속히 취하여야 한다. 이 경우 관리기관의 장은 미래창조과학부 또는 법 제13조에 따른 관계 행정기관, 수사기관 또는 한국인터넷진흥원에 복구에 필요한 지원을 요청할 수 있다.

② 관리기관의 장은 제1항의 복구조치를 위하여 필요한 조직, 자원, 외부기관과의 협력 등을 포함하는 복구지원체계를 구축하여야 한다.

③ 관리기관의 장은 제1항 및 제2항의 내용을 포함하여 전자적 침해사고가 발생한 시설에 대한 복구절차 및 방법에 관하여 필요한 사항을 정하여야 한다. 이 경우 별표 2에서 정하는 사항을 고려하여야 한다.

제21조(대응·복구 훈련의 실시) ① 관리기관의 장은 소속 임직원과 제10조에 따른 기관 또는 업체의 위탁업무 수행에 참여하는 종사자에게 제19조제3항 및 제20조제3항에 따른 침해사고 대응·복구에 관한 절차 및 방법을 정확히 숙지할 수 있도록 필요한 훈련(이하 "대응·복구 훈련"이라 한다)을 정기적으로 실시하여야 한다. 이 경우 관리기관의 장은 필요하다고 인정하는 때에는 다른 관리기관과 공동으로 훈련을 실시할 수 있다.

② 관리기관의 장은 대응·복구 훈련을 실시한 결과 필요하다고 인정하는 때에는 해당되는 대응·복구 절차 및 방법을 수정·보완하여야 한다.

제22조(해킹·바이러스 예방의 날) ① 관리기관의 장은 매월 15일을 해킹·바이러스 예방의 날로 운영한다.

② 관리기관의 장은 해킹·바이러스 예방의 날에 다음 각 호에 해당하는 업무를 수행한다.

1. 제12조 및 제21조에 따른 교육·훈련의 실시
2. 컴퓨터 바이러스 점검 등 필요한 점검의 실시

제5장 보칙

제23조(재검토기한) 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 훈령 발령 후 법령이나 현실여건의 변화 등을 검토하여 이 훈령의 폐지, 개정 등 조치를 하여야 하는 기한은 2016년 10월 28일까지로 한다.

부칙 <제19호,2008.6.24>

이 지침은 발령한 날부터 시행한다.

부칙 <제61호,2009.11.2>

이 훈령은 2009년 11월 2일부터 시행한다.

부칙 <제130호,2012.10.17>

이 훈령은 2012년 11월 1일부터 시행한다.

부칙 <제82호,2013.10.29>

이 훈령은 2013년 10월 29일부터 시행한다.

<별표 1>

침해사고 예방조치시 고려사항(제16조 관련)

가. 관리·운영 측면의 고려사항

구 분	주요 고려 사항
관리·운영절차	o 관리·운영절차의 수립시 고려사항 - 시스템 문제발생시 재동작 및 복구 절차 - 시스템 모니터링 방안 - 중요 산출물에 대한 관리 방안 - 업무수행시 발생될 예외사항 및 오류사항 처리 방안 - 정보처리 및 취급 절차
제한구역 설정 및 보호	o 제한구역 설정시 고려 사항 - 보호대상 설정 - 특히 중요한 시설이나 장비는 제한구역으로 설정 - 출입 통제 방안 - 반출·입 물품에 대한 기록 유지 - 정전대비 별도의 전원 공급 시설
장비·시설의 도입 및 설치	o 시스템 구입 및 설치시 일반적 고려 사항 - 현재 시스템의 성능과 가용능력의 한계에 대한 분석 - 시스템의 기능적, 운영적 요구사항 정의 및 시기의 예측 - 기존 시스템과의 적합성 확보 - 정보보호 시스템의 설치시는 보호치침과의 부합성 및 설치 필요성에 대하여 검증 - 정기적인 점검 및 안전성에 대한 재검토 o 정보보호시스템 도입 및 설치·운영시 고려 사항 - 요구사항 파악 - 도입·설치의 목적 - 성능 및 도입·설치의 타당성에 대한 검토 - 관리의 편이성 - 로그관리의 편이성 - 정보보호시스템에 대한 로그 감시 기능

구 분	주요 고려 사항
변경관리 절차	o 장비, 소프트웨어, 절차들의 변경사항에 대한 관리 책임 및 절차 수립시 고려사항 - 주요 변경사항 및 변경대상에 관한 정의·기록 유지 - 변경 실패에 따른 복구나 폐기에 대한 책임 정의 절차 - 변경에 대한 잠정적인 영향 평가 - 요구된 변경사항에 대한 승인절차 - 모든 관련자에게 변경사항에 대한 공지 및 교육
로그 관리	o 운영자 로그관리방안 수립시 고려사항 - 시스템 시작, 종료시간, 사용자 인증실패, 접속시도, 시스템 에러 및 수정 내용 등에 대한 로그 유지 - 로그 기록 방법, 대상, 보존 기간, 백업 등 - 주기적 로그 점검 및 방법 - 접근기록에 대한 정기적 분석 및 불법시도에 대한 조치 방법 - 보안 로그 기록 점검사항에 대한 주기적 보고 o 정보보호시스템의 로그 기록시 필수 고려사항 - 성공적이거나 거부된 접속 - 정보보호시스템 구성요소로부터의 에러 메시지 - 다중 접근 시도 - 불안한 포트로의 접근 - 로그를 저장할 메모리 - 기록이 멈추게 되지 않도록 사전 대책 강구
장애 관리	o 장애관리시 고려사항 - 장애의 감지 및 복구를 위해 운영상황 감시 기능 설정 - 장애관리 보고 절차 수립 - 장애시 전체시스템에 대한 피해 최소화를 위해 장애차단 기능 설정 - 장애 복구 기능 설정 - 장애처리후 로그에 대한 재점검으로 장애의 완전 복구상태 확인

구 분	주요 고려 사항
저장매체 관리	o 테이프, 디스켓, 출력보고서 등의 저장매체 관리시 고려 사항 - 저장매체에 대한 목록관리, 분류, 접근통제, 보관장소, 보관기간, 보관절차 등 수립 - 저장매체에 대한 복사, 변경, 배포, 폐기 방안 - 저장매체 정보저장, 취급 및 전달 절차 수립 - 저장매체 사용에 대한 허가, 점검 수립 및 기록유지 - 저장매체 저장 내용 삭제·폐기 절차
악의적 소프트웨어 관리	o 컴퓨터바이러스 등 악의적 소프트웨어로부터의 보호를 위한 통제·탐지 조치시 고려 사항 - 사용자에게 바이러스의 위험성에 대한 인식 필요 - 비인가 및 불법 소프트웨어 사용금지 - 알려진 바이러스 백신프로그램 사용 - 지속적인 바이러스 백신프로그램 업데이트 및 검사 - 검증되지 않은 저장매체는 사용전에 검사 - 외부 네트워크나 매체로부터 파일 또는 소프트웨어 다운로드시 대책 마련
백 업	o 시스템, 데이터, DB 등 정보자산에 대한 백업조치시 고려 사항 - 정보자산에 대한 장애 대비 백업 및 복구 절차 규정 - 데이터의 중요도에 따른 백업 대상, 백업 방식, 백업주기, 백업 기준 등을 설정 - 자연재해로부터 보호받을 수 있는 안전한 장소에 대한 지정 - 주기적으로 백업 받은 데이터에 대한 복구 테스트 실시 - 중요정보에 대하여는 제3의 장소 등 물리적으로 분리된 곳에 백업데이터 보관

나. 기술적 측면에서의 고려사항

구 분	주요 고려 사항
사용자 관리	o 사용자 계정 관리시 고려 사항 - 시스템 접근에 대한 공식적인 사용자 등록 및 해지 절차 수립 - 주기적으로 인가된 사용자 여부 및 접근권한 점검 - 사용자의 공식적인 로그를 보관 - 동일사용자 계정의 다른 사용자 계정 재발급 방지 - 시스템 관리자가 일반 업무시 일반 사용자 계정 사용
패스워드 관리	o 패스워드 관리시 고려사항 - 책임추적성을 위해 패스워드 할당 - 패스워드의 안전한 보관 - 패스워드의 노출가능성이 있으면 즉시 변경 - 패스워드 설정시 기피해야 할 요건 . 특정 달, 요일, 머리 글자, 주민등록번호, 자동차번호 . 회사이름, 전화번호 또는 비슷한 숫자 그룹 . 2개 이상의 연관된 신원확인 가능 문자, 숫자, 영문 알파벳 그룹 - 주기적으로 패스워드를 변경, 지난 패스워드 사용금지 - 특별권한이 부여된 ID의 패스워드는 정기적으로 점검 - 첫 로그온시 임시 패스워드는 변경 - 비밀번호 오류 횟수의 제한
네트워크 접근 통제	o 네트워크 접근 통제시 고려 사항 - 네트워크로 접근하는 사용자에 대한 인가 절차 - 원격접속 사용자 인가 절차 - 비인가된 접근을 막기 위해 서비스 경로의 제한 및 분리 - 관계회사 등과 네트워크 공유시에는 물리적 또는 논리적으로 분리 - 원격 장비의 관리를 위한 책임 및 절차를 수립 - 개발업무 네트워크와 다른 업무용 네트워크와의 분리 운영 - 인증, 암호 활용을 통한 원격 접속 사용자에 대한 접근통제 - 네트워크를 통해 시스템 운영시 시스템 관리는 원칙적으로 내부 특정 단말로 제한

<별표 2>

침해사고 대응 및 복구 조치시 고려사항(제19조 및 제21조 관련)

구 분	주요 고려 사항
침해사고 대응·복구 절차 및 방법	o 침해사고에 대한 복구 절차 및 방법 수립시 고려 사항 - 침해사고의 정의 및 범위 - 긴급연락체계 구축 - 침해사고 발생시 대응 요령 및 절차 - 침해사고 복구조직 구성 - 침해사고 복구 장비 및 자원 조달 - 침해사고 대응 및 복구 훈련 실시 사항
침해사고 보고	o 침해사고 보고시 고려 사항 - 침해 날짜와 시간 - 침해 사고 보고자 및 보고 일시 - 침해 사고 내용 - 침해 사고 대응 내역
침해사고 발생시 응급 조치	o 침해사고 발생후 응급 조치시 고려사항 - 손상된 시스템은 동작을 즉시 정지 - 내부망의 외부 접속을 즉시 차단 - 긴급복구가 즉시 수행되어야 하는 곳은 정보보호전문가에 의한 침입탐지 및 복구
침해사고 복구	o 침해사고 복구시 고려사항 - 사고원인의 분석 및 정의 - 필요한 경우, 재발을 방지하기 위한 대책의 수립 및 시행 - 정보자원 및 시스템 백업을 통한 시스템 재구축 방법 - 시스템 및 정보통신망에 대한 취약점 제거

정보통신기반 보호법

[시행 2015.12.23] [법률 제13343호, 2015.6.22, 타법개정]

제1장 총칙

제1조(목적) 이 법은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다.

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2007.12.21>

1. "정보통신기반시설"이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 규정에 의한 정보통신망을 말한다.
2. "전자적 침해행위"라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말한다.
3. "침해사고"란 전자적 침해행위로 인하여 발생한 사태를 말한다.

제2장 주요정보통신기반시설의 보호체계

제3조(정보통신기반보호위원회) ①제8조의 규정에 의하여 지정된 주요정보통신기반시설(이하 "주요정보통신기반시설"이라 한다)의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회(이하 "위원회"라 한다)를 둔다.

②위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.

③위원회의 위원장은 국무조정실장이 되고, 위원회의 위원은 대통령령이 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 자로 한다.<개정 2007.12.21, 2008.2.29, 2013.3.23>

④위원회의 효율적인 운영을 위하여 위원회에 공공분야와 민간분야를 각각 담당하는 실무위원회를 둔다.<개정 2007.12.21>

⑤위원회 및 실무위원회의 구성·운영 등에 관하여 필요한 사항은 대통령령으로 정한다.

제4조(위원회의 기능) 위원회는 다음 각호의 사항을 심의한다. <개정 2007.12.21>

1. 주요정보통신기반시설 보호정책의 조정에 관한 사항

2. 제6조제1항에 따른 주요정보통신기반시설에 관한 보호계획의 종합·조정에 관한 사항
3. 제6조제1항에 따른 주요정보통신기반시설에 관한 보호계획의 추진 실적에 관한 사항
4. 주요정보통신기반시설 보호와 관련된 제도의 개선에 관한 사항
5. 그 밖에 주요정보통신기반시설 보호와 관련된 주요 정책사항으로서 위원장이 부의하는 사항

제5조(주요정보통신기반시설보호대책의 수립 등) ①주요정보통신기반시설을 관리하는 기관(이하 "관리기관"이라 한다)의 장은 제9조제1항의 규정에 의한 취약점 분석·평가의 결과에 따라 소관 주요정보통신기반시설 및 관리 정보를 안전하게 보호하기 위한 예방, 백업, 복구 등 물리적·기술적 대책을 포함한 관리대책(이하 "주요정보통신기반시설보호대책"이라 한다)을 수립·시행하여야 한다. <개정 2015.1.20>

②관리기관의 장은 제1항의 규정에 의하여 주요정보통신기반시설보호대책을 수립한 때에는 이를 주요정보통신기반시설을 관할하는 중앙행정기관(이하 "관계중앙행정기관"이라 한다)의 장에게 제출하여야 한다. 다만, 관리기관의 장이 관계중앙행정기관의 장인 경우에는 그러하지 아니하다.

③지방자치단체의 장이 관리·감독하는 관리기관의 주요정보통신기반시설보호대책은 지방자치단체의 장이 행정자치부장관에게 제출하여야 한다.<개정 2008.2.29, 2013.3.23, 2014.11.19>

④관리기관의 장은 소관 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자(이하 "정보보호책임자"라 한다)를 지정하여야 한다. 다만, 관리기관의 장이 관계중앙행정기관의 장인 경우에는 그러하지 아니하다.

⑤정보보호책임자의 지정 및 업무 등에 관하여 필요한 사항은 대통령령으로 정한다.

제5조의2(주요정보통신기반시설보호대책 이행 여부의 확인) ① 미래창조과학부장관과 국가정보원장 등 대통령령으로 정하는 국가기관의 장(이하 "국가정보원장등" 이라 한다)은 관리기관에 대하여 주요정보통신기반시설보호대책의 이행 여부를 확인할 수 있다. <개정 2008.2.29, 2013.3.23>

② 미래창조과학부장관과 국가정보원장등은 제1항에 따른 확인을 위하여 필요한 경우 관계중앙행정기관의 장에게 제5조제2항에 따라 제출받은 주요정보통신기반시설보호대책 등의 자료 제출을 요청할 수 있다.<개정 2008.2.29, 2013.3.23>

③ 미래창조과학부장관과 국가정보원장등은 제1항에 따라 확인한 주요정보통신기반시설보호대책의 이행 여부를 관계중앙행정기관의 장에게 통보할 수 있다.<개정 2008.2.29, 2013.3.23>

④ 제1항에 따른 주요정보통신기반시설보호대책 이행 여부의 확인절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

[본조신설 2007.12.21]

제6조(주요정보통신기반시설보호계획의 수립 등) ①관계중앙행정기관의 장은 제5조제2항의 규정에 의하여 제출받은 주요정보통신기반시설보호대책을 종합·조정하여 소관분야에 대한 주요정보통신기반시설에 관한 보호계획(이하 "주요정보통신기반시설보호계획"이라 한다)을 수

립·시행하여야 한다.

②관계중앙행정기관의 장은 전년도 주요정보통신기반시설보호계획의 추진실적과 다음 연도의 주요정보통신기반시설보호계획을 위원회에 제출하여 그 심의를 받아야 한다. 다만, 위원회의 위원장이 보안이 요구된다고 인정하는 사항에 대하여는 그러하지 아니하다.

③주요정보통신기반시설보호계획에는 다음 각호의 사항이 포함되어야 한다.<개정 2015.1.20>

1. 주요정보통신기반시설의 취약점 분석·평가에 관한 사항
2. 주요정보통신기반시설 및 관리 정보의 침해사고에 대한 예방, 백업, 복구대책에 관한 사항
3. 그 밖에 주요정보통신기반시설의 보호에 관하여 필요한 사항

④미래창조과학부장관과 국가정보원장은 협의하여 주요정보통신기반시설보호대책 및 주요정보통신기반시설보호계획의 수립지침을 정하여 이를 관계중앙행정기관의 장에게 통보할 수 있다.<개정 2007.12.21, 2008.2.29, 2013.3.23>

⑤관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자(이하 "정보보호책임관"이라 한다)를 지정하여야 한다.

⑥주요정보통신기반시설보호계획의 수립·시행에 관한 사항과 정보보호책임관의 지정 및 업무 등에 관하여 필요한 사항은 대통령령으로 정한다.

제7조(주요정보통신기반시설의 보호지원) ①관리기관의 장이 필요하다고 인정하거나 위원회의 위원장이 특정 관리기관의 주요정보통신기반시설보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려된다고 판단하여 그 보완을 명하는 경우 해당 관리기관의 장은 미래창조과학부장관과 국가정보원장등 또는 필요한 경우 대통령령이 정하는 전문기관의 장에게 다음 각 호의 업무에 대한 기술적 지원을 요청할 수 있다. <개정 2007.12.21, 2008.2.29, 2013.3.23>

1. 주요정보통신기반시설보호대책의 수립
2. 주요정보통신기반시설의 침해사고 예방 및 복구
3. 제11조에 따른 보호조치 명령·권고의 이행

②국가안전보장에 중대한 영향을 미치는 다음 각 호의 주요정보통신기반시설에 대한 관리기관의 장이 제1항에 따라 기술적 지원을 요청하는 경우 국가정보원장에게 우선적으로 그 지원을 요청하여야 한다. 다만, 국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가정보원장은 관계중앙행정기관의 장과 협의하여 그 지원을 할 수 있다.<개정 2007.12.21>

1. 도로·철도·지하철·공항·항만 등 주요 교통시설
2. 전력, 가스, 석유 등 에너지·수자원 시설
3. 방송중계·국가지도통신망 시설
4. 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설

③국가정보원장은 제1항 및 제2항에 불구하고 금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는 아니된다.<개정 2007.12.21>

제3장 주요정보통신기반시설의 지정 및 취약점 분석

제8조(주요정보통신기반시설의 지정 등) ①중앙행정기관의 장은 소관분야의 정보통신기반시설 중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.

1. 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
2. 제1호의 규정에 의한 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
3. 다른 정보통신기반시설과의 상호연계성
4. 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
5. 침해사고의 발생가능성 또는 그 복구의 용이성

②중앙행정기관의 장은 제1항의 규정에 의한 지정 여부를 결정하기 위하여 필요한 자료의 제출을 해당 관리기관에 요구할 수 있다.

③관계중앙행정기관의 장은 관리기관이 해당 업무를 폐지·정지 또는 변경하는 경우에는 직권 또는 해당 관리기관의 신청에 의하여 주요정보통신기반시설의 지정을 취소할 수 있다.

④지방자치단체의 장이 관리·감독하는 기관의 정보통신기반시설에 대하여는 행정자치부장관이 지방자치단체의 장과 협의하여 주요정보통신기반시설로 지정하거나 그 지정을 취소할 수 있다.<개정 2008.2.29, 2013.3.23, 2014.11.19>

⑤중앙행정기관의 장이 제1항 및 제3항의 규정에 의하여 지정 또는 지정 취소를 하고자 하는 경우에는 위원회의 심의를 받아야 한다. 이 경우 위원회는 제1항 및 제3항의 규정에 의하여 지정 또는 지정취소의 대상이 되는 관리기관의 장을 위원회에 출석하게 하여 그 의견을 들을 수 있다.

⑥중앙행정기관의 장은 제1항 및 제3항의 규정에 의하여 주요정보통신기반시설을 지정 또는 지정 취소한 때에는 이를 고시하여야 한다. 다만, 국가안전보장을 위하여 필요한 경우에는 위원회의 심의를 받아 이를 고시하지 아니할 수 있다.

⑦주요정보통신기반시설의 지정 및 지정취소 등에 관하여 필요한 사항은 이를 대통령령으로 정한다.

제8조의2(주요정보통신기반시설의 지정 권고) ① 미래창조과학부장관과 국가정보원장등은 특정한 정보통신기반시설을 주요정보통신기반시설로 지정할 필요가 있다고 판단되는 경우에는 중앙행정기관의 장에게 해당 정보통신기반시설을 주요정보통신기반시설로 지정하도록 권고할 수 있다. <개정 2008.2.29, 2013.3.23>

② 미래창조과학부장관과 국가정보원장등은 제1항에 따른 권고를 위하여 필요한 경우에는 중앙행정기관의 장에게 해당 정보통신기반시설에 관한 자료를 요청할 수 있다.<개정 2008.2.29, 2013.3.23>

③ 제1항에 따른 주요정보통신기반시설의 지정 권고 절차, 그 밖에 필요한 사항은 대통령령으로 정한다.

[본조신설 2007.12.21]

제9조(취약점의 분석·평가) ①관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다.

②관리기관의 장은 제1항의 규정에 의하여 취약점을 분석·평가하고자 하는 경우에는 대통령령이 정하는 바에 따라 취약점을 분석·평가하는 전담반을 구성하여야 한다.

③관리기관의 장은 제1항의 규정에 의하여 취약점을 분석·평가하고자 하는 경우에는 다음 각호의 1에 해당하는 기관으로 하여금 소관 주요정보통신기반시설의 취약점을 분석·평가하게 할 수 있다. 다만, 이 경우 제2항의 규정에 의한 전담반을 구성하지 아니할 수 있다.<개정 2002.12.18, 2007.12.21, 2009.5.22, 2013.3.23, 2015.6.22>

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조의 규정에 의한 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다)
2. 제16조의 규정에 의한 정보공유·분석센터(대통령령이 정하는 기준을 충족하는 정보공유·분석센터에 한한다)
3. 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호 전문서비스 기업
4. 「정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조의 규정에 의한 한국전자통신연구원

④미래창조과학부장관은 관계중앙행정기관의 장 및 국가정보원장과 협의하여 제1항의 규정에 의한 취약점 분석·평가에 관한 기준을 정하고 이를 관계중앙행정기관의 장에게 통보하여야 한다.<개정 2008.2.29, 2013.3.23>

⑤주요정보통신기반시설의 취약점 분석·평가의 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제4장 주요정보통신기반시설의 보호 및 침해사고의 대응

제10조(보호지침) ①관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설에 대하여 보호지침을 제정하고 해당분야의 관리기관의 장에게 이를 지키도록 권고할 수 있다.

②관계중앙행정기관의 장은 기술의 발전 등을 감안하여 제1항의 규정에 의한 보호지침을 주기적으로 수정·보완하여야 한다.

제11조(보호조치 명령 등) 관계중앙행정기관의 장은 다음 각 호의 어느 하나에 해당하는 경우 해당 관리기관의 장에게 주요정보통신기반시설의 보호에 필요한 조치를 명령 또는 권고할 수 있다.

1. 제5조제2항에 따라 제출받은 주요정보통신기반시설보호대책을 분석하여 별도의 보호조치가 필요하다고 인정하는 경우
2. 제5조의2제3항에 따라 통보된 주요정보통신기반시설보호대책의 이행 여부를 분석하여 별도의 보호조치가 필요하다고 인정하는 경우

[전문개정 2007.12.21]

제12조(주요정보통신기반시설 침해행위 등의 금지) 누구든지 다음 각호의 1에 해당하는 행위를 하여서는 아니된다.

1. 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위
2. 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위
3. 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위

제13조(침해사고의 통지) ①관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 인터넷진흥원(이하 "관계기관등"이라 한다)에 그 사실을 통지하여야 한다. 이 경우 관계기관등은 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치를 취하여야 한다. <개정 2013.3.23>

②정부는 제1항의 규정에 의하여 침해사고를 통지함으로써 피해확산의 방지에 기여한 관리기관에 예산의 범위안에서 복구비 등 재정적 지원을 할 수 있다.

제14조(복구조치) ①관리기관의 장은 소관 주요정보통신기반시설에 대한 침해사고가 발생한 때에는 해당 정보통신기반시설의 복구 및 보호에 필요한 조치를 신속히 취하여야 한다.

②관리기관의 장은 제1항의 규정에 의한 복구 및 보호조치를 위하여 필요한 경우 관계중앙행정기관의 장 또는 인터넷진흥원의 장에게 지원을 요청할 수 있다. 다만, 제7조제2항의 규정에 해당하는 경우에는 그러하지 아니하다.<개정 2013.3.23>

③관계중앙행정기관의 장 또는 인터넷진흥원의 장은 제2항의 규정에 의한 지원요청을 받은 때에는 피해복구가 신속히 이루어질 수 있도록 기술지원 등 필요한 지원을 하여야 하고, 피해확산을 방지할 수 있도록 관리기관의 장과 함께 적절한 조치를 취하여야 한다.<개정 2013.3.23>

제15조(대책본부의 구성등) ①위원회의 위원장은 주요정보통신기반시설에 대하여 침해사고가 광범위하게 발생한 경우 그에 필요한 응급대책, 기술지원 및 피해복구 등을 수행하기 위한 기간을 정하여 위원회에 정보통신기반침해사고대책본부(이하 "대책본부"라 한다)를 둘 수 있다.

②위원회의 위원장은 대책본부의 업무와 관련 있는 공무원의 파견을 관계 행정기관의 장에게 요청할 수 있다.

③위원회의 위원장은 침해사고가 발생한 정보통신기반시설을 관할하는 중앙행정기관의 장과 협의하여 대책본부장을 임명한다.

④대책본부장은 관계 행정기관의 장, 관리기관의 장 및 인터넷진흥원의 장에게 주요정보통신기반시설 침해사고의 대응을 위한 협력과 지원을 요청할 수 있다.<개정 2013.3.23>

⑤제4항의 규정에 의하여 협력과 지원을 요청받은 관계 행정기관의 장등은 특별한 사유가 없는 한 이에 응하여야 한다.
⑥대책본부의 구성·운영 등에 관하여 필요한 사항은 대통령령으로 정한다.

제16조(정보공유·분석센터) ①금융·통신 등 분야별 정보통신기반시설을 보호하기 위하여 다음 각호의 업무를 수행하고자 하는 자는 정보공유·분석센터를 구축·운영할 수 있다.
1. 취약점 및 침해요인과 그 대응방안에 관한 정보 제공
2. 침해사고가 발생하는 경우 실시간 경보·분석체계 운영
② 삭제 <2015.12.22>
③ 삭제 <2015.12.22>
④정부는 제1항 각호의 업무를 수행하는 정보공유·분석센터의 구축을 장려하고 그에 대한 재정적·기술적 지원을 할 수 있다.<개정 2015.12.22>
⑤ 삭제 <2015.12.22>

제5장 삭제 <2009.5.22>

제17조 삭제 <2009.5.22>

제18조 삭제 <2009.5.22>

제19조 삭제 <2009.5.22>

제20조 삭제 <2009.5.22>

제21조 삭제 <2009.5.22>

제22조 삭제 <2009.5.22>

제23조 삭제 <2009.5.22>

제6장 기술지원 및 민간협력 등

제24조(기술개발 등) ①정부는 정보통신기반시설을 보호하기 위하여 필요한 기술의 개발 및 전문인력 양성에 관한 시책을 강구할 수 있다.
②정부는 정보통신기반시설의 보호에 필요한 기술개발을 효율적으로 추진하기 위하여 필요한 때에는 정보보호 기술개발과 관련된 연구기관 및 민간단체로 하여금 이를 대행하게 할 수 있다. 이 경우 이에 소요되는 비용의 전부 또는 일부를 지원할 수 있다.

제25조(관리기관에 대한 지원) 정부는 관리기관에 대하여 주요정보통신기반시설을 보호하기 위하여 필요한 기술의 이전, 장비의 제공 그 밖의 필요한 지원을 할 수있다.

제26조(국제협력) ①정부는 정보통신기반시설의 보호에 관한 국제적 동향을 파악하고 국제협력을 추진하여야 한다.

②정부는 정보통신기반시설의 보호에 관한 국제협력을 촉진하기 위하여 관련기술 및 인력의 국제교류와 국제표준화 및 국제공동연구개발 등에 관한 사업을 지원할 수 있다.

제27조(비밀유지의무) 다음 각 호의 어느 하나에 해당하는 기관에 종사하는 자 또는 종사하였던 자는 그 직무상 알게된 비밀을 누설하여서는 아니된다. 다만, 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다. <개정 2007.12.21>

1. 제3조에 따른 위원회 및 실무위원회
2. 제9조제3항의 규정에 의하여 주요정보통신기반시설에 대한 취약점 분석·평가업무를 하는 기관
3. 제13조의 규정에 의하여 침해사고의 통지 접수 및 복구조치와 관련한 업무를 하는 관계기관 등
4. 제16조제1항 각호의 업무를 수행하는 정보공유·분석센터

제7장 벌칙

제28조(벌칙) ①제12조의 규정을 위반하여 주요정보통신기반시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.

②제1항의 미수범은 처벌한다.

제29조(벌칙) 제27조의 규정을 위반하여 비밀을 누설한 자는 5년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.

제30조(과태료) ①다음 각 호의 어느 하나에 해당하는 자는 1천만원 이하의 과태료에처한다. <개정 2007.12.21>

1. 제11조에 따른 보호조치 명령을 위반한 자
2. 삭제 <2015.12.22>
3. 삭제 <2009.5.22>
4. 삭제 <2009.5.22>
5. 삭제 <2009.5.22>

②제1항의 규정에 의한 과태료는 대통령령이 정하는 바에 따라 관계중앙행정기관의 장 또는 미래창조과학부장관(이하 "부과권자"라 한다)이 부과·징수한다.<개정 2008.2.29, 2009.5.22, 2013.3.23>

③제2항의 규정에 의한 과태료처분에 불복이 있는 자는 그 처분의 고지를 받은 날부터 30일 이내에 부과권자에게 이의를 제기할 수 있다.

④제2항의 규정에 의한 과태료처분을 받은 자가 제3항의 규정에 의하여 이의를 제기한 때에는 부과권자는 지체없이 관할법원에 그 사실을 통보하여야 하며, 그 통보를 받은 관할법원은 「

비송사건절차법」에 의한 과태료의 재판을 한다.<개정 2007.12.21>

⑤제3항의 규정에 의한 기간 내에 이의를 제기하지 아니하고 과태료를 납부하지 아니한 때에는 국세체납처분의 예에 의하여 이를 징수한다.

부칙 <제6383호,2001.1.26>

이 법은 2001년 7월 1일부터 시행한다.

부칙 <제6796호,2002.12.18>

①(시행일) 이 법은 공포한 날부터 시행한다.

②(정보보호전문업체의 명칭 변경에 따른 경과조치) 이 법 시행당시 종전의 규정에 의하여 지정된 정보보호전문업체는 이 법의 규정에 의하여 지정된 정보보호컨설팅전문업체로 본다.

부칙 <제7428호,2005.3.31>

제1조 (시행일) 이 법은 공포 후 1년이 경과한 날부터 시행한다.

제2조 내지 제4조 생략

제5조 (다른 법률의 개정) ①내지 <100>생략

<101>정보통신기반보호법 일부를 다음과 같이 개정한다.

제18조제1호 나목중 "파산자"를 "파산선고를 받은 자"로 한다.

<102>내지 <145>생략

제6조 생략

부칙 <제8777호,2007.12.21>

①(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다.

②(적용례) 제5조의2의 개정규정은 2007년에 수립된 주요정보통신기반시설보호대책부터 적용한다.

부칙 <제8852호,2008.2.29>

제1조 (시행일) 이 법은 공포한 날부터 시행한다. 다만, 、、、<생략>、、、, 부칙 제6조에 따라 개정되는 법률 중 이 법의 시행 전에 공포되었으나 시행일이 도래하지 아니한 법률을 개정한 부분은 각각 해당 법률의 시행일부터 시행한다.

제2조부터 제5조까지 생략

제6조 (다른 법률의 개정) ① 부터 <429> 까지 생략

<430> 정보통신기반 보호법 일부를 다음과 같이 개정한다.

제5조제3항, 제8조제4항 중 "행정자치부장관"을 "행정안전부장관"으로 한다.

제30조제2항 중 "정보통신부장관"을 "행정안전부장관·지식경제부장관"으로 한다.

제6조제4항, 제9조제4항, 제11조제2항 본문, 제16조제3항 중 "정보통신부장관"을 각각 "행정안전부장관"으로 한다.

제17조제1항 각 호 외의 부분·제3항, 제19조제1항 각 호 외의 부분, 제20조, 제21조 각 호 외의 부분 본문 및 제22조제1항 중 "정보통신부장관"을 각각 "지식경제부장관"으로 한다.

제17조제3항·제4항, 제19조제1항 각 호 외의 부분, 제20조, 제21조 각 호 외의 부분 및 제23조제3항 중 "정보통신부령"을 "지식경제부령"으로 한다.

<431> 정보통신기반보호법 일부개정법률 일부를 다음과 같이 개정한다.

제3조제3항 중 "국무조정실장"을 "국무총리실장"으로 한다.

제21조 제1항·제2항 중 "정보통신부장관"을 각각 "지식경제부장관"으로 한다.

제21조제1항 중 "정보통신부령"을 "지식경제부령"으로 한다.

제5조의2제1항부터 제3항까지, 제6조제4항, 제7조제1항 각 호 외의 부분, 제8조의2제1항·제2항 중 "정보통신부장관"을 각각 "행정안전부장관"으로 한다.

<432> 부터 <760> 까지 생략

제7조 생략

부칙 <제9708호,2009.5.22>

제1조(시행일) 이 법은 공포 후 3개월이 경과한 날부터 시행한다. <단서 생략>

제2조부터 제9조까지 생략

제10조(다른 법률의 개정) ① 부터 ⑫ 까지 생략

⑬ 정보통신기반 보호법 일부를 다음과 같이 개정한다.

제9조제3항제3호를 다음과 같이 한다.

3. 「정보통신산업 진흥법」 제33조에 따라 지정된 지식정보보안 컨설팅전문업체

제5장(제17조부터 제23조까지) 및 제30조제1항제3호부터 제5호까지를 각각 삭제한다.

제30조제2항 중 "관계중앙행정기관의 장 또는 행정안전부장관·지식경제부장관(이하 "부과권자"라 한다)"을 "관계중앙행정기관의 장 또는 행정안전부장관(이하 "부과권자"라 한다)"으로 한다.

⑭ 및 ⑮ 생략

제11조 및 제12조 생략

부칙 <제11690호,2013.3.23>

제1조(시행일) ① 이 법은 공포한 날부터 시행한다.

② 생략

제2조부터 제5조까지 생략

제6조(다른 법률의 개정) ①부터 <191>까지 생략

<192> 정보통신기반 보호법 일부를 다음과 같이 개정한다.

제3조제3항 중 "국무총리실장"을 "국무조정실장"으로 한다.

제5조제3항 및 제8조제4항 중 "행정안전부장관"을 각각 "안전행정부장관"으로 한다.

제5조의2제1항부터 제3항까지, 제6조제4항, 제7조제1항 각 호 외의 부분, 제8조의2제1항·제2항, 제9조제4항, 제16조제3항 및 제30조제2항 중 "행정안전부장관"을 각각 "미래창조과학부장관"으로 한다.

제9조제3항제1호 중 "한국정보보호진흥원(이하 "보호진흥원"이라 한다)"을 "한국인터넷진흥원(이하 "인터넷진흥원"이라 한다)"으로 한다.

제13조제1항 전단, 제14조제2항 본문, 같은 조 제3항 및 제15조제4항 중 "보호진흥원"을 각각 "인터넷진흥원"으로 한다.

<193>부터 <710>까지 생략

제7조 생략

부칙 <제12844호,2014.11.19>

제1조(시행일) 이 법은 공포한 날부터 시행한다. 다만, 부칙 제6조에 따라 개정되는 법률 중 이 법 시행 전에 공포되었으나 시행일이 도래하지 아니한 법률을 개정한 부분은 각각 해당 법률의 시행일부터 시행한다.

제2조부터 제5조까지 생략

제6조(다른 법률의 개정) ①부터 <21>까지 생략

<22> 정보통신기반 보호법 일부를 다음과 같이 개정한다.

제5조제3항 및 제8조제4항 중 "안전행정부장관"을 각각 "행정자치부장관"으로 한다.

<23>부터 <258>까지 생략

제7조 생략

부칙 <제13013호,2015.1.20>

이 법은 공포 후 6개월이 경과한 날부터 시행한다.

부칙 <제13343호,2015.6.22>

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다.

제2조 생략

제3조(다른 법률의 개정) ① 정보통신기반 보호법 일부를 다음과 같이 개정한다.

제9조제3항제3호를 다음과 같이 한다.

3. 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호 전문서비스 기업

② 및 ③ 생략

부칙 <제13590호,2015.12.22>

이 법은 공포한 날부터 시행한다.

정보통신기반 보호법 시행령

[시행 2015.12.23] [대통령령 제26728호, 2015.12.22, 타법개정]

제1장 총칙

제1조(목적) 이 영은 정보통신기반보호법에서 위임된 사항과 그 시행에 관하여 필요한 사항을 규정함을 목적으로 한다.

제2조(정보통신기반보호위원회의 위원) 「정보통신기반 보호법」(이하 "법"이라 한다) 제3조 제3항에서 "대통령령이 정하는 중앙행정기관의 차관급 공무원"이란 다음 각 호의 사람을 말한다. 이 경우 차관급 공무원이 2명 이상인 기관은 해당 기관의 장이 지정하는 사람을 말한다. <개정 2013.3.23, 2014.11.19>

1. 기획재정부차관
2. 미래창조과학부차관
3. 외교부차관
4. 법무부차관
5. 국방부차관
6. 행정자치부차관
7. 산업통상자원부차관
8. 보건복지부차관
9. 고용노동부차관
10. 국토교통부차관
11. 해양수산부차관
12. 국가정보원 차장
13. 금융위원회 부위원장
14. 방송통신위원회 상임위원

[전문개정 2012.5.23]

제3조(정보통신기반보호위원회의 운영) ①정보통신기반보호위원회(이하 "위원회"라 한다)의 위원장은 회의를 소집하고, 그 의장이 된다.

②위원장이 부득이한 사유로 직무를 수행할 수 없는 때에는 위원장이 지명하는 위원의 순으로 그 직무를 대행한다.

③위원회의 사무를 처리하기 위하여 위원회에 간사 1인을 두되, 간사는 국무조정실의 정보통신기반시설 보호 업무를 담당하는 고위공무원단에 속하는 공무원이 된다.<개정 2008.2.29, 2012.5.23, 2013.3.23>

④위원회의 회의를 소집하고자 하는 때에는 회의 일시·장소 및 부의사항을 회의개최 7일전까지 각 위원에게 서면 또는 전자문서로 통지하여야 한다. 다만, 긴급을 요하거나 부득이한 사유가 있는 경우에는 그러하지 아니하다.

⑤위원장은 법 제4조 각호의 규정에 의한 사항의 심의를 위하여 필요하다고 인정되는 경우에는 관련 전문가 또는 전문기관의 장으로 하여금 그에 관한 검토보고를 하게 할 수 있다.

제4조(의사 및 의결정족수) 위원회는 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 의결한다.

제5조(실무위원회의 구성·운영) ① 법 제3조제4항에 따라 위원회에 두는 공공분야를 담당하는 실무위원회(이하 "공공분야 실무위원회"라 한다)와 민간분야를 담당하는 실무위원회(이하 "민간분야 실무위원회"라 한다)는 각각 위원장 1명을 포함한 25명 이내의 위원으로 구성한다.

② 공공분야 실무위원회의 위원장은 국가정보원 차장이 되고, 민간분야 실무위원회의 위원장은 미래창조과학부 제2차관이 되며, 각 실무위원회 위원장은 해당 실무위원회의 회의를 소집하고 그 의장이 된다.<개정 2013.3.23>

③ 각 실무위원회의 위원은 다음 각 호의 어느 하나에 해당하는 사람 중에서 각 실무위원회의 위원장이 임명하거나 위촉한다.

1. 법 제8조에 따라 지정된 주요정보통신기반시설(이하 "주요정보통신기반시설"이라 한다)을 관할하는 중앙행정기관(이하 "관계중앙행정기관"이라 한다)의 고위공무원단에 속하는 공무원 또는 그에 상당하는 공무원
2. 주요정보통신기반시설을 관리하는 기관(이하 "관리기관"이라 한다)의 임원 또는 직원

④ 각 실무위원회는 다음 각 호의 구분에 따른 주요정보통신기반시설의 보호에 관하여 위원회의 심의를 지원한다.

1. 공공분야 실무위원회: 다음 각 목의 주요정보통신기반시설
   가. 중앙행정기관·지방자치단체 및 그 소속 기관의 장이 관리하는 주요정보통신기반시설
   나. 국회·법원·헌법재판소·중앙선거관리위원회 및 그 소속 기관의 장이 관리하는 주요정보통신기반시설
   다. 「전자정부법」 제2조제3호에 따른 공공기관이 관리하는 주요정보통신기반시설
2. 민간분야 실무위원회: 제1호에 따른 주요정보통신기반시설 외의 주요정보통신기반시설

⑤ 각 실무위원회는 제4항 각 호의 구분에 따른 주요정보통신기반시설의 보호에 관하여 위원회가 위임하거나 위원회의 위원장이 지시한 사항을 검토·심의한다.

⑥ 실무위원회의 운영에 관하여는 제3조제2항부터 제5항까지 및 제4조를 각각 준용한다. 이 경우 "위원회"는 "각 실무위원회"로, "위원장"은 "실무위원회 위원장"으로, "국무조정실의 정보통신기반시설 보호 업무를 담당하는 고위공무원단에 속하는 공무원"은 "실무위원회 위원장

이 지명하는 소속 공무원"으로 본다.<개정 2013.3.23>

[전문개정 2012.5.23]

제6조(위원회의 수당 등) 위원회 또는 실무위원회에 출석한 위원、관계인 및 전문가에 대하여 예산의 범위안에서 수당 및 여비를 지급할 수 있다. 다만, 공무원이 그 소관 업무와 직접적으로 관련되는 위원회에 출석하는 경우에는 그러하지 아니하다.

제7조(운영세칙) 이 영에서 규정한 것 이외에 위원회 및 실무위원회의 운영에 관하여 필요한 사항은 각 해당위원회의 의결을 거쳐 해당 위원회의 위원장이 각각 정한다.

제8조(주요정보통신기반시설보호대책의 수립) 법 제5조제2항 또는 제3항에 따라 관리기관의 장 및 지방자치단체의 장은 다음 연도의 법 제5조제1항에 따른 주요정보통신기반시설보호대책(이하 "주요정보통신기반시설보호대책"이라 한다)을 수립하여 매년 8월 31일까지 관계중앙행정기관의 장에게 제출하여야 한다.

[전문개정 2012.5.23]

제9조(정보보호책임자의 지정 등) ①법 제5조제4항 본문에 따라 관리기관의 장은 소관 주요정보통신기반시설의 보호 업무를 담당하는 4급、4급상당 공무원, 5급、5급상당 공무원, 영관급 장교 또는 임원급 관리、운영자를 정보보호책임자로 지정하여야 한다. <개정 2012.5.23>

②제1항의 규정에 의한 정보보호책임자가 총괄하는 업무는 각호와 같다.

1. 법 제5조제1항의 규정에 의한 주요정보통신기반시설보호대책의 수립、시행
2. 법 제7조제1항 및 제2항 본문의 규정에 의한 기술적 지원의 요청
3. 법 제9조의 규정에 의한 취약점 분석、평가 및 전담반 구성
4. 법 제11조제1항의 규정에 의한 주요정보통신기반시설의 보호에 필요한 조치 명령 또는 권고의 이행
5. 법 제13조제1항 전단의 규정에 의한 침해사고의 통지
6. 법 제14조제1항의 규정에 의한 해당 주요정보통신기반시설의 복구 및 보호에 필요한 조치
7. 기타 다른 법령에 규정된 주요정보통신기반시설의 보호업무에 관한 사항

③관리기관의 장이 정보보호책임자를 지정한 때에는 이를 관할 중앙행정기관의 장에게 통지하여야 한다.

제9조의2(주요정보통신기반시설보호대책 이행 여부의 확인) ① 법 제5조의2제1항에서 "국가정보원장 등 대통령령으로 정하는 국가기관의 장"이란 국가정보원장 및 국방부장관을 말한다.

② 법 제5조의2제1항에 따라 미래창조과학부장관, 국가정보원장 및 국방부장관은 다음 각 호의 구분에 따른 관할 주요정보통신기반시설에 대한 관리기관의 주요정보통신기반시설보호대책 이행 여부를 확인할 수 있다.<개정 2013.3.23>

1. 미래창조과학부장관: 제5조제4항제2호에 따른 주요정보통신기반시설
2. 국가정보원장: 제5조제4항제1호에 따른 주요정보통신기반시설(제3호의 국방 분야 주요정보통신기반시설은 제외한다)

3. 국방부장관: 국방 분야 주요정보통신기반시설

③ 미래창조과학부장관, 국가정보원장 및 국방부장관은 법 제5조의2에 따라 주요정보통신기반시설보호대책 이행 여부를 확인하기 위하여 필요한 자료의 제출을 제2항의 구분에 따른 관할 주요정보통신기반시설 관리기관에 요청하고, 해당 주요정보통신기반시설보호대책에 따른 보호조치의 세부적인 내용을 확인·점검할 수 있다.<개정 2013.3.23>

④ 미래창조과학부장관과 국가정보원장은 법 제5조의2에 따라 주요정보통신기반시설보호대책의 이행 여부를 확인하려는 경우 미리 확인 절차 등에 관하여 관계중앙행정기관의 장과 협의하여야 하고, 미래창조과학부장관, 국가정보원장 및 국방부장관은 확인 절차 등에 관하여 해당 관리기관에 통보하여야 한다.<개정 2013.3.23>

⑤ 미래창조과학부장관, 국가정보원장 및 국방부장관은 법 제5조의2에 따른 주요정보통신기반시설보호대책 이행 여부 확인을 위하여 필요한 경우 제12조에 따른 주요정보통신기반시설보호지원기관에 지원을 요청할 수 있다.<개정 2013.3.23>

⑥ 제1항부터 제5항까지에서 규정한 사항 외에 법 제5조의2에 따른 주요정보통신기반시설보호대책 이행 여부의 확인에 관한 세부 사항은 미래창조과학부장관과 국가정보원장이 협의하여 정한다.<개정 2013.3.23>

[본조신설 2012.5.23]

제9조의3(주요정보통신기반시설보호대책 이행 여부 확인 결과 보고 등) ① 미래창조과학부장관, 국가정보원장 및 국방부장관은 법 제5조의2에 따른 주요정보통신기반시설보호대책의 이행 여부 확인 결과를 위원회에 보고하여야 한다. <개정 2013.3.23>

② 미래창조과학부장관, 국가정보원장 및 국방부장관은 법 제5조의2에 따른 주요정보통신기반시설보호대책의 이행 여부 확인 결과 보완이 필요하다고 판단되는 관리기관에 대해서는 개선을 권고할 수 있다.<개정 2013.3.23>

③ 미래창조과학부장관과 국가정보원장은 법 제5조의2에 따른 주요정보통신기반시설보호대책의 이행 여부 확인 결과를 다음 연도의 주요정보통신기반시설보호대책 및 법 제6조제1항에 따른 주요정보통신기반시설보호계획(이하 "주요정보통신기반시설보호계획"이라 한다)의 수립지침에 반영할 수 있다.<개정 2013.3.23>

④ 미래창조과학부장관과 국가정보원장은 법 제7조에 따른 주요정보통신기반시설의 보호지원을 효율적으로 하기 위하여 주요정보통신기반시설보호대책의 이행 여부 확인 결과를 서로 제공하여야 한다.<개정 2013.3.23>

[본조신설 2012.5.23]

제10조(주요정보통신기반시설보호계획의 수립 등) ①관계중앙행정기관의 장은 법 제6조제2항에 따라 전년도 주요정보통신기반시설보호계획의 추진실적과 다음 연도의 주요정보통신기반시설보호계획을 매년 10월 31일까지 위원회에 제출하여야 한다. <개정 2012.5.23>

②미래창조과학부장관과 국가정보원장은 법 제6조제4항에 따라 매년 5월 31일까지 다음 연도의 주요정보통신기반시설보호대책 및 주요정보통신기반시설보호계획의 수립지침을 작성하

여 이를 관계중앙행정기관의 장에게 통보할 수 있다. 이 경우 주요정보통신기반시설보호대책의 수립지침을 통보받은 관계중앙행정기관의 장은 관할 주요정보통신기반시설의 관리기관의 장(법 제5조제3항에 따라 주요정보통신기반시설보호대책을 제출하여야 하는 지방자치단체의 장을 포함한다)에게 그 수립지침을 통보하여야 한다.<개정 2008.2.29, 2012.5.23, 2013.3.23>

③관계중앙행정기관의 장은 다음 연도의 주요정보통신기반시설보호계획을 위원회의 심의를 거쳐 12월 31일까지 확정한다.<개정 2012.5.23>

[제목개정 2012.5.23]

제11조(정보보호책임관의 지정 등) ①관계중앙행정기관의 장은 주요정보통신기반시설 보호업무를 담당하는 과장급 공무원을 법 제6조제5항의 규정에 의한 정보보호책임관으로 지정하여야 한다.

②제1항의 규정에 의한 정보보호책임관이 총괄하는 업무는 다음 각호와 같다.

1. 법 제6조제1항의 규정에 의한 주요정보통신기반시설보호계획의 수립·시행
2. 법 제8조의 규정에 의한 주요정보통신기반시설의 지정 및 지정 취소
3. 법 제10조의 규정에 의한 보호지침의 제정·수정 및 보완
4. 법 제13조제1항 후단의 규정에 의한 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치
5. 법 제14조제3항의 규정에 의한 피해복구 지원 및 피해확산 방지에 필요한 조치
6. 기타 다른 법령에 규정된 주요정보통신기반시설의 보호업무에 관한 사항

제12조(주요정보통신기반시설 보호지원기관의 범위) 법 제7조제1항 각 호 외의 부분에서 "대통령령이 정하는 전문기관"이란 다음 각 호의 기관을 말한다. <개정 2015.12.22>

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따라 설립된 한국인터넷진흥원
2. 법 제9조제3항제2호에 따른 정보공유·분석센터
3. 「정보보호산업의 진흥에 관한 법률」 제23조제1항제1호 및 제2호에 따라 지정된 정보보호 전문서비스 기업
4. 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조에 따라 설립된 한국전자통신연구원의 국가보안기술 연구·개발을 전담하는 부설연구소

[전문개정 2012.5.23]

제13조(지정단위의 선정) ①중앙행정기관의 장은 주요정보통신기반시설로 지정됨이 상당하다고 판단되는 시설의 관리기관(이하 "지정대상시설관리기관"이라 한다)의 장에게 법 제8조제1항 각호의 사항을 고려하여 주요정보통신기반시설을 지정하기 위한 기본단위(이하 "지정단위"라 한다)를 선정하도록 한다.

②지정대상시설관리기관의 장은 법 제8조제1항 각호의 사항을 고려하고 당해 기관의 특수성을 반영하여 지정단위를 선정한다.

③지정대상시설관리기관의 장은 지정단위와 관련된 세부시설의 범위를 정할 수 있다.
④ 삭제 <2014.12.9>
⑤중앙행정기관의 장은 제2항에 따른 지정단위 선정 및 제3항에 따른 지정단위와 관련된 세부시설 범위의 타당성 등을 검토하고, 필요한 경우 이를 조정할 수 있다. 다만, 중앙행정기관의 장이 지정대상시설관리기관의 장인 경우에는 소관 시설에 대하여 직접 지정단위와 관련된 세부시설의 범위를 정한다.<개정 2012.5.23, 2014.12.9>

제14조(지정여부의 자체평가) ①중앙행정기관의 장은 주요정보통신기반시설의 지정여부 평가를 위한 기준을 마련하여 지정대상시설관리기관의 장에게 통보할 수 있다.
②지정대상시설관리기관의 장은 제13조제2항 및 제3항의 규정에 의하여 선정된 지정단위 및 그와 관련된 세부시설에 대하여 제1항의 규정에 의한 지정여부 평가를 위한 기준을 근거로 주요정보통신기반시설 지정여부를 자체 평가하고, 그 결과를 중앙행정기관의 장에게 제출한다. 다만, 지정대상시설관리기관의 장인 중앙행정기관의 장이 지정여부를 평가한 경우에는 그러하지 아니하다.

제15조(지정여부 심사) ①중앙행정기관의 장은 지정대상시설관리기관의 장이 제14조제2항 본문의 규정에 의하여 제출한 주요정보통신기반시설 지정여부에 대한 자체 평가결과에 대하여 법 제8조제1항 각호에 따라 객관적이고 적정하게 평가가 이루어졌는지 여부를 심사한다.
②중앙행정기관의 장은 제1항의 규정에 의한 심사를 하는 때에는 지정의 객관성을 확보하기 위하여 관계전문가로 구성된 협의회에서 심의하게 할 수 있다.
③중앙행정기관의 장은 제1항의 규정에 의한 심사에서 지정대상시설관리기관의 장이 해당 시설에 대한 평가를 부실하게 하였거나 상당한 이유없이 누락하였다고 판단되는 경우 이를 다시 평가하도록 지시하거나 권고할 수 있다.

제16조(지정 및 지정취소의 통보 등) 중앙행정기관의 장은 주요정보통신기반시설을 지정 또는 지정 취소하는 경우 지체없이 해당 관리기관의 장에게 그 사실을 통보하고 다음 각호의 사항을 관보에 고시하여야 한다.
1. 지정번호
2. 주요정보통신기반시설의 명칭
3. 관리기관의 명칭
4. 수행업무
5. 지정 또는 지정취소 사유

제16조의2(주요정보통신기반시설의 지정 권고 등) ① 미래창조과학부장관과 국가정보원장은 법 제8조의2에 따른 주요정보통신기반시설 지정 대상의 선정을 위하여 제9조의2제2항 각 호의 구분에 따른 관할별로 주요정보통신기반시설지정조사반(이하 "조사반"이라 한다)을 두고, 각 조사반으로 하여금 법 제8조제1항 각 호의 사항을 고려하여 주요정보통신기반시설 지정 필요성을 검토하게 할 수 있다. <개정 2013.3.23>

② 미래창조과학부장관과 국가정보원장은 법 제8조의2제1항에 따라 중앙행정기관의 장에게 주요정보통신기반시설로 지정할 것을 권고하기 전에 미리 지정 대상 정보통신기반시설을 관리하는 기관의 장 및 관할 중앙행정기관의 장과 협의할 수 있다.<개정 2013.3.23>
③ 중앙행정기관의 장은 제1항에 따라 관할 정보통신기반시설에 대해 주요정보통신기반시설의 지정 권고를 받은 경우 60일 이내에 제13조에 따른 지정단위 선정, 제14조에 따른 자체평가 및 제15조에 따른 심사 절차를 거쳐 주요정보통신기반시설 지정 여부를 결정하고, 이를 지정 권고한 미래창조과학부장관 또는 국가정보원장에게 통보하여야 한다.<개정 2013.3.23>
④ 제2항에 따른 조사반의 구성과 운영에 필요한 사항은 미래창조과학부장관과 국가정보원장이 협의하여 정한다.<개정 2013.3.23>

[본조신설 2012.5.23]

제17조(취약점 분석·평가의 시기) ①관리기관의 장은 소관 정보통신기반시설이 주요정보통신기반시설로 지정된 때에는 지정 후 6월 이내에 법 제9조제1항의 규정에 의한 취약점의 분석·평가를 실시하여야 한다. 다만, 관리기관의 장은 소관 주요정보통신기반시설 지정 후 6월 이내에 동 시설에 대한 취약점의 분석·평가를 시행하지 못할 특별한 사유가 있다고 판단되는 경우에는 관할 중앙행정기관의 장의 승인을 얻어 지정 후 9월 이내에 이를 실시하여야 한다.
②관리기관의 장은 제1항에 따라 소관 주요정보통신기반시설이 지정된 후 당해 주요정보통신기반시설에 대한 최초의 취약점 분석·평가를 한 후에는 매년 취약점의 분석·평가를 실시한다. 다만, 소관 주요정보통신기반시설에 중대한 변화가 발생하였거나 관리기관의 장이 취약점 분석·평가가 필요하다고 판단하는 경우에는 1년이 되지 아니한 때에도 취약점의 분석·평가를 실시할 수 있다.<개정 2012.5.23>

제18조(취약점 분석·평가 방법 및 절차) ①법 제9조제2항의 규정에 의하여 관리기관의 장은 취약점을 분석·평가하기 위한 전담반을 구성하는 때에는 별표 1의 사항을 고려하여 취약점 분석·평가의 객관성과 실효성을 확보할 수 있도록 하여야 한다.
②관리기관의 장은 법 제9조제3항 각호의 1에 해당하는 기관으로 하여금 소관 주요정보통신기반시설의 취약점을 분석·평가하게 하는 때에는 취약점 분석·평가 수행기관이 취득한 관리기관의 비밀정보가 외부에 유출되지 아니하도록 적정한 조치를 취하여야 한다.
③법 제9조제3항의 규정에 의하여 관리기관의 장이 동항 각호의 1에 해당하는 기관으로 하여금 취약점을 분석·평가하게 하는 때에는 취약점 분석·평가 업무를 위탁받은 기관이 이를 직접 수행하도록 하여야 한다.
④법 제9조제4항의 규정에 의한 취약점 분석·평가 기준에는 다음 각호의 사항이 포함되어야 한다.

1. 취약점 분석·평가의 절차
2. 취약점 분석·평가의 범위 및 항목
3. 취약점 분석·평가의 방법

제19조(정보공유·분석센터의 취약점 분석·평가) ①법 제9조제3항제2호에서 "대통령령이 정하는 기준"이라 함은 별표 2의 기준을 말한다.

②정보공유·분석센터에 가입한 복수의 관리기관이 정보통신망을 통하여 영업을 수행하는 분야에 있어서 상호 연동된 주요정보통신기반시설에 대한 취약점 분석·평가는 해당 관리기관의 동의를 얻어 수행하여야 한다.

제20조(보호지침의 제정) ①법 제10조의 규정에 의한 보호지침에는 주요정보통신기반시설 보호에 필요한 다음 각호에 관한 사항이 포함되어야 한다.

1. 정보보호체계의 관리 및 운영
2. 취약점 분석·평가 및 침해사고 예방
3. 침해사고에 대한 대응 및 복구

②관계중앙행정기관의 장은 보호지침을 제정·수정 또는 보완한 경우에는 이를 소관 관리기관의 장에게 통지한다.

제21조(침해사고의 통지) ①법 제13조제1항 전단의 규정에 의한 침해사고의 통지에는 다음 각호의 사항이 포함되어야 한다.

1. 침해사고발생 일시 및 시설
2. 침해사고로 인한 피해내역
3. 기타 신속한 대응·복구를 위하여 필요한 사항

②법 제13조제1항의 규정에 의한 관계 행정기관은 국가보안업무를 수행하는 기관(국가기관 또는 지방자치단체의 장이 관리기관의 장인 주요정보통신기반시설 및 법 제7조제2항 각호에 해당하는 주요정보통신기반시설의 경우에 한한다) 또는 관계중앙행정기관으로 한다.

③침해사고 상황의 통지 절차 및 방법에 관하여 이 영에서 규정한 것 이외의 필요한 사항은 관계중앙행정기관의 장이 정할 수 있다.

제22조(정보통신기반침해사고대책본부의 구성 등) ①법 제15조제1항의 규정에 의한 정보통신기반침해사고대책본부(이하 "대책본부"라 한다)는 정보통신기반보호와 직접 관련이 있는 중앙행정기관 소속 공무원중에서 대책본부장이 지명하는 자 및 법 제15조제2항의 규정에 의하여 파견된 자로 구성한다.

②대책본부장을 보좌하기 위하여 차장 2인을 두되, 차장은 제1항의 규정에 의한 대책본부의 구성원 중에서 대책본부장이 임명한다.

③대책본부장은 침해사고에 적절히 대응하기 위하여 필요한 기능별로 실무반을 설치·운영할 수 있다.

제23조(대책본부의 운영) ①대책본부장은 대책본부를 대표하고, 그 업무를 총괄한다.

②대책본부장은 침해사고 피해의 효율적인 수습을 위하여 필요하다고 인정할 때에는 제22조제1항의 규정에 의한 대책본부의 구성원이 참여하는 회의(이하 "대책본부회의"라 한다. 이하 이 조에서 같다)를 소집할 수 있다. 다만, 다음 각호의 사항에 관하여는 반드시 대책본부 회의

를 거쳐야 한다.

1. 피해시설에 대한 복구조치
2. 피해확산 방지에 필요한 조치
3. 피해액 산정의 기준
4. 유사한 침해사고의 방지를 위한 예방대책

③ 대책본부장은 침해사고 조사결과와 침해사고 재발방지를 위한 예방대책을 위원회에 보고하여야 한다.<신설 2012.5.23>

④이 영에서 규정한 것 외에 대책본부의 운영, 대책본부회의 및 제22조제3항의 규정에 의한 기능별 실무반의 구성·운영 등에 관하여 필요한 사항은 대책본부장이 정한다.<개정 2012.5.23>

제24조(정보공유·분석센터 구축의 통지) ①법 제16조제2항에 따라 정보공유·분석센터의 장은 미래창조과학부령이 정하는 정보공유·분석센터구축통지서에 따라 다음 각호의 사항을 정보공유·분석센터를 구축한 날부터 30일 이내에 관계중앙행정기관의 장에게 통지하여야 한다. <개정 2008.2.29, 2012.5.23, 2013.3.23>

1. 명칭 및 사무소의 소재지
2. 대표자 및 임원의 인적사항(성명·주소·생년월일 및 경력)
3. 주요업무
4. 회비·수수료 등 재원조달방식
5. 조직운영규칙(법인인 경우에는 정관을 포함한다)
6. 업무를 외부에 위탁하는 경우에는 해당 수탁기관의 제1호 및 제2호에 관한 사항

②제1항의 규정에 의한 통지를 받은 중앙행정기관의 장은 통지받은 내용중 누락된 사항이 없는지 여부를 확인하고 관리대장을 작성하여 유지·관리하여야 한다. 이 경우 누락된 사항이 발견된 때에는 30일 이내의 기간을 정하여 이를 보완하게 할 수 있다.

③정보공유·분석센터의 장은 제2항의 규정에 의하여 통지한 내용을 변경하는 때에는 변경사유가 발생한 날부터 30일 이내에 관할 중앙행정기관의 장에게 변경사항을 통지하여야 한다.

제24조의2(규제의 재검토) 미래창조과학부장관은 다음 각 호의 사항에 대하여 다음 각 호의 기준일을 기준으로 2년마다(매 2년이 되는 해의 기준일과 같은 날 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

1. 제8조에 따른 주요정보통신기반시설 보호대책의 수립 시기: 2015년 1월 1일
2. 제9조에 따른 정보보호책임자의 지정 및 업무: 2015년 1월 1일
3. 제17조에 따른 취약점 분석·평가의 시기: 2015년 1월 1일

[본조신설 2014.12.9]

제25조(과태료의 부과기준) 법 제30조제1항에 따른 과태료의 부과기준은 별표 3과 같다.

[전문개정 2011.4.6]

부칙 <제17308호,2001.7.16>

①(시행일) 이 영은 공포한 날부터 시행한다.

②(2002년도 주요정보통신기반시설보호계획의 작성 등의 일정에 관한 특례) 법 제6조의 규정에 의한 2002년도 주요정보통신기반시설보호계획의 작성지침의 통보, 위원회에의 제출 및 확정의 일정에 관하여는 제10조의 규정에 불구하고 정보통신부장관이 따로 정하는 바에 의한다.

부칙 <제18006호,2003.6.23>(전기통신사업법시행령)

①(시행일) 이 영은 공포한 날부터 시행한다.

②(다른 법령의 개정) 정보통신기반보호법시행령중 다음과 같이 개정한다.

제12조제2항제2호중 "정보보호전문업체"를 "정보보호컨설팅전문업체"로 한다.

부칙 <제18312호,2004.3.17>(전자적민원처리를위한가석방자관리규정등중개정령)

이 영은 공포한 날부터 시행한다.

부칙 <제18594호,2004.12.3>(과학기술분야정부출연연구기관등의설립·운영및육성에관한법률시행령)

제1조 (시행일) 이 영은 공포한 날부터 시행한다.

제2조 및 제3조 생략

제4조 (다른 법령의 개정) ①내지 <29>생략

<30>정보통신기반보호법시행령중 다음과 같이 개정한다.

제12조제2항제3호중 "정부출연연구기관등의설립·운영및육성에관한법률"을 "과학기술분야정부출연연구기관등의설립·운영및육성에관한법률"로 한다.

<31>내지 <42>생략

제5조 생략

부칙 <제19513호,2006.6.12>(고위공무원단 인사규정)

제1조 (시행일) 이 영은 2006년 7월 1일부터 시행한다.

제2조 및 제3조 생략

제4조 (다른 법령의 개정) ①내지 <186>생략

<187>정보통신기반보호법시행령 일부를 다음과 같이 개정한다.

제5조제5항 본문중 "1급 또는 1급상당 공무원"을 "고위공무원단에 속하는 공무원"으로 하고, 동항 단서중 "정보통신부와 국가정보원의 정보통신기반보호업무를 관장하는 1급 또는 1급상당 공무원"을 "정보통신부와 국가정보원의 정보통신기반보호업무를 관장하는 1급 또는 1급상당 공무원(고위공무원단에 속하는 공무원을 포함한다)"으로 한다.

<188>내지 <241>생략

부칙 <제20741호,2008.2.29>(행정안전부와 그 소속기관 직제)

제1조(시행일) 이 영은 공포한 날부터 시행한다. <단서 생략>

제2조부터 제5조까지 생략

제6조(다른 법령의 개정) ① 부터 <69> 까지 생략

<70> 정보통신기반보호법 시행령 일부를 다음과 같이 개정한다.

제2조 중 "재정경제부장관、법무부장관、국방부장관、행정자치부장관、과학기술부장관、산업자원부장관、정보통신부장관、건설교통부장관、해양수산부장관、기획예산처장관、국가정보원장、금융감독위원회위원장"을 "기획재정부장관、법무부장관、국방부장관、행정안전부장관、교육과학기술부장관、지식경제부장관、국토해양부장관、국가정보원장、금융위원회위원장"으로 한다.

제3조제3항 중 "국무조정실장"을 "국무총리실장"으로 한다.

제5조제3항 및 제10조제2항 중 "정보통신부장관"을 각각 "행정안전부장관"으로 한다.

제5조제5항 본문 및 단서 중 "정보통신부"를 각각 "행정안전부"로 한다.

제24조제1항 각 호 외의 부분 중 "정보통신부령"을 "행정안전부령"으로 한다.

제25조제1항 중 "관계 중앙행정기관의 장 또는 정보통신부장관"을 "관계 중앙행정기관의 장, 행정안전부장관 또는 지식경제부장관"으로 한다.

제25조제4항 중 "정보통신부령"을 "행정안전부령 또는 지식경제부령"으로 한다.

<71> 부터 <105> 까지 생략

부칙 <제21214호,2008.12.31>

제1조(시행일) 이 영은 공포한 날부터 시행한다. <단서 생략>

제2조부터 제4조까지 생략

제5조(다른 법령의 개정) ① 부터 <75> 까지 생략

<76> 정보통신기반보호법시행령 일부를 다음과 같이 개정한다.

별표 2 나목의 기준란 중 "정보통신부령이"를 "지식경제부령으로"로 하고, 같은 표 라목의 기준란 중 "정보통신부장관"을 "행정안전부장관"으로 하며, 같은 표 비고란의 제2호 중 "정보통신부장관"을 "행정안전부장관"으로 한다.

<77> 부터 <175> 까지 생략

부칙 <제21692호,2009.8.18>

제1조(시행일) 이 영은 2009년 8월 23일부터 시행한다.

제2조부터 제4조까지 생략

제5조(다른 법령의 개정) ① 부터 <22> 까지 생략

<23> 정보통신기반보호법시행령 일부를 다음과 같이 개정한다.

제12조제2항제2호를 다음과 같이 한다.

2. 「정보통신산업 진흥법」 제33조에 따른 지식정보보안 컨설팅전문업체

제25조제1항 중 "관계 중앙행정기관의 장, 행정안전부장관 또는 지식경제부장관(이하 "부과권자"라 한다)"을 "관계 중앙행정기관의 장 또는 행정안전부장관(이하 "부과권자"라 한다)"으로 하고, 같은 조 제4항 중 "행정안전부령 또는 지식경제부령"을 "행정안전부령"으로 한다.

<24> 부터 <28> 까지 생략

제6조 생략

부칙 <제22879호,2011.4.6>

제1조(시행일) 이 영은 공포한 날부터 시행한다.

제2조(과태료에 관한 경과조치) ① 이 영 시행 전의 위반행위에 대하여 과태료의 부과기준을 적용할 때에는 별표 3의 개정규정에도 불구하고 종전의 예에 따른다.

② 이 영 시행 전의 위반행위로 받은 과태료 부과처분은 별표 3의 개정규정에 따른 위반행위의 횟수 산정에 포함하지 아니한다.

부칙 <제23806호,2012.5.23>

제1조(시행일) 이 영은 공포한 날부터 시행한다. 다만, 제17조제2항의 개정규정은 2013년 1월 1일부터 시행한다.

제2조(취약점 분석·평가 주기 변경에 따른 경과조치) 2013년 1월 1일 전에 종전의 제17조제2항에 따라 취약점 분석·평가를 실시한 관리기관의 장은 그 취약점 분석·평가의 실시 시기에도 불구하고 2013년 1월 1일부터 2013년 12월 31일 사이에 제17조제2항의 개정규정에 따른 최초의 취약점 분석·평가를 실시하여야 한다.

부칙 <제24425호,2013.3.23>

제1조(시행일) 이 영은 공포한 날부터 시행한다. 다만, 부칙 제6조에 따라 개정되는 대통령령 중 이 영 시행 전에 공포되었으나 시행일이 도래하지 아니한 대통령령을 개정한 부분은 각각 해당 대통령령의 시행일부터 시행한다.

제2조부터 제5조까지 생략

제6조(다른 법령의 개정) ①부터 <86>까지 생략

<87> 정보통신기반 보호법 시행령 일부를 다음과 같이 개정한다.

제2조 각 호를 다음과 같이 한다.

1. 기획재정부차관
2. 미래창조과학부차관
3. 외교부차관
4. 법무부차관
5. 국방부차관
6. 안전행정부차관
7. 산업통상자원부차관
8. 보건복지부차관
9. 고용노동부차관
10. 국토교통부차관
11. 해양수산부차관
12. 국가정보원 차장
13. 금융위원회 부위원장
14. 방송통신위원회 상임위원

제3조제3항 중 "국무총리실"을 "국무조정실"로 한다.

제5조제2항 중 "행정안전부 제1차관"을 "미래창조과학부 제2차관"으로 한다.

제5조제6항 후단 중 ""국무총리실의 정보통신기반시설 보호 업무를 담당하는 고위공무원단에 속하는 공무원""을 ""국무조정실의 정보통신기반시설 보호 업무를 담당하는 고위공무원단에 속하는 공무원""으로 한다.

제9조의2제2항 각 호 외의 부분, 같은 항 제1호, 같은 조 제3항부터 제6항까지, 제9조의3제1항부터 제4항까지, 제10조제2항 전단, 제16조의2제1항부터 제4항까지 중 "행정안전부장관"을 각각 "미래창조과학부장관"으로 한다.

제24조제1항 각 호 외의 부분 중 "행정안전부령"을 "미래창조과학부령"으로 한다.

별표 2 나목의 기준란 중 "행정안전부령"을 "미래창조과학부령"으로 하고, 같은 표 라목의 기준란 및 같은 표의 비고 제2호 중 "행정안전부장관"을 각각 "미래창조과학부장관"으로 한다.

<88>부터 <129>까지 생략

부칙 <제25751호,2014.11.19>

제1조(시행일) 이 영은 공포한 날부터 시행한다. 다만, 부칙 제5조에 따라 개정되는 대통령령 중 이 영 시행 전에 공포되었으나 시행일이 도래하지 아니한 대통령령을 개정한 부분은 각각 해당 대통령령의 시행일부터 시행한다.

제2조부터 제4조까지 생략

제5조(다른 법령의 개정) ①부터 <41>까지 생략

<42> 정보통신기반 보호법 시행령 일부를 다음과 같이 개정한다.

제2조제6호를 다음과 같이 한다.

6. 행정자치부차관

<43>부터 <418>까지 생략

부칙 <제25840호,2014.12.9>

제1조(시행일) 이 영은 2015년 1월 1일부터 시행한다.

제2조부터 제16조까지 생략

부칙 <제26728호,2015.12.22>

제1조(시행일) 이 영은 2015년 12월 23일부터 시행한다.

제2조 생략

제3조(다른 법령의 개정) ① 생략

② 정보통신기반 보호법 시행령 일부를 다음과 같이 개정한다.

제12조제3호를 다음과 같이 한다.

3. 「정보보호산업의 진흥에 관한 법률」 제23조제1항제1호 및 제2호에 따라 지정된 정보보호 전문서비스 기업

③ 생략

[별표 1]

취약점 분석·평가 전담반 구성기준(제18조제1항관련)

구성원	역할 또는 경력·자격기준
반장(정보보호책임자)	취약점 분석·평가 시행의 총괄
관리기술 담당	관리적·물리적 정보보호등 조직의 정보보호관리체계의 관리·운영경력 소유자, 정보시스템 감리 경력자
메인프레임 담당	중형급이상의 컴퓨터 관리 경력자
응용프로그램 담당	해당기관의 주요정보통신기반시설에 대한 핵심 프로그램 개발·유지보수 경력자
서버 담당	유닉스, 리눅스, Windosw-NT등 각종 서버관련 기술 보유자
정보보호 담당	정보보호시스템 평가 및 운영자, 정보보호정책·위험분석 또는 취약점 점검·평가등의 보안관리기술 경력자
네트워크 담당	WAN, LAN, NMS 및 무선통신등에 관한 기술 및 각종 통신 프로토콜 기술 보유자

비 고 : 관리기관은 소관주요정보통신기반시설의 특성에 따라 전담반 구성요건을 고려하여야 취약점 분석·평가를 수행할 수 있는 적정인원의 전문인력을 확보하여야 한다.

[별표 2] <개정 2013.3.23>

취약점 분석·평가를 수행하는 정보공유·분석센터의 기준(제19조제1항관련)

항 목	기 준
가. 납입자본금	20억원이상
나. 기술인력의 수	미래창조과학부령으로 정하는 자격·학력 또는 경력을 가진 기술인력 15인이상(5인이상의 고급기술인력을 포함한다)
다. 시설 및 장비	- 신원확인 및 출입통제를 위한 설비 - 법 제17조제1항 각호의 업무를 수행하거나 지원하기 위한 설비 - 기록 및 자료의 안전관리를 위한 설비
라. 정보보호관리규정	- 업무수행구역 및 설비에 대한 보호대책 - 인원에 대한 보호대책(인사관리 및 교육훈련에 관한 사항을 포함한다) - 문서 및 전산자료에 대한 보호대책 - 그밖에 보안유지를 위하여 미래창조과학부장관이 필요하다고 인정하는 보호대책

비 고

1. 취약점 분석·평가를 수행하는 정보공유·분석센터의 장은 "라. 정보보호관리 규정"을 제정하고 이를 준수하여야 한다.
2. 취약점 분석·평가를 수행하는 정보공유·분석센터의 기준에 관한 세부적인 사항과 그 기준심사에 관하여 필요한 사항은 미래창조과학부장관이 정하여 고시한다.

[별표 3]

과태료의 부과기준(제25조 관련)

1. 일반기준

가. 위반행위의 횟수에 따른 과태료의 부과기준은 최근 3년간 같은 위반행위로 과태료를 부과받은 경우에 적용한다. 이 경우 위반행위에 대하여 과태료 부과처분을 한 날과 다시 같은 위반행위를 적발한 날을 각각 기준으로 하여 위반횟수를 계산한다.

나. 부과권자는 위반행위자가 다음의 어느 하나에 해당하는 경우에는 제2호에 따른 과태료 금액의 2분의 1의 범위에서 그 금액을 감경할 수 있다. 다만, 과태료를 체납하고 있는 위반행위자의 경우에는 그러하지 아니하다.

1) 위반행위자가 「질서위반행위규제법 시행령」 제2조의2제1항 각 호의 어느 하나에 해당하는 경우

2) 위반행위가 사소한 부주의나 오류로 인한 것으로 인정되는 경우

3) 위반행위자가 위법행위로 인한 결과를 시정하였거나 해소한 경우

4) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 감경할 필요가 있다고 인정되는 경우

다. 부과권자는 위반행위자가 다음의 어느 하나에 해당하는 경우에는 제2호에 따른 과태료 금액의 2분의 1의 범위에서 그 금액을 가중할 수 있다. 다만, 가중할 사유가 여러 개 있는 경우라도 법 제30조제1항에 따른 과태료 금액의 상한을 넘을 수 없다.

1) 위반의 내용·정도가 중대하여 소비자 등에게 미치는 피해가 크다고 인정되는 경우

2) 법 위반상태의 기간이 3개월 이상인 경우

3) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 가중할 필요가 있다고 인정되는 경우

2. 개별기준

위반행위	근거 법조문	과태료 금액(단위: 만원)		
		1차	2차	3차 이상
가. 법 제11조에 따른 보호조치 명령을 위반한 경우	법 제30조제1항제1호	200	500	1000
나. 법 제16조제2항에 따른 통지를 하지 않은 경우	법 제30조제1항제2호	200	500	1000

정보통신기반 보호법 시행규칙

[시행 2013.3.24] [미래창조과학부령 제00001호, 2013.3.24, 타법개정]

제1조(목적) 이 규칙은 정보통신기반보호법 및 동법시행령에서 위임된 사항과 그 시행에 관하여 필요한 사항을 규정함을 목적으로 한다.

제2조(정보공유·분석센터의 기술인력의 자격요건 등) ① 「정보통신기반 보호법 시행령」(이하 "영"이라 한다) 제19조제1항에 따른 영 별표 2 나목에서 "미래창조과학부령으로 정하는 자격·학력 또는 경력을 가진 기술인력"이란 별표의 자격기준을 갖춘 기술인력을 말한다. <개정 2013.3.23, 2013.3.24>

② 미래창조과학부장관은 제1항 및 별표에 따른 기술인력 중 고급기술인력으로서의 전문능력을 갖추었는지를 심사하기 위하여 필요한 경우에는 별표 비고의 제2호부터 제4호까지의 규정에 따른 정보통신 분야, 정보시스템 보안 분야 또는 특수 분야에 관한 학식과 경험이 풍부한 사람을 위원으로 하는 기술심의위원회를 구성·운영할 수 있다.<개정 2013.3.23, 2013.3.24> [전문개정 2011.4.6]

제3조(정보공유·분석센터 구축통지서) ①영 제24조제1항의 규정에 의하여 정보공유·분석센터 구축의 통지를 하고자 하는 자는 별지 제1호서식의 정보공유·분석센터구축통지서에 다음 각호의 서류를 첨부하여 관계중앙행정기관의 장에게 제출하여야 한다. <개정 2006.7.19>

1. 대표자 및 임원의 성명·주민등록번호·주소 및 경력 등의 인적사항이 기재된 서류
2. 조직운영규칙(법인인 경우에는 정관을 포함한다)
3. 업무를 외부에 위탁하는 경우 위탁 업무의 범위와 수탁기관에 관한 다음 각목의 사항이 기재된 서류
   가. 명칭
   나. 사무소의 소재지
   다. 대표자 및 임원의 성명·주민등록번호·주소·경력 등의 인적사항이 기재된 서류

②제1항에 따라 통지를 받은 담당공무원은 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 「출입국관리법」 제88조의2제1항에 따른 외국인등록사실증명(법인의 대표자 또는 임원이 외국인인 경우에 한한다)을 확인하여야 한다. 다만, 법인의 대표자 또는 임원이 확인에 동의하지 아니하는 경우에는 이를 첨부하도록 하여야 한다.<신설 2006.7.19, 2008.3.3, 2011.4.6>

제4조 삭제 <2011.4.6>

제5조 삭제 <2011.4.6>

제6조 삭제 <2011.4.6>

제7조 삭제 <2011.4.6>

제8조 삭제 <2011.4.6>

제9조 삭제 <2011.4.6>

제10조 삭제 <2011.4.6>

제11조 삭제 <2011.4.6>

제12조 삭제 <2011.4.6>

제13조 삭제 <2011.4.6>

부칙 <제115호,2001.8.4>

이 규칙은 공포한 날부터 시행한다.

부칙 <제140호,2003.6.23>

이 규칙은 공포한 날부터 시행한다.

부칙 <제151호,2004.7.6>(전자적민원처리를위한별정우체국법시행규칙등중개정령)

이 규칙은 공포한 날부터 시행한다.

부칙 <제200호,2006.7.19>(행정정보의 공동이용 및 문서감축을 위한 우편대체법 시행규칙 등 일부개정령)

이 규칙은 공포한 날부터 시행한다.

부칙 <제1호,2008.3.3>(지식경제부와 그 소속기관 직제 시행규칙)

제1조(시행일) 이 규칙은 공포한 날부터 시행한다.

제2조부터 제4조까지 생략

제5조(다른 법령의 개정) ① 부터 <52> 까지 생략

<53> 정보통신기반보호법시행규칙 일부를 다음과 같이 개정한다.

제4조, 제5조제1항 본문、제9호, 제6조제1항、제2항、제3항、제4항 각 호 외의 부분, 제7조제1항제4호 전단 및 후단, 제7조제1항제5호라목, 제7조제2항、제3항、제4항, 제9조제1항 각 호 외의 부분、제2항, 제10조 각 호 외의 부분 중 "정보통신부장관"을 각각 "지식경제부장관"으로 한다.

제3조제2항, 별지 제1호서식, 별지 제2호서식 중 "전자정부구현을 위한 행정업무 등의 전자화촉진에 관한 법률"을 각각 "「전자정부법」"으로 한다.

제2조 중 "정보통신부령"을 "지식경제부령"으로 한다.

별표 1의 비고란 제1호 중 "정보통신부장관을"을 "지식경제부장관 또는 방송통신위원회를"로, "정보통신부장관이"를 "지식경제부장관 또는 방송통신위원회가"로 하고, 같은 란 제2호부터 제7호까지 중 "정보통신부장관이"를 각각 "지식경제부장관 또는 방송통신위원회가"로 한다.

별표 2의 비고란 제1호、제2호 및 제4호 중 "정보통신부장관"을 각각 "지식경제부장관"으로 한다.

별지 제2호서식 앞쪽, 별지 제3호서식, 별지 제4호서식, 별지 제5호서식, 별지 제6호서식 중 "정보통신부장관"을 각각 "지식경제부장관"으로 한다.

별지 제2호서식 뒤쪽 중 "정보통신부"를 "지식경제부"로 한다.

별지 3호서식 중 "정보통신부장관"을 "지식경제부장관"으로 하고, 같은 서식 그림 부분 중 "정통"을 "지식경제"로 한다.

<54> 부터 <64> 까지 생략

부칙 <제209호,2011.4.6>

이 규칙은 공포 후 3개월이 경과한 날부터 시행한다.

부칙 <제297호,2012.5.31>

제1조(시행일) 이 규칙은 공포한 날부터 시행한다.

제2조(서식 개정에 관한 경과조치) 이 규칙 시행 당시 종전의 규정에 따른 서식은 2012년 8월 31일까지 이 규칙에 따른 서식과 함께 사용할 수 있다.

부칙 <제1호,2013.3.23>

제1조(시행일) 이 규칙은 공포한 날부터 시행한다.

제2조부터 제4조까지 생략

제5조(다른 법령의 개정) ①부터 <24>까지 생략

<25> 정보통신기반 보호법 시행규칙 일부를 다음과 같이 개정한다.

제2조제1항 중 "행정안전부령"을 "미래창조과학부령"으로 하고, 같은 조 제2항 중 "행정안전부장관"을 "미래창조과학부장관"으로 한다.

별표의 비고 제1호가목 중 "지식경제부장관 또는 방송통신위원회 위원장"을 "산업통상자원부장관 또는 미래창조과학부장관"으로 하고, 같은 호 나목, 같은 비고 제2호·제3호, 같은 비고 제4호라목 및 같은 비고 제5호·제6호·제7호 중 "행정안전부장관"을 각각 "미래창조과학부장관"으로 한다.

<26>부터 <51>까지 생략

부칙 <제1호,2013.3.24>

제1조(시행일) 이 규칙은 공포한 날부터 시행한다.

제2조부터 제5조까지 생략

제6조(다른 법령의 개정) ①부터 <30>까지 생략

<31> 정보통신기반 보호법 시행규칙 일부를 다음과 같이 개정한다.

제2조제1항 중 "행정안전부령"을 "미래창조과학부령"으로 하고, 같은 조 제2항 중 "행정안전부장관"을 "미래창조과학부장관"으로 한다.

별표 비고 제1호가목 중 "지식경제부장관"을 "산업통상자원부장관"으로, "방송통신위원회 위원장"을 "미래창조과학부장관"으로 하고, 같은 호 나목, 같은 표 비고 제2호·제3호, 같은 표 비고 제4호라목 및 같은 표 비고 제5호부터 제7호까지 중 "행정안전부장관"을 각각 "미래창조과학부장관"으로 한다.

[별표] <개정 2013.3.24>

기술인력의 자격기준(제2조제1항 관련)

구분	관련 자격 또는 관련 학력을 보유한 사람	관련 자격 또는 관련 학력을 보유하지 않은 사람
일반 기술 인력	1. 학사 이상의 학위를 취득한 사람 2. 기사 이상의 자격을 취득한 사람 3. 전문대학을 졸업한 후 2년 이상의 정보통신 관련 경력이 있는 사람 4. 산업기사의 자격을 취득한 후 2년 이상의 정보통신 관련 경력이 있는 사람 5. 기능사의 자격을 취득한 후 4년 이상의 정보통신 관련 경력이 있는 사람	1. 학사 이상의 학위를 취득한 후 2년 이상의 정보통신 관련 경력이 있는 사람 2. 전문대학을 졸업한 후 4년 이상의 정보통신 관련 경력이 있는 사람
고급 기술 인력	1. 2년 이상의 정보보호 관련 경력이 있고 박사학위를 취득한 사람 2. 2년 이상의 정보보호 관련 경력이 있고 기술사의 자격을 취득한 사람 3. 2년 이상의 정보통신 관련 경력과 3년 이상의 정보보호 관련 경력이 있고 석사학위를 취득한 사람 4. 학사학위를 취득한 후 4년 이상의 정보통신 관련 경력과 3년 이상의 정보보호 관련 경력이 있는	1. 학사 이상의 학위를 취득한 후 6년 이상의 정보통신 관련 경력과 3년 이상의 정보보호 관련 경력이 있는 사람 2. 전문대학을 졸업한 후 8년 이상의 정보통신 관련 경력과 4년 이상의 정보보호 관련 경력이 있는 사람

6. 기사의 자격을 취득한 후 4년 이상의 정보통신 관련 경력과 3년 이상의 정보보호 관련 경력이 있는 사람	

다음 각 호의 사람은 관련 자격 또는 관련 학력의 보유 여부와 관계 없이 고급기술인력으로 인정한다.

1. 2년 이상의 정보보호 관련 경력이 있고 변호사 또는 공인회계사의 자격을 취득한 사람
2. 3년 이상의 정보보호 관련 경력이 있고 정보보호 관련 분야 국내외 자격을 취득한 사람
3. 3년 이상의 정보보호 관련 경력이 있고 특수 분야 경력자에 해당하는 사람(특수 분야 경력과 정보보호 관련 경력은 중복하여 인정되지 않는다)
4. 제2조제2항에 따른 기술심의위원회가 다음 각 목의 어느 하나에 해당하는 사람 가운데 고급기술인력으로서의 전문능력을 갖추고 있다고 인정하는 사람
   가. 최근 3년간 과제책임자로서 계약금액 1억원 이상의 정보보호 컨설팅 수행실적이 2건 이상 있는 사람
   나. 학사 이상의 학위(정보통신 관련 학과의 학위만 해당한다)를 취득한 후 3년 이상의 정보보호 관련 경력이 있는 사람으로서 최근 3년간 다음 중 어느 하나의 실적이 있는 사람
      1) 계약금액 1억원 이상의 정보보호 컨설팅 수행실적 2건 이상
      2) 계약금액 2천만원 이상의 정보보호 컨설팅 수행실적 5건 이상

비 고

1. "관련 자격 또는 관련 학력을 보유한 사람"이란 다음 각 목의 어느 하나에

다. 그 밖에 관계 법령에 따라 국내 또는 외국에서 나목과 같은 수준이나 그 이상의 수준으로 인정되는 학력을 가진 사람

2. "정보통신 관련 경력"이란 공공기관, 민간기업, 교육기관 등에서 미래창조과학부장관이 인정하는 정보통신 분야의 업무를 수행한 기간을 말한다.
3. "정보보호 관련 경력"이란 공공기관, 민간기업, 교육기관 등에서 미래창조과학부장관이 인정하는 정보시스템 보안 분야의 업무를 수행한 기간을 말한다.
4. "특수 분야 경력자"란 학사 이상의 학위를 취득한 후 다음 각 목의 어느 하나에 해당하는 분야의 업무에 3년 이상 종사하였음을 관계 서류의 제출을 통하여 증명할 수 있는 사람을 말한다.
   가. 대형컴퓨터시스템 분야
   나. 산업용 전자제어시스템 분야
   다. 초고속정보통신망 분야
   라. 그 밖에 미래창조과학부장관이 인정하는 특수 분야
5. "정보보호 컨설팅 수행실적"이란 공공기관, 민간기업, 교육기관 등의 정보시스템 보안에 대하여 해당 기술인력이 프로젝트 참여비율 50%이상(위 별표의 관련 자격 또는 관련 학력의 보유 여부와 관계 없이 인정되는 고급기술인력란 제4호가목의 경우에는 그러하지 아니하다)으로 직접 수행한 컨설팅용역으로서 미래창조과학부장관이 인정하는 실적(지정을 신청한 날 현재 용역 수행이 끝난 실적만 해당한다)을 말한다.
6. "정보보호 관련 분야 국내외 자격"이란 정보보호와 밀접한 관계가 있는 국내 또는 외국의 기술자격으로서 미래창조과학부장관이 정하는 자격을 말한다.
7. 위 별표 각 호의 요건에서 고급기술인력에 관한 정보통신 관련 경력, 정보보호 관련 경력, 특수 분야 경력 및 정보보호 컨설팅 수행실적의 확인은 미래창조과학부장관이 정하는 바에 따른다.
8. 위 별표 각 호의 요건에서 정보통신 관련 경력과 정보보호 관련 경력은 서로 중복하여 인정되지 않는다. 다만, 정보통신 관련 경력이 부족한 경우에는

되, 그 인정 방법 및 기준에 관하여는 위 별표의 규정을 준용한다.

■ 정보통신기반 보호법 시행규칙 [별지 제1호서식] <개정 2012.5.31>

정보공유·분석센터구축통지서

접수번호	접수일자	처리기간 즉시

명칭		
사무소 소재지		
대표자	성명	생년월일
	주소	경력
주요 업무		
재원조달방식		

「정보통신기반 보호법」 제16조, 같은 법 시행령 제24조 및 같은 법 시행규칙 제3조에 따라 위와 같이 통지합니다.

년 월 일

통지인 (서명 또는 인)

귀하

첨부서류		
통지인 제출서류	1. 대표자 및 임원의 성명, 생년월일, 주소 및 경력 등의 인적사항이 기록된 서류 2. 조직운영규칙 1부(법인인 경우에는 정관을 포함합니다) 3. 업무를 외부에 위탁하는 경우 위탁 업무의 범위와 수탁기관에 관한 다음 각 목의 사항이 기록된 서류 가. 명칭 나. 사무소의 소재지 다. 대표자 및 임원의 성명·생년월일·주소·경력 등의 인적사항이 기록된 서류	수수료 없음
담당 공무원 확인사항	「출입국관리법」 제88조의2제1항에 따른 외국인등록사실증명(법인의 대표자 및 임원이 외국인인 경우에만 해당합니다)	

행정정보 공동이용 동의서
본인은 이 건 업무처리와 관련하여 담당 공무원이 「전자정부법」 제36조에 따른 행정정보의 공동이용을 통하여 위의 담당 공무원

[별지 제2호 서식] 삭제 <2011.4.6>

[별지 제3호 서식] 삭제 <2011.4.6>

[별지 제4호 서식] 삭제 <2011.4.6>

[별지 제5호 서식] 삭제 <2011.4.6>

[별지 제6호 서식] 삭제 <2011.4.6>

신용정보법

1. 신용정보업감독규정
2. 신용정보업감독규정
3. 신용정보업감독업무시행세칙
4. 신용정보업감독업무시행세칙
5. 신용정보의 이용 및 보호에 관한 법률
6. 신용정보의 이용 및 보호에 관한 법률 시행령
7. 신용정보의 이용 및 보호에 관한 법률 시행규칙

신용정보업감독규정

[시행 2016.10.20] [고시 제2016 - 40호, 2016.10.20, 일부개정]

제1조(목적) 이 규정은「신용정보의 이용 및 보호에 관한 법률」, 같은 법 시행령 및 같은 법 시행규칙에서 정하는 금융위원회 소관사항의 시행에 필요한 사항을 정함을 목적으로 한다.

제2조(정의) 이 규정에서 사용하는 용어의 정의는「신용정보의 이용 및 보호에 관한 법률」(이하 "법"이라 한다), 같은 법 시행령(이하 "영"이라 한다) 및 같은 법 시행규칙(이하 "규칙"이라 한다)에서 정하는 바에 따른다.

제2조의2(신용정보의 범위) ① 영 제2조제1항제5호자목에서 "금융위원회가 정하여 고시하는 정보"는 다음 각 호의 정보를 말한다.

1. 법 제20조에 따라 신용조회회사가 기록을 보존하는 정보 중에서 신용정보주체의 신용도 판단에 이용되는 정보를 제3자에게 제공한 신용조회기록
2. 한국자산관리공사의 신용회복지원 관련 규정에 의한 채무재조정 약정정보
3. 신용회복위원회의 신용회복지원협약에 따른 신용회복지원 확정정보

② 영 제2조제1항제5호차목에서 "금융위원회가 정하여 고시하는 정보"란 국민행복기금이 협약금융기관등으로부터 채권을 매입한 정보 및 채무조정 약정을 체결한 정보를 말한다.

③ 영 제2조제1항제5호카목에서 "금융위원회가 정하여 고시하는 정보"란 신용정보주체의 신용정보를 종합적으로 평가·반영하여 생성한 개인신용평점 또는 개인신용등급 등을 말한다.

④ 영 제2조제1항제5호타목에서 "금융위원회가 정하여 고시하는 정보"란 기업 및 법인인 신용정보주체의 신용을 판단하기 위하여 신용정보를 활용함으로써 그 판단의 결과를 기호, 숫자 등을 사용하여 평점 또는 등급으로 표시한 정보를 말한다.

⑤ 영 제2조제1항제5호파목에서 "금융위원회가 정하여 고시하는 정보"란 기업 및 법인인 신용정보주체의 신용을 판단하기 위하여 기술평가(「기술신용보증기금법」제28조제1항제6호의 기술평가를 말한다)를 하고 신용정보와 해당 기업 및 법인의 기술에 관한 정보를 활용함으로써 그 판단의 결과를 기호, 숫자 등을 사용하여 평점 또는 등급으로 표시한 정보, 그 기술의 가액 또는 평가의견 등을 말한다.

제3조(신용정보제공·이용자의 범위) 영 제2조제3항에서 "그 밖에 금융위원회가 정하여 고시하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다. <개정 2016.9.21.>

1.「서민의 금융생활 지원에 관한 법률」 제3조에 따른 서민금융진흥원 및 같은 법 제26조에 따른 사업수행기관
2.「서민의 금융생활 지원에 관한 법률」 제56조에 따른 신용회복위원회
3.「상법」에 따라 설립된 주식회사 국민행복기금

제4조(신용정보업에 딸린 업무) 영 제3조제3호에 따른 "그 밖에 금융위원회가 정하여 고시하는 업무"란 다음 각 호의 업무를 말한다. 다만, 신용조사업에 딸린 업무는 제1호부터 제3호까지의 규정에 한정한다.

1. 사업장현황조사 업무
2. 민원서류 열람 및 교부신청 업무
3. 해당 업무를 영위하는 과정에서 발생하는 교육, 홍보, 출판업무
4. 채권자등에 대한 채권관리관련 업무
5. 기한 전 채무납입 안내 대행업무
6. 연체 전 채권의 변제청구 및 통지등에 대한 대행 업무
7. 「자산유동화에 관한 법률」제10조에 따른 자산관리업무

제5조(신용정보업 허가 등의 절차) ① 다음 각 호에 따른 절차는 별표 1과 같다.

1. 법 제4조에 따른 신용정보업 허가
2. 법 제10조에 따른 신용정보업의 양도、양수、분할、합병(분할합병을 포함한다. 이하 같다) 등의 인가
3. 법 제25조에 따른 신용정보집중기관의 허가

② 다음 각 호에 따른 허가 등을 신청하려는 자(이하 "신청인"이라 한다)는 다음 각 호에서 각각 정하는 서식 및 별표 1의2에 따른 신청서류를 제출하여야 한다.

1. 영 제4조에 따라 신용정보업의 허가를 받으려는 신청인: 별지 제1호 서식
2. 영 제4조에 따라 신용정보업 의 허가받은 사항에 대한 변경허가를 받으려는 신청인: 별지 제2호 서식
3. 법 제10조제1항에 따라 신용정보업의 양도、양수、분할、합병 인가를 받으려는 신청인: 별지 제2호의2 서식
4. 영 제21조제1항에 따라 신용정보집중기관으로 허가를 받으려는 신청인: 별지 제2호의3 서식

③「금융위원회의 설치 등에 관한 법률」제24조에 따른 금융감독원의 원장(이하 "금융감독원장"이라 한다)은 제2항에 따른 신청내용의 사실여부를 확인하고 이해관계인 등으로부터 제출된 의견을 고려하여 신청내용이 법 제6조 및 영 제6조에 따른 허가기준, 영 제10조제1항 각 호에 따른 인가기준, 법 제25조제3항 각 호에 따른 허가기준을 충족하는지 심사한다.

④ 금융감독원장은 신청내용을 확인하기 위하여 필요한 경우에는 이해관계인, 발기인 또는 임원과의 면담 등의 방법으로 실지조사를 할 수 있으며, 신청인은 이에 적극 협조하여야 한다.

⑤ 금융위원회는 신청인에게 3개월 이내(예비허가 또는 예비인가를 받은 경우에는 1개월 이내)에 허가 또는 인가 여부를 결정하고, 그 결과와 이유를 지체 없이 신청인에게 문서로 통지하여야 한다. 이 경우 신청서에 흠결이 있을 때에는 보완을 요구할 수 있다.

⑥ 제5항 전단에 따른 심사기간을 산정할 때에는 다음 각 호의 어느 하나에 해당하는 기간은 심사기간에 산입하지 아니한다.

1. 법 제6조 및 영 제6조에 따른 허가기준, 영 제10조제1항 각 호에 따른 인가기준 또는 법 제25조제3항 각 호에 따른 허가기준을 충족하는지를 확인하기 위하여 다른 기관 등으로부터 필요한 자료를 제공받는 데에 걸리는 기간
2. 제5항 후단에 따라 신청서 흠결의 보완을 요구한 경우에는 그 보완기간
3. 신청인을 상대로 형사소송 절차가 진행되고 있거나 금융위원회, 공정거래위원회, 국세청 또는 금융감독원 등(외국기업인 경우에는 이들에 준하는 본국의 감독기관 등을 포함한다)에 의한 조사·검사 등의 절차가 진행되고 있고, 그 소송이나 조사·검사 등의 내용이 승인심사에 중대한 영향을 미칠 수 있다고 인정되는 경우에는 그 소송이나 조사·검사 등의 절차가 끝날 때까지의 기간

⑦ 금융위원회는 허가 또는 인가의 조건을 붙일 수 있다.

⑧ 금융위원회는 제7항에 따라 조건을 붙인 경우에는 금융감독원장으로 하여금 그 이행여부를 확인하도록 하여야 한다.

⑨ 신청인은 제2항에 따른 신청을 하기 전에 금융위원회에 예비허가 또는 예비인가를 신청할 수 있다.

⑩ 금융위원회는 제9항에 따른 예비허가 또는 예비인가 신청을 받은 경우에는 2개월 이내에 예비허가 또는 예비인가 여부를 결정하여 그 결과와 이유를 지체 없이 신청인에게 문서로 통지하여야 한다. 이 경우 예비허가 또는 예비인가 신청에 관하여 흠결이 있는 경우에는 보완을 요구할 수 있다.

⑪ 예비허가 신청 및 심사 절차는 제2항부터 제8항까지의 규정을 준용한다. 이 경우 "허가" 또는 "인가"는 각각 "예비허가" 또는 "예비인가"로 본다.

⑫ 제1항부터 제11항까지의 규정에 따른 허가 또는 인가절차를 위해 그 밖에 필요한 사항은 금융감독원장이 정한다.

제6조(정보처리·정보통신설비) ① 영 제6조제1항제1호나목에서 "금융위원회가 정하여 고시하는 정보처리·정보통신설비"란 해당 신용조회업무의 범위와 규모에 비추어 신용정보를 원활히 처리할 수 있는 수준의 정보처리·정보통신설비로서 별표 2에 규정된 사항을 말한다.

② 삭제<2014.4.22.>

제7조(사실상의 영향력을 행사하는 주주 또는 출자자) 금융위원회는 신용정보회사 및 그 주주에 대하여 당해 신용정보회사의 주주가 영 6조제3항제5호나목에 해당하는지 여부를 확인하는데 필요한 자료의 제출을 요구할 수 있다.

제8조(주요출자자 요건) 영 제6조제4항 [별표1]제1호라목3)에서 "그 밖에 금융위원회가 정하는 건전한 금융거래질서를 해친 사실이 없을 것"이란 주요출자자가 최대주주로서 금융기관인 경우 최근 1년간 기관경고 조치 또는 최근 3년간 시정명령이나 업무정지 이상의 조치를 받은 사실이 없는 경우(기관경고를 받은 후 최대주주 및 그 특수관계인인 주주 전체가 변경된 경우 또는 금융산업의 신속한 구조개선을 지원할 필요가 있거나 조치를 받은 사실이 영위하고자 하는 업무의 건전한 영위를 어렵게 한다고 볼 수 없는 경우 제외)를 말하며 주요출자자가 금융회사의 임직원(전직 포함)인 경우 최근 3년간 금융위원회로부터 직무정지 또는 정직이상의 조치를 받은 사실이 없는 경우를 말한다.

제9조(자본금 또는 기본재산 감소의 신고) ① 신용정보회사가 영 제8조제1항 각 호의 사항을 신고하려는 경우에는 별지 제3호 서식에 따라 신고하여야 한다.

② 영 제8조제1항제1호에서 정하는 신고가 있는 경우에는 다음 각 호에서 정하는 기준에 적합한지 여부를 심사한다.

1. 자본금 또는 기본재산의 감소의 불가피성이 인정될 것
2. 신용정보주체 및 채권자의 권익과 신용정보 보호에 지장을 줄 염려가 없을 것

③ 영 제8조제1항제2호에서 정하는 신고가 있는 경우에는 다음 각 호에서 정하는 기준에 적합한지 여부를 심사한다.

1. 회사의 건전한 경영을 저해하지 아니할 것
2. 법 및 다른 법령을 위반하지 아니할 것

제10조(경미한 사항의 보고) 신용정보회사가 영 제8조제2항 각 호의 어느 하나에 해당하는 사항을 보고하려는 경우에는 별지 제4호 서식에 따라 보고하여야 한다.

제11조(지배주주승인신청서 등) ① 법 제9조제1항에 따른 지배주주가 되고자 하는 자는 별지 제5호 서식에 따른 승인신청서(첨부서류를 포함한다)를 금융위원회에 제출하여야 한다.

② 법 제9조제1항에 따른 금융위원회 승인의 효력은 신용정보회사의 지배주주가 되고자 하는 자가 승인을 받은 날로부터 6개월 이내에 당해 신용정보회사의 주식을 취득하지 아니하는 경우에는 소멸한다. 다만, 금융위원회의 승인 당시 주식취득기한을 따로 정하였거나 승인 후 주식취득기한의 연장에 대하여 금융위원회의 승인을 받은 경우에는 그 기간을 달리 정할 수 있다.

③ 신용정보회사의 지배주주가 되고자 하는 자가 법 제9조제1항에 따라 승인을 받은 후 주식을 취득한 때에는 그 사실을 10일 이내에 금융위원회에 보고하고 당해 신용정보회사에 통보하여야 한다.

④ 합병 신주를 교부받아 신용정보회사의 지배주주가 되는 경우에는 법 제9조제1항에 따라 신용정보회사의 주식을 취득하여 지배주주가 되려는 경우로 보지 아니한다.

⑤ 영 제9조제6항에서 "금융위원회가 정하는 기간"이란 다음 각 호의 어느 하나에 해당하는 기간을 말한다.

1. 영 제9조제2항에 따른 승인요건을 충족하는지 확인하기 위하여 다른 기관 등으로부터 필요한 자료를 제공받는 데에 걸리는 기간
2. 영 제9조제5항 후단에 따라 승인신청서의 흠결의 보완을 요구한 경우에는 그 보완기간
3. 승인을 받으려는 자를 상대로 형사소송 절차가 진행되고 있거나 금융위원회, 공정거래위원회, 국세청 또는 금융감독원 등(외국기업인 경우에는 이들에 준하는 본국의 감독기관 등을 포함한다)에 의한 조사·검사 등의 절차가 진행되고 있고, 그 소송이나 조사·검사 등의 내용이 승인심사에 중대한 영향을 미칠 수 있다고 인정되는 경우에는 그 소송이나 조사·검사 등의 절차가 끝날 때까지의 기간

제11조의2(신용정보업의 양도·양수 등의 인가의 세부요건) 영 제10조제1항 각 호에 따른 인가의 세부요건은 별표 2의2와 같다.

제12조(휴업 또는 폐업의 신고) 규칙 제4조에 따른 휴업·폐업신고서는 별지 제6호 서식에 따른다.

제13조(겸업신고 등) ① 금융감독원장은 법 제11조제1항에 따라 신용정보회사가 겸업신고를 한 경우에는 규칙 제5조제1항에 따른 요건에 적합한지 여부를 심사하여 수리한다.

② 규칙 제5조제1항에 따라 겸업신고를 하려는 자는 별지 제7호 서식에 따른 신청서를 제출하여야 한다.

제13조의2(신용조회회사에 조사·분석 등을 의뢰할 수 있는 공공단체의 범위) ① 영 제11조의2제2호에서 "금융위원회가 정하여 고시하는 기관"이란 다음 각 호의 어느 하나에 해당하는 기관을 말한다.

1. 국가나 지방자치단체가 납입자본금을 출자한 법인
2. 국가나 지방자치단체가 출연한 기관
3. 「보조금 관리에 관한 법률」 제9조 또는 「지방재정법」 제17조제1항 각 호 외의 부분 단서에 따라 국가나 지방자치단체로부터 연간 5천만원 이상의 보조금을 받는 기관 또는 단체
4. 그 밖에 다른 법률에 따라 국가나 지방자치단체로부터 투자·출자·출연을 받는 기관 또는 단체

② 영 제11조의2제9호에서 "금융위원회가 정하여 고시하는 기관"이란 다음 각 호의 어느 하나에 해당하는 기관을 말한다.

1. 「지방공기업법」 제2조에 따른 지방직영기업 및 같은 법 제76조에 따른 지방공단
2. 「공직자윤리법」 제3조제1항제12호에 따른 공직유관단체

③ 금융위원회는 법 제11조제2항 단서에 따라 신용조회회사가 승인을 신청한 내용이 규칙 제5조제2항에 따른 요건에 적합한지 여부를 심사하여 승인한다.

④ 법 제11조제2항 단서에 따라 승인을 신청하려는 자는 별지 제7호의2 서식에 따른 신청서를 제출하여야 한다.

제14조(임원의 겸직 금지) ① 법 제13조에 따라 신용정보회사의 상임임원의 겸직승인 신청이 있는 경우에는 다음 각 호에서 정하는 기준에 적합한지 여부를 심사하여 승인한다.

1. 상임임원의 겸직이 관련법규에 저촉되지 않을 것
2. 상임임원의 겸직이 당해 신용정보회사 및 관련회사의 경영합리화 또는 구조조정의 원활한 추진 등을 위해 불가피할 것

② 제1항에 따라 겸직승인 신청을 하는 경우에는 별지 제8호 서식에 따른 신청서를 제출하여야 한다.

제15조(수집된 신용정보의 처리의 위탁) ① 영 제14조제2항에 따른 "금융위원회가 정하여 고시하는 자"란 영 제5조제1항제1호부터 제21호까지의 규정에 따른 금융기관을 말한다.

② 영 제14조제4항제1호에서 "금융위원회가 정하여 고시하는 절차와 방법에 따른 보안서버의 구축 또는 암호화"란 별표 3의 Ⅱ. 3.의 보호조치를 말한다.

③ 법 제17조제7항에서 "금융위원회가 인정하는 경우"란 다음 각 호의 어느 하나에 해당하지 않는 경우를 말한다.

1. 관련 법령에서 해당 업무의 위탁을 금지하고 있는 경우
2. 재위탁자 또는 재수탁자가 최근 3년 이내에 신용정보주체의 정보관리, 감독관련 자료 제출 등 감독기관의 검사와 관련한 사항으로 기관경고 이상의 제재 또는 형사처벌을 2회 이상 받은 사실이 있는 경우
3. 그 밖에 재위탁으로 인하여 재위탁자의 건전성 또는 신인도를 크게 저해하거나, 금융질서의 문란 또는 신용정보주체의 피해 발생이 심히 우려되는 경우

④ 수탁자가 전항에 따라 신용정보의 처리를 재위탁하는 경우 별표 4 중 재위탁에 관한 신용정보 보안관리 대책에 관한 사항을 재위탁계약의 내용에 포함하여야 한다.

⑤ 신용정보처리 위탁에 관한 사항은 법, 영, 이 규정이 정한 사항을 제외하고 「금융회사의 정보처리 업무 위탁에 관한 규정(이하 "위탁규정"이라 한다)」을 준용한다. 이 경우 위탁규정 제2조제1항에 따른 "금융회사"는 "신용정보회사등"으로 본다.

⑥ 제1항의 자가 수탁자가 영 제14조제1항의 요건을 갖추었음을 확인할 수 있는 서류를 첨부하여 위탁규정 제7조에 따라 금융감독원에 보고한 경우에는 법 제17조제3항에 따라 금융위원회에 알린 것으로 본다.

제16조(정확성 확인을 위한 자료제출 요구) 신용정보집중기관 및 신용조회회사는 영 제15조제2항에 따라 등록되는 신용정보의 정확성을 점검하기 위하여 신용정보를 등록한 자에게 정확성 여부를 입증할 수 있는 자료의 제출을 요청할 수 있다.

제17조(신용조회회사등의 신용정보 등록·변경·관리) ① 신용정보집중기관 및 신용조회회사는 영 제2조제1항의 신용정보별로 등록·변경·관리 기준을 마련한다.

② 신용정보집중기관 및 신용조회회사가 영 제15조제2항에 따라 등록되는 신용정보의 정확성과 최신성을 점검할 수 있는 기준 및 절차를 마련하는 경우에는 다음 각 호의 사항이 포함되어야 한다.

1. 신용정보를 등록하는 자의 선별기준(신용조회회사만 해당한다)
2. 신용정보를 등록하는 자별 정보 등록 방식에 관한 사항
3. 사실과 다른 정보 또는 제18조 각 호의 기간이 만료된 정보의 등록시 제재에 관련한 사항

③ 신용정보집중기관 및 신용조회회사는 신용정보 이용자가 조회한 목적에 일치하는 조회사유코드를 입력하도록 하는 등 신용조회기록의 정확성 점검에 관한 사항을 마련하여야 한다.

제18조(오래된 신용정보의 등록 금지) 신용정보제공·이용자는 어음 부도거래정보를 제외한 영 제2조제1항제3호의 정보를 다음 각 호에서 정한 기간이 만료된 이후에는 신용정보집중기관 또는 신용조회회사에 등록할 수 없다.

1. 등록사유 발생일로부터 7년
2. 채권관련정보는 소멸시효가 완성된 날

제18조의2(불이익 정보의 범위) 영 제15조제4항제6호에서 "금융위원회가 정하여 고시하는 신용정보"란 제2조의2제1항제2호·제3호 및 같은 조 제2항의 신용정보를 말한다.

제19조(오래된 신용정보의 삭제) ① 영 제15조제6항에 따른 신용정보의 삭제방법은 신용정보주체에게 불이익을 초래하게 된 사유가 해소된 날(이하 '해제사유 발생일'이라 한다) 또는 등록사유 발생일로부터 제2항 각 호에 따른 기간 내에 신용정보집중기관 및 신용조회회사의 등록·관리 대상에서 삭제하는 것을 말한다.

② 영 제15조제6항에 따라 신용정보를 등록·관리대상에서 삭제하는 기준 및 절차는 다음 각 호와 같다.

1. 영 제15조제4항제1호, 제4호 및 제5호의 신용정보는 변제 또는 납부하지 아니한 기간 이내로 하되 해제사유 발생일로부터 최장 1년 이내. 다만 신용정보집중기관 및 신용조회회사가 분쟁의 입증자료 또는 정책자료로 활용하기 위해 관리하는 경우 및 신용조회회사가 신용등급의 산정 또는 신용정보를 가공하여 제공하기 위해 관리하는 경우에는 해제사유 발생일로부터 최장 5년 이내
2. 영 제15조제4항제2호의 신용정보는 해제 사유 발생일로부터 최장 5년 이내
3. 영 제15조제4항제3호 및 제6호의 신용정보는 등록사유 발생일로부터 최장 5년 이내

③ 신용정보집중기관 또는 신용조회회사에 등록되는 어음부도거래정보를 제외한 제2항제1호 및 제2호의 신용정보는 그 불이익을 초래하게 된 사유가 해소되지 않고 등록사유 발생일로부터 7년이 경과한 경우에는 그 날을 당해 정보의 해제사유 발생일로 본다.

④ 신용정보제공·이용자 및 신용조회회사가 신용정보집중기관으로부터 입수하여 활용하는 제2항의 신용정보의 관리기간은 당해 신용정보를 제공한 신용정보집중기관이 정하는 관리기간을 따른다. 다만 신용조회회사가 제2항제1호 및 제2호의 신용정보를 신용등급을 산정하거나 가공하여 제공하기 위해 관리하는 경우에는 관리기간을 해제사유 발생일로부터 최장 5년 이내로 한다.

제20조(기술적·물리적·관리적 보안대책) 영 제16조제2항에 따라 신용정보회사등이 마련해야 할 기술적·물리적·관리적 보안대책의 구체적인 기준은 별표 3과 같다.

제21조(보안관리약정 체결) 신용정보제공·이용자가 다른 신용정보제공·이용자 또는 신용조회회사와 서로 개인신용정보를 제공하는 경우에는 법 제19조제2항에 따라 별표 4의 신용정보 보안관리 대책을 포함한 계약을 체결하여야 한다.

제22조(내부관리규정의 마련) ① 법 제20조제1항에 따른 신용정보관리기준은 별표 4의2와 같다.

② 신용정보회사등은 제1항에 따른 신용정보관리기준의 준수 및 이행을 위해 신용정보회사등의 특성 등을 반영하여 내부관리규정을 구체적이고 상세하게 마련하여야 한다.

③ 제1항 및 제2항에도 불구하고 신용정보회사등은 신용정보회사등의 특성 등에 따라 특별한 사정이 있는 경우 제1항에 따른 신용정보관리기준과 달리 내부관리규정을 마련하여 준수할 수 있다. 다만, 이 경우에도 법, 영, 규칙 및 이 규정을 위반하여서는 아니 된다.

④ 제3항에 따라 신용정보회사등이 내부관리규정을 제1항의 신용정보관리기준과 달리 마련하는 경우 같은 항에 따른 그 특별한 사정을 내부관리규정에서 명확히 설명하여야 한다.

⑤ 금융위원회는 제3항에 따라 마련한 내부관리규정이 신용정보 및 신용정보주체의 권익 보호에 적합하지 않다고 판단할 경우 시정을 명할 수 있다.

제22조의2(신용정보관리·보호인의 지정대상 등) ① 영 제17조제2항제3호 후단에 따라 상시 종업원 수를 산정하는 경우「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자의 수로 한다.

② 법 제25조제2항제1호에 따른 종합신용정보집중기관(이하 "종합신용정보집중기관"이라 한다)의 신용정보관리·보호인은 법 제20조제5항에 따라 보고서를 대표자 및 이사회에 보고하기 전에 법 제26조제1항에 따른 신용정보집중관리위원회(이하 "신용정보집중관리위원회"라 한다)에 보고하여야 한다.

③ 법 제20조제5항에 따라 신용정보관리·보호인은 다음 각 호의 사항을 매 사업연도 종료 후 3개월 이내에 금융감독원장이 정하는 서식에 따라 금융감독원장에게 제출하여야 한다.<개정 2016. 10. 20>

1. 신용정보관리·보호인이 직전 사업연도 중 법 제20조제4항 각 호의 업무를 수행한 실적
2. 제1호의 실적을 기재한 보고서를 대표이사 및 이사회에 보고한 실적

제22조의3(개인신용정보의 보유기간 등) ① 법 제20조의2제1항에 따른 "금융위원회가 정하여 고시하는 기한"이란 3개월을 말한다.

② 신용정보제공·이용자가 영 제17조의2제1항제1호나목에 따라 접근할 수 있는 임직원을 지정할 때에는 접근권한 관리책임자를 두어야 한다.

③ 영 제17조의2제1항제1호다목에 따라 신용정보제공·이용자는 개인신용정보가 안전하게 보호될 수 있도록 제2항에 따라 접근권한을 부여받은 자가 해당 개인신용정보를 이용하려는

경우에는 접근권한 관리책임자의 사전 승인을 얻어 그 개인신용정보를 이용하게 하고, 그 이용 내역을 3년간 보관하여야 한다.
[시행일: 2016.3.12.] 제22조의3

제22조의4(개인신용정보가 포함된 문서 등의 관리 방법) 영 제17조의2제1항제1호 각 목의 구분에 따른 방법으로 상거래관계가 종료된 신용정보주체의 개인신용정보를 관리하는 것이 불가능하거나 현저히 곤란한 경우에는 다음 각 호의 방법으로 관리할 수 있다.
1. 보존기간을 정하여 잠금장치가 있는 안전한 장소 등에 보관할 것
2. 물리적 보관장소에 대하여는 출입ㆍ통제 절차를 수립ㆍ운영 할 것
3. 보존되는 개인신용정보의 현황파악, 열람, 대여 등에 관한 통제시스템을 확립할 것
4. 보존기간이 만료한 개인신용정보에 대한 안전한 폐기계획을 수립ㆍ시행하고 신용정보관리ㆍ보호인 또는 대표이사가 폐기결과를 확인 할 것

제23조(폐업시 보유정보의 처리) 신용정보회사 또는 신용정보집중기관이 폐업을 하고자 하는 경우에는 금융감독원장이 소속 직원 중에서 지명하는 자의 입회하에 다음 각 호의 자료를 처분, 소거 또는 폐기하여야 한다.
1. 신용정보 자료철 및 신용정보 관리대장
2. 신용정보 데이터베이스
3. 그 밖에 신용정보가 수록ㆍ보관된 파일등

제24조(공공단체의 범위) 영 제19조제1항제1호 및 제3호까지에 따른 "금융위원회가 정하여 고시하는 기관"의 범위는 별표 5에 따른다.

제24조의2(공공기관 제공 신용정보의 등록 및 이용기준) 영 제19조제4항에 따라 공공기관이 종합신용정보집중기관에 제공하는 신용정보의 등록 및 이용기준은 별표 6 제6호와 같다.

제25조 삭제 <2015.9.11>

제25조의2 삭제 <2015.9.11>

제26조(신용정보의 등록 및 이용기준) 영 제21조제2항의 금융기관은 영 제21조제3항에서 정하는 집중관리ㆍ활용대상 신용정보를 집중관리ㆍ활용하기에 적합한 형태로 처리하여 종합신용정보집중기관에 등록하여야 한다.

제26조의2 삭제 <2015.9.11>

제26조의3(종합신용정보집중기관업무의 분리) ① 영 제21조제5항에 따라 종합신용정보집중기관이 법 제25조의2 각 호의 업무(이하 "집중기관업무"라 한다) 외의 다른 업무(이하 "기타업무"라 한다)를 수행하는 경우 다음 각 호에 따라 집중기관업무와 구별하여야 한다.
1. 재무에 관한 사항

가. 집중기관업무와 기타업무를 구분하여 별도의 회계장부를 마련하고 구분하여 회계처리할 것

나. 집중기관업무 관련 예·결산에 관한 사항에 대하여 신용정보집중관리위원회가 심의·의결할 것

2. 임직원(대표자인 임원, 감사는 제외한다)이 집중기관업무와 기타업무를 겸직하지 아니할 것

3. 집중기관업무와 기타업무간에 정보의 교류를 차단하고, 정기적으로 이해상충이 발생할 가능성을 파악·평가할 것

② 종합신용정보집중기관의 신용정보관리·보호인은 제1항에 따른 사항을 정기적으로 점검하여 신용정보집중관리위원회에 보고하여야 한다.

제26조의4(신용정보집중기관의 허가 세부요건) ① 영 제21조제6항제1호에서 "금융위원회가 정하여 고시하는 정보처리·정보통신설비"는 제6조제1항을 준용한다. 이 경우 "신용조회업무"는 "신용정보집중관리·활용업무"로 본다.

② 영 제21조제7항에 따른 신용정보집중기관 허가의 세부요건은 별표 5의2와 같다.

③ 영 제21조제9항에 따라 종합신용정보집중기관을 통해 집중관리·활용되는 신용정보의 구체적인 등록 및 이용기준은 별표 6과 같다.

④ 신용정보집중기관에 정보를 제공하거나 신용정보집중기관의 정보를 이용하는 자는 신용정보집중기관이 정하는 바에 따라 전산매체 또는 서면으로 신용정보를 제공·이용하여야 한다.

제26조의5(종합신용정보집중기관의 업무) 영 제21조의2제2항제3호에서 "그 밖에 금융위원회가 정하여 고시하는 업무"란 특정 개인을 알아볼 수 없는 정보에 관한 가공·분석·조사업무를 말한다.<개정 2016. 10. 20>

제26조의6(제재금의 최고한도 금액) 영 제22조제2항에 따른 제재금의 최고 한도 금액은 신용정보 제공의 누락 및 지연, 거짓 등록 등 위반건당 1백만원으로 한다.<개정 2016. 10. 20>

제27조 삭제 <2015.9.11>

제28조(신용정보집중관리위원회 협의·심의·결정 사항의 보고) 법 제26조제3항에 따라 신용정보집중관리위원회가 협의·심의·결정한 사항을 보고하는 경우에는 별지 제12호 서식에 따라 보고하여야 한다.

제29조(미성년자 고용 또는 채용가능 업무) 법 제27조제1항제1호 단서에서 "금융위원회가 정하는 업무"란 다음 각 호의 어느 하나에 해당하는 업무를 말한다.

1. 신용정보의 내부처리를 위한 자료의 작성, 입력 및 출력 등을 보조하는 업무

2. 법 제23조제2항에 따른 공공기관이 보유하는 신용정보로서 타인에게 제공되거나 공개되어도 신용정보주체에게 불이익을 초래할 우려가 없는 정보를 열람하거나 제공받는 업무

제30조(위임직채권추심인의 자격요건) ① 영 제24조제1항제3호에서 "그 밖에 제1호에 준하는 자격이 있다고 금융위원회가 인정한 사람"이란 법 제44조의 신용정보협회(이하 "협회"라 한다)가 주관하는 신용관리사 자격시험에 합격한 사람을 말한다.
② 영 제24조제2항에 따라 채권추심회사가 그 소속 위임직채권추심인이 되려는 자를 등록하고자 하는 때에는 별지 제13호 서식에 따른 등록신청서를 협회의 장에게 제출하여야 한다.
③ 제2항에 따른 등록신청서에는 소속 위임직채권추심인이 되고자 하는 자가 영 제24조제1항의 자격요건을 갖추었는지 여부를 확인할 수 있는 서류를 첨부하여야 한다.
④ 협회의 장이 위임직채권추심인 등록신청을 수리한 때에는 이를 별지 제14호 서식에 따른 위임직채권추심인등록부에 기재하고 그 사실을 채권추심회사에 지체없이 통지하여야 한다.
⑤ 위임직채권추심인의 등록에 관하여 필요한 세부사항은 협회의 장이 정한다.

제31조 삭제 <2015.9.11>

제32조 삭제 <2014.4.22.>

제33조 삭제 <2014.4.22.>

제33조의2 삭제 <2014.4.22.>

제33조의3 삭제 <2014.4.22.>

제34조(개인신용정보의 제공·활용에 대한 동의) 신용정보제공·이용자는 영 제28조제2항 각 호의 내용에 변경이 있는 경우에는 인터넷 홈페이지 게시 등을 통해 해당 신용정보주체에게 알려야 한다.
[시행일: 2016.3.12.] 제34조

제35조(개인신용정보의 조회에 대한 동의) 영 제28조제6항 각 호의 내용에 변경이 있는 경우에는 인터넷 홈페이지 게시 등을 통해 해당 신용정보주체에게 알려야 한다.

제36조 삭제 <2015.9.11.>
[시행일: 2016.3.12.] 제36조

제37조(조회동의 확인 방법) ① 신용조회회사 또는 신용정보집중기관이 영 제28조제7항에 따라 동의를 받았는지를 확인하고자 하는 경우에는 다음 각 호의 어느 하나의 방식으로 확인할 수 있다.
1. 동의서 사본을 제출받는 방식
2. 법 제32조제1항 제2호부터 제3호까지에 따른 방식
3. 개인신용정보를 제공받으려는 자로부터 해당 개인의 조회동의 사실을 확인하였다는 기록을 전자적으로 제공받는 방식
② 신용조회회사 또는 신용정보집중기관은 개인신용정보를 제공받으려는 자의 업태, 정보관리능력 등을 고려하여 제1항 각호의 방식 중 법 제32조제3항에 따른 확인업무를 적절하게 수

행할 수 있다고 판단되는 방식을 선택하여야 한다.

③ 제1항제3호의 방식을 통해 동의를 받았는지 확인하는 신용조회회사 또는 신용정보집중기관은 사실 확인의 진위여부를 주기적으로 점검하여야 한다.

제38조 삭제 <2015.9.11.>

[시행일: 2016.3.12.] 제38조

제38조의2(금융질서문란행위자) 영 제28조제11항제5호에서 "금융위원회가 정하여 고시하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1.「외국환거래법」제20조를 위반하여 허위의 보고를 하거나 거짓으로 자료를 제출한 자

2.「민법」제32조에 따라 금융위원회로부터 허가를 받은 신용회복위원회에 허위의 자료를 제출하거나 허위의 진술을 하고 채무를 조정 받았거나 조정된 채무를 이행하는 과정에서 재산의 도피, 은닉 또는 고의의 책임재산 감소행위를 한 자

3.「전자금융거래법」 제6조제3항 각 호의 어느 하나에 해당하는 행위를 한 자. 다만, 다음 각 목의 어느 하나에 해당하는 경우는 제외한다.

가. 다른 법률에 특별한 규정이 있는 경우

나. 같은 법 제18조에 따른 선불전자지급수단이나 전자화폐의 양도 또는 담보제공을 위하여 필요한 경우(같은 법 제6조제3항제3호의 행위 및 이를 알선하는 행위는 제외한다)

[시행일: 2016.3.12.] 제38조의2

제38조의3(개인신용정보 제공사실의 통지유예 등) 신용정보회사등은 영 별표 2의2 제11호, 제12호 및 제13호에 따른 개인신용정보 제공이 발생한 경우로서 신용정보 제공요구자가 다음 각 호의 어느 하나에 해당하는 사유가 지속되고 있음을 제시하고 통지의 유예를 서면으로 반복하여 요청하는 경우에는 요청받은 날부터 두 차례만(제1호의 경우는 제외한다) 매1회 3개월의 범위에서 유예요청기간 동안 통보를 유예할 수 있다.

1. 해당 통지가 사람의 생명이나 신체의 안전을 위협할 우려가 있는 경우

2. 해당 통지가 증거 인멸, 증인 위협 등 공정한 사법절차의 진행을 방해할 우려가 명백한 경우

3. 해당 통지가 질문ㆍ조사 등의 행정절차의 진행을 방해하거나 과도하게 지연시킬 우려가 명백한 경우

[시행일: 2016.3.12.] 제38조의3

제38조의4(영업양도 등에 따라 제공받은 개인신용정보의 관리) 법 제32조제8항에 따라 개인신용정보를 제공받은 자는 해당 개인신용정보를 다음 각 호의 구분에 따라 현재 거래 중인 신용정보주체의 개인신용정보와 구분하여 관리하여야 한다.

1. 제공받은 개인신용정보는 영업양도ㆍ분할ㆍ합병 등을 이유로 제공받은 개인신용정보라는 사실을 표시하여 관리

2. 개인신용정보를 제공받았을 때 이미 거래가 종료되어 분리보관 중인 개인신용정보의 경우 제1호에 따른 표시를 하고 현재 거래 중인 신용정보주체의 개인신용정보와 분리하여 관리

[시행일: 2016.3.12.] 제38조의4

제39조(개인신용정보를 제공받는 자의 확인) ① 신용정보회사등이 개인신용정보를 제공할 경우에는 제공받는 자로부터 제공받는 자의 성명, 주민등록번호 및 주소(법인의 경우에는 법인명, 대표자의 성명 및 본점 소재지) 등의 인적사항과 정보이용목적이 기재된 의뢰서 및 이용목적을 확인할 수 있는 근거서류를 받아야 하며 다음 각 호의 증표 및 서류에 따라 제공받는 자의 신원을 확인하여야 한다.

1. 제공받는 자가 개인인 경우에는 주민등록증, 운전면허증 또는 성명, 주민등록번호 및 주소가 기재되고 사진이 첨부된 그 밖의 신분증명서
2. 제공받는 자가 법인인 경우에는 법인의 대표자(또는 그로부터 위임받은 자)임을 확인할 수 있는 서류와 해당 개인의 신분증명서

② 신용정보집중기관이 신용정보제공·이용자 및 신용조회회사에게 개인신용정보를 제공하는 경우와 신용조회회사가 법 제2조제8호의 업무로 개인신용정보를 제공하는 경우에는 법 제20조제2항의 기록을 보유하는 것으로 제1항에 따른 제공받는 자의 확인을 갈음한다.

제39조의2(신용정보 이용 및 제공사실 조회시스템에 대한 조치기간) 영 제30조제1항 본문에 따른 "금융위원회가 정하여 고시하는 기간"이란 7일 이내를 말한다. 다만, 법, 영 및 그 밖에 다른 법령에서 달리 정하는 경우에는 그 법령에서 정하는 바에 따른다.

[시행일: 2016.3.12.] 제39조의2

제40조(신용정보 이용 및 제공사실의 통지요구 등) ① 법 제35조제2항 및 영 제30조제7항에 따라 신용정보회사등이 신용정보주체에게 본인의 개인신용정보를 이용하거나 제공한 사항을 통지하는 경우에는 별지 제15호 서식에 따라 서면, 전자우편, 문자메시지, 그 밖에 이와 유사한 방법으로 통지한다.

② 신용정보회사등은 신용정보주체에게 법 제35조제2항에 따라 통지를 요청할 수 있다는 사실, 통지요청의 방법, 통지의 주기 및 수수료 등을 알려야 한다.

[시행일: 2016.3.12.] 제40조

제40조의2(상거래 거절 근거 신용정보의 고지) 영 제31조제1항제2호 단서에서 "금융위원회가 정하여 고시하는 정보"란 제2조의2제2항의 정보를 말한다.

[시행일: 2016.3.12.] 제40조의2

제40조의3(동의 철회의 방법) 영 제32조제1항에 따른 "금융위원회가 정하여 고시하는 방법"이란 신용정보제공·이용자의 사무실·점포 등을 방문하여 동의 철회서를 제출하는 방법을 말한다.

제41조(신용정보의 정정청구) ① 법 제38조제1항에 따라 신용정보주체가 신용정보회사등에게 본인정보의 정정을 청구하고자 할 때에는 정정대상정보와 정정청구사유를 기재하여 서면 또는 신용정보회사등의 인터넷홈페이지를 통해 신청하여야 한다.

② 정정청구를 받은 신용정보회사등은 사실여부의 조사·확인을 위하여 필요한 경우 신용정보주체에게 관련 증빙자료의 제시를 요청할 수 있다.
③ 신용정보집중기관 및 신용조회회사는 신용정보주체의 정정청구에 따른 사실 확인을 위하여 필요한 경우에는 당해 신용정보를 등록한 신용정보제공·이용자에게 등록된 정보의 사실여부를 입증할 수 있는 자료를 요청할 수 있다.

제42조(시정요청서) 영 제33조제3항에 따른 시정요청은 별지 제16호 서식에 따른다.

제43조(시정조치 결과보고서) 신용정보회사등이 법 제38조제7항에 따라 시정조치를 한 경우에는 별지 제17호 서식에 따라 그 결과를 보고하여야 한다.

제43조의2(신용조회회사의 정보제공 중지의 요건 등) ① 법 제38조의2제1항에 따른 "금융위원회가 정하는 방식"이란 영 제30조제3항에 따른 방식을 말한다.
② 영 제33조의2제1항에서 각 호의 어느 하나에 해당하는 사실이 발생함에 따라 그 요청을 받은 것으로 인정되는 경우란 다음 각 호의 어느 하나에 해당하는 경우를 말한다.
1. 신용정보회사등이 법 제39조의2제1항에 따른 누설 통지 또는 같은 조 제3항에 따른 누설 신고를 한 이후 신용정보주체가 법 제38조의2제1항에 따른 조회사실 통지를 요청한 경우
2. 신용정보주체가 「주민등록법 시행령」 제42조제1항에 따른 주민등록증 분실신고 또는 이와 유사한 방법으로 개인식별번호(영 제29조 각 호의 번호를 말한다)가 포함된 신분증을 분실한 사실을 입증하고 법 제38조의2제1항에 따른 조회사실 통지를 요청한 경우
[시행일: 2016.3.12.] 제43조의2

제43조의3(삭제 요구에 따른 통지방법) 법 제38조의3제4항에 따른 금융위원회가 정하여 고시하는 방법이란 영 제33조의2제3항 각 호의 어느 하나에 따른 방법을 말한다.
[시행일: 2016.3.12.] 제43조의3

제43조의4(신용정보 누설사실의 공시기간) 영 제34조의2제2항에 따른 "금융위원회가 정하여 고시하는 기간"이란 다음 각 호의 기간을 말한다.
1. 영 제34조의2제2항제1호의 경우: 15일
2. 영 제34조의2제2항제2호의 경우: 15일
3. 영 제34조의2제2항제3호의 경우: 7일

제43조의5(신용정보의 누설신고) 영 제34조의2제6항에 따라 신고하는 신용정보회사등은 별지 제18호 서식에 따른 신고서를 제출하여야 한다.

제43조의6(모집업무수탁자에 관한 보고) 영 제35조의2제6항 및 제7항에 따른 보고의 서식 및 방법은 금융감독원장이 정한다.

제43조의7(손해배상책임의 이행을 위한 보험 등 가입 기준) ① 영 제35조의9에 따른 "금융위원회가 정하여 고시하는 자" 및 그 자가 법 제43조의3에 따라 보험 또는 공제에 가입하는 경우

의 그 최소 가입금액은 다음 각 호와 같다.

1. 신용정보집중기관, 신용조회회사, 영 제5조제1항제1호부터 제7호까지의 자(제1호에 따른 은행 중 지방은행 및 「은행법」 제58조에 따라 인가를 받은 외국은행의 국내지점은 제외한다): 20억원
2. 영 제5조제1항제1호 중 지방은행, 외국은행의 국내지점, 같은 항 제8호(명의개서대행회사는 제외한다), 제15호부터 제18호까지의 자, 제20호, 제21호(정리금융기관은 제외한다)의 자 및 영 제21조제2항제9호에 해당하는 자: 10억원
3. 영 제35조의9 각 호의 어느 하나에 해당하는 자 중 제1호 및 제2호 이외의 자(영 제21조제2항제8호에 해당하는 자, 같은 조 같은 항 제19호에 해당하는 자 중에서 「대부업 등의 등록 및 금융이용자 보호에 관한 법률 시행령」 제7조의2제1항제1호·제5호에 해당하는 자 및 같은 조 같은 항 제22호에 해당하는 자는 제외한다): 5억원. 다만, 영 제5조제1항제9호부터 제14호까지 및 제19호에 해당하는 자가 소속 중앙회 또는 연합회를 통하여 신용정보처리 관련 기술부문의 주요부분을 공동으로 이용하는 경우, 중앙회 또는 연합회가 공동 이용 금융회사 전체의 사고를 보장하는 내용으로 제1호의 금액 이상의 보험 또는 공제에 가입하면 공동 이용 금융회사는 본호의 보험 또는 공제에 가입한 것으로 본다.

② 제1항 각 호의 자가 준비금을 적립하는 경우 제1항 각 호에서 정하는 금액 이상의 금액을 보유하여야 한다.

③ 제1항 각 호의 자가 보험 또는 공제 가입과 준비금 적립을 병행하는 경우 보험 또는 공제의 최소 가입금액은 제1항 각 호에서 정한 금액에서 적립한 준비금을 뺀 금액으로 한다.

④ 「전자금융거래법」 제9조제4항에 따라 가입한 보험·공제 또는 적립한 준비금이 법 제43조에 따른 손해배상 책임의 이행을 보장하는 경우 제1항에서 정한 금액에서 그 금액을 뺀 금액이상으로 한다.

⑤ 제1항부터 제4항까지의 규정은 500명 이상의 신용정보주체에 관한 개인신용정보를 수집·이용·처리하지 않는 자에 대하여는 적용하지 아니한다.

제44조(검사결과의 보고방법) 금융감독원장은 법 제45조제6항에 따른 결과보고를 하는 경우 「금융기관검사및제재에관한규정」 제3장을 준용한다.

제45조 삭제 <2014.4.22.>

제46조(회계처리기준등) ① 신용정보회사는 회계처리 및 재무제표 작성에 관하여 「주식회사의 외부감사에 관한 법률」 제13조에 따른 회계처리기준을 따라야 한다.

② 신용정보회사는 결산재무제표와 「주식회사의 외부감사에 관한 법률」 제3조에 따른 감사인의 감사보고서를 사업연도말로부터 3개월 이내에 금융감독원장에게 제출하여야 한다.

③ 제2항에 따라 제출한 재무제표와 제1항에 따라 제출한 사업연도말 업무보고서가 일치하지 않는 경우에는 그 내용과 사유를 금융감독원장에게 보고하여야 한다.

제47조(세부사항) 금융감독원장은 이 규정의 시행에 필요한 세부사항을 정할 수 있다.

제48조(재검토기한) 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 규정 발령 후의 법령이나 현실여건의 변화 등을 검토하여 이 규정의 유지, 폐지, 개정 등의 조치를 하여야 하는 기한은 2015년 7월 1일을 기준으로 매 2년이 되는 시점(매 2년째의 6월 30일까지를 말한다)으로 한다.<개정 2015.7.1.>

부칙 <제2001-113호,2002.1.4>

이 규정은 공고한 날부터 시행한다.

부칙 <제2002-42호,2002.7.4>

이 규정은 공고한 날부터 시행한다. 다만, 제12조의 개정규정에 의한 <별지제9호서식>은 2002.10.1부터 시행한다.

부칙 <제2003-19호,2003.3.19>

이 규정은 공고한 날부터 시행한다.

부칙 <제2003-52호,2003.11.5>

이 규정은 공고한 날부터 시행한다.

부칙 <제2004-41호,2004.6.30>

이 규정은 공고한 날부터 시행한다. 다만, 제13조의2 및 제13조의3은 2004년 7월 30일부터 시행한다.

부칙 <제2005-53호,2005.11.3>

이 규정은 공고한 날부터 시행한다.

부칙 <제2008-8호,2008.4.7>

이 규정은 고시한 날부터 시행한다.

부칙 <제2009 - 30호,2009.5.12>

제1조 (시행일) 이 규정은 고시한 날부터 시행한다.

부칙 <제2009 - 50호,2009.8.26>

이 규정은 고시한 날부터 시행한다.

부칙 <제2009 - 56호,2009.10.2>

제1조(시행일) 이 규정은 2009년 10월 2일부터 시행한다.

제2조(경과조치) ① 이 규정시행당시 종전의 관련 규정에 따라 행한 조치는 이 규정에 따라 시행한 것으로 본다.

② 제46조는 2010 사업연도부터 적용한다.

③ 제34조제4항제2호의 경우 2010년 1월 1일까지는 금융회사에게 등록한 비밀번호로서 갈음할 수 있다.

부칙 <제2011 - 15호,2011.8.18>

이 규정은 2011년 8월 20일 부터 시행한다.

부칙 <제2012 - 12호,2012.6.26>

이 규정은 2012년 6월 26일 부터 시행한다.

부칙 <제2013 - 1호,2013.1.31>

이 규정은 공고한 날부터 시행한다.

부칙 <제2013 - 9호,2013.4.23>

이 규정은 공고한 날부터 시행한다.

부칙 <제2014 - 11호,2014.4.22>

이 규정은 공고한 날부터 시행한다.

부칙 <제2014 - 13호,2014.6.11>

이 규정은 공고한 날부터 시행한다.

부칙 <제2014 - 24호,2014.8.6>

이 규정은 공고한 날부터 시행한다.

부칙 <제2015 - 20호,2015.6.30>

이 규정은 2015년 7월 1일부터 시행한다.

부칙 <제2015 - 30호,2015.9.7>

이 규정은 공고한 날부터 시행한다.

부칙 <제2015 - 31호,2015.9.11>

제1조(시행일) 이 규정은 고시한 날부터 시행한다. 다만, 제22조의3, 제34조, 제36조, 제38조, 제38조의2, 제38조의3, 제38조의4, 제39조의2, 제40조, 제43조의2 및 제43조의3의 개정규정은 2016년 3월 12일부터 시행한다.

제2조(신용정보관리·보호인의 업무 보고의 적용례) 제22조의2제3항의 개정규정은 2016년도 신용정보관리·보호인의 업무실적 및 보고실적에 대한 보고부터 적용한다.

제3조(내부관리규정 마련에 관한 경과조치) 신용정보회사등은 제22조제2항에 따른 내부관리규정을 이 규정의 시행일부터 3개월 이내에 마련하여야 한다.

제4조(다른 규정의 폐지) 신용정보업인허가지침(금융위원회고시 제2012 - 12호)은 폐지한다.

부칙 <제2016 - 14호,2016.3.16>

제1조(시행일) 이 규정은 고시한 날부터 시행한다.

부칙 <제2016 - 32호,2016.9.21>

제1조(시행일) 이 규정은 2016년 9월 23일부터 시행한다.

제2조 생략

제3조(다른 고시의 개정) ① 생략

② 신용정보업감독규정 일부를 다음과 같이 개정한다.

제3조제1호부터 제3호까지를 각각 다음과 같이 한다.

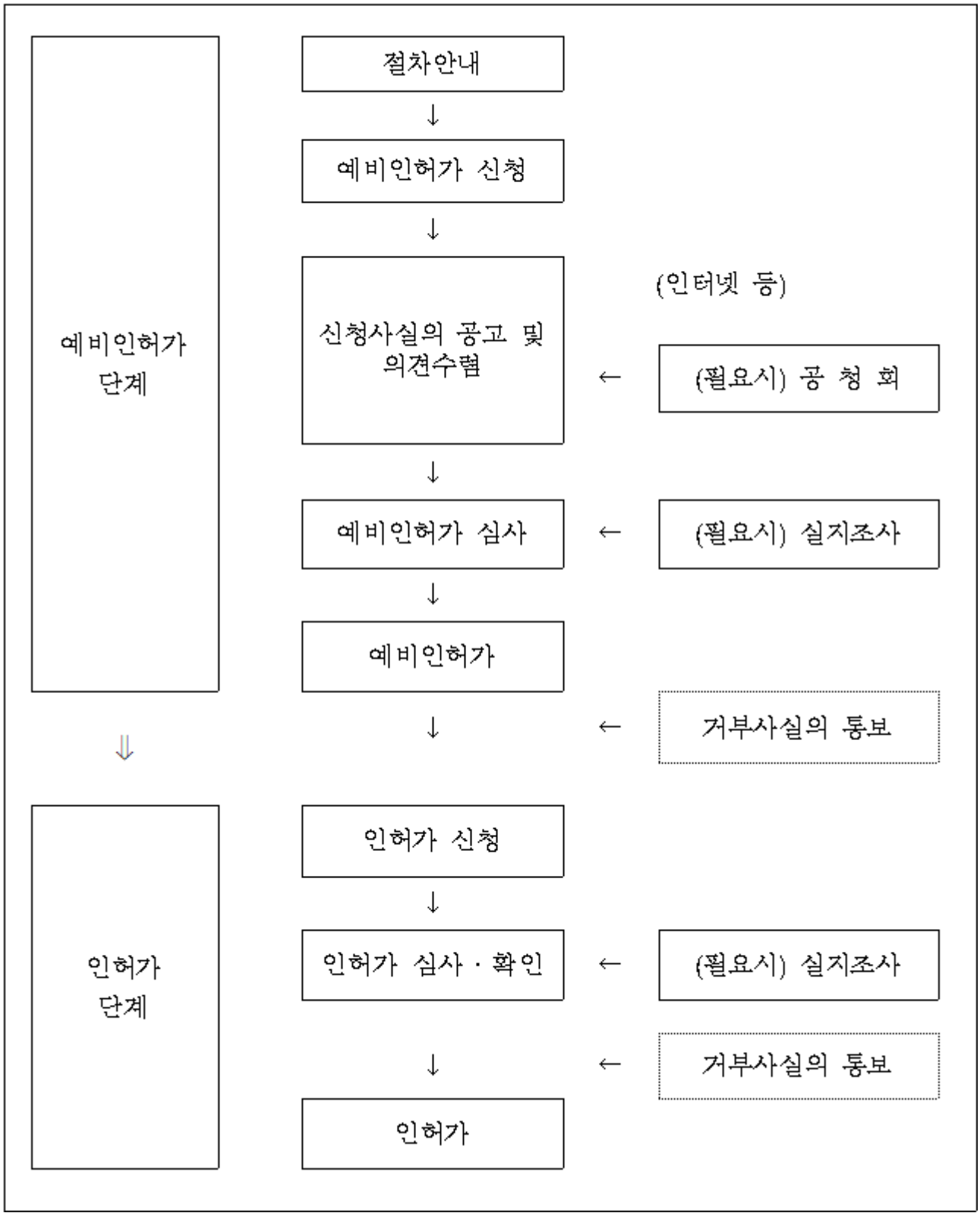
1. 「서민의 금융생활 지원에 관한 법률」 제3조에 따른 서민금융진흥원 및 같은 법 제26조에 따른 사업수행기관
2. 「서민의 금융생활 지원에 관한 법률」 제56조에 따른 신용회복위원회
3. 「상법」에 따라 설립된 주식회사 국민행복기금

부칙 <제2016-40호,2016.10.20>

제1조(시행일) 이 규정은 고시한 날부터 시행한다.

[별표 1]

신용정보업 및 신용정보집중기관 허가 등의 절차(제5조제1항 관련)



[별표 1의2]

신용정보업 및 신용정보집중기관 허가 등의 신청서류

(제5조제2항 관련)

1. 신용정보업

구분	예비인·허가	인·허가
1. 신용정보업 영위허가 (신용정보업무 추가 영위허가 포함)	- 신용정보업 예비허가신청서 - 정관(안) - 2년간의 사업계획서 및 예상수지계산서 - 발기인 총회의사록(이사회의사록) 사본 - 출자자(또는 주주) 구성 및 자금조달 계획 - 출자자의 인감증명서가 첨부된 출자확약서(출자비율 5%미만인 개인출자자는 제외) - 출자자의 출자자금 조달계획서 - 출자자가 금융회사인 경우는 당해 금융회사 인허가권자의 인허가서 사본 또는 등록증 사본, 법인등기부등본, 사업자등록증 사본, 최근사업연도의 감사보고서 및 당해 금융회사의 일반현황 - 출자자가(당해 법인이 금융회사가 아닌 출자자 중 최다 출자자에 한함)가 일반법인인 경우 법인등기부등본, 사업자 등록증 사본, 최근 사업연도의 재무제표 * 신청인이 이미 설립된 법인인 경우에는 상기 첨부서류에 준하는 서류로 대체 가능 - 출자자(또는 주주) 관계가 법 제5조(신용정보업별 허가 대상)에 저촉되지 않음을 확인하는 서류 등 - 합작계약서(합작법인인 경우) - 주요출자자가 주요출자자 요건을 충족함을 확인하는 서류 - 인력 및 물적시설(채용, 구매 등이 예정된	- 신용정보업 허가신청서 - 정관 및 법인등기부 등본 - 재무제표 - 2년간의 사업계획서 및 예상수지계산서 - 자본금 또는 기본재산의 지분을 기재한 서류 - 발기인 총회의사록(이사회의사록) 사본 - 출자자(또는 주주) 관계 확인서류 - 자본금 납입증명 서류 - 외국인출자자인 경우 외국인의 출자가 「외국환거래법」 등에 저촉되지 않음을 확인하는 서류 - 출자자(또는 주주) 관계가 법 제5조(신용정보업별 허가 대상)에 저촉되지 않음을 확인하는 서류 등 - 합작계약서(합작법인인 경우) - 주요출자자가 주요출자자 요건을 충족함을 확인하는 서류 - 인력 및 물적시설을 갖추었음을 확인하는 서류 - 허가 신청한 업무의 전문성을 갖추었음을 확인하는 자료 - 임직원에 관한 서류 - 임원의 이력서 - 직원의 상시고용을 확인하는 서류 - 법 제22조제1항, 법 제27조제1항에 해당하지 않음을 확인하는 서류(필요시 이를 확인하는 각서 제출로 대체 가능)

구분	예비인·허가	인·허가
	인력물적시설 포함)의 현황을 확인할 수 있는 서류 - 허가 신청한 업무의 전문성을 갖출 수 있음을 확인할 수 있는 자료 - 임원(예정자 포함)이력서	- 제22조제2항에 따른 내부관리규정 - 회계처리·감사·조직관리 등 내부통제에 관한 규정 - 예비허가내용 및 조건의 이행을 증명하는 서류
2. 분할·합병 인가	- 분할 · 합병 예비인가 신청서 - 분할 · 합병 목적 및 사유 - 정관변경(안) - 자본금 또는 기본재산의 지분을 기재한 서류 - 재무제표 - 2년간의 사업계획서(분할 · 합병 후 2년간 추정재무제표, 인력 및 조직운영계획, 업무범위 및 영업전략 등) 및 예상수지계산서 - 분할 · 합병 관련 계약서 또는 예약서 - 분할 · 합병에 관한 이사회 의사록 - 본점 및 영업소의 현황 및 변경계획(명칭, 주소 등) - 출자자(또는 주주) 구성 및 경영지배구조 계획 - 채권자 등 이해관계인의 권익보호계획 - 분할 후 영위 할 수 없는 업무가 있는 경우 그 업무의 정리계획	- 분할 · 합병 인가 신청서 - 분할 · 합병 목적 및 사유 - 정관 및 법인등기부등본 - 자본금 또는 기본재산의 지분을 기재한 서류 - 재무제표 - 2년간의 사업계획서(분할 · 합병 후 2년간 추정재무제표, 인력 및 조직운영계획, 업무범위 및 영업전략 등) 및 예상수지계산서 - 분할 · 합병 관련 계약서 또는 예약서 - 분할 · 합병에 관한 이사회 의사록 및 주주총회 의사록 - 본점 및 영업소의 현황 및 변경계획(명칭, 주소 등) - 출자자(또는 주주) 구성 및 경영지배구조 - 채권자 등 이해관계인의 보호절차 이행을 증명하는 서류 - 분할 후 영위 할 수 없는 업무가 있는 경우 그 업무의 정리계획 - 예비인가내용 및 조건의 이행을 증명하는 서류
<합병 후 존속하는	- 정관변경(안) - 임원(예정자 포함) 이력서	- 정관 및 법인등기부등본 - 임원 이력서

구분	예비인·허가	인·허가
법인 및 분할 또는 합병에 따라 설립되는 법인의 경우>	- 법 제5조, 법 제6조, 법 제22조제1항, 법 제27조제1항에 저촉되지 않음을 증명하는 서류(신용정보업 영위 허가 참조)	- 법 제5조, 법 제6조, 법 제22조제1항, 법 제27조제1항에 저촉되지 않음을 증명하는 서류(신용정보업 영위 허가 참조) - 제22조제2항에 따른 내부관리규정 - 회계처리·감사·조직관리 등 내부통제에 관한 규정
3. 사업양수인가	- 사업양수 예비인가 신청서 - 사업양수 목적 및 사유 - 정관변경(안) - 자본금 또는 기본재산의 지분을 기재한 서류 - 재무제표 - 2년간의 사업계획서(양수 후 2년간 추정 재무제표, 인력 및 조직운영계획, 업무범위 및 영업전략 등) 및 예상수지계산서 - 사업양수 관련 계약서 또는 예약서 - 사업양수에 관한 이사회 의사록 - 본점 및 영업소의 현황 - 출자자(또는 주주) 구성 및 경영지배구조 계획 - 채권자 등 이해관계인의 권익보호계획 - 임원(예정자 포함) 이력서 - 법 제5조, 법 제6조, 법 제22조제1항, 법 제27조제1항에 저촉되지 않음을 증명하는 서류(신용정보업 영위 허가 참조) - 양수회사의 양수자금 조달계획서	- 사업양수 인가 신청서 - 사업양수 목적 및 사유 - 정관 및 법인등기부등본 - 자본금 또는 기본재산의 지분을 기재한 서류 - 재무제표 - 2년간의 사업계획서(양수 후 2년간 추정 재무제표, 인력 및 조직운영계획, 업무범위 및 영업전략 등) 및 예상수지계산서 - 사업양수 관련 계약서 또는 예약서 - 사업양수에 관한 이사회 의사록 및 주주총회 의사록 - 본점 및 영업소의 현황 - 출자자(또는 주주) 구성 및 경영지배구조 - 채권자 등 이해관계인의 보호절차 이행을 증명하는 서류 - 예비인가내용 및 조건의 이행을 증명하는 서류 - 임원 이력서 - 법 제5조, 법 제6조, 법 제22조제1항, 법 제27조제1항에 저촉되지 않음을 증명하는 서류(신용정보업 영위 허가 참조) - 제22조제2항에 따른 내부관리규정 - 회계처리·감사·조직관리 등 내부통제에 관한 규정

구분	예비인·허가	인·허가
4. 사업양도 인가	- 사업양도 예비인가 신청서 - 사업양도 목적 및 사유 - 정관변경(안) - 재무제표 - 2년간의 사업계획서(양도 후 2년간 추정재무제표, 인력 및 조직운영계획, 업무범위 및 영업전략 등)(일부양도의 경우에 한함) - 사업양도 관련 계약서 또는 예약서 - 사업양도에 관한 이사회 의사록 - 채권자 등 이해관계인의 권익보호계획, 자산 및 부채에 대한 조치내역 및 계획	- 사업양도 인가 신청서 - 사업양도 목적 및 사유 - 정관 - 재무제표 - 2년간의 사업계획서(양도 후 2년간 추정재무제표, 인력 및 조직운영계획, 업무범위 및 영업전략 등)(일부양도의 경우에 한함) - 사업양도 관련 계약서 또는 예약서 - 사업양도에 관한 이사회 의사록 및 주주총회 의사록 - 채권자 등 이해관계인의 보호절차 이행을 증명하는 서류 - 사업양도후 해산하는 경우에는 청산사무의 추진계획 - 사업의 일부 양도 후 영위할 수 없는 업무가 있는 경우 그 업무의 정리계획 - 예비인가내용 및 조건의 이행을 증명하는 서류

2. 신용정보집중기관

예비허가	허가
- 신용정보집중기관 예비허가신청서 - 정관 또는 정관(안) - 재산목록 및 그 내용을 확인할 수 있는 서류 - 2년간 사업연도분의 사업계획 및 수입·지출예산을 적은 서류 1부 - 발기인 총회의사록(이사회 의사록(이사회를	- 신용정보집중기관 허가신청서 - 정관 또는 정관(안) - 재산목록 및 그 내용을 확인할 수 있는 서류 - 2년간 사업연도분의 사업계획 및 수입·지출예산을 적은 서류 1부 - 발기인 총회의사록(이사회 의사록(이사회를

예비허가	허가
구성하지 아니한 경우 총회 회의록))	구성하지 아니한 경우 총회 회의록))
- 신용정보집중관리위원회(공익위원선임위원회 및 소위원회 포함) 구성 및 운영(안)(종합신용정보집중기관에 한함)	- 신용정보집중관리위원회(공익위원선임위원회 및 소위원회 포함) 구성 및 운영(안) (종합신용정보집중기관에 한함)
- 영 제21조제5항제1호가목에 따른 위험관리체계 및 내부통제장치를 마련할 수 있음을 확인할 수 있는 서류 1부	- 영 제21조제5항제1호가목에 따른 위험관리체계 및 내부통제장치가 마련되어 있음을 입증하는 서류 1부
- 영 제21조제5항제1호나목에 따른 이해상충방지체계를 마련할 수 있음을 확인할 수 있는 서류 1부(집중기관업무 외의 다른 업무를 하는 경우에 한함)	- 영 제21조제5항제1호나목에 따른 이해상충방지체계가 마련되어 있음을 입증하는 서류 1부(집중기관업무 외의 다른 업무를 하는 경우에 한함)
- 영 제21조제5항제1호라목에 따른 사원의 구성에 관한 계획 및 업무방법 등을 마련할 수 있음을 확인할 수 있는 서류 1부(종합신용정보집중기관에 한함)	- 영 제21조제5항제1호라목에 따른 사원의 구성에 관한 계획 및 업무방법 등이 마련되어 있음을 입증하는 서류 1부(종합신용정보집중기관에 한함)
- 인력 및 물적시설(채용, 구매 등이 예정된 인력·물적시설 포함)의 현황을 확인할 수 있는 서류 1부	- 인력 및 물적시설(채용, 구매 등이 예정된 인력·물적시설 포함)의 현황을 확인할 수 있는 서류 1부
- 신용정보를 집중관리·활용하는데 있어서 전문성을 갖출 수 있음을 확인할 수 있는 자료 1부	- 신용정보를 집중관리·활용하는데 있어서 전문성을 갖추었음을 확인할 수 있는 자료 1부
- 임원(예정자 포함) 이력서 1부	- 임원(예정자 포함) 이력서 1부
- 주무부처의 비영리법인 설립허가증(개별신용정보집중기관에 한함)	- 주무부처의 비영리법인 설립허가증(개별신용정보집중기관에 한함)
- 집중관리·활용의 필요성	- 법인등기부등본
	- 제22조제2항에 따른 내부관리규정
	- 집중관리·활용의 필요성
	- 예비허가내용 및 조건을 이행하였음을 확인할 수 있는 서류

[별표 2]

신용조회업 및 신용정보집중기관 허가에 필요한 정보처리·정보통신설비 요건

(제6조제1항 및 제26조의4제1항 관련)

구성	세부 요건
시스템 구성	1. 시스템 구성에 다음 항목을 포함할 것 가. D/B서버, 통신서버, 보안서버 등 통신구간 암호화 시스템 나. WEB서버(인터넷서비스를 제공할 경우에 한함) 다. 저장장치 라. 그 밖에 주변장치 2. 백업 및 복구시스템 3. 시스템 보안 및 시설 보안을 포함한 보안관리 체계
시스템 성능	1. 보유정보를 적절하게 처리할 수 있는 성능을 갖출 것 2. 온라인서비스 또는 공중통신망을 통한 정보의 수집 및 제공을 적절하게 처리할 수 있는 성능을 갖출 것 3. 백업 및 복구작업이 최소한의 시간내에 가능할 것
보안체계	1. 방화벽(Fire-Wall)을 갖출 것 2. 침입을 탐지·경고·차단할 수 있는 보안시스템을 갖출 것 3. 내부네트워크와 신용조회네트워크를 분리하여 운용할 것 4. 정보이용자 확인 체계(사용자 인증)를 갖출 것 5. 데이터 암호화처리 체계를 갖출 것 6. 외부침입 방지, 출입자관리 통제 및 데이터 반·출입 통제에 대한 대책을 강구할 것 7. 백업 및 소산관리 대책을 강구할 것
운용능력	1. 시스템 운용능력을 갖출 것 2. 프로그램 개발능력을 갖출 것

[별표 2의2]

신용정보업의 양도·양수 등의 인가의 세부요건

(제11조의2 관련)

1. 사업의 전부 양도

가. 해당 신용정보회사의 경영 및 재무상태 등에 비추어 부득이 할 것

나. 신용정보주체의 보호 및 건전한 신용질서 유지에 지장을 초래하지 않을 것

다. 「상법」 등 관계 법령에 따른 절차 이행에 하자가 없을 것

2. 사업의 일부 양도

가. 제1호가목부터 다목까지의 기준을 충족할 것

나. 사업의 일부 양도 후 2년간의 추정재무제표 및 수익전망이 영업계획에 비추어 타당성이 있을 것

다. 주된 시장, 주된 고객, 주된 서비스 내용 등 영업전략 및 업무범위가 적정할 것

라. 사업의 일부 양도 후 영위할 수 없는 업무의 정리계획이 적정할 것

3. 분할의 경우

가. 신용정보업의 효율화 및 건전한 신용질서 유지에 관한 사항

1) 신용정보업의 효율적 영위, 구조조정의 촉진 등 분할 목적이 타당할 것

2) 기존 거래자에 대한 불이익이 없을 것

나. 영업계획 및 조직운영계획에 관한 사항

1) 분할 이후 2년간의 추정재무제표 및 수익전망이 영업계획에 비추어 타당성이 있을 것

2) 주된 시장, 주된 고객, 주된 서비스 내용 등 영업전략 및 업무범위가 적정할 것

3) 분할 후 영위할 수 없는 업무의 정리계획이 적정할 것

4) 조직 및 인력운영체제가 적합할 것

다. 소유구조 변경에 관한 사항

분할 후 주주구성계획이 법 제5조에 적합하고 주요출자자는 영 제6조제4항에 따른 <별표 1>의 요건을 충족할 것

라.「상법」 등 관계 법령에 따른 절차 이행에 하자가 없을 것

4. 합병의 경우

가. 신용정보업의 효율화 및 건전한 신용질서 유지에 관한 사항

1) 신용정보업의 효율적 영위, 구조조정의 촉진 등 합병의 목적이 타당할 것

2) 기존 거래자에 대한 불이익이 없을 것

3) 합병에 대한 공정거래위원회의 경쟁제한성 검토결과가 적정할 것

나. 영업계획 및 조직운영계획에 관한 사항

1) 합병 이후 2년간의 추정재무제표 및 수익전망이 영업계획에 비추어 타당성이 있을 것

2) 주된 시장, 주된 고객, 주된 서비스 내용 등 영업전략 및 업무범위가 적정할 것

3) 합병 후 영위할 수 없는 업무의 정리계획이 적정할 것

4) 조직 및 인력운영체제가 적합할 것

다. 소유구조 변경에 관한 사항

합병 후 주주구성계획이 법 제5조에 적합하고 주요출자자는 영 제6조제4항에 따른 <별표 1>의 요건을 충족할 것

라.「상법」 등 관계 법령에 따른 절차 이행에 하자가 없을 것

5. 사업의 양수

합병의 경우를 준용한다.

[별표 3]

기술적·물리적·관리적 보안대책 마련 기준(제20조 관련)

Ⅰ. 목 적

이 기준은 영 제16조제1항에서 정하는 신용정보의 기술적·물리적·관리적 보안대책과 관련된 구체적인 기준을 정함을 목적으로 한다.

Ⅱ. 기술적·물리적 보안대책

1. 접근통제

① 신용정보회사등은 개인신용정보를 처리할 수 있도록 체계적으로 구성한 전산시스템(이하 "개인신용정보처리시스템"이라 한다)에 대한 접근권한을 서비스제공을 위하여 필요한 최소한의 인원에게만 부여한다.

② 신용정보회사등은 전보 또는 퇴직 등 인사이동이 발생하여 신용정보회사등의 지휘·감독을 받아 개인신용정보를 처리하는 업무를 담당하는 자(이하 "개인신용정보취급자"라 한다)가 변경되었을 경우 지체 없이 개인신용정보처리시스템의 접근권한을 변경 또는 말소한다.

③ 신용정보회사등은 제1항 및 제2항에 따른 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관한다.

④ 신용정보회사등은 개인신용정보처리시스템에 침입차단시스템과 침입탐지시스템을 설치하여 보호한다.

⑤ 신용정보회사등은 개인신용정보주체 및 개인신용정보취급자가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자를 비밀번호로 이용하지 않도록 비밀번호 작성규칙을 수립하고 이행한다.

⑥ 신용정보회사등은 취급 중인 개인신용정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되지 않도록 개인신용정보처리시스템 및 개인신용정보취급자의 PC를 설정한다.

⑦ 신용정보회사등은 제휴, 위탁 또는 외부주문에 의한 개인신용정보처리시스템, 신용평가모형 또는 위험관리모형 개발업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치·운영한다.

⑧ 신용정보회사등은 업무목적을 위하여 불가피한 경우에만 외부사용자에게 개인신용정보처리시스템에 대한 최소한의 접근권한을 부여하고, 권한 부여에 관한 기록을 3년 이상 보관하는 등 적절한 통제시스템을 갖추어야 한다.

2. 접속기록의 위·변조방지

① 신용정보회사등은 개인신용정보취급자가 개인신용정보처리시스템에 접속하여 개인신용정보를 처리한 경우에는 처리일시, 처리내역 등 접속기록을 저장하고 이를 월 1회 이상 정기적으로 확인·감독한다.
② 신용정보회사등은 개인신용정보처리시스템의 접속기록을 1년 이상 저장하고, 위·변조되지 않도록 별도 저장장치에 백업 보관한다.

3. 개인신용정보의 암호화

① 신용정보회사등은 비밀번호, 바이오정보 등 본인임을 인증하는 정보는 암호화하여 저장하며, 이는 조회할 수 없도록 하여야 한다. 다만, 조회가 불가피하다고 인정되는 경우에는 그 조회사유·내용 등을 기록·관리하여야 한다.
② 신용정보회사등은 정보통신망을 통해 개인신용정보 및 인증정보를 송·수신할 때에는 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호의 어느 하나의 기능을 갖추어야 한다.

1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 개인신용정보를 암호화하여 송·수신하는 기능

2. 웹서버에 암호화 응용프로그램을 설치하여 개인신용정보를 암호화하여 송·수신하는 기능

③ 신용정보회사등은 개인신용정보를 PC에 저장할 때에는 이를 암호화해야 한다.
④ 신용정보회사등은 다음 각 호의 기준에 따라 주민등록번호의 암호화 등의 조치를 취하여야 한다.

1. 정보통신망을 통하여 송수신하거나 보조저장매체를 통하여 전달하는 경우에는 암호화하여야 한다.
2. 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone) 에 저장할 때에는 암호화하여야 한다.
3. 신용정보회사등이 내부망에 주민등록번호를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

가. 「개인정보 보호법」 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과

나. 그 밖의 신용정보회사등의 경우에는 개인신용정보처리시스템에 적용되고 있는 개인신용정보 보호를 위한 수단과 개인신용정보 유출시 신용정보주체의 권익을 해할 가능성 및 그 위험의 정도를 분석한 결과

4. 업무용 컴퓨터 또는 모바일 기기에 저장하여 관리하는 경우에는 상용 암호화 소프트웨어 또는 안전한 알고리즘을 사용하여 암호화하여야 한다.

⑤ 신용정보집중기관과 신용조회회사가 서로 개인식별번호를 제공하는 경우에는 상용 암호화 소프트웨어 또는 안전한 알고리즘을 사용하여 암호화하여야 한다.

⑥ 신용정보회사등이 개인신용정보의 처리를 위탁하는 경우 개인식별번호를 암호화하여 수탁자에게 제공하여야 한다.

4. 컴퓨터바이러스 방지

① 신용정보회사등은 개인신용정보처리시스템 및 개인신용정보취급자가 개인신용정보 처리에 이용하는 정보처리기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치한다.

② 제1항에 따른 백신 소프트웨어는 월 1회 이상 주기적으로 갱신·점검하고, 바이러스 경보가 발령된 경우 및 백신 소프트웨어 제작 업체에서 업데이트 공지를 한 경우에는 즉시 최신 소프트웨어로 갱신·점검한다.

5. 출력·복사시 보호조치

① 신용정보회사등은 개인신용정보처리시스템에서 개인신용정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화 한다.

② 신용정보회사등은 개인신용정보를 조회(활용)하는 경우 조회자의 신원, 조회일시, 대상정보, 목적, 용도 등의 기록을 관리하여야 하며, 개인신용정보취급자가 개인신용정보를 보조저장매체에 저장하거나 이메일 등의 방법으로 외부에 전송하는 경우에는 관리책임자의 사전 승인을 받아야 한다.

③ 개인신용정보취급자는 제1항 및 제2항의 준수에 필요한 내부시스템을 구축하여야 하며 사전 승인시 승인신청자에게 관련 법령을 준수하여야 한다는 사실을 주지시켜야 한다.

Ⅲ. 관리적 보안대책

1. 신용정보관리·보호인

① 신용정보관리·보호인은 다음 각 호의 업무를 담당한다.

1. 신용정보의 수집·이용·제공·폐기 등 관리 및 보호계획의 수립 및 시행
2. 신용정보의 수집·이용·제공·폐기 등 관리 및 보호 실태와 관행에 대한 정기적인 조사 및 개선
3. 신용정보 열람 및 정정청구 등 신용정보주체의 권리행사 및 피해구제
4. 신용정보 유출 등을 방지하기 위한 내부통제시스템의 구축 및 운영
5. 임직원 및 전속 모집인 등에 대한 신용정보보호교육계획의 수립 및 시행
6. 임직원 및 전속 모집인 등의 신용정보보호 관련 법령 및 규정 준수 여부 점검

② 신용정보관리·보호인은 제1항의 업무처리에 따른 기록을 3년간 보존하며, 점검결과를 경영진에 보고하고 업무처리절차에 적절히 반영하여야 한다.

2. 개인신용정보의 조회권한 구분

① 신용정보관리·보호인은 개인신용정보 조회 권한이 직급별·업무별로 차등 부여되도록 하여야 한다.

② 신용정보회사등은 개인신용정보의 조회기록에 대하여는 다음 각 호에 따라 주기적으로 그 적정성 여부를 점검하여야 하며, 점검결과를 업무에 반영하여야 한다.

1. 개인신용정보취급자의 개인신용정보 취급상황을 확인할 수 있는 수단 및 이의 점검·감사체제 정비
2. 개인신용정보 이상 과다 조회 부서 및 직원 등에 대해 수시 점검 실시
   가. 조회 권한을 초과하여 고객 정보 조회를 일정횟수 이상 시도한 직원에 대한 통제장치 마련
   나. 영업점 및 신용정보 관리부서의 개인신용정보 조회 건수에 대해 정기적으로 점검하고 조회건수가 평소보다 급증한 부서 및 직원들을 샘플링하여 점검 실시

③ 신용정보 관리·보호인은 개인신용정보취급자가 입력하는 조회사유의 정확성 등 신용조회기록의 정확성을 점검하여야 한다.

3. 개인신용정보의 이용제한 등

① 신용정보회사등은 신용평가모형 또는 위험관리모형 개발 위탁시 개인신용정보를 제공할 수 없다. 다만, 모형 개발을 위하여 불가피한 경우에는 실제 개인인신용정보를 변환하여 제공한 후 모형 개발 완료 즉시 삭제하여야 한다.

② 신용조회회사가 신용평가모형 및 위험관리모형을 개발하는 경우, 개인신용정보를 사용하지 않으면 모형 개발 또는 검증 등이 불가능하여 불가피하게 필요한 경우 외에는 실제 개인신용정보를 사용하여서는 아니 된다.

4. 제재기준 마련

신용정보회사등은 개인신용정보 오·남용에 대한 자체 제재기준을 마련하여야 한다.

[별표 4] 신용정보제공계약에 포함될 신용정보 보안관리 대책(제21조 관련)

1. 신용정보제공·이용자 간에 신용정보를 제공하는 경우

가. 제공되는 신용정보의 범위 및 제공·이용 목적

나. 제공된 신용정보의 업무목적 외 사용 및 제3자 앞 제공 금지에 관한 사항

다. 제공된 신용정보의 이용자 제한 및 전담 관리자 지정에 관한 사항

라. 신용정보제공·이용자간 신용정보 송수신시 정보유출 방지에 관한 사항

마. 신용정보의 사용·보관 기간 및 동 기간 경과 후 신용정보의 폐기·반납에 관한 사항

바. 가목부터 마목까지를 위반한 경우의 책임소재 및 제재에 관한 사항

2. 신용조회회사와 신용정보제공·이용자 간에 신용정보를 제공하는 경우

가. 1의 가목부터 마목까지의 사항

나. 신용정보를 제공받은 신용정보제공·이용자에 대한 이 법 등 관련 법규의 준수여부 점검 등에 관한 사항

다. 개인신용정보를 조회하는 근거가 되는 자료 또는 서류 등의 보관에 관한 사항

라. 개인신용정보 조회시 조회용도에 맞는 조회사유코드를 적절하게 입력하는 것에 관한 사항

마. 신용정보 보호 등을 위한 교육에 관한 사항

바. 가목부터 마목까지를 위반한 경우의 책임소재 및 제재에 관한 사항

3. 수집된 신용정보 처리 위탁에 따라 신용정보를 제공하는 경우

가. 1의 가목부터 마목까지의 사항

나. 수탁자에 대한 관리·감독에 관한 사항

다. 신용정보주체의 신용정보 보호 및 비밀유지에 관한 사항

라. 신용정보 처리 재위탁의 제한에 관한 사항

마. 수탁자가 위탁받은 업무를 재위탁하는 경우 위탁자에 대한 보고에 관한 사항

바. 그 밖에 신용정보 보호를 위하여 필요한 사항

사. 가목부터 바목까지를 위반한 경우의 책임소재 및 제재에 관한 사항

4. 신용정보 처리의 재위탁에 따라 제공하는 경우

가. 재위탁업무의 목적과 범위, 기간 및 재위탁하는 신용정보의 내용

나. 재수탁자 및 재수탁자의 임직원의 보안서약서 작성 및 제출에 관한 사항

다. 신용정보 보호 및 안전한 처리를 위한 기술적·물리적·관리적 보안대책에 관한 사항

라. 목적 달성 후 파기, 반납에 관한 사항 및 파기확인서 등 그 결과를 원수탁자에게 통보하는 사항

마. 원수탁자가 재수탁자를 관리·감독하는 사항(실태점검을 위하여 재수탁자의 업무공간에 출입하여 점검하는 사항을 포함한다)

바. 가목부터 마목까지를 위반한 경우의 책임소재 및 제재에 관한 사항

[별표 4의2]

신용정보 관리기준(제22조제1항 관련)

구 분			관리기준
1. 신용정보처리기준	1.1. 개인식별정보(영 제29조 각 호의 정보를 말한다)의 처리에 대한 동의	1.1.1. 동의 형태	▸ 개인신용정보 처리에 대한 동의와 별도 동의
		1.1.2. 동의 사항	▸ 개인식별정보의 수집·이용 목적 ▸ 수집하려는 개인식별정보의 항목 ▸ 수집된 개인식별정보의 보유 및 이용 기간 ▸ 동의 사항 변경 시 신용정보주체에게 고지 후 동의 획득
	1.2. 개인신용정보의 수집·이용에 대한 동의	1.2.1. (공통) 동의 및 고지사항	▸ 개인신용정보의 수집·이용 목적 ▸ 수집하려는 개인신용정보의 항목 ▸ 수집된 개인신용정보의 보유·이용 기간 ▸ 동의와 관련하여 녹취 시에는 녹취사실 고지 ▸ 영 제17조의2제4항에 따른 금융거래 등 상거래관계가 종료된 날에 관한 사항
	1.3. 개인신용정보의 제공에 대한 동의	1.3.1. (공통) 동의 및 고지사항	▸ 개인신용정보를 제공받는 자 ▸ 개인신용정보를 제공받는 자의 이용 목적 ▸ 제공하는 개인신용정보의 내용 ▸ 개인신용정보를 제공받는 자의 정보 보유 기간 및 이용 기간 ▸ 동의와 관련하여 녹취 시에는 녹취사실 사전고지 ▸ 영 제17조의2제4항에 따른 금융거래 등 상거래관계가 종료된 날에 관한 사항
		1.3.2. 필수적 제3자 제공에 대한 고지사항	▸ 개인신용정보의 필수적 제3자 제공과 금융거래 등 상거래 계약 체결 및 이행과의 관련성
		1.3.3. 선택적 제3자 제공에 대한 고지사항	▸ 개인신용정보의 선택적 제3자 제공은 금융거래 등 상거래 계약 체결에 필수적이지 않다는 사실 ▸ 개인신용정보의 선택적 제3자 제공 시의 혜택
	1.4. 동의를 받는 방법	1.4.1. 동의서 양식	▸ 필수적 동의사항과 선택적 동의사항을 구분하여 동의를 받는 경우 "필수사항"과 "선택사항"을 별도 페이지로 구분하거나 각각의 동의서 양식을 구분하는 등 신용정보주체가 각각의 동의사항을 쉽게 구분하여 이해할 수 있도록 조치 ▸ 개인신용정보를 제공받는 제3자가 복수인 경우 사업내용, 연관된 부가서비스 등을 기준으로 개별 또는 다수 그룹으로 구분
	1.5. 신용정보의 제공	1.5.1. 신용정보의 제공 계약	▸ 신용정보의 보안관리 대책에 대하여는 별표 4를 적용 ▸ 신용정보의 제공에 대한 신용정보의 기술적·물리적·관리적 보안조치에 관한 사항에 대하여는 별표 3을 적용

구 분			관리기준
		1.5.2. 법 제32조제6항에 따른 개인신용정보의 제공	▸ 법 제32조제7항에 따라 개인신용정보 제공 사실 통지
		1.5.3. 신용정보를 제공받는 자의 확인	▸ 개인신용정보를 제공받는 자의 신원과 이용 목적을 확인 ▸ 1.5.1.에 따른 신용정보의 이용·보관 기간 및 동 기간 경과 후 신용정보의 폐기 또는 반납에 관한 사항의 결과 확인
	1.6. 신용정보의 삭제	1.6.1. 파기의 방법	▸ 삭제 후 복구 및 재생되지 않는 방법으로 조치
	1.7. 개인신용정보의 보유기간 등 (법 제20조의2)	1.7.1. 선택적 신용정보 삭제	▸ 법 제20조의2제1항에 따른 금융거래 등 상거래관계가 종료된 날부터 3개월 내에 선택적 신용정보 삭제
		1.7.2. 필수적 신용정보 분리 보관 및 접근제한	▸ 법 제20조의2제1항에 따라 필수적 신용정보(이하 "필수적 신용정보")를 관리하는 경우 현재 거래 중인 고객 정보와 분리 보관 ▸ 필수적 신용정보를 관리하는 관리책임자 지정 ▸ 관리책임자로부터 권한을 부여받은 개인신용정보취급자에 한하여 필수적 신용정보 접근 가능 ▸ 필수적 신용정보의 취급 권한부여 및 이용 내역 기록보존 (최소 3년)
		1.7.3 신용정보 삭제	▸ 법 제20조의2제2항에 따라 금융거래 등 상거래관계가 종료된 날부터 최장 5년내에 신용정보 삭제 ▸ 개인신용정보 삭제의 시행 및 확인은 신용정보관리·보호인의 책임 하에 수행 ▸ 신용정보관리·보호인은 개인신용정보 삭제 후 파기 결과를 확인 ▸ 신용정보제공·이용자는 개인신용정보의 삭제에 관한 사항 기록·관리
		1.7.4 신용정보의 보관	▸ 1.7.2의 필수적 신용정보 취급자 제한을 준용
	1.8.1. 신용정보 처리의 위탁	1.8.1. 신용정보 보호 조치의무	▸ 1.5.1. 신용정보의 제공계약 준용
		1.8.2. 법 제17조제5항에 따른 수탁자의 교육의 내용	▸ 신용정보 보호 관련 법령 및 제도의 내용 ▸ 신용정보의 보호 및 안전한 처리에 관한 사항
2. 신용정보관리·	2.1. 신용정보 관리·보호인	2.1.1. 신용정보관리·보호인의 업무	▸ 법 제20조제4항에 따른 업무 ▸ 별표 3의 관리적 보안대책에서 정하는 업무 ▸ 정보유출 대응매뉴얼(contingency plan) 마련 ▸ 관리적 보안대책 시행결과에 따른 시정·개선에 필요한 조치
		2.1.2.	▸ 신용정보관리·보호인을 지정하거나 변경하는 경우 신용정보

구 분			관리기준
보호인		신용정보관리·보호인의 공개	관리·보호인의 지정 및 변경 사실, 성명과 부서의 명칭, 전화번호 등 연락처를 홈페이지 등을 통하여 공개 ▸ 신용정보관리·보호인을 공개하는 경우 신용정보 보호와 관련한 고충처리 및 상담을 실제로 처리할 수 있는 연락처(담당자의 성명, 부서의 명칭, 전화번호)를 함께 기재
3. 신용정보의 누설 발생 시 조치	3.1. 개인신용정보의 누설의 예시	3.1.1. 신용정보회사등의 신용정보에 대한 통제 상실 또는 권한 없는 자의 접근	※ 신용정보회사등가 개인신용정보에 대하여 통제를 상실하거나 권한 없는 자의 접근을 허용한 경우로서 아래의 예시 및 이와 유사한 경우 등에는 개인신용정보 누설로 볼 수 있음 ▸ 개인신용정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우 ▸ 개인신용정보가 저장된 데이터베이스 또는 개인신용정보처리시스템에 권한 없는 자가 접근한 경우 ▸ 신용정보회사등의 고의 또는 과실로 개인신용정보가 포함된 파일 또는 종이문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우
	3.2. 신용정보주체에 대한 누설의 통지	3.2.1. 통지 사항	▸ 누설된 신용정보의 항목 ▸ 누설된 시점과 그 경위 ▸ 누설로 인하여 발생할 수 있는 피해를 최소화하기 위하여 신용정보주체가 할 수 있는 방법 등에 관한 정보 ▸ 신용정보회사등의 대응조치 및 피해 구제절차 ▸ 신용정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
		3.2.2. 통지 시기 및 방법 등	▸ 신용정보회사등은 누설 발생 확인 시 3.2.1.의 사항을 서면, 전화, 전자우편 등의 방법으로 해당 신용정보주체에게 통지 ▸ 누설된 신용정보의 신용정보주체가 1만 명 이상인 경우에는 영 제34조의2제2항 각 호에 따른 추가적인 공개 조치 ▸ 3.2.1.의 사항 통지 후 미확인사실에 대하여는 확인즉시 신용정보주체에게 통지
	3.3. 누설 신고	3.3.1. 신고 방법	▸ 서면, 전자우편, 모사전송 또는 이와 유사한 방법을 통하여 금융위원회 또는 금융감독원에 신용정보 누설신고서를 제출 ▸ 특별한 사정이 있는 경우에는 우선 금융위원회 또는 금융감독원에 누설사실을 알리고 추가 유출방지를 위한 조치를 취한 후 신용정보 누설신고서를 제출
4. 신용정보주체의 권리 보장	4.1. 신용정보 이용 및 제공 사실의 조회 (법 제35조)	4.1.1. 절차 보장	▸ 신용정보회사등은 신용정보주체가 영 제30조제3항의 방법으로 본인확인 후 개인신용정보 이용 및 제공 사실을 조회할 수 있는 개인신용정보조회시스템을 홈페이지 등을 통하여 제공 ▸ 신용정보주체가 개인신용정보조회시스템 등에 대한 접근을 용이하게 할 수 있도록 편의조치
		4.1.2. 신용정보 이용 및 제공 사실 통지	▸ 법 제35조제2항에 따른 통지의 간격은 연1회 이상 가능 하도록 통지 시스템 구축 ▸ 영 제30조제8항에 따른 수수료는 필요한 인적·물적 비용을

구 분			관리기준
		청구권 보장	고려하여 적정한 수준에서 채택
	4.2. 신용정보의 열람 및 정정청구권 (법 제38조)	4.2.1. 절차 보장	▸ 신용정보주체가 영 제30조제3항의 방법으로 본인확인 후 본인 신용정보를 열람·정정 청구 가능한 시스템 또는 절차 마련 ▸ 신용조회회사는 법 제39조 및 영 34조에 따라 개인신용정보주체에게 본인정보에 대한 무료 열람권 제공 ▸ 신용정보의 정정청구 접수 후 7일 이내에 신용정보주체에 처리결과 및 법 제38조제4항에 따른 시정요청 절차 고지
		4.2.2. 사실 조사	▸ 정정청구를 접수받은 경우 지체 없이 사실 조사에 착수 ▸ 정정 사유 확인 즉시 개인신용정보전산시스템에 정정청구 중 또는 사실조회 중임을 기입 및 해당 신용정보의 제공·이용 중단 ▸ 정정 후 최근 6개월 이내에 제공받은 자와 해당 신용정보주체가 요구하는 자에게 정정 사실 고지
	4.3. 상거래 거절 근거 신용정보의 고지 (법 제36조)	4.3.1. 절차 보장	▸ 본인확인 방법 및 신용정보주체의 요구에 따른 처리결과 고지의 업무처리방법 마련
		4.3.2. 고지 사항	▸ 영 제31조제1항 각 호에서 정하는 신용정보 중 신용정보주체와의 상거래관계 설정의 거절이나 중지의 근거가 된 신용정보 ▸ 해당 신용정보를 제공한 신용조회회사 및 신용정보집중기관의 명칭, 주소, 연락처 ▸ 신용조회회사 및 신용정보집중기관이 상거래관계의 설정을 거절하거나 중지하도록 결정한 것이 아니라는 사실 ▸ 신용조회회사 또는 신용정보집중기관으로부터 제공받은 정보 외에 다른 정보를 함께 사용하였을 경우에는 그 사실 및 그 다른 정보
	4.4. 개인신용정보 제공·이용 의 철회권 (법 제37조)	4.4.1. 절차 보장	▸ 신용정보제공·이용자는 개인신용정보 제공·이용 동의 철회 청구 시스템 또는 절차 마련 ▸ 1.3.3.의 고지사항에 법 제37조제1항·제2항 및 영 제32조제1항 및 제2항에 따른 개인신용정보 제공·이용 동의 철회권 및 영업 목적 연락중지 청구권 행사방법 및 담당자 연락처 등을 포함
		4.4.2. 고지 사항 등	▸ 철회청구를 받은 날부터 1개월 내에 해당 제3자에 대한 신용정보의 신규 제공중단 및 신용정보의 영업 목적 연락중지 조치 ▸ 제공동의 철회권 행사로 인하여 중단되는 서비스가 있는 경우 이에 대한 설명 의무
	4.5. 개인신용정보의 삭제 요구권 (법 제38조	4.5.1. 절차 보장	▸ 개인신용정보주체가 본인 개인신용정보의 삭제를 요구할 수 있는 절차 마련
		4.5.2. 고지 사항 등	▸ 개인신용정보 삭제로 인하여 개인신용정보주체에게 불이익 발생할 경우 이에 대한 충분한 사전 설명 후 삭제 조치 ▸ 삭제 후 그 결과를 개인신용정보주체에게 통지

구 분			관리기준
	의3)		▸ 삭제청구에 불구하고 개인신용정보를 법 제38조의3제1항 단서에 의하여 보관하는 경우에는 보관사유의 근거 및 안전한 보관에 관한 사항을 개인신용정보주체에 통지 ▸ 개인신용정보 삭제청구 처리 대장(최소 3년이상 보존)
5. 신용정보활용체제의 공시(법 제31조)	5.1. 공시 방법	5.1.1. 신용정보활용체제의 변경	▸ 신용정보활용체제를 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 지속적으로 공개 ▸ 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개
	5.2. 작성기준	5.2.1. 필수적 기재사항	▸ 관리하는 신용정보의 종류 및 이용 목적 ▸ 신용정보를 제3자에게 제공하는 경우 제공하는 신용정보의 종류, 제공 대상, 제공받는 자의 이용 목적 ▸ 신용정보의 보유 기간 및 이용 기간이 있는 경우 해당 기간, 신용정보 파기의 절차 및 방법 ▸ 법 제17조에 따라 신용정보의 처리를 위탁하는 경우 그 업무의 내용 및 수탁자 ▸ 신용정보주체의 권리와 그 행사방법 ▸ 법 제20조제3항에 따른 신용정보관리·보호인 또는 신용정보 관리·보호 관련 고충을 처리하는 사람의 성명, 부서 및 연락처 ▸ 신용등급 산정에 반영되는 신용정보의 종류, 반영비중 및 반영기간(신용조회회사만 해당)
		5.2.2. 임의적 기재사항	▸ 신용정보주체의 권익침해에 대한 구제방법 ▸ 신용정보의 열람청구를 접수·처리하는 부서
6. 신용조회업무	6.1. 정보의 수집	6.1.1. 수집의 제한	▸ 법에서 수집을 금지하는 정보가 수집되지 않도록 수집항목을 구성·관리 ▸ 수집항목의 적정성을 정기적으로 점검하고 필요시 수집항목을 조정
		6.1.2. 수집절차·방법의 표준화	▸ 표준화된 정보수집을 위한 정보수집 기준 마련 ▸ 정보 수집시 수집정보의 정확성을 확인할 수 있는 방법 및 절차 마련
		6.1.3. 수집정보의 검증 및 정정	▸ 수집된 정보의 정확성을 검증하는 방법·기준 및 업무처리절차 마련 ▸ 부정확하거나 사실과 다른 것으로 확인된 정보의 정정·삭제 기준 및 업무처리절차 마련 ▸ 검증업무가 수집업무와 독립적으로 처리될 수 있는 업무처리절차 및 기준 마련
	6.2. 신용등급의 산출 및 제공	6.2.1. 신용등급의 산출	▸ 기업평가시 평가대상 기업의 규모 및 업종에 따른 평가기준 마련 ▸ 등급산출의 적정성 심의 기준, 절차 마련(등급평정위원회 등) ▸ 심의시 독립적인 의사결정 보장을 위한 업무처리절차 및 기준 마련
		6.2.2.	▸ 연 1회 이상 평가모형의 변별력 검증을 시행하고 관련 기

구 분			관리기준
		모형검증 등 사후 관리	록을 보존(최소 3년) ▸ 평가업무와 독립적으로 검증 업무가 처리될 수 있는 업무처리절차 및 기준 마련 ▸ 모형검증 결과를 보고받는 별도 위원회 구성에 관한 사항 ▸ 기업평가이후 피평가기업의 신용상태에 중대한 영향을 미치는 상황 변화 등이 발생한 경우 신용등급 변경 기준 및 업무처리절차
		6.2.3. 이해상충 방지	▸ 등급 산출과 관련한 이해상충 방지체계 마련 ▸ 기업평가 관련 평가조직 및 영업조직의 분리
		6.2.4. 정보제공시 차별·강요금지	▸ 의뢰인에게 정보제공시 합리적 이유 없는 차별적 취급 금지 ▸ 평가서 발급 의뢰인에게 상품·서비스의 가입·이용 강제 금지

[별표 5]

공공단체의 지정범위(제24조 관련)

1. 「한국은행법」에 따른 한국은행
2. 「금융위원회의 설치 등에 관한 법률」에 따른 금융감독원
3. 「자본시장과 금융투자업에 관한 법률」에 따른 한국거래소
4. 「한국장학재단 설립 등에 관한 법률」에 따른 한국장학재단
5. 「한국전력공사법」에 따른 한국전력공사
6. 「대한무역투자진흥공사법」에 따른 대한무역투자진흥공사
7. 「한국가스공사법」에 따른 한국가스공사
8. 「한국광물자원공사법」에 따른 한국광물자원공사
9. 「예금자보호법」에 따른 예금보험공사
10. 「금융회사부실자산 등의 효율적 처리 및 한국자산관리공사의 설립에 관한 법률」에 따른 한국자산관리공사
11. 「공인회계사법」에 따른 한국공인회계사회
12. 「국민연금법」에 따른 국민연금관리공단
13. 「국민건강보험법」에 따른 국민건강보험공단
14. 「산업재해보상보험법」에 따른 근로복지공단

[별표 5의2]

신용정보집중기관 허가 세부요건

(제26조의4제2항 관련)

1. 인력

가. 신용정보주체를 보호하고 신용정보를 집중관리·활용하기 위한 전문성을 갖춘 다음의 어느 하나에 해당하는 인력을 적절하게 확보하고 배치할 것

(1) 공인회계사, 변호사 등의 자격 소지자

(2) 영 제2조제3항제1호·제3호·제4호에 해당하는 기관, 영 제5조제1항 각 호에 해당하는 기관 또는 다음 각 목의 금융 관련 단체에서 3년 이상 신용정보 관련 업무에 종사한 경력이 있는 사람 5명 이상이 포함될 것

가. 신용조회회사

나. 신용정보집중기관

다.「민법」 제32조에 따라 기획재정부장관의 허가를 받아 설립된 금융결제원

라.「보험업법」에 따른 보험요율 산출기관

(3) 그 밖에 신용정보집중기관 업무에 대한 전문성이 상기 인력에 준한다고 볼 수 있는 상당한 근거가 있는 자

나. 신용정보집중기관의 임원이 다음의 어느 하나에 해당하는 사실이 없을 것

(1) 최근 5년간 종합신용정보집중기관에 금융질서문란행위자로 등록된 사실

(2) 그 밖에 금융위원회가 신용정보집중기관의 경영의 건전성에 현저한 영향을 미칠 수 있다고 인정하는 것으로서 해당 대상자가 충분한 반증을 제시하지 못하는 사실

2. 물적 설비

가. 제26조의4제1항에 따른 정보처리·정보통신설비를 갖출 것

나. 업무공간과 사무장비

(1) 집중관리·활용하는 신용정보 중에서 개인의 건강에 대한 정보 등 특별히 민감한 정보는 별도 업무공간을 갖추는 등 정보차단벽(Chinese Wall)이 설치될 수 있도록 할 것

(2) 부서인원 대비 충분한 업무공간 및 사무장비를 갖출 것

(3) 내부기관 및 감독기관 등이 감독·검사업무를 수행함에 있어 법적 장애가 없을 것

다. 업무의 연속성을 유지할 수 있는 보완설비

(1) 파업 등 불시사태 또는 비상사태에 대비한 비상계획(Contingency Plan)이 마련되어 있을 것

3. 사업계획

가. 사업계획이 이 법 및 타 법령에 의하여 신용정보집중기관이 수행하도록 정한 업무를 적절하게 수행할 수 있을 것

나. 내부통제장치 및 신용정보주체 보호

(1) 총회(이사회가 설치된 경우 이사회 포함)와 경영진의 관계, 총회(이사회가 설치된 경우 이사회 포함)의 구성 및 운영방향, 감사의 권한과 책임 등이 적절할 것

(2) 임직원의 법규준수, 정보보호 및 임직원 위법행위 예방을 위한 적절한 감독 및 내부통제체계가 구축되어 있을 것

4. 업무방법

가. 업무방법의 마련 등이 집중관리·활용에 참여하는 기관의 종류에 따른 대표성과 중립성을 만족할 것

(1) 종합신용정보집중기관의 경우 업무방법에 관한 절차 및 내용에 있어서 참여하는 기관 및 집단간의 대표성과 중립성이 만족될 수 있도록 업무방법을 마련할 것

(2) 같은 종류의 금융회사 또는 같은 종류의 사업자간에 집중관리·활용하는 신용정보의 경우 금융회사 또는 사업자간 대표성과 중립성이 만족될 수 있도록 업무방법을 마련할 것

나. 신용정보주체를 보호할 수 있는 관리체계가 마련되어 있을 것

다. 신용정보의 효율적 이용과 체계적 관리를 도모할 수 있는 관리체계가 마련되어 있을 것

5. 지배구조 관련 사항

가. 「민법」 제32조에 따라 설립된 비영리법인일 것

나. 사원구성계획이 집중관리·활용에 참여하는 기관의 종류에 따른 대표성과 중립성을 만족할 것

6. 제26조의3에 따른 업무분리계획(종합신용정보집중기관이 기타업무를 수행하는 경우에 한정한다)

가. 재무에 관한 사항

(1) 집중기관업무와 기타업무사이에 별도의 회계장부를 마련하고 구분하여 회계처리 할 것

(2) 집중기관업무에 관련된 예·결산에 대하여 신용정보집중관리위원회의 의결을 받을 것

나. 인사에 관한 사항

(1) 임원(대표권을 가진 이사, 감사를 제외한다)이 집중기관업무와 기타업무를 겸직하지 아니할 것

(2) 집중기관업무의 독립성 및 연속성을 담보할 수 있는 인사관리체계를 마련할 것

다. 조직에 관한 사항

(1) 집중기관업무와 기타업무 간 정보의 교류를 차단할 것

(2) 집중기관업무와 기타업무 사이에 이해상충이 발생할 가능성을 파악·평가하고, 이를 적절히 관리할 수 있는 내부통제기준을 마련할 것

라. 시설에 관한 사항

(1) 집중기관업무와 기타업무 사이에 사무실 등 업무공간을 분리할 것

(2) 집중기관업무와 기타업무 사이에 전산자료가 독립적으로 저장되어 관리·감독·열람될 수 있도록 할 것

[별표 6]

신용정보 등록 및 이용기준(제24조의2제2항 및 제26조의4제3항 관련)

1. 식별정보

등록정보	등록기관	등록기준		이용기관
		대상주체	등록시기	
영 [별표2]의 식별정보	영 제21조제2항의 기관 중 당해 등록정보 보유기관	해당 개인, 기업 및 법인	등록사유발생시	식별정보와 연결된 정보의 이용기관

1) 영 제21조제2항의 기관이 「자산유동화에 관한 법률」제10조제1항에 따라 유동화자산의 관리를 위탁받은 경우 해당 유동화자산의 등록정보 보유기관으로 본다. 이하 이 표에서 같다.

2. 거래정보

(1) 개인

등록정보	등록기관	등록기준		이용기관
		대상주체	등록시기	
가. 대출, 당좌거래 등 관련 거래 정보				
대출현황(대출일자, 대출금액, 담보현황, 카드론·현금서비스 실적 등 포함)	영 제21조제2항의 기관 중 해당 등록정보 보유기관	해당 개인 (단, 종합신용정보집중기관은 전산수용능력등을 감안하여 대출금 집중기준을 조정할 수 있음)	등록사유발생일로부터 7영업일 이내	○ 영 제21조제2항의 기관 ○ 법 제4조에 따른 신용정보회사(신용정보회사는 해당 정보를 영 제21조제2항의 기관에 대해서만 제공할 수 있음)
대출성상품에 대한 청약철회에 따른 원상회복채권 정보	영 제21조제2항의 기관 중 해당 등록정보 보유기관	해당 개인	위와 같음	위와 같음
채무보증현황(채무보증일자, 채무보증금액 등 포함)	영 제21조제2항의 기관 중 해당 등록정보 보유기관	위와 같음	위와 같음	위와 같음
당좌·가계당좌예금개설 및 해지 현황	은행(농·수협 포함)	위와 같음	위와 같음	○ 영 제21조제2항의 기관 ○ 법 제4조에 따른 신용정보회사
나. 신용카드 관련 거래 정보				
신용카드현황(발급·해지사실 및 결제금액[주] 포함)	은행(농·수협 포함) 및 여신전문금융회사	위와 같음	위와 같음	위와 같음

2개 이상의 신용카드를 소지한 신용정보주체에 관한 관련거래 정보(신용판매·현금서비스 이용금액, 신용판매·현금서비스 리볼빙 이용잔액, 연체금액, 신용판매·현금서비스 신용공여한도 등 포함)	은행(농·수협 포함) 및 여신전문금융회사 중 해당 등록정보 보유기관	위와 같음	위와 같음	은행(농·수협 포함) 및 여신전문금융회사 중 등록기관에 해당하는 자
신용카드의 도난·분실 등 사고 발생에 관한 정보, 사고 종결에 관한 보상 및 처리정보 [주]	위와 같음	위와 같음	위와 같음	위와 같음
다. 보험계약 관련 거래정보				
보험계약 현황(보험계약일, 보험기간, 보험상품명, 급부명, 가입금액, 보험료, 보험회사명 및 보험계약상태, 피보험목적물 정보, 청약정보(청약시부터 계약 또는 거절시까지만 보유 가능) 등 포함)	보험회사, 수산업협동조합, 신용협동조합, 새마을금고 및 체신관서 중 해당 등록정보 보유기관	해당 개인	위와 같음	보험회사, 수산업협동조합, 신용협동조합, 새마을금고 및 체신관서 중 등록기관에 해당하는 자
피보험자 또는 보험금 청구권자에 관한 정보(성명, 개인식별번호, 직업 및 보험계약자와의 관계에 관한 정보 등 포함)	위와 같음	해당 개인이 체결한 보험계약(이하 "해당 보험계약"이라 함)의 피보험자 또는 보험금 청구권자	위와 같음	위와 같음
모집업무수탁자 정보(해당 보험계약을 모집한 모집업무수탁자의 이름·명칭 및 등록번호 등 포함)	위와 같음	해당 보험계약을 모집한 보험설계사, 보험대리점 또는 보험중개사	위와 같음	위와 같음
보험금 청구·지급 현황(사고접수일자, 보험금 청구일자, 보험금 지급일자, 보험금액, 실지급금액, 병원·정비공장 정보 등 포함)	위와 같음	해당 보험계약의 보험금 청구권자	위와 같음	위와 같음
보험금 지급사유(사고발생일시, 사고원인, 질병·부상·치료정보, 피해물 및 보상정보, 자동차보험의 경우에는 사고운전자	위와 같음	위와 같음	위와 같음	위와 같음

성명, 주민등록번호 등 포함)				
피해자 정보(피해자의 성명, 주민등록번호 포함)	위와 같음	해당 보험계약에서 보장하는 보험사고의 피해자	위와 같음	위와 같음
라. 금융투자상품 매매 관련				
코넥스소액전용투자계좌 관련 계좌 개설 및 폐쇄 정보 등	투자중개업자	해당 개인	등록사유발생시	투자중개업자

주) 신용카드결제금액, 신용카드의 도난·분실 등 사고 발생에 관한 정보, 사고 종결에 관한 보상 및 처리정보는 해당 신용정보를 보유한 신용카드업자가 동의하는 경우에 한함

(2) 기업 및 법인

등록정보	등록기관	등록기준		이용기관
		대상주체	등록시기	
가. 대출, 당좌거래 등 관련 거래 정보				
신용 공여 현황[1] (담보, 한도거래, 신용공여기간 등 포함)	영 제21조제2항의 기관 중 해당 등록정보 보유기관	○해당 기업 및 법인(종합신용정보집중기관은 전산수용능력 등을 감안하여 대출금 집중기준을 조정할 수 있음) ○주채무계열 및 기타 계열기업군 소속기업체	신용정보집중관리위원회가 정함	○ 영 제21조제2항의 기관 ○ 법 제4조에 따른 신용정보회사(신용정보회사는 해당 정보를 영 제21조제2항의 기관, 「공인회계사법」에 따른 공인회계사회, 영 제2조제3항제7호의 감사인 및 「자본시장과 금융투자업에 관한 법률」에 따른 신용평가회사에 대해서만 제공할 수 있음)
가계당좌·당좌예금 개설 및 해지 현황	은행(농·수협 포함)	○해당 기업 및 법인	위와 같음	○ 영 제21조제2항의 기관 ○ 법 제4조에 따른 신용정보회사
나. 신용카드 관련 거래 정보				
신용카드현황(발급·해지 사실 및 결제금액[2], 연체정보 포함)	은행(농·수협 포함) 및 여신전문금융회사	위와 같음	등록사유발생일로부터 7영업일 이내	위와 같음

신용카드의 도난·분실 등 사고 발생에 관한 정보[2], 사고 종결에 관한 보상 및 처리정보[2]	위와 같음	위와 같음	위와 같음	은행(농·수협 포함) 및 여신전문금융회사
다. 금융투자상품 매매 관련				
코넥스소액전용투자계좌 관련 계좌 개설 및 폐쇄 정보 등	투자중개업자	해당 기업체	등록사유발생시	투자중개업자

주 1) 은행 및 금융투자회사는 「은행업감독규정」 제3조 및 「금융투자업규정」 제8-33조에서 정한 신용공여, 그 밖의 금융회사는 이에 준하는 정보

2) 신용카드결제금액, 신용카드의 도난·분실 등 사고 발생에 관한 정보, 사고 종결에 관한 보상 및 처리정보는 해당 신용정보를 보유한 신용카드업자가 동의하는 경우에 한함

3. 신용도판단정보

등록정보	등록기관	등록기준		이용기관
		대상주체	등록시기	
대출금 등의 연체 현황	영 제21조제2항의 기관 중 해당 등록정보 보유기관	○해당 개인 ○해당 기업 및 법인 ○관련인[주]	신용정보집중관리위원회가 정함	○ 영 제21조제2항의 기관 ○ 법 제4조에 따른 신용정보회사
대위변제, 대지급 발생 현황	위와 같음	위와 같음	위와 같음	위와 같음
무보증사채 상환불이행 현황	위와 같음	위와 같음	위와 같음	위와 같음
어음·수표 거래정지 처분 또는 부도거래 현황	위와 같음	○해당 기업 및 법인 ○관련인	위와 같음	위와 같음
금융투자상품의 투자매매·중개 관련 정보	금융투자업자 중 등록정보 보유기관	○해당 개인 ○해당 기업 및 법인	위와 같음	위와 같음
영 [별표 2]의 금융질서 문란정보	영 제21조제2항의 기관 중 해당 등록정보 보유기관	○해당 개인 ○해당 기업 및 법인 ○관련인	위와 같음	위와 같음
대출성상품에 대한 청약철회에 따른 원상회복의무 불이행정보	영 제21조제2항의 기관 중 해당 등록정보 보유기관	○해당 개인	위와 같음	위와 같음

주) 영 제2조제1항제3호 각 목의 어느 하나에 한함

4. 신용거래능력판단정보

등록정보	등록기관	등록기준		이용기관
		대상주체	등록시기	
증자 및 사채발행계획 확정내용	협조기관 (금융감독원)	○해당 기업 및 법인(종합신용	신용정보집중관리위원회가 정	○ 영 제21조제2항의 기관

		정보집중기관은 전산수용능력등을 감안하여 집중기준을 조정할 수 있음) ○ 주채무계열 및 기타 계열기업군 소속기업체	함	○ 법 제4조에 따른 신용정보회사
영 제2조제1항제4호에 따른 기업의 개황, 사업의 내용, 재무에 관한 사항, 감사인의 감사의견 및 납세실적 등과 영 [별표 2]에 의한 신용능력정보	영 제21조제2항의 기관 중 해당 등록정보 보유기관	해당 기업 및 법인	위와 같음	위와 같음

5. 기술신용정보

등록정보	등록기관	등록기준		이용기관
		대상주체	등록시기	
기술신용정보(기술신용평가가액과 이와 관련된 평가의견은 제외한다.)주)	○기술신용보증기금 ○신용조회회사 중 해당 등록정보 보유기관	해당 기업 및 법인	등록사유발생일로부터 7영업일 이내	-
기업 및 법인의 기술신용등급, 신용공여 현황 및 신용도판단정보	영 제21조제2항의 기관 중 해당 등록정보 보유기관	위와 같음	위와 같음	○ 기술신용보증기금 ○ 신용조회회사 중 기술신용정보 등록기관

주) 종합신용정보집중기관이 영 제21조의2제2항제2호에 따른 업무를 수행하는 경우에 한하여 등록기관으로부터 해당 정보를 집중

6. 공공정보

등록정보	등록기관	등록기준		이용기관
		대상주체	등록시기	
-경제법령 위반	영 제21조제2항의 기관 중 해당 등록정보 보유기관	위반자	신용정보집중관리위원회가 정함	○ 영 제21조제2항의 기관 ○ 법 제4조에 따른 신용정보회사
-사망자정보, 주민등록번호 또는 성명의 변경정	법 제23조제2항에 따른 공공기관 또	해당 개인	○법 23조제2항에 따른 공공	위와 같음

보	는 영 제21조제2항의 기관 중 해당 등록정보 보유기관		단체 보유정보 등록 시는 당해 공공기관과 협의하여 정함 ○ 영 제21조제2항의 기관 보유정보 등록시기는 신용정보집중관리위원회가 정함	
-국외이주신고 및 이주포기신고정보	위와 같음	위와 같음	위와 같음	위와 같음
-회생·간이회생·개인회생 결정, 파산·면책 결정, 채무불이행자명부 등재 ·말소 결정 등 법원의 재판·결정정보 -국세·지방세·관세의 체납정보 -과태료·사회보험료·공공요금 등의 체납정보 -신용회복위원회의 신용회복지원협약에 따른 신용회복지원 확정 정보 -한국자산관리공사의 신용회복지원 관련 규정에 의한 채무재조정 약정정보 -국민행복기금이 협약금융기관등으로부터 채권을 매입한 정보 및 채무조정 약정을 체결한 정보 -그밖의 공공정보(특허권, 법인등록에 관한 정보등)	위와 같음	해당 주체	○ 해당 공공기관과 협의하여 정함 ○ 영 제21조제2항에 따른 기관 보유정보 등록시기는 신용정보집중관리위원회가 정함	위와 같음
-고용보험, 산업재해보상보험, 국민건강보험 및 국민연금의 납부에 관한 정보	법 제23조제2항에 따른 공공기관	위와 같음	해당 공공기관과 협의하여 정함	신용조회회사(신용등급 산정에 활용하는 경우에 한한다.)
-전기사용에 관한 정보로서 전력사용량 및 전기요금 납부정보	위와 같음	위와 같음	위와 같음	위와 같음
-정부납품실적 및 납품액	위와 같음	위와 같음	위와 같음	영 제21조제2항의 기관, 신용조회회사(단, 신용조회회사는 영 제21조제2항의 기관 이외에는 제공할 수 없음)

[별지 제1호 서식] 신용정보업 (예비허가, 허가) 신청서(제5조제2항제1호 관련)

(앞면)

<table>
<tr><td colspan="5">신용정보업 (예비허가, 허가) 신청서</td><td>처리기간
: 90일
(예비허가를 받은 경우: 30일</td></tr>
<tr><td rowspan="3">신청인</td><td>성명(대표자)</td><td></td><td>주민등록번호</td><td colspan="2"></td></tr>
<tr><td>상호 또는 명칭</td><td colspan="4">(전화번호)</td></tr>
<tr><td>본점 및 영업소의 소재지</td><td></td><td>자본금 또는 기본재산</td><td colspan="2"></td></tr>
<tr><td>법인의 목적</td><td colspan="5"></td></tr>
<tr><td>허가받고자 하는 업무</td><td colspan="5"></td></tr>
<tr><td colspan="6">「신용정보의 이용 및 보호에 관한 법률 시행령」 제4조제1항에 따라 위와 같이 신청합니다.

0000년 00월 00일
신청인 _____ 서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="5">※구비서류
1. 정관 및 법인등기부 등본
2. 재무제표
3. 2년간의 사업계획서 및 예상수지계산서
4. 그 밖에 별표 1의2의 제1호가목에 따른 서류 및 이와 관련한 부속서류</td><td>수수료
없음</td></tr>
</table>

(뒷면)

<table>
<tr><td colspan="2">대표자 및 임원에 관한 사항</td><td></td></tr>
<tr><td colspan="2">인력에 관한 사항</td><td></td></tr>
<tr><td rowspan="2">물적 시설에 관한 사항</td><td>정보처리·정보통신설비 / 전산설비 및 자료관리체계</td><td></td></tr>
<tr><td>그밖의 시설</td><td></td></tr>
</table>

[별지 제2호 서식] 신용정보업 변경허가신청서(제5조제2항제2호 관련)

<table>
<tr><td colspan="4">신용정보업 변경허가신청서</td><td>처리기간
: 30일</td></tr>
<tr><td rowspan="3">신청인</td><td>대표자의 성명</td><td></td><td>신용정보업허가일자</td><td>0000년 00월 00일</td></tr>
<tr><td>상호</td><td></td><td>허가번호</td><td></td></tr>
<tr><td>본점 소재지</td><td colspan="3"></td></tr>
<tr><td>변경
사항</td><td colspan="4"></td></tr>
<tr><td colspan="5">「신용정보의 이용 및 보호에 관한 법률 시행령」 제4조제1항에 따라 위와 같이 신청합니다.

0000년 00월 00일
신청인 _____ 서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※구비서류
1. 변경사항을 확인할 수 있는 서류 1부</td><td>수수료
없음</td></tr>
</table>

[별지 제2의2호 서식] 양도·양수·분할·합병 (예비인가, 인가) 신청서(제5조제2항 제3호 관련)

<table>
<tr><td colspan="6">양도·양수·분할·합병 (예비인가, 인가)신청서</td><td colspan="3">처리기간
90일
(예비인가를 받은 경우 30일)</td></tr>
<tr><td rowspan="8">양수
합병
법인</td><td>상호</td><td colspan="3"></td><td>대표자</td><td>성명</td><td></td></tr>
<tr><td colspan="3"></td><td></td><td>주민등록번호</td><td></td></tr>
<tr><td rowspan="2">임원에 관한 사항</td><td>구분</td><td>성명</td><td colspan="4">주민등록번호</td></tr>
<tr><td></td><td></td><td colspan="4"></td></tr>
<tr><td>본점소재지</td><td colspan="3"></td><td>연락처</td><td colspan="2">전화:
팩스:</td></tr>
<tr><td>법인의 목적</td><td colspan="6"></td></tr>
<tr><td>영위하고자 하는 업무</td><td colspan="6"></td></tr>
<tr><td colspan="4">인력 및 물적시설에 관한 사항</td><td colspan="4"></td></tr>
<tr><td colspan="4">자본금 또는 기본재산에 관한 사항</td><td colspan="4"></td></tr>
<tr><td rowspan="8">양도
피합병
법인</td><td>상호</td><td colspan="3"></td><td>대표자</td><td>성명</td><td></td></tr>
<tr><td colspan="3"></td><td></td><td>주민등록번호</td><td></td></tr>
<tr><td rowspan="2">임원에 관한 사항</td><td>구분</td><td>성명</td><td colspan="4">주민등록번호</td></tr>
<tr><td>대표이사
감사</td><td></td><td colspan="4"></td></tr>
<tr><td>본점소재지</td><td colspan="3"></td><td>연락처</td><td colspan="2">전화:
팩스:</td></tr>
<tr><td>법인의 목적</td><td colspan="6"></td></tr>
<tr><td>영위하고자 하는 업무</td><td colspan="6"></td></tr>
<tr><td colspan="4">인력 및 물적시설에 관한 사항</td><td colspan="4"></td></tr>
<tr><td colspan="4">자본금 또는 기본재산에 관한 사항</td><td colspan="4"></td></tr>
<tr><td rowspan="6">존속
법인</td><td>상호</td><td colspan="3"></td><td>대표자</td><td>성명</td><td></td></tr>
<tr><td colspan="3"></td><td></td><td>주민등록번호</td><td></td></tr>
<tr><td rowspan="2">임원에 관한 사항</td><td>구분</td><td>성명</td><td colspan="4">주민등록번호</td></tr>
<tr><td></td><td></td><td colspan="4"></td></tr>
<tr><td>본점소재지</td><td colspan="3"></td><td>연락처</td><td colspan="2">전화:
팩스:</td></tr>
<tr><td>법인의 목적</td><td colspan="6"></td></tr>
</table>

	영위하고자 하는 업무	
	인력 및 물적시설에 관한 사항	
	자본금 또는 기본재산에 관한 사항	

「신용정보업감독규정」 제5조제2항에 따라 위와 같이 신용정보업의 (양도, 양수, 분할,분할합병, 합병)의 (예비인가, 인가)를 신청합니다.

0000년 00월 00일

신청인 _____ (인)

금융감독원장 귀하

※구비서류 1. 정관 및 법인등기부 등본	수수료
2. 재무제표 3. 사업양도·양수, 분할·합병 관련 계약서 또는 예약서 4. 그 밖에 별표 1의2의 제1호나목, 다목 및 라목의 구분에 따른 서류 및 이와 관련한 부속서류	없음

[별지 제2의3호 서식] 신용정보집중기관 허가신청서(제5조제2항제4호 관련)

<table>
<tr><td colspan="3">신용정보집중기관 허가신청서</td><td>처리기간
: 90일
(예비허가를 받은 경우 30일)</td></tr>
<tr><td rowspan="3">신청인에 관한 사항</td><td>집중기관의 명칭</td><td colspan="2"></td></tr>
<tr><td>대표자의 성명</td><td colspan="2"></td></tr>
<tr><td>소재지</td><td colspan="2"></td></tr>
<tr><td>허가받고자 하는 집중기관의 유형</td><td colspan="3">종합신용정보집중기관( ), 개별신용정보집중기관( )</td></tr>
<tr><td>집중관리·활용하려는 신용정보의 범위</td><td colspan="3"></td></tr>
<tr><td>교환대상자</td><td colspan="3"></td></tr>
<tr><td colspan="4">「신용정보의 이용 및 보호에 관한 법률 시행령」 제21조제1항에 따라 위와 같이 신청합니다.

0000년 00월 00일
신청인 _____ 서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="3">※구비서류
1. 정관 또는 정관(안)
2. 재산목록 및 그 증명서류
3. 2년간 사업연도분의 사업계획 및 수입·지출 예산을 적은 서류
4. 그 밖에 별표 1의2의 제2호에 따른 서류 및 이와 관련한 부속서류</td><td>수수료
없음</td></tr>
</table>

[별지 제3호 서식] 신용정보회사가 허가받은 사항에 관한 변경신고서(제9조제1항 관련)

<table>
<tr><td colspan="4">신용정보회사가 허가받은 사항에 관한 변경신고서</td><td>처리기간
15일</td></tr>
<tr><td rowspan="3">신고인</td><td>대표자의 성명</td><td></td><td>신용정보업
허가일자</td><td>0000년 00월 00일</td></tr>
<tr><td>상호</td><td></td><td>허가번호</td><td></td></tr>
<tr><td>본점소재지</td><td></td><td></td><td></td></tr>
<tr><td>변경
사항</td><td colspan="4">1. □ 자본금 또는 기본재산의 감소
2. □ 상호 등 정관의 변경</td></tr>
<tr><td>변경
사유</td><td colspan="4"></td></tr>
<tr><td colspan="5">「신용정보의 이용 및 보호에 관한 법률 시행령」 제8조제1항에 따라 위와 같이 신고합니다.

0000년 00월 00일
신고인 _____서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※ 구비서류
1. 변경사항을 확인할 수 있는 서류
2. 제9조제2항 또는 제9조제3항에 따른 심사에 필요한 자료</td><td>수수료
없음</td></tr>
</table>

[별지 제4호 서식] 신용정보회사가 허가받은 사항에 관한 변경 보고서(제10조 관련)

<table>
<tr><td colspan="4">신용정보회사가 허가받은 사항에 관한 변경 보고서</td><td>처리기간
15일</td></tr>
<tr><td rowspan="3">보고자</td><td>대표자의 성명</td><td></td><td>신용정보업
허가일자</td><td>0000년 00월 00일</td></tr>
<tr><td>상호</td><td></td><td>허가번호</td><td></td></tr>
<tr><td>본점소재지</td><td></td><td></td><td></td></tr>
<tr><td>변경
사항</td><td colspan="4">1. ☐ 대표자 및 임원의 변경
2. ☐ 법령의 개정내용을 반영하거나 법령에 의하여 인·허가 받은 내용을 반영하는 사항
3. ☐ 정관의 변경 중 정관의 실질적인 내용이 변경되지 아니하는 조문체제의 변경, 자구수정 등</td></tr>
<tr><td>변경
사유</td><td colspan="4"></td></tr>
<tr><td colspan="5">「신용정보의 이용 및 보호에 관한 법률 시행령」 제8조제2항에 따라 위와 같이 보고합니다.

0000년 00월 00일
보고자 _____서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※ 구비서류
1. 변경사항을 확인할 수 있는 서류</td><td>수수료
없음</td></tr>
</table>

[별지 제5호 서식] 지배주주 변경승인신청서(제11조 관련)

1. 신청인에 관한 사항
   - 상호(성명), 업종, 국적, 사업자등록번호(주민등록번호), 본점소재지(주소지) 등
2. 지배주주가 되려는 자의 주식취득대상 신용정보회사가 발행한 주식의 소유현황
   (주식수, 지분율, 취득방법, 취득금액 등)
3. 지배주주가 되려는 자의 주식취득대상 신용정보회사가 발행하였거나 발행할 주식의 취득계획(발행회사명 및 개황, 주식취득 목적, 취득하고자 하는 주식수, 지분율, 예정시기, 취득방법 등)

■ 첨부서류

1. 정관(이에 준하는 것을 포함하며, 법인의 경우에 한한다) 1부
2. 외국 기업의 경우에는 법인등기부 등본에 준하는 서류 1부
3. 최근 사업연도말 현재 재무제표 및 최근 사업연도말 이후 반기가 경과한 경우 반기재무제표(법인의 경우에 한한다) 1부
4. 제3호에 따른 재무제표에 대한 회계감사인의 감사보고서·검토보고서 1부
5. 지배주주가 되려는 자가 금융회사인 경우 그 금융기관에 적용되는 재무건전성 기준에 따라 산출한 재무상태 및 이에 대한 회계감사인의 검토보고서 1부
6. 상호출자제한기업집단 또는 주채무계열에 속하는 경우 그 소속기업 중 금융회사를 제외한 기업의 부채비율 산출내역서(최근 사업연도말 이후 승인신청일까지의 자기자본 변동내역서 포함) 및 회계감사인의 검토보고서 1부
7. 그밖에 신청사실의 타당성을 심사하기 위하여 필요한 서류

※ 영문제출가능서류는 영문, 국문서류를 함께 제출

「신용정보의 이용 및 보호에 관한 법률」 제9조제1항에 따라
위와 같이 지배주주의 변경승인을 신청합니다.

년 월 일

신청인(대리인) 서명 또는 인

금융위원회 위원장 귀하

[별지 제6호 서식] 신용정보업(휴업, 폐업) 신고서(제12조 관련)

<table>
<tr><td colspan="3">신용정보업(휴업, 폐업) 신고서</td><td>처리기간
즉시</td></tr>
<tr><td>상호</td><td></td><td>허가번호</td><td></td></tr>
<tr><td>본점소재지</td><td></td><td>허가일자</td><td></td></tr>
<tr><td>휴업기간</td><td>0000년 0월 0일부터
0000년 0월 0일까지</td><td>폐업연월일</td><td>0000년 0월 0일</td></tr>
<tr><td>사유</td><td colspan="3"></td></tr>
<tr><td colspan="4">「신용정보의 이용 및 보호에 관한 법률 시행규칙」 제4조에 따라 (휴업, 폐업) 하고자 위와 같이 신고합니다.

0000년 00월 00일
신고인 _____ 서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="3">※ 첨부서류
신용정보업 허가증</td><td>수수료
없음</td></tr>
</table>

[별지 제7호 서식] 신용정보회사의 겸업신고서(제13조제2항 관련)

<table>
<tr><td colspan="4">신용정보회사의 겸업신고서</td><td>처리기간
: 15일</td></tr>
<tr><td rowspan="2">신
청
인</td><td>상호</td><td></td><td>대표자의 성명</td><td></td></tr>
<tr><td>주소</td><td></td><td>연락처</td><td></td></tr>
<tr><td colspan="2">신고하고자 하는
업무 및 업무방법</td><td colspan="3"></td></tr>
<tr><td colspan="5">「신용정보업감독규정」 제13조제2항에 따라 위와 같이 신고합니다.

0000년 00월 00일
신고인 _____ 서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※ 구비서류
1. 겸업업무의 예상 영업규모, 손익전망 등에 비추어 해당 신용정보회사의 건전경영을 저해할 염려가 없고 수익기반 확충에 기여할 수 있는지 여부
2. 겸업업무가 관련법령에 따라 행정관청의 인가·허가·등록 및 승인 등의 조치가 필요한 경우 해당 인가·허가·등록 및 승인 등을 받았음을 증명할 수 있는 서류 또는 확약서
3. 겸업업무를 수행함에 따라 발생할 수 있는 이해상충 및 불공정행위 방지를 위하여 필요한 조직, 전문인력 및 적절한 업무체계를 증명할 수 있는 서류 또는 확약서</td><td>수수료

없음</td></tr>
</table>

[별지 제7의2호 서식] 신용조회회사의 겸업승인 신청서(제13조의2제4항 관련)

<table>
<tr><td colspan="4">신용조회회사의 겸업승인 신청서</td><td>처리기간 : 30일</td></tr>
<tr><td rowspan="2">신
청
인</td><td>상호</td><td></td><td>대표자의 성명</td><td></td></tr>
<tr><td>주소</td><td></td><td>연락처</td><td></td></tr>
<tr><td colspan="2">승인받고자 하는 업무의 내용</td><td colspan="3"></td></tr>
<tr><td colspan="5">「신용정보업감독규정」 제13조의2제4항에 따라 위와 같이 신청합니다.

0000년 00월 00일
신청인 _____ 서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※ 구비서류
1. 겸업업무의 예상 영업규모, 손익 전망 등에 비추어 해당 신용조회회사의 건전한 경영을 저해할 염려가 없고 수익기반 확충에 기여할 수 있는지 여부를 확인할 수 있는 서류
2. 겸업업무가 관련 법령에 따라 행정관청의 인가·허가·등록 및 승인 등을 받아야 하는 경우 해당 인가·허가·등록 및 승인 등을 받았음을 증명할 수 있는 서류 또는 확약서
3. 겸업업무를 수행함에 따라 발생할 수 있는 이해상충 및 불공정행위를 방지하기 위하여 필요한 조직, 전문인력 및 적절한 업무체계를 갖췄음을 증명할 수 있는 서류 또는 확약서
4. 신용조회회사가 의뢰를 받고자 하는 공공목적의 조사·분석 등의 업무의 내용</td><td>수수료

없음</td></tr>
</table>

[별지 제8호 서식] 신용정보회사 상임임원의 겸직승인 신청서(제14조제2항 관련)

<table>
<tr><td colspan="5">신용정보회사 상임임원의 겸직승인 신청서</td><td>처리기간
: 15일</td></tr>
<tr><td rowspan="5">신
청
인</td><td>성명</td><td></td><td rowspan="5">겸직
대상
법인</td><td>상호</td><td></td></tr>
<tr><td>주민등록번호</td><td></td><td>주소</td><td></td></tr>
<tr><td>소속</td><td></td><td>업종</td><td></td></tr>
<tr><td>직위</td><td></td><td>대표자</td><td></td></tr>
<tr><td>연락처</td><td></td><td>법인번호</td><td></td></tr>
<tr><td colspan="2">겸직하고자
하는 업무</td><td colspan="4"></td></tr>
<tr><td colspan="2">겸직 사유</td><td colspan="4"></td></tr>
<tr><td colspan="6">「신용정보업감독규정」 제14조제2항에 따라 위와 같이 신청합니다.

0000년 00월 00일
신청인 _____ 서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="5">※ 구비서류</td><td>수수료
없음</td></tr>
</table>

[별지 제9호 서식] 삭제 <2015.9.11.>

[별지 제10호 서식] 삭제 <2015.9.11.>

[별지 제11호 서식] 별지 제2의3호로 이동 <2015.9.11.>

[별지 제12호 서식] 신용정보집중관리위원회 협의·심의·결정 사항의 보고(제28조 관련)

<table>
<tr><td colspan="2">신용정보집중관리위원회 협의 · 심의 · 결정 사항의 보고</td><td>처리기간
15일</td></tr>
<tr><td>협의
·
심의
·
결정
사항</td><td colspan="2">1. 협의·심의·결정 일자
☐
2. 협의·심의·결정 내용
☐
☐</td></tr>
<tr><td colspan="3">「신용정보의 이용 및 보호에 관한 법률」 제26조제3항에 따라 위와 같이 보고합니다.

0000년 00월 00일
보고자 _____서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="2">※ 구비서류
협의 · 심의 · 결정과 관련된 서류</td><td>수수료
없음</td></tr>
</table>

[별지 제13호 서식] 위임직채권추심인 등록신청서(제30조제2항 관련)

<table>
<tr><td colspan="6">위임직채권추심인 등록신청서</td></tr>
<tr><td rowspan="2">신청인</td><td>상호</td><td></td><td>대표자의 성명</td><td colspan="2"></td></tr>
<tr><td>주소</td><td></td><td>연락처</td><td colspan="2"></td></tr>
<tr><td rowspan="5">등록대상자</td><td rowspan="2">자 격 구 분
(☑ 표시)</td><td>☐ 신용관리사</td><td colspan="3">자격증 번호 ( )</td></tr>
<tr><td>☐ 연 수</td><td colspan="3">○ 연수기관 :
○ 연수기간 :</td></tr>
<tr><td>성명</td><td></td><td>주민등록번호</td><td colspan="2"></td></tr>
<tr><td rowspan="2">주소</td><td rowspan="2"></td><td>연락처</td><td colspan="2"></td></tr>
<tr><td>E-mail</td><td colspan="2"></td></tr>
<tr><td colspan="5">「신용정보업감독규정」 제30조제2항에 따라 위와 같이 위임직채권추심인 등록을 신청합니다.

년 월 일

신청인 (인)

신 용 정 보 협 회 장 귀 하</td><td>수수료</td></tr>
<tr><td colspan="6">※ 첨부서류
자격요건을 갖추었는지 여부를 확인할 수 있는 서류
※ 위 내용의 변경이 없는 범위 안에서 전산파일 형태로 제출할 수 있습니다.</td></tr>
</table>

[별지 제14호 서식] 위임직채권추심인 등록부(제30조제4항 관련)

<table>
<tr><td colspan="5">【 인 적 사 항 】</td></tr>
<tr><td>성 명</td><td colspan="3"></td><td rowspan="5">사 진</td></tr>
<tr><td>주민번호</td><td colspan="3"></td></tr>
<tr><td>연 락 처</td><td colspan="3"></td></tr>
<tr><td>E-mail</td><td colspan="3"></td></tr>
<tr><td>소속회사</td><td colspan="3"></td></tr>
<tr><td>등록번호</td><td></td><td>등록 일자</td><td colspan="2"></td></tr>
<tr><td rowspan="2">자격 구분</td><td rowspan="2">□ 신용관리사</td><td colspan="3">자격증 번호 ( )</td></tr>
<tr><td colspan="3">합격일(년 월 일) ___회차</td></tr>
<tr><td></td><td>□ 연 수</td><td colspan="3">○ 연수기관 :
○ 연수일자 :</td></tr>
<tr><td>주 소</td><td colspan="4"></td></tr>
<tr><td colspan="5">【 변경 사항 】</td></tr>
<tr><td>연 월 일</td><td colspan="4">내 용</td></tr>
<tr><td></td><td colspan="4"></td></tr>
<tr><td></td><td colspan="4"></td></tr>
<tr><td></td><td colspan="4"></td></tr>
<tr><td></td><td colspan="4"></td></tr>
</table>

[별지 제15호 서식] 신용정보 이용 및 제공사실 통지서(제40조제1항 관련)

신용정보 이용 및 제공사실 통지서

귀하

「신용정보의 이용 및 보호에 관한 법률」 제35조에 따라 당사가 년 월 일(통지요구일)부터 최근 3년간 귀하의 개인신용정보를 이용·제공(직접 제공한 경우에 한함)한 내역을 아래와 같이 통보합니다.

□ 이용내역

이용날짜	이용목적	이용한 신용정보의 내용	보유 및 이용기간

□ 제공내역

제공받은 자	제공목적	제공한 날짜	제공한 신용정보의 내용	보유 및 이용기간

* 기재내용에 대한 상세 설명내용 별도 첨부

본 통지내용이 사실과 다르거나 기타 문의사항이 있으신 경우에는 아래 담당자에게 연락하여 주시기 바랍니다.

20 . . .

○○○○㈜ 대표이사 (인)

담 당 자	직위 : 성명 : (전화번호 :)
영업점 주소	

<참고 : 신용정보 이용 및 제공사실 통지서 작성 방법>

□ 이용 및 제공된 신용정보를 구체적으로 안내

ㅇ 식별정보, 신용거래정보, 신용능력정보, 공공정보, 신용등급(평점)정보, 신용조회정보 등으로 구분

ㅇ 종류별로 세부 설명을 기술할 것

□ 이용목적에 대한 안내

ㅇ 법 제33조제1호에 따른 동의에 근거한 이용 또는 다른 법령상 의무를 준수하기 위하여 불가피한 경우 등을 구분하여 명시

□ 제공받은 자의 범위

ㅇ 이용자는 금융회사, 신용정보집중기관, 신용정보회사, 공공기관, 그밖에 신용정보제공·이용자, 본인 등 당해 신용정보주체의 신용정보를 제공받은 자를 모두 포함한다는 사실 기재

□ 제공한 목적에 대한 안내

ㅇ 여신심사, 신용카드발급, 신용상황변동확인, 신용정보 집중(수집), 채권추심, 신용조사, 고용, 민원처리, 재판, 수사, 본인조회 등으로 구분

ㅇ 종류별로 세부 설명을 기술할 것

(예) 여신심사 : 대출, 지급보증 등의 신규 취급, 기간연장, 한도변경, 여신사후관리 등을 위해 신용정보를 조회

□ 그밖의 안내 사항

ㅇ 그밖에 본 통지내용과 관련하여 신용정보주체에게 안내할 필요가 있는 내용 기재

[별지 제16호 서식] 신용정보 시정요청서(제42조 관련)

<table>
<tr><td colspan="4">신용정보 시정요청서</td><td>처리기간 : 15일</td></tr>
<tr><td rowspan="2">요청인</td><td>성명</td><td></td><td>주민등록번호</td><td></td></tr>
<tr><td>주소</td><td></td><td></td><td></td></tr>
<tr><td colspan="2">열람 및 정정청구기관</td><td></td><td></td><td></td></tr>
<tr><td colspan="2">시정요청내용</td><td></td><td></td><td></td></tr>
<tr><td colspan="5">「신용정보의 이용 및 보호에 관한 법률」 제38조제4항에 따라 위와 같이 요청합니다.

0000년 00월 00일
신청인 _____ 서명 또는 (인)

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※ 첨부서류
1. 정정청구를 한 내용을 기재한 서면 1부
2. 정정청구에 대한 처리결과 통지서 1부
3. 문제가 된 신용정보의 사실여부를 확인할 수 있는 서류 1부</td><td>수수료

없음</td></tr>
</table>

[별지 제17호 서식] 시정조치 결과보고서(제43조 관련)

<table>
<tr><td colspan="4">시정조치 결과보고서</td><td>처리기간
15일</td></tr>
<tr><td rowspan="3">보고자</td><td>상호 또는 명칭</td><td></td><td rowspan="2">사업자등록번호 또는 법인등록번호(비영리법인의 경우 고유번호)</td><td rowspan="2"></td></tr>
<tr><td>대표자의 성명</td><td></td></tr>
<tr><td>본점 또는 기관 소재지</td><td colspan="3"></td></tr>
<tr><td>보고 내용</td><td colspan="4">1. 시정요청 내용

2. 발생사유

3. 시정조치 내용</td></tr>
<tr><td colspan="5">「신용정보의 이용 및 보호에 관한 법률」 제38조제7항에 따라 위와 같이 보고합니다.

0000년 00월 00일
보고자 _____서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4"></td><td>수수료
없음</td></tr>
</table>

[별지 제18호 서식] 신용정보회사등의 신용정보 누설신고서(제43조의5 관련)

<table>
<tr><td colspan="3">신용정보회사등의 신용정보 누설신고서</td><td>처리기간
: 즉시</td></tr>
<tr><td>상호 또는 명칭</td><td></td><td>사업자등록번호 또는 법인등록번호(비영리법인의 경우 고유번호)</td><td></td></tr>
<tr><td>본점 또는 기관 소재지</td><td></td><td>대표자</td><td></td></tr>
<tr><td colspan="2">누설된 신용정보의 항목</td><td colspan="2"></td></tr>
<tr><td colspan="2">누설된 시점</td><td colspan="2"></td></tr>
<tr><td colspan="2">누설 경위</td><td colspan="2"></td></tr>
<tr><td colspan="2">누설로 인하여 발생할 수 있는 피해를 최소화하기 위하여 취한 조치</td><td colspan="2"></td></tr>
<tr><td colspan="2">누설로 인하여 발생할 수 있는 피해와 관련한 피해구제 절차</td><td colspan="2"></td></tr>
<tr><td colspan="2">신용정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처</td><td colspan="2"></td></tr>
<tr><td colspan="2">기타 참고사항</td><td colspan="2"></td></tr>
<tr><td colspan="4">「신용정보업감독규정」 제43조의5에 따라 위와 같이 신고합니다.

0000년 00월 00일
신고인 _____ 서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="3">※ 구비서류
1. 누설경위와 관련한 증거서류 등 관련문서
2. 누설로 인하여 발생할 수 있는 피해를 최소화하기 위하여 취한 조치와 관련한 증빙서류 등 관련문서</td><td>수수료

없음</td></tr>
</table>

신용정보업감독규정

[시행 2016.10.20] [고시 제2016 - 40호, 2016.10.20, 일부개정]

제1조(목적) 이 규정은「신용정보의 이용 및 보호에 관한 법률」, 같은 법 시행령 및 같은 법 시행규칙에서 정하는 금융위원회 소관사항의 시행에 필요한 사항을 정함을 목적으로 한다.

제2조(정의) 이 규정에서 사용하는 용어의 정의는「신용정보의 이용 및 보호에 관한 법률」(이하 "법"이라 한다), 같은 법 시행령(이하 "영"이라 한다) 및 같은 법 시행규칙(이하 "규칙"이라 한다)에서 정하는 바에 따른다.

제2조의2(신용정보의 범위) ① 영 제2조제1항제5호자목에서 "금융위원회가 정하여 고시하는 정보"는 다음 각 호의 정보를 말한다.

1. 법 제20조에 따라 신용조회회사가 기록을 보존하는 정보 중에서 신용정보주체의 신용도 판단에 이용되는 정보를 제3자에게 제공한 신용조회기록
2. 한국자산관리공사의 신용회복지원 관련 규정에 의한 채무재조정 약정정보
3. 신용회복위원회의 신용회복지원협약에 따른 신용회복지원 확정정보

② 영 제2조제1항제5호차목에서 "금융위원회가 정하여 고시하는 정보"란 국민행복기금이 협약금융기관등으로부터 채권을 매입한 정보 및 채무조정 약정을 체결한 정보를 말한다.

③ 영 제2조제1항제5호카목에서 "금융위원회가 정하여 고시하는 정보"란 신용정보주체의 신용정보를 종합적으로 평가·반영하여 생성한 개인신용평점 또는 개인신용등급 등을 말한다.

④ 영 제2조제1항제5호타목에서 "금융위원회가 정하여 고시하는 정보"란 기업 및 법인인 신용정보주체의 신용을 판단하기 위하여 신용정보를 활용함으로써 그 판단의 결과를 기호, 숫자 등을 사용하여 평점 또는 등급으로 표시한 정보를 말한다.

⑤ 영 제2조제1항제5호파목에서 "금융위원회가 정하여 고시하는 정보"란 기업 및 법인인 신용정보주체의 신용을 판단하기 위하여 기술평가(「기술신용보증기금법」제28조제1항제6호의 기술평가를 말한다)를 하고 신용정보와 해당 기업 및 법인의 기술에 관한 정보를 활용함으로써 그 판단의 결과를 기호, 숫자 등을 사용하여 평점 또는 등급으로 표시한 정보, 그 기술의 가액 또는 평가의견 등을 말한다.

제3조(신용정보제공·이용자의 범위) 영 제2조제3항에서 "그 밖에 금융위원회가 정하여 고시하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다. <개정 2016.9.21.>

1.「서민의 금융생활 지원에 관한 법률」 제3조에 따른 서민금융진흥원 및 같은 법 제26조에 따른 사업수행기관
2.「서민의 금융생활 지원에 관한 법률」 제56조에 따른 신용회복위원회
3.「상법」에 따라 설립된 주식회사 국민행복기금

제4조(신용정보업에 딸린 업무) 영 제3조제3호에 따른 "그 밖에 금융위원회가 정하여 고시하는 업무"란 다음 각 호의 업무를 말한다. 다만, 신용조사업에 딸린 업무는 제1호부터 제3호까지의 규정에 한정한다.

1. 사업장현황조사 업무
2. 민원서류 열람 및 교부신청 업무
3. 해당 업무를 영위하는 과정에서 발생하는 교육, 홍보, 출판업무
4. 채권자등에 대한 채권관리관련 업무
5. 기한 전 채무납입 안내 대행업무
6. 연체 전 채권의 변제청구 및 통지등에 대한 대행 업무
7. 「자산유동화에 관한 법률」제10조에 따른 자산관리업무

제5조(신용정보업 허가 등의 절차) ① 다음 각 호에 따른 절차는 별표 1과 같다.

1. 법 제4조에 따른 신용정보업 허가
2. 법 제10조에 따른 신용정보업의 양도、양수、분할、합병(분할합병을 포함한다. 이하 같다) 등의 인가
3. 법 제25조에 따른 신용정보집중기관의 허가

② 다음 각 호에 따른 허가 등을 신청하려는 자(이하 "신청인"이라 한다)는 다음 각 호에서 각각 정하는 서식 및 별표 1의2에 따른 신청서류를 제출하여야 한다.

1. 영 제4조에 따라 신용정보업의 허가를 받으려는 신청인: 별지 제1호 서식
2. 영 제4조에 따라 신용정보업 의 허가받은 사항에 대한 변경허가를 받으려는 신청인: 별지 제2호 서식
3. 법 제10조제1항에 따라 신용정보업의 양도、양수、분할、합병 인가를 받으려는 신청인: 별지 제2호의2 서식
4. 영 제21조제1항에 따라 신용정보집중기관으로 허가를 받으려는 신청인: 별지 제2호의3 서식

③「금융위원회의 설치 등에 관한 법률」제24조에 따른 금융감독원의 원장(이하 "금융감독원장"이라 한다)은 제2항에 따른 신청내용의 사실여부를 확인하고 이해관계인 등으로부터 제출된 의견을 고려하여 신청내용이 법 제6조 및 영 제6조에 따른 허가기준, 영 제10조제1항 각 호에 따른 인가기준, 법 제25조제3항 각 호에 따른 허가기준을 충족하는지 심사한다.

④ 금융감독원장은 신청내용을 확인하기 위하여 필요한 경우에는 이해관계인, 발기인 또는 임원과의 면담 등의 방법으로 실지조사를 할 수 있으며, 신청인은 이에 적극 협조하여야 한다.

⑤ 금융위원회는 신청인에게 3개월 이내(예비허가 또는 예비인가를 받은 경우에는 1개월 이내)에 허가 또는 인가 여부를 결정하고, 그 결과와 이유를 지체 없이 신청인에게 문서로 통지하여야 한다. 이 경우 신청서에 흠결이 있을 때에는 보완을 요구할 수 있다.

⑥ 제5항 전단에 따른 심사기간을 산정할 때에는 다음 각 호의 어느 하나에 해당하는 기간은 심사기간에 산입하지 아니한다.

1. 법 제6조 및 영 제6조에 따른 허가기준, 영 제10조제1항 각 호에 따른 인가기준 또는 법 제25조제3항 각 호에 따른 허가기준을 충족하는지를 확인하기 위하여 다른 기관 등으로부터 필요한 자료를 제공받는 데에 걸리는 기간
2. 제5항 후단에 따라 신청서 흠결의 보완을 요구한 경우에는 그 보완기간
3. 신청인을 상대로 형사소송 절차가 진행되고 있거나 금융위원회, 공정거래위원회, 국세청 또는 금융감독원 등(외국기업인 경우에는 이들에 준하는 본국의 감독기관 등을 포함한다)에 의한 조사·검사 등의 절차가 진행되고 있고, 그 소송이나 조사·검사 등의 내용이 승인심사에 중대한 영향을 미칠 수 있다고 인정되는 경우에는 그 소송이나 조사·검사 등의 절차가 끝날 때까지의 기간

⑦ 금융위원회는 허가 또는 인가의 조건을 붙일 수 있다.

⑧ 금융위원회는 제7항에 따라 조건을 붙인 경우에는 금융감독원장으로 하여금 그 이행여부를 확인하도록 하여야 한다.

⑨ 신청인은 제2항에 따른 신청을 하기 전에 금융위원회에 예비허가 또는 예비인가를 신청할 수 있다.

⑩ 금융위원회는 제9항에 따른 예비허가 또는 예비인가 신청을 받은 경우에는 2개월 이내에 예비허가 또는 예비인가 여부를 결정하여 그 결과와 이유를 지체 없이 신청인에게 문서로 통지하여야 한다. 이 경우 예비허가 또는 예비인가 신청에 관하여 흠결이 있는 경우에는 보완을 요구할 수 있다.

⑪ 예비허가 신청 및 심사 절차는 제2항부터 제8항까지의 규정을 준용한다. 이 경우 "허가" 또는 "인가"는 각각 "예비허가" 또는 "예비인가"로 본다.

⑫ 제1항부터 제11항까지의 규정에 따른 허가 또는 인가절차를 위해 그 밖에 필요한 사항은 금융감독원장이 정한다.

제6조(정보처리·정보통신설비) ① 영 제6조제1항제1호나목에서 "금융위원회가 정하여 고시하는 정보처리·정보통신설비"란 해당 신용조회업무의 범위와 규모에 비추어 신용정보를 원활히 처리할 수 있는 수준의 정보처리·정보통신설비로서 별표 2에 규정된 사항을 말한다.

② 삭제<2014.4.22.>

제7조(사실상의 영향력을 행사하는 주주 또는 출자자) 금융위원회는 신용정보회사 및 그 주주에 대하여 당해 신용정보회사의 주주가 영 6조제3항제5호나목에 해당하는지 여부를 확인하는데 필요한 자료의 제출을 요구할 수 있다.

제8조(주요출자자 요건) 영 제6조제4항 [별표1]제1호라목3)에서 "그 밖에 금융위원회가 정하는 건전한 금융거래질서를 해친 사실이 없을 것"이란 주요출자자가 최대주주로서 금융기관인 경우 최근 1년간 기관경고 조치 또는 최근 3년간 시정명령이나 업무정지 이상의 조치를 받은 사실이 없는 경우(기관경고를 받은 후 최대주주 및 그 특수관계인인 주주 전체가 변경된 경우 또는 금융산업의 신속한 구조개선을 지원할 필요가 있거나 조치를 받은 사실이 영위하고자 하는 업무의 건전한 영위를 어렵게 한다고 볼 수 없는 경우 제외)를 말하며 주요출자자가 금융회사의 임직원(전직 포함)인 경우 최근 3년간 금융위원회로부터 직무정지 또는 정직이상의 조치를 받은 사실이 없는 경우를 말한다.

제9조(자본금 또는 기본재산 감소의 신고) ① 신용정보회사가 영 제8조제1항 각 호의 사항을 신고하려는 경우에는 별지 제3호 서식에 따라 신고하여야 한다.

② 영 제8조제1항제1호에서 정하는 신고가 있는 경우에는 다음 각 호에서 정하는 기준에 적합한지 여부를 심사한다.

1. 자본금 또는 기본재산의 감소의 불가피성이 인정될 것
2. 신용정보주체 및 채권자의 권익과 신용정보 보호에 지장을 줄 염려가 없을 것

③ 영 제8조제1항제2호에서 정하는 신고가 있는 경우에는 다음 각 호에서 정하는 기준에 적합한지 여부를 심사한다.

1. 회사의 건전한 경영을 저해하지 아니할 것
2. 법 및 다른 법령을 위반하지 아니할 것

제10조(경미한 사항의 보고) 신용정보회사가 영 제8조제2항 각 호의 어느 하나에 해당하는 사항을 보고하려는 경우에는 별지 제4호 서식에 따라 보고하여야 한다.

제11조(지배주주승인신청서 등) ① 법 제9조제1항에 따른 지배주주가 되고자 하는 자는 별지 제5호 서식에 따른 승인신청서(첨부서류를 포함한다)를 금융위원회에 제출하여야 한다.

② 법 제9조제1항에 따른 금융위원회 승인의 효력은 신용정보회사의 지배주주가 되고자 하는 자가 승인을 받은 날로부터 6개월 이내에 당해 신용정보회사의 주식을 취득하지 아니하는 경우에는 소멸한다. 다만, 금융위원회의 승인 당시 주식취득기한을 따로 정하였거나 승인 후 주식취득기한의 연장에 대하여 금융위원회의 승인을 받은 경우에는 그 기간을 달리 정할 수 있다.

③ 신용정보회사의 지배주주가 되고자 하는 자가 법 제9조제1항에 따라 승인을 받은 후 주식을 취득한 때에는 그 사실을 10일 이내에 금융위원회에 보고하고 당해 신용정보회사에 통보하여야 한다.

④ 합병 신주를 교부받아 신용정보회사의 지배주주가 되는 경우에는 법 제9조제1항에 따라 신용정보회사의 주식을 취득하여 지배주주가 되려는 경우로 보지 아니한다.

⑤ 영 제9조제6항에서 "금융위원회가 정하는 기간"이란 다음 각 호의 어느 하나에 해당하는 기간을 말한다.

1. 영 제9조제2항에 따른 승인요건을 충족하는지 확인하기 위하여 다른 기관 등으로부터 필요한 자료를 제공받는 데에 걸리는 기간
2. 영 제9조제5항 후단에 따라 승인신청서의 흠결의 보완을 요구한 경우에는 그 보완기간
3. 승인을 받으려는 자를 상대로 형사소송 절차가 진행되고 있거나 금융위원회, 공정거래위원회, 국세청 또는 금융감독원 등(외국기업인 경우에는 이들에 준하는 본국의 감독기관 등을 포함한다)에 의한 조사·검사 등의 절차가 진행되고 있고, 그 소송이나 조사·검사 등의 내용이 승인심사에 중대한 영향을 미칠 수 있다고 인정되는 경우에는 그 소송이나 조사·검사 등의 절차가 끝날 때까지의 기간

제11조의2(신용정보업의 양도·양수 등의 인가의 세부요건) 영 제10조제1항 각 호에 따른 인가의 세부요건은 별표 2의2와 같다.

제12조(휴업 또는 폐업의 신고) 규칙 제4조에 따른 휴업·폐업신고서는 별지 제6호 서식에 따른다.

제13조(겸업신고 등) ① 금융감독원장은 법 제11조제1항에 따라 신용정보회사가 겸업신고를 한 경우에는 규칙 제5조제1항에 따른 요건에 적합한지 여부를 심사하여 수리한다.

② 규칙 제5조제1항에 따라 겸업신고를 하려는 자는 별지 제7호 서식에 따른 신청서를 제출하여야 한다.

제13조의2(신용조회회사에 조사·분석 등을 의뢰할 수 있는 공공단체의 범위) ① 영 제11조의2제2호에서 "금융위원회가 정하여 고시하는 기관"이란 다음 각 호의 어느 하나에 해당하는 기관을 말한다.

1. 국가나 지방자치단체가 납입자본금을 출자한 법인
2. 국가나 지방자치단체가 출연한 기관
3. 「보조금 관리에 관한 법률」 제9조 또는 「지방재정법」 제17조제1항 각 호 외의 부분 단서에 따라 국가나 지방자치단체로부터 연간 5천만원 이상의 보조금을 받는 기관 또는 단체
4. 그 밖에 다른 법률에 따라 국가나 지방자치단체로부터 투자·출자·출연을 받는 기관 또는 단체

② 영 제11조의2제9호에서 "금융위원회가 정하여 고시하는 기관"이란 다음 각 호의 어느 하나에 해당하는 기관을 말한다.

1. 「지방공기업법」 제2조에 따른 지방직영기업 및 같은 법 제76조에 따른 지방공단
2. 「공직자윤리법」 제3조제1항제12호에 따른 공직유관단체

③ 금융위원회는 법 제11조제2항 단서에 따라 신용조회회사가 승인을 신청한 내용이 규칙 제5조제2항에 따른 요건에 적합한지 여부를 심사하여 승인한다.

④ 법 제11조제2항 단서에 따라 승인을 신청하려는 자는 별지 제7호의2 서식에 따른 신청서를 제출하여야 한다.

제14조(임원의 겸직 금지) ① 법 제13조에 따라 신용정보회사의 상임임원의 겸직승인 신청이 있는 경우에는 다음 각 호에서 정하는 기준에 적합한지 여부를 심사하여 승인한다.

1. 상임임원의 겸직이 관련법규에 저촉되지 않을 것
2. 상임임원의 겸직이 당해 신용정보회사 및 관련회사의 경영합리화 또는 구조조정의 원활한 추진 등을 위해 불가피할 것

② 제1항에 따라 겸직승인 신청을 하는 경우에는 별지 제8호 서식에 따른 신청서를 제출하여야 한다.

제15조(수집된 신용정보의 처리의 위탁) ① 영 제14조제2항에 따른 "금융위원회가 정하여 고시하는 자"란 영 제5조제1항제1호부터 제21호까지의 규정에 따른 금융기관을 말한다.

② 영 제14조제4항제1호에서 "금융위원회가 정하여 고시하는 절차와 방법에 따른 보안서버의 구축 또는 암호화"란 별표 3의 Ⅱ. 3.의 보호조치를 말한다.

③ 법 제17조제7항에서 "금융위원회가 인정하는 경우"란 다음 각 호의 어느 하나에 해당하지 않는 경우를 말한다.

1. 관련 법령에서 해당 업무의 위탁을 금지하고 있는 경우
2. 재위탁자 또는 재수탁자가 최근 3년 이내에 신용정보주체의 정보관리, 감독관련 자료 제출 등 감독기관의 검사와 관련한 사항으로 기관경고 이상의 제재 또는 형사처벌을 2회 이상 받은 사실이 있는 경우
3. 그 밖에 재위탁으로 인하여 재위탁자의 건전성 또는 신인도를 크게 저해하거나, 금융질서의 문란 또는 신용정보주체의 피해 발생이 심히 우려되는 경우

④ 수탁자가 전항에 따라 신용정보의 처리를 재위탁하는 경우 별표 4 중 재위탁에 관한 신용정보 보안관리 대책에 관한 사항을 재위탁계약의 내용에 포함하여야 한다.

⑤ 신용정보처리 위탁에 관한 사항은 법, 영, 이 규정이 정한 사항을 제외하고 「금융회사의 정보처리 업무 위탁에 관한 규정(이하 "위탁규정"이라 한다)」을 준용한다. 이 경우 위탁규정 제2조제1항에 따른 "금융회사"는 "신용정보회사등"으로 본다.

⑥ 제1항의 자가 수탁자가 영 제14조제1항의 요건을 갖추었음을 확인할 수 있는 서류를 첨부하여 위탁규정 제7조에 따라 금융감독원에 보고한 경우에는 법 제17조제3항에 따라 금융위원회에 알린 것으로 본다.

제16조(정확성 확인을 위한 자료제출 요구) 신용정보집중기관 및 신용조회회사는 영 제15조제2항에 따라 등록되는 신용정보의 정확성을 점검하기 위하여 신용정보를 등록한 자에게 정확성 여부를 입증할 수 있는 자료의 제출을 요청할 수 있다.

제17조(신용조회회사등의 신용정보 등록·변경·관리) ① 신용정보집중기관 및 신용조회회사는 영 제2조제1항의 신용정보별로 등록·변경·관리 기준을 마련한다.

② 신용정보집중기관 및 신용조회회사가 영 제15조제2항에 따라 등록되는 신용정보의 정확성과 최신성을 점검할 수 있는 기준 및 절차를 마련하는 경우에는 다음 각 호의 사항이 포함되어야 한다.

1. 신용정보를 등록하는 자의 선별기준(신용조회회사만 해당한다)
2. 신용정보를 등록하는 자별 정보 등록 방식에 관한 사항
3. 사실과 다른 정보 또는 제18조 각 호의 기간이 만료된 정보의 등록시 제재에 관련한 사항

③ 신용정보집중기관 및 신용조회회사는 신용정보 이용자가 조회한 목적에 일치하는 조회사유코드를 입력하도록 하는 등 신용조회기록의 정확성 점검에 관한 사항을 마련하여야 한다.

제18조(오래된 신용정보의 등록 금지) 신용정보제공·이용자는 어음 부도거래정보를 제외한 영 제2조제1항제3호의 정보를 다음 각 호에서 정한 기간이 만료된 이후에는 신용정보집중기관 또는 신용조회회사에 등록할 수 없다.

1. 등록사유 발생일로부터 7년
2. 채권관련정보는 소멸시효가 완성된 날

제18조의2(불이익 정보의 범위) 영 제15조제4항제6호에서 "금융위원회가 정하여 고시하는 신용정보"란 제2조의2제1항제2호·제3호 및 같은 조 제2항의 신용정보를 말한다.

제19조(오래된 신용정보의 삭제) ① 영 제15조제6항에 따른 신용정보의 삭제방법은 신용정보주체에게 불이익을 초래하게 된 사유가 해소된 날(이하 '해제사유 발생일'이라 한다) 또는 등록사유 발생일로부터 제2항 각 호에 따른 기간 내에 신용정보집중기관 및 신용조회회사의 등록·관리 대상에서 삭제하는 것을 말한다.

② 영 제15조제6항에 따라 신용정보를 등록·관리대상에서 삭제하는 기준 및 절차는 다음 각 호와 같다.

1. 영 제15조제4항제1호, 제4호 및 제5호의 신용정보는 변제 또는 납부하지 아니한 기간 이내로 하되 해제사유 발생일로부터 최장 1년 이내. 다만 신용정보집중기관 및 신용조회회사가 분쟁의 입증자료 또는 정책자료로 활용하기 위해 관리하는 경우 및 신용조회회사가 신용등급의 산정 또는 신용정보를 가공하여 제공하기 위해 관리하는 경우에는 해제사유 발생일로부터 최장 5년 이내
2. 영 제15조제4항제2호의 신용정보는 해제 사유 발생일로부터 최장 5년 이내
3. 영 제15조제4항제3호 및 제6호의 신용정보는 등록사유 발생일로부터 최장 5년 이내

③ 신용정보집중기관 또는 신용조회회사에 등록되는 어음부도거래정보를 제외한 제2항제1호 및 제2호의 신용정보는 그 불이익을 초래하게 된 사유가 해소되지 않고 등록사유 발생일로부터 7년이 경과한 경우에는 그 날을 당해 정보의 해제사유 발생일로 본다.

④ 신용정보제공·이용자 및 신용조회회사가 신용정보집중기관으로부터 입수하여 활용하는 제2항의 신용정보의 관리기간은 당해 신용정보를 제공한 신용정보집중기관이 정하는 관리기간을 따른다. 다만 신용조회회사가 제2항제1호 및 제2호의 신용정보를 신용등급을 산정하거나 가공하여 제공하기 위해 관리하는 경우에는 관리기간을 해제사유 발생일로부터 최장 5년 이내로 한다.

제20조(기술적·물리적·관리적 보안대책) 영 제16조제2항에 따라 신용정보회사등이 마련해야 할 기술적·물리적·관리적 보안대책의 구체적인 기준은 별표 3과 같다.

제21조(보안관리약정 체결) 신용정보제공·이용자가 다른 신용정보제공·이용자 또는 신용조회회사와 서로 개인신용정보를 제공하는 경우에는 법 제19조제2항에 따라 별표 4의 신용정보 보안관리 대책을 포함한 계약을 체결하여야 한다.

제22조(내부관리규정의 마련) ① 법 제20조제1항에 따른 신용정보관리기준은 별표 4의2와 같다.

② 신용정보회사등은 제1항에 따른 신용정보관리기준의 준수 및 이행을 위해 신용정보회사등의 특성 등을 반영하여 내부관리규정을 구체적이고 상세하게 마련하여야 한다.

③ 제1항 및 제2항에도 불구하고 신용정보회사등은 신용정보회사등의 특성 등에 따라 특별한 사정이 있는 경우 제1항에 따른 신용정보관리기준과 달리 내부관리규정을 마련하여 준수할 수 있다. 다만, 이 경우에도 법, 영, 규칙 및 이 규정을 위반하여서는 아니 된다.

④ 제3항에 따라 신용정보회사등이 내부관리규정을 제1항의 신용정보관리기준과 달리 마련하는 경우 같은 항에 따른 그 특별한 사정을 내부관리규정에서 명확히 설명하여야 한다.

⑤ 금융위원회는 제3항에 따라 마련한 내부관리규정이 신용정보 및 신용정보주체의 권익 보호에 적합하지 않다고 판단할 경우 시정을 명할 수 있다.

제22조의2(신용정보관리·보호인의 지정대상 등) ① 영 제17조제2항제3호 후단에 따라 상시 종업원 수를 산정하는 경우「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자의 수로 한다.

② 법 제25조제2항제1호에 따른 종합신용정보집중기관(이하 "종합신용정보집중기관"이라 한다)의 신용정보관리·보호인은 법 제20조제5항에 따라 보고서를 대표자 및 이사회에 보고하기 전에 법 제26조제1항에 따른 신용정보집중관리위원회(이하 "신용정보집중관리위원회"라 한다)에 보고하여야 한다.

③ 법 제20조제5항에 따라 신용정보관리·보호인은 다음 각 호의 사항을 매 사업연도 종료 후 3개월 이내에 금융감독원장이 정하는 서식에 따라 금융감독원장에게 제출하여야 한다.<개정 2016. 10. 20>

1. 신용정보관리·보호인이 직전 사업연도 중 법 제20조제4항 각 호의 업무를 수행한 실적
2. 제1호의 실적을 기재한 보고서를 대표이사 및 이사회에 보고한 실적

제22조의3(개인신용정보의 보유기간 등) ① 법 제20조의2제1항에 따른 "금융위원회가 정하여 고시하는 기한"이란 3개월을 말한다.

② 신용정보제공·이용자가 영 제17조의2제1항제1호나목에 따라 접근할 수 있는 임직원을 지정할 때에는 접근권한 관리책임자를 두어야 한다.

③ 영 제17조의2제1항제1호다목에 따라 신용정보제공·이용자는 개인신용정보가 안전하게 보호될 수 있도록 제2항에 따라 접근권한을 부여받은 자가 해당 개인신용정보를 이용하려는

경우에는 접근권한 관리책임자의 사전 승인을 얻어 그 개인신용정보를 이용하게 하고, 그 이용 내역을 3년간 보관하여야 한다.
[시행일: 2016.3.12.] 제22조의3

제22조의4(개인신용정보가 포함된 문서 등의 관리 방법) 영 제17조의2제1항제1호 각 목의 구분에 따른 방법으로 상거래관계가 종료된 신용정보주체의 개인신용정보를 관리하는 것이 불가능하거나 현저히 곤란한 경우에는 다음 각 호의 방법으로 관리할 수 있다.
1. 보존기간을 정하여 잠금장치가 있는 안전한 장소 등에 보관할 것
2. 물리적 보관장소에 대하여는 출입ㆍ통제 절차를 수립ㆍ운영 할 것
3. 보존되는 개인신용정보의 현황파악, 열람, 대여 등에 관한 통제시스템을 확립할 것
4. 보존기간이 만료한 개인신용정보에 대한 안전한 폐기계획을 수립ㆍ시행하고 신용정보관리ㆍ보호인 또는 대표이사가 폐기결과를 확인 할 것

제23조(폐업시 보유정보의 처리) 신용정보회사 또는 신용정보집중기관이 폐업을 하고자 하는 경우에는 금융감독원장이 소속 직원 중에서 지명하는 자의 입회하에 다음 각 호의 자료를 처분, 소거 또는 폐기하여야 한다.
1. 신용정보 자료철 및 신용정보 관리대장
2. 신용정보 데이터베이스
3. 그 밖에 신용정보가 수록ㆍ보관된 파일등

제24조(공공단체의 범위) 영 제19조제1항제1호 및 제3호까지에 따른 "금융위원회가 정하여 고시하는 기관"의 범위는 별표 5에 따른다.

제24조의2(공공기관 제공 신용정보의 등록 및 이용기준) 영 제19조제4항에 따라 공공기관이 종합신용정보집중기관에 제공하는 신용정보의 등록 및 이용기준은 별표 6 제6호와 같다.

제25조 삭제 <2015.9.11>

제25조의2 삭제 <2015.9.11>

제26조(신용정보의 등록 및 이용기준) 영 제21조제2항의 금융기관은 영 제21조제3항에서 정하는 집중관리ㆍ활용대상 신용정보를 집중관리ㆍ활용하기에 적합한 형태로 처리하여 종합신용정보집중기관에 등록하여야 한다.

제26조의2 삭제 <2015.9.11>

제26조의3(종합신용정보집중기관업무의 분리) ① 영 제21조제5항에 따라 종합신용정보집중기관이 법 제25조의2 각 호의 업무(이하 "집중기관업무"라 한다) 외의 다른 업무(이하 "기타업무"라 한다)를 수행하는 경우 다음 각 호에 따라 집중기관업무와 구별하여야 한다.
1. 재무에 관한 사항

가. 집중기관업무와 기타업무를 구분하여 별도의 회계장부를 마련하고 구분하여 회계처리할 것

나. 집중기관업무 관련 예·결산에 관한 사항에 대하여 신용정보집중관리위원회가 심의·의결할 것

2. 임직원(대표자인 임원, 감사는 제외한다)이 집중기관업무와 기타업무를 겸직하지 아니할 것

3. 집중기관업무와 기타업무간에 정보의 교류를 차단하고, 정기적으로 이해상충이 발생할 가능성을 파악·평가할 것

② 종합신용정보집중기관의 신용정보관리·보호인은 제1항에 따른 사항을 정기적으로 점검하여 신용정보집중관리위원회에 보고하여야 한다.

제26조의4(신용정보집중기관의 허가 세부요건) ① 영 제21조제6항제1호에서 "금융위원회가 정하여 고시하는 정보처리·정보통신설비"는 제6조제1항을 준용한다. 이 경우 "신용조회업무"는 "신용정보집중관리·활용업무"로 본다.

② 영 제21조제7항에 따른 신용정보집중기관 허가의 세부요건은 별표 5의2와 같다.

③ 영 제21조제9항에 따라 종합신용정보집중기관을 통해 집중관리·활용되는 신용정보의 구체적인 등록 및 이용기준은 별표 6과 같다.

④ 신용정보집중기관에 정보를 제공하거나 신용정보집중기관의 정보를 이용하는 자는 신용정보집중기관이 정하는 바에 따라 전산매체 또는 서면으로 신용정보를 제공·이용하여야 한다.

제26조의5(종합신용정보집중기관의 업무) 영 제21조의2제2항제3호에서 "그 밖에 금융위원회가 정하여 고시하는 업무"란 특정 개인을 알아볼 수 없는 정보에 관한 가공·분석·조사업무를 말한다.<개정 2016. 10. 20>

제26조의6(제재금의 최고한도 금액) 영 제22조제2항에 따른 제재금의 최고 한도 금액은 신용정보 제공의 누락 및 지연, 거짓 등록 등 위반건당 1백만원으로 한다.<개정 2016. 10. 20>

제27조 삭제 <2015.9.11>

제28조(신용정보집중관리위원회 협의·심의·결정 사항의 보고) 법 제26조제3항에 따라 신용정보집중관리위원회가 협의·심의·결정한 사항을 보고하는 경우에는 별지 제12호 서식에 따라 보고하여야 한다.

제29조(미성년자 고용 또는 채용가능 업무) 법 제27조제1항제1호 단서에서 "금융위원회가 정하는 업무"란 다음 각 호의 어느 하나에 해당하는 업무를 말한다.

1. 신용정보의 내부처리를 위한 자료의 작성, 입력 및 출력 등을 보조하는 업무

2. 법 제23조제2항에 따른 공공기관이 보유하는 신용정보로서 타인에게 제공되거나 공개되어도 신용정보주체에게 불이익을 초래할 우려가 없는 정보를 열람하거나 제공받는 업무

제30조(위임직채권추심인의 자격요건) ① 영 제24조제1항제3호에서 "그 밖에 제1호에 준하는 자격이 있다고 금융위원회가 인정한 사람"이란 법 제44조의 신용정보협회(이하 "협회"라 한다)가 주관하는 신용관리사 자격시험에 합격한 사람을 말한다.
② 영 제24조제2항에 따라 채권추심회사가 그 소속 위임직채권추심인이 되려는 자를 등록하고자 하는 때에는 별지 제13호 서식에 따른 등록신청서를 협회의 장에게 제출하여야 한다.
③ 제2항에 따른 등록신청서에는 소속 위임직채권추심인이 되고자 하는 자가 영 제24조제1항의 자격요건을 갖추었는지 여부를 확인할 수 있는 서류를 첨부하여야 한다.
④ 협회의 장이 위임직채권추심인 등록신청을 수리한 때에는 이를 별지 제14호 서식에 따른 위임직채권추심인등록부에 기재하고 그 사실을 채권추심회사에 지체없이 통지하여야 한다.
⑤ 위임직채권추심인의 등록에 관하여 필요한 세부사항은 협회의 장이 정한다.

제31조 삭제 <2015.9.11>

제32조 삭제 <2014.4.22.>

제33조 삭제 <2014.4.22.>

제33조의2 삭제 <2014.4.22.>

제33조의3 삭제 <2014.4.22.>

제34조(개인신용정보의 제공·활용에 대한 동의) 신용정보제공·이용자는 영 제28조제2항 각 호의 내용에 변경이 있는 경우에는 인터넷 홈페이지 게시 등을 통해 해당 신용정보주체에게 알려야 한다.
[시행일: 2016.3.12.] 제34조

제35조(개인신용정보의 조회에 대한 동의) 영 제28조제6항 각 호의 내용에 변경이 있는 경우에는 인터넷 홈페이지 게시 등을 통해 해당 신용정보주체에게 알려야 한다.

제36조 삭제 <2015.9.11.>
[시행일: 2016.3.12.] 제36조

제37조(조회동의 확인 방법) ① 신용조회회사 또는 신용정보집중기관이 영 제28조제7항에 따라 동의를 받았는지를 확인하고자 하는 경우에는 다음 각 호의 어느 하나의 방식으로 확인할 수 있다.
1. 동의서 사본을 제출받는 방식
2. 법 제32조제1항 제2호부터 제3호까지에 따른 방식
3. 개인신용정보를 제공받으려는 자로부터 해당 개인의 조회동의 사실을 확인하였다는 기록을 전자적으로 제공받는 방식
② 신용조회회사 또는 신용정보집중기관은 개인신용정보를 제공받으려는 자의 업태, 정보관리능력 등을 고려하여 제1항 각호의 방식 중 법 제32조제3항에 따른 확인업무를 적절하게 수

행할 수 있다고 판단되는 방식을 선택하여야 한다.

③ 제1항제3호의 방식을 통해 동의를 받았는지 확인하는 신용조회회사 또는 신용정보집중기관은 사실 확인의 진위여부를 주기적으로 점검하여야 한다.

제38조 삭제 <2015.9.11.>

[시행일: 2016.3.12.] 제38조

제38조의2(금융질서문란행위자) 영 제28조제11항제5호에서 "금융위원회가 정하여 고시하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1.「외국환거래법」제20조를 위반하여 허위의 보고를 하거나 거짓으로 자료를 제출한 자

2.「민법」제32조에 따라 금융위원회로부터 허가를 받은 신용회복위원회에 허위의 자료를 제출하거나 허위의 진술을 하고 채무를 조정 받았거나 조정된 채무를 이행하는 과정에서 재산의 도피, 은닉 또는 고의의 책임재산 감소행위를 한 자

3.「전자금융거래법」 제6조제3항 각 호의 어느 하나에 해당하는 행위를 한 자. 다만, 다음 각 목의 어느 하나에 해당하는 경우는 제외한다.

가. 다른 법률에 특별한 규정이 있는 경우

나. 같은 법 제18조에 따른 선불전자지급수단이나 전자화폐의 양도 또는 담보제공을 위하여 필요한 경우(같은 법 제6조제3항제3호의 행위 및 이를 알선하는 행위는 제외한다)

[시행일: 2016.3.12.] 제38조의2

제38조의3(개인신용정보 제공사실의 통지유예 등) 신용정보회사등은 영 별표 2의2 제11호, 제12호 및 제13호에 따른 개인신용정보 제공이 발생한 경우로서 신용정보 제공요구자가 다음 각 호의 어느 하나에 해당하는 사유가 지속되고 있음을 제시하고 통지의 유예를 서면으로 반복하여 요청하는 경우에는 요청받은 날부터 두 차례만(제1호의 경우는 제외한다) 매1회 3개월의 범위에서 유예요청기간 동안 통보를 유예할 수 있다.

1. 해당 통지가 사람의 생명이나 신체의 안전을 위협할 우려가 있는 경우

2. 해당 통지가 증거 인멸, 증인 위협 등 공정한 사법절차의 진행을 방해할 우려가 명백한 경우

3. 해당 통지가 질문ㆍ조사 등의 행정절차의 진행을 방해하거나 과도하게 지연시킬 우려가 명백한 경우

[시행일: 2016.3.12.] 제38조의3

제38조의4(영업양도 등에 따라 제공받은 개인신용정보의 관리) 법 제32조제8항에 따라 개인신용정보를 제공받은 자는 해당 개인신용정보를 다음 각 호의 구분에 따라 현재 거래 중인 신용정보주체의 개인신용정보와 구분하여 관리하여야 한다.

1. 제공받은 개인신용정보는 영업양도ㆍ분할ㆍ합병 등을 이유로 제공받은 개인신용정보라는 사실을 표시하여 관리

2. 개인신용정보를 제공받았을 때 이미 거래가 종료되어 분리보관 중인 개인신용정보의 경우 제1호에 따른 표시를 하고 현재 거래 중인 신용정보주체의 개인신용정보와 분리하여 관리

[시행일: 2016.3.12.] 제38조의4

제39조(개인신용정보를 제공받는 자의 확인) ① 신용정보회사등이 개인신용정보를 제공할 경우에는 제공받는 자로부터 제공받는 자의 성명, 주민등록번호 및 주소(법인의 경우에는 법인명, 대표자의 성명 및 본점 소재지) 등의 인적사항과 정보이용목적이 기재된 의뢰서 및 이용목적을 확인할 수 있는 근거서류를 받아야 하며 다음 각 호의 증표 및 서류에 따라 제공받는 자의 신원을 확인하여야 한다.

1. 제공받는 자가 개인인 경우에는 주민등록증, 운전면허증 또는 성명, 주민등록번호 및 주소가 기재되고 사진이 첨부된 그 밖의 신분증명서
2. 제공받는 자가 법인인 경우에는 법인의 대표자(또는 그로부터 위임받은 자)임을 확인할 수 있는 서류와 해당 개인의 신분증명서

② 신용정보집중기관이 신용정보제공·이용자 및 신용조회회사에게 개인신용정보를 제공하는 경우와 신용조회회사가 법 제2조제8호의 업무로 개인신용정보를 제공하는 경우에는 법 제20조제2항의 기록을 보유하는 것으로 제1항에 따른 제공받는 자의 확인을 갈음한다.

제39조의2(신용정보 이용 및 제공사실 조회시스템에 대한 조치기간) 영 제30조제1항 본문에 따른 "금융위원회가 정하여 고시하는 기간"이란 7일 이내를 말한다. 다만, 법, 영 및 그 밖에 다른 법령에서 달리 정하는 경우에는 그 법령에서 정하는 바에 따른다.

[시행일: 2016.3.12.] 제39조의2

제40조(신용정보 이용 및 제공사실의 통지요구 등) ① 법 제35조제2항 및 영 제30조제7항에 따라 신용정보회사등이 신용정보주체에게 본인의 개인신용정보를 이용하거나 제공한 사항을 통지하는 경우에는 별지 제15호 서식에 따라 서면, 전자우편, 문자메시지, 그 밖에 이와 유사한 방법으로 통지한다.

② 신용정보회사등은 신용정보주체에게 법 제35조제2항에 따라 통지를 요청할 수 있다는 사실, 통지요청의 방법, 통지의 주기 및 수수료 등을 알려야 한다.

[시행일: 2016.3.12.] 제40조

제40조의2(상거래 거절 근거 신용정보의 고지) 영 제31조제1항제2호 단서에서 "금융위원회가 정하여 고시하는 정보"란 제2조의2제2항의 정보를 말한다.

[시행일: 2016.3.12.] 제40조의2

제40조의3(동의 철회의 방법) 영 제32조제1항에 따른 "금융위원회가 정하여 고시하는 방법"이란 신용정보제공·이용자의 사무실·점포 등을 방문하여 동의 철회서를 제출하는 방법을 말한다.

제41조(신용정보의 정정청구) ① 법 제38조제1항에 따라 신용정보주체가 신용정보회사등에게 본인정보의 정정을 청구하고자 할 때에는 정정대상정보와 정정청구사유를 기재하여 서면 또는 신용정보회사등의 인터넷홈페이지를 통해 신청하여야 한다.

② 정정청구를 받은 신용정보회사등은 사실여부의 조사·확인을 위하여 필요한 경우 신용정보주체에게 관련 증빙자료의 제시를 요청할 수 있다.
③ 신용정보집중기관 및 신용조회회사는 신용정보주체의 정정청구에 따른 사실 확인을 위하여 필요한 경우에는 당해 신용정보를 등록한 신용정보제공·이용자에게 등록된 정보의 사실여부를 입증할 수 있는 자료를 요청할 수 있다.

제42조(시정요청서) 영 제33조제3항에 따른 시정요청은 별지 제16호 서식에 따른다.

제43조(시정조치 결과보고서) 신용정보회사등이 법 제38조제7항에 따라 시정조치를 한 경우에는 별지 제17호 서식에 따라 그 결과를 보고하여야 한다.

제43조의2(신용조회회사의 정보제공 중지의 요건 등) ① 법 제38조의2제1항에 따른 "금융위원회가 정하는 방식"이란 영 제30조제3항에 따른 방식을 말한다.
② 영 제33조의2제1항에서 각 호의 어느 하나에 해당하는 사실이 발생함에 따라 그 요청을 받은 것으로 인정되는 경우란 다음 각 호의 어느 하나에 해당하는 경우를 말한다.
1. 신용정보회사등이 법 제39조의2제1항에 따른 누설 통지 또는 같은 조 제3항에 따른 누설 신고를 한 이후 신용정보주체가 법 제38조의2제1항에 따른 조회사실 통지를 요청한 경우
2. 신용정보주체가 「주민등록법 시행령」 제42조제1항에 따른 주민등록증 분실신고 또는 이와 유사한 방법으로 개인식별번호(영 제29조 각 호의 번호를 말한다)가 포함된 신분증을 분실한 사실을 입증하고 법 제38조의2제1항에 따른 조회사실 통지를 요청한 경우
[시행일: 2016.3.12.] 제43조의2

제43조의3(삭제 요구에 따른 통지방법) 법 제38조의3제4항에 따른 금융위원회가 정하여 고시하는 방법이란 영 제33조의2제3항 각 호의 어느 하나에 따른 방법을 말한다.
[시행일: 2016.3.12.] 제43조의3

제43조의4(신용정보 누설사실의 공시기간) 영 제34조의2제2항에 따른 "금융위원회가 정하여 고시하는 기간"이란 다음 각 호의 기간을 말한다.
1. 영 제34조의2제2항제1호의 경우: 15일
2. 영 제34조의2제2항제2호의 경우: 15일
3. 영 제34조의2제2항제3호의 경우: 7일

제43조의5(신용정보의 누설신고) 영 제34조의2제6항에 따라 신고하는 신용정보회사등은 별지 제18호 서식에 따른 신고서를 제출하여야 한다.

제43조의6(모집업무수탁자에 관한 보고) 영 제35조의2제6항 및 제7항에 따른 보고의 서식 및 방법은 금융감독원장이 정한다.

제43조의7(손해배상책임의 이행을 위한 보험 등 가입 기준) ① 영 제35조의9에 따른 "금융위원회가 정하여 고시하는 자" 및 그 자가 법 제43조의3에 따라 보험 또는 공제에 가입하는 경우

의 그 최소 가입금액은 다음 각 호와 같다.

1. 신용정보집중기관, 신용조회회사, 영 제5조제1항제1호부터 제7호까지의 자(제1호에 따른 은행 중 지방은행 및 「은행법」 제58조에 따라 인가를 받은 외국은행의 국내지점은 제외한다): 20억원
2. 영 제5조제1항제1호 중 지방은행, 외국은행의 국내지점, 같은 항 제8호(명의개서대행회사는 제외한다), 제15호부터 제18호까지의 자, 제20호, 제21호(정리금융기관은 제외한다)의 자 및 영 제21조제2항제9호에 해당하는 자: 10억원
3. 영 제35조의9 각 호의 어느 하나에 해당하는 자 중 제1호 및 제2호 이외의 자(영 제21조제2항제8호에 해당하는 자, 같은 조 같은 항 제19호에 해당하는 자 중에서 「대부업 등의 등록 및 금융이용자 보호에 관한 법률 시행령」 제7조의2제1항제1호·제5호에 해당하는 자 및 같은 조 같은 항 제22호에 해당하는 자는 제외한다): 5억원. 다만, 영 제5조제1항제9호부터 제14호까지 및 제19호에 해당하는 자가 소속 중앙회 또는 연합회를 통하여 신용정보처리 관련 기술부문의 주요부분을 공동으로 이용하는 경우, 중앙회 또는 연합회가 공동 이용 금융회사 전체의 사고를 보장하는 내용으로 제1호의 금액 이상의 보험 또는 공제에 가입하면 공동 이용 금융회사는 본호의 보험 또는 공제에 가입한 것으로 본다.

② 제1항 각 호의 자가 준비금을 적립하는 경우 제1항 각 호에서 정하는 금액 이상의 금액을 보유하여야 한다.

③ 제1항 각 호의 자가 보험 또는 공제 가입과 준비금 적립을 병행하는 경우 보험 또는 공제의 최소 가입금액은 제1항 각 호에서 정한 금액에서 적립한 준비금을 뺀 금액으로 한다.

④ 「전자금융거래법」 제9조제4항에 따라 가입한 보험·공제 또는 적립한 준비금이 법 제43조에 따른 손해배상 책임의 이행을 보장하는 경우 제1항에서 정한 금액에서 그 금액을 뺀 금액이상으로 한다.

⑤ 제1항부터 제4항까지의 규정은 500명 이상의 신용정보주체에 관한 개인신용정보를 수집·이용·처리하지 않는 자에 대하여는 적용하지 아니한다.

제44조(검사결과의 보고방법) 금융감독원장은 법 제45조제6항에 따른 결과보고를 하는 경우 「금융기관검사및제재에관한규정」 제3장을 준용한다.

제45조 삭제 <2014.4.22.>

제46조(회계처리기준등) ① 신용정보회사는 회계처리 및 재무제표 작성에 관하여 「주식회사의 외부감사에 관한 법률」 제13조에 따른 회계처리기준을 따라야 한다.

② 신용정보회사는 결산재무제표와 「주식회사의 외부감사에 관한 법률」 제3조에 따른 감사인의 감사보고서를 사업연도말로부터 3개월 이내에 금융감독원장에게 제출하여야 한다.

③ 제2항에 따라 제출한 재무제표와 제1항에 따라 제출한 사업연도말 업무보고서가 일치하지 않는 경우에는 그 내용과 사유를 금융감독원장에게 보고하여야 한다.

제47조(세부사항) 금융감독원장은 이 규정의 시행에 필요한 세부사항을 정할 수 있다.

제48조(재검토기한) 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 규정 발령 후의 법령이나 현실여건의 변화 등을 검토하여 이 규정의 유지, 폐지, 개정 등의 조치를 하여야 하는 기한은 2015년 7월 1일을 기준으로 매 2년이 되는 시점(매 2년째의 6월 30일까지를 말한다)으로 한다.<개정 2015.7.1.>

부칙 <제2001-113호,2002.1.4>

이 규정은 공고한 날부터 시행한다.

부칙 <제2002-42호,2002.7.4>

이 규정은 공고한 날부터 시행한다. 다만, 제12조의 개정규정에 의한 <별지제9호서식>은 2002.10.1부터 시행한다.

부칙 <제2003-19호,2003.3.19>

이 규정은 공고한 날부터 시행한다.

부칙 <제2003-52호,2003.11.5>

이 규정은 공고한 날부터 시행한다.

부칙 <제2004-41호,2004.6.30>

이 규정은 공고한 날부터 시행한다. 다만, 제13조의2 및 제13조의3은 2004년 7월 30일부터 시행한다.

부칙 <제2005-53호,2005.11.3>

이 규정은 공고한 날부터 시행한다.

부칙 <제2008-8호,2008.4.7>

이 규정은 고시한 날부터 시행한다.

부칙 <제2009 - 30호,2009.5.12>

제1조 (시행일) 이 규정은 고시한 날부터 시행한다.

부칙 <제2009 - 50호,2009.8.26>

이 규정은 고시한 날부터 시행한다.

부칙 <제2009 - 56호,2009.10.2>

제1조(시행일) 이 규정은 2009년 10월 2일부터 시행한다.

제2조(경과조치) ① 이 규정시행당시 종전의 관련 규정에 따라 행한 조치는 이 규정에 따라 시행한 것으로 본다.

② 제46조는 2010 사업연도부터 적용한다.

③ 제34조제4항제2호의 경우 2010년 1월 1일까지는 금융회사에게 등록한 비밀번호로서 갈음할 수 있다.

부칙 <제2011 - 15호,2011.8.18>

이 규정은 2011년 8월 20일 부터 시행한다.

부칙 <제2012 - 12호,2012.6.26>

이 규정은 2012년 6월 26일 부터 시행한다.

부칙 <제2013 - 1호,2013.1.31>

이 규정은 공고한 날부터 시행한다.

부칙 <제2013 - 9호,2013.4.23>

이 규정은 공고한 날부터 시행한다.

부칙 <제2014 - 11호,2014.4.22>

이 규정은 공고한 날부터 시행한다.

부칙 <제2014 - 13호,2014.6.11>

이 규정은 공고한 날부터 시행한다.

부칙 <제2014 - 24호,2014.8.6>

이 규정은 공고한 날부터 시행한다.

부칙 <제2015 - 20호,2015.6.30>

이 규정은 2015년 7월 1일부터 시행한다.

부칙 <제2015 - 30호,2015.9.7>

이 규정은 공고한 날부터 시행한다.

부칙 <제2015 - 31호,2015.9.11>

제1조(시행일) 이 규정은 고시한 날부터 시행한다. 다만, 제22조의3, 제34조, 제36조, 제38조, 제38조의2, 제38조의3, 제38조의4, 제39조의2, 제40조, 제43조의2 및 제43조의3의 개정규정은 2016년 3월 12일부터 시행한다.

제2조(신용정보관리·보호인의 업무 보고의 적용례) 제22조의2제3항의 개정규정은 2016년도 신용정보관리·보호인의 업무실적 및 보고실적에 대한 보고부터 적용한다.

제3조(내부관리규정 마련에 관한 경과조치) 신용정보회사등은 제22조제2항에 따른 내부관리규정을 이 규정의 시행일부터 3개월 이내에 마련하여야 한다.

제4조(다른 규정의 폐지) 신용정보업인허가지침(금융위원회고시 제2012 - 12호)은 폐지한다.

부칙 <제2016 - 14호,2016.3.16>

제1조(시행일) 이 규정은 고시한 날부터 시행한다.

부칙 <제2016 - 32호,2016.9.21>

제1조(시행일) 이 규정은 2016년 9월 23일부터 시행한다.

제2조 생략

제3조(다른 고시의 개정) ① 생략

② 신용정보업감독규정 일부를 다음과 같이 개정한다.

제3조제1호부터 제3호까지를 각각 다음과 같이 한다.

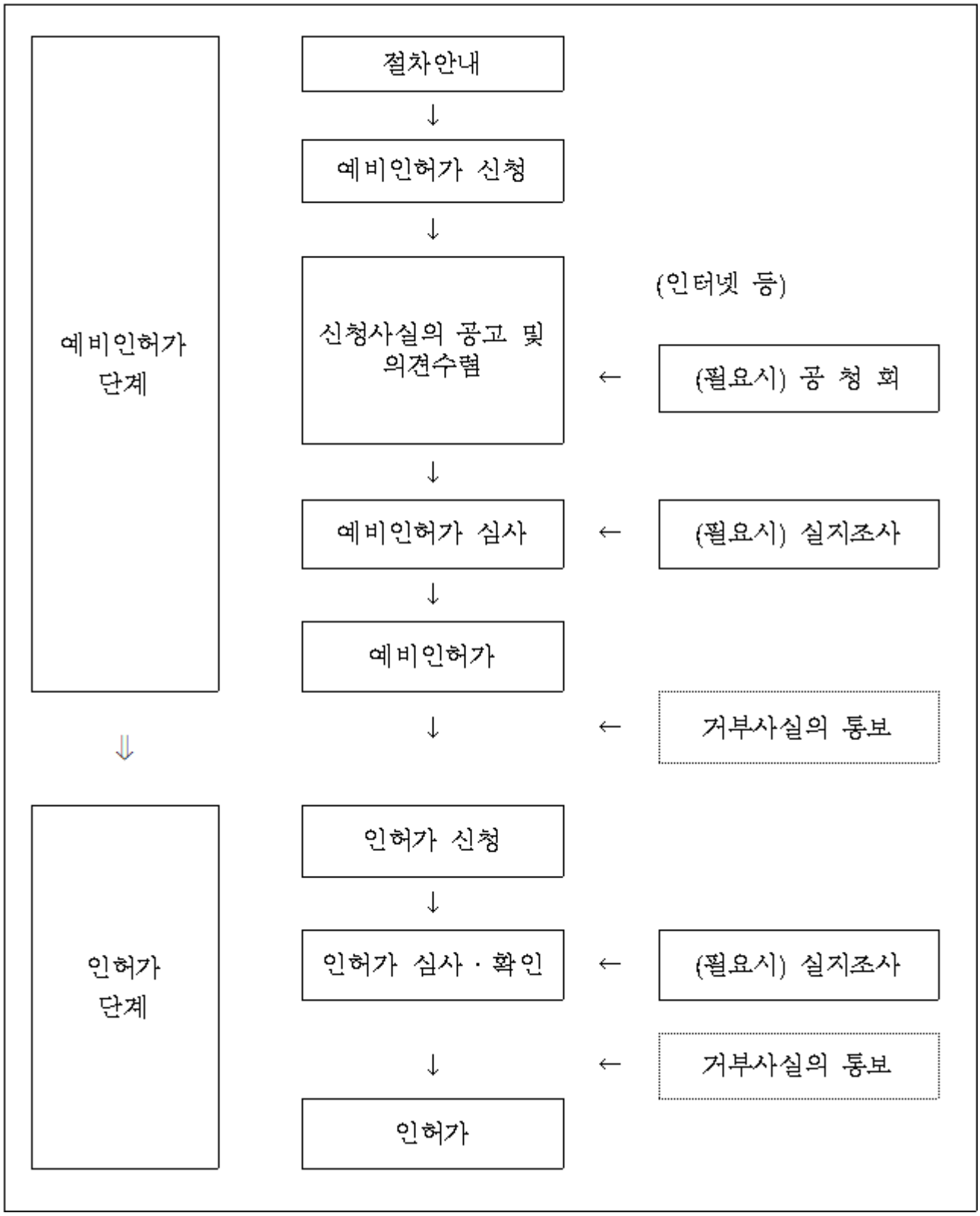
1. 「서민의 금융생활 지원에 관한 법률」 제3조에 따른 서민금융진흥원 및 같은 법 제26조에 따른 사업수행기관
2. 「서민의 금융생활 지원에 관한 법률」 제56조에 따른 신용회복위원회
3. 「상법」에 따라 설립된 주식회사 국민행복기금

부칙 <제2016-40호,2016.10.20>

제1조(시행일) 이 규정은 고시한 날부터 시행한다.

[별표 1]

신용정보업 및 신용정보집중기관 허가 등의 절차(제5조제1항 관련)



[별표 1의2]

신용정보업 및 신용정보집중기관 허가 등의 신청서류

(제5조제2항 관련)

1. 신용정보업

구분	예비인·허가	인·허가
1. 신용정보업 영위허가 (신용정보업무 추가 영위허가 포함)	- 신용정보업 예비허가신청서 - 정관(안) - 2년간의 사업계획서 및 예상수지계산서 - 발기인 총회의사록(이사회의사록) 사본 - 출자자(또는 주주) 구성 및 자금조달 계획 - 출자자의 인감증명서가 첨부된 출자확약서(출자비율 5%미만인 개인출자자는 제외) - 출자자의 출자자금 조달계획서 - 출자자가 금융회사인 경우는 당해 금융회사 인허가권자의 인허가서 사본 또는 등록증 사본, 법인등기부등본, 사업자등록증 사본, 최근사업연도의 감사보고서 및 당해 금융회사의 일반현황 - 출자자가(당해 법인이 금융회사가 아닌 출자자 중 최다 출자자에 한함)가 일반법인인 경우 법인등기부등본, 사업자 등록증 사본, 최근 사업연도의 재무제표 * 신청인이 이미 설립된 법인인 경우에는 상기 첨부서류에 준하는 서류로 대체 가능 - 출자자(또는 주주) 관계가 법 제5조(신용정보업별 허가 대상)에 저촉되지 않음을 확인하는 서류 등 - 합작계약서(합작법인인 경우) - 주요출자자가 주요출자자 요건을 충족함을 확인하는 서류 - 인력 및 물적시설(채용, 구매 등이 예정된	- 신용정보업 허가신청서 - 정관 및 법인등기부 등본 - 재무제표 - 2년간의 사업계획서 및 예상수지계산서 - 자본금 또는 기본재산의 지분을 기재한 서류 - 발기인 총회의사록(이사회의사록) 사본 - 출자자(또는 주주) 관계 확인서류 - 자본금 납입증명 서류 - 외국인출자자인 경우 외국인의 출자가 「외국환거래법」 등에 저촉되지 않음을 확인하는 서류 - 출자자(또는 주주) 관계가 법 제5조(신용정보업별 허가 대상)에 저촉되지 않음을 확인하는 서류 등 - 합작계약서(합작법인인 경우) - 주요출자자가 주요출자자 요건을 충족함을 확인하는 서류 - 인력 및 물적시설을 갖추었음을 확인하는 서류 - 허가 신청한 업무의 전문성을 갖추었음을 확인하는 자료 - 임직원에 관한 서류 - 임원의 이력서 - 직원의 상시고용을 확인하는 서류 - 법 제22조제1항, 법 제27조제1항에 해당하지 않음을 확인하는 서류(필요시 이를 확인하는 각서 제출로 대체 가능)

구분	예비인·허가	인·허가
	인력물적시설 포함)의 현황을 확인할 수 있는 서류 - 허가 신청한 업무의 전문성을 갖출 수 있음을 확인할 수 있는 자료 - 임원(예정자 포함)이력서	- 제22조제2항에 따른 내부관리규정 - 회계처리·감사·조직관리 등 내부통제에 관한 규정 - 예비허가내용 및 조건의 이행을 증명하는 서류
2. 분할·합병 인가	- 분할 · 합병 예비인가 신청서 - 분할 · 합병 목적 및 사유 - 정관변경(안) - 자본금 또는 기본재산의 지분을 기재한 서류 - 재무제표 - 2년간의 사업계획서(분할 · 합병 후 2년간 추정재무제표, 인력 및 조직운영계획, 업무범위 및 영업전략 등) 및 예상수지계산서 - 분할 · 합병 관련 계약서 또는 예약서 - 분할 · 합병에 관한 이사회 의사록 - 본점 및 영업소의 현황 및 변경계획(명칭, 주소 등) - 출자자(또는 주주) 구성 및 경영지배구조 계획 - 채권자 등 이해관계인의 권익보호계획 - 분할 후 영위 할 수 없는 업무가 있는 경우 그 업무의 정리계획	- 분할 · 합병 인가 신청서 - 분할 · 합병 목적 및 사유 - 정관 및 법인등기부등본 - 자본금 또는 기본재산의 지분을 기재한 서류 - 재무제표 - 2년간의 사업계획서(분할 · 합병 후 2년간 추정재무제표, 인력 및 조직운영계획, 업무범위 및 영업전략 등) 및 예상수지계산서 - 분할 · 합병 관련 계약서 또는 예약서 - 분할 · 합병에 관한 이사회 의사록 및 주주총회 의사록 - 본점 및 영업소의 현황 및 변경계획(명칭, 주소 등) - 출자자(또는 주주) 구성 및 경영지배구조 - 채권자 등 이해관계인의 보호절차 이행을 증명하는 서류 - 분할 후 영위 할 수 없는 업무가 있는 경우 그 업무의 정리계획 - 예비인가내용 및 조건의 이행을 증명하는 서류
<합병 후 존속하는	- 정관변경(안) - 임원(예정자 포함) 이력서	- 정관 및 법인등기부등본 - 임원 이력서

구분	예비인·허가	인·허가
법인 및 분할 또는 합병에 따라 설립되는 법인의 경우>	- 법 제5조, 법 제6조, 법 제22조제1항, 법 제27조제1항에 저촉되지 않음을 증명하는 서류(신용정보업 영위 허가 참조)	- 법 제5조, 법 제6조, 법 제22조제1항, 법 제27조제1항에 저촉되지 않음을 증명하는 서류(신용정보업 영위 허가 참조) - 제22조제2항에 따른 내부관리규정 - 회계처리·감사·조직관리 등 내부통제에 관한 규정
3. 사업양수인가	- 사업양수 예비인가 신청서 - 사업양수 목적 및 사유 - 정관변경(안) - 자본금 또는 기본재산의 지분을 기재한 서류 - 재무제표 - 2년간의 사업계획서(양수 후 2년간 추정 재무제표, 인력 및 조직운영계획, 업무범위 및 영업전략 등) 및 예상수지계산서 - 사업양수 관련 계약서 또는 예약서 - 사업양수에 관한 이사회 의사록 - 본점 및 영업소의 현황 - 출자자(또는 주주) 구성 및 경영지배구조 계획 - 채권자 등 이해관계인의 권익보호계획 - 임원(예정자 포함) 이력서 - 법 제5조, 법 제6조, 법 제22조제1항, 법 제27조제1항에 저촉되지 않음을 증명하는 서류(신용정보업 영위 허가 참조) - 양수회사의 양수자금 조달계획서	- 사업양수 인가 신청서 - 사업양수 목적 및 사유 - 정관 및 법인등기부등본 - 자본금 또는 기본재산의 지분을 기재한 서류 - 재무제표 - 2년간의 사업계획서(양수 후 2년간 추정 재무제표, 인력 및 조직운영계획, 업무범위 및 영업전략 등) 및 예상수지계산서 - 사업양수 관련 계약서 또는 예약서 - 사업양수에 관한 이사회 의사록 및 주주총회 의사록 - 본점 및 영업소의 현황 - 출자자(또는 주주) 구성 및 경영지배구조 - 채권자 등 이해관계인의 보호절차 이행을 증명하는 서류 - 예비인가내용 및 조건의 이행을 증명하는 서류 - 임원 이력서 - 법 제5조, 법 제6조, 법 제22조제1항, 법 제27조제1항에 저촉되지 않음을 증명하는 서류(신용정보업 영위 허가 참조) - 제22조제2항에 따른 내부관리규정 - 회계처리·감사·조직관리 등 내부통제에 관한 규정

구분	예비인·허가	인·허가
4. 사업양도 인가	- 사업양도 예비인가 신청서 - 사업양도 목적 및 사유 - 정관변경(안) - 재무제표 - 2년간의 사업계획서(양도 후 2년간 추정재무제표, 인력 및 조직운영계획, 업무범위 및 영업전략 등)(일부양도의 경우에 한함) - 사업양도 관련 계약서 또는 예약서 - 사업양도에 관한 이사회 의사록 - 채권자 등 이해관계인의 권익보호계획, 자산 및 부채에 대한 조치내역 및 계획	- 사업양도 인가 신청서 - 사업양도 목적 및 사유 - 정관 - 재무제표 - 2년간의 사업계획서(양도 후 2년간 추정재무제표, 인력 및 조직운영계획, 업무범위 및 영업전략 등)(일부양도의 경우에 한함) - 사업양도 관련 계약서 또는 예약서 - 사업양도에 관한 이사회 의사록 및 주주총회 의사록 - 채권자 등 이해관계인의 보호절차 이행을 증명하는 서류 - 사업양도후 해산하는 경우에는 청산사무의 추진계획 - 사업의 일부 양도 후 영위할 수 없는 업무가 있는 경우 그 업무의 정리계획 - 예비인가내용 및 조건의 이행을 증명하는 서류

2. 신용정보집중기관

예비허가	허가
- 신용정보집중기관 예비허가신청서 - 정관 또는 정관(안) - 재산목록 및 그 내용을 확인할 수 있는 서류 - 2년간 사업연도분의 사업계획 및 수입·지출예산을 적은 서류 1부 - 발기인 총회의사록(이사회 의사록(이사회를	- 신용정보집중기관 허가신청서 - 정관 또는 정관(안) - 재산목록 및 그 내용을 확인할 수 있는 서류 - 2년간 사업연도분의 사업계획 및 수입·지출예산을 적은 서류 1부 - 발기인 총회의사록(이사회 의사록(이사회를

예비허가	허가
구성하지 아니한 경우 총회 회의록))	구성하지 아니한 경우 총회 회의록))
- 신용정보집중관리위원회(공익위원선임위원회 및 소위원회 포함) 구성 및 운영(안)(종합신용정보집중기관에 한함)	- 신용정보집중관리위원회(공익위원선임위원회 및 소위원회 포함) 구성 및 운영(안) (종합신용정보집중기관에 한함)
- 영 제21조제5항제1호가목에 따른 위험관리체계 및 내부통제장치를 마련할 수 있음을 확인할 수 있는 서류 1부	- 영 제21조제5항제1호가목에 따른 위험관리체계 및 내부통제장치가 마련되어 있음을 입증하는 서류 1부
- 영 제21조제5항제1호나목에 따른 이해상충방지체계를 마련할 수 있음을 확인할 수 있는 서류 1부(집중기관업무 외의 다른 업무를 하는 경우에 한함)	- 영 제21조제5항제1호나목에 따른 이해상충방지체계가 마련되어 있음을 입증하는 서류 1부(집중기관업무 외의 다른 업무를 하는 경우에 한함)
- 영 제21조제5항제1호라목에 따른 사원의 구성에 관한 계획 및 업무방법 등을 마련할 수 있음을 확인할 수 있는 서류 1부(종합신용정보집중기관에 한함)	- 영 제21조제5항제1호라목에 따른 사원의 구성에 관한 계획 및 업무방법 등이 마련되어 있음을 입증하는 서류 1부(종합신용정보집중기관에 한함)
- 인력 및 물적시설(채용, 구매 등이 예정된 인력·물적시설 포함)의 현황을 확인할 수 있는 서류 1부	- 인력 및 물적시설(채용, 구매 등이 예정된 인력·물적시설 포함)의 현황을 확인할 수 있는 서류 1부
- 신용정보를 집중관리·활용하는데 있어서 전문성을 갖출 수 있음을 확인할 수 있는 자료 1부	- 신용정보를 집중관리·활용하는데 있어서 전문성을 갖추었음을 확인할 수 있는 자료 1부
- 임원(예정자 포함) 이력서 1부	- 임원(예정자 포함) 이력서 1부
- 주무부처의 비영리법인 설립허가증(개별신용정보집중기관에 한함)	- 주무부처의 비영리법인 설립허가증(개별신용정보집중기관에 한함)
- 집중관리·활용의 필요성	- 법인등기부등본
	- 제22조제2항에 따른 내부관리규정
	- 집중관리·활용의 필요성
	- 예비허가내용 및 조건을 이행하였음을 확인할 수 있는 서류

[별표 2]

신용조회업 및 신용정보집중기관 허가에 필요한 정보처리·정보통신설비 요건

(제6조제1항 및 제26조의4제1항 관련)

구성	세부 요건
시스템 구성	1. 시스템 구성에 다음 항목을 포함할 것 가. D/B서버, 통신서버, 보안서버 등 통신구간 암호화 시스템 나. WEB서버(인터넷서비스를 제공할 경우에 한함) 다. 저장장치 라. 그 밖에 주변장치 2. 백업 및 복구시스템 3. 시스템 보안 및 시설 보안을 포함한 보안관리 체계
시스템 성능	1. 보유정보를 적절하게 처리할 수 있는 성능을 갖출 것 2. 온라인서비스 또는 공중통신망을 통한 정보의 수집 및 제공을 적절하게 처리할 수 있는 성능을 갖출 것 3. 백업 및 복구작업이 최소한의 시간내에 가능할 것
보안체계	1. 방화벽(Fire-Wall)을 갖출 것 2. 침입을 탐지·경고·차단할 수 있는 보안시스템을 갖출 것 3. 내부네트워크와 신용조회네트워크를 분리하여 운용할 것 4. 정보이용자 확인 체계(사용자 인증)를 갖출 것 5. 데이터 암호화처리 체계를 갖출 것 6. 외부침입 방지, 출입자관리 통제 및 데이터 반·출입 통제에 대한 대책을 강구할 것 7. 백업 및 소산관리 대책을 강구할 것
운용능력	1. 시스템 운용능력을 갖출 것 2. 프로그램 개발능력을 갖출 것

[별표 2의2]

신용정보업의 양도·양수 등의 인가의 세부요건

(제11조의2 관련)

1. 사업의 전부 양도

가. 해당 신용정보회사의 경영 및 재무상태 등에 비추어 부득이 할 것

나. 신용정보주체의 보호 및 건전한 신용질서 유지에 지장을 초래하지 않을 것

다. 「상법」 등 관계 법령에 따른 절차 이행에 하자가 없을 것

2. 사업의 일부 양도

가. 제1호가목부터 다목까지의 기준을 충족할 것

나. 사업의 일부 양도 후 2년간의 추정재무제표 및 수익전망이 영업계획에 비추어 타당성이 있을 것

다. 주된 시장, 주된 고객, 주된 서비스 내용 등 영업전략 및 업무범위가 적정할 것

라. 사업의 일부 양도 후 영위할 수 없는 업무의 정리계획이 적정할 것

3. 분할의 경우

가. 신용정보업의 효율화 및 건전한 신용질서 유지에 관한 사항

1) 신용정보업의 효율적 영위, 구조조정의 촉진 등 분할 목적이 타당할 것

2) 기존 거래자에 대한 불이익이 없을 것

나. 영업계획 및 조직운영계획에 관한 사항

1) 분할 이후 2년간의 추정재무제표 및 수익전망이 영업계획에 비추어 타당성이 있을 것

2) 주된 시장, 주된 고객, 주된 서비스 내용 등 영업전략 및 업무범위가 적정할 것

3) 분할 후 영위할 수 없는 업무의 정리계획이 적정할 것

4) 조직 및 인력운영체제가 적합할 것

다. 소유구조 변경에 관한 사항

분할 후 주주구성계획이 법 제5조에 적합하고 주요출자자는 영 제6조제4항에 따른 <별표 1>의 요건을 충족할 것

라. 「상법」 등 관계 법령에 따른 절차 이행에 하자가 없을 것

4. 합병의 경우

가. 신용정보업의 효율화 및 건전한 신용질서 유지에 관한 사항

1) 신용정보업의 효율적 영위, 구조조정의 촉진 등 합병의 목적이 타당할 것

2) 기존 거래자에 대한 불이익이 없을 것

3) 합병에 대한 공정거래위원회의 경쟁제한성 검토결과가 적정할 것

나. 영업계획 및 조직운영계획에 관한 사항

1) 합병 이후 2년간의 추정재무제표 및 수익전망이 영업계획에 비추어 타당성이 있을 것

2) 주된 시장, 주된 고객, 주된 서비스 내용 등 영업전략 및 업무범위가 적정할 것

3) 합병 후 영위할 수 없는 업무의 정리계획이 적정할 것

4) 조직 및 인력운영체제가 적합할 것

다. 소유구조 변경에 관한 사항

합병 후 주주구성계획이 법 제5조에 적합하고 주요출자자는 영 제6조제4항에 따른 <별표 1>의 요건을 충족할 것

라. 「상법」 등 관계 법령에 따른 절차 이행에 하자가 없을 것

5. 사업의 양수

합병의 경우를 준용한다.

[별표 3]

기술적·물리적·관리적 보안대책 마련 기준(제20조 관련)

Ⅰ. 목 적

이 기준은 영 제16조제1항에서 정하는 신용정보의 기술적·물리적·관리적 보안대책과 관련된 구체적인 기준을 정함을 목적으로 한다.

Ⅱ. 기술적·물리적 보안대책

1. 접근통제

① 신용정보회사등은 개인신용정보를 처리할 수 있도록 체계적으로 구성한 전산시스템(이하 "개인신용정보처리시스템"이라 한다)에 대한 접근권한을 서비스제공을 위하여 필요한 최소한의 인원에게만 부여한다.

② 신용정보회사등은 전보 또는 퇴직 등 인사이동이 발생하여 신용정보회사등의 지휘·감독을 받아 개인신용정보를 처리하는 업무를 담당하는 자(이하 "개인신용정보취급자"라 한다)가 변경되었을 경우 지체 없이 개인신용정보처리시스템의 접근권한을 변경 또는 말소한다.

③ 신용정보회사등은 제1항 및 제2항에 따른 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관한다.

④ 신용정보회사등은 개인신용정보처리시스템에 침입차단시스템과 침입탐지시스템을 설치하여 보호한다.

⑤ 신용정보회사등은 개인신용정보주체 및 개인신용정보취급자가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자를 비밀번호로 이용하지 않도록 비밀번호 작성규칙을 수립하고 이행한다.

⑥ 신용정보회사등은 취급 중인 개인신용정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되지 않도록 개인신용정보처리시스템 및 개인신용정보취급자의 PC를 설정한다.

⑦ 신용정보회사등은 제휴, 위탁 또는 외부주문에 의한 개인신용정보처리시스템, 신용평가모형 또는 위험관리모형 개발업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치·운영한다.

⑧ 신용정보회사등은 업무목적을 위하여 불가피한 경우에만 외부사용자에게 개인신용정보처리시스템에 대한 최소한의 접근권한을 부여하고, 권한 부여에 관한 기록을 3년 이상 보관하는 등 적절한 통제시스템을 갖추어야 한다.

2. 접속기록의 위·변조방지

① 신용정보회사등은 개인신용정보취급자가 개인신용정보처리시스템에 접속하여 개인신용정보를 처리한 경우에는 처리일시, 처리내역 등 접속기록을 저장하고 이를 월 1회 이상 정기적으로 확인·감독한다.
② 신용정보회사등은 개인신용정보처리시스템의 접속기록을 1년 이상 저장하고, 위·변조되지 않도록 별도 저장장치에 백업 보관한다.

3. 개인신용정보의 암호화

① 신용정보회사등은 비밀번호, 바이오정보 등 본인임을 인증하는 정보는 암호화하여 저장하며, 이는 조회할 수 없도록 하여야 한다. 다만, 조회가 불가피하다고 인정되는 경우에는 그 조회사유·내용 등을 기록·관리하여야 한다.
② 신용정보회사등은 정보통신망을 통해 개인신용정보 및 인증정보를 송·수신할 때에는 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호의 어느 하나의 기능을 갖추어야 한다.

1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 개인신용정보를 암호화하여 송·수신하는 기능

2. 웹서버에 암호화 응용프로그램을 설치하여 개인신용정보를 암호화하여 송·수신하는 기능

③ 신용정보회사등은 개인신용정보를 PC에 저장할 때에는 이를 암호화해야 한다.
④ 신용정보회사등은 다음 각 호의 기준에 따라 주민등록번호의 암호화 등의 조치를 취하여야 한다.

1. 정보통신망을 통하여 송수신하거나 보조저장매체를 통하여 전달하는 경우에는 암호화하여야 한다.
2. 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone) 에 저장할 때에는 암호화하여야 한다.
3. 신용정보회사등이 내부망에 주민등록번호를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

가. 「개인정보 보호법」 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과

나. 그 밖의 신용정보회사등의 경우에는 개인신용정보처리시스템에 적용되고 있는 개인신용정보 보호를 위한 수단과 개인신용정보 유출시 신용정보주체의 권익을 해할 가능성 및 그 위험의 정도를 분석한 결과

4. 업무용 컴퓨터 또는 모바일 기기에 저장하여 관리하는 경우에는 상용 암호화 소프트웨어 또는 안전한 알고리즘을 사용하여 암호화하여야 한다.

⑤ 신용정보집중기관과 신용조회회사가 서로 개인식별번호를 제공하는 경우에는 상용 암호화 소프트웨어 또는 안전한 알고리즘을 사용하여 암호화하여야 한다.

⑥ 신용정보회사등이 개인신용정보의 처리를 위탁하는 경우 개인식별번호를 암호화하여 수탁자에게 제공하여야 한다.

4. 컴퓨터바이러스 방지

① 신용정보회사등은 개인신용정보처리시스템 및 개인신용정보취급자가 개인신용정보 처리에 이용하는 정보처리기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치한다.

② 제1항에 따른 백신 소프트웨어는 월 1회 이상 주기적으로 갱신·점검하고, 바이러스 경보가 발령된 경우 및 백신 소프트웨어 제작 업체에서 업데이트 공지를 한 경우에는 즉시 최신 소프트웨어로 갱신·점검한다.

5. 출력·복사시 보호조치

① 신용정보회사등은 개인신용정보처리시스템에서 개인신용정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화 한다.

② 신용정보회사등은 개인신용정보를 조회(활용)하는 경우 조회자의 신원, 조회일시, 대상정보, 목적, 용도 등의 기록을 관리하여야 하며, 개인신용정보취급자가 개인신용정보를 보조저장매체에 저장하거나 이메일 등의 방법으로 외부에 전송하는 경우에는 관리책임자의 사전 승인을 받아야 한다.

③ 개인신용정보취급자는 제1항 및 제2항의 준수에 필요한 내부시스템을 구축하여야 하며 사전 승인시 승인신청자에게 관련 법령을 준수하여야 한다는 사실을 주지시켜야 한다.

Ⅲ. 관리적 보안대책

1. 신용정보관리·보호인

① 신용정보관리·보호인은 다음 각 호의 업무를 담당한다.

1. 신용정보의 수집·이용·제공·폐기 등 관리 및 보호계획의 수립 및 시행
2. 신용정보의 수집·이용·제공·폐기 등 관리 및 보호 실태와 관행에 대한 정기적인 조사 및 개선
3. 신용정보 열람 및 정정청구 등 신용정보주체의 권리행사 및 피해구제
4. 신용정보 유출 등을 방지하기 위한 내부통제시스템의 구축 및 운영
5. 임직원 및 전속 모집인 등에 대한 신용정보보호교육계획의 수립 및 시행
6. 임직원 및 전속 모집인 등의 신용정보보호 관련 법령 및 규정 준수 여부 점검

② 신용정보관리·보호인은 제1항의 업무처리에 따른 기록을 3년간 보존하며, 점검결과를 경영진에 보고하고 업무처리절차에 적절히 반영하여야 한다.

2. 개인신용정보의 조회권한 구분

① 신용정보관리·보호인은 개인신용정보 조회 권한이 직급별·업무별로 차등 부여되도록 하여야 한다.

② 신용정보회사등은 개인신용정보의 조회기록에 대하여는 다음 각 호에 따라 주기적으로 그 적정성 여부를 점검하여야 하며, 점검결과를 업무에 반영하여야 한다.

1. 개인신용정보취급자의 개인신용정보 취급상황을 확인할 수 있는 수단 및 이의 점검·감사체제 정비
2. 개인신용정보 이상 과다 조회 부서 및 직원 등에 대해 수시 점검 실시
   가. 조회 권한을 초과하여 고객 정보 조회를 일정횟수 이상 시도한 직원에 대한 통제장치 마련
   나. 영업점 및 신용정보 관리부서의 개인신용정보 조회 건수에 대해 정기적으로 점검하고 조회건수가 평소보다 급증한 부서 및 직원들을 샘플링하여 점검 실시

③ 신용정보 관리·보호인은 개인신용정보취급자가 입력하는 조회사유의 정확성 등 신용조회기록의 정확성을 점검하여야 한다.

3. 개인신용정보의 이용제한 등

① 신용정보회사등은 신용평가모형 또는 위험관리모형 개발 위탁시 개인신용정보를 제공할 수 없다. 다만, 모형 개발을 위하여 불가피한 경우에는 실제 개인인신용정보를 변환하여 제공한 후 모형 개발 완료 즉시 삭제하여야 한다.

② 신용조회회사가 신용평가모형 및 위험관리모형을 개발하는 경우, 개인신용정보를 사용하지 않으면 모형 개발 또는 검증 등이 불가능하여 불가피하게 필요한 경우 외에는 실제 개인신용정보를 사용하여서는 아니 된다.

4. 제재기준 마련

신용정보회사등은 개인신용정보 오·남용에 대한 자체 제재기준을 마련하여야 한다.

[별표 4] 신용정보제공계약에 포함될 신용정보 보안관리 대책(제21조 관련)

1. 신용정보제공·이용자 간에 신용정보를 제공하는 경우

가. 제공되는 신용정보의 범위 및 제공·이용 목적

나. 제공된 신용정보의 업무목적 외 사용 및 제3자 앞 제공 금지에 관한 사항

다. 제공된 신용정보의 이용자 제한 및 전담 관리자 지정에 관한 사항

라. 신용정보제공·이용자간 신용정보 송수신시 정보유출 방지에 관한 사항

마. 신용정보의 사용·보관 기간 및 동 기간 경과 후 신용정보의 폐기·반납에 관한 사항

바. 가목부터 마목까지를 위반한 경우의 책임소재 및 제재에 관한 사항

2. 신용조회회사와 신용정보제공·이용자 간에 신용정보를 제공하는 경우

가. 1의 가목부터 마목까지의 사항

나. 신용정보를 제공받은 신용정보제공·이용자에 대한 이 법 등 관련 법규의 준수여부 점검 등에 관한 사항

다. 개인신용정보를 조회하는 근거가 되는 자료 또는 서류 등의 보관에 관한 사항

라. 개인신용정보 조회시 조회용도에 맞는 조회사유코드를 적절하게 입력하는 것에 관한 사항

마. 신용정보 보호 등을 위한 교육에 관한 사항

바. 가목부터 마목까지를 위반한 경우의 책임소재 및 제재에 관한 사항

3. 수집된 신용정보 처리 위탁에 따라 신용정보를 제공하는 경우

가. 1의 가목부터 마목까지의 사항

나. 수탁자에 대한 관리·감독에 관한 사항

다. 신용정보주체의 신용정보 보호 및 비밀유지에 관한 사항

라. 신용정보 처리 재위탁의 제한에 관한 사항

마. 수탁자가 위탁받은 업무를 재위탁하는 경우 위탁자에 대한 보고에 관한 사항

바. 그 밖에 신용정보 보호를 위하여 필요한 사항

사. 가목부터 바목까지를 위반한 경우의 책임소재 및 제재에 관한 사항

4. 신용정보 처리의 재위탁에 따라 제공하는 경우

가. 재위탁업무의 목적과 범위, 기간 및 재위탁하는 신용정보의 내용

나. 재수탁자 및 재수탁자의 임직원의 보안서약서 작성 및 제출에 관한 사항

다. 신용정보 보호 및 안전한 처리를 위한 기술적·물리적·관리적 보안대책에 관한 사항

라. 목적 달성 후 파기, 반납에 관한 사항 및 파기확인서 등 그 결과를 원수탁자에게 통보하는 사항

마. 원수탁자가 재수탁자를 관리·감독하는 사항(실태점검을 위하여 재수탁자의 업무공간에 출입하여 점검하는 사항을 포함한다)

바. 가목부터 마목까지를 위반한 경우의 책임소재 및 제재에 관한 사항

[별표 4의2]

신용정보 관리기준(제22조제1항 관련)

구 분			관리기준
1. 신용정보처리기준	1.1. 개인식별정보(영 제29조 각 호의 정보를 말한다)의 처리에 대한 동의	1.1.1. 동의 형태	▸ 개인신용정보 처리에 대한 동의와 별도 동의
		1.1.2. 동의 사항	▸ 개인식별정보의 수집·이용 목적 ▸ 수집하려는 개인식별정보의 항목 ▸ 수집된 개인식별정보의 보유 및 이용 기간 ▸ 동의 사항 변경 시 신용정보주체에게 고지 후 동의 획득
	1.2. 개인신용정보의 수집·이용에 대한 동의	1.2.1. (공통) 동의 및 고지사항	▸ 개인신용정보의 수집·이용 목적 ▸ 수집하려는 개인신용정보의 항목 ▸ 수집된 개인신용정보의 보유·이용 기간 ▸ 동의와 관련하여 녹취 시에는 녹취사실 고지 ▸ 영 제17조의2제4항에 따른 금융거래 등 상거래관계가 종료된 날에 관한 사항
	1.3. 개인신용정보의 제공에 대한 동의	1.3.1. (공통) 동의 및 고지사항	▸ 개인신용정보를 제공받는 자 ▸ 개인신용정보를 제공받는 자의 이용 목적 ▸ 제공하는 개인신용정보의 내용 ▸ 개인신용정보를 제공받는 자의 정보 보유 기간 및 이용 기간 ▸ 동의와 관련하여 녹취 시에는 녹취사실 사전고지 ▸ 영 제17조의2제4항에 따른 금융거래 등 상거래관계가 종료된 날에 관한 사항
		1.3.2. 필수적 제3자 제공에 대한 고지사항	▸ 개인신용정보의 필수적 제3자 제공과 금융거래 등 상거래 계약 체결 및 이행과의 관련성
		1.3.3. 선택적 제3자 제공에 대한 고지사항	▸ 개인신용정보의 선택적 제3자 제공은 금융거래 등 상거래 계약 체결에 필수적이지 않다는 사실 ▸ 개인신용정보의 선택적 제3자 제공 시의 혜택
	1.4. 동의를 받는 방법	1.4.1. 동의서 양식	▸ 필수적 동의사항과 선택적 동의사항을 구분하여 동의를 받는 경우 "필수사항"과 "선택사항"을 별도 페이지로 구분하거나 각각의 동의서 양식을 구분하는 등 신용정보주체가 각각의 동의사항을 쉽게 구분하여 이해할 수 있도록 조치 ▸ 개인신용정보를 제공받는 제3자가 복수인 경우 사업내용, 연관된 부가서비스 등을 기준으로 개별 또는 다수 그룹으로 구분
	1.5. 신용정보의 제공	1.5.1. 신용정보의 제공 계약	▸ 신용정보의 보안관리 대책에 대하여는 별표 4를 적용 ▸ 신용정보의 제공에 대한 신용정보의 기술적·물리적·관리적 보안조치에 관한 사항에 대하여는 별표 3을 적용

구 분			관리기준
		1.5.2. 법 제32조제6항에 따른 개인신용정보의 제공	▸ 법 제32조제7항에 따라 개인신용정보 제공 사실 통지
		1.5.3. 신용정보를 제공받는 자의 확인	▸ 개인신용정보를 제공받는 자의 신원과 이용 목적을 확인 ▸ 1.5.1.에 따른 신용정보의 이용·보관 기간 및 동 기간 경과 후 신용정보의 폐기 또는 반납에 관한 사항의 결과 확인
	1.6. 신용정보의 삭제	1.6.1. 파기의 방법	▸ 삭제 후 복구 및 재생되지 않는 방법으로 조치
	1.7. 개인신용정보의 보유기간 등 (법 제20조의2)	1.7.1. 선택적 신용정보 삭제	▸ 법 제20조의2제1항에 따른 금융거래 등 상거래관계가 종료된 날부터 3개월 내에 선택적 신용정보 삭제
		1.7.2. 필수적 신용정보 분리 보관 및 접근제한	▸ 법 제20조의2제1항에 따라 필수적 신용정보(이하 "필수적 신용정보")를 관리하는 경우 현재 거래 중인 고객 정보와 분리 보관 ▸ 필수적 신용정보를 관리하는 관리책임자 지정 ▸ 관리책임자로부터 권한을 부여받은 개인신용정보취급자에 한하여 필수적 신용정보 접근 가능 ▸ 필수적 신용정보의 취급 권한부여 및 이용 내역 기록보존 (최소 3년)
		1.7.3 신용정보 삭제	▸ 법 제20조의2제2항에 따라 금융거래 등 상거래관계가 종료된 날부터 최장 5년내에 신용정보 삭제 ▸ 개인신용정보 삭제의 시행 및 확인은 신용정보관리·보호인의 책임 하에 수행 ▸ 신용정보관리·보호인은 개인신용정보 삭제 후 파기 결과를 확인 ▸ 신용정보제공·이용자는 개인신용정보의 삭제에 관한 사항 기록·관리
		1.7.4 신용정보의 보관	▸ 1.7.2의 필수적 신용정보 취급자 제한을 준용
	1.8.1. 신용정보 처리의 위탁	1.8.1. 신용정보 보호 조치의무	▸ 1.5.1. 신용정보의 제공계약 준용
		1.8.2. 법 제17조제5항에 따른 수탁자의 교육의 내용	▸ 신용정보 보호 관련 법령 및 제도의 내용 ▸ 신용정보의 보호 및 안전한 처리에 관한 사항
2. 신용정보관리·	2.1. 신용정보 관리·보호인	2.1.1. 신용정보관리·보호인의 업무	▸ 법 제20조제4항에 따른 업무 ▸ 별표 3의 관리적 보안대책에서 정하는 업무 ▸ 정보유출 대응매뉴얼(contingency plan) 마련 ▸ 관리적 보안대책 시행결과에 따른 시정·개선에 필요한 조치
		2.1.2.	▸ 신용정보관리·보호인을 지정하거나 변경하는 경우 신용정보

구 분			관리기준
보호인		신용정보관리·보호인의 공개	관리·보호인의 지정 및 변경 사실, 성명과 부서의 명칭, 전화번호 등 연락처를 홈페이지 등을 통하여 공개 ▸ 신용정보관리·보호인을 공개하는 경우 신용정보 보호와 관련한 고충처리 및 상담을 실제로 처리할 수 있는 연락처(담당자의 성명, 부서의 명칭, 전화번호)를 함께 기재
3. 신용정보의 누설 발생 시 조치	3.1. 개인신용정보의 누설의 예시	3.1.1. 신용정보회사등의 신용정보에 대한 통제 상실 또는 권한 없는 자의 접근	※ 신용정보회사등가 개인신용정보에 대하여 통제를 상실하거나 권한 없는 자의 접근을 허용한 경우로서 아래의 예시 및 이와 유사한 경우 등에는 개인신용정보 누설로 볼 수 있음 ▸ 개인신용정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우 ▸ 개인신용정보가 저장된 데이터베이스 또는 개인신용정보처리시스템에 권한 없는 자가 접근한 경우 ▸ 신용정보회사등의 고의 또는 과실로 개인신용정보가 포함된 파일 또는 종이문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우
	3.2. 신용정보주체에 대한 누설의 통지	3.2.1. 통지 사항	▸ 누설된 신용정보의 항목 ▸ 누설된 시점과 그 경위 ▸ 누설로 인하여 발생할 수 있는 피해를 최소화하기 위하여 신용정보주체가 할 수 있는 방법 등에 관한 정보 ▸ 신용정보회사등의 대응조치 및 피해 구제절차 ▸ 신용정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
		3.2.2. 통지 시기 및 방법 등	▸ 신용정보회사등은 누설 발생 확인 시 3.2.1.의 사항을 서면, 전화, 전자우편 등의 방법으로 해당 신용정보주체에게 통지 ▸ 누설된 신용정보의 신용정보주체가 1만 명 이상인 경우에는 영 제34조의2제2항 각 호에 따른 추가적인 공개 조치 ▸ 3.2.1.의 사항 통지 후 미확인사실에 대하여는 확인즉시 신용정보주체에게 통지
	3.3. 누설 신고	3.3.1. 신고 방법	▸ 서면, 전자우편, 모사전송 또는 이와 유사한 방법을 통하여 금융위원회 또는 금융감독원에 신용정보 누설신고서를 제출 ▸ 특별한 사정이 있는 경우에는 우선 금융위원회 또는 금융감독원에 누설사실을 알리고 추가 유출방지를 위한 조치를 취한 후 신용정보 누설신고서를 제출
4. 신용정보주체의 권리 보장	4.1. 신용정보 이용 및 제공 사실의 조회 (법 제35조)	4.1.1. 절차 보장	▸ 신용정보회사등은 신용정보주체가 영 제30조제3항의 방법으로 본인확인 후 개인신용정보 이용 및 제공 사실을 조회할 수 있는 개인신용정보조회시스템을 홈페이지 등을 통하여 제공 ▸ 신용정보주체가 개인신용정보조회시스템 등에 대한 접근을 용이하게 할 수 있도록 편의조치
		4.1.2. 신용정보 이용 및 제공 사실 통지	▸ 법 제35조제2항에 따른 통지의 간격은 연1회 이상 가능 하도록 통지 시스템 구축 ▸ 영 제30조제8항에 따른 수수료는 필요한 인적·물적 비용을

구 분			관리기준
		청구권 보장	고려하여 적정한 수준에서 채택
	4.2. 신용정보의 열람 및 정정청구권 (법 제38조)	4.2.1. 절차 보장	▸ 신용정보주체가 영 제30조제3항의 방법으로 본인확인 후 본인 신용정보를 열람·정정 청구 가능한 시스템 또는 절차 마련 ▸ 신용조회회사는 법 제39조 및 영 34조에 따라 개인신용정보주체에게 본인정보에 대한 무료 열람권 제공 ▸ 신용정보의 정정청구 접수 후 7일 이내에 신용정보주체에 처리결과 및 법 제38조제4항에 따른 시정요청 절차 고지
		4.2.2. 사실 조사	▸ 정정청구를 접수받은 경우 지체 없이 사실 조사에 착수 ▸ 정정 사유 확인 즉시 개인신용정보전산시스템에 정정청구 중 또는 사실조회 중임을 기입 및 해당 신용정보의 제공·이용 중단 ▸ 정정 후 최근 6개월 이내에 제공받은 자와 해당 신용정보주체가 요구하는 자에게 정정 사실 고지
	4.3. 상거래 거절 근거 신용정보의 고지 (법 제36조)	4.3.1. 절차 보장	▸ 본인확인 방법 및 신용정보주체의 요구에 따른 처리결과 고지의 업무처리방법 마련
		4.3.2. 고지 사항	▸ 영 제31조제1항 각 호에서 정하는 신용정보 중 신용정보주체와의 상거래관계 설정의 거절이나 중지의 근거가 된 신용정보 ▸ 해당 신용정보를 제공한 신용조회회사 및 신용정보집중기관의 명칭, 주소, 연락처 ▸ 신용조회회사 및 신용정보집중기관이 상거래관계의 설정을 거절하거나 중지하도록 결정한 것이 아니라는 사실 ▸ 신용조회회사 또는 신용정보집중기관으로부터 제공받은 정보 외에 다른 정보를 함께 사용하였을 경우에는 그 사실 및 그 다른 정보
	4.4. 개인신용정보 제공·이용 의 철회권 (법 제37조)	4.4.1. 절차 보장	▸ 신용정보제공·이용자는 개인신용정보 제공·이용 동의 철회 청구 시스템 또는 절차 마련 ▸ 1.3.3.의 고지사항에 법 제37조제1항·제2항 및 영 제32조제1항 및 제2항에 따른 개인신용정보 제공·이용 동의 철회권 및 영업 목적 연락중지 청구권 행사방법 및 담당자 연락처 등을 포함
		4.4.2. 고지 사항 등	▸ 철회청구를 받은 날부터 1개월 내에 해당 제3자에 대한 신용정보의 신규 제공중단 및 신용정보의 영업 목적 연락중지 조치 ▸ 제공동의 철회권 행사로 인하여 중단되는 서비스가 있는 경우 이에 대한 설명 의무
	4.5. 개인신용정보의 삭제 요구권 (법 제38조	4.5.1. 절차 보장	▸ 개인신용정보주체가 본인 개인신용정보의 삭제를 요구할 수 있는 절차 마련
		4.5.2. 고지 사항 등	▸ 개인신용정보 삭제로 인하여 개인신용정보주체에게 불이익 발생할 경우 이에 대한 충분한 사전 설명 후 삭제 조치 ▸ 삭제 후 그 결과를 개인신용정보주체에게 통지

구 분			관리기준
	의3)		▸ 삭제청구에 불구하고 개인신용정보를 법 제38조의3제1항 단서에 의하여 보관하는 경우에는 보관사유의 근거 및 안전한 보관에 관한 사항을 개인신용정보주체에 통지 ▸ 개인신용정보 삭제청구 처리 대장(최소 3년이상 보존)
5. 신용정보활용체제의 공시(법 제31조)	5.1. 공시 방법	5.1.1. 신용정보활용체제의 변경	▸ 신용정보활용체제를 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 지속적으로 공개 ▸ 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개
	5.2. 작성기준	5.2.1. 필수적 기재사항	▸ 관리하는 신용정보의 종류 및 이용 목적 ▸ 신용정보를 제3자에게 제공하는 경우 제공하는 신용정보의 종류, 제공 대상, 제공받는 자의 이용 목적 ▸ 신용정보의 보유 기간 및 이용 기간이 있는 경우 해당 기간, 신용정보 파기의 절차 및 방법 ▸ 법 제17조에 따라 신용정보의 처리를 위탁하는 경우 그 업무의 내용 및 수탁자 ▸ 신용정보주체의 권리와 그 행사방법 ▸ 법 제20조제3항에 따른 신용정보관리·보호인 또는 신용정보 관리·보호 관련 고충을 처리하는 사람의 성명, 부서 및 연락처 ▸ 신용등급 산정에 반영되는 신용정보의 종류, 반영비중 및 반영기간(신용조회회사만 해당)
		5.2.2. 임의적 기재사항	▸ 신용정보주체의 권익침해에 대한 구제방법 ▸ 신용정보의 열람청구를 접수·처리하는 부서
6. 신용조회업무	6.1. 정보의 수집	6.1.1. 수집의 제한	▸ 법에서 수집을 금지하는 정보가 수집되지 않도록 수집항목을 구성·관리 ▸ 수집항목의 적정성을 정기적으로 점검하고 필요시 수집항목을 조정
		6.1.2. 수집절차·방법의 표준화	▸ 표준화된 정보수집을 위한 정보수집 기준 마련 ▸ 정보 수집시 수집정보의 정확성을 확인할 수 있는 방법 및 절차 마련
		6.1.3. 수집정보의 검증 및 정정	▸ 수집된 정보의 정확성을 검증하는 방법·기준 및 업무처리절차 마련 ▸ 부정확하거나 사실과 다른 것으로 확인된 정보의 정정·삭제 기준 및 업무처리절차 마련 ▸ 검증업무가 수집업무와 독립적으로 처리될 수 있는 업무처리절차 및 기준 마련
	6.2. 신용등급의 산출 및 제공	6.2.1. 신용등급의 산출	▸ 기업평가시 평가대상 기업의 규모 및 업종에 따른 평가기준 마련 ▸ 등급산출의 적정성 심의 기준, 절차 마련(등급평정위원회 등) ▸ 심의시 독립적인 의사결정 보장을 위한 업무처리절차 및 기준 마련
		6.2.2.	▸ 연 1회 이상 평가모형의 변별력 검증을 시행하고 관련 기

구 분			관리기준
		모형검증 등 사후 관리	록을 보존(최소 3년) ▸ 평가업무와 독립적으로 검증 업무가 처리될 수 있는 업무처리절차 및 기준 마련 ▸ 모형검증 결과를 보고받는 별도 위원회 구성에 관한 사항 ▸ 기업평가이후 피평가기업의 신용상태에 중대한 영향을 미치는 상황 변화 등이 발생한 경우 신용등급 변경 기준 및 업무처리절차
		6.2.3. 이해상충 방지	▸ 등급 산출과 관련한 이해상충 방지체계 마련 ▸ 기업평가 관련 평가조직 및 영업조직의 분리
		6.2.4. 정보제공시 차별·강요금지	▸ 의뢰인에게 정보제공시 합리적 이유 없는 차별적 취급 금지 ▸ 평가서 발급 의뢰인에게 상품·서비스의 가입·이용 강제 금지

[별표 5]

공공단체의 지정범위(제24조 관련)

1. 「한국은행법」에 따른 한국은행
2. 「금융위원회의 설치 등에 관한 법률」에 따른 금융감독원
3. 「자본시장과 금융투자업에 관한 법률」에 따른 한국거래소
4. 「한국장학재단 설립 등에 관한 법률」에 따른 한국장학재단
5. 「한국전력공사법」에 따른 한국전력공사
6. 「대한무역투자진흥공사법」에 따른 대한무역투자진흥공사
7. 「한국가스공사법」에 따른 한국가스공사
8. 「한국광물자원공사법」에 따른 한국광물자원공사
9. 「예금자보호법」에 따른 예금보험공사
10. 「금융회사부실자산 등의 효율적 처리 및 한국자산관리공사의 설립에 관한 법률」에 따른 한국자산관리공사
11. 「공인회계사법」에 따른 한국공인회계사회
12. 「국민연금법」에 따른 국민연금관리공단
13. 「국민건강보험법」에 따른 국민건강보험공단
14. 「산업재해보상보험법」에 따른 근로복지공단

[별표 5의2]

신용정보집중기관 허가 세부요건

(제26조의4제2항 관련)

1. 인력

가. 신용정보주체를 보호하고 신용정보를 집중관리·활용하기 위한 전문성을 갖춘 다음의 어느 하나에 해당하는 인력을 적절하게 확보하고 배치할 것

(1) 공인회계사, 변호사 등의 자격 소지자

(2) 영 제2조제3항제1호·제3호·제4호에 해당하는 기관, 영 제5조제1항 각 호에 해당하는 기관 또는 다음 각 목의 금융 관련 단체에서 3년 이상 신용정보 관련 업무에 종사한 경력이 있는 사람 5명 이상이 포함될 것

가. 신용조회회사

나. 신용정보집중기관

다.「민법」 제32조에 따라 기획재정부장관의 허가를 받아 설립된 금융결제원

라.「보험업법」에 따른 보험요율 산출기관

(3) 그 밖에 신용정보집중기관 업무에 대한 전문성이 상기 인력에 준한다고 볼 수 있는 상당한 근거가 있는 자

나. 신용정보집중기관의 임원이 다음의 어느 하나에 해당하는 사실이 없을 것

(1) 최근 5년간 종합신용정보집중기관에 금융질서문란행위자로 등록된 사실

(2) 그 밖에 금융위원회가 신용정보집중기관의 경영의 건전성에 현저한 영향을 미칠 수 있다고 인정하는 것으로서 해당 대상자가 충분한 반증을 제시하지 못하는 사실

2. 물적 설비

가. 제26조의4제1항에 따른 정보처리·정보통신설비를 갖출 것

나. 업무공간과 사무장비

(1) 집중관리·활용하는 신용정보 중에서 개인의 건강에 대한 정보 등 특별히 민감한 정보는 별도 업무공간을 갖추는 등 정보차단벽(Chinese Wall)이 설치될 수 있도록 할 것

(2) 부서인원 대비 충분한 업무공간 및 사무장비를 갖출 것

(3) 내부기관 및 감독기관 등이 감독·검사업무를 수행함에 있어 법적 장애가 없을 것

다. 업무의 연속성을 유지할 수 있는 보완설비

(1) 파업 등 불시사태 또는 비상사태에 대비한 비상계획(Contingency Plan)이 마련되어 있을 것

3. 사업계획

가. 사업계획이 이 법 및 타 법령에 의하여 신용정보집중기관이 수행하도록 정한 업무를 적절하게 수행할 수 있을 것

나. 내부통제장치 및 신용정보주체 보호

(1) 총회(이사회가 설치된 경우 이사회 포함)와 경영진의 관계, 총회(이사회가 설치된 경우 이사회 포함)의 구성 및 운영방향, 감사의 권한과 책임 등이 적절할 것

(2) 임직원의 법규준수, 정보보호 및 임직원 위법행위 예방을 위한 적절한 감독 및 내부통제체계가 구축되어 있을 것

4. 업무방법

가. 업무방법의 마련 등이 집중관리·활용에 참여하는 기관의 종류에 따른 대표성과 중립성을 만족할 것

(1) 종합신용정보집중기관의 경우 업무방법에 관한 절차 및 내용에 있어서 참여하는 기관 및 집단간의 대표성과 중립성이 만족될 수 있도록 업무방법을 마련할 것

(2) 같은 종류의 금융회사 또는 같은 종류의 사업자간에 집중관리·활용하는 신용정보의 경우 금융회사 또는 사업자간 대표성과 중립성이 만족될 수 있도록 업무방법을 마련할 것

나. 신용정보주체를 보호할 수 있는 관리체계가 마련되어 있을 것

다. 신용정보의 효율적 이용과 체계적 관리를 도모할 수 있는 관리체계가 마련되어 있을 것

5. 지배구조 관련 사항

가. 「민법」 제32조에 따라 설립된 비영리법인일 것

나. 사원구성계획이 집중관리·활용에 참여하는 기관의 종류에 따른 대표성과 중립성을 만족할 것

6. 제26조의3에 따른 업무분리계획(종합신용정보집중기관이 기타업무를 수행하는 경우에 한정한다)

가. 재무에 관한 사항

(1) 집중기관업무와 기타업무사이에 별도의 회계장부를 마련하고 구분하여 회계처리 할 것

(2) 집중기관업무에 관련된 예·결산에 대하여 신용정보집중관리위원회의 의결을 받을 것

나. 인사에 관한 사항

(1) 임원(대표권을 가진 이사, 감사를 제외한다)이 집중기관업무와 기타업무를 겸직하지 아니할 것

(2) 집중기관업무의 독립성 및 연속성을 담보할 수 있는 인사관리체계를 마련할 것

다. 조직에 관한 사항

(1) 집중기관업무와 기타업무 간 정보의 교류를 차단할 것

(2) 집중기관업무와 기타업무 사이에 이해상충이 발생할 가능성을 파악·평가하고, 이를 적절히 관리할 수 있는 내부통제기준을 마련할 것

라. 시설에 관한 사항

(1) 집중기관업무와 기타업무 사이에 사무실 등 업무공간을 분리할 것

(2) 집중기관업무와 기타업무 사이에 전산자료가 독립적으로 저장되어 관리·감독·열람될 수 있도록 할 것

[별표 6]

신용정보 등록 및 이용기준(제24조의2제2항 및 제26조의4제3항 관련)

1. 식별정보

등록정보	등록기관	등록기준		이용기관
		대상주체	등록시기	
영 [별표2]의 식별정보	영 제21조제2항의 기관 중 당해 등록정보 보유기관	해당 개인, 기업 및 법인	등록사유발생시	식별정보와 연결된 정보의 이용기관

1) 영 제21조제2항의 기관이 「자산유동화에 관한 법률」제10조제1항에 따라 유동화자산의 관리를 위탁받은 경우 해당 유동화자산의 등록정보 보유기관으로 본다. 이하 이 표에서 같다.

2. 거래정보

(1) 개인

등록정보	등록기관	등록기준		이용기관
		대상주체	등록시기	
가. 대출, 당좌거래 등 관련 거래 정보				
대출현황(대출일자, 대출금액, 담보현황, 카드론·현금서비스 실적 등 포함)	영 제21조제2항의 기관 중 해당 등록정보 보유기관	해당 개인 (단, 종합신용정보집중기관은 전산수용능력등을 감안하여 대출금 집중기준을 조정할 수 있음)	등록사유발생일로부터 7영업일 이내	○ 영 제21조제2항의 기관 ○ 법 제4조에 따른 신용정보회사(신용정보회사는 해당 정보를 영 제21조제2항의 기관에 대해서만 제공할 수 있음)
대출성상품에 대한 청약철회에 따른 원상회복채권 정보	영 제21조제2항의 기관 중 해당 등록정보 보유기관	해당 개인	위와 같음	위와 같음
채무보증현황(채무보증일자, 채무보증금액 등 포함)	영 제21조제2항의 기관 중 해당 등록정보 보유기관	위와 같음	위와 같음	위와 같음
당좌·가계당좌예금개설 및 해지 현황	은행(농·수협 포함)	위와 같음	위와 같음	○ 영 제21조제2항의 기관 ○ 법 제4조에 따른 신용정보회사
나. 신용카드 관련 거래 정보				
신용카드현황(발급·해지사실 및 결제금액[주] 포함)	은행(농·수협 포함) 및 여신전문금융회사	위와 같음	위와 같음	위와 같음

2개 이상의 신용카드를 소지한 신용정보주체에 관한 관련거래 정보(신용판매·현금서비스 이용금액, 신용판매·현금서비스 리볼빙 이용잔액, 연체금액, 신용판매·현금서비스 신용공여한도 등 포함)	은행(농·수협 포함) 및 여신전문금융회사 중 해당 등록정보 보유기관	위와 같음	위와 같음	은행(농·수협 포함) 및 여신전문금융회사 중 등록기관에 해당하는 자
신용카드의 도난·분실 등 사고 발생에 관한 정보, 사고 종결에 관한 보상 및 처리정보 [주]	위와 같음	위와 같음	위와 같음	위와 같음
다. 보험계약 관련 거래정보				
보험계약 현황(보험계약일, 보험기간, 보험상품명, 급부명, 가입금액, 보험료, 보험회사명 및 보험계약상태, 피보험목적물 정보, 청약정보(청약시부터 계약 또는 거절시까지만 보유 가능) 등 포함)	보험회사, 수산업협동조합, 신용협동조합, 새마을금고 및 체신관서 중 해당 등록정보 보유기관	해당 개인	위와 같음	보험회사, 수산업협동조합, 신용협동조합, 새마을금고 및 체신관서 중 등록기관에 해당하는 자
피보험자 또는 보험금 청구권자에 관한 정보(성명, 개인식별번호, 직업 및 보험계약자와의 관계에 관한 정보 등 포함)	위와 같음	해당 개인이 체결한 보험계약(이하 "해당 보험계약"이라 함)의 피보험자 또는 보험금 청구권자	위와 같음	위와 같음
모집업무수탁자 정보(해당 보험계약을 모집한 모집업무수탁자의 이름·명칭 및 등록번호 등 포함)	위와 같음	해당 보험계약을 모집한 보험설계사, 보험대리점 또는 보험중개사	위와 같음	위와 같음
보험금 청구·지급 현황(사고접수일자, 보험금 청구일자, 보험금 지급일자, 보험금액, 실지급금액, 병원·정비공장 정보 등 포함)	위와 같음	해당 보험계약의 보험금 청구권자	위와 같음	위와 같음
보험금 지급사유(사고발생일시, 사고원인, 질병·부상·치료정보, 피해물 및 보상정보, 자동차보험의 경우에는 사고운전자	위와 같음	위와 같음	위와 같음	위와 같음

성명, 주민등록번호 등 포함)				
피해자 정보(피해자의 성명, 주민등록번호 포함)	위와 같음	해당 보험계약에서 보장하는 보험사고의 피해자	위와 같음	위와 같음
라. 금융투자상품 매매 관련				
코넥스소액전용투자계좌 관련 계좌 개설 및 폐쇄 정보 등	투자중개업자	해당 개인	등록사유발생시	투자중개업자

주) 신용카드결제금액, 신용카드의 도난·분실 등 사고 발생에 관한 정보, 사고 종결에 관한 보상 및 처리정보는 해당 신용정보를 보유한 신용카드업자가 동의하는 경우에 한함

(2) 기업 및 법인

등록정보	등록기관	등록기준		이용기관
		대상주체	등록시기	
가. 대출, 당좌거래 등 관련 거래 정보				
신용 공여 현황[1] (담보, 한도거래, 신용공여기간 등 포함)	영 제21조제2항의 기관 중 해당 등록정보 보유기관	○해당 기업 및 법인(종합신용정보집중기관은 전산수용능력 등을 감안하여 대출금 집중기준을 조정할 수 있음) ○주채무계열 및 기타 계열기업군 소속기업체	신용정보집중관리위원회가 정함	○ 영 제21조제2항의 기관 ○ 법 제4조에 따른 신용정보회사(신용정보회사는 해당 정보를 영 제21조제2항의 기관, 「공인회계사법」에 따른 공인회계사회, 영 제2조제3항제7호의 감사인 및 「자본시장과 금융투자업에 관한 법률」에 따른 신용평가회사에 대해서만 제공할 수 있음)
가계당좌·당좌예금 개설 및 해지 현황	은행(농·수협 포함)	○해당 기업 및 법인	위와 같음	○ 영 제21조제2항의 기관 ○ 법 제4조에 따른 신용정보회사
나. 신용카드 관련 거래 정보				
신용카드현황(발급·해지 사실 및 결제금액[2], 연체정보 포함)	은행(농·수협 포함) 및 여신전문금융회사	위와 같음	등록사유발생일로부터 7영업일 이내	위와 같음

신용카드의 도난·분실 등 사고 발생에 관한 정보[2], 사고 종결에 관한 보상 및 처리정보[2]	위와 같음	위와 같음	위와 같음	은행(농·수협 포함) 및 여신전문금융회사
다. 금융투자상품 매매 관련				
코넥스소액전용투자계좌 관련 계좌 개설 및 폐쇄 정보 등	투자중개업자	해당 기업체	등록사유발생시	투자중개업자

주 1) 은행 및 금융투자회사는 「은행업감독규정」 제3조 및 「금융투자업규정」 제8-33조에서 정한 신용공여, 그 밖의 금융회사는 이에 준하는 정보

2) 신용카드결제금액, 신용카드의 도난·분실 등 사고 발생에 관한 정보, 사고 종결에 관한 보상 및 처리정보는 해당 신용정보를 보유한 신용카드업자가 동의하는 경우에 한함

3. 신용도판단정보

등록정보	등록기관	등록기준		이용기관
		대상주체	등록시기	
대출금 등의 연체 현황	영 제21조제2항의 기관 중 해당 등록정보 보유기관	○해당 개인 ○해당 기업 및 법인 ○관련인[주]	신용정보집중관리위원회가 정함	○ 영 제21조제2항의 기관 ○ 법 제4조에 따른 신용정보회사
대위변제, 대지급 발생 현황	위와 같음	위와 같음	위와 같음	위와 같음
무보증사채 상환불이행 현황	위와 같음	위와 같음	위와 같음	위와 같음
어음·수표 거래정지 처분 또는 부도거래 현황	위와 같음	○해당 기업 및 법인 ○관련인	위와 같음	위와 같음
금융투자상품의 투자매매·중개 관련 정보	금융투자업자 중 등록정보 보유기관	○해당 개인 ○해당 기업 및 법인	위와 같음	위와 같음
영 [별표 2]의 금융질서 문란정보	영 제21조제2항의 기관 중 해당 등록정보 보유기관	○해당 개인 ○해당 기업 및 법인 ○관련인	위와 같음	위와 같음
대출성상품에 대한 청약철회에 따른 원상회복의무 불이행정보	영 제21조제2항의 기관 중 해당 등록정보 보유기관	○해당 개인	위와 같음	위와 같음

주) 영 제2조제1항제3호 각 목의 어느 하나에 한함

4. 신용거래능력판단정보

등록정보	등록기관	등록기준		이용기관
		대상주체	등록시기	
증자 및 사채발행계획 확정내용	협조기관 (금융감독원)	○해당 기업 및 법인(종합신용	신용정보집중관리위원회가 정	○ 영 제21조제2항의 기관

		정보집중기관은 전산수용능력등을 감안하여 집중기준을 조정할 수 있음) ○ 주채무계열 및 기타 계열기업군 소속기업체	함	○ 법 제4조에 따른 신용정보회사
영 제2조제1항제4호에 따른 기업의 개황, 사업의 내용, 재무에 관한 사항, 감사인의 감사의견 및 납세실적 등과 영 [별표 2]에 의한 신용능력정보	영 제21조제2항의 기관 중 해당 등록정보 보유기관	해당 기업 및 법인	위와 같음	위와 같음

5. 기술신용정보

등록정보	등록기관	등록기준		이용기관
		대상주체	등록시기	
기술신용정보(기술신용평가가액과 이와 관련된 평가의견은 제외한다.)주)	○기술신용보증기금 ○신용조회회사 중 해당 등록정보 보유기관	해당 기업 및 법인	등록사유발생일로부터 7영업일 이내	-
기업 및 법인의 기술신용등급, 신용공여 현황 및 신용도판단정보	영 제21조제2항의 기관 중 해당 등록정보 보유기관	위와 같음	위와 같음	○ 기술신용보증기금 ○ 신용조회회사 중 기술신용정보 등록기관

주) 종합신용정보집중기관이 영 제21조의2제2항제2호에 따른 업무를 수행하는 경우에 한하여 등록기관으로부터 해당 정보를 집중

6. 공공정보

등록정보	등록기관	등록기준		이용기관
		대상주체	등록시기	
-경제법령 위반	영 제21조제2항의 기관 중 해당 등록정보 보유기관	위반자	신용정보집중관리위원회가 정함	○ 영 제21조제2항의 기관 ○ 법 제4조에 따른 신용정보회사
-사망자정보, 주민등록번호 또는 성명의 변경정	법 제23조제2항에 따른 공공기관 또	해당 개인	○법 23조제2항에 따른 공공	위와 같음

보	는 영 제21조제2항의 기관 중 해당 등록정보 보유기관		단체 보유정보 등록 시는 당해 공공기관과 협의하여 정함 ○ 영 제21조제2항의 기관 보유정보 등록시기는 신용정보집중관리위원회가 정함	
-국외이주신고 및 이주포기신고정보	위와 같음	위와 같음	위와 같음	위와 같음
-회생·간이회생·개인회생 결정, 파산·면책 결정, 채무불이행자명부 등재 ·말소 결정 등 법원의 재판·결정정보 -국세·지방세·관세의 체납정보 -과태료·사회보험료·공공요금 등의 체납정보 -신용회복위원회의 신용회복지원협약에 따른 신용회복지원 확정 정보 -한국자산관리공사의 신용회복지원 관련 규정에 의한 채무재조정 약정정보 -국민행복기금이 협약금융기관등으로부터 채권을 매입한 정보 및 채무조정 약정을 체결한 정보 -그밖의 공공정보(특허권, 법인등록에 관한 정보등)	위와 같음	해당 주체	○ 해당 공공기관과 협의하여 정함 ○ 영 제21조제2항에 따른 기관 보유정보 등록시기는 신용정보집중관리위원회가 정함	위와 같음
-고용보험, 산업재해보상보험, 국민건강보험 및 국민연금의 납부에 관한 정보	법 제23조제2항에 따른 공공기관	위와 같음	해당 공공기관과 협의하여 정함	신용조회회사(신용등급 산정에 활용하는 경우에 한한다.)
-전기사용에 관한 정보로서 전력사용량 및 전기요금 납부정보	위와 같음	위와 같음	위와 같음	위와 같음
-정부납품실적 및 납품액	위와 같음	위와 같음	위와 같음	영 제21조제2항의 기관, 신용조회회사(단, 신용조회회사는 영 제21조제2항의 기관 이외에는 제공할 수 없음)

[별지 제1호 서식] 신용정보업 (예비허가, 허가) 신청서(제5조제2항제1호 관련)

(앞면)

<table>
<tr><td colspan="5">신용정보업 (예비허가, 허가) 신청서</td><td>처리기간
: 90일
(예비허가를 받은 경우: 30일</td></tr>
<tr><td rowspan="3">신청인</td><td>성명(대표자)</td><td></td><td>주민등록번호</td><td colspan="2"></td></tr>
<tr><td>상호 또는 명칭</td><td colspan="4">(전화번호)</td></tr>
<tr><td>본점 및 영업소의 소재지</td><td></td><td>자본금 또는 기본재산</td><td colspan="2"></td></tr>
<tr><td>법인의 목적</td><td colspan="5"></td></tr>
<tr><td>허가받고자 하는 업무</td><td colspan="5"></td></tr>
<tr><td colspan="6">「신용정보의 이용 및 보호에 관한 법률 시행령」 제4조제1항에 따라 위와 같이 신청합니다.

0000년 00월 00일
신청인 _____ 서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="5">※구비서류
1. 정관 및 법인등기부 등본
2. 재무제표
3. 2년간의 사업계획서 및 예상수지계산서
4. 그 밖에 별표 1의2의 제1호가목에 따른 서류 및 이와 관련한 부속서류</td><td>수수료
없음</td></tr>
</table>

(뒷면)

<table>
<tr><td colspan="2">대표자 및 임원에 관한 사항</td><td></td></tr>
<tr><td colspan="2">인력에 관한 사항</td><td></td></tr>
<tr><td rowspan="2">물적 시설에 관한 사항</td><td>정보처리·정보통신설비 / 전산설비 및 자료관리체계</td><td></td></tr>
<tr><td>그밖의 시설</td><td></td></tr>
</table>

[별지 제2호 서식] 신용정보업 변경허가신청서(제5조제2항제2호 관련)

<table>
<tr><td colspan="4">신용정보업 변경허가신청서</td><td>처리기간
: 30일</td></tr>
<tr><td rowspan="3">신청인</td><td>대표자의 성명</td><td></td><td>신용정보업허가일자</td><td>0000년 00월 00일</td></tr>
<tr><td>상호</td><td></td><td>허가번호</td><td></td></tr>
<tr><td>본점 소재지</td><td colspan="3"></td></tr>
<tr><td>변경
사항</td><td colspan="4"></td></tr>
<tr><td colspan="5">「신용정보의 이용 및 보호에 관한 법률 시행령」 제4조제1항에 따라 위와 같이 신청합니다.

0000년 00월 00일
신청인 _____ 서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※구비서류
1. 변경사항을 확인할 수 있는 서류 1부</td><td>수수료
없음</td></tr>
</table>

[별지 제2의2호 서식] 양도·양수·분할·합병 (예비인가, 인가) 신청서(제5조제2항 제3호 관련)

<table>
<tr><td colspan="6">양도·양수·분할·합병 (예비인가, 인가)신청서</td><td colspan="3">처리기간
90일
(예비인가를 받은 경우 30일)</td></tr>
<tr><td rowspan="8">양수
합병
법인</td><td>상호</td><td colspan="3"></td><td>대표자</td><td>성명</td><td></td></tr>
<tr><td colspan="3"></td><td>주민등록번호</td><td></td></tr>
<tr><td rowspan="2">임원에 관한 사항</td><td>구분</td><td>성명</td><td colspan="4">주민등록번호</td></tr>
<tr><td></td><td></td><td colspan="4"></td></tr>
<tr><td>본점소재지</td><td colspan="3"></td><td>연락처</td><td colspan="2">전화:
팩스:</td></tr>
<tr><td>법인의 목적</td><td colspan="6"></td></tr>
<tr><td>영위하고자 하는 업무</td><td colspan="6"></td></tr>
<tr><td colspan="3">인력 및 물적시설에 관한 사항</td><td colspan="4"></td></tr>
<tr><td colspan="3">자본금 또는 기본재산에 관한 사항</td><td colspan="4"></td></tr>
<tr><td rowspan="8">양도
피합병
법인</td><td>상호</td><td colspan="3"></td><td>대표자</td><td>성명</td><td></td></tr>
<tr><td colspan="3"></td><td>주민등록번호</td><td></td></tr>
<tr><td rowspan="2">임원에 관한 사항</td><td>구분</td><td>성명</td><td colspan="4">주민등록번호</td></tr>
<tr><td>대표이사
감사</td><td></td><td colspan="4"></td></tr>
<tr><td>본점소재지</td><td colspan="3"></td><td>연락처</td><td colspan="2">전화:
팩스:</td></tr>
<tr><td>법인의 목적</td><td colspan="6"></td></tr>
<tr><td>영위하고자 하는 업무</td><td colspan="6"></td></tr>
<tr><td colspan="3">인력 및 물적시설에 관한 사항</td><td colspan="4"></td></tr>
<tr><td colspan="3">자본금 또는 기본재산에 관한 사항</td><td colspan="4"></td></tr>
<tr><td rowspan="6">존속
법인</td><td>상호</td><td colspan="3"></td><td>대표자</td><td>성명</td><td></td></tr>
<tr><td colspan="3"></td><td>주민등록번호</td><td></td></tr>
<tr><td rowspan="2">임원에 관한 사항</td><td>구분</td><td>성명</td><td colspan="4">주민등록번호</td></tr>
<tr><td></td><td></td><td colspan="4"></td></tr>
<tr><td>본점소재지</td><td colspan="3"></td><td>연락처</td><td colspan="2">전화:
팩스:</td></tr>
<tr><td>법인의 목적</td><td colspan="6"></td></tr>
</table>

	영위하고자 하는 업무	
	인력 및 물적시설에 관한 사항	
	자본금 또는 기본재산에 관한 사항	

「신용정보업감독규정」 제5조제2항에 따라 위와 같이 신용정보업의 (양도, 양수, 분할,분할합병, 합병)의 (예비인가, 인가)를 신청합니다.

0000년 00월 00일

신청인 _____ (인)

금융감독원장 귀하

※구비서류 1. 정관 및 법인등기부 등본	수수료
2. 재무제표 3. 사업양도·양수, 분할·합병 관련 계약서 또는 예약서 4. 그 밖에 별표 1의2의 제1호나목, 다목 및 라목의 구분에 따른 서류 및 이와 관련한 부속서류	없음

[별지 제2의3호 서식] 신용정보집중기관 허가신청서(제5조제2항제4호 관련)

<table>
<tr><td colspan="3">신용정보집중기관 허가신청서</td><td>처리기간
: 90일
(예비허가를 받은 경우 30일)</td></tr>
<tr><td rowspan="3">신청인에 관한 사항</td><td>집중기관의 명칭</td><td colspan="2"></td></tr>
<tr><td>대표자의 성명</td><td colspan="2"></td></tr>
<tr><td>소재지</td><td colspan="2"></td></tr>
<tr><td>허가받고자 하는 집중기관의 유형</td><td colspan="3">종합신용정보집중기관( ), 개별신용정보집중기관( )</td></tr>
<tr><td>집중관리·활용하려는 신용정보의 범위</td><td colspan="3"></td></tr>
<tr><td>교환대상자</td><td colspan="3"></td></tr>
<tr><td colspan="4">「신용정보의 이용 및 보호에 관한 법률 시행령」 제21조제1항에 따라 위와 같이 신청합니다.

0000년 00월 00일
신청인 _____ 서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="3">※구비서류
1. 정관 또는 정관(안)
2. 재산목록 및 그 증명서류
3. 2년간 사업연도분의 사업계획 및 수입·지출 예산을 적은 서류
4. 그 밖에 별표 1의2의 제2호에 따른 서류 및 이와 관련한 부속서류</td><td>수수료
없음</td></tr>
</table>

[별지 제3호 서식] 신용정보회사가 허가받은 사항에 관한 변경신고서(제9조제1항 관련)

<table>
<tr><td colspan="4">신용정보회사가 허가받은 사항에 관한 변경신고서</td><td>처리기간
15일</td></tr>
<tr><td rowspan="3">신고인</td><td>대표자의 성명</td><td></td><td>신용정보업
허가일자</td><td>0000년 00월 00일</td></tr>
<tr><td>상호</td><td></td><td>허가번호</td><td></td></tr>
<tr><td>본점소재지</td><td></td><td></td><td></td></tr>
<tr><td>변경
사항</td><td colspan="4">1. □ 자본금 또는 기본재산의 감소
2. □ 상호 등 정관의 변경</td></tr>
<tr><td>변경
사유</td><td colspan="4"></td></tr>
<tr><td colspan="5">「신용정보의 이용 및 보호에 관한 법률 시행령」 제8조제1항에 따라 위와 같이 신고합니다.

0000년 00월 00일
신고인 _____서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※ 구비서류
1. 변경사항을 확인할 수 있는 서류
2. 제9조제2항 또는 제9조제3항에 따른 심사에 필요한 자료</td><td>수수료
없음</td></tr>
</table>

[별지 제4호 서식] 신용정보회사가 허가받은 사항에 관한 변경 보고서(제10조 관련)

<table>
<tr><td colspan="4">신용정보회사가 허가받은 사항에 관한 변경 보고서</td><td>처리기간
15일</td></tr>
<tr><td rowspan="3">보고자</td><td>대표자의 성명</td><td></td><td>신용정보업
허가일자</td><td>0000년 00월 00일</td></tr>
<tr><td>상호</td><td></td><td>허가번호</td><td></td></tr>
<tr><td>본점소재지</td><td></td><td></td><td></td></tr>
<tr><td>변경
사항</td><td colspan="4">1. ☐ 대표자 및 임원의 변경
2. ☐ 법령의 개정내용을 반영하거나 법령에 의하여 인·허가 받은 내용을 반영하는 사항
3. ☐ 정관의 변경 중 정관의 실질적인 내용이 변경되지 아니하는 조문체제의 변경, 자구수정 등</td></tr>
<tr><td>변경
사유</td><td colspan="4"></td></tr>
<tr><td colspan="5">「신용정보의 이용 및 보호에 관한 법률 시행령」 제8조제2항에 따라 위와 같이 보고합니다.

0000년 00월 00일
보고자 _____서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※ 구비서류
1. 변경사항을 확인할 수 있는 서류</td><td>수수료
없음</td></tr>
</table>

[별지 제5호 서식] 지배주주 변경승인신청서(제11조 관련)

1. 신청인에 관한 사항
   - 상호(성명), 업종, 국적, 사업자등록번호(주민등록번호), 본점소재지(주소지) 등
2. 지배주주가 되려는 자의 주식취득대상 신용정보회사가 발행한 주식의 소유현황
   (주식수, 지분율, 취득방법, 취득금액 등)
3. 지배주주가 되려는 자의 주식취득대상 신용정보회사가 발행하였거나 발행할 주식의 취득계획(발행회사명 및 개황, 주식취득 목적, 취득하고자 하는 주식수, 지분율, 예정시기, 취득방법 등)

■ 첨부서류

1. 정관(이에 준하는 것을 포함하며, 법인의 경우에 한한다) 1부
2. 외국 기업의 경우에는 법인등기부 등본에 준하는 서류 1부
3. 최근 사업연도말 현재 재무제표 및 최근 사업연도말 이후 반기가 경과한 경우 반기재무제표(법인의 경우에 한한다) 1부
4. 제3호에 따른 재무제표에 대한 회계감사인의 감사보고서·검토보고서 1부
5. 지배주주가 되려는 자가 금융회사인 경우 그 금융기관에 적용되는 재무건전성 기준에 따라 산출한 재무상태 및 이에 대한 회계감사인의 검토보고서 1부
6. 상호출자제한기업집단 또는 주채무계열에 속하는 경우 그 소속기업 중 금융회사를 제외한 기업의 부채비율 산출내역서(최근 사업연도말 이후 승인신청일까지의 자기자본 변동내역서 포함) 및 회계감사인의 검토보고서 1부
7. 그밖에 신청사실의 타당성을 심사하기 위하여 필요한 서류

※ 영문제출가능서류는 영문, 국문서류를 함께 제출

「신용정보의 이용 및 보호에 관한 법률」 제9조제1항에 따라
위와 같이 지배주주의 변경승인을 신청합니다.

년 월 일

신청인(대리인) 서명 또는 인

금융위원회 위원장 귀하

[별지 제6호 서식] 신용정보업(휴업, 폐업) 신고서(제12조 관련)

<table>
<tr><td colspan="3">신용정보업(휴업, 폐업) 신고서</td><td>처리기간
즉시</td></tr>
<tr><td>상호</td><td></td><td>허가번호</td><td></td></tr>
<tr><td>본점소재지</td><td></td><td>허가일자</td><td></td></tr>
<tr><td>휴업기간</td><td>0000년 0월 0일부터
0000년 0월 0일까지</td><td>폐업연월일</td><td>0000년 0월 0일</td></tr>
<tr><td>사유</td><td colspan="3"></td></tr>
<tr><td colspan="4">「신용정보의 이용 및 보호에 관한 법률 시행규칙」 제4조에 따라 (휴업, 폐업) 하고자 위와 같이 신고합니다.

0000년 00월 00일
신고인 _____ 서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="3">※ 첨부서류
신용정보업 허가증</td><td>수수료
없음</td></tr>
</table>

[별지 제7호 서식] 신용정보회사의 겸업신고서(제13조제2항 관련)

<table>
<tr><td colspan="4">신용정보회사의 겸업신고서</td><td>처리기간
: 15일</td></tr>
<tr><td rowspan="2">신
청
인</td><td>상호</td><td></td><td>대표자의 성명</td><td></td></tr>
<tr><td>주소</td><td></td><td>연락처</td><td></td></tr>
<tr><td colspan="2">신고하고자 하는
업무 및 업무방법</td><td colspan="3"></td></tr>
<tr><td colspan="5">「신용정보업감독규정」 제13조제2항에 따라 위와 같이 신고합니다.

0000년 00월 00일
신고인 _____ 서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※ 구비서류
1. 겸업업무의 예상 영업규모, 손익전망 등에 비추어 해당 신용정보회사의 건전경영을 저해할 염려가 없고 수익기반 확충에 기여할 수 있는지 여부
2. 겸업업무가 관련법령에 따라 행정관청의 인가·허가·등록 및 승인 등의 조치가 필요한 경우 해당 인가·허가·등록 및 승인 등을 받았음을 증명할 수 있는 서류 또는 확약서
3. 겸업업무를 수행함에 따라 발생할 수 있는 이해상충 및 불공정행위 방지를 위하여 필요한 조직, 전문인력 및 적절한 업무체계를 증명할 수 있는 서류 또는 확약서</td><td>수수료

없음</td></tr>
</table>

[별지 제7의2호 서식] 신용조회회사의 겸업승인 신청서(제13조의2제4항 관련)

<table>
<tr><td colspan="4">신용조회회사의 겸업승인 신청서</td><td>처리기간 : 30일</td></tr>
<tr><td rowspan="2">신
청
인</td><td>상호</td><td></td><td>대표자의 성명</td><td></td></tr>
<tr><td>주소</td><td></td><td>연락처</td><td></td></tr>
<tr><td colspan="2">승인받고자 하는 업무의 내용</td><td colspan="3"></td></tr>
<tr><td colspan="5">「신용정보업감독규정」 제13조의2제4항에 따라 위와 같이 신청합니다.

0000년 00월 00일
신청인 _____ 서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※ 구비서류
1. 겸업업무의 예상 영업규모, 손익 전망 등에 비추어 해당 신용조회회사의 건전한 경영을 저해할 염려가 없고 수익기반 확충에 기여할 수 있는지 여부를 확인할 수 있는 서류
2. 겸업업무가 관련 법령에 따라 행정관청의 인가·허가·등록 및 승인 등을 받아야 하는 경우 해당 인가·허가·등록 및 승인 등을 받았음을 증명할 수 있는 서류 또는 확약서
3. 겸업업무를 수행함에 따라 발생할 수 있는 이해상충 및 불공정행위를 방지하기 위하여 필요한 조직, 전문인력 및 적절한 업무체계를 갖췄음을 증명할 수 있는 서류 또는 확약서
4. 신용조회회사가 의뢰를 받고자 하는 공공목적의 조사·분석 등의 업무의 내용</td><td>수수료

없음</td></tr>
</table>

[별지 제8호 서식] 신용정보회사 상임임원의 겸직승인 신청서(제14조제2항 관련)

<table>
<tr><td colspan="5">신용정보회사 상임임원의 겸직승인 신청서</td><td>처리기간
: 15일</td></tr>
<tr><td rowspan="5">신
청
인</td><td>성명</td><td></td><td rowspan="5">겸직
대상
법인</td><td>상호</td><td></td></tr>
<tr><td>주민등록번호</td><td></td><td>주소</td><td></td></tr>
<tr><td>소속</td><td></td><td>업종</td><td></td></tr>
<tr><td>직위</td><td></td><td>대표자</td><td></td></tr>
<tr><td>연락처</td><td></td><td>법인번호</td><td></td></tr>
<tr><td colspan="2">겸직하고자
하는 업무</td><td colspan="4"></td></tr>
<tr><td colspan="2">겸직 사유</td><td colspan="4"></td></tr>
<tr><td colspan="6">「신용정보업감독규정」 제14조제2항에 따라 위와 같이 신청합니다.

0000년 00월 00일
신청인 _____ 서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="5">※ 구비서류</td><td>수수료
없음</td></tr>
</table>

[별지 제9호 서식] 삭제 <2015.9.11.>

[별지 제10호 서식] 삭제 <2015.9.11.>

[별지 제11호 서식] 별지 제2의3호로 이동 <2015.9.11.>

[별지 제12호 서식] 신용정보집중관리위원회 협의·심의·결정 사항의 보고(제28조 관련)

<table>
<tr><td colspan="2">신용정보집중관리위원회 협의 · 심의 · 결정 사항의 보고</td><td>처리기간
15일</td></tr>
<tr><td>협의
·
심의
·
결정
사항</td><td colspan="2">1. 협의·심의·결정 일자
☐
2. 협의·심의·결정 내용
☐
☐</td></tr>
<tr><td colspan="3">「신용정보의 이용 및 보호에 관한 법률」 제26조제3항에 따라 위와 같이 보고합니다.

0000년 00월 00일
보고자 _____서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="2">※ 구비서류
협의 · 심의 · 결정과 관련된 서류</td><td>수수료
없음</td></tr>
</table>

[별지 제13호 서식] 위임직채권추심인 등록신청서(제30조제2항 관련)

<table>
<tr><td colspan="6">위임직채권추심인 등록신청서</td></tr>
<tr><td rowspan="2">신청인</td><td>상호</td><td></td><td>대표자의 성명</td><td colspan="2"></td></tr>
<tr><td>주소</td><td></td><td>연락처</td><td colspan="2"></td></tr>
<tr><td rowspan="5">등록대상자</td><td rowspan="2">자 격 구 분
(☑ 표시)</td><td>☐ 신용관리사</td><td colspan="3">자격증 번호 ( )</td></tr>
<tr><td>☐ 연 수</td><td colspan="3">○ 연수기관 :
○ 연수기간 :</td></tr>
<tr><td>성명</td><td></td><td>주민등록번호</td><td colspan="2"></td></tr>
<tr><td rowspan="2">주소</td><td rowspan="2"></td><td>연락처</td><td colspan="2"></td></tr>
<tr><td>E-mail</td><td colspan="2"></td></tr>
<tr><td colspan="5">「신용정보업감독규정」 제30조제2항에 따라 위와 같이 위임직채권추심인 등록을 신청합니다.

년 월 일

신청인 (인)

신 용 정 보 협 회 장 귀 하</td><td>수수료</td></tr>
<tr><td colspan="6">※ 첨부서류
자격요건을 갖추었는지 여부를 확인할 수 있는 서류
※ 위 내용의 변경이 없는 범위 안에서 전산파일 형태로 제출할 수 있습니다.</td></tr>
</table>

[별지 제14호 서식] 위임직채권추심인 등록부(제30조제4항 관련)

<table>
<tr><td colspan="5">【 인 적 사 항 】</td></tr>
<tr><td>성 명</td><td colspan="2"></td><td colspan="2" rowspan="5">사 진</td></tr>
<tr><td>주민번호</td><td colspan="2"></td></tr>
<tr><td>연 락 처</td><td colspan="2"></td></tr>
<tr><td>E-mail</td><td colspan="2"></td></tr>
<tr><td>소속회사</td><td colspan="2"></td></tr>
<tr><td>등록번호</td><td></td><td>등록 일자</td><td colspan="2"></td></tr>
<tr><td rowspan="2">자격 구분</td><td rowspan="2">□ 신용관리사</td><td colspan="3">자격증 번호 ( )</td></tr>
<tr><td colspan="3">합격일(년 월 일) ____회차</td></tr>
<tr><td></td><td>□ 연 수</td><td colspan="3">ㅇ 연수기관 :
ㅇ 연수일자 :</td></tr>
<tr><td>주 소</td><td colspan="4"></td></tr>
<tr><td colspan="5">【 변경 사항 】</td></tr>
<tr><td>연 월 일</td><td colspan="4">내 용</td></tr>
<tr><td></td><td colspan="4"></td></tr>
<tr><td></td><td colspan="4"></td></tr>
<tr><td></td><td colspan="4"></td></tr>
<tr><td></td><td colspan="4"></td></tr>
</table>

[별지 제15호 서식] 신용정보 이용 및 제공사실 통지서(제40조제1항 관련)

신용정보 이용 및 제공사실 통지서

귀하

「신용정보의 이용 및 보호에 관한 법률」 제35조에 따라 당사가 년 월 일(통지요구일) 부터 최근 3년간 귀하의 개인신용정보를 이용·제공(직접 제공한 경우에 한함)한 내역을 아래와 같이 통보합니다.

□ 이용내역

이용날짜	이용목적	이용한 신용정보의 내용	보유 및 이용기간

□ 제공내역

제공받은 자	제공목적	제공한 날짜	제공한 신용정보의 내용	보유 및 이용기간

* 기재내용에 대한 상세 설명내용 별도 첨부

본 통지내용이 사실과 다르거나 기타 문의사항이 있으신 경우에는 아래 담당자에게 연락하여 주시기 바랍니다.

20 . . .

○○○○㈜ 대표이사 (인)

담 당 자	직위 : 성명 : (전화번호 :)
영업점 주소	

<참고 : 신용정보 이용 및 제공사실 통지서 작성 방법>

□ 이용 및 제공된 신용정보를 구체적으로 안내

ㅇ 식별정보, 신용거래정보, 신용능력정보, 공공정보, 신용등급(평점)정보, 신용조회정보 등으로 구분

ㅇ 종류별로 세부 설명을 기술할 것

□ 이용목적에 대한 안내

ㅇ 법 제33조제1호에 따른 동의에 근거한 이용 또는 다른 법령상 의무를 준수하기 위하여 불가피한 경우 등을 구분하여 명시

□ 제공받은 자의 범위

ㅇ 이용자는 금융회사, 신용정보집중기관, 신용정보회사, 공공기관, 그밖에 신용정보제공·이용자, 본인 등 당해 신용정보주체의 신용정보를 제공받은 자를 모두 포함한다는 사실 기재

□ 제공한 목적에 대한 안내

ㅇ 여신심사, 신용카드발급, 신용상황변동확인, 신용정보 집중(수집), 채권추심, 신용조사, 고용, 민원처리, 재판, 수사, 본인조회 등으로 구분

ㅇ 종류별로 세부 설명을 기술할 것

(예) 여신심사 : 대출, 지급보증 등의 신규 취급, 기간연장, 한도변경, 여신사후관리 등을 위해 신용정보를 조회

□ 그밖의 안내 사항

ㅇ 그밖에 본 통지내용과 관련하여 신용정보주체에게 안내할 필요가 있는 내용 기재

[별지 제16호 서식] 신용정보 시정요청서(제42조 관련)

<table>
<tr><td colspan="4">신용정보 시정요청서</td><td>처리기간 : 15일</td></tr>
<tr><td rowspan="2">요청인</td><td>성명</td><td></td><td>주민등록번호</td><td></td></tr>
<tr><td>주소</td><td></td><td></td><td></td></tr>
<tr><td colspan="2">열람 및 정정청구기관</td><td></td><td></td><td></td></tr>
<tr><td colspan="2">시정요청내용</td><td></td><td></td><td></td></tr>
<tr><td colspan="5">「신용정보의 이용 및 보호에 관한 법률」 제38조제4항에 따라 위와 같이 요청합니다.

0000년 00월 00일
신청인 _____ 서명 또는 (인)

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※ 첨부서류
1. 정정청구를 한 내용을 기재한 서면 1부
2. 정정청구에 대한 처리결과 통지서 1부
3. 문제가 된 신용정보의 사실여부를 확인할 수 있는 서류 1부</td><td>수수료

없음</td></tr>
</table>

[별지 제17호 서식] 시정조치 결과보고서(제43조 관련)

<table>
<tr><td colspan="4">시정조치 결과보고서</td><td>처리기간
15일</td></tr>
<tr><td rowspan="3">보고자</td><td>상호 또는 명칭</td><td></td><td rowspan="2">사업자등록번호 또는 법인등록번호(비영리법인의 경우 고유번호)</td><td rowspan="2"></td></tr>
<tr><td>대표자의 성명</td><td></td></tr>
<tr><td>본점 또는 기관 소재지</td><td colspan="3"></td></tr>
<tr><td>보고 내용</td><td colspan="4">1. 시정요청 내용

2. 발생사유

3. 시정조치 내용</td></tr>
<tr><td colspan="5">「신용정보의 이용 및 보호에 관한 법률」 제38조제7항에 따라 위와 같이 보고합니다.

0000년 00월 00일
보고자 _____서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4"></td><td>수수료
없음</td></tr>
</table>

[별지 제18호 서식] 신용정보회사등의 신용정보 누설신고서(제43조의5 관련)

<table>
<tr><td colspan="4">신용정보회사등의 신용정보 누설신고서</td><td>처리기간
: 즉시</td></tr>
<tr><td>상호 또는 명칭</td><td></td><td>사업자등록번호 또는 법인등록번호(비영리법인의 경우 고유번호)</td><td colspan="2"></td></tr>
<tr><td>본점 또는 기관 소재지</td><td></td><td>대표자</td><td colspan="2"></td></tr>
<tr><td colspan="2">누설된 신용정보의 항목</td><td colspan="3"></td></tr>
<tr><td colspan="2">누설된 시점</td><td colspan="3"></td></tr>
<tr><td colspan="2">누설 경위</td><td colspan="3"></td></tr>
<tr><td colspan="2">누설로 인하여 발생할 수 있는 피해를 최소화하기 위하여 취한 조치</td><td colspan="3"></td></tr>
<tr><td colspan="2">누설로 인하여 발생할 수 있는 피해와 관련한 피해구제 절차</td><td colspan="3"></td></tr>
<tr><td colspan="2">신용정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처</td><td colspan="3"></td></tr>
<tr><td colspan="2">기타 참고사항</td><td colspan="3"></td></tr>
<tr><td colspan="5">「신용정보업감독규정」 제43조의5에 따라 위와 같이 신고합니다.

0000년 00월 00일
신고인 _____ 서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※ 구비서류
1. 누설경위와 관련한 증거서류 등 관련문서
2. 누설로 인하여 발생할 수 있는 피해를 최소화하기 위하여 취한 조치와 관련한 증빙서류 등 관련문서</td><td>수수료

없음</td></tr>
</table>

신용정보업감독업무시행세칙

[시행 2016.7.28] [세칙 제9999호, 2016.7.27, 일부개정]

제1조(목적) 이 세칙은 「신용정보의 이용 및 보호에 관한 법률」(이하 "법"이라 한다) 및 동법 시행령(이하 "영"이라 한다), 동법 시행규칙(이하 "규칙"이라 한다), 신용정보업감독규정(이하 "규정"이라 한다)에서 정하는 금융감독원장(이하 "감독원장"이라 한다) 소관사항의 시행에 필요한 사항을 정함을 목적으로 한다.

제1조의2(연차보고서) 규정 제22조의2제3항에 따라 감독원장이 정하는 서식은 <별지 제1호 서식>과 같다.

제2조(폐업시 보유정보의 처리) 신용정보회사 또는 신용정보집중기관이 규정 제23조에 따라 자료를 처분, 소거 또는 폐기한 경우에는 그 결과를 <별지 제2호 서식>에 따라 감독원장에게 제출하여야 한다.

제3조 삭제 <2015.11.25.>

제4조 삭제 <2015.11.25.>

제5조 삭제 <2015.11.25.>

제5조의2(모집업무수탁자의 모집경로 확인 등 보고) ① 규정 제43조의6에 따른 신용정보제공·이용자의 보고 서식은 <별지 제3호의2 서식>과 같다.
② 규정 제43조의6에 따른 등록기관의 보고 서식은 <별지 제3호의3 서식>과 같다.

제6조(회계처리 불일치 보고서) 규정 제46조제3항에 따른 불일치의 내용과 사유는 <별지 제4호 서식>에 따라 보고하여야 한다.

제7조(업무보고서)① 신용정보회사 및 신용정보집중기관은 법 제47조에 따른 업무보고서를 <별지 제5호 서식>에 따라 매분기 종료일 다음 달 말일까지 감독원장에게 제출하여야 한다.
② 제1항의 업무보고서 제출은 정보통신망(「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」에 따른 정보통신망을 말한다)을 이용한 전자문서의 방법으로 할 수 있다.
③ 업무보고서는 회계연도말은 결산 결과, 매분기말은 가결산 결과를 반영하여 작성한다.

부칙 <제9999호,2008.5.6>

이 세칙은 2008년 5월 9일부터 시행한다.

부칙 <제9999호,2009.9.30>

제1조(시행일) 이 세칙은 2009년 10월 2일부터 시행한다. 다만, <별표>의 신용평가회사의 표준내부통제기준은 2010년 1월 2일부터 시행한다.

제2조(적용례) <별지 제5호 서식>의 개정 내용은 2009년 12월 31일 기준 업무보고서부터 적용한다.

부칙 <제9999호,2011.9.30>

이 세칙은 2011년 9월 30일부터 시행한다.

부칙 <제9999호,2013.1.29>

이 세칙은 2013년 1월 29일부터 시행한다.

부칙 <제9999호,2015.11.25>

이 세칙은 2015년 11월 25일부터 시행한다.

부칙 <제9999호,2016.7.27>

제1조(시행일) 이 세칙은 2016년 7월 28일부터 시행한다.

제2조(적용례) <별지 제5호 서식> 업무보고서는 2016년 6월말 기준 업무보고서부터 적용한다.

<별표>

신용평가회사 표준내부통제기준

목 차

제1장 총칙 1

1.1 목적 1
1.2 적용 범위 1
1.3 용어의 정의 1
1.4 업무분장 및 조직 구성 2

제2장 내부통제 조직 및 운영 2

2.1. 준법감시체제 2
2.2. 준법감시책임자 2
2.2.1 선임 및 해임 2
2.2.2 권한 및 의무 3
2.2.3 준법감시부서의 설치 3
2.2.4 준법감시업무의 독립성 3
2.3. 내부통제기준의 제·개정 등 4
2.4. 감사 기준 4

제3장 신용평가업무 행위 준칙 4

3.1 신용평가의 공정성 4
3.1.1 신용평가의 원칙 4
3.1.2 구조화금융상품에 대한 신용평가 5
3.2 신용등급평가위원회 5
3.3 신용평가의 적정성 5
3.4 신용평가의 사후관리 5

제4장 이해상충의 관리 6

4.1 일반 원칙 6
4.2 신용평가의 이해상충 방지 6
4.2.1 회사의 이해상충 방지 6
4.2.1.1 절차와 정책 6
4.2.1.2 평가조직과 영업조직의 분리 6
4.2.1.3 이직자에 대한 신용평가 재검토 6
4.2.1.4 순환보직체계 마련 7
4.3 신용평가 금지 7
4.3.1. 이해상충 관계에 있는 관계회사 등에 대한 신용평가 금지 7
4.3.2. 이해상충 관계에 있는 내부직원의 신용평가 금지 7
4.4. 이해상충 관련 기재사항 7
4.5. 보상체계 7
4.6. 수수료 협상 8
4.7. 신용평가업무 참여 금지 8

제5장 신용평가결과 등의 제공 및 공시 ····· 8

5.1. 신용평가서의 제공 ····· 8
5.2. 공시의 의의 ····· 8
5.3. 공시의 원칙 ····· 9
5.4. 신용평가 결과의 공시 ····· 9
5.5. 신용평가 실적의 공시 ····· 9
5.6. 신용평가 방법론의 공시 ····· 9
5.7. 신용평가 관련 주요 정책의 공시 ····· 9
5.8. 구조화금융상품의 공시 ····· 10

제6장 일반 영업행위 준칙 ····· 10
6.1. 영업의 일반 원칙 ····· 10
6.2. 수수료 부과기준 등의 공시 ····· 10
6.3. 편익 등의 수령 제한 ····· 10

제7장 불공정행위 금지 ····· 11

제8장 신용평가자료 및 기밀정보의 관리 ····· 11

8.1. 신용평가 자료의 보관 및 유지 ····· 11
8.2. 신용평가 자료의 범위 ····· 11
8.3. 기밀정보관리의 절차 및 정책 ····· 12
8.4. 기밀정보의 이용 ····· 13
8.5. 기밀정보 관련 거래 금지 ····· 13
8.6. 전산자료의 관리 ····· 13

제9장 윤리의무 ····· 13

9.1 기본윤리 ····· 13
9.2 신용평가 및 영업활동에 있어서의 윤리 ····· 13
9.3. 보고의무 ····· 14
9.4 임직원의 금융투자상품 매매 ····· 14

제10장 준수여부 점검 등 ····· 15

10.1 준수여부의 점검 ····· 15
10.2.체크리스트 및 점검보고 체계의 마련 ····· 15
10.3.내부제보·신고제도의 운영 ····· 15
10.4.임직원 교육 ····· 16
10.5.위반시 처리사항 ····· 16

제1장 총칙

1.1 목적

이 표준내부통제기준(이하 〃기준〃이라 한다)은 "신용정보의 이용 및 보호에 관한 법률" (이하 "법" 이라 한다) 제29조에 따라 신용평가회사(이하 〃회사〃라 한다)와 그 임직원(계약직 및 임시직 등을 포함한다. 이하 이 기준에서 같다)이 회사의 업무를 수행함에 있어 준수하여야 할 절차 및 기준에 관한 사항을 정함으로써 신용평가의 공정성, 투명성 및 신뢰성을 확보하고 회사의 경영 건전성을 제고하며 고객 및 투자자 보호에 기여함을 목적으로 한다.

1.2 적용 범위

1. 이 기준은 회사와 그 임직원의 업무에 적용하며, 계약에 의하여 회사 업무의 일부를 위탁받은 자의 행위는 그 위임받은 범위내에서 이를 회사의 행위로 본다.
2. 회사와 그 임직원의 행위에 관하여 법, 시행령, 시행규칙 및 법에 의한 규정(감독업무시행세칙을 포함한다. 이하 〃관련법규〃라 한다)에서 정하는 사항 이외에는 이 기준에서 정하는 바에 따른다.
3. 회사는 각 회사의 특성과 사정을 고려하여 내부통제기준을 마련하되 이 기준의 내용에 부합하여야 하며, 이 기준과 상충되는 경우에는 이 기준을 우선하여 적용한다.
4. 회사의 내부통제에 관하여 이 기준에서 정하지 아니한 사항과 이 기준의 세부사항은 회사의 내규에 의하거나 별도의 세칙이나 지침에 위임할 수 있다.

1.3 용어정의

이 기준에서 사용하는 용어의 정의는 다음과 같다. 다만, 이 기준에서 정하지 아니한 용어는 관련법규에서 정하는 바에 따른다.

1. "신용등급"이라 함은 원리금상환가능성 또는 신용도에 대한 현재 의견을 표현한 기호체계를 말한다.
2. "신용등급평가위원회"라 함은 신용등급을 결정하기 위하여 회사의 내규에 의거하여 구성한 회의체를 말한다.
3. "신용평가대상"이라 함은 법 제2조 제12호에 따라 회사가 평가하는 금융상품, 신용공여 및 기업, 법인, 간접투자기구 등과 발행인 기타 신용평가를 의뢰하는 자를 말한다.
4. "기밀정보"라 함은 신용평가과정에서 신용평가대상 또는 그 대리인이 회사에 제공한 정보 중에서 소유권 및 기밀성에 대하여 문서상으로 명시한 정보를 말한다. 다만, 다음 각 목의 어느 하나에 해당하는 정보는 제외한다.

가. 이미 알려졌거나 공시된 정보
나. 신용평가대상 또는 그의 대리인이 공개하기 전에 기밀유지 조건 없이 신용평가회사에 제공한 정보
다. 신용평가대상에 대한 기밀유지 의무에 저촉되지 않는 것으로서 제3자로부터 제공된 정보 또는 해당 정보를 제공하는 것이 금지되지 않는 것으로서 제3자로부터 기밀유지 조건 없이 회사가 제공받은 정보
라. 회사가 기밀정보를 참조하지 않고 독자적으로 개발한 정보

5. "준법감시책임자"라 함은 회사와 그 임직원이 내부통제기준에서 정하는 정책과 절차

를 준수하도록 관리·감독하는 자를 말한다.
6. "애널리스트"라 함은 신용평가분석을 직접적으로 수행하는 직원(업종별 책임자를 포함한다)을 말한다.

1.4. 업무분장 및 조직 구성

① 회사는 영업의 종류, 업무의 성격, 이해상충의 정도 등을 감안하여 조직을 구성하여야 한다.
② 회사는 신용평가조직과 영업조직을 분리하여 조직을 구성하여야 하며, 이들 조직간 정보 및 인사의 교류를 제한하여야 한다.
③ 회사는 별도로 허가 또는 인가받아 겸영하는 업무가 있는 경우 법 제4조에 의한 신용평가업무 및 그에 딸린 업무와도 분리하여 조직을 구성하여야 한다.
④ 회사는 제1항 내지 제3항에 의한 조직이 효율적으로 기능할 수 있도록 조직구성과 업무분장에 관한 별도의 세부기준을 제정·운영할 수 있다.

제2장 내부통제 조직 및 운영

2.1 준법감시체제

① 회사는 임직원이 신용평가, 기타 업무를 수행함에 있어서 이해상충방지, 공정성 제고 및 위법·부당행위의 사전 예방에 필요한 효율적인 준법감시체제를 구축·운영하여야 한다.
② 제1항에 의한 준법감시체제는 다음 각 호의 사항을 수행할 수 있어야 한다.
1. 관련법규 등의 준수 프로그램의 입안·관리
2. 임직원의 관련법규 등의 준수 실태 모니터링
3. 임직원에 대한 준법관련 교육·자문
4. 금융위원회, 금융감독원(이하 "감독당국"이라 한다)과의 협조
5. 기타 제1호 내지 제4호에 부수되는 업무

2.2 준법감시책임자

2.2.1 선임 및 해임

① 준법감시책임자는 대표이사가 지정한다.
② 회사는 준법감시책임자가 독립적으로 직무를 수행할 수 있도록 하고, 적정 임기를 보장하여야 한다.
③ 최근 5년간 관련법규 또는 금융관련 법령을 위반하여 감독당국으로부터 법 제45조제7항에 따른 문책경고 또는 견책요구 이상에 해당하는 조치를 받은 자는 준법감시책임자가 될 수 없으며, 준법감시책임자로 임명된 이후 이에 해당하게 된 때에는 그 직을 상실한다.
④ 회사는 준법감시책임자를 임면하는 경우 그 사실을 금융감독원에 보고하여야 한다.

2.2.2 권한 및 의무

① 준법감시책임자는 다음 각 호의 사항에 대한 권한 및 의무를 가진다.
1. 업무전반에 대한 접근 및 회사에 대한 각종 자료제출 요구
2. 임직원의 위법·부당행위에 관하여 대표이사 및 감사에 대한 보고 및 시정요구
3. 내부통제기준 준수여부에 대한 정기 또는 수시 점검
4. 준법감시 강화를 위한 임직원 교육
5. 신용평가의 공정성, 신뢰성의 확보를 위한 업무전반에 대한 상시 감시·감독시스템의 구축·운영
6. 신용평가과정에서 이해상충을 관리하고 신용평가과정의 공정성을 위태롭게 할 수 있는 리스크 점검
7. 신용평가과정에서 사용하는 절차와 방법론과 관련한 내부통제 준수여부 점검
8. 신용평가, 평가방법론(평가모델을 사용하는 경우 평가모델을 포함한다. 이하 이 기준에서 같다)과 이와 관련한 불만, 이 기준 및 관련법규 등의 준수 관련한 불만, 신용평가 담당직원 및 이용자가 제기하는 신용평가관련 불만의 접수, 보관 및 처리를 위한 절차 마련
9. 이 기준에 따른 정책과 절차의 관장
10. 기타 대표이사가 필요하다고 인정하는 사항

② 준법감시책임자는 관련법규에서 정하는 바에 따라 감독당국에 제출하는 회사의 신용평가실적서와 업무보고서 등을 검토하고, 정확하고 신속한 공시를 위한 내부통제를 구축관리하며, 내부점검결과 중요사항을 발견하는 경우 감독당국에 관련 사실을 보고해야 한다.

2.2.3 준법감시부서의 설치

① 회사는 준법감시업무가 효율적으로 수행될 수 있도록 충분한 경험과 능력을 보유한 적절한 수의 인력으로 구성된 지원조직(이하 "준법감시부서" 라 한다)을 갖추어 준법감시책임자의 직무수행을 지원하여야 한다.

② 회사는 준법감시업무에 대한 자문기능 수행을 위하여 준법감시책임자, 인사담당부서장 및 전문가 등으로 구성된 준법감시위원회를 설치·운영할 수 있다.

2.2.4 준법감시업무의 독립성

① 회사는 준법감시책임자 및 준법감시부서가 자신의 직무를 공정하게 수행할 수 있도록 업무의 독립성을 보장하여야 하며, 그 직무수행과 관련된 사유로 부당한 인사상의 불이익을 주어서는 아니 된다.

② 준법감시책임자는 선량한 관리자로서의 주의 의무를 다하여 그 직무를 수행하여야 하며, 다음 각 호의 업무를 수행하는 직무를 담당하여서는 아니 된다.
1. 회사가 영위하고 있는 평가업무 및 그에 딸린 업무
2. 회사가 영위하고 있는 겸영업무
3. 평가방법론 개발 업무
4. 준법감시업무 담당 직원을 제외한 기타 임직원의 보상수준을 설정 또는 결정하는 회의의 참석

③ 준법감시책임자의 임기는 대표이사가 정하되, 2년 이상으로 한다.

④ 준법감시책임자는 관련법규와 이 기준의 준수여부를 점검하고, 위반행위에 대하여는 이를 조사하여 대표이사 및 감사에 보고하여야 한다. 다만, 경미한 사안이라고 판단되는 경우 보고대상에서 제외할 수 있다.

⑤ 기타 준법감시조직과 관련한 회사의 조직 및 업무분장에 대하여는 회사의 내규에서 정하는 바에 따른다.

2.3 내부통제기준의 제·개정 등

① 내부통제기준은 회사의 대표이사가 제정하고 필요한 경우 관련부서와 협의하여 개정할 수 있다.
② 준법감시책임자는 이 기준을 기초로 내부통제의 구체적인 지침, 컴플라이언스 매뉴얼, 임직원 윤리지침 등을 제정·시행할 수 있다.

2.4 감사 기준

회사는 감사가 수행하는 감사의 방법과 절차 등과 관련한 기준을 별도로 제정·운영하여야 한다.

제3장 신용평가업무 행위준칙

3.1. 신용평가의 공정성

3.1.1. 신용평가의 원칙

① 회사는 신용평가대상을 자산별·업종별로 구분하여 각각 평가의 기준과 방법을 기술한 평가방법론을 갖추고, 애널리스트가 해당 평가방법론에 기초하여 신용평가업무를 수행하도록 한다.
② 회사는 신용평가와 관련된 적합한 지식과 경험을 보유한 애널리스트로 평가실무팀을 구성하여 신용평가업무를 수행하도록 한다.
③ 회사는 신용평가를 위한 데이터가 부족하여 신뢰성 있는 신용평가의 수행에 심각한 의문이 제기되는 경우 신용등급 부여를 자제한다.
④ 회사는 신용평가과정에 편견이 개입되는 것을 방지하고 신용평가과정의 일관성이 유지되도록 한다.
⑤ 회사는 평가방법론을 주기적으로 점검하고 개선에 필요한 인적, 재정적 자원을 충분히 배분한다.

3.1.2. 구조화금융상품에 대한 신용평가

회사는 구조화금융상품에 대한 신용등급 부여과정이 객관적인 방식으로 이루어지도록 다음 각호의 내용을 준수하기 위한 세부 절차를 마련하여야 한다.

1. 평가방법론 및 이의 수정 내용을 정기적으로 검토하는 절차를 마련한다.
2. 구조화금융상품의 기초 자산의 리스크성격이 현저하게 변경되는 경우 신용등급을 결정하는 기존의 평가방법론이 평가에 적절한지 여부를 재평가한다.
3. 새로운 구조화금융상품의 복합적 성격이나 구조 또는 기초 자산에 대한 데이터가 부족하여 신뢰성 있는 신용평가의 수행 여부에 심각한 의문이 제기되는 경우 신용등급 부여를 자제한다.
4. 애널리스트가 구조화금융상품의 설계를 제안하거나 권고하지 않도록 한다.

3.2. 신용등급평가위원회

① 회사는 전문성과 다양한 의견을 가진 애널리스트가 참여하는 신용등급평가위원회(이하 "평가위원회"라 한다)를 구성한다.
② 회사는 평가위원회가 주주, 이사회, 기타 회사의 일반적인 의사결정기구와 독립적으로 의사결정을 하도록 보장하여야 한다.
② 평가위원회는 신용등급을 결정함에 있어 신용평가와 관련된 요소들 이외의 요소에 의해 영향을 받지 않도록 유의해야 한다. 즉, 회사, 신용평가대상, 투자자 또는 기타 시장참여자에게 미칠 수 있는 경제적, 정치적 효과를 고려하여 신용등급을 결정하여서는 아니 된다.
③ 평가위원회 참석자는 자유롭게 의견을 개진하되, 반대의견이나 논란의 여지가 있는 의견도 충분히 고려한다.

3.3. 신용평가의 적정성

① 회사는 신용등급을 공시하기 전에 신용평가대상 또는 그의 대리인에게 신용평가 결과를 알려주고, 신용평가대상 또는 그의 대리인이 추가적으로 자료를 제출할 기회를 주고, 어떤 사실에 관한 오류가 있는 경우 이를 설명할 기회를 부여한다. 이는 충분한 정보를 가지고 신용등급을 부여하기 위한 것으로 이에 대하여 신용평가대상 또는 그의 대리인의 답변이 있는 경우 이를 충분히 검토한다.
② 회사는 객관적인 자료를 근거로 신용등급을 결정하고, 신용평가보고서에 이용자를 오도할 수 있는 내용을 포함하지 않도록 한다.

3.4. 신용평가의 사후관리

회사는 신용등급이 부여된 이후에는 지속적으로 신용평가대상에 대하여 모니터링을 실시하고 정기적으로 그 결과를 발표한다.

제4장 이해상충의 관리

4.1 일반원칙

① 임직원은 업무를 수행하기 위해 이 기준과 관련법규를 숙지하여야 한다.
② 임직원은 자신의 업무를 수행함에 있어 위법·부당한 방법으로 회사나 고객을 상대로 자신의 이익 또는 보상을 추구해서는 아니 된다.
③ 회사의 사전승인을 얻어 회사 업무 이외의 대외활동을 하는 경우 자신의 이익을 위하여 업무상 취득한 정보 등을 이용하여서는 아니 된다.

4.2. 신용평가의 이해상충 방지

4.2.1. 회사의 이해상충 방지

4.2.1.1. 절차와 정책

① 회사는 이해상충 문제를 확인하고 제거·관리하는 것과 관련된 내부절차를 서면으로 제정한다.
② 회사는 신용평가 이외의 서비스에 관한 내부정책을 수립하고 이에 의거하여 이해상충 가능성이 있는 다른 사업으로부터 신용평가사업 및 애널리스트를 분리시킨다.
③ 회사는 이해상충과 관련한 제보에 대하여 심사한 후 이해상충을 완화시키는데 필요한 조치를 취한다.

4.2.1.2 평가조직과 영업조직의 분리

① 회사는 신용평가대상 또는 그의 대리인과의 수수료·계약 체결, 평가의뢰권유 등 영업업무를 수행하는 조직과 신용평가조직을 분리·구성하여 운영하여야 한다.
② 회사는 평가조직과 영업조직간 정보 및 인사의 교류를 제한해야 한다.
③ 신용평가 관련 영업을 전담하는 직원은 평가위원회 구성원으로 참여할 수 없다.

4.2.1.3 이직자에 대한 신용평가 재검토

애널리스트가 퇴직한 경우, 그 애널리스트가 관여한 신용평가대상이나 신용평가업무로써 거래했던 금융회사 등으로 이직하는 경우, 회사는 그가 이직하기 이전 2년 이상의 기간 동안 수행한 관련 신용평가업무를 점검해야 한다.

4.2.1.4 순환보직체계

회사는 애널리스트가 5년을 초과하는 기간 동안 동일한 신용평가대상을 평가하지 않도록 순환보직체계를 마련해야 하며, 동일 신용평가대상에 대한 신용평가활동에 관여하기 위해서는 최소 2년이 지나야 한다. (이 규정의 적용을 위하여 회사는 이 기준 최초 시행일로부터 2년의 유예기간을 둘 수 있다)

4.3. 신용평가 금지

4.3.1. 이해상충 관계에 있는 관계회사 등에 대한 신용평가 금지

회사는 다음 각 호의 어느 하나에 해당하는 이해관계에 있는 자에 대하여 신용평가를 할 수 없다. 다만, 제2호 및 제3호에 해당하는 자에 대해서는 신용평가서에 그 내역을 기재하여 공시하는 경우에는 그러하지 아니하다.

1. 회사는 법 제29조 제2항의 규정에 의한 출자관계에 있는 자
2. 당해 회사의 직전 사업년도 총수익의 10% 이상을 기여한 자
3. 당해 회사로부터 신용평가를 제외한 기타 용역을 제공받은 이후 1년이 경과하지 않은 자
4. 기타 관련법규에서 금지하고 있는 경우

4.3.2. 이해상충 관계에 있는 내부직원의 신용평가 금지

임직원과 다음 각 호의 어느 하나의 관계에 있는 자에 대하여 해당 임직원은 신용평가를 할 수 없다.

1. 회사의 애널리스트가 신용평가대상의 지분을 소유하고 있거나, 수수료 협의 또는 그밖의 중요한 사업관계 등을 맺고 있는 경우
2. 회사의 애널리스트가 신용평가대상 차주나 신용평가대상 증권의 발행자, 인수기관 등으로 부터 선물 또는 접대를 받은 경우(구체적인 사항에 대해서는 이 기준 6.3에서 정하는 바에 따른다)
3. 기타 관련법규에서 금지하고 있는 경우

4.4. 이해상충 관련 기재사항

① 회사는 법 제29조 제2항의 규정에 의해 대통령령이 정하는 자 이외의 자로서 당해 회사와 출자관계에 있는 자가 발행하는 금융상품 등에 대하여 신용평가를 하는 경우에는 신용평가서에 그 출자관계에 관한 사항을 기재하여야 한다.
② 회사는 신용평가서 교부시 발행자에 대한 신용평가의 적정여부를 확인할 수 있는 내용(발행자와의 지분관계, 평가일로부터 과거 1년간의 딸린 업무 및 겸영 업무 등 제공내역)을 기재한다.

4.5. 보상체계

① 회사는 실질적 또는 잠재적 이해상충문제를 제거하거나 효과적으로 관리할 수 있도록 임직원의 보수체계를 결정하여야 한다.
② 회사는 애널리스트의 보상과 성과평가를 애널리스트 자신이 평가한 신용평가대상으로부터 받는 수익과 연동되지 않도록 보상체계를 마련하여야 한다.

4.6. 수수료 협상

신용평가업무에 관여하고 있는 애널리스트와 신용등급 결정에 참여하는 자는 신용평가대상 또는 그의 대리인과 신용평가수수료에 관한 협의를 하거나 참여하지 않아야 한다.

4.7. 신용평가업무 참여 금지

① 회사의 임직원은 다음 각 호의 어느 하나에 해당하는 경우 해당 신용등급결정과정에 참여하거나 영향을 미치지 않도록 해야 한다.
1. 신용평가대상이 발행한 증권 또는 파생상품을 소유한 경우
2. 최근에 신용평가대상에 고용되었거나 기타 사업상 관계가 있는 경우
3. 친척(배우자, 부모(배우자의 부모를 포함한다), 자녀 또는 형제자매)이 현재 신용평가대상에서 근무하고 있는 경우
② 회사의 애널리스트(그의 배우자, 미성년 자녀를 포함한다)는 자신이 평가한 신용평가대상이 발행, 보증 또는 지원한 증권이나 파생상품을 매수, 매도하거나 기타 거래에 참여할 수 없다.
③ 회사의 애널리스트는 신용평가대상과 이해상충을 초래할 수 있는 개인적인 관계를 갖게 되는 경우 이를 준법감시책임자에게 알려야 한다.

제5장 신용평가결과의 제공 및 공시

5.1. 신용평가서 등의 제공

① 회사가 신용평가를 의뢰한 자에게 신용평가서를 내어주는 경우 관련법규에서 정하는 신용평가실적서(평가의견서, 신용평가실적서, 신용등급변화표, 평균누적부도율표를 포함한다) 등을 함께 제공한다.
② 회사는 신용평가서 및 신용평가실적서 등을 제공하는 경우 신용평가의 한계와 특성, 제한된 데이터의 내용 및 이용가능한 정보가 충분한지 여부를 명확히 기재해야 한다.

5.2. 공시의 의의

공시라 함은 신용평가업무와 관련된 사항을 회사 인터넷 홈페이지, 발간물, 언론, 증권유관기관 등을 통해 신용평가 정보이용자에게 전달하는 과정을 말한다.

5.3. 공시의 원칙

① 공시내용은 정확하게 공시되어야 한다.
② 공시대상의 공시내용이 확정되면 적시에 공시하여야 한다.
③ 공시업무는 정보이용자간 정보의 불균형이 발생하지 않도록 이루어져야 한다.

5.4. 신용평가 결과의 공시

① 회사는 신용등급, 신용등급과 관련된 등급감시(Rating Watch), 등급전망(Rating Outlook), 평가의견 등을 공시대상에 포함해야 한다.
② 회사는 본평가, 정기평가 및 수시평가가 이루어진 경우 그 결과를 적시에 공시해야 한다.

5.5. 신용평가 실적의 공시

① 회사는 신용평가 정보이용자가 회사의 평가능력을 파악하는데 도움을 주기 위하여 관련법규에서 정하고 있는 신용평가실적서 등을 감독당국에 제출하고 한국거래소, 금융투자협회에 비치·공시한다.
② 회사는 평가대상에 대한 등급별 분포 현황, 신용등급 변화표, 일정기간 이상의 등급별 연간 부도율, 평균누적 부도율 등의 정보를 인터넷 홈페이지 등의 방법을 통하여 공시한다.
③ 회사는 신용평가의 적합성 검증을 위하여 신용평가 결과에 대한 부도분석(Default Study) 및 채권 스프레드 관련 분석(Spread Study)을 매년 공시해야 하며 그 내용에는 성과 통계(부도율 통계), 신용등급 변동 현황, 부도기업분석, 신용등급과 시장수익률간의 관계 분석 등에 대한 내용이 포함되어야 한다.

5.6. 신용평가 방법론의 공시

① 회사는 평가방법론 및 그와 관련된 주요 관행, 절차 및 평가 프로세스에 중대한 변경이 있는 경우 이를 인터넷 홈페이지 게시 또는 보도자료를 통해 공개한다.
② 회사는 중대한 변경내용을 신용평가에 직접 적용하기 이전에 시장에 알리거나 이해관계자로부터 의견을 구할 수 있다.

5.7. 신용평가 관련 주요 정책의 공시

회사는 신용평가 업무 수행과 관련한 행동 규범, 신용등급 및 부도의 정의, 신용평가 수수료 체계 등 신용평가와 관련한 주요 정책에 대하여 공시하여야 한다.

5.8. 구조화금융상품의 공시

① 회사는 구조화금융상품에 대한 신용평가의 평가방법론과 주요 평가 가정에 대해 공시해야 한다.
② 회사는 기초자산의 정보에 대한 검증 여부, 평가등급 모니터링의 빈도를 공시해야 한다.
③ 회사는 구조화금융상품의 신용등급 결정에 주요한 역할을 하는 기초자산에 관한 정보를 공시해야 한다. 다만, 다른 법령에 의하여 공시된 경우에는 그러하지 아니하다.

제6장 영업행위 준칙

6.1. 영업의 원칙

회사와 그 임직원은 고객을 보호하고 공정한 거래질서를 유지하기 위하여 다음 각 호의 영업상 원칙을 준수하여야 한다.
1. 선량한 관리자로서의 주의의무를 다한다.
2. 신용평가대상 등 고객의 인적사항 및 기타 정보 등을 부당하게 이용하거나 유출하지 아니한다.
3. 고객에 대한 허위정보의 제공 및 문서 위·변조, 사기 또는 기망 등 위법·부당행위를 하지 아니한다.

6.2. 신용평가수수료 부과기준 등의 공시

① 회사는 수수료 부과 기준 및 절차에 관한 사항을 정하고 이를 인터넷 홈페이지 등을 통하여 공시하여야 한다.
② 회사는 수수료 부과기준을 적용함에 있어 의뢰인 또는 거래상대방을 정당한 사유없이 차별하여서는 아니 된다.

6.3. 편익 등의 수수 제한

① 임직원은 직무와 관련하여 의뢰인, 거래상대방 등으로 부터 금전·물품·편익 등의 재

산상 이익을 제공받아서는 아니 된다.

② 회사와 그 임직원은 일반인이 통상적으로 이해할 수 있는 수준내에서 회사가 정한 절차에 의하지 아니하고는 의뢰인, 거래상대방에게 금전·물품·편익 등의 재산상 이익을 제공하여서는 아니 된다.

③ 다음 각 호의 어느 하나에 해당하는 물품 등은 재산상 이익으로 보지 아니한다.

1. 회사가 자체적으로 작성한 조사분석자료
2. 경제적 가치가 5만원 이하인 경품류 또는 식사
3. 애·경사 등과 관련한 20만원 이하의 경조비 및 조화·화환

제7장 불공정행위 금지

회사와 그 임직원은 다음 각 호의 어느 하나의 행위를 하여서는 아니된다.

1. 특정 신용등급의 부여를 조건으로 의뢰인에게 자사 및 계열사의 서비스나 상품을 이용하도록 강요하거나 권유하는 행위
2. 회사가 제공하는 서비스 상품의 이용여부에 따라 신용등급을 조정 또는 조정예정을 위협하거나, 등급부여를 거부하는 행위
3. 신용평가 수행과정에서 업무상 취득한 정보를 이용하여 부당한 이익을 얻거나, 타인이 부당한 이익을 얻도록 하는 행위
4. 구조화금융상품(ABS, ABCP, MBS 등)을 구성하는 기초자산의 전체 또는 일부에 대하여 회사가 제공하는 평가를 받지 않는 경우, 구조화금융상품 거래의 일환으로 발행된 금융상품 등에 대해 낮은 신용등급을 부여 또는 부여예정을 위협하거나, 기존의 신용등급을 하락 또는 하락예정을 위협, 신용평가를 거부하거나 신용등급을 철회하는 행위

제8장 신용평가자료 및 기밀정보의 관리

8.1. 평가 자료의 보관 및 유지

① 회사는 평가자료(신용평가업무 및 그에 딸린 업무 관련 자료를 말한다. 이하 이 장에서 같다) 보관에 관한 내부정책과 관련 법규 등에 의거하여 기업내부정보 등의 수집·처리 및 이용 등에 관한 내부관리지침을 마련해야 한다.

② 8.2.에서 언급된 기록은 신용등급 소멸일 부터 최소 3년 동안 회사의 건물내에 보관해야 하고, 평가대상으로부터 입수한 자료 중 기밀자료에 대해서는 대외비로 하며, 평가자료의 보관 및 관리에 대해서는 정기적으로 사후감독이 이루어져야 한다.

③ 회사는 신용평가업 영위와 관련된 자료를 그 종류별로 관련법규 및 회사 내부적으로 정하는 최소보존 기간(계약서 등 권리·의무 및 중요한 사실관계에 관한 자료의 경우에는 당해 권리·의무 및 사실관계의 종료일부터 기산) 동안 서면, 전산자료, 마이크로필름 등의 형태로 기록·유지하여야 한다.

④ 평가계약에 의해 회사, 평가대상, 관련 제3자의 권리와 의무로 규정된 기록은 적어도 그 권리와 의무가 소멸된 이후 적어도 3년 동안 보관해 두어야 한다.

8.2. 신용평가 자료의 범위

신용평가자료는 신용평가대상 또는 그의 대리인으로부터 제출받은 신용평가 관련자료, 평가담당자가 신용평가업무 수행과정에서 수집 및 작성한 자료 등을 의미하며, 그 범위는 다음 각 호와 같다.

1. 제출받은 신용평가 관련 자료
   가) 3개년 감사보고서
   나) 피평가업체의 사업실적 및 재무상태를 파악할 수 있는 자료
   다) 기타 신용등급결정에 필요한 자료 등
2. 신용평가업무 수행과정 관련 자료
   가) 신용평가(분석)보고서, 보고서 의견의 기반을 형성하는데 사용된 내부 기록
   나) 경제 및 산업 동향 분석 자료
   다) 신용평가대상의 사업 및 재무역량 관련 분석자료
   라) 신용등급결정에 대한 내부회의록(평가위원회 회의록)
   마) 각 신용등급을 결정하거나 신용등급결정에 참여한 애널리스트 등의 명단, 신용평가가 의뢰된 것인지 아닌지의 여부에 관한 정보와 신용평가가 이루어진 날짜
   바) 신용평가대상 또는 관련 제3자 또는 신용평가 이용자로부터 받은 수수료와 관련한 기록
   사) 회사가 신용등급을 결정하는데 사용한 절차와 방법론의 서류화된 기록

8.3. 기밀정보관리의 절차 및 정책

① 회사는 기밀정보에 대해서는 일반적인 신용평가 관련 자료와 별도의 관리체계를 수립하여 관리한다.

② 회사와 그 임직원은 신용평가대상 또는 그의 대리인으로부터 받은 기밀정보를 보호하여야 한다.

③ 신용평가대상으로부터 기밀정보의 활용에 대해 허락을 받은 경우를 제외하고는 언론보도, 연구조사모임, 투자자 혹은 다른 신용평가대상과의 대화를 통해 기밀정보가 유출되지 않도록 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 기밀정보를 명시적으로 공개하지 않는 한도 내에서 기밀정보를 반영한 신용등급 또는 평가의견을 공표하는 행위
2. 관련 법규 또는 정부기관의 적법한 요청에 의해 기밀정보를 공개하는 행위

④ 회사는 제3자 혹은 대리인에게 일부 업무를 위임하는 경우에도 기밀정보를 보호하고 유출을 방지하도록 기밀준수협약을 체결한다.

⑤ 임직원은 타인(회사의 임직원을 포함한다)에게 기밀정보를 제공하고자 하는 경우 다음 각 호의 원칙을 준수하여야 한다.

1. 기밀정보의 제공은 그 필요성이 인정되는 경우에 한하여 회사가 정하는 사전승인 절차에 따라 이루어져야 한다.
2. 제1호의 사전승인 절차에는 다음 각 목의 사항이 포함되어야 한다.
   가. 기밀정보 제공의 승인을 요청한 자 및 기밀정보를 제공받을 자의 소속 부서(외부인인 경우 소속 기관명) 및 성명
   나. 기밀정보의 제공 필요성 또는 사유
   다. 기밀정보의 제공 방법 및 절차, 제공일시 등
3. 기밀정보를 제공하는 자는 제공 과정 중 기밀정보가 권한 없는 자에게 전달되지 아니하도록 성실한 주의의무를 다하여야 한다.
4. 기밀정보를 제공받은 자는 이 기준에서 정하는 기밀유지의무를 성실히 준수하여야

하며, 제공받은 목적 이외의 목적으로 사용하거나 타인으로 하여금 사용하도록 하여서는 아니 된다.

8.4. 기밀정보의 이용

회사는 업무 수행에 관련된 목적으로만 기밀정보를 이용한다.

8.5. 기밀정보 관련 거래 금지

회사의 임직원은 신용평가대상에 관한 기밀정보를 취득한 경우 해당 신용평가대상의 증권 및 파생상품을 거래하는 것이 금지된다.

8.6. 전산자료의 관리

① 회사는 이해상충 방지 및 기밀정보 보호 등을 위해 신용평가업무와 다른 영업업무 간, 별도로 허가 또는 인가받아 겸영하는 업무가 있는 경우 동 업무와 신용평가업무 및 그에 딸린 업무와 전산상 분리하여 운영될 수 있도록 하여야 하며, 동 업무들간 정보차단벽이 설치되어야 한다.
② 회사는 전산처리의 내부통제와 전산처리되는 정보의 유출 및 파괴를 방지하고 컴퓨터 범죄를 예방하여 전산망의 안정성, 신뢰성을 확보하기 위하여 별도 지침을 만들어서 운영하여야 한다.

제9장 윤리의무

9.1 임직원의 기본윤리

① 임직원은 정직과 신뢰를 가장 중요한 가치관으로 삼고, 도덕적 윤리에 입각하여 직무를 공정하게 수행하여야 하고, 국내외의 모든 사업 및 영업활동에서 관련법규 등을 성실히 준수하며, 정당하고 윤리적인 방법을 통하여 공정한 경쟁을 도모하여야 한다.
② 임직원은 회사에서 부여받은 업무를 수행함에 있어 필요한 이 기준과 관련법규 등을 정확히 숙지하여야 한다.
③ 임직원은 다른 임직원이 이 기준 및 관련법규 등을 위반하여 업무를 처리하거나 위반 가능성을 사전에 인지한 경우 그 행위에 관여하거나 조력하여서는 아니 되며, 인지한 내용을 준법감시책임자에게 즉시 통지하여야 한다.

9.2 신용평가 및 영업활동에 있어서의 윤리

임직원은 그 업무를 수행함에 있어 항상 자본시장의 중요 인프라 기능을 담당하는 자로서의 품위를 지키고, 신의성실의 원칙과 이 기준 및 관련법규등을 준수하며, 사회의 발전을 저해하거나 회사의 목표와 투자자의 이익에 배치되는 행위를 하여서는 아니 된다.

9.3. 보고의무

① 임직원은 다음 각 호의 어느 하나에 해당하는 경우 상위 결재권자와 준법감시책임자에게 그 사실을 지체없이 보고하여야 한다.
1. 자신 또는 다른 임직원이 이 기준, 관련법규등 및 회사의 정책 등을 위반하였거나 위반한 것으로 의심되는 경우
2. 위법·부당행위와 연루되었거나 다른 임직원이 연루된 것을 인지한 경우
3. 자신 또는 다른 임직원이 체포 또는 기소되거나 유죄판결을 받은 경우

② 임직원은 업무를 수행함에 있어서 이 기준, 회사의 정책 및 관련법규등에 위배되는지의 여부가 의심스럽거나 통상적으로 수행하던 절차 및 기준과 상이한 경우 준법감시책임자의 확인을 받아야 한다.

9.4 애널리스트 등의 금융투자상품 매매

① 임직원은 금융투자상품의 매매거래와 관련하여 다음 각 호의 사항을 준수하여야 한다.
1. 신용평가대상자 등 고객, 회사, 주주 및 관련 제3자와의 사이에서 실질적 또는 잠재적인 이해상충이 발생하지 않도록 하여야 한다.
2. 업무상 직위를 이용하여 신용평가대상자 등 고객, 회사 또는 관련 제3자에 손실을 끼치는 행위를 하여서는 아니 된다.
3. 회사 또는 신용평가대상의 미공개정보를 이용한 매매거래를 하여서는 아니 된다.
4. 금융투자상품의 매매거래를 위한 계좌는 본인의 실명으로 개설하여야 한다.

② 임직원은 자기계산으로 증권시장에 상장된 지분증권, 주식관련 채무증권, 파생상품(자본시장과금융투자업에관한법률에서 정의된 바에 따른다) 등 금융투자상품(이하 이 장에서 "지분증권등" 이라 한다)을 매매하고자 하는 경우 자기의 명의로 하여야 한다.

③ 신용평가업무 또는 그에 딸린 업무를 수행하는 임직원은 지분증권 등을 매매한 경우 다음 각 호의 사항을 준법감시책임자에게 신고하여야 한다.
1. 계좌명
2. 계좌번호
3. 계좌개설점
4. 지분증권 등 내역

④ 임직원은 준법감시책임자가 매매, 그 밖의 거래에 관한 소명을 요구하는 경우 이에 성실히 응하여야 한다.

제10장 준수여부 점검 등

10.1. 준수여부 점검

① 준법감시책임자는 임직원의 법규 위반을 사전에 방지하고 내부통제제도의 운영상 나타난 취약점을 파악하기 위하여 법규준수 여부 등을 주기적으로 점검하여야 한다.

② 준법감시책임자는 다음 각 호의 방법 등에 의하여 준수여부를 점검한다.
1. 임직원의 업무수행절차 및 법규준수 등에 대한 점검
2. 일상업무에 대한 법규준수 및 내부통제 측면에서의 사전검토

3. 준법감시수행자의 요구에 의해 작성, 제출된 신고서나 보고서 또는 점검표 등의 검토 및 확인
4. 내부제보·신고 사항에 대한 조사

10.2. 체크리스트 및 점검보고 체계의 마련

① 준법감시책임자는 내부통제기준 준수여부 점검을 효율적으로 수행하기 위해 체크리스트를 마련하고 다음 각 호의 방법에 따라 준법모니터링 프로그램을 구축운영하여야 한다.
1. 관련법규와 이 기준에서 정하는 내용을 포함하여 준법모니터링 프로그램을 구축·운영하고, 필요한 경우 지체없이 보완한다.
2. 준법모니터링 프로그램에 따라 임직원의 관련법규와 이 기준의 준수 여부를 점검하고, 그 결과를 기록·유지한다.
3. 제2호에 따른 점검결과 및 개선계획 등을 주요 내용으로 하는 내부통제보고서를 대표이사에게 정기적으로 보고하고, 특별한 사유가 발생한 경우에는 지체없이 보고한다.

② 임직원은 회사가 정하는 준법서약서를 작성하여 준법감시인에게 제출하여야 한다.

③ 회사는 효율적인 내부통제를 위하여 회사의 업무진행절차를 구체적으로 규정화하고 전산화하여야 하며, 전산시스템은 적절한 단계로 구분하여 수행되도록 설계되어야 한다.

10.3. 내부제보·신고제도의 운영

① 준법감시책임자는 내부통제가 원활하게 작동될 수 있도록 다양한 경로의 내부제보·신고제도를 운영할 수 있다.

② 내부제보·신고제도는 임직원의 접근이 용이하도록 운영되어야 한다.

③ 준법감시책임자는 내부제보·신고자의 인적사항을 공개 또는 누설하여서는 아니되며, 내부제보·신고자는 인사상, 기타 불이익을 받지 아니한다.

④ 임직원은 타인에 대한 비방, 중상을 목적으로 내부제보·신고제도를 악용하여서는 아니된다.

⑤ 준법감시책임자는 내부제보·신고 우수자나 이 기준의 준수 우수자 등에 대한 포상을 건의할 수 있다.

10.4. 임직원 교육

준법감시책임자는 임직원의 법규준수를 지원하기 위하여 관련법규상 각종 금지사항 및 의무사항의 내용 및 규제취지 등에 대하여 필요한 교육을 정기 또는 수시로 실시한다.

10.5. 위반시 처리사항

① 준법감시책임자는 임직원의 중대한 위법 행위나 이 기준 위반행위를 발견한 경우에는 대표이사에게 보고하여야 한다.

② 준법감시책임자는 제1항의 규정에 의한 보고시 제재의견을 첨부할 수 있다.

③ 준법감시책임자는 법규 위반사항이 재발하지 아니 하도록 내부통제의 취약부분을 점검·개선하는 등 신속하고 효과적인 조치를 취하여야 한다.

④ 내부통제기준을 위반한 임직원에 대한 처리에 관하여는 상벌규정 등 회사의 내규에 서 정하는 바에 따른다.

<별지 제1호 서식>

신용정보관리·보호인의 업무수행 실적 등 보고

문서번호:
수　　신: 금융감독원장
참　　조: 00검사국장

「신용정보업감독규정」 제22조의2제3항에 따라 신용정보관리·보호인의 업무수행실적 및 대표이사, 이사회에 대한 보고실적을 아래와 같이 보고합니다.

상호		대표자	
본점 소재지		신용정보관리·보호인	

1. 법 제20조제4항 각호의 업무수행 실적

구분	이행일(기간)	주요 내용
신용정보 관리 및 보호 계획의 수립 및 시행		
신용정보 관리 및 보호실태와 관행에 대한 정기적인 조사 및 개선		
신용정보주체의 권리행사 및 피해구제		
내부통제 시스템의 구축 및 운영		
신용정보 보호 교육 계획의 수립 및 시행		
신용정보 보호 관련 법령 및 규정 준수여부 점검		

2. 법 제20조제5항에 따른 보고 실적

보고 주기	

보고 내역

구분	보고일	주요 보고사항 및 후속조치 등
대표이사		
이사회		

※ 첨부서류

1. 대표이사 및 이사회에 보고한 보고서
2. 업무수행 실적에 관한 증빙서류(첨부서류 1.과 중복되는 경우 생략 가능)

0000년 00월 00일

신용정보관리·보호인 _____ 서명 또는 (인)

<별지 제2호 서식>

<table>
<tr><td colspan="4">폐업에 따른 보유정보 처리 결과 보고서</td><td>처리기간
15일</td></tr>
<tr><td rowspan="4">제출자</td><td>성명(대표자)</td><td></td><td>신용정보업
허가일자</td><td>0000년 00월 00일</td></tr>
<tr><td>상호 또는 명칭</td><td></td><td>허가번호</td><td></td></tr>
<tr><td rowspan="2">본점 및 지점
소재지</td><td rowspan="2"></td><td>폐업일자</td><td></td></tr>
<tr><td>폐업사유</td><td></td></tr>
<tr><td>처리
내용</td><td colspan="4">1. 대상자료
□ 신용정보 자료철 및 신용정보 관리대장
□ 신용정보 데이터베이스
□ 그밖에 신용정보가 수록·보관된 파일등

2. 처리일자 : 0000년 00월 00일 ~ 0000년 00월 00일

3. 처리방법 :

4. 처리결과 :

※ 입회인(소속, 직위, 성명) :</td></tr>
<tr><td colspan="5">「신용정보업감독규정」 제23조에 따른 보유정보 처리결과를 위와 같이 보고합니다.

0000년 00월 00일
제출자 _____서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※ 구비서류
처리결과를 확인할 수 있는 서류</td><td>수수료
없음</td></tr>
</table>

<별지 제3호의2 서식>

모집업무수탁자의 모집경로 확인 등 보고

문서번호:

수 신: 금융감독원장

참 조: 00검사국장

「신용정보의 이용 및 보호에 관한 법률 시행령」제35조의2제6항에 따라 모집업무수탁자의 모집경로 등을 확인한 사항을 아래와 같이 보고합니다.

상호		대표자	
본점 소재지		신용정보관리·보호인	

모집경로 등 확인 사항(법 제41조의2제1항 각호에 따른 확인 사항)

구분	확인일 (대상기간)	주요 내용
불법취득신용정보를 모집업무에 이용하였는지 여부		
모집업무에 이용한 개인신용정보 등을 취득한 경로		
모집업무에 이용한 개인신용정보를 안전하게 보관하고 있는지 여부		
모집업무에 이용한 개인신용정보를 이용목적 달성, 이용기간 종료 등에 따라 적절히 파기하였는지 여부		
개인신용정보를 위탁한 업무 목적 외에 이용하였거나 제3자에게 제공하였는지 여부		

※ 첨부서류

1. 모집경로 등 확인의무 이행에 관한 증빙서류
2. 불법취득신용정보를 모집업무에 이용한 경우 그 사실을 확인할 수 있는 증빙서류
3. 모집업무에 이용한 개인신용정보를 적절히 보관, 파기하지 않은 경우 그 사실을 확인할 수 있는 증빙서류
4. 개인신용정보를 위탁한 업무 목적 외에 이용하였거나 제3자에게 제공한 경우 그 사실을 확인할 수 있는 증빙서류

0000년 00월 00일

0000 대표이사 ____ 서명 또는 (인)

<별지 제3호의3 서식>

신용정보제공·이용자의 확인 등 보고사항 보고

문서번호:
수 신: 금융감독원장
참 조: 00검사국장

「신용정보의 이용 및 보호에 관한 법률 시행령」 제35조의2제7항에 따라 신용정보제공·이용자가 알린 사항을 아래와 같이 보고합니다.

보고자	상호		대표자	
	본점 소재지		신용정보관리·보호인	

영 제35조의2제5항에 따른 보고의 접수 내역		
신용정보제공·이용자의 상호	보고일	주요 내용

※ 첨부서류
1. 신용정보제공·이용자가 등록기관에 보고한 서류의 사본

0000년 00월 00일
보고자 _____ 서명 또는 (인)

<별지 제4호 서식>

<table>
<tr><td colspan="5">불일치 사유보고서</td></tr>
<tr><td rowspan="3">보고자</td><td>상호</td><td></td><td>신용정보업
허가일자</td><td>0000년 00월 00일</td></tr>
<tr><td>대표자</td><td></td><td>허가번호</td><td></td></tr>
<tr><td>본점 소재지</td><td colspan="3"></td></tr>
<tr><td>보고
내용</td><td colspan="4">1. 재무제표와 업무보고서 불일치 내용

2. 불일치 사유</td></tr>
<tr><td colspan="5">「신용정보업감독규정」 제46조에 따라 위와 같이 보고합니다.

0000년 00월 00일
보고자 _____서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※ 구비서류
보고내용을 확인할 수 있는 서류</td><td>수수료
없음</td></tr>
</table>

<별지 제5호 서식> 업무보고서의 자세한 내용은 상단 메뉴 첨부파일을 이용하십시오.

신용정보업감독업무시행세칙

[시행 2016.7.28] [세칙 제9999호, 2016.7.27, 일부개정]

제1조(목적) 이 세칙은 「신용정보의 이용 및 보호에 관한 법률」(이하 "법"이라 한다) 및 동법 시행령(이하 "영"이라 한다), 동법 시행규칙(이하 "규칙"이라 한다), 신용정보업감독규정(이하 "규정"이라 한다)에서 정하는 금융감독원장(이하 "감독원장"이라 한다) 소관사항의 시행에 필요한 사항을 정함을 목적으로 한다.

제1조의2(연차보고서) 규정 제22조의2제3항에 따라 감독원장이 정하는 서식은 <별지 제1호 서식>과 같다.

제2조(폐업시 보유정보의 처리) 신용정보회사 또는 신용정보집중기관이 규정 제23조에 따라 자료를 처분, 소거 또는 폐기한 경우에는 그 결과를 <별지 제2호 서식>에 따라 감독원장에게 제출하여야 한다.

제3조 삭제 <2015.11.25.>

제4조 삭제 <2015.11.25.>

제5조 삭제 <2015.11.25.>

제5조의2(모집업무수탁자의 모집경로 확인 등 보고) ① 규정 제43조의6에 따른 신용정보제공·이용자의 보고 서식은 <별지 제3호의2 서식>과 같다.
② 규정 제43조의6에 따른 등록기관의 보고 서식은 <별지 제3호의3 서식>과 같다.

제6조(회계처리 불일치 보고서) 규정 제46조제3항에 따른 불일치의 내용과 사유는 <별지 제4호 서식>에 따라 보고하여야 한다.

제7조(업무보고서)① 신용정보회사 및 신용정보집중기관은 법 제47조에 따른 업무보고서를 <별지 제5호 서식>에 따라 매분기 종료일 다음 달 말일까지 감독원장에게 제출하여야 한다.
② 제1항의 업무보고서 제출은 정보통신망(「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」에 따른 정보통신망을 말한다)을 이용한 전자문서의 방법으로 할 수 있다.
③ 업무보고서는 회계연도말은 결산 결과, 매분기말은 가결산 결과를 반영하여 작성한다.

부칙 <제9999호,2008.5.6>

이 세칙은 2008년 5월 9일부터 시행한다.

부칙 <제9999호,2009.9.30>

제1조(시행일) 이 세칙은 2009년 10월 2일부터 시행한다. 다만, <별표>의 신용평가회사의 표준내부통제기준은 2010년 1월 2일부터 시행한다.

제2조(적용례) <별지 제5호 서식>의 개정 내용은 2009년 12월 31일 기준 업무보고서부터 적용한다.

부칙 <제9999호,2011.9.30>

이 세칙은 2011년 9월 30일부터 시행한다.

부칙 <제9999호,2013.1.29>

이 세칙은 2013년 1월 29일부터 시행한다.

부칙 <제9999호,2015.11.25>

이 세칙은 2015년 11월 25일부터 시행한다.

부칙 <제9999호,2016.7.27>

제1조(시행일) 이 세칙은 2016년 7월 28일부터 시행한다.

제2조(적용례) <별지 제5호 서식> 업무보고서는 2016년 6월말 기준 업무보고서부터 적용한다.

<별표>

신용평가회사 표준내부통제기준

목 차

제1장 총칙 1

1.1 목적 1
1.2 적용 범위 1
1.3 용어의 정의 1
1.4 업무분장 및 조직 구성 2

제2장 내부통제 조직 및 운영 2

2.1. 준법감시체제 2
2.2. 준법감시책임자 2
2.2.1 선임 및 해임 2
2.2.2 권한 및 의무 3
2.2.3 준법감시부서의 설치 3
2.2.4 준법감시업무의 독립성 3
2.3. 내부통제기준의 제·개정 등 4
2.4. 감사 기준 4

제3장 신용평가업무 행위 준칙 4

3.1 신용평가의 공정성 4
3.1.1 신용평가의 원칙 4
3.1.2 구조화금융상품에 대한 신용평가 5
3.2 신용등급평가위원회 5
3.3 신용평가의 적정성 5
3.4 신용평가의 사후관리 5

제4장 이해상충의 관리 6

4.1 일반 원칙 6
4.2 신용평가의 이해상충 방지 6
4.2.1 회사의 이해상충 방지 6
4.2.1.1 절차와 정책 6
4.2.1.2 평가조직과 영업조직의 분리 6
4.2.1.3 이직자에 대한 신용평가 재검토 6
4.2.1.4 순환보직체계 마련 7
4.3 신용평가 금지 7
4.3.1. 이해상충 관계에 있는 관계회사 등에 대한 신용평가 금지 7
4.3.2. 이해상충 관계에 있는 내부직원의 신용평가 금지 7
4.4. 이해상충 관련 기재사항 7
4.5. 보상체계 7
4.6. 수수료 협상 8
4.7. 신용평가업무 참여 금지 8

제5장 신용평가결과 등의 제공 및 공시 ····· 8

5.1. 신용평가서의 제공 ····· 8
5.2. 공시의 의의 ····· 8
5.3. 공시의 원칙 ····· 9
5.4. 신용평가 결과의 공시 ····· 9
5.5. 신용평가 실적의 공시 ····· 9
5.6. 신용평가 방법론의 공시 ····· 9
5.7. 신용평가 관련 주요 정책의 공시 ····· 9
5.8. 구조화금융상품의 공시 ····· 10

제6장 일반 영업행위 준칙 ····· 10
6.1. 영업의 일반 원칙 ····· 10
6.2. 수수료 부과기준 등의 공시 ····· 10
6.3. 편익 등의 수령 제한 ····· 10

제7장 불공정행위 금지 ····· 11

제8장 신용평가자료 및 기밀정보의 관리 ····· 11

8.1. 신용평가 자료의 보관 및 유지 ····· 11
8.2. 신용평가 자료의 범위 ····· 11
8.3. 기밀정보관리의 절차 및 정책 ····· 12
8.4. 기밀정보의 이용 ····· 13
8.5. 기밀정보 관련 거래 금지 ····· 13
8.6. 전산자료의 관리 ····· 13

제9장 윤리의무 ····· 13

9.1 기본윤리 ····· 13
9.2 신용평가 및 영업활동에 있어서의 윤리 ····· 13
9.3. 보고의무 ····· 14
9.4 임직원의 금융투자상품 매매 ····· 14

제10장 준수여부 점검 등 ····· 15

10.1 준수여부의 점검 ····· 15
10.2.체크리스트 및 점검보고 체계의 마련 ····· 15
10.3.내부제보·신고제도의 운영 ····· 15
10.4.임직원 교육 ····· 16
10.5.위반시 처리사항 ····· 16

제1장 총칙

1.1 목적

이 표준내부통제기준(이하 〃기준〃이라 한다)은 "신용정보의 이용 및 보호에 관한 법률" (이하 "법" 이라 한다) 제29조에 따라 신용평가회사(이하 〃회사〃라 한다)와 그 임직원(계약직 및 임시직 등을 포함한다. 이하 이 기준에서 같다)이 회사의 업무를 수행함에 있어 준수하여야 할 절차 및 기준에 관한 사항을 정함으로써 신용평가의 공정성, 투명성 및 신뢰성을 확보하고 회사의 경영 건전성을 제고하며 고객 및 투자자 보호에 기여함을 목적으로 한다.

1.2 적용 범위

1. 이 기준은 회사와 그 임직원의 업무에 적용하며, 계약에 의하여 회사 업무의 일부를 위탁받은 자의 행위는 그 위임받은 범위내에서 이를 회사의 행위로 본다.
2. 회사와 그 임직원의 행위에 관하여 법, 시행령, 시행규칙 및 법에 의한 규정(감독업무시행세칙을 포함한다. 이하 〃관련법규〃라 한다)에서 정하는 사항 이외에는 이 기준에서 정하는 바에 따른다.
3. 회사는 각 회사의 특성과 사정을 고려하여 내부통제기준을 마련하되 이 기준의 내용에 부합하여야 하며, 이 기준과 상충되는 경우에는 이 기준을 우선하여 적용한다.
4. 회사의 내부통제에 관하여 이 기준에서 정하지 아니한 사항과 이 기준의 세부사항은 회사의 내규에 의하거나 별도의 세칙이나 지침에 위임할 수 있다.

1.3 용어정의

이 기준에서 사용하는 용어의 정의는 다음과 같다. 다만, 이 기준에서 정하지 아니한 용어는 관련법규에서 정하는 바에 따른다.

1. "신용등급"이라 함은 원리금상환가능성 또는 신용도에 대한 현재 의견을 표현한 기호체계를 말한다.
2. "신용등급평가위원회"라 함은 신용등급을 결정하기 위하여 회사의 내규에 의거하여 구성한 회의체를 말한다.
3. "신용평가대상"이라 함은 법 제2조 제12호에 따라 회사가 평가하는 금융상품, 신용공여 및 기업, 법인, 간접투자기구 등과 발행인 기타 신용평가를 의뢰하는 자를 말한다.
4. "기밀정보"라 함은 신용평가과정에서 신용평가대상 또는 그 대리인이 회사에 제공한 정보 중에서 소유권 및 기밀성에 대하여 문서상으로 명시한 정보를 말한다. 다만, 다음 각 목의 어느 하나에 해당하는 정보는 제외한다.

가. 이미 알려졌거나 공시된 정보
나. 신용평가대상 또는 그의 대리인이 공개하기 전에 기밀유지 조건 없이 신용평가회사에 제공한 정보
다. 신용평가대상에 대한 기밀유지 의무에 저촉되지 않는 것으로서 제3자로부터 제공된 정보 또는 해당 정보를 제공하는 것이 금지되지 않는 것으로서 제3자로부터 기밀유지 조건 없이 회사가 제공받은 정보
라. 회사가 기밀정보를 참조하지 않고 독자적으로 개발한 정보

5. "준법감시책임자"라 함은 회사와 그 임직원이 내부통제기준에서 정하는 정책과 절차

를 준수하도록 관리·감독하는 자를 말한다.
6. "애널리스트"라 함은 신용평가분석을 직접적으로 수행하는 직원(업종별 책임자를 포함한다)을 말한다.

1.4. 업무분장 및 조직 구성

① 회사는 영업의 종류, 업무의 성격, 이해상충의 정도 등을 감안하여 조직을 구성하여야 한다.
② 회사는 신용평가조직과 영업조직을 분리하여 조직을 구성하여야 하며, 이들 조직간 정보 및 인사의 교류를 제한하여야 한다.
③ 회사는 별도로 허가 또는 인가받아 겸영하는 업무가 있는 경우 법 제4조에 의한 신용평가업무 및 그에 딸린 업무와도 분리하여 조직을 구성하여야 한다.
④ 회사는 제1항 내지 제3항에 의한 조직이 효율적으로 기능할 수 있도록 조직구성과 업무분장에 관한 별도의 세부기준을 제정·운영할 수 있다.

제2장 내부통제 조직 및 운영

2.1 준법감시체제

① 회사는 임직원이 신용평가, 기타 업무를 수행함에 있어서 이해상충방지, 공정성 제고 및 위법·부당행위의 사전 예방에 필요한 효율적인 준법감시체제를 구축·운영하여야 한다.
② 제1항에 의한 준법감시체제는 다음 각 호의 사항을 수행할 수 있어야 한다.
1. 관련법규 등의 준수 프로그램의 입안·관리
2. 임직원의 관련법규 등의 준수 실태 모니터링
3. 임직원에 대한 준법관련 교육·자문
4. 금융위원회, 금융감독원(이하 "감독당국"이라 한다)과의 협조
5. 기타 제1호 내지 제4호에 부수되는 업무

2.2 준법감시책임자

2.2.1 선임 및 해임

① 준법감시책임자는 대표이사가 지정한다.
② 회사는 준법감시책임자가 독립적으로 직무를 수행할 수 있도록 하고, 적정 임기를 보장하여야 한다.
③ 최근 5년간 관련법규 또는 금융관련 법령을 위반하여 감독당국으로부터 법 제45조제7항에 따른 문책경고 또는 견책요구 이상에 해당하는 조치를 받은 자는 준법감시책임자가 될 수 없으며, 준법감시책임자로 임명된 이후 이에 해당하게 된 때에는 그 직을 상실한다.
④ 회사는 준법감시책임자를 임면하는 경우 그 사실을 금융감독원에 보고하여야 한다.

2.2.2 권한 및 의무

① 준법감시책임자는 다음 각 호의 사항에 대한 권한 및 의무를 가진다.
1. 업무전반에 대한 접근 및 회사에 대한 각종 자료제출 요구
2. 임직원의 위법·부당행위에 관하여 대표이사 및 감사에 대한 보고 및 시정요구
3. 내부통제기준 준수여부에 대한 정기 또는 수시 점검
4. 준법감시 강화를 위한 임직원 교육
5. 신용평가의 공정성, 신뢰성의 확보를 위한 업무전반에 대한 상시 감시·감독시스템의 구축·운영
6. 신용평가과정에서 이해상충을 관리하고 신용평가과정의 공정성을 위태롭게 할 수 있는 리스크 점검
7. 신용평가과정에서 사용하는 절차와 방법론과 관련한 내부통제 준수여부 점검
8. 신용평가, 평가방법론(평가모델을 사용하는 경우 평가모델을 포함한다. 이하 이 기준에서 같다)과 이와 관련한 불만, 이 기준 및 관련법규 등의 준수 관련한 불만, 신용평가 담당직원 및 이용자가 제기하는 신용평가관련 불만의 접수, 보관 및 처리를 위한 절차 마련
9. 이 기준에 따른 정책과 절차의 관장
10. 기타 대표이사가 필요하다고 인정하는 사항

② 준법감시책임자는 관련법규에서 정하는 바에 따라 감독당국에 제출하는 회사의 신용평가실적서와 업무보고서 등을 검토하고, 정확하고 신속한 공시를 위한 내부통제를 구축관리하며, 내부점검결과 중요사항을 발견하는 경우 감독당국에 관련 사실을 보고해야 한다.

2.2.3 준법감시부서의 설치

① 회사는 준법감시업무가 효율적으로 수행될 수 있도록 충분한 경험과 능력을 보유한 적절한 수의 인력으로 구성된 지원조직(이하 "준법감시부서" 라 한다)을 갖추어 준법감시책임자의 직무수행을 지원하여야 한다.

② 회사는 준법감시업무에 대한 자문기능 수행을 위하여 준법감시책임자, 인사담당부서장 및 전문가 등으로 구성된 준법감시위원회를 설치·운영할 수 있다.

2.2.4 준법감시업무의 독립성

① 회사는 준법감시책임자 및 준법감시부서가 자신의 직무를 공정하게 수행할 수 있도록 업무의 독립성을 보장하여야 하며, 그 직무수행과 관련된 사유로 부당한 인사상의 불이익을 주어서는 아니 된다.

② 준법감시책임자는 선량한 관리자로서의 주의 의무를 다하여 그 직무를 수행하여야 하며, 다음 각 호의 업무를 수행하는 직무를 담당하여서는 아니 된다.
1. 회사가 영위하고 있는 평가업무 및 그에 딸린 업무
2. 회사가 영위하고 있는 겸영업무
3. 평가방법론 개발 업무
4. 준법감시업무 담당 직원을 제외한 기타 임직원의 보상수준을 설정 또는 결정하는 회의의 참석

③ 준법감시책임자의 임기는 대표이사가 정하되, 2년 이상으로 한다.

④ 준법감시책임자는 관련법규와 이 기준의 준수여부를 점검하고, 위반행위에 대하여는 이를 조사하여 대표이사 및 감사에 보고하여야 한다. 다만, 경미한 사안이라고 판단되는 경우 보고대상에서 제외할 수 있다.

⑤ 기타 준법감시조직과 관련한 회사의 조직 및 업무분장에 대하여는 회사의 내규에서 정하는 바에 따른다.

2.3 내부통제기준의 제·개정 등

① 내부통제기준은 회사의 대표이사가 제정하고 필요한 경우 관련부서와 협의하여 개정할 수 있다.
② 준법감시책임자는 이 기준을 기초로 내부통제의 구체적인 지침, 컴플라이언스 매뉴얼, 임직원 윤리지침 등을 제정·시행할 수 있다.

2.4 감사 기준

회사는 감사가 수행하는 감사의 방법과 절차 등과 관련한 기준을 별도로 제정·운영하여야 한다.

제3장 신용평가업무 행위준칙

3.1. 신용평가의 공정성

3.1.1. 신용평가의 원칙

① 회사는 신용평가대상을 자산별·업종별로 구분하여 각각 평가의 기준과 방법을 기술한 평가방법론을 갖추고, 애널리스트가 해당 평가방법론에 기초하여 신용평가업무를 수행하도록 한다.
② 회사는 신용평가와 관련된 적합한 지식과 경험을 보유한 애널리스트로 평가실무팀을 구성하여 신용평가업무를 수행하도록 한다.
③ 회사는 신용평가를 위한 데이터가 부족하여 신뢰성 있는 신용평가의 수행에 심각한 의문이 제기되는 경우 신용등급 부여를 자제한다.
④ 회사는 신용평가과정에 편견이 개입되는 것을 방지하고 신용평가과정의 일관성이 유지되도록 한다.
⑤ 회사는 평가방법론을 주기적으로 점검하고 개선에 필요한 인적, 재정적 자원을 충분히 배분한다.

3.1.2. 구조화금융상품에 대한 신용평가

회사는 구조화금융상품에 대한 신용등급 부여과정이 객관적인 방식으로 이루어지도록 다음 각호의 내용을 준수하기 위한 세부 절차를 마련하여야 한다.

1. 평가방법론 및 이의 수정 내용을 정기적으로 검토하는 절차를 마련한다.
2. 구조화금융상품의 기초 자산의 리스크성격이 현저하게 변경되는 경우 신용등급을 결정하는 기존의 평가방법론이 평가에 적절한지 여부를 재평가한다.
3. 새로운 구조화금융상품의 복합적 성격이나 구조 또는 기초 자산에 대한 데이터가 부족하여 신뢰성 있는 신용평가의 수행 여부에 심각한 의문이 제기되는 경우 신용등급 부여를 자제한다.
4. 애널리스트가 구조화금융상품의 설계를 제안하거나 권고하지 않도록 한다.

3.2. 신용등급평가위원회

① 회사는 전문성과 다양한 의견을 가진 애널리스트가 참여하는 신용등급평가위원회(이하 "평가위원회"라 한다)를 구성한다.
② 회사는 평가위원회가 주주, 이사회, 기타 회사의 일반적인 의사결정기구와 독립적으로 의사결정을 하도록 보장하여야 한다.
② 평가위원회는 신용등급을 결정함에 있어 신용평가와 관련된 요소들 이외의 요소에 의해 영향을 받지 않도록 유의해야 한다. 즉, 회사, 신용평가대상, 투자자 또는 기타 시장참여자에게 미칠 수 있는 경제적, 정치적 효과를 고려하여 신용등급을 결정하여서는 아니 된다.
③ 평가위원회 참석자는 자유롭게 의견을 개진하되, 반대의견이나 논란의 여지가 있는 의견도 충분히 고려한다.

3.3. 신용평가의 적정성

① 회사는 신용등급을 공시하기 전에 신용평가대상 또는 그의 대리인에게 신용평가 결과를 알려주고, 신용평가대상 또는 그의 대리인이 추가적으로 자료를 제출할 기회를 주고, 어떤 사실에 관한 오류가 있는 경우 이를 설명할 기회를 부여한다. 이는 충분한 정보를 가지고 신용등급을 부여하기 위한 것으로 이에 대하여 신용평가대상 또는 그의 대리인의 답변이 있는 경우 이를 충분히 검토한다.
② 회사는 객관적인 자료를 근거로 신용등급을 결정하고, 신용평가보고서에 이용자를 오도할 수 있는 내용을 포함하지 않도록 한다.

3.4. 신용평가의 사후관리

회사는 신용등급이 부여된 이후에는 지속적으로 신용평가대상에 대하여 모니터링을 실시하고 정기적으로 그 결과를 발표한다.

제4장 이해상충의 관리

4.1 일반원칙

① 임직원은 업무를 수행하기 위해 이 기준과 관련법규를 숙지하여야 한다.
② 임직원은 자신의 업무를 수행함에 있어 위법·부당한 방법으로 회사나 고객을 상대로 자신의 이익 또는 보상을 추구해서는 아니 된다.
③ 회사의 사전승인을 얻어 회사 업무 이외의 대외활동을 하는 경우 자신의 이익을 위하여 업무상 취득한 정보 등을 이용하여서는 아니 된다.

4.2. 신용평가의 이해상충 방지

4.2.1. 회사의 이해상충 방지

4.2.1.1. 절차와 정책

① 회사는 이해상충 문제를 확인하고 제거·관리하는 것과 관련된 내부절차를 서면으로 제정한다.
② 회사는 신용평가 이외의 서비스에 관한 내부정책을 수립하고 이에 의거하여 이해상충 가능성이 있는 다른 사업으로부터 신용평가사업 및 애널리스트를 분리시킨다.
③ 회사는 이해상충과 관련한 제보에 대하여 심사한 후 이해상충을 완화시키는데 필요한 조치를 취한다.

4.2.1.2 평가조직과 영업조직의 분리

① 회사는 신용평가대상 또는 그의 대리인과의 수수료·계약 체결, 평가의뢰권유 등 영업업무를 수행하는 조직과 신용평가조직을 분리·구성하여 운영하여야 한다.
② 회사는 평가조직과 영업조직간 정보 및 인사의 교류를 제한해야 한다.
③ 신용평가 관련 영업을 전담하는 직원은 평가위원회 구성원으로 참여할 수 없다.

4.2.1.3 이직자에 대한 신용평가 재검토

애널리스트가 퇴직한 경우, 그 애널리스트가 관여한 신용평가대상이나 신용평가업무로써 거래했던 금융회사 등으로 이직하는 경우, 회사는 그가 이직하기 이전 2년 이상의 기간 동안 수행한 관련 신용평가업무를 점검해야 한다.

4.2.1.4 순환보직체계

회사는 애널리스트가 5년을 초과하는 기간 동안 동일한 신용평가대상을 평가하지 않도록 순환보직체계를 마련해야 하며, 동일 신용평가대상에 대한 신용평가활동에 관여하기 위해서는 최소 2년이 지나야 한다. (이 규정의 적용을 위하여 회사는 이 기준 최초 시행일로부터 2년의 유예기간을 둘 수 있다)

4.3. 신용평가 금지

4.3.1. 이해상충 관계에 있는 관계회사 등에 대한 신용평가 금지

회사는 다음 각 호의 어느 하나에 해당하는 이해관계에 있는 자에 대하여 신용평가를 할 수 없다. 다만, 제2호 및 제3호에 해당하는 자에 대해서는 신용평가서에 그 내역을 기재하여 공시하는 경우에는 그러하지 아니하다.

1. 회사는 법 제29조 제2항의 규정에 의한 출자관계에 있는 자
2. 당해 회사의 직전 사업년도 총수익의 10% 이상을 기여한 자
3. 당해 회사로부터 신용평가를 제외한 기타 용역을 제공받은 이후 1년이 경과하지 않은 자
4. 기타 관련법규에서 금지하고 있는 경우

4.3.2. 이해상충 관계에 있는 내부직원의 신용평가 금지

임직원과 다음 각 호의 어느 하나의 관계에 있는 자에 대하여 해당 임직원은 신용평가를 할 수 없다.

1. 회사의 애널리스트가 신용평가대상의 지분을 소유하고 있거나, 수수료 협의 또는 그밖의 중요한 사업관계 등을 맺고 있는 경우
2. 회사의 애널리스트가 신용평가대상 차주나 신용평가대상 증권의 발행자, 인수기관 등으로 부터 선물 또는 접대를 받은 경우(구체적인 사항에 대해서는 이 기준 6.3에서 정하는 바에 따른다)
3. 기타 관련법규에서 금지하고 있는 경우

4.4. 이해상충 관련 기재사항

① 회사는 법 제29조 제2항의 규정에 의해 대통령령이 정하는 자 이외의 자로서 당해 회사와 출자관계에 있는 자가 발행하는 금융상품 등에 대하여 신용평가를 하는 경우에는 신용평가서에 그 출자관계에 관한 사항을 기재하여야 한다.
② 회사는 신용평가서 교부시 발행자에 대한 신용평가의 적정여부를 확인할 수 있는 내용(발행자와의 지분관계, 평가일로부터 과거 1년간의 딸린 업무 및 겸영 업무 등 제공내역)을 기재한다.

4.5. 보상체계

① 회사는 실질적 또는 잠재적 이해상충문제를 제거하거나 효과적으로 관리할 수 있도록 임직원의 보수체계를 결정하여야 한다.
② 회사는 애널리스트의 보상과 성과평가를 애널리스트 자신이 평가한 신용평가대상으로부터 받는 수익과 연동되지 않도록 보상체계를 마련하여야 한다.

4.6. 수수료 협상

신용평가업무에 관여하고 있는 애널리스트와 신용등급 결정에 참여하는 자는 신용평가대상 또는 그의 대리인과 신용평가수수료에 관한 협의를 하거나 참여하지 않아야 한다.

4.7. 신용평가업무 참여 금지

① 회사의 임직원은 다음 각 호의 어느 하나에 해당하는 경우 해당 신용등급결정과정에 참여하거나 영향을 미치지 않도록 해야 한다.
1. 신용평가대상이 발행한 증권 또는 파생상품을 소유한 경우
2. 최근에 신용평가대상에 고용되었거나 기타 사업상 관계가 있는 경우
3. 친척(배우자, 부모(배우자의 부모를 포함한다), 자녀 또는 형제자매)이 현재 신용평가대상에서 근무하고 있는 경우
② 회사의 애널리스트(그의 배우자, 미성년 자녀를 포함한다)는 자신이 평가한 신용평가대상이 발행, 보증 또는 지원한 증권이나 파생상품을 매수, 매도하거나 기타 거래에 참여할 수 없다.
③ 회사의 애널리스트는 신용평가대상과 이해상충을 초래할 수 있는 개인적인 관계를 갖게 되는 경우 이를 준법감시책임자에게 알려야 한다.

제5장 신용평가결과의 제공 및 공시

5.1. 신용평가서 등의 제공

① 회사가 신용평가를 의뢰한 자에게 신용평가서를 내어주는 경우 관련법규에서 정하는 신용평가실적서(평가의견서, 신용평가실적서, 신용등급변화표, 평균누적부도율표를 포함한다) 등을 함께 제공한다.
② 회사는 신용평가서 및 신용평가실적서 등을 제공하는 경우 신용평가의 한계와 특성, 제한된 데이터의 내용 및 이용가능한 정보가 충분한지 여부를 명확히 기재해야 한다.

5.2. 공시의 의의

공시라 함은 신용평가업무와 관련된 사항을 회사 인터넷 홈페이지, 발간물, 언론, 증권유관기관 등을 통해 신용평가 정보이용자에게 전달하는 과정을 말한다.

5.3. 공시의 원칙

① 공시내용은 정확하게 공시되어야 한다.
② 공시대상의 공시내용이 확정되면 적시에 공시하여야 한다.
③ 공시업무는 정보이용자간 정보의 불균형이 발생하지 않도록 이루어져야 한다.

5.4. 신용평가 결과의 공시

① 회사는 신용등급, 신용등급과 관련된 등급감시(Rating Watch), 등급전망(Rating Outlook), 평가의견 등을 공시대상에 포함해야 한다.
② 회사는 본평가, 정기평가 및 수시평가가 이루어진 경우 그 결과를 적시에 공시해야 한다.

5.5. 신용평가 실적의 공시

① 회사는 신용평가 정보이용자가 회사의 평가능력을 파악하는데 도움을 주기 위하여 관련법규에서 정하고 있는 신용평가실적서 등을 감독당국에 제출하고 한국거래소, 금융투자협회에 비치·공시한다.
② 회사는 평가대상에 대한 등급별 분포 현황, 신용등급 변화표, 일정기간 이상의 등급별 연간 부도율, 평균누적 부도율 등의 정보를 인터넷 홈페이지 등의 방법을 통하여 공시한다.
③ 회사는 신용평가의 적합성 검증을 위하여 신용평가 결과에 대한 부도분석(Default Study) 및 채권 스프레드 관련 분석(Spread Study)을 매년 공시해야 하며 그 내용에는 성과 통계(부도율 통계), 신용등급 변동 현황, 부도기업분석, 신용등급과 시장 수익률간의 관계 분석 등에 대한 내용이 포함되어야 한다.

5.6. 신용평가 방법론의 공시

① 회사는 평가방법론 및 그와 관련된 주요 관행, 절차 및 평가 프로세스에 중대한 변경이 있는 경우 이를 인터넷 홈페이지 게시 또는 보도자료를 통해 공개한다.
② 회사는 중대한 변경내용을 신용평가에 직접 적용하기 이전에 시장에 알리거나 이해관계자로부터 의견을 구할 수 있다.

5.7. 신용평가 관련 주요 정책의 공시

회사는 신용평가 업무 수행과 관련한 행동 규범, 신용등급 및 부도의 정의, 신용평가 수수료 체계 등 신용평가와 관련한 주요 정책에 대하여 공시하여야 한다.

5.8. 구조화금융상품의 공시

① 회사는 구조화금융상품에 대한 신용평가의 평가방법론과 주요 평가 가정에 대해 공시해야 한다.
② 회사는 기초자산의 정보에 대한 검증 여부, 평가등급 모니터링의 빈도를 공시해야 한다.
③ 회사는 구조화금융상품의 신용등급 결정에 주요한 역할을 하는 기초자산에 관한 정보를 공시해야 한다. 다만, 다른 법령에 의하여 공시된 경우에는 그러하지 아니하다.

제6장 영업행위 준칙

6.1. 영업의 원칙

회사와 그 임직원은 고객을 보호하고 공정한 거래질서를 유지하기 위하여 다음 각 호의 영업상 원칙을 준수하여야 한다.

1. 선량한 관리자로서의 주의의무를 다한다.
2. 신용평가대상 등 고객의 인적사항 및 기타 정보 등을 부당하게 이용하거나 유출하지 아니한다.
3. 고객에 대한 허위정보의 제공 및 문서 위·변조, 사기 또는 기망 등 위법·부당행위를 하지 아니한다.

6.2. 신용평가수수료 부과기준 등의 공시

① 회사는 수수료 부과 기준 및 절차에 관한 사항을 정하고 이를 인터넷 홈페이지 등을 통하여 공시하여야 한다.
② 회사는 수수료 부과기준을 적용함에 있어 의뢰인 또는 거래상대방을 정당한 사유없이 차별하여서는 아니 된다.

6.3. 편익 등의 수수 제한

① 임직원은 직무와 관련하여 의뢰인, 거래상대방 등으로 부터 금전·물품·편익 등의 재

산상 이익을 제공받아서는 아니 된다.

② 회사와 그 임직원은 일반인이 통상적으로 이해할 수 있는 수준내에서 회사가 정한 절차에 의하지 아니하고는 의뢰인, 거래상대방에게 금전·물품·편익 등의 재산상 이익을 제공하여서는 아니 된다.

③ 다음 각 호의 어느 하나에 해당하는 물품 등은 재산상 이익으로 보지 아니한다.

1. 회사가 자체적으로 작성한 조사분석자료
2. 경제적 가치가 5만원 이하인 경품류 또는 식사
3. 애·경사 등과 관련한 20만원 이하의 경조비 및 조화·화환

제7장 불공정행위 금지

회사와 그 임직원은 다음 각 호의 어느 하나의 행위를 하여서는 아니된다.

1. 특정 신용등급의 부여를 조건으로 의뢰인에게 자사 및 계열사의 서비스나 상품을 이용하도록 강요하거나 권유하는 행위
2. 회사가 제공하는 서비스 상품의 이용여부에 따라 신용등급을 조정 또는 조정예정을 위협하거나, 등급부여를 거부하는 행위
3. 신용평가 수행과정에서 업무상 취득한 정보를 이용하여 부당한 이익을 얻거나, 타인이 부당한 이익을 얻도록 하는 행위
4. 구조화금융상품(ABS, ABCP, MBS 등)을 구성하는 기초자산의 전체 또는 일부에 대하여 회사가 제공하는 평가를 받지 않는 경우, 구조화금융상품 거래의 일환으로 발행된 금융상품 등에 대해 낮은 신용등급을 부여 또는 부여예정을 위협하거나, 기존의 신용등급을 하락 또는 하락예정을 위협, 신용평가를 거부하거나 신용등급을 철회하는 행위

제8장 신용평가자료 및 기밀정보의 관리

8.1. 평가 자료의 보관 및 유지

① 회사는 평가자료(신용평가업무 및 그에 딸린 업무 관련 자료를 말한다. 이하 이 장에서 같다) 보관에 관한 내부정책과 관련 법규 등에 의거하여 기업내부정보 등의 수집·처리 및 이용 등에 관한 내부관리지침을 마련해야 한다.

② 8.2.에서 언급된 기록은 신용등급 소멸일 부터 최소 3년 동안 회사의 건물내에 보관해야 하고, 평가대상으로부터 입수한 자료 중 기밀자료에 대해서는 대외비로 하며, 평가자료의 보관 및 관리에 대해서는 정기적으로 사후감독이 이루어져야 한다.

③ 회사는 신용평가업 영위와 관련된 자료를 그 종류별로 관련법규 및 회사 내부적으로 정하는 최소보존 기간(계약서 등 권리·의무 및 중요한 사실관계에 관한 자료의 경우에는 당해 권리·의무 및 사실관계의 종료일부터 기산) 동안 서면, 전산자료, 마이크로필름 등의 형태로 기록·유지하여야 한다.

④ 평가계약에 의해 회사, 평가대상, 관련 제3자의 권리와 의무로 규정된 기록은 적어도 그 권리와 의무가 소멸된 이후 적어도 3년 동안 보관해 두어야 한다.

8.2. 신용평가 자료의 범위

신용평가자료는 신용평가대상 또는 그의 대리인으로부터 제출받은 신용평가 관련자료, 평가담당자가 신용평가업무 수행과정에서 수집 및 작성한 자료 등을 의미하며, 그 범위는 다음 각 호와 같다.

1. 제출받은 신용평가 관련 자료
   가) 3개년 감사보고서
   나) 피평가업체의 사업실적 및 재무상태를 파악할 수 있는 자료
   다) 기타 신용등급결정에 필요한 자료 등
2. 신용평가업무 수행과정 관련 자료
   가) 신용평가(분석)보고서, 보고서 의견의 기반을 형성하는데 사용된 내부 기록
   나) 경제 및 산업 동향 분석 자료
   다) 신용평가대상의 사업 및 재무역량 관련 분석자료
   라) 신용등급결정에 대한 내부회의록(평가위원회 회의록)
   마) 각 신용등급을 결정하거나 신용등급결정에 참여한 애널리스트 등의 명단, 신용평가가 의뢰된 것인지 아닌지의 여부에 관한 정보와 신용평가가 이루어진 날짜
   바) 신용평가대상 또는 관련 제3자 또는 신용평가 이용자료부터 받은 수수료와 관련한 기록
   사) 회사가 신용등급을 결정하는데 사용한 절차와 방법론의 서류화된 기록

8.3. 기밀정보관리의 절차 및 정책

① 회사는 기밀정보에 대해서는 일반적인 신용평가 관련 자료와 별도의 관리체계를 수립하여 관리한다.

② 회사와 그 임직원은 신용평가대상 또는 그의 대리인으로부터 받은 기밀정보를 보호하여야 한다.

③ 신용평가대상으로부터 기밀정보의 활용에 대해 허락을 받은 경우를 제외하고는 언론보도, 연구조사모임, 투자자 혹은 다른 신용평가대상과의 대화를 통해 기밀정보가 유출되지 않도록 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 기밀정보를 명시적으로 공개하지 않는 한도 내에서 기밀정보를 반영한 신용등급 또는 평가의견을 공표하는 행위
2. 관련 법규 또는 정부기관의 적법한 요청에 의해 기밀정보를 공개하는 행위

④ 회사는 제3자 혹은 대리인에게 일부 업무를 위임하는 경우에도 기밀정보를 보호하고 유출을 방지하도록 기밀준수협약을 체결한다.

⑤ 임직원은 타인(회사의 임직원을 포함한다)에게 기밀정보를 제공하고자 하는 경우 다음 각 호의 원칙을 준수하여야 한다.

1. 기밀정보의 제공은 그 필요성이 인정되는 경우에 한하여 회사가 정하는 사전승인 절차에 따라 이루어져야 한다.
2. 제1호의 사전승인 절차에는 다음 각 목의 사항이 포함되어야 한다.
   가. 기밀정보 제공의 승인을 요청한 자 및 기밀정보를 제공받을 자의 소속 부서(외부인인 경우 소속 기관명) 및 성명
   나. 기밀정보의 제공 필요성 또는 사유
   다. 기밀정보의 제공 방법 및 절차, 제공일시 등
3. 기밀정보를 제공하는 자는 제공 과정 중 기밀정보가 권한 없는 자에게 전달되지 아니하도록 성실한 주의의무를 다하여야 한다.
4. 기밀정보를 제공받은 자는 이 기준에서 정하는 기밀유지의무를 성실히 준수하여야

하며, 제공받은 목적 이외의 목적으로 사용하거나 타인으로 하여금 사용하도록 하여서는 아니 된다.

8.4. 기밀정보의 이용

회사는 업무 수행에 관련된 목적으로만 기밀정보를 이용한다.

8.5. 기밀정보 관련 거래 금지

회사의 임직원은 신용평가대상에 관한 기밀정보를 취득한 경우 해당 신용평가대상의 증권 및 파생상품을 거래하는 것이 금지된다.

8.6. 전산자료의 관리

① 회사는 이해상충 방지 및 기밀정보 보호 등을 위해 신용평가업무와 다른 영업업무 간, 별도로 허가 또는 인가받아 겸영하는 업무가 있는 경우 동 업무와 신용평가업무 및 그에 딸린 업무와 전산상 분리하여 운영될 수 있도록 하여야 하며, 동 업무들간 정보차단벽이 설치되어야 한다.
② 회사는 전산처리의 내부통제와 전산처리되는 정보의 유출 및 파괴를 방지하고 컴퓨터 범죄를 예방하여 전산망의 안정성, 신뢰성을 확보하기 위하여 별도 지침을 만들어서 운영하여야 한다.

제9장 윤리의무

9.1 임직원의 기본윤리

① 임직원은 정직과 신뢰를 가장 중요한 가치관으로 삼고, 도덕적 윤리에 입각하여 직무를 공정하게 수행하여야 하고, 국내외의 모든 사업 및 영업활동에서 관련법규 등을 성실히 준수하며, 정당하고 윤리적인 방법을 통하여 공정한 경쟁을 도모하여야 한다.
② 임직원은 회사에서 부여받은 업무를 수행함에 있어 필요한 이 기준과 관련법규 등을 정확히 숙지하여야 한다.
③ 임직원은 다른 임직원이 이 기준 및 관련법규 등을 위반하여 업무를 처리하거나 위반 가능성을 사전에 인지한 경우 그 행위에 관여하거나 조력하여서는 아니 되며, 인지한 내용을 준법감시책임자에게 즉시 통지하여야 한다.

9.2 신용평가 및 영업활동에 있어서의 윤리

임직원은 그 업무를 수행함에 있어 항상 자본시장의 중요 인프라 기능을 담당하는 자로서의 품위를 지키고, 신의성실의 원칙과 이 기준 및 관련법규등을 준수하며, 사회의 발전을 저해하거나 회사의 목표와 투자자의 이익에 배치되는 행위를 하여서는 아니 된다.

9.3. 보고의무

① 임직원은 다음 각 호의 어느 하나에 해당하는 경우 상위 결재권자와 준법감시책임자에게 그 사실을 지체없이 보고하여야 한다.
1. 자신 또는 다른 임직원이 이 기준, 관련법규등 및 회사의 정책 등을 위반하였거나 위반한 것으로 의심되는 경우
2. 위법·부당행위와 연루되었거나 다른 임직원이 연루된 것을 인지한 경우
3. 자신 또는 다른 임직원이 체포 또는 기소되거나 유죄판결을 받은 경우

② 임직원은 업무를 수행함에 있어서 이 기준, 회사의 정책 및 관련법규등에 위배되는지의 여부가 의심스럽거나 통상적으로 수행하던 절차 및 기준과 상이한 경우 준법감시책임자의 확인을 받아야 한다.

9.4 애널리스트 등의 금융투자상품 매매

① 임직원은 금융투자상품의 매매거래와 관련하여 다음 각 호의 사항을 준수하여야 한다.
1. 신용평가대상자 등 고객, 회사, 주주 및 관련 제3자와의 사이에서 실질적 또는 잠재적인 이해상충이 발생하지 않도록 하여야 한다.
2. 업무상 직위를 이용하여 신용평가대상자 등 고객, 회사 또는 관련 제3자에 손실을 끼치는 행위를 하여서는 아니 된다.
3. 회사 또는 신용평가대상의 미공개정보를 이용한 매매거래를 하여서는 아니 된다.
4. 금융투자상품의 매매거래를 위한 계좌는 본인의 실명으로 개설하여야 한다.

② 임직원은 자기계산으로 증권시장에 상장된 지분증권, 주식관련 채무증권, 파생상품(자본시장과금융투자업에관한법률에서 정의된 바에 따른다) 등 금융투자상품(이하 이 장에서 "지분증권등" 이라 한다)을 매매하고자 하는 경우 자기의 명의로 하여야 한다.

③ 신용평가업무 또는 그에 딸린 업무를 수행하는 임직원은 지분증권 등을 매매한 경우 다음 각 호의 사항을 준법감시책임자에게 신고하여야 한다.
1. 계좌명
2. 계좌번호
3. 계좌개설점
4. 지분증권 등 내역

④ 임직원은 준법감시책임자가 매매, 그 밖의 거래에 관한 소명을 요구하는 경우 이에 성실히 응하여야 한다.

제10장 준수여부 점검 등

10.1. 준수여부 점검

① 준법감시책임자는 임직원의 법규 위반을 사전에 방지하고 내부통제제도의 운영상 나타난 취약점을 파악하기 위하여 법규준수 여부 등을 주기적으로 점검하여야 한다.

② 준법감시책임자는 다음 각 호의 방법 등에 의하여 준수여부를 점검한다.
1. 임직원의 업무수행절차 및 법규준수 등에 대한 점검
2. 일상업무에 대한 법규준수 및 내부통제 측면에서의 사전검토

3. 준법감시수행자의 요구에 의해 작성, 제출된 신고서나 보고서 또는 점검표 등의 검토 및 확인
4. 내부제보·신고 사항에 대한 조사

10.2. 체크리스트 및 점검보고 체계의 마련

① 준법감시책임자는 내부통제기준 준수여부 점검을 효율적으로 수행하기 위해 체크리스트를 마련하고 다음 각 호의 방법에 따라 준법모니터링 프로그램을 구축운영하여야 한다.
1. 관련법규와 이 기준에서 정하는 내용을 포함하여 준법모니터링 프로그램을 구축·운영하고, 필요한 경우 지체없이 보완한다.
2. 준법모니터링 프로그램에 따라 임직원의 관련법규와 이 기준의 준수 여부를 점검하고, 그 결과를 기록·유지한다.
3. 제2호에 따른 점검결과 및 개선계획 등을 주요 내용으로 하는 내부통제보고서를 대표이사에게 정기적으로 보고하고, 특별한 사유가 발생한 경우에는 지체없이 보고한다.

② 임직원은 회사가 정하는 준법서약서를 작성하여 준법감시인에게 제출하여야 한다.

③ 회사는 효율적인 내부통제를 위하여 회사의 업무진행절차를 구체적으로 규정화하고 전산화하여야 하며, 전산시스템은 적절한 단계로 구분하여 수행되도록 설계되어야 한다.

10.3. 내부제보·신고제도의 운영

① 준법감시책임자는 내부통제가 원활하게 작동될 수 있도록 다양한 경로의 내부제보·신고제도를 운영할 수 있다.

② 내부제보·신고제도는 임직원의 접근이 용이하도록 운영되어야 한다.

③ 준법감시책임자는 내부제보·신고자의 인적사항을 공개 또는 누설하여서는 아니되며, 내부제보·신고자는 인사상, 기타 불이익을 받지 아니한다.

④ 임직원은 타인에 대한 비방, 중상을 목적으로 내부제보·신고제도를 악용하여서는 아니된다.

⑤ 준법감시책임자는 내부제보·신고 우수자나 이 기준의 준수 우수자 등에 대한 포상을 건의할 수 있다.

10.4. 임직원 교육

준법감시책임자는 임직원의 법규준수를 지원하기 위하여 관련법규상 각종 금지사항 및 의무사항의 내용 및 규제취지 등에 대하여 필요한 교육을 정기 또는 수시로 실시한다.

10.5. 위반시 처리사항

① 준법감시책임자는 임직원의 중대한 위법 행위나 이 기준 위반행위를 발견한 경우에는 대표이사에게 보고하여야 한다.

② 준법감시책임자는 제1항의 규정에 의한 보고시 제재의견을 첨부할 수 있다.

③ 준법감시책임자는 법규 위반사항이 재발하지 아니 하도록 내부통제의 취약부분을 점검·개선하는 등 신속하고 효과적인 조치를 취하여야 한다.

④ 내부통제기준을 위반한 임직원에 대한 처리에 관하여는 상벌규정 등 회사의 내규에 서 정하는 바에 따른다.

<별지 제1호 서식>

신용정보관리·보호인의 업무수행 실적 등 보고

문서번호:
수　　신: 금융감독원장
참　　조: 00검사국장

「신용정보업감독규정」 제22조의2제3항에 따라 신용정보관리·보호인의 업무수행실적 및 대표이사, 이사회에 대한 보고실적을 아래와 같이 보고합니다.

상호		대표자	
본점 소재지		신용정보관리·보호인	

1. 법 제20조제4항 각호의 업무수행 실적

구분	이행일(기간)	주요 내용
신용정보 관리 및 보호 계획의 수립 및 시행		
신용정보 관리 및 보호실태와 관행에 대한 정기적인 조사 및 개선		
신용정보주체의 권리행사 및 피해구제		
내부통제 시스템의 구축 및 운영		
신용정보 보호 교육 계획의 수립 및 시행		
신용정보 보호 관련 법령 및 규정 준수여부 점검		

2. 법 제20조제5항에 따른 보고 실적

보고 주기	

보고 내역

구분	보고일	주요 보고사항 및 후속조치 등
대표이사		
이사회		

※ 첨부서류

1. 대표이사 및 이사회에 보고한 보고서
2. 업무수행 실적에 관한 증빙서류(첨부서류 1.과 중복되는 경우 생략 가능)

0000년 00월 00일

신용정보관리·보호인 _____ 서명 또는 (인)

<별지 제2호 서식>

<table>
<tr><td colspan="4">폐업에 따른 보유정보 처리 결과 보고서</td><td>처리기간
15일</td></tr>
<tr><td rowspan="4">제출자</td><td>성명(대표자)</td><td></td><td>신용정보업
허가일자</td><td>0000년 00월 00일</td></tr>
<tr><td>상호 또는 명칭</td><td></td><td>허가번호</td><td></td></tr>
<tr><td rowspan="2">본점 및 지점
소재지</td><td rowspan="2"></td><td>폐업일자</td><td></td></tr>
<tr><td>폐업사유</td><td></td></tr>
<tr><td>처리
내용</td><td colspan="4">1. 대상자료
□ 신용정보 자료철 및 신용정보 관리대장
□ 신용정보 데이터베이스
□ 그밖에 신용정보가 수록·보관된 파일등

2. 처리일자 : 0000년 00월 00일 ~ 0000년 00월 00일

3. 처리방법 :

4. 처리결과 :

※ 입회인(소속, 직위, 성명) :</td></tr>
<tr><td colspan="5">「신용정보업감독규정」 제23조에 따른 보유정보 처리결과를 위와 같이 보고합니다.

0000년 00월 00일
제출자 _____서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※ 구비서류
처리결과를 확인할 수 있는 서류</td><td>수수료
없음</td></tr>
</table>

<별지 제3호의2 서식>

모집업무수탁자의 모집경로 확인 등 보고

문서번호:

수 신: 금융감독원장

참 조: 00검사국장

「신용정보의 이용 및 보호에 관한 법률 시행령」제35조의2제6항에 따라 모집업무수탁자의 모집경로 등을 확인한 사항을 아래와 같이 보고합니다.

상호		대표자	
본점 소재지		신용정보관리·보호인	

모집경로 등 확인 사항(법 제41조의2제1항 각호에 따른 확인 사항)

구분	확인일 (대상기간)	주요 내용
불법취득신용정보를 모집업무에 이용하였는지 여부		
모집업무에 이용한 개인신용정보 등을 취득한 경로		
모집업무에 이용한 개인신용정보를 안전하게 보관하고 있는지 여부		
모집업무에 이용한 개인신용정보를 이용목적 달성, 이용기간 종료 등에 따라 적절히 파기하였는지 여부		
개인신용정보를 위탁한 업무 목적 외에 이용하였거나 제3자에게 제공하였는지 여부		

※ 첨부서류

1. 모집경로 등 확인의무 이행에 관한 증빙서류
2. 불법취득신용정보를 모집업무에 이용한 경우 그 사실을 확인할 수 있는 증빙서류
3. 모집업무에 이용한 개인신용정보를 적절히 보관, 파기하지 않은 경우 그 사실을 확인할 수 있는 증빙서류
4. 개인신용정보를 위탁한 업무 목적 외에 이용하였거나 제3자에게 제공한 경우 그 사실을 확인할 수 있는 증빙서류

0000년 00월 00일

0000 대표이사 ____ 서명 또는 (인)

<별지 제3호의3 서식>

신용정보제공·이용자의 확인 등 보고사항 보고

문서번호:
수 신: 금융감독원장
참 조: 00검사국장

「신용정보의 이용 및 보호에 관한 법률 시행령」 제35조의2제7항에 따라 신용정보제공·이용자가 알린 사항을 아래와 같이 보고합니다.

보고자	상호		대표자	
	본점 소재지		신용정보관리·보호인	

영 제35조의2제5항에 따른 보고의 접수 내역		
신용정보제공·이용자의 상호	보고일	주요 내용

※ 첨부서류
1. 신용정보제공·이용자가 등록기관에 보고한 서류의 사본

0000년 00월 00일
보고자 _____ 서명 또는 (인)

<별지 제4호 서식>

<table>
<tr><td colspan="5">불일치 사유보고서</td></tr>
<tr><td rowspan="3">보고자</td><td>상호</td><td></td><td>신용정보업
허가일자</td><td>0000년 00월 00일</td></tr>
<tr><td>대표자</td><td></td><td>허가번호</td><td></td></tr>
<tr><td>본점 소재지</td><td colspan="3"></td></tr>
<tr><td>보고
내용</td><td colspan="4">1. 재무제표와 업무보고서 불일치 내용

2. 불일치 사유</td></tr>
<tr><td colspan="5">「신용정보업감독규정」 제46조에 따라 위와 같이 보고합니다.

0000년 00월 00일
보고자 _____서명 또는 인

금융감독원장 귀하</td></tr>
<tr><td colspan="4">※ 구비서류
보고내용을 확인할 수 있는 서류</td><td>수수료
없음</td></tr>
</table>

<별지 제5호 서식> 업무보고서의 자세한 내용은 상단 메뉴 첨부파일을 이용하십시오.

신용정보의 이용 및 보호에 관한 법률

[시행 2016.9.30] [법률 제14122호, 2016.3.29, 타법개정]

제1장 총칙

제1조(목적) 이 법은 신용정보업을 건전하게 육성하고 신용정보의 효율적 이용과 체계적 관리를 도모하며 신용정보의 오용·남용으로부터 사생활의 비밀 등을 적절히 보호함으로써 건전한 신용질서의 확립에 이바지함을 목적으로 한다.

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2011.5.19, 2015.3.11>

1. "신용정보"란 금융거래 등 상거래에 있어서 거래 상대방의 신용을 판단할 때 필요한 다음 각 목의 정보로서 대통령령으로 정하는 정보를 말한다.
   가. 특정 신용정보주체를 식별할 수 있는 정보
   나. 신용정보주체의 거래내용을 판단할 수 있는 정보
   다. 신용정보주체의 신용도를 판단할 수 있는 정보
   라. 신용정보주체의 신용거래능력을 판단할 수 있는 정보
   마. 그 밖에 가목부터 라목까지와 유사한 정보
2. "개인신용정보"란 신용정보 중 개인의 신용도와 신용거래능력 등을 판단할 때 필요한 정보로서 대통령령으로 정하는 정보를 말한다.
3. "신용정보주체"란 처리된 신용정보로 식별되는 자로서 그 신용정보의 주체가 되는 자를 말한다.
4. "신용정보업"이란 제4조제1항 각 호에 따른 업무의 전부 또는 일부를 업(業)으로 하는 것을 말한다.
5. "신용정보회사"란 신용정보업을 할 목적으로 제4조에 따라 금융위원회의 허가를 받은 자를 말한다.
6. "신용정보집중기관"이란 신용정보를 집중하여 관리·활용하는 자로서 제25조제1항에 따라 금융위원회로부터 허가받은 자를 말한다.
7. "신용정보제공·이용자"란 고객과의 금융거래 등 상거래를 위하여 본인의 영업과 관련하여 얻거나 만들어 낸 신용정보를 타인에게 제공하거나 타인으로부터 신용정보를 제공받아 본인의 영업에 이용하는 자와 그 밖에 이에 준하는 자로서 대통령령으로 정하는 자를 말한다.
8. "신용조회업무"란 신용정보를 수집·처리하는 행위, 신용정보주체의 신용도·신용거래능력 등을 나타내는 신용정보를 만들어 내는 행위 및 의뢰인의 조회에 따라 신용정보를 제공하는 행위를 말한다.

9. "신용조사업무"란 타인의 의뢰를 받아 신용정보를 조사하고, 그 신용정보를 그 의뢰인에게 제공하는 행위를 말한다.
10. "채권추심업무"란 채권자의 위임을 받아 변제하기로 약정한 날까지 채무를 변제하지 아니한 자에 대한 재산조사, 변제의 촉구 또는 채무자로부터의 변제금 수령을 통하여 채권자를 대신하여 추심채권을 행사하는 행위를 말한다.
11. 채권추심의 대상이 되는 "채권"이란 「상법」에 따른 상행위로 생긴 금전채권, 판결 등에 따라 권원(權原)이 인정된 민사채권으로서 대통령령으로 정하는 채권, 특별법에 따라 설립된 조합·공제조합·금고 및 그 중앙회·연합회 등의 조합원·회원 등에 대한 대출·보증, 그 밖의 여신 및 보험 업무에 따른 금전채권 및 다른 법률에서 신용정보회사에 대한 채권추심의 위탁을 허용한 채권을 말한다.
12. 삭제 <2013.5.28>
13. "처리"란 다음 각 목의 어느 하나에 해당하는 행위를 말한다.
가. 컴퓨터를 이용하여 신용정보를 입력·저장·가공·편집·검색·삭제 또는 출력하는 행위
나. 신용정보를 배달·우송 또는 전송 등의 방법으로 타인에게 제공하는 행위
다. 그 밖에 가목 또는 나목과 비슷한 행위

제3조(신용정보업의 육성) ① 금융위원회는 신용정보회사의 신용정보 제공능력의 향상과 신용정보의 원활한 이용에 필요하다고 인정하면 신용정보업의 육성에 관한 계획을 세울 수 있다.
② 금융위원회는 제1항에 따른 계획을 원활하게 추진하기 위하여 필요하면 관계 행정기관의 장에게 협조를 요청할 수 있으며, 그 요청을 받은 관계 행정기관의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.

제3조의2(다른 법률과의 관계) ① 신용정보의 이용 및 보호에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.
② 개인정보의 보호에 관하여 이 법에 특별한 규정이 있는 경우를 제외하고는 「개인정보 보호법」에서 정하는 바에 따른다.
[본조신설 2015.3.11]

제2장 신용정보업의 허가 등

제4조(신용정보업의 종류 및 영업의 허가) ① 신용정보업의 종류 및 그 업무는 다음 각 호와 같다. 이 경우 제2호 및 제3호의 딸린 업무는 대통령령으로 정한다. <개정 2015.3.11>
1. 신용조회업: 신용조회업무 및 다음 각 목의 업무
가. 본인인증 및 신용정보주체의 식별확인업무로서 금융위원회가 승인한 업무
나. 신용평가모형 및 위험관리모형의 개발 및 판매 업무

2. 신용조사업: 신용조사업무 및 그에 딸린 업무
3. 채권추심업: 채권추심업무 및 그에 딸린 업무
4. 삭제 <2013.5.28>

② 신용정보업을 하려는 자는 제1항 각 호에 따른 업무의 종류별로 금융위원회의 허가를 받아야 한다.

③ 제2항에 따른 허가를 받으려는 자는 대통령령으로 정하는 바에 따라 금융위원회에 신청서를 제출하여야 한다.

④ 금융위원회는 제2항에 따른 허가에 조건을 붙일 수 있다.

⑤ 제2항에 따른 허가와 관련된 허가신청서의 작성 방법 등 허가신청에 관한 사항, 허가심사의 절차 및 기준에 관한 사항, 그 밖에 필요한 사항은 총리령으로 정한다.

제5조(신용정보업별 허가 대상) ① 신용조회업, 신용조사업 및 채권추심업 허가를 받을 수 있는 자는 다음 각 호의 자로 제한한다. <개정 2010.4.5, 2016.3.29>

1. 대통령령으로 정하는 금융기관 등이 100분의 50 이상을 출자한 법인
2. 「신용보증기금법」에 따른 신용보증기금
3. 「기술보증기금법」에 따른 기술보증기금
4. 「지역신용보증재단법」에 따라 설립된 신용보증재단
5. 「무역보험법」에 따라 설립된 한국무역보험공사
6. 제4조제1항제1호부터 제3호까지의 규정에 따른 업무의 전부 또는 일부를 허가받은 자가 100분의 50 이상을 출자한 법인. 다만, 출자자가 출자를 받은 법인과 같은 종류의 업무를 하는 경우는 제외한다.

② 삭제 <2013.5.28>

제6조(허가의 요건) ① 제4조제2항에 따른 신용정보업의 허가를 받으려는 자는 다음 각 호의 요건을 갖추어야 한다.

1. 신용정보업을 하기에 충분한 인력과 전산설비 등 물적 시설을 갖출 것
2. 사업계획이 타당하고 건전할 것
3. 대통령령으로 정하는 주요출자자가 충분한 출자능력, 건전한 재무상태 및 사회적 신용을 갖출 것
4. 신용정보업을 하기에 충분한 전문성을 갖출 것

② 신용정보업의 허가를 받으려는 자는 다음 각 호의 구분에 따른 자본금 또는 기본재산을 갖추어야 한다.<개정 2013.5.28>

1. 신용조회업을 하려는 경우에는 50억원 이상
2. 신용조사업 및 채권추심업을 각각 또는 함께 하려는 경우에는 50억원 이내에서 대통령령으로 정하는 금액 이상

③ 제1항에 따른 허가의 세부요건에 관하여 필요한 사항은 대통령령으로 정한다.

④ 신용정보회사는 신용정보업을 하는 동안에는 제1항제1호에 따른 요건을 계속 유지하여야 한다.

제7조(허가 등의 공고) 금융위원회는 제4조제2항에 따른 허가를 하거나 제14조제1항에 따라 허가 또는 인가를 취소한 경우에는 지체 없이 그 내용을 관보에 공고하고 인터넷 홈페이지 등을 이용하여 일반인에게 알려야 한다.

제8조(신고 및 보고 사항) 신용정보회사가 제4조제2항에 따라 허가받은 사항 중 대통령령으로 정하는 사항을 변경하려면 미리 금융위원회에 신고하여야 한다. 다만, 대통령령으로 정하는 경미한 사항을 변경하려면 그 사유가 발생한 날부터 7일 이내에 그 사실을 금융위원회에 보고하여야 한다.

제9조(지배주주의 변경승인 등) ① 신용정보회사의 주식(출자지분을 포함한다. 이하 이 조에서 같다)을 취득하여 대통령령으로 정하는 지배주주가 되려는 자는 제6조제1항제3호에 따른 주요출자자 요건 중 건전한 경영을 위하여 대통령령으로 정하는 요건을 갖추어 미리 금융위원회의 승인을 받아야 한다.
② 금융위원회는 6개월 이내의 기간을 정하여 제1항에 따른 승인 없이 취득한 주식을 처분할 것을 명할 수 있다.
③ 제1항에 따른 승인 없이 주식을 취득한 자는 그 취득분에 대하여 의결권을 행사할 수 없다.
④ 제1항에 따른 승인 및 제2항에 따른 처분명령의 세부요건에 관하여 필요한 사항은 대통령령으로 정한다.

제10조(신용정보업의 양도·양수 등의 인가 등) ① 신용정보회사가 그 사업의 전부 또는 일부를 양도·양수 또는 분할하거나, 다른 법인과 합병(「상법」 제530조의2에 따른 분할합병을 포함한다. 이하 같다)하려는 경우에는 대통령령으로 정하는 바에 따라 금융위원회의 인가를 받아야 한다.
② 신용정보회사가 제1항에 따라 인가를 받아 그 사업을 양도 또는 분할하거나 다른 법인과 합병한 경우에는 양수인, 분할 후 설립되는 법인 또는 합병 후 존속하는 법인(신용정보회사인 법인이 신용정보회사가 아닌 법인을 흡수합병하는 경우는 제외한다)이나 합병에 따라 설립되는 법인은 양도인, 분할 전의 법인 또는 합병 전의 법인의 신용정보회사로서의 지위를 승계한다. 이 경우 종전의 신용정보회사에 대한 허가는 그 효력(제1항에 따른 일부 양도 또는 분할의 경우에는 그 양도 또는 분할한 사업의 범위로 제한한다)을 잃는다.
③ 제1항 및 제2항에 따른 양수인, 합병 후 존속하는 법인 및 분할 또는 합병에 따라 설립되는 법인에 대하여는 제5조, 제6조, 제22조제1항 및 제27조제1항부터 제7항까지의 규정을 준용한다.<개정 2013.5.28>
④ 신용정보회사가 영업의 전부 또는 일부를 일시적으로 중단하거나 폐업하려면 총리령으로 정하는 바에 따라 미리 금융위원회에 신고하여야 한다.

제11조(겸업) ①신용정보회사는 다음 각 호의 업무 외에는 총리령으로 정하는 바에 따라 금융위원회에 미리 신고하고 허가받은 업무와 관련된 업무를 겸업할 수 있다. 이 경우 개별 법률에 따라 행정관청의 인가·허가·등록 및 승인 등의 조치가 필요한 업무는 해당 개별 법률에 따라 인가·허가·등록 및 승인 등을 미리 받아야 할 수 있다. <개정 2013.5.28, 2015.3.11>

1. 개인에 대하여 타인의 신용정보 및 신용정보를 가공(加工)한 신용정보를 제공하는 업무
2. 다른 회사 채권에 대한 부채증명서 발급 대행 업무(대통령령으로 정하는 경우를 제외한다)
3. 부실채권 매입, 채권추심 등 타인의 권리실행을 위한 소송사건 등의 대리업무 등 신용정보회사의 업무 범위를 벗어난 업무
4. 그 밖에 신용정보주체 또는 사회에 명백하게 해악을 끼칠 수 있는 업무로서 대통령령으로 정하는 업무

② 제1항에도 불구하고 신용조회회사는 영리를 목적으로 신용정보업 외의 다른 업무를 겸업하여서는 아니 된다. 다만, 국가·지방자치단체 및 대통령령으로 정하는 공공단체의 의뢰에 따른 공공 목적의 조사·분석 등의 업무로서 금융위원회가 승인하는 경우에는 그러하지 아니하다.<신설 2015.3.11>

제12조(유사명칭의 사용 금지) 이 법에 따라 허가받은 신용정보회사가 아닌 자는 상호 중에 신용정보·신용조사 또는 이와 비슷한 명칭을 사용하지 못한다. <개정 2013.5.28>

제13조(임원의 겸직 금지) 신용정보회사의 상임 임원은 금융위원회의 승인 없이 다른 영리법인의 상무(常務)에 종사할 수 없다.

제14조(허가 등의 취소와 업무의 정지) ① 금융위원회는 신용정보회사가 다음 각 호의 어느 하나에 해당하는 경우에는 허가 또는 인가를 취소할 수 있다. 다만, 금융위원회는 신용정보회사가 다음 각 호의 어느 하나에 해당하더라도 대통령령으로 정하는 사유에 해당하면 6개월 이내의 기간을 정하여 허가 또는 인가를 취소하기 전에 시정명령을 할 수 있다. <개정 2013.5.28, 2015.3.11>

1. 거짓이나 그 밖의 부정한 방법으로 제4조제2항에 따른 허가를 받거나 제10조제1항에 따른 인가를 받은 경우
2. 제5조제1항제1호에 따른 금융기관 등의 출자요건을 위반한 경우. 다만, 신용정보회사의 주식이 「자본시장과 금융투자업에 관한 법률」 제8조의2제4항제1호에 따른 증권시장에 상장되어 있는 경우로서 제5조제1항제1호에 따른 금융기관 등이 100분의 33 이상을 출자한 경우에는 제외한다.
3. 삭제 <2013.5.28>
4. 신용정보회사[허가를 받은 날부터 3개 사업연도(신용조회업이 포함된 경우에는 5개 사업연도)가 지나지 아니한 경우는 제외한다]의 자기자본(최근 사업연도 말 현재 대차대조표상 자산총액에서 부채총액을 뺀 금액을 말한다. 이하 같다)이 제6조제2항에 따른 자본금 또는 기본재산의 요건에 미치지 못한 경우

5. 업무정지명령을 위반하거나 업무정지에 해당하는 행위를 한 자가 그 사유발생일 전 3년 이내에 업무정지처분을 받은 사실이 있는 경우
6. 제40조제1호부터 제4호까지의 어느 하나를 위반한 경우
7. 삭제 <2013.5.28>
8. 「채권의 공정한 추심에 관한 법률」 제9조 각 호의 어느 하나를 위반하여 채권추심행위를 한 경우(채권추심업만 해당한다)
9. 허가 또는 인가의 내용이나 조건을 위반한 경우
10. 정당한 사유 없이 1년 이상 계속하여 허가받은 영업을 하지 아니한 경우
11. 제41조제1항을 위반하여 채권추심행위를 한 경우(채권추심업만 해당한다)

② 금융위원회는 신용정보회사가 다음 각 호의 어느 하나에 해당하는 경우에는 6개월의 범위에서 기간을 정하여 그 업무의 전부 또는 일부의 정지를 명할 수 있다.<개정 2013.5.28, 2015.3.11>

1. 제6조제4항을 위반한 경우
2. 제11조를 위반한 경우
3. 제16조에 따른 수집·조사 등의 제한 사항을 위반한 경우
4. 제17조제4항 또는 제19조를 위반하여 신용정보를 분실·도난·유출·변조 또는 훼손당한 경우
5. 제22조제1항 및 제27조제1항을 위반한 경우
6. 신용조회회사가 제22조의3을 위반하여 계열회사 등에 개인신용정보를 제공한 경우
7. 제40조제5호를 위반한 경우
8. 제42조제1항·제3항 또는 제4항을 위반한 경우
9. 별표에 규정된 처분 사유에 해당하는 경우
10. 「채권의 공정한 추심에 관한 법률」 제12조제2호·제5호를 위반하여 채권추심행위를 한 경우(채권추심업만 해당한다)
11. 그 밖에 법령 또는 정관을 위반하거나 경영상태가 건전하지 못하여 공익을 심각하게 해치거나 해칠 우려가 있는 경우

제3장 신용정보의 수집·조사 및 처리

제15조(수집·조사 및 처리의 원칙) ① 신용정보회사, 신용정보집중기관 및 신용정보제공·이용자(이하 "신용정보회사등"이라 한다)는 신용정보를 수집·조사 및 처리할 수 있다. 이 경우 이 법 또는 정관으로 정한 업무 범위에서 수집·조사 및 처리의 목적을 명확히 하여야 하며, 이 법 및 「개인정보 보호법」에 따라 그 목적 달성에 필요한 최소한의 범위에서 합리적이고 공정한 수단을 사용하여 신용정보를 수집·조사 및 처리하여야 한다.

② 신용정보회사등이 개인신용정보를 수집하는 때에는 해당 신용정보주체의 동의를 받아야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
2. 신용정보주체와의 금융거래 등 상거래계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
3. 신용정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 신용정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 신용정보제공·이용자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 신용정보주체의 권리보다 우선하는 경우. 이 경우 신용정보제공·이용자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한정한다.

[전문개정 2015.3.11]

제16조(수집·조사 및 처리의 제한) ① 신용정보회사등은 다음 각 호의 정보를 수집·조사하여서는 아니 된다.

1. 국가의 안보 및 기밀에 관한 정보
2. 기업의 영업비밀 또는 독창적인 연구개발 정보
3. 개인의 정치적 사상, 종교적 신념, 그 밖에 신용정보와 관계없는 사생활에 관한 정보
4. 확실하지 아니한 개인신용정보
5. 다른 법률에 따라 수집이 금지된 정보
6. 그 밖에 대통령령으로 정하는 정보

② 신용정보회사등이 개인의 질병에 관한 정보를 수집·조사하거나 타인에게 제공하려면 미리 제32조제1항에 따른 해당 개인의 동의를 받아야 하며 대통령령으로 정하는 목적으로만 그 정보를 이용하여야 한다.

제17조(수집·조사 및 처리의 위탁) ① 신용정보회사등은 그 업무 범위에서 의뢰인의 동의를 받아 다른 신용정보회사등에 신용정보의 수집·조사를 위탁할 수 있다.

② 신용정보회사등은 수집된 신용정보의 처리를 일정한 금액 이상의 자본금 등 대통령령으로 정하는 일정한 요건을 갖춘 자에게 위탁할 수 있으며 이에 따라 위탁을 받은 자(이하 "수탁자"라 한다)의 위탁받은 업무의 처리에 관하여는 제19조부터 제21조까지, 제40조, 제43조, 제43조의2 및 제45조(해당 조문에 대한 벌칙 및 과태료규정을 포함한다)를 적용한다.<개정 2015.3.11>

③ 제2항에 따라 신용정보의 처리를 위탁하려는 신용정보회사등으로서 대통령령으로 정하는 자는 제공하는 신용정보의 범위 등을 대통령령으로 정하는 바에 따라 금융위원회에 알려야 한다.

④ 신용정보회사등은 제2항에 따라 신용정보의 처리를 위탁하기 위하여 수탁자에게 개인신용정보를 제공하는 경우 특정 신용정보주체를 식별할 수 있는 정보는 대통령령으로 정하는 바에 따라 암호화 등의 보호 조치를 하여야 한다.<신설 2015.3.11>

⑤ 신용정보회사등은 수탁자에게 신용정보를 제공한 경우 신용정보를 분실·도난·유출·변조 또는 훼손당하지 아니하도록 대통령령으로 정하는 바에 따라 수탁자를 교육하여야 하고 수탁자의 안전한 신용정보 처리에 관한 사항을 위탁계약에 반영하여야 한다.<신설 2015.3.11>
⑥ 수탁자는 제2항에 따라 위탁받은 업무 범위를 초과하여 제공받은 신용정보를 이용하여서는 아니 된다.<신설 2015.3.11>
⑦ 수탁자는 제2항에 따라 위탁받은 업무를 제3자에게 재위탁하여서는 아니 된다. 다만, 신용정보의 보호 및 안전한 처리를 저해하지 아니하는 범위에서 금융위원회가 인정하는 경우에는 그러하지 아니하다.<신설 2015.3.11>

제4장 신용정보의 유통·이용 및 관리

제18조(신용정보의 정확성 및 최신성의 유지) ① 신용정보회사등은 신용정보의 정확성과 최신성이 유지될 수 있도록 대통령령으로 정하는 바에 따라 신용정보의 등록·변경 및 관리 등을 하여야 한다.
② 신용정보회사등은 신용정보주체에게 불이익을 줄 수 있는 신용정보를 그 불이익을 초래하게 된 사유가 해소된 날부터 최장 5년 이내에 등록·관리 대상에서 삭제하여야 한다.<개정 2011.5.19>
③ 제2항에 따른 해당 신용정보의 구체적인 종류, 기록보존 및 활용기간 등은 대통령령으로 정한다.<신설 2011.5.19>

제19조(신용정보전산시스템의 안전보호) ① 신용정보회사등은 신용정보전산시스템(제25조제6항에 따른 신용정보공동전산망을 포함한다. 이하 같다)에 대한 제3자의 불법적인 접근, 입력된 정보의 변경·훼손 및 파괴, 그 밖의 위험에 대하여 대통령령으로 정하는 바에 따라 기술적·물리적·관리적 보안대책을 수립·시행하여야 한다. <개정 2015.3.11>
② 신용정보제공·이용자가 다른 신용정보제공·이용자 또는 신용조회회사와 서로 이 법에 따라 신용정보를 제공하는 경우에는 금융위원회가 정하여 고시하는 바에 따라 신용정보 보안관리 대책을 포함한 계약을 체결하여야 한다.

제20조(신용정보 관리책임의 명확화 및 업무처리기록의 보존) ① 신용정보회사등은 신용정보의 수집·처리·이용 및 보호 등에 대하여 금융위원회가 정하는 신용정보 관리기준을 준수하여야 한다. <개정 2015.3.11>
② 신용정보회사등은 다음 각 호의 사항에 대한 기록을 3년간 보존하여야 한다.
1. 의뢰인의 주소와 성명 또는 정보제공·교환기관의 주소와 이름
2. 의뢰받은 업무 내용 및 의뢰받은 날짜
3. 의뢰받은 업무의 처리 내용 또는 제공한 신용정보의 내용과 제공한 날짜
4. 그 밖에 대통령령으로 정하는 사항

③ 신용정보회사, 신용정보집중기관 및 대통령령으로 정하는 신용정보제공·이용자는 제4항에 따른 업무를 하는 신용정보관리·보호인을 1명 이상 지정하여야 한다. 다만, 총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 자는 신용정보관리·보호인을 임원으로 하여야 한다.<개정 2015.3.11>

④ 제3항에 따른 신용정보관리·보호인은 다음 각 호의 업무를 수행한다.<신설 2015.3.11>

1. 신용정보의 수집·보유·제공·삭제 등 관리 및 보호 계획의 수립 및 시행
2. 신용정보의 수집·보유·제공·삭제 등 관리 및 보호 실태와 관행에 대한 정기적인 조사 및 개선
3. 신용정보 열람 및 정정청구 등 신용정보주체의 권리행사 및 피해구제
4. 신용정보 유출 등을 방지하기 위한 내부통제시스템의 구축 및 운영
5. 임직원 및 전속 모집인 등에 대한 신용정보보호교육계획의 수립 및 시행
6. 임직원 및 전속 모집인 등의 신용정보보호 관련 법령 및 규정 준수 여부 점검
7. 그 밖에 신용정보의 관리 및 보호를 위하여 대통령령으로 정하는 업무

⑤ 신용정보관리·보호인은 제4항 각 호의 업무에 관하여 금융위원회가 정하는 바에 따라 주기적으로 보고서를 작성하여야 하며, 이를 대표이사 및 이사회에 보고하고 금융위원회에 제출하여야 한다.<신설 2015.3.11>

⑥ 제3항에 따른 신용정보관리·보호인의 자격요건과 그 밖에 지정에 필요한 사항은 대통령령으로 정한다.<개정 2015.3.11>

⑦ 「금융지주회사법」 제48조의2제6항에 따라 선임된 고객정보관리인이 제6항의 자격요건에 해당하면 제3항에 따라 지정된 신용정보관리·보호인으로 본다.<개정 2015.3.11>

제20조의2(개인신용정보의 보유기간 등) ① 신용정보제공·이용자는 금융거래 등 상거래관계(고용관계는 제외한다. 이하 같다)가 종료된 날부터 금융위원회가 정하여 고시하는 기한까지 해당 신용정보주체의 개인신용정보가 안전하게 보호될 수 있도록 접근권한을 강화하는 등 대통령령으로 정하는 바에 따라 관리하여야 한다.

② 신용정보제공·이용자는 금융거래 등 상거래관계가 종료된 날부터 최장 5년 이내(해당 기간 이전에 정보 수집·제공 등의 목적이 달성된 경우에는 그 목적이 달성된 날부터 3개월 이내)에 해당 신용정보주체의 개인신용정보를 관리대상에서 삭제하여야 한다. 다만, 다음 각 호의 경우에는 그러하지 아니하다.

1. 다른 법률에 따른 의무를 이행하기 위하여 불가피한 경우
2. 개인의 급박한 생명·신체·재산의 이익을 위하여 필요하다고 인정되는 경우
3. 그 밖에 예금·보험금의 지급, 보험사기자의 재가입 방지를 위한 경우 등 개인신용정보를 보존할 필요가 있는 경우로서 대통령령으로 정하는 경우

③ 신용정보제공·이용자가 제2항 단서에 따라 개인신용정보를 삭제하지 아니하고 보존하는 경우에는 현재 거래 중인 신용정보주체의 개인신용정보와 분리하는 등 대통령령으로 정하는 바에 따라 관리하여야 한다.

④ 신용정보제공·이용자가 제3항에 따라 분리하여 보존하는 개인신용정보를 활용하는 경우에는 신용정보주체에게 통지하여야 한다.

⑤ 제1항 및 제2항에 따른 개인신용정보의 종류, 관리기간, 삭제의 방법·절차 및 금융거래 등 상거래관계가 종료된 날의 기준 등은 대통령령으로 정한다.

[본조신설 2015.3.11]

제21조(폐업 시 보유정보의 처리) 신용정보회사나 신용정보집중기관이 폐업하려는 경우에는 금융위원회가 정하여 고시하는 바에 따라 보유정보를 처분하거나 폐기하여야 한다.

제5장 신용정보업

제1절 신용조회업 등

제22조(신용조회업 종사자) ① 신용조회회사(신용조회업 허가를 받은 자를 말한다. 이하 같다)는 다음 각 호의 어느 하나에 해당하는 자를 임원으로 채용하거나 고용하여서는 아니 된다.

1. 미성년자
2. 한정치산자 또는 금치산자
3. 파산선고를 받고 복권되지 아니한 자
4. 금고 이상의 실형을 선고받고 그 집행이 끝나거나(집행이 끝난 것으로 보는 경우를 포함한다) 집행이 면제된 날부터 3년이 지나지 아니한 자
5. 금고 이상의 형의 집행유예를 선고받고 그 유예기간 중에 있는 자
6. 이 법 또는 그 밖의 법령에 따라 해임되거나 면직된 후 5년이 지나지 아니한 자
7. 이 법 또는 그 밖의 법령에 따라 영업의 허가·인가 등이 취소된 법인이나 회사의 임직원이었던 자(그 취소사유의 발생에 직접 또는 이에 상응하는 책임이 있는 자로서 대통령령으로 정하는 자만 해당한다)로서 그 법인이나 회사에 대한 취소가 있었던 날부터 5년이 지나지 아니한 자

② 신용조회업에 종사하는 임직원이 신용정보를 수집하려는 경우에는 신용조회업에 종사하고 있음을 나타내는 증표를 지니고 이를 관계인에게 내보여야 한다.

제22조의2(신용정보 등의 보고) 신용조회회사는 신용정보의 활용범위, 활용기간, 제공 대상자 등을 대통령령으로 정하는 바에 따라 금융위원회에 보고하여야 한다.

[본조신설 2011.5.19]

제22조의3(계열회사 등에 대한 개인신용정보 제공 금지) 신용조회회사는 제32조제2항에도 불구하고 제9조제1항에 따른 지배주주 및 「독점규제 및 공정거래에 관한 법률」 제2조제3호에 따른 계열회사에 개인신용정보를 제공할 수 없다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 신용조회회사가 제4조제1항제1호에 따른 업무수행을 위하여 제공하는 경우

2. 제32조제6항제4호에 따라 제공하는 경우

[본조신설 2015.3.11]

제23조(공공기관에 대한 신용정보의 제공 요청 등) ① 삭제 <2015.3.11>

② 신용정보집중기관이 국가·지방자치단체 또는 대통령령으로 정하는 공공단체(이하 "공공기관"이라 한다)의 장에게 신용정보주체의 신용도·신용거래능력 등의 판단에 필요한 신용정보로서 대통령령으로 정하는 신용정보의 제공을 요청하면 그 요청을 받은 공공기관의 장은 다음 각 호의 법률에도 불구하고 해당 신용정보집중기관에 정보를 제공할 수 있다. 이 경우 정보를 제공하는 기준과 절차 등은 대통령령으로 정한다.<개정 2011.3.29, 2015.3.11>

1. 「공공기관의 정보공개에 관한 법률」
2. 「개인정보 보호법」
3. 「국민건강보험법」
4. 「국민연금법」
5. 「한국전력공사법」
6. 「주민등록법」

③ 신용정보집중기관은 제2항에 따라 공공기관으로부터 제공받은 신용정보를 대통령령으로 정하는 신용정보의 이용자에게 제공할 수 있다.<개정 2015.3.11>

④ 신용정보집중기관 또는 제3항에 따른 신용정보의 이용자가 신용정보제공·이용자에게 제2항 및 제3항에 따라 공공기관으로부터 제공받은 개인신용정보를 제공하는 경우에는 제32조제3항에서 정하는 바에 따라 신용정보제공·이용자가 해당 개인으로부터 신용정보 제공·이용에 대한 동의를 받았는지를 확인하여야 한다.<개정 2015.3.11>

⑤ 제3항에 따라 신용정보를 제공받은 신용정보의 이용자는 그 정보를 타인에게 제공하여서는 아니 된다.<개정 2015.3.11>

⑥ 제2항에 따라 신용정보의 제공을 요청하는 자는 관계 법령에 따라 열람료 또는 수수료 등을 내야 한다.<개정 2015.3.11>

⑦ 신용정보회사등은 공공기관의 장이 관계 법령에서 정하는 공무상 목적으로 이용하기 위하여 신용정보의 제공을 문서로 요청한 경우에는 그 신용정보를 제공할 수 있다.

[제목개정 2015.3.11]

제24조(주민등록전산정보자료의 이용) ① 신용정보집중기관 및 대통령령으로 정하는 신용정보제공·이용자는 다음 각 호의 어느 하나에 해당하는 경우에는 행정자치부장관에게 「주민등록법」 제30조제1항에 따른 주민등록전산정보자료의 제공을 요청할 수 있다. 이 경우 요청을 받은 행정자치부장관은 특별한 사유가 없으면 그 요청에 따라야 한다. <개정 2013.3.23, 2014.11.19>

1. 「상법」 제64조 등 다른 법률에 따라 소멸시효가 완성된 예금 및 보험금 등의 지급을 위한 경우로서 해당 예금 및 보험금 등의 원권리자에게 관련 사항을 알리기 위한 경우

2. 금융거래계약의 만기 도래, 실효(失效), 해지 등 계약의 변경사유 발생 등 거래 상대방의 권리·의무에 영향을 미치는 사항을 알리기 위한 경우

② 제1항에 따라 주민등록전산정보자료를 요청하는 경우에는 금융위원회위원장의 심사를 받아야 한다.

③ 제2항에 따라 금융위원회위원장의 심사를 받은 경우에는 「주민등록법」 제30조제1항에 따른 관계 중앙행정기관의 장의 심사를 거친 것으로 본다. 처리절차, 사용료 또는 수수료 등에 관한 사항은 「주민등록법」에 따른다.

제25조(신용정보집중기관) ① 신용정보를 집중하여 수집·보관함으로써 체계적·종합적으로 관리하고, 신용정보회사등 상호 간에 신용정보를 교환·활용(이하 "집중관리·활용"이라 한다)하려는 자는 금융위원회로부터 신용정보집중기관으로 허가를 받아야 한다. <개정 2015.3.11>

② 제1항에 따른 신용정보집중기관은 다음 각 호의 구분에 따라 허가를 받아야 한다.<개정 2015.3.11>

1. 종합신용정보집중기관: 대통령령으로 정하는 금융기관 전체로부터의 신용정보를 집중관리·활용하는 신용정보집중기관
2. 개별신용정보집중기관: 제1호에 따른 금융기관 외의 같은 종류의 사업자가 설립한 협회 등의 협약 등에 따라 신용정보를 집중관리·활용하는 신용정보집중기관

③ 제1항에 따른 신용정보집중기관으로 허가를 받으려는 자는 다음 각 호의 요건을 갖추어야 한다.<개정 2015.3.11>

1. 「민법」 제32조에 따라 설립된 비영리법인일 것
2. 신용정보를 집중관리·활용하는 데 있어서 대통령령으로 정하는 바에 따라 공공성과 중립성을 갖출 것
3. 대통령령으로 정하는 시설·설비 및 인력을 갖출 것

④ 제1항 및 제2항에 따른 허가 및 그 취소 등에 필요한 사항과 집중관리·활용되는 신용정보의 내용·범위 및 교환 대상자는 대통령령으로 정한다. 다만, 신용정보집중기관과 신용조회회사 사이의 신용정보 교환 및 이용은 신용조회회사의 의뢰에 따라 신용정보집중기관이 신용조회회사에 신용정보를 제공하는 방식으로 한다.<개정 2015.3.11>

⑤ 제2항제1호에 따른 종합신용정보집중기관(이하 "종합신용정보집중기관"이라 한다)은 집중되는 신용정보의 정확성·신속성을 확보하기 위하여 제26조에 따른 신용정보집중관리위원회가 정하는 바에 따라 신용정보를 제공하는 금융기관의 신용정보 제공의무 이행 실태를 조사할 수 있다.<개정 2015.3.11>

⑥ 신용정보집중기관은 대통령령으로 정하는 바에 따라 신용정보공동전산망(이하 "공동전산망"이라 한다)을 구축할 수 있으며, 공동전산망에 참여하는 자는 그 유지·관리 등에 필요한 협조를 하여야 한다. 이 경우 신용정보집중기관은 「전기통신사업법」 제2조제1항제1호에 따른 전기통신사업자이어야 한다.

제25조의2(종합신용정보집중기관의 업무) 종합신용정보집중기관은 다음 각 호의 업무를 수행한다.

1. 신용정보의 집중관리 및 활용
2. 공공 목적의 조사 및 분석 업무
3. 신용정보의 가공·분석 및 제공 등과 관련하여 대통령령으로 정하는 업무
4. 신용정보주체 주소변경의 통보대행 업무
5. 다른 법령에서 종합신용정보집중기관이 할 수 있도록 정한 업무
6. 그 밖에 제1호부터 제5호까지에 준하는 업무로서 대통령령으로 정하는 업무

[본조신설 2015.3.11]

제26조(신용정보집중관리위원회) ① 다음 각 호의 업무를 수행하기 위하여 종합신용정보집중기관에 신용정보집중관리위원회(이하 "위원회"라 한다)를 둔다. <개정 2015.3.11>

1. 제25조의2 각 호의 업무와 관련한 중요 사안에 대한 심의
2. 신용정보의 집중관리·활용에 드는 경상경비, 신규사업의 투자비 등의 분담에 관한 사항
3. 제25조제2항제1호에 따른 금융기관의 신용정보제공의무 이행 실태에 관한 조사 및 대통령령으로 정하는 바에 따른 제재를 부과하는 사항
4. 신용정보의 업무목적 외 누설 또는 이용의 방지대책에 관한 사항
5. 그 밖에 신용정보의 집중관리·활용에 필요한 사항

② 삭제 <2015.3.11>

③ 위원회는 제1항 각 호의 사항을 결정한 경우 금융위원회가 정하는 바에 따라 금융위원회에 보고하여야 한다.<개정 2015.3.11>

[제목개정 2015.3.11]

제26조의2(신용정보집중관리위원회의 구성·운영 등) ① 위원회는 위원장 1명을 포함한 15명 이내의 위원으로 구성한다.

② 위원회의 위원장은 종합신용정보집중기관의 장으로 하며, 위원은 공익성, 중립성, 업권별 대표성, 신용정보에 관한 전문지식 등을 고려하여 구성한다.

③ 그 밖에 위원회의 구성 및 운영 등에 필요한 사항은 대통령령으로 정한다.

[본조신설 2015.3.11]

제2절 신용조사업 및 채권추심업

제27조(종사자 및 위임직채권추심인 등) ① 신용조사회사(신용조사업 허가를 받은 자를 말한다. 이하 같다) 또는 채권추심회사(채권추심업 허가를 받은 자를 말한다. 이하 같다)는 다음 각 호의 어느 하나에 해당하는 자를 임직원으로 채용하거나 고용하여서는 아니 되며, 위임 또는 그에 준하는 방법으로 채권추심업무를 하여서는 아니 된다.

1. 미성년자. 다만, 금융위원회가 정하여 고시하는 업무에 채용하거나 고용하는 경우는 제외한다.
2. 한정치산자 또는 금치산자
3. 파산선고를 받고 복권되지 아니한 자
4. 금고 이상의 실형을 선고받고 그 집행이 끝나거나(집행이 끝난 것으로 보는 경우를 포함한다) 집행이 면제된 날부터 3년이 지나지 아니한 자
5. 금고 이상의 형의 집행유예를 선고받고 그 유예기간 중에 있는 자
6. 이 법 또는 그 밖의 법령에 따라 해임되거나 면직된 후 5년이 지나지 아니한 자
7. 이 법 또는 그 밖의 법령에 따라 영업의 허가·인가 등이 취소된 법인이나 회사의 임직원이었던 자(그 취소사유의 발생에 직접 또는 이에 상응하는 책임이 있는 자로서 대통령령으로 정하는 자만 해당한다)로서 그 법인 또는 회사에 대한 취소가 있은 날부터 5년이 지나지 아니한 자
8. 제2항제2호에 따른 위임직채권추심인이었던 자로서 등록이 취소된 지 5년이 지나지 아니한 자

② 채권추심회사는 다음 각 호의 어느 하나에 해당하는 자를 통하여 추심업무를 하여야 한다.

1. 채권추심회사의 임직원
2. 채권추심회사가 위임 또는 그에 준하는 방법으로 채권추심업무를 하도록 한 자(이하 "위임직채권추심인"이라 한다)

③ 채권추심회사는 그 소속 위임직채권추심인이 되려는 자를 금융위원회에 등록하여야 한다.

④ 위임직채권추심인은 소속 채권추심회사 외의 자를 위하여 채권추심업무를 할 수 없다.

⑤ 채권추심회사는 추심채권이 아닌 채권을 추심할 수 없으며 다음 각 호의 어느 하나에 해당하는 위임직채권추심인을 통하여 채권추심업무를 하여서는 아니 된다.

1. 제3항에 따라 등록되지 아니한 위임직채권추심인
2. 다른 채권추심회사의 소속으로 등록된 위임직채권추심인
3. 제7항에 따라 업무정지 중에 있는 위임직채권추심인

⑥ 금융위원회는 위임직채권추심인이 다음 각 호의 어느 하나에 해당하면 그 등록을 취소할 수 있다.

1. 거짓이나 그 밖의 부정한 방법으로 제3항에 따른 등록을 한 경우
2. 제7항에 따른 업무정지명령을 위반하거나 업무정지에 해당하는 행위를 한 자가 그 사유발생일 전 1년 이내에 업무정지처분을 받은 사실이 있는 경우
3. 제40조제1호부터 제4호까지의 어느 하나를 위반한 경우
4. 「채권의 공정한 추심에 관한 법률」 제9조 각 호의 어느 하나를 위반하여 채권추심행위를 한 경우
5. 등록의 내용이나 조건을 위반한 경우
6. 정당한 사유 없이 1년 이상 계속하여 등록한 영업을 하지 아니한 경우

⑦ 금융위원회는 위임직채권추심인이 다음 각 호의 어느 하나에 해당하면 6개월의 범위에서 기간을 정하여 그 업무의 전부 또는 일부의 정지를 명할 수 있다.

1. 제4항을 위반한 경우
2. 제16조에 따른 수집·조사 등의 제한 사항을 위반한 경우
3. 제40조제5호의 행위를 한 경우
4. 「채권의 공정한 추심에 관한 법률」 제12조제2호·제5호를 위반한 경우
5. 그 밖에 법령 또는 소속 채권추심회사의 정관을 위반하여 공익을 심각하게 해치거나 해칠 우려가 있는 경우

⑧ 신용조사업 또는 채권추심업에 종사하는 임직원이나 위임직채권추심인이 신용정보의 수집·조사 또는 채권추심업무를 하려는 경우에는 신용조사업 또는 채권추심업에 종사함을 나타내는 증표를 지니고 이를 관계인에게 내보여야 한다.

⑨ 위임직채권추심인의 자격요건 및 등록절차는 대통령령으로 정한다.

⑩ 위임직채권추심인이 되고자 하는 자가 등록을 신청한 때에는 총리령으로 정하는 바에 따라 수수료를 내야 한다.

제3절 삭제 <2013.5.28>

제28조 삭제 <2013.5.28>

제29조 삭제 <2013.5.28>

제30조 삭제 <2013.5.28>

제6장 신용정보주체의 보호

제31조(신용정보활용체제의 공시) 신용정보회사, 신용정보집중기관 및 대통령령으로 정하는 신용정보제공·이용자는 관리하는 신용정보의 종류, 이용 목적, 제공 대상 및 신용정보주체의 권리 등에 관한 사항을 대통령령으로 정하는 바에 따라 공시하여야 한다.

제32조(개인신용정보의 제공·활용에 대한 동의) ① 신용정보제공·이용자가 개인신용정보를 타인에게 제공하려는 경우에는 대통령령으로 정하는 바에 따라 해당 신용정보주체로부터 다음 각 호의 어느 하나에 해당하는 방식으로 개인신용정보를 제공할 때마다 미리 개별적으로 동의를 받아야 한다. 다만, 기존에 동의한 목적 또는 이용 범위에서 개인신용정보의 정확성·최신성을 유지하기 위한 경우에는 그러하지 아니하다. <개정 2015.3.11>

1. 서면
2. 「전자서명법」 제2조제3호에 따른 공인전자서명이 있는 전자문서(「전자거래기본법」 제2조제1호에 따른 전자문서를 말한다)

3. 개인신용정보의 제공 내용 및 제공 목적 등을 고려하여 정보 제공 동의의 안정성과 신뢰성이 확보될 수 있는 유무선 통신으로 개인비밀번호를 입력하는 방식
4. 유무선 통신으로 동의 내용을 해당 개인에게 알리고 동의를 받는 방법. 이 경우 본인 여부 및 동의 내용, 그에 대한 해당 개인의 답변을 음성녹음하는 등 증거자료를 확보·유지하여야 하며, 대통령령으로 정하는 바에 따른 사후 고지절차를 거친다.
5. 그 밖에 대통령령으로 정하는 방식

② 신용조회회사 또는 신용정보집중기관으로부터 개인신용정보를 제공받으려는 자는 대통령령으로 정하는 바에 따라 해당 신용정보주체로부터 제1항 각 호의 어느 하나에 해당하는 방식으로 개인신용정보를 제공받을 때마다 개별적으로 동의(기존에 동의한 목적 또는 이용 범위에서 개인신용정보의 정확성·최신성을 유지하기 위한 경우는 제외한다)를 받아야 한다. 이 경우 개인신용정보를 제공받으려는 자는 개인신용정보의 조회 시 신용등급이 하락할 수 있는 때에는 해당 신용정보주체에게 이를 고지하여야 한다.<개정 2015.3.11>

③ 신용조회회사 또는 신용정보집중기관이 개인신용정보를 제2항에 따라 제공하는 경우에는 해당 개인신용정보를 제공받으려는 자가 제2항에 따른 동의를 받았는지를 대통령령으로 정하는 바에 따라 확인하여야 한다.

④ 신용정보회사등은 개인신용정보의 제공 및 활용과 관련하여 동의를 받을 때에는 대통령령으로 정하는 바에 따라 서비스 제공을 위하여 필수적 동의사항과 그 밖의 선택적 동의사항을 구분하여 설명한 후 각각 동의를 받아야 한다. 이 경우 필수적 동의사항은 서비스 제공과의 관련성을 설명하여야 하며, 선택적 동의사항은 정보제공에 동의하지 아니할 수 있다는 사실을 고지하여야 한다.<신설 2015.3.11>

⑤ 신용정보회사등은 신용정보주체가 선택적 동의사항에 동의하지 아니한다는 이유로 신용정보주체에게 서비스의 제공을 거부하여서는 아니 된다.<신설 2015.3.11.>

⑥ 신용정보회사등이 개인신용정보를 제공하는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 제1항부터 제5항까지를 적용하지 아니한다.<개정 2015.3.11.>

1. 신용정보회사가 다른 신용정보회사 또는 신용정보집중기관과 서로 집중관리·활용하기 위하여 제공하는 경우
2. 계약의 이행에 필요한 경우로서 제17조제2항에 따라 신용정보의 처리를 위탁하기 위하여 제공하는 경우
3. 영업양도·분할·합병 등의 이유로 권리·의무의 전부 또는 일부를 이전하면서 그와 관련된 개인신용정보를 제공하는 경우
4. 채권추심(추심채권을 추심하는 경우만 해당한다), 인가·허가의 목적, 기업의 신용도 판단, 유가증권의 양수 등 대통령령으로 정하는 목적으로 사용하는 자에게 제공하는 경우
5. 법원의 제출명령 또는 법관이 발부한 영장에 따라 제공하는 경우
6. 범죄 때문에 피해자의 생명이나 신체에 심각한 위험 발생이 예상되는 등 긴급한 상황에서 제5호에 따른 법관의 영장을 발부받을 시간적 여유가 없는 경우로서 검사 또는 사법경찰관의 요구에 따라 제공하는 경우. 이 경우 개인신용정보를 제공받은 검사는 지체 없이 법관에

게 영장을 청구하여야 하고, 사법경찰관은 검사에게 신청하여 검사의 청구로 영장을 청구하여야 하며, 개인신용정보를 제공받은 때부터 36시간 이내에 영장을 발부받지 못하면 지체 없이 제공받은 개인신용정보를 폐기하여야 한다.

7. 조세에 관한 법률에 따른 질문·검사 또는 조사를 위하여 관할 관서의 장이 서면으로 요구하거나 조세에 관한 법률에 따라 제출의무가 있는 과세자료의 제공을 요구함에 따라 제공하는 경우
8. 국제협약 등에 따라 외국의 금융감독기구에 금융회사가 가지고 있는 개인신용정보를 제공하는 경우
9. 대통령령으로 정하는 금융질서문란행위자 및 기업의 과점주주, 최다출자자 등 관련인의 신용도를 판단할 수 있는 정보를 제공하는 경우
10. 그 밖에 다른 법률에 따라 제공하는 경우

⑦ 제6항 각 호에 따라 개인신용정보를 타인에게 제공하려는 자 또는 제공받은 자는 대통령령으로 정하는 바에 따라 개인신용정보의 제공 사실 및 이유 등을 사전에 해당 신용정보주체에게 알려야 한다. 다만, 대통령령으로 정하는 불가피한 사유가 있는 경우에는 인터넷 홈페이지 게재 또는 그 밖에 유사한 방법을 통하여 사후에 알리거나 공시할 수 있다.<개정 2011.5.19., 2015.3.11>

⑧ 제6항제3호에 따라 개인신용정보를 타인에게 제공하는 신용정보제공·이용자로서 대통령령으로 정하는 자는 제공하는 신용정보의 범위 등 대통령령으로 정하는 사항에 관하여 금융위원회의 승인을 받아야 한다.<개정 2015.3.11>

⑨ 제8항에 따른 승인을 받아 개인신용정보를 제공받은 자는 해당 개인신용정보를 금융위원회가 정하는 바에 따라 현재 거래 중인 신용정보주체의 개인신용정보와 분리하여 관리하여야 한다.<신설 2015.3.11>

⑩ 신용정보회사등이 개인신용정보를 제공하는 경우에는 금융위원회가 정하여 고시하는 바에 따라 개인신용정보를 제공받는 자의 신원(身元)과 이용 목적을 확인하여야 한다.<개정 2015.3.11>

⑪ 개인신용정보를 제공한 신용정보제공·이용자는 제1항에 따라 미리 개별적 동의를 받았는지 여부 등에 대한 다툼이 있는 경우 이를 증명하여야 한다.<개정 2015.3.11>

제33조(개인신용정보의 이용) 개인신용정보는 해당 신용정보주체가 신청한 금융거래 등 상거래 관계의 설정 및 유지 여부 등을 판단하기 위한 목적으로만 이용하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. <개정 2015.3.11>

1. 개인이 제32조제1항 각 호의 방식으로 이 조 각 호 외의 부분 본문에서 정한 목적 외의 다른 목적에의 이용에 동의한 경우
2. 개인이 직접 제공한 개인신용정보(그 개인과의 상거래에서 생긴 신용정보를 포함한다)를 제공받은 목적으로 이용하는 경우(상품과 서비스를 소개하거나 그 구매를 권유할 목적으로 이용하는 경우는 제외한다)

3. 제32조제6항 각 호의 경우
4. 그 밖에 제1호부터 제3호까지의 규정에 준하는 경우로서 대통령령으로 정하는 경우

제34조(개인식별정보의 제공·이용) 신용정보제공·이용자가 개인을 식별하기 위하여 필요로 하는 정보로서 대통령령으로 정하는 정보를 제공·이용하는 경우에는 제32조 및 제33조를 준용한다.

[전문개정 2015.3.11]

제35조(신용정보 이용 및 제공사실의 조회) ① 신용정보회사등은 개인신용정보를 이용하거나 제공한 경우 대통령령으로 정하는 바에 따라 다음 각 호의 구분에 따른 사항을 신용정보주체가 조회할 수 있도록 하여야 한다. 다만, 내부 경영관리의 목적으로 이용하거나 반복적인 업무위탁을 위하여 제공하는 경우 등 대통령령으로 정하는 경우에는 그러하지 아니하다.

1. 개인신용정보를 이용한 경우: 이용 주체, 이용 목적, 이용 날짜, 이용한 신용정보의 내용, 그 밖에 대통령령으로 정하는 사항
2. 개인신용정보를 제공한 경우: 제공 주체, 제공받은 자, 제공 목적, 제공한 날짜, 제공한 신용정보의 내용, 그 밖에 대통령령으로 정하는 사항

② 신용정보회사등은 제1항에 따라 조회를 한 신용정보주체의 요청이 있는 경우 개인신용정보를 이용하거나 제공하는 때에 제1항 각 호의 구분에 따른 사항을 대통령령으로 정하는 바에 따라 신용정보주체에게 통지하여야 한다.

③ 신용정보회사등은 신용정보주체에게 제2항에 따른 통지를 요청할 수 있음을 알려주어야 한다.

[전문개정 2015.3.11]

제36조(상거래 거절 근거 신용정보의 고지 등) ① 신용정보제공·이용자가 신용조회회사 및 신용정보집중기관으로부터 제공받은 개인신용정보로서 대통령령으로 정하는 정보에 근거하여 상대방과의 상거래관계 설정을 거절하거나 중지한 경우에는 해당 신용정보주체의 요구가 있으면 그 거절 또는 중지의 근거가 된 정보 등 대통령령으로 정하는 사항을 본인에게 고지하여야 한다.

② 신용정보주체는 제1항에 따라 고지받은 본인정보의 내용에 이의가 있으면 제1항에 따른 고지를 받은 날부터 60일 이내에 해당 신용정보를 수집·제공한 신용조회회사 및 신용정보집중기관에게 그 신용정보의 정확성을 확인하도록 요청할 수 있다.

③ 제2항에 따른 확인절차 등에 관하여는 제38조를 준용한다.

제37조(개인신용정보 제공·이용 동의 철회권 등) ① 개인인 신용정보주체는 제32조제1항 각 호의 방식으로 동의를 받은 신용정보제공·이용자에게 신용조회회사 또는 신용정보집중기관에 제공하여 개인의 신용도 등을 평가하기 위한 목적 외의 목적으로 행한 개인신용정보 제공 동의를 대통령령으로 정하는 바에 따라 철회할 수 있다. 다만, 동의를 받은 신용정보제공·이용자 외의 신용정보제공·이용자에게 해당 개인신용정보를 제공하지 아니하면 해당 신용정보

주체와 약정한 용역의 제공을 하지 못하게 되는 등 계약 이행이 어려워지거나 제33조 각 호 외의 부분 본문에 따른 목적을 달성할 수 없는 경우에는 고객이 동의를 철회하려면 그 용역의 제공을 받지 아니할 의사를 명확하게 밝혀야 한다.

② 개인인 신용정보주체는 대통령령으로 정하는 바에 따라 신용정보제공·이용자에 대하여 상품이나 용역을 소개하거나 구매를 권유할 목적으로 본인에게 연락하는 것을 중지하도록 청구할 수 있다.

③ 신용정보제공·이용자는 서면, 전자문서 또는 구두에 의한 방법으로 제1항 및 제2항에 따른 권리의 내용, 행사방법 등을 거래 상대방인 개인에게 고지하고, 거래 상대방이 제1항 및 제2항의 요구를 하면 즉시 이에 따라야 한다. 이 때 구두에 의한 방법으로 이를 고지한 경우 대통령령으로 정하는 바에 따른 추가적인 사후 고지절차를 거쳐야 한다.

④ 신용정보제공·이용자는 대통령령으로 정하는 바에 따라 제3항에 따른 의무를 이행하기 위한 절차를 갖추어야 한다.

⑤ 신용정보제공·이용자는 제2항에 따른 청구에 따라 발생하는 전화요금 등 금전적 비용을 개인인 신용정보주체가 부담하지 아니하도록 대통령령으로 정하는 바에 따라 필요한 조치를 하여야 한다.

제38조(신용정보의 열람 및 정정청구 등) ① 신용정보주체는 신용정보회사등에 본인의 신분을 나타내는 증표를 내보이거나 전화, 인터넷 홈페이지의 이용 등 대통령령으로 정하는 방법으로 본인임을 확인받아 신용정보회사등이 가지고 있는 본인정보의 제공 또는 열람을 청구할 수 있으며, 본인정보가 사실과 다른 경우에는 금융위원회가 정하여 고시하는 바에 따라 정정을 청구할 수 있다.

② 제1항에 따라 정정청구를 받은 신용정보회사등은 정정청구에 정당한 사유가 있다고 인정하면 즉시 문제가 된 신용정보에 대하여 정정청구 중 또는 사실조회 중임을 기입하고, 지체 없이 해당 신용정보의 제공·이용을 중단한 후 사실인지를 조사하여 사실과 다르거나 확인할 수 없는 신용정보는 삭제하거나 정정하여야 한다.

③ 제2항에 따라 신용정보를 삭제하거나 정정한 신용정보회사등은 해당 신용정보를 최근 6개월 이내에 제공받은 자와 해당 신용정보주체가 요구하는 자에게 해당 신용정보에서 삭제하거나 정정한 내용을 알려야 한다.

④ 신용정보회사등은 제2항과 제3항에 따른 처리결과를 7일 이내에 해당 신용정보주체에게 알려야 하며, 해당 신용정보주체는 처리결과에 이의가 있으면 대통령령으로 정하는 바에 따라 금융위원회에 그 시정을 요청할 수 있다.

⑤ 금융위원회는 제4항에 따른 시정을 요청받으면 「금융위원회의 설치 등에 관한 법률」 제24조에 따라 설립된 금융감독원의 원장(이하 "금융감독원장"이라 한다)으로 하여금 그 사실 여부를 조사하게 하고, 조사결과에 따라 신용정보회사등에 대하여 시정을 명하거나 그 밖에 필요한 조치를 할 수 있다.

⑥ 제5항에 따라 조사를 하는 자는 그 권한을 표시하는 증표를 지니고 이를 관계인에게 내보여야 한다.

⑦ 신용정보회사등이 제5항에 따른 금융위원회의 시정명령에 따라 시정조치를 한 경우에는 그 결과를 금융위원회에 보고하여야 한다.

제38조의2(신용조회사실의 통지 요청) ① 신용정보주체는 신용조회회사에 본인의 개인신용정보가 조회되는 사실을 통지하여 줄 것을 요청할 수 있다. 이 경우 신용정보주체는 금융위원회가 정하는 방식에 따라 본인임을 확인받아야 한다.

② 제1항의 요청을 받은 신용조회회사는 명의도용 가능성 등 대통령령으로 정하는 경우의 조회가 발생한 때에는 해당 조회에 따른 정보제공을 중지하고 그 사실을 지체 없이 해당 신용정보주체에게 통지하여야 한다.

③ 제2항의 정보제공 중지 및 통지 방법, 통지에 따른 비용 부담 등에 필요한 사항은 대통령령으로 정한다.

[본조신설 2015.3.11]

제38조의3(개인신용정보의 삭제 요구) ① 신용정보주체는 금융거래 등 상거래관계가 종료되고 대통령령으로 정하는 기간이 경과한 경우 신용정보제공·이용자에게 본인의 개인신용정보의 삭제를 요구할 수 있다. 다만, 제20조의2제2항 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

② 신용정보제공·이용자가 제1항의 요구를 받았을 때에는 지체 없이 해당 개인신용정보를 삭제하고 그 결과를 신용정보주체에게 통지하여야 한다.

③ 신용정보제공·이용자는 신용정보주체의 요구가 제1항 단서에 해당될 때에는 다른 개인신용정보와 분리하는 등 대통령령으로 정하는 바에 따라 관리하여야 하며, 그 결과를 신용정보주체에게 통지하여야 한다.

④ 제2항 및 제3항에 따른 통지의 방법은 금융위원회가 정하여 고시한다.

[본조신설 2015.3.11]

제39조(무료 열람권) 신용조회회사는 1년 이내로서 대통령령으로 정하는 일정한 기간마다 개인인 신용정보주체가 본인정보를 1회 이상 무료로 제공받거나 열람할 수 있도록 하여야 한다.

제39조의2(신용정보 누설통지 등) ① 신용정보회사등은 신용정보가 업무 목적 외로 누설되었음을 알게 된 때에는 지체 없이 해당 신용정보주체에게 다음 각 호의 사실을 통지하여야 한다.

1. 누설된 신용정보의 항목
2. 누설된 시점과 그 경위
3. 누설로 인하여 발생할 수 있는 피해를 최소화하기 위하여 신용정보주체가 할 수 있는 방법 등에 관한 정보
4. 신용정보회사등의 대응조치 및 피해 구제절차
5. 신용정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 신용정보회사등은 신용정보가 누설된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

③ 신용정보회사등은 대통령령으로 정하는 규모 이상의 신용정보가 누설된 경우 제1항에 따른 통지 및 제2항에 따른 조치결과를 지체 없이 금융위원회 또는 대통령령으로 정하는 전문기관(이하 이 조에서 "금융위원회등"이라 한다)에 신고하여야 한다. 이 경우 금융위원회등은 피해 확산 방지, 피해 복구 등을 위한 기술을 지원할 수 있다.
④ 금융위원회등은 제3항에 따른 신고를 받은 때에는 이를 행정자치부장관에게 알려야 한다.
⑤ 금융위원회등은 제2항에 따라 신용정보회사등이 행한 조치에 대하여 조사할 수 있으며, 그 조치가 미흡하다고 판단되는 경우 금융위원회는 시정을 요구할 수 있다.
⑥ 제1항에 따른 통지의 시기, 방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.
[본조신설 2015.3.11]

제40조(신용정보회사등의 금지사항) 신용정보회사등은 다음 각 호의 행위를 하여서는 아니 되며, 신용정보회사등이 아니면 제4호 본문의 행위를 업으로 하거나 제5호의 행위를 하여서는 아니 된다. <개정 2015.3.11>
1. 의뢰인에게 허위 사실을 알리는 일
2. 신용정보에 관한 조사 의뢰를 강요하는 일
3. 신용정보 조사 대상자에게 조사자료 제공과 답변을 강요하는 일
4. 특정인의 소재 및 연락처(이하 "소재등"이라 한다)를 알아내거나 금융거래 등 상거래관계 외의 사생활 등을 조사하는 일. 다만, 채권추심업을 허가받은 신용정보회사가 그 업무를 하기 위하여 특정인의 소재등을 알아내는 경우 또는 다른 법령에 따라 특정인의 소재등을 알아내는 것이 허용되는 경우에는 그러하지 아니하다.
5. 정보원, 탐정, 그 밖에 이와 비슷한 명칭을 사용하는 일
6. 삭제 <2013.5.28>
7. 개인신용정보 또는 개인식별정보를 대통령령으로 정하는 전자적 매체나 방식을 이용하여 영리목적의 광고성 정보를 전송하는 행위에 이용하는 일. 다만, 다음 각 목의 어느 하나에 해당하는 경우는 제외한다.
가. 신용정보주체로부터 별도의 동의를 받은 경우
나. 기존에 체결한 금융거래의 유지 및 관리를 위하여 필요한 경우
다. 그 밖에 대통령령으로 정하는 경우

제41조(채권추심회사의 금지 사항) ① 채권추심회사는 자기의 명의를 빌려주어 타인으로 하여금 채권추심업을 하게 하여서는 아니 된다.
② 채권추심회사는 다른 법령에서 허용된 경우 외에는 상호 중에 "신용정보"라는 표현이 포함된 명칭 이외의 명칭을 사용하여서는 아니 된다. 다만, 채권추심회사가 신용조회업 또는 「자본시장과 금융투자업에 관한 법률」 제335조의3제1항에 따라 신용평가업인가를 받아 신용평가업을 함께하는 경우에는 그러하지 아니하다.<개정 2013.5.28>

제41조의2(모집업무수탁자의 모집경로 확인 등) ① 신용정보제공·이용자는 본인의 영업을 영위할 목적으로 모집업무(그 명칭과 상관없이 본인의 영업과 관련한 계약체결을 대리하거나 중

개하는 업무를 말한다. 이하 같다)를 제3자에게 위탁하는 경우 그 모집업무를 위탁받은 자로서 대통령령으로 정하는 자(이하 "모집업무수탁자"라 한다)에 대하여 다음 각 호의 사항을 확인하여야 한다.

1. 거짓이나 그 밖의 부정한 수단이나 방법으로 취득하거나 제공받은 신용정보(이하 "불법취득신용정보"라 한다)를 모집업무에 이용하였는지 여부
2. 모집업무에 이용한 개인신용정보 등을 취득한 경로
3. 그 밖에 대통령령으로 정하는 사항

② 신용정보제공·이용자는 모집업무수탁자가 불법취득신용정보를 모집업무에 이용한 사실을 확인한 경우 해당 모집업무수탁자와의 위탁계약을 해지하여야 한다.

③ 신용정보제공·이용자는 제2항에 따라 모집업무수탁자와의 위탁계약을 해지한 경우 이를 금융위원회 또는 대통령령으로 정하는 등록기관에 알려야 한다.

④ 제1항에 따른 확인, 제3항에 따른 보고의 시기·방법 등에 필요한 사항은 대통령령으로 정한다.

[본조신설 2015.3.11]

제42조(업무 목적 외 누설금지 등) ① 신용정보회사등과 제17조제2항에 따라 신용정보의 처리를 위탁받은 자의 임직원이거나 임직원이었던 자(이하 "신용정보업관련자"라 한다)는 업무상 알게 된 타인의 신용정보 및 사생활 등 개인적 비밀(이하 "개인비밀"이라 한다)을 업무 목적 외에 누설하거나 이용하여서는 아니 된다.

② 신용정보회사등과 신용정보업관련자가 이 법에 따라 신용정보회사등에 신용정보를 제공하는 행위는 제1항에 따른 업무 목적 외의 누설이나 이용으로 보지 아니한다.

③ 제1항을 위반하여 누설된 개인비밀을 취득한 자(그로부터 누설된 개인비밀을 다시 취득한 자를 포함한다)는 그 개인비밀이 제1항을 위반하여 누설된 것임을 알게 된 경우 그 개인비밀을 타인에게 제공하거나 이용하여서는 아니 된다.

④ 신용정보회사등과 신용정보업관련자로부터 개인신용정보를 제공받은 자는 그 개인신용정보를 타인에게 제공하여서는 아니 된다. 다만, 이 법 또는 다른 법률에 따라 제공이 허용되는 경우에는 그러하지 아니하다.

제42조의2(과징금의 부과 등) ① 금융위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 신용정보회사등에게 대통령령으로 정하는 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 다만, 제1호에 해당하는 행위가 있는 경우에는 50억원 이하의 과징금을 부과할 수 있다.

1. 제19조제1항을 위반하여 개인비밀을 분실·도난·누출·변조 또는 훼손당한 경우
2. 제42조제1항을 위반하여 개인비밀을 업무 목적 외에 누설하거나 이용한 경우
3. 제42조제3항을 위반하여 불법 누설된 개인비밀임을 알고 있음에도 그 개인비밀을 타인에게 제공하거나 이용한 경우

② 제1항에 따른 과징금을 부과하는 경우 신용정보회사등이 매출액 산정자료의 제출을 거부하거나 거짓의 자료를 제출한 때에는 해당 신용정보회사등과 비슷한 규모의 신용정보회사등의 재무제표나 그 밖의 회계자료 등의 자료에 근거하여 매출액을 추정할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 200억원 이하의 과징금을 부과할 수 있다.

③ 금융위원회는 제1항에 따른 과징금을 부과하려면 다음 각 호의 사항을 고려하여야 한다.

1. 위반행위의 내용 및 정도
2. 위반행위의 기간 및 횟수
3. 위반행위로 인하여 취득한 이익의 규모

④ 제1항에 따른 과징금은 제3항을 고려하여 산정하되, 구체적인 산정기준과 산정절차는 대통령령으로 정한다.

⑤ 금융위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 이를 내지 아니하면 납부기한의 다음 날부터 내지 아니한 과징금의 연 100분의 6에 해당하는 가산금을 징수한다.

⑥ 금융위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 이를 내지 아니한 경우에는 기간을 정하여 독촉을 하고, 그 지정된 기간에 과징금과 제5항에 따른 가산금을 내지 아니하면 국세 체납처분의 예에 따라 징수한다.

⑦ 법원의 판결 등의 사유로 제1항에 따라 부과된 과징금을 환급하는 경우에는 과징금을 낸 날부터 환급하는 날까지 연 100분의 6에 해당하는 환급가산금을 지급하여야 한다.

⑧ 신용정보제공·이용자가 위탁계약을 맺고 거래하는 모집인(「여신전문금융업법」 제14조의2제2호에 따른 모집인을 말한다) 등 대통령령으로 정하는 자가 제1항 각 호에 해당하는 경우에는 그 위반행위의 범위에서 해당 신용정보제공·이용자의 직원으로 본다. 다만, 그 신용정보제공·이용자가 그 모집인 등의 위반행위를 방지하기 위하여 상당한 주의와 감독을 다한 경우에는 그러하지 아니하다.

⑨ 그 밖에 과징금의 부과·징수에 관하여 필요한 사항은 대통령령으로 정한다.

[본조신설 2015.3.11]

제43조(손해배상의 책임) ① 신용정보회사등과 그 밖의 신용정보 이용자가 이 법을 위반하여 신용정보주체에게 피해를 입힌 경우에는 해당 신용정보주체에 대하여 손해배상의 책임을 진다. 다만, 신용정보회사등과 그 밖의 신용정보 이용자가 고의 또는 과실이 없음을 증명한 경우에는 그러하지 아니하다.

② 신용정보회사등이나 그 밖의 신용정보 이용자(수탁자를 포함한다. 이하 이 조에서 같다)가 고의 또는 중대한 과실로 이 법을 위반하여 개인신용정보가 누설되거나 분실·도난·누출·변조 또는 훼손되어 신용정보주체에게 피해를 입힌 경우에는 해당 신용정보주체에 대하여 그 손해의 3배를 넘지 아니하는 범위에서 배상할 책임이 있다. 다만, 신용정보회사등이나 그 밖의 신용정보 이용자가 고의 또는 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다.<신설 2015.3.11>

③ 법원은 제2항의 배상액을 정할 때에는 다음 각 호의 사항을 고려하여야 한다.<신설 2015.3.11>

1. 고의 또는 손해 발생의 우려를 인식한 정도
2. 위반행위로 인하여 입은 피해 규모
3. 위반행위로 인하여 신용정보회사등이나 그 밖의 신용정보 이용자가 취득한 경제적 이익
4. 위반행위에 따른 벌금 및 과징금
5. 위반행위의 기간·횟수 등
6. 신용정보회사등이나 그 밖의 신용정보 이용자의 재산상태
7. 신용정보회사등이나 그 밖의 신용정보 이용자의 개인신용정보 분실·도난·누출 후 해당 개인신용정보 회수 노력의 정도
8. 신용정보회사등이나 그 밖의 신용정보 이용자의 피해구제 노력의 정도

④ 채권추심회사 또는 위임직채권추심인이 이 법을 위반하여 채무자 및 그 관계인에게 손해를 입힌 경우에는 그 손해를 배상하여야 한다. 다만, 채권추심회사 또는 위임직채권추심인이 자신에게 고의 또는 과실이 없음을 증명한 경우에는 그러하지 아니하다.<개정 2015.3.11>

⑤ 제4조제1항의 업무를 의뢰받은 신용정보회사가 자신에게 책임 있는 사유로 의뢰인에게 손해를 입힌 경우에는 그 손해를 배상하여야 한다.<개정 2015.3.11>

⑥ 제17조제2항에 따라 신용정보의 처리를 위탁받은 자가 이 법을 위반하여 신용정보주체에게 피해를 입힌 경우에는 위탁자는 수탁자와 연대하여 손해배상책임을 진다.<개정 2015.3.11>

⑦ 위임직채권추심인이 이 법 또는 「채권의 공정한 추심에 관한 법률」을 위반하여 채무자나 채무자의 관계인에게 손해를 입힌 경우 채권추심회사는 위임직채권추심인과 연대하여 손해배상책임을 진다. 다만, 채권추심회사가 자신에게 고의 또는 과실이 없음을 증명한 경우에는 그러하지 아니하다.<개정 2015.3.11>

제43조의2(법정손해배상의 청구) ① 신용정보주체는 다음 각 호의 모두에 해당하는 경우에는 대통령령으로 정하는 기간 내에 신용정보회사등이나 그 밖의 신용정보 이용자(수탁자를 포함한다. 이하 이 조에서 같다)에게 제43조에 따른 손해배상을 청구하는 대신 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 신용정보회사등이나 그 밖의 신용정보 이용자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

1. 신용정보회사등이나 그 밖의 신용정보 이용자가 고의 또는 과실로 이 법의 규정을 위반한 경우
2. 개인신용정보가 분실·도난·누출·변조 또는 훼손된 경우

② 법원은 제1항에 따른 청구가 있는 경우에 변론 전체의 취지와 증거조사의 결과를 고려하여 제1항의 범위에서 상당한 손해액을 인정할 수 있다.

③ 제43조에 따른 청구를 한 자는 법원이 변론을 종결할 때까지 그 청구를 제1항에 따른 청구로 변경할 수 있다.

[본조신설 2015.3.11]

제43조의3(손해배상의 보장) 대통령령으로 정하는 신용정보회사등은 제43조에 따른 손해배상 책임의 이행을 위하여 금융위원회가 정하는 기준에 따라 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다.

[본조신설 2015.3.11]

제44조(신용정보협회) ① 신용정보회사는 신용정보업의 건전한 발전을 도모하고 신용정보회사들 사이의 업무질서를 유지하기 위하여 신용정보협회를 설립할 수 있다.

② 신용정보협회는 법인으로 한다.

③ 신용정보협회는 정관으로 정하는 바에 따라 다음 각 호의 업무를 한다.

1. 신용정보회사 간의 건전한 업무질서를 유지하기 위한 업무
2. 신용정보업의 발전을 위한 조사·연구 업무
3. 신용정보업 이용자 민원의 상담·처리
4. 그 밖에 대통령령으로 정하는 업무

④ 신용정보협회에 대하여 이 법에서 정한 것을 제외하고는 「민법」 중 사단법인에 관한 규정을 준용한다.

제7장 보칙

제45조(감독·검사 등) ① 금융위원회는 신용정보회사등에 대하여 이 법 또는 이 법에 따른 명령의 준수 여부를 감독한다.

② 금융위원회는 제1항에 따른 감독에 필요하면 신용정보회사등에 대하여 그 업무 및 재산상황에 관한 보고 등 필요한 명령을 할 수 있다.

③ 금융감독원장은 그 소속 직원으로 하여금 이 법에 따른 신용정보회사등의 업무와 재산상황을 검사하도록 할 수 있다.

④ 금융감독원장은 제3항에 따른 검사에 필요하다고 인정하면 자료의 제출, 관계자의 출석 및 의견의 진술을 신용정보회사등에 요구할 수 있다.

⑤ 제3항에 따라 검사를 하는 자는 그 권한을 표시하는 증표를 지니고 이를 관계인에게 내보여야 한다.

⑥ 금융감독원장은 제3항에 따른 검사를 마치면 그 결과를 금융위원회가 정하는 바에 따라 금융위원회에 보고하여야 한다.

⑦ 금융위원회는 신용정보회사등이 이 법 또는 이 법에 따른 명령을 위반하여 신용정보업의 건전한 경영과 신용정보주체의 권익을 해칠 우려가 있다고 인정하면 다음 각 호의 어느 하나에 해당하는 조치를 하거나, 금융감독원장으로 하여금 제1호부터 제3호까지의 규정에 해당하는 조치를 하게 할 수 있다.

1. 신용정보회사등에 대한 주의 또는 경고
2. 임원에 대한 주의 또는 경고
3. 직원에 대한 주의 및 정직, 감봉, 견책 등의 문책 요구
4. 임원에 대한 해임권고, 직무정지 요구 또는 직원에 대한 면직 요구
5. 위반행위에 대한 시정명령
6. 신용정보제공의 중지

제46조 삭제 <2013.5.28>

제47조(업무보고서의 제출) ① 신용정보회사 및 신용정보집중기관은 매 분기의 업무보고서를 매 분기 마지막 달의 다음 달 말일까지 금융감독원장이 정하는 서식에 따라 작성하여 금융감독원장에게 제출하여야 한다.

② 제1항에 따른 보고서에는 대표자, 담당 책임자 또는 그 대리인이 서명·날인하여야 한다.

③ 제1항에 따른 업무보고서를 작성하기 위한 세부 사항과 그 밖에 필요한 사항은 금융감독원장이 정한다.

제48조(청문) 금융위원회는 제14조제1항에 따라 신용정보회사의 허가 또는 인가를 취소하거나 제27조제6항에 따라 위임직채권추심인의 등록을 취소하려면 청문을 하여야 한다.

제49조(권한의 위임·위탁) 이 법에 따른 금융위원회의 권한 중 대통령령으로 정하는 권한은 대통령령으로 정하는 바에 따라 특별시장·광역시장·도지사·특별자치도지사, 금융감독원장, 신용정보협회, 그 밖에 대통령령으로 정하는 자에게 위임하거나 위탁할 수 있다.

제50조(벌칙) ① 제42조제1항 또는 제3항을 위반한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.

② 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

1. 제4조제2항 또는 제10조제1항을 위반하여 허가 또는 인가를 받지 아니하고 제4조제1항 각 호의 업무를 한 자
2. 거짓이나 그 밖의 부정한 방법으로 제4조제2항 또는 제10조제1항에 따른 허가 또는 인가를 받은 자
3. 제16조를 위반한 자
4. 제17조제6항을 위반한 자
5. 권한 없이 제19조제1항에 따른 신용정보전산시스템의 정보를 변경·삭제하거나 그 밖의 방법으로 이용할 수 없게 한 자 또는 권한 없이 신용정보를 검색·복제하거나 그 밖의 방법으로 이용한 자
6. 제32조제1항 또는 제2항(제34조에 따라 준용하는 경우를 포함한다)을 위반한 자
7. 제33조(제34조에 따라 준용하는 경우를 포함한다)를 위반한 자

8. 제42조제4항을 위반한 자

③ 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

1. 제14조제2항에 따른 업무정지 기간에 업무를 한 자
2. 신용정보집중기관이 아니면서 제25조제6항에 따른 공동전산망을 구축한 자
3. 제40조제1호부터 제5호까지의 어느 하나를 위반한 자
4. 제41조제1항을 위반한 자
5. 제41조의2제1항을 위반하여 모집업무수탁자가 불법취득신용정보를 모집업무에 이용하였는지 등을 확인하지 아니한 자

④ 다음 각 호의 어느 하나에 해당하는 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

1. 제9조제1항을 위반하여 승인 없이 주식을 취득한 자
2. 제9조제2항에 따른 명령을 위반하여 승인 없이 취득한 주식을 처분하지 아니한 자
3. 제17조제2항을 위반하여 일정한 요건을 갖추지 아니한 자에게 신용정보의 처리를 위탁한 자 및 그 위탁을 받은 자
4. 제18조제2항을 위반한 자
5. 제20조제2항을 위반한 자
6. 제27조제3항을 위반하여 위임직채권추심인으로 금융위원회에 등록하지 아니하고 채권추심업무를 한 자
7. 제27조제4항을 위반한 자
8. 제27조제5항을 위반하여 추심채권이 아닌 채권을 추심하거나 등록되지 아니한 위임직채권추심인, 다른 채권추심회사의 소속으로 등록된 위임직채권추심인 또는 업무정지 중인 위임직채권추심인을 통하여 채권추심업무를 한 자
9. 제27조제7항에 따른 업무정지 중에 채권추심업무를 한 자

[전문개정 2015.3.11]

제51조(양벌규정) 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제50조의 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형을 과(科)한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.

제52조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다.

1. 제15조제2항을 위반한 자
2. 제19조를 위반한 자

3. 제20조제5항을 위반한 자
4. 제32조제4항 또는 제5항(제34조에 따라 준용하는 경우를 포함한다)을 위반한 자
5. 제41조의2제2항을 위반하여 모집업무수탁업자와 위탁계약을 해지하지 아니한 자

② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.

1. 제17조제4항을 위반한 자
2. 제20조제1항 또는 제3항을 위반한 자
3. 제20조의2제2항을 위반한 자
4. 제21조를 위반한 자
5. 제23조제5항을 위반한 자
6. 제32조제8항 또는 제9항(제34조에 따라 준용하는 경우를 포함한다)을 위반한 자
7. 제36조제1항 또는 제3항을 위반한 자
8. 제37조제3항을 위반한 자
9. 제38조제2항부터 제5항까지 또는 제7항을 위반한 자
10. 제38조의2를 위반한 자
11. 제38조의3을 위반한 자
12. 제39조를 위반한 자
13. 제39조의2제1항을 위반하여 신용정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자
14. 제39조의2제3항을 위반하여 조치결과를 신고하지 아니한 자
15. 제40조제7호를 위반한 자

③ 제10조제4항 또는 제17조제7항을 위반한 자에게는 2천만원 이하의 과태료를 부과한다.

④ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.

1. 제8조를 위반한 자
2. 제11조부터 제13조까지의 어느 하나를 위반한 자
3. 제17조제1항을 위반하여 의뢰인의 동의 없이 신용정보의 수집·조사를 위탁한 자
4. 제17조제5항을 위반한 자
5. 제18조제1항을 위반한 자
6. 제20조의2제1항·제3항 또는 제4항을 위반한 자
7. 제22조의2를 위반하여 금융위원회에 보고를 하지 아니한 자
8. 제27조제8항을 위반하여 채권추심업무를 할 때 증표를 내보이지 아니한 자
9. 제31조를 위반한 자
10. 제32조제3항·제7항 또는 제10항(제34조에 따라 준용하는 경우를 포함한다)을 위반한 자
11. 제35조를 위반한 자
12. 제41조의2제3항을 위반하여 위탁계약 해지에 관한 사항을 알리지 아니한 자
13. 제45조제2항부터 제4항까지의 규정에 따른 명령에 따르지 아니하거나 검사 및 요구를 거부·방해 또는 기피한 자

14. 제47조를 위반하여 보고서를 제출하지 아니하거나 사실과 다른 내용의 보고서를 제출한 자

⑤ 제1항부터 제4항까지의 규정에 따른 과태료는 대통령령으로 정하는 바에 따라 금융위원회가 부과·징수한다.

[전문개정 2015.3.11]

부칙 <제9617호,2009.4.1>

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다.

제2조(유사명칭 사용에 관한 적용례) 법률 제6428호 신용정보의이용및보호에관한법률중개정법률 시행 전에 그 상호 중에 신용평가 또는 이와 비슷한 명칭을 사용한 자에 대하여는 제12조의 개정규정을 적용하지 아니한다.

제3조(개인신용정보의 제공·활용에 관한 특례) 이 법 시행 전에 개인인 신용정보주체가 제32조제1항의 개정규정에 따른 동의를 받아 개인신용정보를 확인한 후 해당 개인과 금융거래 등 상거래관계를 설정한 경우 그 상거래관계의 유지·관리를 위한 목적으로 해당 신용정보주체에 관한 개인신용정보를 제공받으려는 경우에는 제32조제2항의 개정규정을 적용하지 아니한다.

제4조(신용정보업자에 대한 경과조치) 이 법 시행 당시 종전의 규정에 따라 신용정보업의 허가를 받은 신용정보업자는 이 법에 따라 허가받은 신용정보회사로 본다.

제5조(벌칙 및 과태료에 관한 경과조치) 이 법 시행 전의 행위에 대하여 벌칙을 적용하거나 과태료를 부과하는 경우에는 종전의 규정에 따른다.

제6조(신용조사회사에 대한 경과조치) ① 법률 제4866호 신용정보의이용및보호에관한법률로 폐지된 「신용조사업법」에 따라 신용조사업의 허가를 받은 자가 제6조제2항제1호의 개정규정의 자본금 요건을 충족하는 경우에는 제5조제1항의 개정규정에도 불구하고 신용조회업 허가를 할 수 있으며, 제6조제2항제2호의 개정규정의 자본금 요건을 충족하는 경우에는 제5조제1항의 개정규정에도 불구하고 채권추심업 허가를 할 수 있다.

② 제1항에 따른 신용조사업의 허가를 받은 자가 그 사업을 양도하려는 경우에는 그 양수인은 제4조제2항의 개정규정에 따라 신용정보업 허가를 받은 법인이어야 한다.

제7조(변경허가에 관한 경과조치) 이 법 시행 당시 종전의 규정에 따라 신용정보업의 변경허가를 받은 자는 제8조의 개정규정에 따라 변경 신고 또는 보고를 한 것으로 본다.

제8조(지배주주 변경승인에 관한 경과조치) 이 법 시행 당시 신용정보회사의 지배주주는 제9조의 개정규정에 따라 지배주주의 변경승인을 받은 것으로 본다.

제9조(신용정보업 종사자의 결격사유에 관한 경과조치) 이 법 시행 당시 신용정보업에 종사하고 있는 자가 이 법 시행 전에 생긴 사유로 제22조제1항, 제27조제1항 및 제28조의 개정규정에 따른 결격사유에 해당하게 된 경우에는 각 개정규정에도 불구하고 종전의 규정에 따른다.

제10조(위임직채권추심인 등록에 관한 경과조치) 채권추심회사는 제27조제5항의 개정규정에도 불구하고 이 법 시행일 현재 제27조제3항의 개정규정에 따라 등록되지 아니한 자사 소속 위임직채권추심인을 통하여 채권추심업무를 할 수 있다. 다만, 이 법 시행일부터 3개월 이내에 제27조제3항의 개정규정에 따른 등록을 하여야 하며 같은 기간 경과 후에는 등록되지 아니한 위임직채권추심인을 통하여 채권추심업무를 하여서는 아니 된다.

제11조(협회 설립 등에 관한 경과조치) 이 법 시행 전 종전의 「민법」에 따라 설립된 사단법인 신용정보협회는 제44조의 개정규정에 따라 설립된 신용정보협회로 본다.

제12조(다른 법률의 개정) ① 고용보험 및 산업재해보상보험의 보험료징수 등에 관한 법률 일부를 다음과 같이 개정한다.

제29조의2제1항 각 호 외의 부분 본문 중 "「신용정보의 이용 및 보호에 관한 법률」 제17조제2항제1호의 규정"을 "「신용정보의 이용 및 보호에 관한 법률」 제25조제2항제1호"로 한다.

② 공직자윤리법 일부를 다음과 같이 개정한다.

제6조제5항 전단, 같은 조 제9항 및 제8조제5항 중 "「신용정보의 이용 및 보호에 관한 법률」 제24조"를 각각 "「신용정보의 이용 및 보호에 관한 법률」 제33조"로 한다.

③ 관세법 일부를 다음과 같이 개정한다.

제44조제3항 중 "신용정보업자 또는 신용정보집중기관"을 "신용정보회사 또는 같은 법 제25조에 따른 신용정보집중기관"으로 한다.

④ 국민기초생활 보장법 일부를 다음과 같이 개정한다.

제23조의2제1항 및 제2항 중 "「신용정보의 이용 및 보호에 관한 법률」 제23조제1항"을 각각 "「신용정보의 이용 및 보호에 관한 법률」 제32조제1항"으로 하고, 같은 조 제1항 중 "「신용정보의 이용 및 보호에 관한 법률」 제2조제5호"를 "「신용정보의 이용 및 보호에 관한 법률」 제25조"로 하며, 같은 조 제3항 중 "「신용정보의 이용 및 보호에 관한 법률」 제23조"를 "「신용정보의 이용 및 보호에 관한 법률」 제32조"로 하고, 같은 조 제4항 중 "「신용정보의 이용 및 보호에 관한 법률」 제24조의2"를 "「신용정보의 이용 및 보호에 관한 법률」 제35조"로 한다.

⑤ 국세징수법 일부를 다음과 같이 개정한다.

제7조의2제1항 각 호 외의 부분 본문 중 "신용정보의이용및보호에관한법률 제2조의 규정에 의한 신용정보업자 또는 신용정보집중기관"을 "「신용정보의 이용 및 보호에 관한 법률」 제2조에 따른 신용정보회사 또는 같은 법 제25조에 따른 신용정보집중기관"으로 한다.

⑥ 금융기관부실자산 등의 효율적 처리 및 한국자산관리공사의 설립에 관한 법률 일부를 다음과 같이 개정한다.

제26조제3항 중 "「신용정보의 이용 및 보호에 관한 법률」 제4조의 규정에 의한"을 "「신용정보의 이용 및 보호에 관한 법률」 제4조 및 제5조에 따른"으로 한다.

⑦ 금융지주회사법 일부를 다음과 같이 개정한다.

제48조의2제1항 중 "신용정보의이용및보호에관한법률 제23조 및 제24조제1항의 규정에 불구하고 동법 제23조제1호·제3호 및 제4호의 규정에 의한 개인에 관한 신용정보(이하 "개인신용정보"라 한다)"를 "「금융실명거래 및 비밀보장에 관한 법률」 제4조제2항 및 「신용정보의 이용 및 보호에 관한 법률」 제32조·제33조에도 불구하고 「금융실명거래 및 비밀보장에 관한 법률」 제4조에 따른 금융거래의 내용에 관한 정보 또는 자료 및 「신용정보의 이용 및 보호에 관한 법률」 제32조제1항에 따른 대통령령으로 정하는 개인신용정보(이하 "개인신용정보"라 한다)"로 하고, 같은 조 제3항 중 "신용정보의이용및보호에관한법률 제24조제2항의 규정"을 "「신용정보의 이용 및 보호에 관한 법률」 제32조제7항"으로 한다.

⑧ 기술신용보증기금법 일부를 다음과 같이 개정한다.

제47조의2제1항 및 제2항 단서 중 "신용정보업자"를 각각 "신용정보회사"로 한다.

⑨ 기업구조조정 촉진법 일부를 다음과 같이 개정한다.

제7조제5항 중 "「신용정보의 이용 및 보호에 관한 법률」 제17조제2항제1호"를 "「신용정보의 이용 및 보호에 관한 법률」 제25조제2항제1호"로 한다.

⑩ 기초노령연금법 일부를 다음과 같이 개정한다.

제7조의2제1항 중 "「신용정보의 이용 및 보호에 관한 법률」 제23조제1항"을 "「신용정보의 이용 및 보호에 관한 법률」 제32조제1항"으로, "「신용정보의 이용 및 보호에 관한 법률」 제2조제5호"를 "「신용정보의 이용 및 보호에 관한 법률」 제25조"로 하고, 같은 조 제2항 중 "「신용정보의 이용 및 보호에 관한 법률」 제23조제1항"을 "「신용정보의 이용 및 보호에 관한 법률」 제32조제1항"으로 한다.

제7조의2제3항 중 "「신용정보의 이용 및 보호에 관한 법률」 제23조"를 "「신용정보의 이용 및 보호에 관한 법률」 제32조"로 한다.

제7조의2제4항 중 "「신용정보의 이용 및 보호에 관한 법률」 제24조의2"를 "「신용정보의 이용 및 보호에 관한 법률」 제35조"로 한다.

⑪ 농림수산업자 신용보증법 일부를 다음과 같이 개정한다.

제10조의2제1항 및 제2항 단서 중 "신용정보업자"를 각각 "신용정보회사"로 한다.

⑫ 대부업 등의 등록 및 금융이용자 보호에 관한 법률 일부를 다음과 같이 개정한다.

제4조제6호라목을 다음과 같이 한다.

라. 「신용정보의 이용 및 보호에 관한 법률」 제50조제1항제1호 또는 같은 조 제2항제7호

⑬ 보험업법 일부를 다음과 같이 개정한다.

제115조제1항제2호 중 "동법 제2조제11호에 의한 신용평가업무를"을 "같은 법 제2조제12호에 따른 신용평가업무는"으로 한다.

제176조제11항제2호를 다음과 같이 한다.

2. 「신용정보의 이용 및 보호에 관한 법률」 제33조 각 호에서 정하는 사유에 따른 경우

⑭ 부가가치세법 일부를 다음과 같이 개정한다.

제32조의4제2항 중 "「신용정보의 이용 및 보호에 관한 법률」 제24조의 규정에"를 "「신용정보의 이용 및 보호에 관한 법률」 제33조에도"로 한다.

⑮ 수출보험법 일부를 다음과 같이 개정한다.

제53조제3항 중 "「신용정보의 이용 및 보호에 관한 법률」 제4조제1항 및 제2항에도 불구하고 같은 조 제4항제3호"를 "「신용정보의 이용 및 보호에 관한 법률」 제4조제2항 및 제5조제1항에도 불구하고 같은 법 제4조제1항제3호"로 한다.

<16> 신용보증기금법 일부를 다음과 같이 개정한다.

제32조제1항 본문·단서 및 제2항 단서 중 "신용정보업자"를 각각 "신용정보회사"로 한다.

<17> 외국환거래법 일부를 다음과 같이 개정한다.

제21조제2항 중 "「신용정보의 이용 및 보호에 관한 법률」 제17조에 따른"을 "「신용정보의 이용 및 보호에 관한 법률」 제25조에 따른"으로 한다.

<18> 자산유동화에 관한 법률 일부를 다음과 같이 개정한다.

제10조제1항제2호를 다음과 같이 한다.

2. 「신용정보의 이용 및 보호에 관한 법률」 제4조제1항제1호부터 제3호까지의 업무를 허가받은 신용정보회사

제10조제2항 중 "신용정보의이용및보호에관한법률 제4조의 규정에"를 "「신용정보의 이용 및 보호에 관한 법률」 제4조 및 제5조에도"로, "신용정보의이용및보호에관한법률 제6조제3호의 규정에 의한"을 "「신용정보의 이용 및 보호에 관한 법률」 제4조제1항제3호에 따른"으로 한다.

<19> 주택저당채권유동화회사법 일부를 다음과 같이 개정한다.

제10조제1항제2호를 다음과 같이 한다.

2. 「신용정보의 이용 및 보호에 관한 법률」 제4조제1항제1호부터 제3호까지의 업무를 허가받은 신용정보회사

제10조제2항 중 "신용정보의이용및보호에관한법률 제4조제3항의 규정에"를 "「신용정보의 이용 및 보호에 관한 법률」 제5조제1항에도"로, "동법 제6조제3호의 규정에 의한"을 "같은 법 제4조제1항제3호에 따른"으로 한다.

<20> 질서위반행위규제법 일부를 다음과 같이 개정한다.

제53조제1항 중 "신용정보업자 또는 신용정보집중기관"을 "신용정보회사 또는 같은 법 제25조에 따른 신용정보집중기관"으로 하고, 같은 조 제2항 중 "신용정보업자"를 "신용정보회사"로 한다.

<21> 특정 금융거래정보의 보고 및 이용 등에 관한 법률 일부를 다음과 같이 개정한다.

제10조제2항 중 "「신용정보의 이용 및 보호에 관한 법률」 제17조의 규정에 의한"을 "「신용정보의 이용 및 보호에 관한 법률」 제25조에 따른"으로 한다.

제12조제1항 중 "「신용정보의 이용 및 보호에 관한 법률」 제23조·제27조"를 "「신용정보의 이용 및 보호에 관한 법률」 제32조·제42조"로 하고, 같은 조 제2항 중 "「신용정보의 이용 및 보호에 관한 법률」 제24조의2"를 "「신용정보의 이용 및 보호에 관한 법률」 제35조"로 한다.

<22> 법률 제9415호 한국장학재단 설립 등에 관한 법률 일부를 다음과 같이 개정한다.

제51조제1항 본문ㆍ단서 및 제2항 단서 중 "신용정보업자"를 각각 "신용정보회사"로 한다.

<23> 한국주택금융공사법 일부를 다음과 같이 개정한다.

제45조제1항 각 호 외의 부분 후단 중 "「신용정보의 이용 및 보호에 관한 법률」 제4조제4항의 규정"을 "「신용정보의 이용 및 보호에 관한 법률」 제4조제1항"으로 하고, 같은 항 제3호 및 같은 조 제8항 단서 중 "신용정보업자"를 각각 "신용정보회사"로 한다.

<24> 휴면예금관리재단의 설립 등에 관한 법률 일부를 다음과 같이 개정한다.

제31조제1항 중 "「신용정보의 이용 및 보호에 관한 법률」 제23조"를 "「신용정보의 이용 및 보호에 관한 법률」 제32조"로 한다.

제13조(다른 법령과의 관계) 이 법 시행 당시 다른 법령에서 종전의 「신용정보의 이용 및 보호에 관한 법률」의 규정을 인용한 경우에 이 법 중 그에 해당하는 규정이 있는 경우에는 종전의 규정을 갈음하여 이 법의 해당 규정을 인용한 것으로 본다.

부칙 <제10228호,2010.4.5>

제1조(시행일) 이 법은 공포 후 3개월이 경과한 날부터 시행한다.

제2조 및 제3조 생략

제4조(다른 법률의 개정) ① 부터 ④ 까지 생략

⑤ 신용정보의 이용 및 보호에 관한 법률 일부를 다음과 같이 개정한다.

제5조제1항제5호를 다음과 같이 한다.

5. 「무역보험법」에 따라 설립된 한국무역보험공사

⑥ 부터 ⑨ 까지 생략

제5조 생략

부칙 <제10465호,2011.3.29>

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다. <단서 생략>

제2조부터 제5조까지 생략

제6조(다른 법률의 개정) ①부터 ④까지 생략

⑤ 신용정보의 이용 및 보호에 관한 법률 일부를 다음과 같이 개정한다.

제23조제2항제2호를 다음과 같이 한다.

2. 「개인정보 보호법」

⑥부터 ⑭까지 생략

제7조 생략

부칙 <제10690호,2011.5.19>

이 법은 공포 후 3개월이 경과한 날부터 시행한다.

부칙 <제11690호,2013.3.23>

제1조(시행일) ① 이 법은 공포한 날부터 시행한다.

② 생략

제2조부터 제5조까지 생략

제6조(다른 법률의 개정) ①부터 <696>까지 생략

<697> 신용정보의 이용 및 보호에 관한 법률 일부를 다음과 같이 개정한다.

제24조제1항 각 호 외의 부분 전단 및 후단 중 "행정안전부장관"을 각각 "안전행정부장관"으로 한다.

<698>부터 <710>까지 생략

제7조 생략

부칙 <제11845호,2013.5.28>

제1조(시행일) 이 법은 공포 후 3개월이 경과한 날부터 시행한다. <단서 생략>

제2조부터 제15조까지 생략

제16조(다른 법률의 개정) ①부터 ⑮까지 생략

<16> 신용정보의 이용 및 보호에 관한 법률 일부를 다음과 같이 개정한다.

제2조제12호를 삭제한다.

제4조제1항제4호를 삭제한다.

제5조제2항을 삭제한다.

제6조제2항제1호 중 "신용조회업 및 신용평가업을 각각 또는 함께 하려는"을 "신용조회업을 하려는"으로 한다.

제10조제3항 중 "제22조제1항, 제27조제1항부터 제7항까지 및 제28조를"을 "제22조제1항 및 제27조제1항부터 제7항까지의 규정을"로 한다.

제11조제3호 중 "대리업무, 신용평가회사의 개인신용등급 산정업무 등"을 "대리업무 등"으로 한다.

제12조 중 "신용조사·신용평가"를 "신용조사"로 한다.

제14조제1항제2호 단서 중 "「자본시장과 금융투자업에 관한 법률」 제9조제13항에 따른 증권시장"을 "「자본시장과 금융투자업에 관한 법률」 제8조의2제4항제1호에 따른 증권시장"으로 하고, 같은 항 제3호를 삭제하며, 같은 항 제4호 중 "신용조회업 또는 신용평가업"을 "신용조회업"으로 하고, 같은 항 제6호 중 "경우(신용평가업은 제외한다)"를 "경우"로 하며, 같은 항 제7호를 삭제하고, 같은 조 제2항제3호 중 "경우(신용평가업은 제외한다)"를 "경우"로 하며, 같은 항 제4호 중 "제22조제1항, 제27조제1항 및 제28조를"을 "제22조제1항 및 제27조

제1항을"로 한다.

제5장제3절(제28조부터 제30조까지)을 삭제한다.

제40조제6호를 삭제한다.

제41조제2항 단서 중 "신용평가업을"을 "「자본시장과 금융투자업에 관한 법률」 제335조의3제1항에 따라 신용평가업인가를 받아 신용평가업을"로 한다.

제46조를 삭제한다.

제50조제1항제3호, 제2항제5호 및 제3항제11호·제12호를 각각 삭제한다.

제52조제3항제8호를 삭제한다.

별표 제2호를 삭제한다.

<17>부터 <23>까지 생략

제17조 생략

부칙 <제12844호,2014.11.19>

제1조(시행일) 이 법은 공포한 날부터 시행한다. 다만, 부칙 제6조에 따라 개정되는 법률 중 이 법 시행 전에 공포되었으나 시행일이 도래하지 아니한 법률을 개정한 부분은 각각 해당 법률의 시행일부터 시행한다.

제2조부터 제5조까지 생략

제6조(다른 법률의 개정) ①부터 <248>까지 생략

<249> 신용정보의 이용 및 보호에 관한 법률 일부를 다음과 같이 개정한다.

제24조제1항 각 호 외의 부분 전단 및 후단 중 "안전행정부장관"을 각각 "행정자치부장관"으로 한다.

<250>부터 <258>까지 생략

제7조 생략

부칙 <제13216호,2015.3.11>

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다. 다만, 제20조의2, 제32조, 제33조제3호, 제34조, 제35조, 제38조의2, 제38조의3의 개정규정은 공포 후 1년이 경과한 날부터 시행한다.

제2조(신용정보회사의 출자요건에 관한 적용례) 제14조제1항제2호의 개정규정은 이 법 시행 후 최초로 주식이 「자본시장과 금융투자업에 관한 법률」 제8조의2제4항제1호에 따른 증권시장에 상장되는 신용정보회사부터 적용한다.

제3조(허가 또는 인가의 취소에 관한 적용례) 제14조제1항제5호의 개정규정은 이 법 시행 후 최초로 업무정지처분을 받는 신용정보회사부터 적용한다.

제4조(업무정지에 관한 적용례) ① 제14조제2항제4호 및 제8호의 개정규정은 이 법 시행 후 최초로 위반행위를 한 신용정보회사부터 적용한다.

② 제14조제2항제6호의 개정규정은 이 법 시행 후 최초로 계열회사 등에 신용정보를 제공한 신용조회회사부터 적용한다.

제5조(과징금의 부과에 관한 적용례) 제42조의2의 개정규정은 이 법 시행 후 최초로 위반행위를 한 신용정보회사등부터 적용한다.

제6조(손해배상 책임에 관한 적용례) 제43조의 개정규정은 이 법 시행 후 최초로 신용정보가 유출되어 손해배상 책임을 지는 신용정보회사등이나 그 밖의 신용정보 이용자부터 적용한다.

제7조(법정손해배상 책임에 관한 적용례) 제43조의2의 개정규정은 이 법 시행 후 최초로 신용정보가 유출되어 손해배상 책임을 지는 신용정보회사등이나 그 밖의 신용정보 이용자부터 적용한다.

제8조(신용조회회사의 딸린 업무 및 겸업에 관한 경과조치) ① 이 법 시행 당시 신용조회회사가 종전의 제4조제1항 각 호의 딸린 업무 또는 제11조에 따른 겸업을 하고 있는 경우 이미 체결된 계약에 대하여는 제4조제1항제1호 및 제11조제2항의 개정규정에도 불구하고 이 법 시행 후 3년까지 종전의 규정을 적용한다.

② 신용조회회사는 제4조제1항제1호의 개정규정에도 불구하고 이 법 시행 후 1년 6개월까지 신용정보주체 주소변경의 통보대행 업무를 수행할 수 있다.

제9조(처리위탁에 관한 경과조치) 이 법 시행 당시 종전의 규정에 따라 신용정보의 처리를 위탁한 경우에는 제17조의 개정규정에도 불구하고 종전의 규정에 따른다.

제10조(개인신용정보의 삭제에 관한 경과조치) 제20조의2제2항의 개정규정 시행 당시 상거래관계 종료일부터 5년이 경과한 개인신용정보를 보유한 신용정보제공·이용자는 같은 개정규정에도 불구하고 같은 개정규정 시행 후 3개월 이내에 해당 개인신용정보를 삭제하여야 한다.

제11조(신용정보집중기관의 등록 등에 관한 경과조치) ① 이 법 시행 당시 종전의 규정에 따라 등록한 신용정보집중기관은 제25조의 개정규정에 따라 금융위원회의 허가를 받은 것으로 본다. 다만, 해당 신용정보집중기관은 이 법 시행 후 6개월 이내에 이 법에 따른 요건을 갖추어 금융위원회의 허가를 받아야 한다.

② 이 법 시행 당시 종전의 규정에 따라 종합신용정보집중기관에 둔 신용정보협의회는 제26조의 개정규정에 따른 신용정보집중관리위원회로 본다. 다만, 해당 신용정보집중기관은 제1항 단서에 따라 금융위원회에 허가를 신청하기 전까지 제26조의2의 개정규정에 적합하도록 하여야 한다.

제12조(개인신용정보 제공·활용의 동의에 관한 경과조치) 제32조의 개정규정 시행 당시 종전의 규정에 따라 신용정보제공·이용자가 적법하게 제공·활용하고 있는 개인신용정보의 경우에는 같은 개정규정에 따라 동의를 받은 것으로 본다.

제13조(개인식별정보 제공·이용의 동의에 관한 경과조치) 제34조의 개정규정 시행 당시 종전의 규정에 따라 신용정보제공·이용자가 개인식별정보의 제공·이용에 대한 동의를 받은 경우에는 같은 개정규정에 따라 동의를 받은 것으로 본다.

제14조(벌칙과 과태료에 관한 경과조치) 이 법 시행 전의 행위에 대하여 벌칙이나 과태료의 규정을 적용할 때에는 종전의 규정에 따른다.

제15조(다른 법률의 개정) ① 개발제한구역의 지정 및 관리에 관한 특별조치법 일부를 다음과 같이 개정한다.

제16조의3제3항 단서 중 "「신용정보의 이용 및 보호에 관한 법률」 제32조제5항에도"를 "「신용정보의 이용 및 보호에 관한 법률」 제32조제7항에도"로 한다.

② 금융지주회사법 일부를 다음과 같이 개정한다.

제48조의2제1항 각 호 외의 부분 중 "대통령령으로 정하는 개인신용정보(이하 "개인신용정보"라 한다)를"을 "개인신용정보를"로 하고, 같은 조 제3항 중 "「신용정보의 이용 및 보호에 관한 법률」 제32조제7항"을 "「신용정보의 이용 및 보호에 관한 법률」 제32조제10항"으로 한다.

③ 기초연금법 일부를 다음과 같이 개정한다.

제12조제4항 본문 중 "「신용정보의 이용 및 보호에 관한 법률」 제32조제5항에도"를 "「신용정보의 이용 및 보호에 관한 법률」 제32조제7항에도"로 한다.

④ 대부업 등의 등록 및 금융이용자 보호에 관한 법률 일부를 다음과 같이 개정한다.

제4조제6호라목을 다음과 같이 한다.

라. 「신용정보의 이용 및 보호에 관한 법률」 제50조제2항제1호 또는 같은 조 제3항제3호

⑤ 보험업법 일부를 다음과 같이 개정한다.

제115조제1항제2호를 다음과 같이 한다.

2. 「신용정보의 이용 및 보호에 관한 법률」에 따른 신용정보업

⑥ 아이돌봄 지원법 일부를 다음과 같이 개정한다.

제23조제3항 단서 중 "「신용정보의 이용 및 보호에 관한 법률」 제32조제5항에도"를 "「신용정보의 이용 및 보호에 관한 법률」 제32조제7항에도"로 한다.

⑦ 법률 제12532호 양육비 이행확보 및 지원에 관한 법률 일부를 다음과 같이 개정한다.

제17조제3항 단서 중 "「신용정보의 이용 및 보호에 관한 법률」 제32조제5항에도"를 "「신용정보의 이용 및 보호에 관한 법률」 제32조제7항에도"로 한다.

⑧ 장애인복지법 일부를 다음과 같이 개정한다.

제50조의3제4항 단서 중 "「신용정보의 이용 및 보호에 관한 법률」 제32조제5항에도"를 "「신용정보의 이용 및 보호에 관한 법률」 제32조제7항에도"로 한다.

⑨ 초·중등교육법 일부를 다음과 같이 개정한다.

제60조의6제3항 단서 중 "「신용정보의 이용 및 보호에 관한 법률」 제32조제5항에도"를 "「신용정보의 이용 및 보호에 관한 법률」 제32조제7항에도"로 한다.

⑩ 한국장학재단 설립 등에 관한 법률 일부를 다음과 같이 개정한다.

제50조의3제3항 단서 중 "「신용정보의 이용 및 보호에 관한 법률」 제32조제5항에도"를 "「신용정보의 이용 및 보호에 관한 법률」 제32조제7항에도"로 한다.

⑪ 한부모가족지원법 일부를 다음과 같이 개정한다.

제12조의3제4항 단서 중 "「신용정보의 이용 및 보호에 관한 법률」 제32조제5항에도"를 "「신용정보의 이용 및 보호에 관한 법률」 제32조제7항에도"로 한다.

⑫ 취업 후 학자금 상환 특별법 일부를 다음과 같이 개정한다. <신설 2015.6.22>

제38조제2항 단서 중 "「신용정보의 이용 및 보호에 관한 법률」 제32조제5항에도"를 "「신용정보의 이용 및 보호에 관한 법률」 제32조제7항에도"로 한다.

부칙 <제13337호,2015.6.22>

제1조(시행일) 이 법은 공포한 날부터 시행한다.

제2조부터 제4조까지 생략

제5조(다른 법률의 개정) 법률 제13216호 신용정보의 이용 및 보호에 관한 법률 일부개정법률 일부를 다음과 같이 개정한다.

부칙 제15조에 제12항을 다음과 같이 신설한다.

⑫ 취업 후 학자금 상환 특별법 일부를 다음과 같이 개정한다.

제38조제2항 단서 중 "「신용정보의 이용 및 보호에 관한 법률」 제32조제5항에도"를 "「신용정보의 이용 및 보호에 관한 법률」 제32조제7항에도"로 한다.

부칙 <제14122호,2016.3.29>

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다.

제2조 및 제3조 생략

제4조(다른 법률의 개정) ①부터 ⑬까지 생략

⑭ 신용정보의 이용 및 보호에 관한 법률 일부를 다음과 같이 개정한다.

제5조제1항제3호 중 "「기술신용보증기금법」에 따른 기술신용보증기금"을 "「기술보증기금법」에 따른 기술보증기금"으로 한다.

⑮부터 <24>까지 생략

제5조 생략

[별표] <개정 2015.3.11.>

신용정보회사에 대한 처분 사유(제14조제2항제9호 관련)

1. 제9조제2항에 따른 명령을 위반하여 금융위원회의 승인 없이 취득한 주식을 처분하지 아니한 경우
2. 삭제 <2013.5.28>
3. 제38조제5항에 따른 금융위원회의 시정명령에 따르지 아니한 경우
4. 제45조제2항에 따른 업무 및 재산상황에 관한 보고 등의 명령에 따르지 아니한 경우
5. 제45조제4항에 따른 자료의 제출, 관계자의 출석 및 의견의 진술을 하지 아니한 경우
6. 제45조제7항제4호에 따른 임원에 대한 해임권고 또는 직무정지 요구 및 직원에 대한 면직 요구에 따르지 아니한 경우
7. 제45조제7항제5호에 따른 위반행위에 대한 시정명령을 따르지 아니한 경우
8. 제45조제7항제6호에 따른 신용정보제공의 중지 조치에 따르지 아니한 경우

신용정보의 이용 및 보호에 관한 법률 시행령

[시행 2017.1.10] [대통령령 제27786호, 2017.1.10, 일부개정]

제1조(목적) 이 영은 「신용정보의 이용 및 보호에 관한 법률」에서 위임된 사항과 그 시행에 필요한 사항을 규정함을 목적으로 한다.

제2조(정의) ① 「신용정보의 이용 및 보호에 관한 법률」(이하 "법"이라 한다) 제2조제1호 각 목 외의 부분에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 다른 법령에 따라 공시(公示) 또는 공개된 정보나 다른 법령에 위반됨이 없이 출판물 또는 방송매체나 국가·지방자치단체 또는 공공기관(「공공기관의 정보공개에 관한 법률」 제2조제3호의 기관 중 국가기관 및 지방자치단체를 제외한 기관을 말한다. 이하 이 조에서 같다)의 인터넷 홈페이지 등의 공공매체를 통하여 공시 또는 공개된 정보는 제외한다. <개정 2011.8.17, 2014.2.11, 2015.9.11>

1. 법 제2조제1호가목의 특정 신용정보주체를 식별할 수 있는 정보: 생존하는 개인의 성명, 연락처(주소·전화번호 등을 말한다. 이하 같다), 개인식별번호(제29조 각 호의 번호를 말한다. 이하 같다), 성별, 국적 및 그 밖에 이와 비슷한 정보와 기업(사업을 경영하는 개인 및 법인과 이들의 단체를 말한다. 이하 같다) 및 법인의 상호 및 명칭, 법인등록번호·사업자등록번호 및 고유번호, 본점·영업소 및 기관의 소재지, 설립연월일, 종목, 대표자의 성명·개인식별번호 및 그 밖에 이와 비슷한 정보(제2호부터 제5호까지의 규정의 어느 하나에 해당하는 정보와 결합되는 경우만 해당한다)
2. 법 제2조제1호나목의 신용정보주체의 거래내용을 판단할 수 있는 정보: 대출, 보증, 담보제공, 당좌거래(가계당좌거래를 포함한다), 신용카드, 할부금융, 시설대여와 금융거래 등 상거래와 관련하여 그 거래의 종류, 기간, 금액 및 한도 등에 관한 사항
3. 법 제2조제1호다목의 신용정보주체의 신용도를 판단할 수 있는 정보: 금융거래 등 상거래와 관련하여 발생한 연체, 부도, 대위변제, 대지급과 거짓, 속임수, 그 밖의 부정한 방법에 의한 신용질서 문란행위와 관련된 금액 및 발생·해소의 시기 등에 관한 사항. 이 경우 신용정보주체가 기업인 경우에는 다음 각 목의 어느 하나에 해당하는 자를 포함한다.
   가. 「국세기본법」 제39조제2호에 따른 과점주주로서 최다출자자인 자
   나. 「국세기본법」 제39조제2호에 따른 과점주주인 동시에 해당 기업의 이사 또는 감사로서 그 기업의 채무에 연대보증을 한 자
   다. 해당 기업의 의결권 있는 발행주식총수 또는 지분총액의 100분의 30 이상을 소유하고 있는 자로서 최다출자자인 자

라. 해당 기업의 무한책임사원

4. 법 제2조제1호라목의 신용정보주체의 신용거래능력을 판단할 수 있는 정보: 금융거래 등 상거래에서 신용거래능력을 판단할 수 있는 다음 각 목의 어느 하나에 해당하는 정보

가. 개인의 직업·재산·채무·소득의 총액 및 납세실적

나. 기업 및 법인의 연혁·목적·영업실태·주식 또는 지분보유 현황 등 기업 및 법인의 개황(槪況), 대표자 및 임원에 관한 사항, 판매명세·수주실적 또는 경영상의 주요 계약 등 사업의 내용, 재무제표(연결재무제표를 작성하는 기업의 경우에는 연결재무제표를 포함한다. 이하 같다) 등 재무에 관한 사항과 감사인(「주식회사의 외부감사에 관한 법률」 제3조에 따른 감사인을 말한다. 이하 같다)의 감사의견 및 납세실적

5. 법 제2조제1호마목에 따른 정보로서 다음 각 목의 어느 하나에 해당하는 정보

가. 법원의 성년후견·한정후견·특정후견과 관련된 심판, 실종선고와 관련된 심판, 회생·간이회생·개인회생과 관련된 결정, 파산선고·면책·복권과 관련된 결정, 채무불이행자명부의 등재·말소 결정 및 경매개시결정·경락허가결정 등 경매와 관련된 결정에 관한 정보

나. 국세·지방세·관세 또는 국가채권의 체납 관련 정보

다. 벌금·과태료·과징금 또는 추징금 등의 체납 관련 정보

라. 사회보험료·공공요금 또는 수수료 등 관련 정보

마. 기업의 영업에 관한 정보로서 정부조달 실적 또는 수출·수입액 등의 관련 정보

바. 개인의 주민등록 관련 정보로서 출생·사망·이민·부재에 관한 정보, 주민등록번호·성명의 변경 등에 관한 정보

사. 기업등록 관련 정보로서 설립, 휴업·폐업, 양도·양수, 분할·합병, 주식 또는 지분 변동 등에 관한 정보

아. 다른 법령에 따라 국가, 지방자치단체 또는 공공기관으로부터 받은 행정처분에 관한 정보 중에서 금융거래 등 상거래와 관련된 정보

자. 신용조회회사의 신용정보 제공기록 또는 신용정보주체의 신용회복 등에 관한 사항으로서 금융위원회가 정하여 고시하는 정보

차. 그 밖에 법 제2조제1호가목부터 라목까지의 규정에 따른 정보 및 이 호 가목부터 자목까지의 규정에 따른 정보와 비슷한 정보로서 금융위원회가 정하여 고시하는 정보

카. 신용정보주체가 개인인 경우 그 신용을 판단하기 위하여 법 제2조제1호가목부터 라목까지의 규정에 따른 정보 및 이 호 가목부터 차목까지의 규정에 따른 정보를 활용함으로써 새로이 만들어지는 정보로서 금융위원회가 정하여 고시하는 정보

타. 신용정보주체가 기업 및 법인인 경우 그 신용을 판단하기 위하여 법 제2조제1호가목부터 라목까지의 규정에 따른 정보 및 이 호 가목부터 카목까지의 규정에 따른 정보를 활용함으로써 새로이 만들어지는 정보로서 금융위원회가 정하여 고시하는 정보

파. 신용정보주체가 기업 및 법인인 경우 그 신용을 판단하기 위하여 해당 기업 및 법인의 기술(「기술의 이전 및 사업화 촉진에 관한 법률」 제2조제1호에 따른 기술을 말한다. 이하

같다)과 관련된 기술성·시장성·사업성 등을 종합적으로 평가하고 법 제2조제1호가목부터 라목까지의 규정에 따른 정보 및 이 호 가목부터 타목까지의 규정에 따른 정보와 해당 기술에 관한 정보를 활용함으로써 새로이 만들어지는 정보로서 금융위원회가 정하여 고시하는 정보(이하 "기술신용정보"라 한다)

② 법 제2조제2호에서 "대통령령으로 정하는 정보"란 제1항에 따른 신용정보 중 기업 및 법인에 관한 정보를 제외한 살아 있는 개인에 관한 정보로서 성명·주민등록번호 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보를 포함한다)를 말한다.<개정 2017.1.10>

③ 법 제2조제7호에서 "대통령령으로 정하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.<개정 2015.9.11>

1. 「우체국예금·보험에 관한 법률」에 따른 체신관서
2. 「상호저축은행법」에 따른 상호저축은행중앙회
3. 「중소기업창업 지원법」에 따른 중소기업창업투자회사 및 중소기업창업투자조합
4. 「국채법」 및 「공사채등록법」에 따른 채권등록기관
5. 특별법에 따라 설립된 조합·금고 및 그 중앙회·연합회
6. 특별법에 따라 설립된 공사·공단·은행·보증기금·보증재단 및 그 중앙회·연합회
6의2. 특별법에 따라 설립된 법인 또는 단체로서 다음 각 목의 어느 하나에 해당하는 자
   가. 공제조합
   나. 공제회
   다. 그 밖에 이와 비슷한 법인 또는 단체로서 같은 직장·직종에 종사하거나 같은 지역에 거주하는 구성원의 상호부조, 복리증진 등을 목적으로 구성되어 공제사업을 하는 법인 또는 단체
7. 감사인
8. 그 밖에 금융위원회가 정하여 고시하는 자

④ 법 제2조제11호에서 "대통령령으로 정하는 채권"이란 「민사집행법」 제24조·제26조 또는 제56조에 따라 강제집행을 할 수 있는 금전채권을 말한다.

제3조(신용조사업 및 채권추심업에 딸린 업무) 법 제4조제1항에 따른 신용조사업 및 채권추심업에 딸린 업무는 해당 업(業)을 경영하는 과정에서 발생하는 업무로서 다음 각 호의 업무로 한다.

1. 부동산 및 동산의 임대차 현황 및 가격조사업무
2. 채권자 등에 대한 채권관리시스템 제공 및 구축 관련 자문업무(채권추심업의 경우로 한정한다)
3. 그 밖에 금융위원회가 정하여 고시하는 업무

[전문개정 2015.9.11]

제4조(영업의 허가 신청) 법 제4조제2항에 따른 신용정보업의 허가를 받으려는 자는 금융위원회가 정하여 고시하는 신청서(전자문서로 된 신청서를 포함한다)에 다음 각 호의 서류를 첨부하여 금융위원회에 제출하여야 한다. 이 경우 금융위원회는 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 법인 등기사항증명서를 확인하여야 한다. <개정 2010.5.4, 2011.8.17>

1. 정관
2. 자본금 또는 기본재산의 지분을 적은 서류
3. 재무제표
4. 2년간의 사업계획서 및 예상 수입·지출 계산서
5. 그 밖에 금융위원회가 정하는 서류

제5조(신용정보업별 허가 대상) ① 법 제5조제1항제1호에서 "대통령령으로 정하는 금융기관"이란 다음 각 호의 어느 하나에 해당하는 기관을 말한다. 다만, 제9호부터 제14호까지의 경우에는 그 연합회 또는 중앙회만 말한다. <개정 2010.6.28, 2010.11.15, 2014.12.30, 2015.9.11, 2016.3.11, 2016.5.31, 2016.10.25>

1. 「은행법」에 따라 인가를 받아 설립된 은행(같은 법 제59조에 따라 은행으로 보는 자를 포함한다)
2. 「금융지주회사법」에 따른 금융지주회사
3. 「한국산업은행법」에 따른 한국산업은행
4. 「한국수출입은행법」에 따른 한국수출입은행
5. 「농업협동조합법」 제134조의4에 따른 농협은행

5의2. 「수산업협동조합법」에 따른 수협은행

6. 「중소기업은행법」에 따른 중소기업은행
7. 「한국주택금융공사법」에 따른 한국주택금융공사
8. 「자본시장과 금융투자업에 관한 법률」에 따른 금융투자업자·증권금융회사·종합금융회사·자금중개회사 및 명의개서대행회사
9. 「상호저축은행법」에 따른 상호저축은행과 그 중앙회
10. 「농업협동조합법」에 따른 농업협동조합과 그 중앙회
11. 「수산업협동조합법」에 따른 수산업협동조합과 그 중앙회
12. 「산림조합법」에 따른 산림조합과 그 중앙회
13. 「신용협동조합법」에 따른 신용협동조합과 그 중앙회
14. 「새마을금고법」에 따른 새마을금고와 그 연합회
15. 「보험업법」에 따른 보험회사
16. 「여신전문금융업법」에 따른 여신전문금융회사(「여신전문금융업법」 제3조제3항제1호에 따라 허가를 받거나 등록을 한 자를 포함한다)
17. 「기술보증기금법」에 따른 기술보증기금

18. 「신용보증기금법」에 따른 신용보증기금
19. 「지역신용보증재단법」에 따른 신용보증재단과 그 중앙회
20. 「무역보험법」에 따른 한국무역보험공사
21. 「예금자보호법」에 따른 예금보험공사 및 정리금융회사
22. 외국에서 제1호부터 제20호까지의 금융기관과 유사한 금융업을 경영하는 금융기관
23. 외국 법령에 따라 설립되어 외국에서 법 제4조제1항제1호부터 제3호까지의 업무 중 어느 하나에 해당하는 업무를 수행하는 자

② 삭제 <2015.9.11>

제6조(허가의 세부요건 등) ① 법 제6조제1항 및 제3항에 따라 신용정보업의 허가를 받으려는 자가 갖추어야 할 인력 및 물적 시설의 세부요건은 다음 각 호의 구분에 따른다. <개정 2013.8.27, 2015.9.11>

1. 신용조회업을 하는 경우 다음 각 목의 세부요건을 갖출 것
   가. 상시고용인력에는 공인회계사 또는 3년 이상 신용조회업무(신용정보의 분석에 관한 업무를 포함한다)에 종사하였거나 신용정보집중기관에 근무한 경력이 있는 사람 10명 이상이 포함될 것
   나. 신용정보의 처리를 적정하게 수행할 수 있다고 금융위원회가 정하여 고시하는 정보처리·정보통신설비를 갖출 것
2. 신용조사업과 채권추심업을 각각 또는 함께하는 경우에는 20명 이상의 상시고용인력을 갖출 것
3. 삭제 <2013.8.27>

② 법 제6조제1항제2호에 따른 사업계획은 다음 각 호의 요건에 적합하여야 한다.

1. 수입·지출 전망이 타당하고 실현 가능성이 있을 것
2. 사업계획상의 조직구조 및 관리·운용체계가 사업계획의 추진에 적합하고 이해상충 및 불공정 행위 등 신용정보업을 건전하게 하는 데에 지장을 주지 아니할 것

③ 법 제6조제1항제3호에서 "대통령령으로 정하는 주요출자자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 의결권 있는 발행주식 총수 또는 출자총액을 기준으로 본인 및 그와 「자본시장과 금융투자업에 관한 법률 시행령」 제8조 각 호의 어느 하나에 해당하는 관계에 있는 자(이하 "특수관계인"이라 한다)가 누구의 명의로 하든지 자기의 계산으로 소유하는 주식의 수 또는 출자지분이 가장 많은 경우의 그 본인(이하 "최대주주"라 한다)
2. 최대주주가 법인인 경우에는 다음 각 목의 어느 하나에 해당하는 자
   가. 최대주주인 법인의 최대주주(최대주주인 법인을 사실상 지배하는 자가 그 법인의 최대주주와 다른 경우에는 그 사실상 지배하는 자를 포함한다)
   나. 최대주주인 법인의 대표자
3. 최대주주의 특수관계인인 주주 또는 출자자

4. 누구의 명의로 하든지 자기의 계산으로 소유한 주식 또는 출자지분의 합계액이 의결권 있는 발행주식 총수 또는 출자총액의 100분의 10 이상에 해당하는 자
5. 임원의 임면 등 해당 법인의 주요 경영사항에 대하여 사실상 영향력을 행사하고 있는 주주 또는 출자자로서 다음 각 목의 어느 하나에 해당하는 자
가. 단독으로 또는 다른 주주나 출자자와의 합의·계약 등에 따라 대표이사 또는 이사의 과반수를 선임한 주주 또는 출자자
나. 경영전략, 조직 변경 등 주요 의사 결정이나 업무 집행에 지배적인 영향력을 행사한다고 인정되는 자로서 금융위원회가 정하는 주주 또는 출자자

④ 제3항에 따른 주요출자자는 별표 1의 요건에 적합하여야 한다.

제7조(자본금) 법 제6조제2항제2호에서 "대통령령으로 정하는 금액"이란 30억원을 말한다.

제8조(신고 및 보고 사항) ① 법 제8조 본문에서 "대통령령으로 정하는 사항"이란 다음 각 호의 사항을 말한다.

1. 자본금 또는 기본재산의 감소
2. 상호 등 정관의 변경

② 법 제8조 단서에서 "대통령령으로 정하는 경미한 사항"이란 다음 각 호의 사항을 말한다.

1. 대표자 및 임원의 변경
2. 법령의 개정 내용을 반영하거나 법령에 따라 인가·허가받은 내용을 반영하는 사항
3. 정관의 실질적인 내용이 변경되지 아니하는 조문체계의 변경, 자구(字句) 수정 등에 관한 사항

제9조(지배주주의 변경승인 등) ① 법 제9조제1항에서 "대통령령으로 정하는 지배주주"란 다음 각 호의 자를 말한다. 다만, 국가, 「예금자보호법」에 따른 예금보험공사 및 의결권 있는 주식의 100분의 1 미만 보유자는 제외한다. <개정 2011.8.17>

1. 신용조사회사(법 제4조에 따라 신용조사업의 허가를 받은 자를 말한다. 이하 같다), 채권추심회사(법 제4조에 따라 채권추심업의 허가를 받은 자를 말한다. 이하 같다), 신용조회회사(법 제4조에 따라 신용조회업의 허가를 받은 자를 말한다. 이하 같다)의 경우에는 다음 각 목의 자
가. 제6조제3항제1호 및 제3호 또는 제5호에 해당하는 주요출자자
나. 누구의 명의로 하든지 자기의 계산으로 소유한 주식 또는 출자지분의 합계액이 의결권 있는 발행주식 총수 또는 출자총액의 100분의 30 이상에 해당하는 자
2. 삭제 <2013.8.27>

② 법 제9조제1항에서 "대통령령으로 정하는 요건"이란 별표 1에 따른 주요출자자 요건을 말한다.

③ 법 제9조제1항에 따른 승인을 받으려는 자는 금융위원회가 정하여 고시하는 승인신청서에 다음 각 호의 서류를 첨부하여 금융위원회에 제출하여야 한다.<개정 2011.8.17, 2015.9.11>

1. 정관(이에 준하는 것을 포함하며, 법인인 경우만 해당한다)
2. 외국 기업인 경우에는 법인 등기사항증명서에 준하는 서류
3. 최근 사업연도 말 현재 재무제표 또는 최근 사업연도 말 이후 반기(半期)가 지난 경우에는 반기재무제표(법인인 경우만 해당한다)
4. 제3호에 따른 재무제표에 대한 감사인의 감사보고서 및 검토보고서
5. 그 밖에 승인요건의 심사에 필요한 서류로서 금융위원회가 정하는 서류

④ 제3항에 따른 승인신청서를 접수한 금융위원회는 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 다음 각 호의 행정정보를 확인하여야 한다.<개정 2010.5.4, 2010.11.2, 2011.8.17>

1. 법인 등기사항증명서(국내 법인인 경우만 해당한다)
2. 주민등록표 등본 또는 사업자등록증
3. 지배주주가 되려는 자의 주식 취득대상 신용정보회사의 법인 등기사항증명서

⑤ 금융위원회는 제3항에 따른 승인신청서를 접수한 경우에는 그 내용을 심사하여 60일 이내에 그 승인 여부를 결정하고, 그 결과와 이유를 지체 없이 신청인에게 문서로 통지하여야 한다. 이 경우 승인신청서에 흠이 있는 경우에는 보완을 요구할 수 있다.

⑥ 제5항에 따른 심사기간을 계산할 때에는 승인신청서 흠의 보완기간 등 금융위원회가 정하는 기간은 심사기간에 넣지 아니한다.

⑦ 금융위원회는 법 제9조제2항에 따라 승인 없이 취득한 주식의 처분을 명하는 경우에는 처분 대상 주식의 수, 처분 기한 등을 명시한 서면으로 하여야 한다.

⑧ 제1항부터 제7항까지에서 규정한 사항 외에 변경승인 신청의 방법 및 절차, 제2항에 따른 요건의 구체적인 기준 등에 관하여 필요한 사항은 금융위원회가 정하여 고시한다.

제10조(신용정보업의 양도·양수 등의 인가) ① 금융위원회는 법 제10조제1항에 따라 신용정보업의 양도·양수 또는 분할이나 합병의 인가를 하려는 경우에는 다음 각 호의 구분에 따른 기준에 적합한지를 심사하여야 한다.

1. 양도의 경우
   가. 해당 신용정보회사의 경영 및 재무 상태 등에 비추어 부득이한 경우일 것
   나. 신용정보주체의 보호 및 건전한 신용질서 유지에 지장을 주지 않을 것
   다. 「상법」 및 그 밖의 관계 법령에 따른 절차 이행에 하자가 없을 것
2. 양수·분할·합병의 경우
   가. 신용정보업의 효율화 및 건전한 신용질서의 유지에 지장을 주지 않을 것
   나. 사업의 양수·분할·합병에 따른 영업계획 및 조직운영계획이 적절할 것
   다. 사업의 양수·분할·합병에 따른 신용정보회사의 소유구조 변경이 법령에 적합할 것
   라. 「상법」 및 그 밖의 관계 법령에 따른 절차 이행에 하자가 없을 것

② 금융위원회는 법 제10조제1항에 따른 인가의 세부요건, 신청서류, 그 밖에 필요한 사항을 정하여 고시할 수 있다.

제11조(겸업) 법 제11조제1항제2호에서 "대통령령으로 정하는 경우"란 다음 각 호의 어느 하나에 해당하는 경우를 말한다. <개정 2015.9.11>

1. 「자산유동화에 관한 법률」 제10조에 따라 자산관리자가 부채증명서의 발급 대행을 채권추심회사에 의뢰한 경우 등 관계 법령에서 허용한 경우
2. 외국인인 채권자가 부채증명서의 발급 대행을 채권추심회사에 의뢰한 경우

제11조의2(신용조회회사에 조사·분석 등을 의뢰할 수 있는 공공단체의 범위) 법 제11조제2항 단서에서 "대통령령으로 정하는 공공단체"란 다음 각 호의 어느 하나에 해당하는 기관을 말한다. <개정 2016.9.22>

1. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관
2. 국가 또는 지방자치단체가 자본금·기금 또는 경비를 투자·출연 또는 보조하는 기관으로서 금융위원회가 정하여 고시하는 기관
3. 특별법에 따라 설립된 특수법인
4. 「어음법」 및 「수표법」에 따라 지정된 어음교환소와 「전자어음의 발행 및 유통에 관한 법률」 제3조에 따라 지정된 전자어음관리기관
5. 「초·중등교육법」, 「고등교육법」 또는 그 밖에 다른 법률에 따라 설치된 각급 학교와 「산업교육진흥 및 산학연협력촉진에 관한 법률」 제25조에 따라 설립된 산학협력단
6. 「보험업법」에 따른 보험요율 산출기관
7. 「서민의 금융생활 지원에 관한 법률」 제56조에 따른 신용회복위원회
8. 법 제25조에 따라 금융위원회로부터 허가를 받은 신용정보집중기관
9. 그 밖에 금융위원회가 정하여 고시하는 기관

[본조신설 2015.9.11]

제12조(허가 등의 취소 유예) 법 제14조제1항 단서에서 "대통령령으로 정하는 사유"란 신용정보회사가 법 제14조제1항제2호부터 제4호까지 또는 같은 항 제9호에 따른 허가 또는 인가의 취소사유에 해당하는 경우를 말한다. 다만, 취소사유가 해소될 가능성이 매우 적거나 공익을 해칠 우려가 있는 등 시정명령의 실익(實益)이 없다고 인정되는 경우는 제외한다.

제13조(수집·조사 및 처리의 제한) 법 제16조제2항에서 "대통령령으로 정하는 목적"이란 다음 각 호의 어느 하나에 해당하는 자가 개인의 질병에 관한 정보를 그 정보가 필요한 보험계약·공제계약 및 보험금·공제금 지급업무와 관련하여 이용하는 것을 말한다. <개정 2015.9.11>

1. 「보험업법」에 따른 보험회사
2. 「우체국예금·보험에 관한 법률」에 따른 체신관서
3. 특별법에 따라 설립된 법인 또는 단체로서 다음 각 목의 어느 하나에 해당하는 자
   가. 공제조합
   나. 공제회
   다. 그 밖에 이와 비슷한 법인 또는 단체로서 같은 직장·직종에 종사하거나 같은 지역에 거주하는 구성원의 상호부조, 복리증진 등을 목적으로 구성되어 공제사업을 하는 법인 또는

단체

제14조(수집된 신용정보 처리의 위탁) ① 법 제17조제2항에서 "일정한 금액 이상의 자본금 등 대통령령으로 정하는 일정한 요건을 갖춘 자"란 자본금 또는 자본총액(대차대조표상의 자산총액에서 부채총액을 뺀 금액을 말한다)이 1억원 이상인 기업으로서 다음 각 호의 어느 하나에 해당하는 자를 말한다. <개정 2015.9.11, 2016.3.29>

1. 법 제20조제3항 본문에 따라 신용정보관리·보호인을 지정한 자
2. 「개인정보 보호법」 제31조에 따라 개인정보 보호책임자를 지정한 자
3. 「전자금융거래법」 제21조의2에 따라 정보보호최고책임자를 지정한 자
4. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제27조에 따라 개인정보 관리책임자를 지정한 자

② 법 제17조제3항에서 "대통령령으로 정하는 자"란 신용정보회사, 신용정보집중기관 및 제5조제1항에 따른 금융기관 중 금융위원회가 정하여 고시하는 자를 말한다.

③ 법 제17조제3항에 따라 신용정보의 처리를 위탁하려는 자는 위탁계약 체결 예정일부터 7영업일 이전에 금융위원회가 정하여 고시하는 서식에 따라 제공하는 신용정보의 범위, 제공 목적 및 기간과 고객정보 관리체계 등을 금융위원회에 알려야 한다. 다만, 미리 알려야 할 필요성이 크지 아니한 경우로서 금융위원회가 정하여 고시하는 경우에는 위탁계약을 체결한 날부터 금융위원회가 정하여 고시하는 기간 이내에 알려야 한다.<개정 2015.9.11>

④ 법 제17조제4항에 따라 신용정보회사등이 개인신용정보를 제공하는 경우 다음 각 호의 구분에 따른 보호조치를 하여야 한다.<신설 2015.9.11>

1. 정보통신망 또는 보조저장매체를 통하여 제공하는 경우: 금융위원회가 정하여 고시하는 절차와 방법에 따른 보안서버의 구축 또는 암호화, 그 밖에 금융위원회가 정하여 고시하는 보호조치
2. 제1호 외의 방법으로 제공하는 경우: 봉함(封緘), 그 밖에 금융위원회가 정하여 고시하는 보호조치

⑤ 법 제17조제5항에 따라 신용정보회사등은 수탁자와 위탁계약을 체결하거나 갱신하는 경우에는 연 1회 이상(위탁계약기간이 1년 미만인 경우에는 그 기간 동안 1회 이상을 말한다. 이하 이 항에서 같다) 신용정보의 분실·도난·유출·변조·훼손의 방지 및 안전한 신용정보의 처리에 관하여 수탁자의 소속 임직원에 대한 교육을 실시한다는 내용을 위탁계약에 반영하여야 하며, 그 위탁계약에 따라 교육을 실시하여야 한다. 이 경우 수탁자가 연 1회 이상 그 소속 임직원에 대한 교육을 실시한다는 내용이 위탁계약에 반영되어 있고, 신용정보회사등이 수탁자가 그 위탁계약에 따라 해당 교육을 실시한 사실을 확인한 경우에는 신용정보회사등이 수탁자의 소속 임직원에게 교육을 실시한 것으로 본다.<신설 2015.9.11>

⑥ 제3항부터 제5항까지의 규정에서 정한 사항 외에 위탁계약에 반영하여야 할 세부사항, 그 밖에 수집된 신용정보의 처리의 위탁에 필요한 구체적 사항은 금융위원회가 정하여 고시한다. <신설 2015.9.11>

[제목개정 2015.9.11]

제15조(신용정보의 정확성 및 최신성의 유지) ① 법 제18조제1항에 따라 신용정보제공·이용자는 신용정보를 신용정보집중기관 또는 신용조회회사에 제공하려는 경우에는 그 정보의 정확성을 확인하여 사실과 다른 정보를 등록해서는 아니 된다.

② 신용정보집중기관과 신용조회회사는 등록되는 신용정보의 정확성을 점검할 수 있는 기준 및 절차를 마련하고 이에 따라 등록되는 신용정보의 정확성을 점검·관리하여야 한다.

③ 신용정보회사, 신용정보집중기관 및 신용정보제공·이용자(이하 "신용정보회사등"이라 한다)는 신용정보의 정확성과 최신성이 유지될 수 있도록 금융위원회가 정하여 고시하는 기준과 절차에 따라 신용정보를 등록·변경·관리하여야 한다.

④ 법 제18조제2항에 따라 등록·관리 대상에서 삭제하여야 하는 신용정보의 종류는 다음 각 호와 같다.<개정 2011.8.17, 2015.9.11>

1. 제2조제1항제3호에 따른 신용정보 중 연체, 부도, 대위변제 및 대지급과 관련된 정보
2. 제2조제1항제3호에 따른 신용정보 중 신용질서 문란행위와 관련된 정보
3. 제2조제1항제5호가목에 따른 신용정보 중 법원의 파산선고·면책·복권 결정 및 회생·간이회생·개인회생의 결정과 관련된 정보
4. 제2조제1항제5호나목 및 다목에 따른 체납 관련 정보
5. 제2조제1항제5호라목에 따른 신용정보 중 체납 관련 정보
6. 그 밖에 제1호부터 제5호까지의 정보와 유사한 형태의 불이익정보로서 금융위원회가 정하여 고시하는 신용정보

⑤ 제4항 각 호에 따른 신용정보의 활용기간 및 보존기간은 3년 이상 5년 이내의 범위에서 금융위원회가 정하여 고시한다. 다만, 금융위원회는 신용정보의 특성, 활용용도 및 활용빈도 등을 고려하여 그 활용기간 및 보존기간을 단축할 수 있다.<신설 2011.8.17>

⑥ 제4항 각 호에 따른 신용정보의 삭제 방법, 기준 및 절차 등에 관하여 필요한 세부사항은 금융위원회가 정하여 고시한다.<신설 2011.8.17>

제16조(기술적·물리적·관리적 보안대책의 수립) ① 법 제19조제1항에 따라 신용정보회사등은 신용정보전산시스템의 안전보호를 위하여 다음 각 호의 사항이 포함된 기술적·물리적·관리적 보안대책을 세워야 한다.

1. 신용정보에 제3자가 불법적으로 접근하는 것을 차단하기 위한 침입차단시스템 등 접근통제장치의 설치·운영에 관한 사항
2. 신용정보전산시스템에 입력된 정보의 변경·훼손 및 파괴를 방지하기 위한 사항
3. 신용정보 취급·조회 권한을 직급별·업무별로 차등 부여하는 데에 관한 사항 및 신용정보 조회기록의 주기적인 점검에 관한 사항
4. 그 밖에 신용정보의 안정성 확보를 위하여 필요한 사항

② 금융위원회는 제1항 각 호에 따른 사항의 구체적인 내용을 정하여 고시할 수 있다.

제16조의2(신용정보회사등의 기록보존) 신용정보회사등은 법 제20조제2항에 따라 다음 각 호의 구분에 따른 사항에 대한 기록을 3년간 보존하여야 한다.

1. 개인신용정보를 수집·이용한 경우: 그 정보를 수집·이용한 자, 수집·이용한 날짜, 수집·이용한 정보의 내용 및 수집·이용한 사유와 근거
2. 개인신용정보를 제공한 경우: 그 정보를 제공한 자, 제공한 날짜, 제공한 정보의 내용 및 제공한 사유와 근거
3. 개인신용정보를 폐기한 경우: 그 정보를 폐기한 자, 폐기한 날짜, 폐기한 정보의 내용 및 폐기한 사유와 근거

[본조신설 2015.9.11]

제17조(신용정보관리·보호인의 지정 등) ① 법 제20조제3항 본문에서 "대통령령으로 정하는 신용정보제공·이용자"란 제5조제1항제1호부터 제21호까지 및 제21조제2항제1호부터 제21호까지의 규정에 해당하는 자를 말한다. <개정 2015.9.11>

② 법 제20조제3항 단서에서 "총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.<개정 2015.9.11>

1. 법 제25조제2항제1호에 따른 종합신용정보집중기관(이하 "종합신용정보집중기관"이라 한다)
2. 신용조회회사
3. 신용조사회사, 채권추심회사 및 제1항에서 정하는 자로서 직전 사업연도 말 기준으로 총자산이 2조원 이상이고 상시 종업원 수가 300명 이상인 자. 이 경우 상시 종업원 수의 산정방식은 금융위원회가 정하여 고시한다.

③ 법 제20조제3항 본문에 따라 지정하는 신용정보관리·보호인은 다음 각 호의 어느 하나에 해당하는 사람으로 하여야 한다.<개정 2015.9.11>

1. 사내이사
2. 집행임원(「상법」 제408조의2에 따라 집행임원을 둔 경우로 한정한다)
3. 「상법」제401조의2제1항제3호에 해당하는 자로서 신용정보의 제공·활용·보호 및 관리 등에 관한 업무집행 권한이 있는 사람
4. 그 밖에 신용정보의 제공·활용·보호 및 관리 등을 총괄하는 위치에 있는 직원

④ 법 제20조제3항 단서에 따라 지정하는 신용정보관리·보호인은 제3항제1호부터 제3호까지의 규정의 어느 하나에 해당하는 사람으로 하여야 한다.<개정 2015.9.11>

⑤ 제3항 및 제4항에도 불구하고 신용정보회사등은 다른 법령에 따라 준법감시인을 두는 경우에는 그를 신용정보관리·보호인으로 지정할 수 있다. 다만, 법 제20조제3항 단서에 해당하는 경우 신용정보관리·보호인으로 지정될 수 있는 준법감시인은 제3항제1호부터 제3호까지의 규정의 어느 하나에 해당하는 사람으로 하여야 한다.<신설 2015.9.11>

⑥ 제5항에 따라 준법감시인을 신용정보관리·보호인으로 지정한 경우에는 법 제20조제4항 각 호의 업무에 관한 사항을 준법감시인 선임의 근거가 된 법령에 따른 내부통제기준에 반영하여야 한다.<신설 2015.9.11>

제17조의2(개인신용정보의 관리방법 등) ① 신용정보제공·이용자는 법 제20조의2제1항에 따라 다음 각 호의 구분에 따른 방법으로 금융거래 등 상거래관계(고용관계는 제외한다. 이하 같다)가 종료된 신용정보주체의 개인신용정보를 관리하여야 한다.

1. 금융거래 등 상거래관계의 설정 및 유지 등에 필수적인 개인신용정보의 경우: 다음 각 목의 방법
   가. 상거래관계가 종료되지 아니한 다른 신용정보주체의 정보와 별도로 분리하는 방법
   나. 금융위원회가 정하여 고시하는 절차에 따라 신용정보제공·이용자의 임직원 중에서 해당 개인신용정보에 접근할 수 있는 사람을 지정하는 방법
   다. 그 밖에 해당 신용정보주체의 개인신용정보가 안전하게 보호될 수 있는 방법으로서 금융위원회가 정하여 고시하는 방법
2. 제1호 외의 개인신용정보의 경우: 그 정보를 모두 삭제하는 방법

② 신용정보제공·이용자는 금융거래 등 상거래관계가 종료된 경우 제1항 각 호의 구분에 따른 필수적인 개인신용정보와 그 밖의 개인신용정보로 구분한 때에는 다음 각 호의 사항 등을 고려하여야 한다.

1. 해당 개인신용정보가 없었다면 그 종료된 상거래관계가 설정·유지되지 아니하였을 것인지 여부
2. 해당 개인신용정보가 그 종료된 상거래관계에 따라 신용정보주체에게 제공된 재화 또는 서비스(신용정보주체가 그 신용정보제공·이용자에게 신청한 상거래관계에서 제공하기로 한 재화 또는 서비스를 그 신용정보제공·이용자와 별도의 계약 또는 약정 등을 체결한 제3자가 신용정보주체에게 제공한 경우를 포함한다)와 직접적으로 관련되어 있는지 여부
3. 해당 개인신용정보를 삭제하는 경우 법 또는 다른 법령에 따른 의무를 이행할 수 없는지 여부

③ 법 제20조의2제2항제3호에서 "대통령령으로 정하는 경우"란 다음 각 호의 어느 하나에 해당하는 경우를 말한다.<개정 2016.9.22>

1. 휴면예금(「서민의 금융생활 지원에 관한 법률」 제2조제3호에 따른 휴면예금을 말한다)의 지급을 위하여 필요한 경우
2. 대출사기, 보험사기, 거짓이나 부정한 방법으로 알아낸 타인의 신용카드 정보를 이용한 거래, 그 밖에 건전한 신용질서를 저해하는 행위를 방지하기 위하여 그 행위와 관련된 신용정보주체의 개인신용정보가 필요한 경우
3. 위험관리체제의 구축과 법 제4조제1항제1호나목에 따른 신용평가모형 및 위험관리모형의 개발을 위하여 필요한 경우. 이 경우 다른 법률에 따른 의무를 이행하기 위하여 불가피한 경우 등을 제외하고 개인인 신용정보주체를 식별할 수 없도록 조치하여야 한다.
4. 신용정보제공·이용자 또는 제3자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 신용정보주체의 권리보다 우선하는 경우. 이 경우 신용정보제공·이용자 또는 제3자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우로 한정한다.

5. 신용정보주체가 개인신용정보(제15조제4항 각 호의 개인신용정보는 제외한다)의 삭제 전에 그 삭제를 원하지 아니한다는 의사를 명백히 표시한 경우

④ 법 제20조의2제1항 및 제2항에 따른 금융거래 등 상거래관계가 종료된 날은 신용정보제공·이용자와 신용정보주체 간의 상거래관계가 관계 법령, 약관 또는 합의 등에 따라 계약기간의 만료, 해지권·해제권·취소권의 행사, 소멸시효의 완성, 변제 등으로 인한 채권의 소멸, 그 밖의 사유로 종료된 날로 한다.

⑤ 신용정보제공·이용자는 법 제15조제2항 각 호 외의 부분 본문 및 법 제32조제2항 전단에 따른 동의를 받을 때 제4항에 따른 금융거래 등 상거래관계가 종료된 날을 신용정보주체에게 알려야 한다.

⑥ 신용정보제공·이용자는 제1항제2호 및 법 제20조의2제2항 각 호 외의 부분 본문에 따라 신용정보주체의 개인신용정보를 삭제하는 경우 그 삭제된 개인신용정보가 복구 또는 재생되지 아니하도록 조치하여야 한다.

⑦ 법 제20조의2제3항에 따라 신용정보제공·이용자가 개인신용정보를 관리하는 경우에는 제1항제1호 각 목의 방법에 따른다.

[본조신설 2015.9.11]

제18조(신용조회업 종사자의 결격요건) 법 제22조제1항제7호에서 "대통령령으로 정하는 자"란 허가·인가 등의 취소 원인이 되는 사유가 발생하였을 당시의 임직원(「금융산업의 구조개선에 관한 법률」 제14조에 따라 허가·인가 등이 취소된 법인 또는 회사의 경우에는 같은 법 제10조에 따른 적기시정조치의 원인이 되는 사유 발생 당시의 임직원)으로서 다음 각 호의 어느 하나에 해당하는 사람을 말한다. <개정 2015.9.11>

1. 감사 또는 감사위원회의 위원
2. 허가·인가 등의 취소 원인이 되는 사유의 발생과 관련하여 위법 또는 부당한 행위로 금융위원회 또는 금융감독원(「금융위원회의 설치 등에 관한 법률」에 따른 금융감독원을 말한다. 이하 같다)의 원장으로부터 주의, 경고, 문책, 직무정지, 해임요구 또는 그 밖의 조치를 받은 임원
3. 허가·인가 등의 취소 원인이 되는 사유의 발생과 관련하여 위법 또는 부당한 행위로 금융위원회 또는 금융감독원의 원장(이하 "금융감독원장"이라 한다)으로부터 정직요구 이상에 해당하는 조치를 받은 직원
4. 제2호 또는 제3호에 따른 제재 대상자로서 그 제재를 받기 전에 사임하거나 사직한 사람

제18조의2(신용정보 등의 보고) ① 신용조회회사는 법 제22조의2에 따라 전년도에 수행한 다음 각 호의 업무내용을 그 다음 해 1월 31일까지 금융위원회에 보고하여야 한다.

1. 신용정보의 수집·조사 대상자 및 수집·조사·처리 정보의 종류 등에 관한 사항
2. 신용정보의 제공 대상자 및 제공 범위 등에 관한 사항
3. 신용정보의 활용기간 및 보존기간 등에 관한 사항

② 금융위원회는 제1항에 따른 보고내용이 건전한 신용질서 또는 금융소비자의 권익에 반하는 것으로 판단되는 경우에는 신용조회회사에 해당 보고내용과 관련된 업무처리절차 등을 개선하도록 권고할 수 있다.

[본조신설 2011.8.17]

제19조(공공기관에 대한 신용정보의 제공 요청 등) ① 법 제23조제2항 각 호 외의 부분 전단에서 "대통령령으로 정하는 공공단체"란 다음 각 호의 어느 하나에 해당하는 기관을 말한다. <개정 2015.9.11, 2016.9.22>

1. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관으로서 금융위원회가 정하여 고시하는 기관
2. 국가 또는 지방자치단체가 자본금·기금 또는 경비를 투자·출연 또는 보조하는 기관으로서 금융위원회가 정하여 고시하는 기관
3. 특별법에 따라 설립된 특수법인으로서 금융위원회가 정하여 고시하는 기관
4. 「어음법」 및 「수표법」에 따라 지정된 어음교환소와 「전자어음의 발행 및 유통에 관한 법률」 제3조에 따라 지정된 전자어음관리기관
5. 「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 각급 학교
6. 「보험업법」에 따른 보험요율산출기관
7. 「서민의 금융생활 지원에 관한 법률」 제56조에 따른 신용회복위원회

② 법 제23조제2항 각 호 외의 부분 전단에서 "대통령령으로 정하는 신용정보"란 다음 각 호의 신용정보를 말한다. 이 경우 신용정보의 구체적인 제공 범위는 공공기관(국가·지방자치단체 또는 제1항에 따른 공공단체를 말한다. 이하 이 조에서 같다)의 장과 신용정보집중기관이 협의하여 결정한다.<개정 2015.9.11>

1. 고용보험, 산업재해보상보험, 국민건강보험 및 국민연금에 관한 정보로서 보험료 납부 정보
2. 전기사용에 관한 정보로서 전력사용량 및 전기요금 납부 정보
3. 정부 납품 실적 및 납품액
4. 사망자 정보, 주민등록번호 및 성명 변경 정보
5. 국외 이주신고 및 이주포기신고의 정보
6. 공공기관이 보유하고 있는 신용정보로서 관계 법령에 따라 신용정보집중기관에 제공할 수 있는 신용정보

③ 법 제23조제2항에 따라 제2항 각 호의 정보를 제공받으려는 신용정보집중기관은 공공기관의 장에게 신용정보의 제공을 문서로 요청하여야 하며, 공공기관의 장은 그 신용정보를 제공하려는 경우에는 문서 또는 주기적 파일로 제공하거나 「전자정부법」 제37조제1항에 따른 행정정보공동이용센터 등을 통하여 제공하여야 한다.<개정 2010.5.4, 2015.9.11>

④ 금융위원회는 공공기관의 장이 제공하는 정보의 활용 필요성 등을 고려하여 해당 정보의 등록 및 이용기준 등을 정하여 고시하여야 한다.

⑤ 법 제23조제3항에서 "대통령령으로 정하는 신용정보의 이용자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.<개정 2015.9.11>

1. 제5조제1항제1호부터 제20호까지의 규정에 따른 금융기관
2. 제21조제2항 각 호의 어느 하나에 해당하는 자
3. 신용조회회사

[제목개정 2015.9.11]

제20조(주민등록전산정보자료의 이용) 법 제24조제1항에서 "대통령령으로 정하는 신용정보제공·이용자"란 제5조제1항 각 호의 어느 하나에 해당하는 자를 말한다.

제21조(신용정보의 집중관리·활용) ① 법 제25조제1항에 따라 신용정보집중기관으로 허가를 받으려는 자는 금융위원회가 정하여 고시하는 신청서(전자문서로 된 신청서를 포함한다)에 다음 각 호의 사항을 적고 정관을 첨부하여 금융위원회에 제출하여야 한다. 이 경우 금융위원회는 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 법인 등기사항증명서를 확인하여야 한다. <개정 2010.5.4, 2011.8.17, 2015.9.11>

1. 기관의 명칭, 주소 및 대표자의 성명
2. 집중관리·활용하려는 신용정보의 범위 및 교환 대상자
3. 집중관리·활용의 필요성

② 법 제25조제2항제1호에서 "대통령령으로 정하는 금융기관"이란 제5조제1항제1호부터 제20호까지의 금융기관 및 다음 각 호에 해당하는 기관을 말한다.<개정 2011.1.17, 2012.1.25, 2015.6.30, 2015.9.11, 2016.3.11, 2016.7.6, 2016.9.22>

1. 「건설산업기본법」에 따른 공제조합
2. 「국채법」 및 「공사채등록법」에 따른 채권등록기관
3. 「한국농수산식품유통공사법」에 따른 한국농수산식품유통공사
4. 「서민의 금융생활 지원에 관한 법률」 제56조에 따른 신용회복위원회
5. 「산업재해보상보험법」에 따른 근로복지공단
6. 「소프트웨어산업 진흥법」에 따른 소프트웨어공제조합
7. 「엔지니어링산업 진흥법」에 따른 엔지니어링공제조합
8. 「예금자보호법」에 따른 정리금융회사
9. 「우체국예금·보험에 관한 법률」에 따른 체신관서
10. 「전기공사공제조합법」에 따른 전기공사공제조합
11. 「주택도시기금법」에 따른 주택도시보증공사
12. 「중소기업진흥에 관한 법률」에 따른 중소기업진흥공단
13. 「중소기업창업 지원법」에 따른 중소기업창업투자회사 및 중소기업창업투자조합
14. 「중소기업협동조합법」에 따른 중소기업중앙회
15. 「한국장학재단 설립 등에 관한 법률」에 따른 한국장학재단
16. 「금융회사부실자산 등의 효율적 처리 및 한국자산관리공사의 설립에 관한 법률」에 따른 한국자산관리공사

17. 「상법」에 따라 설립된 주식회사 국민행복기금
18. 「서민의 금융생활 지원에 관한 법률」 제3조에 따른 서민금융진흥원
19. 「대부업 등의 등록 및 금융이용자 보호에 관한 법률」 제3조제2항에 따라 금융위원회에 등록한 대부업자등
20. 「산업발전법」 제40조제1항제1호에 따른 자본재공제조합
21. 「소상공인 보호 및 지원에 관한 법률」 제17조제1항에 따른 소상공인시장진흥공단
22. 「자산유동화에 관한 법률」에 따라 금융위원회에 자산유동화계획을 등록한 유동화전문회사

③ 종합신용정보집중기관을 통하여 집중관리·활용되는 신용정보의 범위는 별표 2와 같다. 다만, 금융위원회는 별표 2에서 규정한 정보 외에 집중관리·활용이 필요하다고 인정하는 정보를 추가로 집중관리·활용의 대상이 될 정보로 지정하여 고시할 수 있다.<개정 2015.9.11>

④ 법 제25조제2항제2호에 따른 개별신용정보집중기관은 같은 종류의 사업자 간의 협약 등으로 집중관리·활용 대상 정보의 범위를 정하여 정관에 반영하여야 한다.<개정 2015.9.11>

⑤ 신용정보집중기관으로 허가를 받으려는 자는 법 제25조제3항제2호에 따라 공공성과 중립성의 확보를 위하여 다음 각 호의 구분에 따른 요건을 모두 갖추어야 한다.<신설 2015.9.11>

1. 종합신용정보집중기관의 경우: 다음 각 목의 요건
   가. 신용정보의 유출 등을 방지하기 위한 위험관리체계와 신용정보주체의 권익을 보호하기 위한 내부통제장치가 마련되어 있을 것
   나. 법 제25조의2 각 호의 업무(이하 이 조에서 "집중기관업무"라 한다) 외의 다른 업무를 하는 경우에는 집중기관업무와 그 다른 업무를 구분하는 등 이해상충을 방지하기 위한 체계를 마련할 것
   다. 법령을 위반하지 아니하고 건전한 신용질서를 해칠 염려가 없을 것
   라. 제5조제1항제1호부터 제20호까지의 규정에 따른 금융기관 및 제21조제2항 각 호의 기관 간 또는 그 기관의 유형·업무특성 등에 따라 분류된 집단 간에 업무집행의 중립성을 보장하고 해당 집단의 대표성이 확보될 수 있도록 사원의 구성에 관한 계획 및 업무방법 등을 마련할 것
2. 개별신용정보집중기관의 경우: 제1호가목부터 다목까지의 규정에 따른 요건

⑥ 법 제25조제3항제3호에 따라 신용정보집중기관으로 허가를 받으려는 자가 갖추어야 할 시설·설비 및 인력의 세부요건은 다음 각 호와 같다.<개정 2015.9.11>

1. 신용정보 집중관리·활용 업무를 적절하게 수행할 수 있다고 금융위원회가 정하여 고시하는 정보처리설비 및 정보통신설비를 갖출 것
2. 상시고용인력에는 제2조제3항제1호·제3호·제4호에 해당하는 기관, 제5조제1항 각 호에 해당하는 기관 또는 다음 각 목의 금융 관련 단체에서 3년 이상 신용정보 관련 업무에 종사한 경력이 있는 사람 5명 이상이 포함될 것
   가. 신용조회회사

나. 신용정보집중기관

다. 「민법」 제32조에 따라 기획재정부장관의 허가를 받아 설립된 금융결제원

라. 「보험업법」에 따른 보험요율산출기관

⑦ 제5항 및 제6항에 따른 허가요건에 관하여 필요한 세부적인 기준은 금융위원회가 정하여 고시한다.<신설 2015.9.11>

⑧ 법 제25조제4항에 따라 금융위원회는 신용정보집중기관이 다음 각 호의 어느 하나에 해당하게 된 경우에는 그 허가를 취소할 수 있다.<개정 2015.9.11>

1. 거짓이나 그 밖의 부정한 방법으로 법 제25조제1항에 따른 허가를 받은 경우
2. 법 제25조제3항에 따른 허가요건을 유지하지 못한 경우
3. 허가의 조건을 위반한 경우
4. 같은 종류의 업체 간에 협약의 불성립 또는 다른 법령에 따른 집중 제한 등 신용정보를 집중관리·활용할 수 없는 사유가 발생한 경우
5. 집중관리·활용하는 신용정보를 무단으로 교환하거나 활용하는 등 신용정보 보호에 관한 의무를 위반한 경우
6. 법 또는 다른 법령을 위반하여 공익을 심각하게 해친 경우

⑨ 법 제25조제4항에 따라 집중관리·활용되는 신용정보의 교환 대상자는 다음 각 호의 자로 하되, 다음 각 호의 자 사이에 집중관리·활용되는 신용정보의 구체적인 범위 및 신용정보별 세부적인 교환 대상자는 금융위원회가 정하여 고시한다.<개정 2015.9.11>

1. 신용정보제공·이용자와 그 신용정보제공·이용자가 신용정보를 제공한 신용정보집중기관 간
2. 신용정보집중기관과 신용정보회사 간
3. 신용정보집중기관 간

⑩ 신용정보집중기관과 신용조회회사가 제9항에 따라 집중관리·활용되는 신용정보를 교환할 때 개인인 신용정보주체를 식별할 수 있는 정보를 제공하려면 제14조제4항 각 호의 구분에 따른 보호조치를 하여야 한다.<신설 2015.9.11>

⑪법 제25조제6항에 따른 신용정보공동전산망은 제2항에 따른 금융기관으로부터 신용정보를 제공받아 집중관리·활용하는 신용정보집중기관과 제2항에 따른 금융기관 외의 같은 업종의 사업자들로부터 신용정보를 제공받아 집중관리·활용하는 신용정보집중기관이 공동전산망에 참여하는 자를 각각 달리하여 구축한다.<개정 2015.9.11>

제21조의2(종합신용정보집중기관의 업무) ① 법 제25조의2제3호에서 "대통령령으로 정하는 업무"란 다음 각 호의 업무를 말한다.

1. 집중관리하는 신용정보를 활용하여 통계작성 및 학술연구 등의 목적을 위하여 특정 신용정보주체를 식별할 수 없는 형태로 제공하는 업무
2. 제21조제9항에 따른 교환 대상자로부터 위탁받은 조사 및 분석 업무
3. 신용정보의 이용에 관한 컨설팅 업무

② 법 제25조의2제6호에서 "대통령령으로 정하는 업무"란 다음 각 호의 업무를 말한다.

1. 신용정보와 관련한 교육·홍보·출판업무
2. 기술신용정보를 만들어 내는 데에 필요한 기술에 관한 정보의 수집·조사 및 처리
3. 그 밖에 금융위원회가 정하여 고시하는 업무

[본조신설 2015.9.11]

제22조(신용정보집중관리위원회의 업무 등) ① 법 제26조제1항제3호에서 "대통령령으로 정하는 바에 따른 제재"란 제21조제2항에 따른 금융기관 및 기관의 신용정보 제공의 누락 및 지연, 거짓 등록 등 위반행위의 종류와 정도에 따라 제재금(制裁金)을 부과하는 것을 말한다. <개정 2015.9.11>

② 제1항에 따른 제재금의 부과에 관한 세부적인 기준과 절차는 법 제26조제1항에 따른 신용정보집중관리위원회(이하 "신용정보집중관리위원회"라 한다)가 정한다.<개정 2015.9.11>

③ 신용정보집중관리위원회는 법 제26조제1항제1호부터 제4호까지의 규정에 따른 업무 외에 다음 각 호의 업무를 한다.<신설 2015.9.11>

1. 신용정보의 집중관리·활용업무에 관한 예산 및 결산의 심의
2. 신용정보집중기관의 임원의 인사에 관한 심의

④ 금융위원회는 법 제26조제3항에 따라 신용정보집중관리위원회가 보고한 내용이 건전한 신용질서 또는 금융소비자의 권익에 반(反)하는 것으로 판단되는 경우에는 그 결정 사항의 변경을 권고할 수 있다.<개정 2015.9.11>

[제목개정 2015.9.11]

제22조의2(신용정보집중관리위원회의 구성과 운영) ① 신용정보집중관리위원회는 다음 각 호의 위원으로 구성한다.

1. 종합신용정보집중기관의 장
2. 집중관리·활용되는 신용정보의 규모, 경비분담비율, 업권별 대표성 등을 고려하여 종합신용정보집중기관의 정관이 정하는 협회·중앙회·연합회 등의 장이 추천하는 사람 중에서 종합신용정보집중기관의 장이 위촉하는 사람
3. 신용정보의 집중관리·활용에 관한 공익성·전문성·중립성 및 성별 등을 고려하여 종합신용정보집중기관의 장이 위촉하는 사람

② 신용정보집중관리위원회는 집중관리·활용하는 신용정보의 특성 등을 고려하여 그 업무를 효율적으로 처리하기 위하여 소위원회를 둘 수 있다.

③ 제1항 및 제2항에서 규정한 사항 외에 신용정보집중관리위원회의 구성 및 운영 등에 필요한 사항은 종합신용정보집중기관의 정관으로 정한다.

[본조신설 2015.9.11]

제23조(신용조사회사 및 채권추심회사의 종사자) 법 제27조제1항제7호에서 "대통령령으로 정하는 자"란 제18조 각 호의 어느 하나에 해당하는 자를 말한다.

제24조(위임직채권추심인의 자격요건 및 등록절차) ① 법 제27조제9항에 따른 위임직채권추심인으로 등록할 수 있는 사람은 다음 각 호의 어느 하나에 해당하는 사람으로 한다. <개정 2015.9.11>

1. 다음 각 목의 어느 하나에 해당하는 기관에서 채권추심업무에 관한 연수과정을 이수한 사람
   가. 법 제44조에 따른 신용정보협회(이하 "신용정보협회"라 한다)
   나. 신용정보협회가 지정하는 채권추심회사
   다. 그 밖에 금융위원회가 정하여 고시하는 기관
2. 삭제 <2015.9.11>
3. 그 밖에 제1호에 준하는 자격이 있다고 금융위원회가 인정한 사람

② 채권추심회사가 그 소속 위임직채권추심인이 되려는 자를 등록하는 경우에는 금융위원회가 정하여 고시하는 신청서에 그 위임직채권추심인이 제1항의 자격요건을 갖추었는지를 확인할 수 있는 서류를 첨부하여 금융위원회에 제출하여야 한다.<개정 2015.9.11>

제25조 삭제 <2013.8.27>

제26조 삭제 <2013.8.27>

제27조(신용정보활용체제의 공시) ① 법 제31조에서 "대통령령으로 정하는 신용정보제공·이용자"란 제5조제1항제1호부터 제21호까지 및 제21조제2항제1호부터 제21호까지의 규정의 어느 하나에 해당하는 기관을 말한다. <개정 2015.9.11, 2016.3.29>

② 신용정보회사, 신용정보집중기관 및 제1항에 해당하는 자는 법 제31조에 따라 다음 각 호의 사항을 공시하여야 한다.<개정 2011.8.17, 2015.9.11>

1. 관리하는 신용정보의 종류 및 이용 목적
2. 신용정보를 제3자에게 제공하는 경우 제공하는 신용정보의 종류, 제공 대상, 제공받는 자의 이용 목적(제1항에 해당하는 자로 한정한다)
3. 신용정보의 보유 기간 및 이용 기간이 있는 경우 해당 기간, 신용정보 파기의 절차 및 방법(제1항에 해당하는 자로 한정한다)
4. 법 제17조에 따라 신용정보의 처리를 위탁하는 경우 그 업무의 내용 및 수탁자
5. 신용정보주체의 권리와 그 행사방법
6. 법 제20조제3항에 따른 신용정보관리·보호인 또는 신용정보 관리·보호 관련 고충을 처리하는 사람의 성명, 부서 및 연락처
7. 신용등급 산정에 반영되는 신용정보의 종류, 반영비중 및 반영기간(신용조회회사만 해당한다)

③ 신용정보회사, 신용정보집중기관 및 제1항에 해당하는 자는 제2항 각 호의 사항을 공시하는 경우에는 다음 각 호의 어느 하나에 해당하는 방법으로 하여야 한다.

1. 점포·사무소 안의 보기 쉬운 장소에 갖춰 두고 열람하게 하는 방법
2. 해당 기관의 인터넷 홈페이지를 통하여 해당 신용정보주체가 열람할 수 있게 하는 방법

제28조(개인신용정보의 제공·활용에 대한 동의) ① 삭제 <2015.9.11>

② 신용정보제공·이용자는 법 제32조제1항 각 호 외의 부분 본문에 따라 해당 신용정보주체로부터 동의를 받으려면 다음 각 호의 사항을 미리 알려야 한다. 다만, 동의 방식의 특성상 동의 내용을 전부 표시하거나 알리기 어려운 경우에는 해당 기관의 인터넷 홈페이지 주소나 사업장 전화번호 등 동의 내용을 확인할 수 있는 방법을 안내하고 동의를 받을 수 있다.<개정 2015.9.11>

1. 개인신용정보를 제공받는 자
2. 개인신용정보를 제공받는 자의 이용 목적
3. 제공하는 개인신용정보의 내용
4. 개인신용정보를 제공받는 자(신용조회회사 및 신용정보집중기관은 제외한다)의 정보 보유 기간 및 이용 기간

③ 신용정보제공·이용자는 법 제32조제1항제4호에 따라 유무선 통신을 통하여 동의를 받은 경우에는 1개월 이내에 서면, 전자우편, 휴대전화 문자메시지, 그 밖에 금융위원회가 정하여 고시하는 방법으로 제2항 각 호의 사항을 고지하여야 한다.<개정 2015.9.11>

④ 법 제32조제1항제5호에서 "대통령령으로 정하는 방식"이란 정보 제공 동의의 안전성과 신뢰성이 확보될 수 있는 수단을 활용함으로써 해당 신용정보주체에게 동의 내용을 알리고 동의의 의사표시를 확인하여 동의를 받는 방식을 말한다.<신설 2015.9.11>

⑤ 제4항의 방식으로 해당 신용정보주체로부터 개인신용정보의 제공에 관한 동의를 받는 경우 신용정보제공·이용자와 신용조회회사 또는 신용정보집중기관으로부터 개인신용정보를 제공받으려는 자는 다음 각 호의 사항 등을 고려하여 정보 제공 동의의 안전성과 신뢰성이 확보될 수 있는 수단을 채택하여 활용하여야 한다.<개정 2015.9.11>

1. 금융거래 등 상거래관계의 유형·특성·위험도
2. 신용정보제공·이용자 또는 신용조회회사 또는 신용정보집중기관으로부터 개인신용정보를 제공받으려는 자의 업무 또는 업종의 특성
3. 정보 제공 동의를 받아야 하는 신용정보주체의 수

⑥ 법 제32조제2항에 따라 신용조회회사 또는 신용정보집중기관으로부터 개인신용정보를 제공받으려는 자는 다음 각 호의 사항을 해당 개인에게 알리고 동의를 받아야 한다. 다만, 동의방식의 특성상 동의 내용을 전부 표시하거나 알리기 어려운 경우에는 해당 기관의 인터넷 홈페이지 주소나 사업장 전화번호 등 동의 내용을 확인할 수 있는 방법을 안내하고 동의를 받을 수 있다.

1. 개인신용정보를 제공하는 자
2. 개인신용정보를 제공받는 자의 이용 목적
3. 제공받는 개인신용정보의 항목
4. 개인신용정보를 제공받는 것에 대한 동의의 효력기간

⑦ 법 제32조제3항에 따라 신용조회회사 또는 신용정보집중기관은 개인신용정보를 제공받으려는 자가 해당 신용정보주체로부터 동의를 받았는지를 서면, 전자적 기록 등으로 확인하고,

확인한 사항의 진위 여부를 주기적으로 점검하여야 한다.<개정 2015.9.11>

⑧ 법 제32조제4항 전단에 따라 신용정보회사등이 필수적 동의사항과 그 밖의 선택적 동의사항을 구분하는 경우에는 다음 각 호의 사항 등을 고려하여야 한다.<신설 2015.9.11>

1. 신용정보주체가 그 동의사항에 대하여 동의하지 아니하면 그 신용정보주체와의 금융거래 등 상거래관계를 설정·유지할 수 없는지 여부
2. 해당 신용정보주체가 그 동의사항에 대하여 동의함으로써 제공·활용되는 개인신용정보가 신용정보회사등과의 상거래관계에 따라 신용정보주체에게 제공되는 재화 또는 서비스(신용정보주체가 그 신용정보회사등에 신청한 상거래관계에서 제공하기로 한 재화 또는 서비스를 그 신용정보회사등과 별도의 계약 또는 약정 등을 체결한 제3자가 신용정보주체에게 제공하는 경우를 포함한다)와 직접적으로 관련되어 있는지 여부
3. 신용정보주체가 그 동의사항에 대하여 동의하지 아니하면 법 또는 다른 법령에 따른 의무를 이행할 수 없는지 여부

⑨ 신용정보회사등이 법 제32조제4항 전단에 따라 필수적 동의 사항과 그 밖의 선택적 동의사항을 구분하여 동의를 받는 경우 동의서 양식을 구분하는 등의 방법으로 신용정보주체가 각 동의사항을 쉽게 이해할 수 있도록 하여야 한다.<신설 2015.9.11>

⑩ 법 제32조제6항제4호에서 "채권추심(추심채권을 추심하는 경우만 해당한다), 인가·허가의 목적, 기업의 신용도 판단, 유가증권의 양수 등 대통령령으로 정하는 목적"이란 다음 각 호의 목적을 말한다.<개정 2011.8.17, 2015.9.11, 2017.1.10>

1. 채권추심을 의뢰한 채권자가 채권추심의 대상이 되는 자의 개인신용정보를 채권추심회사에 제공하거나 채권추심회사로부터 제공받기 위한 목적
2. 채권자 또는 채권추심회사가 변제기일까지 채무를 변제하지 아니한 자 또는 채권추심의 대상이 되는 자에 대한 개인신용정보를 신용조회회사로부터 제공받기 위한 목적
3. 행정기관이 인가·허가 업무에 사용하기 위하여 신용조회회사로부터 개인신용정보를 제공받기 위한 목적
4. 해당 기업과의 금융거래 등 상거래관계의 설정 및 유지 여부 등을 판단하기 위하여 그 기업의 대표자 및 제2조제1항제3호의 각 목의 어느 하나에 해당하는 자의 개인신용정보를 신용정보집중기관 및 신용조회회사로부터 제공받기 위한 목적
5. 제21조제2항에 따른 금융기관이 상거래관계의 설정 및 유지 여부 등을 판단하기 위하여 또는 어음·수표 소지인이 어음·수표의 발행인, 인수인, 배서인 및 보증인의 변제 의사 및 변제자력을 확인하기 위하여 신용정보집중기관 및 신용조회회사로부터 어음·수표의 발행인, 인수인, 배서인 및 보증인의 개인신용정보를 제공받기 위한 목적
6. 「민법」 제450조에 따라 지명채권을 양수한 신용정보제공·이용자가 다음 각 목의 어느 하나에 해당하는 경우에 그 지명채권의 채무자의 개인신용정보를 신용조회회사 또는 신용정보집중기관에 제공하거나 신용조회회사 또는 신용정보집중기관으로부터 제공받기 위한 목적

가. 지명채권의 양도인이 그 지명채권의 원인이 되는 상거래관계가 설정될 당시 법 제32조제1항 각 호의 어느 하나에 해당하는 방식으로 채무자의 개인신용정보를 제공하거나 제공받는 것에 대하여 해당 채무자로부터 동의를 받은 경우

나. 법 또는 다른 법령에 따라 그 지명채권의 채무자의 개인신용정보를 제공하거나 제공받을 수 있는 경우

7. 통계작성 및 학술연구 등을 위하여 필요한 경우로서 신용정보회사등으로부터 특정 개인을 알아볼 수 없는 형태로 개인신용정보를 제공받기 위한 목적

⑪ 법 제32조제6항제9호에서 "대통령령으로 정하는 금융질서문란행위자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.<신설 2015.9.11>

1. 부정한 목적으로 다른 신용정보주체의 개인식별정보(제29조에서 정하는 정보를 말한다. 이하 이 호에서 같다)를 이용하여 금융거래 등 상거래를 하거나 그 상거래를 하려는 타인에게 자신의 개인식별정보를 제공한 자
2. 부정한 목적으로 금융거래 등 상거래와 관련하여 거래상대방에게 위조·변조되거나 허위인 신용정보를 제공한 자
3. 대출사기, 보험사기, 거짓이나 그 밖의 부정한 방법으로 알아낸 타인의 신용카드 정보를 이용한 거래 또는 이와 유사한 금융거래 등 상거래를 한 자
4. 거짓이나 그 밖의 부정한 방법으로 법원의 회생절차개시결정·간이회생절차개시결정·개인회생절차개시결정·파산선고 또는 이와 유사한 결정이나 판결을 받은 자
5. 그 밖에 금융거래 등 상거래와 관련하여 금융질서를 문란하게 한 자로서 금융위원회가 정하여 고시하는 자

⑫ 신용정보회사등이 법 제32조제7항 본문에 따라 신용정보주체에게 개인신용정보의 제공 사실 및 이유 등을 사전에 알리는 경우와 같은 항 단서에 따라 불가피한 사유로 인하여 사후에 알리거나 공시하는 경우에 그 제공의 이유 및 그 알리거나 공시하는 자별로 알리거나 공시하는 시기 및 방법은 별표 2의2와 같다.<개정 2015.9.11>

⑬ 법 제32조제8항에서 "대통령령으로 정하는 자"란 제5조제1항제1호부터 제21호까지의 규정의 어느 하나에 해당하는 기관을 말한다.<개정 2011.8.17, 2015.9.11>

⑭ 법 제32조제8항에서 "제공하는 신용정보의 범위 등 대통령령으로 정하는 사항"이란 제공하는 개인신용정보의 범위, 제공받는 자의 신용정보 관리·보호 체계를 말한다.<개정 2011.8.17, 2015.9.11>

제29조(개인식별정보의 제공·이용) 법 제34조에서 "대통령령으로 정하는 정보"란 생존하는 개인의 성명, 주소, 다음 각 호의 번호, 성별, 국적 등 개인을 식별할 수 있는 정보를 말한다. <개정 2015.9.11>

1.「주민등록법」 제7조제3항에 따른 주민등록번호
2.「여권법」 제7조제1항제1호에 따른 여권번호
3.「도로교통법」 제80조에 따른 운전면허의 면허번호

4.「출입국관리법」 제31조제4항에 따른 외국인등록번호
5.「재외동포의 출입국과 법적 지위에 관한 법률」 제7조제1항에 따른 국내거소신고번호

제30조(신용정보 이용 및 제공사실의 조회 등) ① 신용정보회사등은 법 제35조제1항 각 호 외의 부분 본문에 따라 다음 각 호의 구분에 따른 방법으로 개인신용정보를 이용하거나 제공한 날부터 금융위원회가 정하여 고시하는 기간 이내에 신용정보주체에게 조회사항(같은 항 각 호의 구분에 따른 사항을 말한다. 이하 이 조에서 같다)을 조회할 수 있도록 하여야 한다. 다만, 법 제32조제7항 단서에 따른 불가피한 사유가 있는 경우에는 별표 2의2에 따라 알리거나 공시하는 시기에 조회할 수 있도록 하여야 한다. <개정 2015.9.11, 2016.3.29>

1. 신용정보회사등으로서 다음 각 목의 어느 하나에 해당하는 자의 경우: 신용정보주체가 조회사항을 편리하게 확인할 수 있도록 하기 위한 개인신용정보조회시스템을 구축하고, 인터넷 홈페이지 등에 그 개인신용정보조회시스템을 이용하는 방법 및 절차 등을 게시하는 방법
   가. 신용정보집중기관
   나. 신용정보회사
   다. 제5조제1항제1호부터 제20호까지의 규정에 따른 기관(개인신용정보를 관리하는 전산시스템이 없는 기관으로서 1만명 미만의 신용정보주체에 관한 개인신용정보를 보유한 기관은 제외한다)
   라. 제21조제2항제1호부터 제21호까지의 규정에 따른 기관(개인신용정보를 관리하는 전산시스템이 없는 기관으로서 1만명 미만의 신용정보주체에 관한 개인신용정보를 보유한 기관은 제외한다)
2. 신용정보회사등으로서 제1호에서 정하는 자 외의 자의 경우: 제1호에서 정하는 방법 또는 사무소·점포 등에서 신용정보주체가 조회사항을 열람하게 하는 방법

② 제1항에 따라 신용정보회사등이 신용정보주체에게 조회할 수 있도록 하여야 하는 조회사항은 그 조회가 의뢰된 날을 기준으로 최근 3년간의 조회사항으로 한다.<개정 2015.9.11>

③ 신용정보회사등은 제1항에 따라 조회사항을 신용정보주체가 조회할 수 있도록 하는 경우에는 그 조회를 요구하는 사람이 그 조회사항에 관한 신용정보주체 본인인지 여부를 확인하여야 한다. 이 경우 신용정보회사등은 금융거래 등 상거래관계의 유형·특성·위험도 등을 고려하여 본인 확인의 안전성과 신뢰성이 확보될 수 있는 수단을 채택하여 활용할 수 있다.<개정 2015.9.11>

④ 법 제35조제1항 단서에서 "내부 경영관리의 목적으로 이용하거나 반복적인 업무위탁을 위하여 제공하는 경우 등 대통령령으로 정하는 경우"란 다음 각 호의 어느 하나에 해당하는 목적으로 이용하거나 제공하는 경우를 말한다. 다만, 상품 및 서비스를 소개하거나 구매를 권유할 목적으로 이용하거나 제공하는 경우는 제외한다.<개정 2015.9.11, 2016.3.29>

1. 신용위험관리 등 위험관리와 내부통제
2. 고객분석과 상품 및 서비스의 개발
3. 성과관리

4. 위탁업무의 수행
5. 업무와 재산상태에 대한 검사
6. 그 밖에 다른 법령에서 정하는 바에 따른 국가 또는 지방자치단체에 대한 자료 제공

⑤ 법 제35조제1항제1호에서 "대통령령으로 정하는 사항"이란 해당 개인신용정보의 보유기간 및 이용기간을 말한다.<개정 2015.9.11>

⑥ 법 제35조제1항제2호에서 "대통령령으로 정하는 사항"이란 해당 개인신용정보를 제공받은 자의 보유기간 및 이용기간을 말한다.<신설 2015.9.11>

⑦ 신용정보회사등은 법 제35조제2항에 따라 신용정보주체로부터 통지의 요청을 받으면 금융위원회가 정하여 고시하는 서식 및 방법에 따라 그 요청을 받은 때부터 정기적으로 해당 신용정보주체에게 조회사항을 통지하여야 한다.<신설 2015.9.11>

⑧ 신용정보회사등은 제1항에 따른 조회나 제7항에 따른 통지에 직접 드는 비용을 그 신용정보주체에게 부담하게 할 수 있다. 다만, 제1항에 따른 개인신용정보조회시스템을 통하여 조회사항을 조회할 수 있도록 한 경우에는 신용정보주체가 1년에 1회 이상 무료로 조회할 수 있도록 하여야 한다.<신설 2015.9.11>

⑨ 신용정보회사등은 제1항에 따라 신용정보주체가 조회한 내용과 제7항에 따라 신용정보주체에게 통지한 내용을 3년간 보존하여야 한다.<신설 2015.9.11>

[제목개정 2015.9.11]

제31조(상거래 거절 근거 신용정보의 고지 등) ① 법 제36조제1항에서 "대통령령으로 정하는 정보"란 다음 각 호의 신용정보를 말한다. <개정 2015.9.11>

1. 제2조제1항제3호에 따른 신용정보
2. 제2조제1항제5호 각 목의 신용정보. 이 경우 같은 호 마목, 사목, 카목, 타목 및 파목의 신용정보는 제외하며, 같은 호 라목의 경우에는 체납 관련 정보만 해당하고, 같은 호 자목 및 차목의 경우에는 신용회복정보 및 이와 비슷한 정보로서 금융위원회가 정하여 고시하는 정보만 해당한다.

② 법 제36조제1항에서 "거절 또는 중지의 근거가 된 정보 등 대통령령으로 정하는 사항"이란 다음 각 호의 사항을 말한다.<개정 2015.9.11>

1. 상거래관계 설정의 거절이나 중지의 근거가 된 신용정보
2. 제1호의 정보를 제공한 신용조회회사 및 신용정보집중기관의 명칭, 주소, 연락처
3. 신용조회회사 및 신용정보집중기관이 상거래관계의 설정을 거절하거나 중지하도록 결정한 것이 아니라는 사실 및 신용조회회사 또는 신용정보집중기관으로부터 제공받은 정보 외에 다른 정보를 함께 사용하였을 경우에는 그 사실과 그 다른 정보

제32조(개인신용정보 제공ㆍ이용 동의 철회권 등) ① 법 제37조제1항에 따라 개인인 신용정보주체는 동의 철회의 대상 및 내용 등을 특정하여 해당 기관의 인터넷 홈페이지, 유무선 통신, 서면, 그 밖에 금융위원회가 정하여 고시하는 방법으로 동의를 철회할 수 있다. <개정 2015.9.11>

② 법 제37조제2항에 따라 개인인 신용정보주체는 상품이나 용역을 소개하거나 구매를 권유할 목적으로 연락하는 신용정보제공·이용자에 대하여 연락중지 청구의 대상 및 내용을 특정하여 제1항의 방법으로 본인에게 연락하는 것을 중지할 것을 청구할 수 있다.
③ 제1항 및 제2항에 따른 청구를 받은 신용정보제공·이용자는 청구를 받은 날부터 1개월 이내에 그에 따른 조치를 완료하여야 한다.
④ 법 제37조제3항에 따라 신용정보제공·이용자가 거래 상대방인 개인에게 구두에 의한 방법으로 고지한 경우에는 고지한 날부터 1개월 이내에 고지 내용을 서면, 전자우편, 휴대전화 문자메시지, 인터넷 홈페이지 및 그 밖에 금융위원회가 정하는 방법으로 추가 고지하여야 한다.
⑤ 법 제37조제4항 및 제5항에 따라 신용정보제공·이용자는 수신자 부담 전화, 수취인 부담 우편 등의 조치를 마련하여야 한다.

제33조(신용정보의 열람 및 정정청구 등) ① 법 제38조제1항에서 "본인의 신분을 나타내는 증표를 내보이거나 전화, 인터넷 홈페이지의 이용 등 대통령령으로 정하는 방법"이란 다음 각 호의 방법을 말한다. <개정 2015.9.11>
1. 본인의 신분을 나타내는 증표를 내보이는 방법
2. 전화, 인터넷 홈페이지를 이용하는 방법
3. 제1호 및 제2호의 방법 외의 방법으로서 본인 확인의 안전성과 신뢰성이 확보될 수 있는 수단을 활용하여 본인정보의 제공·열람을 청구하는 자가 신용정보주체 본인임을 확인하는 방법. 이 경우 신용정보회사등은 금융거래 등 상거래관계의 유형·특성·위험도 등을 고려하여 본인 확인의 안전성과 신뢰성이 확보될 수 있는 수단을 채택하여 활용할 수 있다.

② 법 제38조제1항에 따라 신용정보주체는 본인정보를 제공받거나 열람하는 경우 서면, 전자문서 또는 인터넷 홈페이지 등을 통하여 할 수 있다.
③ 신용정보주체가 법 제38조제4항에 따라 시정 요청을 하려는 경우에는 처리결과의 통지를 받은 날(통지가 없는 경우에는 법 제38조제1항에 따른 정정청구를 하고 7영업일이 지난 날)부터 15일 이내에 금융위원회가 정하여 고시하는 시정요청서에 다음 각 호의 서류를 첨부하여 금융위원회에 제출하여야 한다.
1. 법 제38조제1항에 따라 신용정보회사등에 정정청구를 한 내용을 적은 서면
2. 신용정보회사등으로부터 법 제38조제4항에 따른 처리결과를 통지받은 경우에는 그 통지 내용
3. 시정 요청의 대상이 된 신용정보의 사실 여부를 확인할 수 있는 근거자료

제33조의2(신용조회회사의 정보제공 중지의 요건 및 신용정보주체에 대한 통지사항 등) ① 신용조회회사는 법 제38조의2제2항에 따라 신용정보주체로부터 같은 조 제1항의 요청을 받은 경우로서 다음 각 호의 어느 하나에 해당하는 사실이 발생함에 따라 그 요청을 받은 것으로 인정되는 경우에 그 사실로 인하여 그 신용정보주체의 개인신용정보가 도용됨으로써 신용정보제공·이용자, 그 밖의 이용자(이하 이 조에서 "정보제공의뢰자"라 한다)로부터 개인신용정보

의 제공을 의뢰받은 것으로 의심되면 지체 없이 해당 신용정보주체의 개인신용정보를 정보제공의뢰자에게 제공하는 행위를 중지하여야 한다.

1. 해당 신용정보주체의 개인신용정보가 누설된 사실
2. 해당 신용정보주체가 신분증을 분실한 사실
3. 제1호 또는 제2호와 비슷한 사실로서 금융위원회가 정하여 고시하는 사실

② 법 제38조의2제1항 전단 및 제2항에 따라 신용조회회사가 신용정보주체에게 통지하여야 할 사항은 다음 각 호의 구분에 따른다.

1. 정보제공의뢰자에게 해당 신용정보주체의 개인신용정보를 제공하여 법 제38조의2제1항에 따라 통지한 경우: 개인신용정보를 제공받은 자, 제공의 목적, 제공한 내용, 제공한 날짜
2. 정보제공의뢰자에게 해당 신용정보주체의 개인신용정보를 제공하지 아니하고 법 제38조의2제2항에 따라 통지한 경우: 정보제공의뢰자, 의뢰의 목적, 의뢰된 날짜

③ 신용조회회사는 법 제38조의2제3항에 따라 다음 각 호의 어느 하나에 해당하는 방법으로 해당 신용정보주체에게 제2항 각 호의 구분에 따른 사항을 통지하여야 한다.

1. 서면
2. 전화
3. 전자우편
4. 휴대전화 문자메시지
5. 제1호부터 제4호까지의 규정에 따른 방법과 비슷한 방법

④ 신용조회회사는 법 제38조의2제3항에 따라 해당 신용정보주체에게 제2항 및 제3항에 따른 통지에 드는 비용을 부담하게 할 수 있다. 다만, 제1항제1호에 해당하는 사실이 발생한 경우로서 신용정보회사등에 책임 있는 사유로 그 사실이 발생함에 따라 그 통지를 하게 된 경우에는 그 신용정보회사등에 그 비용을 부담하게 하여야 한다.

[본조신설 2015.9.11]

제33조의3(개인신용정보의 삭제 요구) ① 법 제38조의3제1항 본문에 따른 "대통령령으로 정하는 기간"은 다음 각 호의 구분에 따른 기간으로 한다.

1. 제17조의2제1항제1호에 따른 개인신용정보의 경우: 5년
2. 제17조의2제1항제2호에 따른 개인신용정보의 경우: 3개월

② 법 제38조의3제1항 본문에 따른 삭제요구에 따라 신용정보제공·이용자가 개인신용정보를 삭제함으로써 해당 신용정보주체에게 불이익이 발생하는 경우에는 그 정보를 삭제하기 전에 그러한 불이익이 발생할 수 있다는 것을 해당 신용정보주체에게 알려야 한다.

③ 법 제38조의3제3항에 따라 신용정보제공·이용자가 개인신용정보를 관리하는 경우에는 제17조의2제1항제1호 각 목의 방법에 따라 관리한다.

[본조신설 2015.9.11]

제34조(무료 열람권) 법 제39조에서 "대통령령으로 정하는 일정한 기간"이란 4개월을 말한다.

<개정 2011.8.17>

제34조의2(신용정보의 누설사실의 통지 등) ① 신용정보회사등이 법 제39조의2제1항에 따라 통지하려는 경우에는 제33조의2제3항 각 호의 어느 하나에 해당하는 방법으로 개별 신용정보주체에게 신용정보가 누설되었다는 사실을 통지하여야 한다.

② 신용정보회사등은 법 제39조의2제3항 전단에 해당하는 경우에는 제1항에 따른 방법 외에 다음 각 호의 어느 하나에 해당하는 방법으로 금융위원회가 정하여 고시하는 기간 동안 신용정보가 누설되었다는 사실을 널리 알려야 한다.

1. 인터넷 홈페이지에 그 사실을 게시하는 방법
2. 사무실이나 점포 등에서 해당 신용정보주체로 하여금 그 사실을 열람하게 하는 방법
3. 주된 사무소가 있는 특별시·광역시·특별자치시·도 또는 특별자치도 이상의 지역을 보급지역으로 하는 일반일간신문, 일반주간신문 또는 인터넷신문(「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 또는 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문을 말한다)에 그 사실을 게재하는 방법

③ 제1항에도 불구하고 신용정보 누설에 따른 피해가 없는 것이 명백하고 법 제39조의2제2항에 따라 누설된 신용정보의 확산 및 추가 유출을 방지하기 위한 조치가 긴급히 필요하다고 인정되는 경우에는 해당 조치를 취한 후 지체 없이 신용정보주체에게 알릴 수 있다. 이 경우 그 조치의 내용을 함께 알려야 한다.

④ 법 제39조의2제3항 전단에서 "대통령령으로 정하는 규모 이상의 신용정보"란 1만명 이상의 신용정보주체에 관한 개인신용정보를 말한다.

⑤ 법 제39조의2제3항 전단에서 "대통령령으로 정하는 전문기관"이란 금융감독원을 말한다.

⑥ 법 제39조의2제3항 전단에 따라 신고하여야 하는 신용정보회사등은 그 신용정보가 누설되었음을 알게 된 때 지체 없이 금융위원회가 정하여 고시하는 신고서를 금융위원회 또는 금융감독원에 제출하여야 한다.

⑦ 제6항에도 불구하고 제3항 전단에 해당하는 경우에는 우선 금융위원회 또는 금융감독원에 그 신용정보가 누설된 사실을 알리고 추가 유출을 방지하기 위한 조치를 취한 후 지체 없이 제6항에 따른 신고서를 제출할 수 있다. 이 경우 그 조치의 내용을 함께 제출하여야 한다.

[본조신설 2015.9.11]

제34조의3(광고성 정보의 전송이 금지되는 전자적 매체나 방식) 법 제40조제7호에 따른 "대통령령으로 정하는 전자적 매체나 방식"이란 다음 각 호의 어느 하나에 해당하는 매체나 방식을 말한다.

1. 전화
2. 전자우편
3. 휴대전화 문자메시지
4. 그 밖에 정보통신망을 통하여 수신자에게 부호·문자·화상 또는 영상을 전자적 형태로 전송하는 매체나 방식

[본조신설 2015.9.11]

제35조(채권추심회사 등의 금지사항) 채권추심회사 및 소속 위임직채권추심인은 채권추심행위를 하는 과정에서 「채권의 공정한 추심에 관한 법률」 제5조, 제6조 및 제8조를 준수하여야 하며, 같은 법 제9조부터 제13조까지의 규정을 위반하여 채권추심을 해서는 아니 된다.

제35조의2(모집업무수탁자의 모집경로 확인 등) ① 법 제41조의2제1항에 따른 모집업무수탁자는 다음 각 호의 어느 하나에 해당하는 자로 한다.

1. 「여신전문금융업법」 제14조의2제1항제2호 또는 제3호에 따라 신용카드회원을 모집할 수 있는 자
2. 「여신전문금융업법」에 따른 가맹점모집인
3. 「보험업법」에 따른 보험설계사
4. 「보험업법」에 따른 보험대리점
5. 「자본시장과 금융투자업에 관한 법률」 제51조제9항에 따른 투자권유대행인
6. 「대부업 등의 등록 및 금융이용자 보호에 관한 법률」 제3조제1항 단서에 따른 대출모집인

② 법 제41조의2제1항제3호에서 "대통령령으로 정하는 사항"이란 다음 각 호의 사항을 말한다.

1. 모집업무에 이용한 개인신용정보를 안전하게 보관하고 있지 아니한지 여부 및 그 이용 목적을 달성하였거나 이용기간이 종료되었음에도 불구하고 아직 그 정보를 파기하지 아니하였는지 여부
2. 제1호의 개인신용정보를 모집업무 목적 외에 이용하였거나 제3자에게 제공하였는지 여부

③ 법 제41조의2제3항에서 "대통령령으로 정하는 등록기관"이란 제1항 각 호의 어느 하나에 해당하는 자가 신용정보제공·이용자로부터 위탁받은 모집업무에 관한 법령 등에 따라 등록·등재한 기관(이하 이 조에서 "등록기관"이라 한다)을 말한다.

④ 신용정보제공·이용자는 법 제41조의2제1항 각 호의 사항을 매 분기마다 1회 이상 확인하여야 한다.

⑤ 신용정보제공·이용자는 제4항에 따라 확인한 사항을 다음 각 호의 구분에 따른 기한까지 등록기관에 알려야 한다.

1. 모집업무수탁자가 법 제41조의2제1항제1호에 따른 불법취득 신용정보를 모집업무에 이용한 사실을 확인한 경우: 그 확인한 날부터 7일 이내
2. 제1호에서 정하는 사항 외의 사항을 확인한 경우: 매 분기의 말일을 기준으로 해당 분기의 말일부터 1개월 이내

⑥ 신용정보제공·이용자는 제5항제1호의 경우에 제4항에 따라 확인한 사실을 금융위원회에도 알려야 한다.

⑦ 등록기관은 제5항에 따라 신용정보제공·이용자가 알린 사항을 매 분기의 말일을 기준으로 해당 분기의 말일부터 2개월 이내에 금융위원회에 보고하여야 한다.

[본조신설 2015.9.11]

제35조의3(과징금의 산정기준 등) ① 법 제42조의2제1항 본문에서 "대통령령으로 정하는 위반행위와 관련한 매출액"이란 해당 신용정보회사등이 위반행위와 관련된 개인신용정보를 이용한 사업부문의 직전 3개 사업연도의 연평균 매출액(이하 이 조에서 "연평균 매출액"이라 한다)을 말한다. 다만, 다음 각 호의 구분에 따른 경우에는 그 금액을 연평균 매출액으로 한다.

1. 해당 사업연도 첫날을 기준으로 사업을 개시한지 3년이 되지 아니한 경우: 그 사업개시 후 직전 사업연도 말일까지의 매출액을 연평균 매출액으로 환산한 금액
2. 해당 사업연도에 사업을 개시한 경우: 사업개시일부터 위반행위일까지의 매출액을 연평균 매출액으로 환산한 금액

② 법 제42조의2제2항 단서에서 "대통령령으로 정하는 경우"란 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 영업을 개시하지 아니하거나 영업을 중단하는 등의 사유로 영업실적이 없는 경우
2. 재해 등으로 인하여 매출액 산정자료가 소멸되거나 훼손되는 등 객관적인 매출액의 산정이 곤란한 경우

③ 법 제42조의2에 따른 과징금은 다음 각 호의 구분에 따른 과징금 부과의 최고한도 금액에 대하여 그 각 호의 구분에 따라 나누어진 각 단계별로 금융위원회가 정하여 고시하는 과징금 부과비율을 적용하여 산정한 금액으로 한다.

1. 최고한도 금액이 같은 조 제1항 본문에 따라 매출액의 100분의 3에 해당하는 금액인 경우: 2억원 이하, 2억원 초과 20억원 이하, 20억원 초과 200억원 이하, 200억원 초과 2천억원 이하, 2천억원 초과의 다섯 단계
2. 최고한도 금액이 같은 조 제1항 단서에 따라 50억원인 경우: 2억원 이하, 2억원 초과 20억원 이하, 20억원 초과의 세 단계
3. 최고한도 금액이 제4항에서 정하는 금액인 경우: 2억원 이하, 2억원 초과 20억원 이하, 20억원 초과의 세 단계

④ 법 제42조의2제2항 단서에 해당하는 경우에는 다음 각 호의 금액 중 가장 적은 금액을 과징금 부과의 최고한도 금액으로 한다.

1. 해당 신용정보회사등과 비슷한 규모의 신용정보회사등의 연평균 매출액의 100분의 3
2. 해당 신용정보회사등과 같은 종류의 신용정보회사등의 연평균 매출액의 100분의 3
3. 200억원

⑤ 제3항 및 제4항에 따라 산정한 금액은 법 제42조의2제3항 각 호의 사항을 고려하여 이를 가중하거나 감경할 수 있다.

⑥ 금융위원회는 제1항에 따른 매출액 산정을 위하여 재무제표 등 자료가 필요한 경우 20일 이내의 기간을 정하여 해당 신용정보회사등에 관련 자료의 제출을 요청할 수 있다.

⑦ 법 제42조의2제8항에서 "대통령령으로 정하는 자"란 제35조의2제1항 각 호의 어느 하나에 해당하는 자를 말한다.

[본조신설 2015.9.11]

제35조의4(의견제출) ① 금융위원회는 법 제42조의2에 따른 과징금을 부과하기 전에 당사자 또는 이해관계인 등에게 의견을 제출할 기회를 주어야 한다.

② 제1항에 따른 당사자 또는 이해관계인 등은 금융위원회의 회의에 출석하여 의견을 진술하거나 필요한 자료를 제출할 수 있다.

③ 당사자 또는 이해관계인 등은 제2항에 따른 의견 진술 또는 자료 제출을 하는 경우 변호인의 도움을 받거나 그를 대리인으로 지정할 수 있다.

[본조신설 2015.9.11]

제35조의5(과징금의 부과 및 납부절차 등) ① 금융위원회는 법 제42조의2에 따른 과징금을 부과하려는 경우에는 위반사실, 부과금액, 이의제기 방법 및 이의제기 기간 등을 구체적으로 밝혀 과징금을 낼 것을 서면으로 통지하여야 한다.

② 제1항에 따라 통지를 받은 자는 통지받은 날부터 60일 이내에 금융위원회가 정하는 수납기관에 과징금을 내야 한다.

③ 제1항 및 제2항에서 정하는 사항 외에 과징금의 부과에 필요한 세부사항은 금융위원회가 정하여 고시한다.

[본조신설 2015.9.11]

제35조의6(납부기한 연장과 분할 납부) ① 법 제42조의2제9항에 따라 금융위원회는 과징금 부과처분을 받은 자(이하 "과징금납부의무자"라 한다)가 다음 각 호의 어느 하나에 해당하는 사유로 과징금 전액을 한꺼번에 내기 어렵다고 인정될 때에는 그 납부기한을 연장하거나 분할 납부하게 할 수 있다. 이 경우 필요하다고 인정하면 담보를 제공하게 할 수 있다.

1. 재해 등으로 재산에 현저한 손실을 입은 경우
2. 사업 여건의 악화로 사업이 중대한 위기에 처한 경우
3. 과징금을 한꺼번에 내면 자금사정에 현저한 어려움이 예상되는 경우

② 제1항에 따라 납부기한을 연장하거나 분할 납부하게 할 경우 납부기한의 연장은 1년을 초과할 수 없고, 분할 납부의 간격은 6개월 이내로 하며, 분할 납부의 횟수는 3회를 초과할 수 없다.

③ 과징금납부의무자가 제1항에 따라 과징금의 납부기한을 연장하거나 분할 납부를 하려는 경우에는 그 납부기한의 10일 전까지 금융위원회에 신청하여야 한다.

④ 금융위원회는 제1항에 따라 납부기한이 연장되거나 분할 납부가 허용된 과징금납부의무자가 다음 각 호의 어느 하나에 해당하면 납부기한 연장 또는 분할납부 결정을 취소하고 과징금을 한꺼번에 징수할 수 있다.

1. 분할 납부하기로 결정된 과징금을 납부기한까지 내지 아니하였을 때
2. 담보 변경명령이나 그 밖에 담보보전에 필요한 금융위원회의 명령을 이행하지 아니하였을 때
3. 강제집행, 경매의 개시, 파산선고, 법인의 해산, 국세 또는 지방세의 체납처분을 받은 경우나 그 밖에 이와 비슷한 경우로서 과징금의 전부 또는 잔여분을 징수할 수 없다고 인정될 때

[본조신설 2015.9.11]

제35조의7(결손처분) 법 제42조의2제9항에 따라 금융위원회는 과징금납부의무자에게 다음 각 호의 어느 하나에 해당하는 사유가 있으면 결손처분을 할 수 있다.

1. 체납처분이 끝나고 체납액에 충당된 배분금액이 체납액에 미치지 못하는 경우
2. 징수금 등의 징수권에 대한 소멸시효가 완성된 경우
3. 체납자의 행방이 분명하지 아니하거나 재산이 없다는 것이 판명된 경우
4. 체납처분의 목적물인 총재산의 추산가액이 체납처분 비용에 충당하면 남을 여지가 없음이 확인된 경우
5. 체납처분의 목적물인 총재산이 징수금 등보다 우선하는 국세, 지방세, 전세권·질권 또는 저당권으로 담보된 채권 등의 변제에 충당하면 남을 여지가 없음이 확인된 경우
6. 그 밖에 징수 가능성이 없는 경우로서 「채무자 회생 및 파산에 관한 법률」 제251조 본문에 따라 회생채권 등이 면책되는 경우

[본조신설 2015.9.11]

제35조의8(법정손해배상의 청구기간) ① 신용정보주체는 법 제43조의2제1항에 따라 같은 항 각 호의 모두에 해당하는 행위가 있었던 사실을 안 날부터 3년 이내에 신용정보회사등이나 그 밖의 신용정보 이용자(수탁자를 포함한다)에게 손해액의 배상을 청구할 수 있다.

② 제1항에 따른 손해액의 배상은 그 행위가 있었던 날부터 10년이 지나면 청구하지 못한다.

[본조신설 2015.9.11]

제35조의9(손해배상 책임의 이행을 위한 보험 등 가입의무가 있는 신용정보회사등의 범위) 법 제43조의3에서 "대통령령으로 정하는 신용정보회사등"이란 다음 각 호의 자 중에서 금융위원회가 정하여 고시하는 자를 말한다.

1. 신용정보집중기관
2. 신용정보회사
3. 제5조제1항제1호부터 제21호까지의 규정의 어느 하나에 해당하는 자
4. 제21조제2항 각 호의 어느 하나에 해당하는 자

[본조신설 2015.9.11]

제36조(신용정보협회의 업무) 법 제44조제3항제4호에서 "대통령령으로 정하는 업무"란 다음 각 호의 업무를 말한다.

1. 신용정보회사의 경영과 관련된 정보의 수집 및 통계의 작성 업무
2. 신용정보업 관련 교육업무 및 출판업무
3. 법 또는 다른 법령에서 신용정보협회에 위임·위탁한 업무
4. 그 밖에 금융위원회가 정하여 고시하는 업무

제37조(권한의 위임 또는 위탁) ① 금융위원회는 법 제49조에 따라 별표 3에 따른 권한을 금융감독원장에게 위탁하고, 법 제27조제3항에 따른 위임직채권추심인의 등록업무를 신용정보협

회에 위탁한다.

② 금융감독원장 및 신용정보협회는 제1항에 따라 위탁받은 업무의 처리 내용을 6개월마다 금융위원회에 보고하여야 한다.

제37조의2(민감정보 및 고유식별정보의 처리) ①금융위원회(제37조에 따라 금융위원회의 업무를 위탁받은 자를 포함한다), 금융감독원장은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제18조제2호에 따른 범죄경력자료에 해당하는 정보, 개인식별번호가 포함된 자료를 처리할 수 있다. <개정 2014.8.6, 2015.9.11>

1. 법 제4조에 따른 신용정보업 허가 및 법 제8조에 따른 신고 또는 보고에 관한 사무
2. 법 제9조에 따른 지배주주 변경승인에 관한 사무
3. 법 제10조에 따른 신용정보업의 양도·양수 등의 인가 등에 관한 사무
4. 법 제11조제1항에 따른 겸업 신고 수리 및 같은 조 제2항 단서에 따른 겸업 승인에 관한 사무
5. 법 제13조에 따른 임원 겸직 승인에 관한 사무
6. 법 제14조에 따른 허가 등의 취소와 업무의 정지에 관한 사무
7. 법 제27조에 따른 위임직채권추심인의 등록에 관한 사무
8. 법 제38조제4항·제5항·제7항에 따른 시정요청 처리에 관한 사무
9. 법 제45조에 따른 감독·검사에 관한 사무 및 이에 따른 사후조치 등에 관한 사무
10. 법 제48조에 따른 청문에 관한 사무
11. 법 제41조의2제1항에 따른 모집업무수탁자에 대한 확인에 관한 사무 및 같은 조 제3항에 따른 보고에 관한 사무
12. 법 제42조의2에 따른 과징금의 부과 및 징수 등에 관한 사무

② 신용정보회사는 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제18조제2호에 따른 범죄경력자료에 해당하는 정보, 개인식별번호가 포함된 자료를 수집·처리할 수 있다. 다만, 개인식별번호를 개인으로부터 직접 수집할 경우에는 그 개인의 동의를 받아야 한다.<신설 2014.8.6, 2015.9.11>

1. 법 제4조제1항에 따른 신용조회업, 신용조사업 및 금융거래와 관련하여 수행하는 채권추심업에 관한 사무
2. 법 제11조에 따른 겸업 업무 중 금융거래와 관련된 사무
3. 법 제22조제1항 및 제27조제1항에 따른 임직원 채용·고용 시 결격사유 확인에 관한 사무

③ 신용정보집중기관 및 법 제25조제4항에 따른 교환 대상자는 법 제25조제1항 및 제25조의2 각 호에 따른 업무를 수행하기 위해 불가피한 경우 개인식별번호를 수집·처리할 수 있다. 다만, 개인식별번호를 개인으로부터 직접 수집할 경우에는 그 개인의 동의를 받아야 한다.<신설 2014.8.6, 2015.9.11>

④ 제21조제2항에 따른 기관은 금융거래를 위하여 신용정보를 이용하는 사무를 수행하기 위하여 불가피한 경우 개인식별번호가 포함된 자료를 수집·처리할 수 있다. 다만, 개인식별번호를 개인으로부터 직접 수집할 경우에는 그 개인의 동의를 받아야 한다.<신설 2014.8.6,

2015.9.11 >

[본조신설 2012.1.6]

제38조(위반행위별 과태료의 부과기준) 법 제52조제1항부터 제4항까지의 규정에 따른 과태료의 부과기준은 별표 4와 같다.

부칙 <제21765호,2009.10.1 >

제1조(시행일) 이 영은 공포한 날부터 시행한다.

제2조(자본금에 관한 경과조치) 이 영 시행 당시 종전의 규정에 따라 허가를 받은 신용조사회사 및 채권추심회사는 2012년 결산 시까지 제7조의 개정규정에 적합하도록 하여야 한다.

제3조(다른 법령의 인용에 따른 경과조치) 2009년 11월 21일까지는 제21조제2항제12호의 개정규정 중 "「중소기업진흥에 관한 법률」"은 "「중소기업진흥 및 제품구매촉진에 관한 법률」"로 본다.

제4조(다른 법령의 개정) ① 건설산업기본법 시행령 일부를 다음과 같이 개정한다.

제58조제1항 및 제82조제4호 중 "신용정보업자에게"를 각각 "신용정보회사에"로 한다.

② 경제자유구역의 지정 및 운영에 관한 특별법 시행령 일부를 다음과 같이 개정한다.

제20조의4제1호 중 "신용정보업자"를 "신용정보회사"로 한다.

③ 국민기초생활 보장법 시행령 일부를 다음과 같이 개정한다.

제36조의2제1항 중 "「신용정보의 이용 및 보호에 관한 법률」 제2조제5호에 따른 신용정보집중기관"을 "「신용정보의 이용 및 보호에 관한 법률」 제2조제6호에 따른 신용정보집중기관"으로 한다.

④ 국세기본법 시행령 일부를 다음과 같이 개정한다.

제65조의4제15항제2호 중 "「신용정보의 이용 및 보호에 관한 법률」 제17조제2항제1호에 따른 종합신용정보집중기관"을 "「신용정보의 이용 및 보호에 관한 법률」 제25조제2항제1호에 따른 종합신용정보집중기관"으로 한다.

⑤ 국유재산법 시행령 일부를 다음과 같이 개정한다.

제46조제2호 중 "신용평가업자"를 "신용평가회사"로 한다.

⑥ 근로자복지기본법 시행령 일부를 다음과 같이 개정한다.

제8조제1항 중 "「신용정보의 이용 및 보호에 관한 법률」 제2조제4호의 규정에 의한 신용정보업자"를 "「신용정보의 이용 및 보호에 관한 법률」 제2조제5호에 따른 신용정보회사"로 한다.

⑦ 금융지주회사법 시행령 일부를 다음과 같이 개정한다.

제15조제1항제3호가목 중 "신용정보업자"를 "신용정보회사"로 한다.

제24조의5제1항제3호 중 "신용평가업무를 영위하는 신용정보업자"를 "신용평가업무를 수행하는 신용평가회사"로 한다.

⑧ 기업구조조정투자회사법시행령 일부를 다음과 같이 개정한다.
제5조제1항제20호 중 "신용정보의이용및보호에관한법률"을 "「신용정보의 이용 및 보호에 관한 법률」"로 한다.
⑨ 긴급복지지원법 시행령 일부를 다음과 같이 개정한다.
제8조 중 "「신용정보의 이용 및 보호에 관한 법률」 제2조제5호에 따른 신용정보집중기관"을 "「신용정보의 이용 및 보호에 관한 법률」 제2조제6호에 따른 신용정보집중기관"으로 한다.
⑩ 농、축산、임、어업용 기자재 및 석유류에 대한 부가가치세 영세율 및 면세 적용 등에 관한 특례규정 일부를 다음과 같이 개정한다.
제16조제1호다목 중 "「신용정보의 이용 및 보호에 관한 법률」 제17조제2항제1호에 따른 종합신용정보집중기관"을 "「신용정보의 이용 및 보호에 관한 법률」 제25조제2항제1호에 따른 종합신용정보집중기관"으로 한다.
⑪ 독점규제 및 공정거래에 관한 법률 시행령 일부를 다음과 같이 개정한다.
제21조의2 중 "「신용정보의 이용 및 보호에 관한 법률」 제2조(정의)제5호의 규정에 의한 신용정보집중기관"을 "「신용정보의 이용 및 보호에 관한 법률」 제2조제6호에 따른 신용정보집중기관"으로 한다.
⑫ 방문판매 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.
제17조제1호나목 중 "「신용정보의 이용 및 보호에 관한 법률」 제2조제4호의 규정에 의한 신용정보업자"를 "「신용정보의 이용 및 보호에 관한 법률」 제2조제5호에 따른 신용정보회사"로 한다.
⑬ 보험업법 시행령 일부를 다음과 같이 개정한다.
제57조제4항제2호 중 "신용평가업자"를 "신용평가회사"로 한다.
제84조제6호 중 "「신용정보의 이용 및 보호에 관한 법률」 제17조의 규정에 의하여"를 "「신용정보의 이용 및 보호에 관한 법률」 제25조에 따라"로 한다.
⑭ 부가가치세법 시행령 일부를 다음과 같이 개정한다.
제33조제1항제12호 중 "신용정보업자"를 "신용정보회사"로 한다.
⑮ 부동산투자회사법 시행령 일부를 다음과 같이 개정한다.
제33조제3항 중 "「신용정보의 이용 및 보호에 관한 법률」 제2조제4호의 규정에 의한 신용정보업자"를 "「신용정보의 이용 및 보호에 관한 법률」 제2조제5호에 따른 신용정보회사"로 한다.
<16> 산업발전법 시행령 일부를 다음과 같이 개정한다.
제12조제5호 중 "신용평가업자"를 "신용평가회사"로 한다.
<17> 상호저축은행법 시행령 일부를 다음과 같이 개정한다.
제12조의3제3호 중 "신용평가업자"를 "신용평가회사"로 한다.
<18> 소득세법 시행령 일부를 다음과 같이 개정한다.

제208조의5제5항제1호 중 "「신용정보의 이용 및 보호에 관한 법률」 제17조제2항에 따른 종합신용정보집중기관"을 "「신용정보의 이용 및 보호에 관한 법률」 제25조제2항제1호에 따른 종합신용정보집중기관"으로 한다.

<19> 여신전문금융업법 시행령 일부를 다음과 같이 개정한다.

제5조 중 "「신용정보의 이용 및 보호에 관한 법률 시행령」 제2조제2항제1호부터 제22호까지의 기관"을 "「신용정보의 이용 및 보호에 관한 법률 시행령」 제2조제3항제1호, 제3호, 제4호 및 제5조제1항제1호부터 제18호까지의 기관"으로, "「신용정보의 이용 및 보호에 관한 법률」 제17조제2항제1호에 따른 종합신용정보집중기관"을 "「신용정보의 이용 및 보호에 관한 법률」 제25조제2항제1호에 따른 종합신용정보집중기관"으로 한다.

제19조의13제3호 중 "신용평가업자"를 "신용평가회사"로 한다.

<20> 영유아보육법 시행령 일부를 다음과 같이 개정한다.

제21조의8제1항 각 호 외의 부분 중 "「신용정보의 이용 및 보호에 관한 법률」 제2조제5호에 따른 신용정보집중기관"을 "「신용정보의 이용 및 보호에 관한 법률」 제2조제6호에 따른 신용정보집중기관"으로 한다.

<21> 은행법 시행령 일부를 다음과 같이 개정한다.

제13조제1항제23호 및 제13조제3항제12호 중 "신용정보의이용및보호에관한법률"을 "「신용정보의 이용 및 보호에 관한 법률」"로 한다.

제20조의8제1항제3호 중 "신용정보의이용및보호에관한법률에 의한 신용평가업무를 영위하는 신용정보업자"를 "「신용정보의 이용 및 보호에 관한 법률」에 따른 신용평가업무를 수행하는 신용평가회사"로 한다.

<22> 자본시장과 금융투자업에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제11조제1항제1호라목, 제40조제2호, 제80조제5항제2호, 제183조제1항제1호, 제260조제2항제3호다목, 제328조제2항제1호 본문·단서, 같은 항 제2호 본문, 같은 조 제3항 본문, 같은 조 제4항 및 제338조제6항제2호 중 "신용평가업자"를 각각 "신용평가회사"로 한다.

<23> 자산유동화에관한법률시행령 일부를 다음과 같이 개정한다.

제5조제3호 중 "신용정보의이용및보호에관한법률 제9조제1항 각호의 사유"를 "「신용정보의 이용 및 보호에 관한 법률」 제27조제1항 각 호의 사유"로 한다.

<24> 전자금융거래법 시행령 일부를 다음과 같이 개정한다.

제2조제14호 중 "신용정보업자"를 "신용정보회사"로 한다.

<25> 전자상거래 등에서의 소비자보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제27조제1호나목 중 "「신용정보의 이용 및 보호에 관한 법률」 제2조제4호 및 제5호의 규정에 따른 신용정보업자 및 신용정보집중기관"을 "「신용정보의 이용 및 보호에 관한 법률」 제2조제5호 및 제6호에 따른 신용정보회사 및 신용정보집중기관"으로 한다.

<26> 제주특별자치도 설치 및 국제자유도시 조성을 위한 특별법 시행령 일부를 다음과 같이 개정한다.

제24조제1호 중 "신용정보업자"를 "신용정보회사"로 한다.

<27> 조세특례제한법 시행령 일부를 다음과 같이 개정한다.

제81조의2제1항 중 "「신용정보의 이용 및 보호에 관한 법률」 제9조의2의 규정에 의한 신용평가업자 중 2이상의 신용평가업자"를 "「신용정보의 이용 및 보호에 관한 법률」 제28조에 따른 신용평가회사 중 둘 이상의 신용평가회사"로 한다.

제83조의2 중 "「신용정보의 이용 및 보호에 관한 법률」 제17조제2항제1호의 규정에 의한 종합신용정보집중기관"을 "「신용정보의 이용 및 보호에 관한 법률」 제25조제2항제1호에 따른 종합신용정보집중기관"으로 한다.

제92조의6제1항 중 "「신용정보의 이용 및 보호에 관한 법률」 제4조제4항제4호의 업무에 관한 허가를 받은 자(이하 이 조에서 "신용평가업자"라 한다) 중 2인 이상의 신용평가업자"를 "「신용정보의 이용 및 보호에 관한 법률」 제4조제1항제4호의 업무에 관한 허가를 받은 자(이하 이 조에서 "신용평가회사"라 한다) 중 둘 이상의 신용평가회사"로 한다.

<28> 질서위반행위규제법 시행령 일부를 다음과 같이 개정한다.

별지 제3호서식 중 "신용정보업자"를 "신용정보회사"로 한다.

<29> 학술진흥 및 학자금대출 신용보증 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제44조제1항 중 "신용정보업자"를 "신용정보회사"로 한다.

<30> 한국장학재단 설립 등에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제36조제2항 중 "신용정보업자"를 "신용정보회사"로 한다.

<31> 한국주택금융공사법 시행령 일부를 다음과 같이 개정한다.

제31조제1항제2호 중 "신용정보업자"를 "신용정보회사"로 한다.

제5조 (다른 법령과의 관계) 이 영 시행 당시 다른 법령에서 종전의 「신용정보의 이용 및 보호에 관한 법률 시행령」의 규정을 인용한 경우에 이 영 가운데 그에 해당하는 규정이 있으면 종전의 규정을 갈음하여 이 영의 해당 규정을 인용한 것으로 본다.

부칙 <제22151호,2010.5.4>

제1조(시행일) 이 영은 2010년 5월 5일부터 시행한다.

제2조 및 제3조 생략

제4조(다른 법령의 개정) ① 부터 <110> 까지 생략

<111> 신용정보의 이용 및 보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제4조 각 호 외의 부분 후단, 제9조제4항 각 호 외의 부분 및 제21조제1항 각 호 외의 부분 후단 중 "「전자정부법」 제21조제1항 또는 제22조의2제1항"을 각각 "「전자정부법」 제36조제1항 또는 제2항"으로 한다.

제19조제3항 중 "「전자정부법」 제22조제4항"을 "「전자정부법」 제37조제1항"으로 한다.

<112> 부터 <192> 까지 생략

부칙 <제22220호,2010.6.28>

제1조(시행일) 이 영은 2010년 7월 6일부터 시행한다.

제2조(다른 법령의 개정) ① 부터 ④ 까지 생략

⑤ 신용정보의 이용 및 보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제5조제1항제20호를 다음과 같이 한다.

20. 「무역보험법」에 따른 한국무역보험공사

⑥ 부터 ⑭ 까지 생략

제3조 생략

부칙 <제22467호,2010.11.2>

이 영은 공포한 날부터 시행한다.

부칙 <제22493호,2010.11.15>

제1조(시행일) 이 영은 2010년 11월 18일부터 시행한다.

제2조 및 제3조 생략

제4조(다른 법령의 개정) ①부터 <68>까지 생략

<69> 신용정보의 이용 및 보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제5조제1항제1호 중 "금융기관"을 각각 "은행"으로 한다.

<70>부터 <115>까지 생략

제5조 생략

부칙 <제22626호,2011.1.17>

제1조(시행일) 이 영은 공포한 날부터 시행한다.

제2조부터 제4조까지 생략

제5조(다른 법령의 개정) ①부터 <17>까지 생략

<18> 신용정보의 이용 및 보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제21조제2항제7호 중 "「엔지니어링기술 진흥법」"을 "「엔지니어링산업 진흥법」"으로 한다.

<19>부터 <39>까지 생략

제6조 생략

부칙 <제23076호,2011.8.17>

제1조(시행일) 이 영은 2011년 8월 20일부터 시행한다.

제2조(신용조회회사의 보고에 관한 적용례) 제18조의2제1항의 개정규정은 신용조회회사가 2012년 1월 1일부터 12월 31일까지 수행한 업무내용의 보고부터 적용한다.

제3조(신용정보활용체제의 공시에 관한 적용례) 제27조제2항제7호의 개정규정은 이 영 시행 후 최초로 공시하는 것부터 적용한다.

제4조(무료 열람권의 기준일에 대한 적용례) 제34조의 개정규정은 이 영 시행 후 최초로 신용조회회사로부터 본인정보를 제공받거나 열람하는 자부터 적용한다.

제5조(신용정보의 활용기간 등에 관한 경과조치) 이 영 시행 당시 신용정보회사등에 등록·관리되어 있는 신용정보로서 법 제18조제2항에 따른 불이익 사유가 해소된 경우에는 제15조제4항부터 제6항까지의 개정규정에도 불구하고 종전의 규정에 따른다.

제6조(신용정보주체에 대한 통지 또는 공시에 대한 경과조치) 이 영 시행 당시 종전의 규정에 따라 신용정보주체에 대하여 행하여지고 있는 통지 또는 공시는 제28조제9항 또는 제10항의 개정규정에 따른 통지 또는 공시로 본다.

부칙 <제23488호,2012.1.6>

제1조(시행일) 이 영은 공포한 날부터 시행한다. <단서 생략>

제2조 생략

부칙 <제23535호,2012.1.25>

제1조(시행일) 이 영은 2012년 1월 26일부터 시행한다.

제2조(다른 법령의 개정) ①부터 ⑭까지 생략

⑮ 신용정보의 이용 및 보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제21조제2항제3호를 다음과 같이 한다.

3. 「한국농수산식품유통공사법」에 따른 한국농수산식품유통공사

<16>부터 <28>까지 생략

제3조 생략

부칙 <제24076호,2012.8.31>

제1조(시행일) 이 영은 2012년 9월 2일부터 시행한다. <단서 생략>

제2조 생략

제3조(다른 법령의 개정) ①부터 ⑨까지 생략

⑩ 신용정보의 이용 및 보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제30조제1항제1호 및 제33조제1항제1호 중 "「전자거래기본법」"을 각각 "「전자문서 및 전자거래 기본법」"으로 한다.

⑪부터 <16>까지 생략

제4조 생략

부칙 <제24697호,2013.8.27>

제1조(시행일) 이 영은 2013년 8월 29일부터 시행한다. <단서 생략>

제2조부터 제11조까지 생략

제12조(다른 법령의 개정) ①부터 <24>까지 생략

<25> 신용정보의 이용 및 보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제3조제3호를 삭제한다.

제6조제1항제1호가목 중 "신용조회업무(신용정보의 분석에 관한 업무와 신용평가업무를 포함한다)"를 "신용조회업무(신용정보의 분석에 관한 업무를 포함한다)"로 한다.

제6조제1항제3호, 제9조제1항제2호, 제25조 및 제26조 각각 삭제한다.

<26>부터 <35>까지 생략

제13조 생략

부칙 <제25155호,2014.2.11>

제1조(시행일) 이 영은 2014년 2월 14일부터 시행한다.

제2조(다른 법령의 개정) 신용정보의 이용 및 보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제2조제1항제5호나목 중 "지방세 또는 관세"를 "지방세·관세 또는 국가채권"으로 한다.

부칙 <제25532호,2014.8.6>

이 영은 2014년 8월 7일부터 시행한다.

부칙 <제25945호,2014.12.30>

제1조(시행일) 이 영은 법률 제12663호 한국산업은행법 전부개정법률 부칙 제4조제6항에 따른 합병의 등기를 한 날부터 시행한다.

제2조 및 제3조 생략

제4조(다른 법령의 개정) ①부터 <23>까지 생략

<24> 신용정보의 이용 및 보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제5조제1항제5호를 삭제한다.

<25>부터 <37>까지 생략

제5조 생략

부칙 <제26369호,2015.6.30>

제1조(시행일) 이 영은 2015년 7월 1일부터 시행한다.

제2조 생략

제3조(다른 법령의 개정) ①부터 <18>까지 생략

<19> 신용정보의 이용 및 보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제21조제2항제11호를 다음과 같이 한다.

11. 「주택도시기금법」에 따른 주택도시보증공사

<20>부터 <32>까지 생략

제4조 생략

부칙 <제26517호,2015.9.11>

제1조(시행일) 이 영은 2015년 9월 12일부터 시행한다. 다만, 제16조의2, 제17조의2, 제28조, 제29조, 제30조, 제33조의2, 제33조의3의 개정규정은 2016년 3월 12일부터 시행한다.

제2조(금치산자 등에 관한 경과조치) 제2조제1항제5호의 개정규정에 따른 성년후견ㆍ한정후견ㆍ특정후견과 관련된 심판에는 법률 제10429호 민법 일부개정법률 부칙 제2조에 따라 금치산 또는 한정치산 선고의 효력이 유지되는 사람에 대한 금치산 또는 한정치산과 관련된 심판이 포함되는 것으로 본다.

제3조(신용정보관리ㆍ보호인의 지정 등에 관한 경과조치) 제17조제1항 및 제2항의 개정규정에 해당하는 자는 이 영 시행 이후 3개월 이내에 법 제20조제3항에 적합하도록 하여야 한다.

제4조(손해배상 책임의 이행을 위한 보험 등 가입의무가 있는 신용정보회사등의 범위에 관한 경과조치) 제35조의9의 개정규정에 해당하는 자는 이 영 시행 이후 1개월 이내에 법 제43조의3에 적합하도록 하여야 한다.

제5조(과태료의 부과기준에 관한 경과조치) 이 영 시행 전의 행위에 대하여 과태료의 부과기준을 적용할 경우에는 별표4의 개정규정에도 불구하고 종전의 규정에 따른다.

제6조(다른 법령의 개정) ① 건설산업기본법 시행령 일부를 다음과 같이 개정한다.

제58조제1항 중 " 「신용정보의 이용 및 보호에 관한 법률」의 규정에 따라 지정되거나 등록한 신용정보집중기관"을 " 「신용정보의 이용 및 보호에 관한 법률」에 따라 허가받은 신용정보집중기관"으로 한다.

② 국유재산법 시행령 일부를 다음과 같이 개정한다.

국유재산법 시행령 제46조제2호를 다음과 같이 한다.

2. 「자본시장과 금융투자업에 관한 법률」에 따른 신용평가회사

③ 보험업법 시행령 일부를 다음과 같이 개정한다.

제84조제6호 중 "「신용정보의 이용 및 보호에 관한 법률」 제25조에 따라 금융위원회에 등록을 하여"를 "「신용정보의 이용 및 보호에 관한 법률」 제25조에 따라 금융위원회로부터 허가를 받아"로 한다.

④ 새만금사업 추진 및 지원에 관한 특별법 시행령 일부를 다음과 같이 개정한다.

제46조제1호 중 "「신용정보의 이용 및 보호에 관한 법률」 제4조에 따라 신용평가업무에 관한 금융위원회의 허가를 받은 둘 이상의 신용정보회사"를 "둘 이상의 신용평가회사(「자본시장과 금융투자업에 관한 법률」 에 따른 신용평가회사를 말한다)"로 한다.

⑤ 여신전문금융업법 시행령 일부를 다음과 같이 개정한다.

제6조의7제3항제2호 중 "「신용정보의 이용 및 보호에 관한 법률 시행령」 제30조제1항 각 호"를 "「신용정보의 이용 및 보호에 관한 법률 시행령」 제30조제3항 후단"으로 하고, 제19조의19제2항 전단 중 "같은 법 시행령 제28조제2항부터 제4항까지의"를 "같은 법 시행령 제28조제2항 및 제3항의"로 하며, 같은 항 후단 중 ""대출, 보증에 관한 정보 등 대통령령으로 정하는 신용정보"는 "신용정보"로 본다."를 ""개인신용정보"는 "신용정보"로 본다."로 한다.

부칙 <제27037호,2016.3.11>

제1조(시행일) 이 영은 공포한 날부터 시행한다.

제2조(다른 법령의 개정) ①부터 ⑪까지 생략

⑫ 신용정보의 이용 및 보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제5조제1항제21호 및 제21조제2항제8호 중 "정리금융기관"을 각각 "정리금융회사"로 한다.

⑬부터 <17>까지 생략

부칙 <제27070호,2016.3.29>

이 영은 공포한 날부터 시행한다.

부칙 <제27205호,2016.5.31>

제1조(시행일) 이 영은 2016년 9월 30일부터 시행한다. <단서 생략>

제2조(다른 법령의 개정) ①부터 <35>까지 생략

<36> 신용정보의 이용 및 보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제5조제1항제17호를 다음과 같이 한다.

17. 「기술보증기금법」에 따른 기술보증기금

<37>부터 <59>까지 생략

제3조 생략

부칙 <제27322호,2016.7.6>

제1조(시행일) 이 영은 2016년 7월 25일부터 시행한다.

제2조 및 제3조 생략

제4조(다른 법령의 개정) ① 및 ② 생략

③ 신용정보의 이용 및 보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제21조제2항제19호를 다음과 같이 한다.

19. 「대부업 등의 등록 및 금융이용자 보호에 관한 법률」 제3조제2항에 따라 금융위원회에 등록한 대부업자등

④ 및 ⑤ 생략

부칙 <제27511호,2016.9.22>

제1조(시행일) 이 영은 2016년 9월 23일부터 시행한다.

제2조부터 제6조까지 생략

제7조(다른 법령의 개정) ①부터 ④까지 생략

⑤ 신용정보의 이용 및 보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제11조의2제7호를 다음과 같이 한다.

7. 「서민의 금융생활 지원에 관한 법률」 제56조에 따른 신용회복위원회

제17조의2제3항제1호 중 "「휴면예금관리재단의 설립 등에 관한 법률」 제2조제3호에"를 "「서민의 금융생활 지원에 관한 법률」 제2조제3호에"로 한다.

제19조제1항제7호를 다음과 같이 한다.

7. 「서민의 금융생활 지원에 관한 법률」 제56조에 따른 신용회복위원회

제21조제2항제4호 및 제18호를 각각 다음과 같이 한다.

4. 「서민의 금융생활 지원에 관한 법률」 제56조에 따른 신용회복위원회

18. 「서민의 금융생활 지원에 관한 법률」 제3조에 따른 서민금융진흥원

⑥부터 ⑨까지 생략

제8조 생략

부칙 <제27556호,2016.10.25>

제1조(시행일) 이 영은 2016년 12월 1일부터 시행한다.

제2조(다른 법령의 개정) ①부터 <16>까지 생략

<17> 신용정보의 이용 및 보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제5조제1항에 제5호의2를 다음과 같이 신설한다.

5의2. 「수산업협동조합법」에 따른 수협은행

<18>부터 <23>까지 생략

부칙 <제27786호,2017.1.10>

이 영은 공포한 날부터 시행한다.

[별표 1]

주요출자자 요건(제6조제4항 및 제9조제2항 관련)

요건	구분
1. 주요출자자가 「금융위원회의 설치 등에 관한 법률」 제38조에 따라 금융감독원으로부터 검사를 받는 기관인 경우	가. 최근 사업연도 말 현재 대차대조표상 자산총액에서 부채총액을 뺀 금액(이하 "자기자본"이라 한다)이 출자하려는 금액의 2배 이상일 것 나. 재무상태가 다음 기준을 충족할 것 1) 적용되는 「금융산업의 구조개선에 관한 법률」에 적기시정조치의 기준이 규정된 경우에는 그 금융기관의 재무상태가 해당 기준을 넘을 것 2) 적용되는 「금융산업의 구조개선에 관한 법률」에 적기시정조치의 기준이 규정되지 않은 경우에는 그 금융기관이 경영하는 업종과 유사한 업종을 경영하는 금융기관에 적용되는 적기시정조치의 기준을 넘을 것. 다만, 그 금융기관에 대하여 유사 업종의 적기시정조치 기준을 적용하는 것이 현저히 부적합한 경우에는 가목·다목·라목의 기준을 충족하여야 한다. 다. 자본금 납입자금은 주요출자자의 출자능력을 초과하여 금융기관 등으로부터 단순 차입(출자자가 법인인 경우에는 기업어음·회사채 발행 등 부채성 조달자금을 포함한다)에 의한 것이 아니고, 그 출처가 명확할 것 라. 다음 요건을 충족할 것. 다만, 그 사실이 경영하려는 업무의 건전한 경영을 어렵게 한다고 볼 수 없는 경우에는 그러하지 아니하다. 1) 최근 5년간 채무불이행 등으로 건전한 신용질서를 해친 사실이 없을 것 2) 최근 5년간 법, 이 영, 금융 관계 법령(「여신전문금융업법 시행령」 제6조 각 호에 규정된 법령을 말한다), 「독점규제 및 공정거래에 관한 법률」 및 「조세범 처벌법」을 위반하여 벌금 이상의 처벌을 받은 사실이 없을 것 3) 그 밖에 금융위원회가 정하는 건전한 금융거래질서를 해친 사실이 없을 것

2. 주요출자자가 제1호 외의 내국법인인 경우	제1호가목·다목 및 라목의 요건을 충족할 것
3. 주요출자자가 내국인으로서 개인인 경우	가. 제1호다목 및 라목의 요건을 충족할 것 나. 법 제22조제1항 각 호의 어느 하나에 해당되지 않을 것
4. 주요출자자가 외국 법령에 따라 설립된 외국기업인 경우	가. 제1호가목·다목 및 라목의 요건을 충족할 것 나. 국제적으로 인정받는 신용평가기관으로부터 투자적격 이상의 신용평가등급을 받거나 본국의 감독기관이 정하는 재무건전성에 관한 기준을 충족하고 있다는 사실이 확인될 것 다. 최근 3년간 기업의 경영과 관련하여 본국의 감독기관으로부터 법인경고 이상에 해당하는 행정처분을 받거나 벌금형 이상에 해당하는 형사처벌을 받은 사실이 없을 것

[별표 2] <개정 2015.9.11.>

종합신용정보집중기관을 통하여 집중관리·활용되는 신용정보의 범위

(제21조제3항 관련)

1. 개인

구분	집중관리·활용 대상 정보
가. 식별정보	성명 및 개인식별번호
나. 신용거래정보	1) 대출·당좌거래 등에 관한 거래정보로서 다음 가)부터 다)까지의 정보 가) 대출 현황 나) 당좌예금·가계당좌예금의 개설 및 해지 사실 다) 담보 및 채무보증 현황 2) 신용카드에 관한 거래정보로서 다음 가)부터 다)까지의 정보 가) 신용카드의 발급·해지 사실 및 결제·미결제 금액(결제금액은 해당 신용정보를 보유한 신용카드업자가 동의하는 경우만 해당한다) 나) 2개 이상의 신용카드를 소지한 신용정보주체의 신용카드 이용금액, 이용한도, 신용카드에 의한 현금융통한도 다) 신용카드의 분실·도난 등 사고 발생, 그 발생한 사고 종결에 따른 보상, 그 밖의 사고 종결의 처리 사실 3) 보험상품에 관한 거래정보로서 다음 가) 및 나)의 구분에 따른 정보. 이 경우 보험계약자가 기업, 법인 및 단체인 경우에도 피보험자 또는 보험금청구권자(보험수익자, 피보험자 또는 손해보험계약의 제3자 등으로서 보험금을 청구할 권리가 있는 자를 말한다. 이하 같다)가 개인인 경우에는 그 보험상품을 포함한다. 가) 보험계약의 체결에 관한 정보: 보험계약 현황, 보험계약의 피보험자 또는 보험금청구권자에 관한 정보(성명, 개인식별번호, 직업 및 보험계약자와의 관계에 관한 정보를 말한다) 및 해당 보험계약을 모집한 모집업무수탁자에 관한 정보 나) 보험금의 청구 및 지급에 관한 정보: 보험금의 청구·지급 현황, 보험금의 지급 사유(질병에 관한 정보, 손해보험계약에 따른 보험목적에 생긴 손해 사실, 그 밖의 보험사고에 관한 정보를 포함한다), 보험금청구권자(책임보험계약에 따라 손해를 보상받는 피해자를 포함한다)에 관한 정보(성명, 개인식별번호, 피보험자와의 관계에 관한 정보를 말한다)

다. 신용도판단정보 등	1) 대출금, 신용카드 대금, 시설대여 이용료 등의 연체 사실 2) 대위변제·대지급 발생 사실 3) 어음·수표의 거래정지처분을 받은 사실 및 그 부도 사실 4) 증권의 투자매매업·투자중개업에 관한 정보로서 다음 가) 및 나)의 정보 가) 증권시장에 상장된 증권의 매매와 관련하여 투자중개업자에게 매수대금 또는 매도증권을 결제일까지 납입하지 아니한 사실 나) 증권시장에 상장된 증권의 매매를 위하여 투자자에게 제공하는 매수대금의 융자 또는 매도증권의 대여 거래에 관한 정보로서 상환 또는 납입기일까지 그 거래에 따른 채무를 이행하지 아니한 사실 5) 금융질서 문란 정보로서 다음 가)부터 라)까지의 정보 가) 대출금 등을 용도 외로 유용한 사실 및 부정한 방법으로 대출을 받는 등 신용질서를 문란하게 한 사실 나) 거짓이나 그 밖의 부정한 방법으로 신용카드를 발급받거나 사용한 사실 다) 보험사기 사실 라) 그 밖에 가)부터 다)까지의 사실과 비슷한 것으로서 금융질서를 문란하게 한 사실 6) 공공기관이 만들어 낸 정보로서 다음 가)부터 마)까지의 정보 가) 법원의 회생·간이회생·개인회생과 관련된 결정, 파산선고·면책·복권과 관련된 결정, 채무불이행자명부의 등재·말소 결정 사실 나) 국세·지방세·관세 또는 국가채권과 벌금·과태료·과징금·추징금 등의 체납 관련 정보 다) 사회보험료·공공요금 또는 수수료 등 관련 정보 라) 주민등록 관련 정보로서 출생·사망·이민·부재에 관한 정보, 주민등록번호·성명의 변경 등에 관한 정보 마) 다른 법령에 따라 국가, 지방자치단체 또는 공공기관으로부터 받은 행정처분에 관한 정보 중에서 금융거래 등 상거래와 관련된 정보

2. 기업 및 법인

구분	집중관리·활용 대상 정보

가. 식별정보	기업 및 법인의 상호 및 명칭, 사업자등록번호, 법인등록번호 및 고유번호, 본점·영업소 및 기관의 소재지, 종목, 대표자의 성명·개인식별번호
나. 신용거래정보	1) 대출·당좌거래 등에 관한 거래정보로서 다음 가)부터 사)까지의 정보 가) 대출·지급보증 등 신용공여 현황 나) 시설대여 현황 다) 신용보증 현황 라) 보증보험 현황 마) 담보 및 채무보증 현황 바) 당좌예금·가계당좌예금의 개설 및 해지 사실 사) 가)부터 바)까지의 정보로서 해당 기업 및 법인의 기술과 관련된 기술성·시장성·사업성 등을 종합적으로 평가함으로써 만들어진 정보 2) 신용카드에 관한 거래정보로서 다음 가) 및 나)의 정보 가) 신용카드의 발급·해지 사실 및 결제·미결제 금액(결제금액은 해당 신용정보를 보유한 신용카드업자가 동의하는 경우만 해당한다) 나) 신용카드의 분실·도난 등 사고 발생, 그 발생한 사고 종결에 따른 보상, 그 밖의 사고 종결의 처리 사실
다. 신용도판단정보(제2조제1항제3호 각 목의 어느 하나에 해당하는 자의 정보도 포함한다)	1) 기업 및 법인의 신용도 판단 정보로서 다음 가)부터 바)까지의 정보 가) 대출금, 신용카드 자금, 시설대여 이용료 등의 연체 사실 나) 대위변제·대지급 발생 사실 다) 신용보증기금이 대위변제한 사실 라) 어음·수표의 거래정지처분을 받은 사실 및 그 부도 사실 마) 무보증사채의 상환불이행 사실 바) 가)부터 마)까지의 정보로서 해당 기업 및 법인의 기술과 관련된 기술성·시장성·사업성 등을 종합적으로 평가함으로써 이루어진 대출, 신용보증 등에 대하여 연체, 대위변제 등이 발생한 사실 2) 증권의 투자매매업·투자중개업에 관한 정보로서 다음 가) 및 나)의 정보 가) 증권시장에 상장된 증권의 매매와 관련하여 투자중개업자에게 매수대금 또는 매도증권을 결제일까지 납입하지 아니한 사실 나) 증권시장에 상장된 증권의 매매를 위하여 투자자에게

	제공하는 매수대금의 융자 또는 매도증권의 대여 거래에 관한 정보로서 상환 또는 납입기일까지 그 거래에 따른 채무를 이행하지 아니한 사실 3) 금융질서 문란 정보로서 다음 가)부터 라)까지의 정보 가) 대출금 등을 용도 외로 유용한 사실 및 부정한 방법으로 대출을 받는 등 신용질서를 문란하게 한 사실 나) 거짓이나 그 밖의 부정한 방법으로 신용카드를 발급받거나 사용한 사실 다) 보험사기 사실 라) 그 밖에 가)부터 다)까지의 사실과 비슷한 것으로서 금융질서를 문란하게 한 사실 4) 공공기관이 만들어 낸 정보로서 다음 가)부터 마)까지의 정보 가) 법원의 회생·간이회생·개인회생과 관련된 결정, 파산선고·면책·복권과 관련된 결정, 채무불이행자명부의 등재·말소 결정 사실 나) 국세·지방세·관세 또는 국가채권과 벌금·과태료·과징금·추징금 등의 체납 관련 정보 다) 사회보험료·공공요금 또는 수수료 등 관련 정보 라) 주민등록 관련 정보로서 출생·사망·이민·부재에 관한 정보, 주민등록번호·성명의 변경 등에 관한 정보 마) 다른 법령에 따라 국가, 지방자치단체 또는 공공기관으로부터 받은 행정처분에 관한 정보 중에서 금융거래 등 상거래와 관련된 정보
라. 신용거래능력 판단정보 등	1) 계열기업체 현황 등 회사의 개황 2) 사업의 내용 3) 재무제표 등 재무에 관한 사항 4) 자본금 증자 및 사채 발행 현황 5) 기업의 영업에 관한 정보로서 다음 가) 및 나)의 정보 가) 정부조달 실적 또는 수출·수입액 등의 관련 정보 나) 기술신용정보 및 이와 관련된 신용정보 6) 기업등록 관련 정보로서 설립, 휴업·폐업, 양도·양수, 분할·합병, 주식 또는 지분 변동 등에 관한 정보

[별표 2의2] <개정 2017. 1. 10.>

개인신용정보의 제공 사실 및 이유 등을 알리거나 공시하는 시기 및 방법
(제28조제12항 관련)

제공의 이유	알리거나 공시하는 자	알리거나 공시하는 시기	알리거나 공시하는 방법
1. 법 제32조제6항제1호에 따라 신용정보회사가 다른 신용정보회사 또는 신용정보집중기관과 서로 집중관리·활용하기 위하여 개인신용정보를 제공하는 경우	개인신용정보를 제공하는 자	개인신용정보를 제공한 날부터 7일 이내	제34조의2제2항제1호 또는 제2호의 방법
2. 법 제32조제6항제2호에 따라 계약의 이행에 필요한 경우로서 법 제17조제2항에 따라 개인신용정보의 처리를 위탁하기 위하여 제공하는 경우	개인신용정보를 제공하는 자	개인신용정보를 제공하기 전까지	제34조의2제2항제1호 또는 제2호의 방법
3. 법 제32조제6항제3호에 따라 영업양도·분할·합병 등의 이유로 권리·의무의 전부 또는 일부를 이전하면서 그와 관련된 개인신용정보를 제공하는 경우	개인신용정보를 제공하는 자	개인신용정보를 제공하기 전까지	다음 각 목의 구분에 따른 방법 가. 일반적인 경우: 서면, 전화, 문자메시지, 전자우편, 팩스 그 밖에 이와 유사한 방법으로 해당 신용정보주체에게 그 사실을 개별적으로 알리는 방법(제4호의 경우에는 수임사실의 통지와 함께 알리는 방법을 포함한다) 나. 고의 또는 과실
4. 법 제32조제6항제4호 및 이 영 제28조제10항제1호에 따라 채권추심을 의뢰한 채권자가 채권추심의 대상이 되는 자의 개인신용정보를 채권추심회사에 제공하는 경우	채권추심회사	「채권의 공정한 추심에 관한 법률」 제6조에 따른 수임사실의 통지(이하 이 호에서 "수임사실의 통지"라 한다)를 하는 때까지	
5. 법 제32조제6항제4	채권추심	개인신용정보를 제	

호 및 이 영 제28조제10항제1호에 따라 채권추심회사가 채권추심의 대상이 되는 자의 개인신용정보를 채권자에게 제공하는 경우	회사	공하기 전까지	없이 신용정보주체의 연락처 등을 알 수 없는 경우: 제34조의2제2항 각 호의 어느 하나에 해당하는 방법
6. 법 제32조제6항제4호 및 이 영 제28조제10항제2호에 따라 채권자 또는 채권추심회사가 변제기일까지 채무를 변제하지 않은 자 또는 채권추심의 대상이 되는 자에 대한 개인신용정보를 신용조회회사로부터 제공받는 경우	채권자 또는 채권추심회사	개인신용정보를 제공받기 전까지	
7. 법 제32조제6항제4호 및 이 영 제28조제10항제3호에 따라 행정기관이 인가·허가 업무에 사용하기 위하여 신용조회회사로부터 개인신용정보를 제공받는 경우	해당 행정기관	개인신용정보를 제공받기 전까지	서면, 전화, 문자메시지, 전자우편, 팩스 그 밖에 이와 유사한 방법으로 해당 신용정보주체에게 그 사실을 개별적으로 알리는 방법
8. 법 제32조제6항제4호 및 이 영 제28조제10항제4호에 따라 해당 기업과의 금융거래 등 상거래관계의 설정 및 유지 여부 등을 판단하기 위하여 그 기업의 대표자 및 제2조제1항제3호 각 목의 어느 하나에 해당하는 자의 개인신용정보를 신용	개인신용정보를 제공받는 자	개인신용정보를 제공받기 전까지	

정보집중기관 및 신용조회회사로부터 제공받는 경우			
9. 법 제32조제6항제4호 및 이 영 제28조제10항제5호에 따라 제21조제2항에 따른 금융기관이 상거래관계의 설정 및 유지 여부 등을 판단하기 위하여 또는 어음·수표 소지인이 어음·수표의 발행인, 인수인, 배서인 및 보증인의 변제 의사 및 변제자력을 확인하기 위하여 신용정보집중기관 및 신용조회회사로부터 어음·수표의 발행인, 인수인, 배서인 및 보증인의 개인신용정보를 제공받는 경우	개인신용정보를 제공받는 자	개인신용정보를 제공받기 전까지	다음 각 목의 구분에 따른 방법 가. 일반적인 경우: 서면, 전화, 문자메시지, 전자우편, 팩스, 그 밖에 이와 유사한 방법으로 해당 신용정보주체에게 그 사실을 개별적으로 알리는 방법 나. 고의 또는 과실 없이 신용정보주체의 연락처 등을 알 수 없는 경우: 제34조의2제2항 각 호의 어느 하나에 해당하는 방법
10. 법 제32조제6항제4호 및 이 영 제28조제10항제6호에 따라 지명채권을 양수한 신용정보제공·이용자가 그 지명채권의 채무자의 개인신용정보를 신용조회회사 또는 신용정보집중기관에 제공하거나 신용조회회사 또는 신용정보집중기관으로부터 제공받는 경우	신용정보제공·이용자	개인신용정보를 제공하거나 제공받은 날부터 7일 이내	
10의2. 법 제32조제6항제4호 및 이 영 제28조제10항제7호	개인신용정보를 제공하는 자	개인신용정보를 제공하기 전까지	제34조의2제2항제1호 또는 제2호의 방법

에 따라 통계작성 및 학술연구 등을 위하여 필요한 경우로서 신용정보회사 등으로부터 개인신용정보를 특정 개인을 알아볼 수 없는 형태로 제공받는 경우			
11. 법 제32조제6항제5호에 따라 법원의 제출명령 또는 법관이 발부한 영장에 따라 제공하는 경우	개인신용정보를 제공하는 자	개인신용정보를 제공한 날부터 6개월 이내. 다만, 개인신용정보의 제공을 요구하는 자가 다음 각 목의 어느 하나에 해당하는 사유가 지속된다는 사실을 소명하고 개인신용정보의 제공 사실 및 이유 등을 알리는 것의 유예를 서면으로 반복하여 요청하는 경우에는 금융위원회가 정하여 고시하는 기간 동안 그 제공 사실 및 이유 등을 알리는 것을 유예할 수 있다. 가. 그 제공 사실 및 이유 등을 알리는 것이 사람의 생명이나 신체의 안전을 위협할 우려가 있는 경우 나. 그 제공 사실 및 이유 등을 알리는 것이 증거 인멸, 증인 위협	다음 각 목의 구분에 따른 방법 가. 일반적인 경우: 서면, 전화, 문자메시지, 전자우편, 팩스, 그 밖에 이와 유사한 방법으로 해당 신용정보주체에게 그 사실을 개별적으로 알리는 방법 나. 고의 또는 과실 없이 신용정보주체의 연락처 등을 알 수 없는 경우: 제34조의2제2항 각 호의 어느 하나에 해당하는 방법
12. 법 제32조제6항제6호에 따라 범죄 때문에 피해자의 생명이나 신체에 심각한 위험 발생이 예상되는 등 긴급한 상황에서 같은 항 제5호에 따른 법관의 영장을 발부받을 시간적 여유가 없는 경우로서 검사 또는 사법경찰관의 요구에 따라 제공하는 경우	개인신용정보를 제공하는 자		

13. 법 제32조제6항제7호에 따라 조세에 관한 법률에 따른 질문·검사 또는 조사를 위하여 관할 관서의 장이 서면으로 요구하거나 조세에 관한 법률에 따라 제출의무가 있는 과세자료의 제공을 요구함에 따라 제공하는 경우	개인신용정보를 제공하는 자	등 공정한 사법절차의 진행을 방해할 우려가 명백한 경우 다. 그 제공 사실 및 이유 등을 알리는 것이 질문·조사 등의 행정절차의 진행을 방해하거나 과도하게 지연시킬 우려가 명백한 경우	
14. 법 제32조제6항제8호에 따라 국제협약 등에 따라 외국의 금융감독기구에 금융회사가 가지고 있는 개인신용정보를 제공하는 경우	개인신용정보를 제공하는 자	개인신용정보를 제공하기 전까지	
15. 법 제32조제6항제9호 및 이 영 제28조제11항에 따라 금융질서문란행위자 및 기업의 과점주주, 최다출자자 등 관련인의 신용도를 판단할 수 있는 정보를 제공하는 경우	개인신용정보를 제공하는 자	개인신용정보를 제공하기 전까지	
16. 법 제32조제6항제10호에 따른 다른 법률에 따라 제공하는 경우	개인신용정보를 제공하는 자	다음 각 목의 구분에 따른 기한 가. 개인신용정보 제공의 근거가 되는 법률에서 정하는 바가 없는 경우: 개인신용정보를 제공하기 전까지 나. 개인신용정보	다음 각 목의 구분에 따른 방법. 다만, 개인신용정보의 제공의 근거가 되는 법률에서 알리거나 공시하는 방법을 달리 정하는 경우에는 그에 따른다. 가. 일반적인 경우: 서면, 전화, 문자

		제공의 근거가 되는 법률에서 사후에 알리거나 공시하는 것을 정한 경우로서 해당 법률에서 그 기한을 정하지 않은 경우: 개인신용정보를 제공한 날을 기준으로 6개월 이내 다. 개인신용정보 제공의 근거가 되는 법률에서 사후에 알리거나 공시하는 것을 정한 경우로서 해당 법률에서 그 기한을 정한 경우: 해당 법률에서 정한 기한	메시지, 전자우편, 팩스 그 밖에 이와 유사한 방법으로 해당 신용정보주체에게 그 사실을 알리는 방법 나. 고의 또는 과실 없이 신용정보주체의 연락처 등을 알 수 없는 경우: 제34조의2제2항 각 호의 어느 하나에 해당하는 방법

[별표 3] <개정 2015.9.11.>

금융위원회가 금융감독원장에게 위탁하는 권한의 범위

(제37조제1항 관련)

1. 법 제4조에 따른 신용정보업 허가 신청의 접수
1의2. 법 제4조제1항제1호가목에 따른 승인
2. 법 제8조에 따른 허가받은 사항 변경에 관한 신고의 수리 또는 보고의 접수
3. 법 제9조제1항에 따른 지배주주 변경승인 신청의 접수
4. 법 제10조제1항에 따른 신용정보업 양도·양수의 인가 신청의 접수
5. 법 제10조제4항에 따른 신용정보업 전부 또는 일부의 휴업·폐업에 관한 신고의 수리
6. 법 제11조제1항에 따른 겸업 신고의 수리 및 같은 조 제2항 단서에 따른 겸업 승인 신청의 접수
7. 법 제13조에 따른 신용정보회사의 상임 임원이 다른 영리법인의 상무에 종사하는 것에 대한 승인 신청의 접수
8. 법 제17조제3항에 따른 신용정보의 처리 위탁에 관한 보고의 접수
8의2. 법 제20조제5항에 따른 신용정보관리·보호인의 보고의 접수
8의3. 법 제22조의2에 따른 신용조회회사의 보고의 접수(제18조의2제2항에 따른 개선권고를 포함한다)
9. 법 제25조제1항에 따른 신용정보집중기관의 허가 신청의 접수
10. 법 제26조제3항에 따른 신용정보집중관리위원회의 결정사항 보고의 접수 및 제22조제4항에 따른 신용정보집중관리위원회의 결정사항에 대한 변경 권고
11. 삭제 <2015.9.11.>
12. 법 제32조제8항에 따른 제공 대상 신용정보의 범위 등에 대한 승인 신청의 접수
13. 법 제38조제4항에 따른 신용정보회사등의 처리결과에 대한 시정 요청의 접수
14. 법 제38조제5항에 따른 신용정보회사등에 대한 시정명령 및 그 밖에 필요한 조치
15. 법 제38조제7항에 따른 보고의 접수

15의2. 법 제39조의2제3항에 따른 신고의 접수
15의3. 법 제39조의2제5항에 따른 신용정보회사등에 대한 시정 요구
15의4. 법 제41조의2제3항에 따른 위탁계약 해지 보고의 접수
15의5. 제35조의2제6항 및 제7항에 따른 보고의 접수
16. 법 제45조제1항에 따른 신용정보회사등에 대한 감독

[별표 4] <개정 2015.9.11.>

과태료의 부과기준(제38조 관련)

1. 일반기준

가. 하나의 위반행위가 둘 이상의 과태료 부과기준에 해당하는 경우에는 그 중 금액이 큰 과태료 부과기준을 적용한다.

나. 금융위원회는 다음의 어느 하나에 해당하는 경우에는 제2호에 따른 과태료 금액의 2분의 1의 범위에서 그 금액을 줄일 수 있다. 다만, 과태료를 체납하고 있는 위반행위자의 경우에는 그렇지 않다.

1) 위반행위자가 「질서위반행위규제법 시행령」 제2조의2제1항 각 호의 어느 하나에 해당하는 경우

2) 위반행위가 사소한 부주의나 오류로 인한 것으로 인정되는 경우

3) 위반행위자의 법 위반상태를 시정하거나 해소하기 위한 노력이 인정되는 경우

4) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 그 금액을 줄일 필요가 있다고 인정되는 경우

다. 금융위원회는 다음의 어느 하나에 해당하는 경우에는 제2호에 따른 과태료 금액의 2분의 1의 범위에서 그 금액을 늘릴 수 있다. 다만, 법 제52조제1항부터 제4항까지의 규정에 따른 과태료 금액의 상한을 넘을 수 없다.

1) 위반의 내용·정도가 중대하여 신용정보주체 등에 미치는 영향이 크다고 인정되는 경우

2) 법 위반상태의 기간이 6개월 이상인 경우

3) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 그 금액을 늘릴 필요가 있다고 인정되는 경우

2. 개별기준

(단위: 만원)

위반행위	근거 법조문	금액
가. 법 제8조 본문을 위반하여 변경사항을 미리 신고하지 않거나 같은 조 단서를 위반하여 7일 이내에 그 사실을 보고하지 않은 경우	법 제52조 제4항제1호	1,000
나. 법 제10조제4항을 위반하여 영업 중단 또는 폐업을 미리 신고하지 않은 경우	법 제52조 제3항	1,000
다. 법 제11조제1항을 위반하여 겸업을 미리 신고하지	법 제52조	1,000

않은 경우	제4항제2호	
라. 법 제11조제2항을 위반하여 다른 업무를 겸업한 경우	법 제52조 제4항제2호	1,000
마. 법 제12조를 위반하여 유사명칭을 사용한 경우	법 제52조 제4항제2호	1,000
바. 법 제13조를 위반하여 겸직 승인을 받지 않은 경우	법 제52조 제4항제2호	1,000
사. 법 제15조제2항 각 호 외의 부분 본문을 위반하여 동의를 받지 않은 경우	법 제52조 제1항제1호	4,000
아. 법 제17조제1항을 위반하여 의뢰인의 동의 없이 신용정보의 수집·조사를 위탁한 경우	법 제52조 제4항제3호	1,000
자. 법 제17조제4항을 위반하여 보호 조치를 하지 않은 경우	법 제52조 제2항제1호	2,400
차. 법 제17조제5항을 위반하여 교육하지 않거나 위탁계약에 반영하지 않은 경우	법 제52조 제4항제4호	800
카. 법 제17조제7항을 위반하여 재위탁한 경우	법 제52조 제3항	1,600
타. 법 제18조제1항을 위반하여 등록·변경 및 관리하지 않은 경우	법 제52조 제4항제5호	1,000
파. 법 제19조제1항을 위반하여 기술적·물리적·관리적 보안대책을 수립·시행하지 않은 경우	법 제52조 제1항제2호	4,000
하. 법 제19조제2항을 위반하여 보안관리 대책을 포함한 계약을 체결하지 않은 경우	법 제52조 제1항제2호	4,000
거. 법 제20조제1항을 위반하여 신용정보관리기준을 준수하지 않은 경우	법 제52조 제2항제2호	2,000
너. 법 제20조제3항 본문을 위반하여 신용정보관리·보호인을 지정하지 않거나 같은 항 단서를 위반하여 임원으로 지정하지 않은 경우	법 제52조 제2항제2호	2,400
더. 법 제20조제5항을 위반하여 신용정보관리·보호인의 업무에 관한 보고서를 금융위원회에 제출하지 않은 경우	법 제52조 제1항제3호	3,000

러. 법 제20조의2제1항 또는 제3항을 위반하여 관리하지 않은 경우	법 제52조 제4항제6호	1,000
머. 법 제20조의2제2항을 위반하여 개인신용정보를 삭제하지 않은 경우	법 제52조 제2항제3호	2,400
버. 법 제20조의2제4항을 위반하여 통지하지 않은 경우	법 제52조 제4항제6호	800
서. 법 제21조를 위반하여 처분하거나 폐기하지 않은 경우	법 제52조 제2항제4호	2,400
어. 법 제22조의2를 위반하여 금융위원회에 보고하지 않은 경우	법 제52조 제4항제7호	800
저. 법 제23조제5항을 위반하여 신용정보를 타인에게 제공한 경우	법 제52조 제2항제5호	2,400
처. 법 제27조제8항을 위반하여 채권추심업무를 할 때 증표를 내보이지 않은 경우	법 제52조 제4항제8호	600
커. 법 제31조를 위반하여 신용정보활용체제를 공시하지 않은 경우	법 제52조 제4항제9호	800
터. 법 제32조제3항을 위반하여 동의를 받았는지를 확인하지 않은 경우(제34조에 따라 준용하는 경우를 포함한다)	법 제52조 제4항제10호	800
퍼. 법 제32조제4항을 위반하여 구분하여 동의를 받지 않은 경우(제34조에 따라 준용하는 경우를 포함한다)	법 제52조 제1항제4호	3,000
허. 법 제32조제4항을 위반하여 설명하지 않거나 고지하지 않은 경우(제34조에 따라 준용하는 경우를 포함한다)	법 제52조 제1항제4호	800
고. 법 제32조제5항을 위반하여 서비스의 제공을 거부한 경우(제34조에 따라 준용하는 경우를 포함한다)	법 제52조 제1항제4호	3,000
노. 법 제32조제7항을 위반하여 알리지 않거나 공시하지 않은 경우(제34조에 따라 준용하는 경우를 포함한다)	법 제52조 제4항제10호	800
도. 법 제32조제8항을 위반하여 승인을 받지 않은 경우(제34조에 따라 준용하는 경우를 포함한다)	법 제52조 제2항제6호	2,000

로. 법 제32조제9항을 위반하여 개인신용정보를 분리관리하지 않은 경우(제34조에 따라 준용하는 경우를 포함한다)	법 제52조 제2항제6호	1,000
모. 법 제32조제10항을 위반하여 개인신용정보를 제공받는 자의 신원과 이용 목적을 확인하지 않은 경우(제34조에 따라 준용하는 경우를 포함한다)	법 제52조 제4항제10호	800
보. 법 제35조제1항을 위반하여 개인신용정보의 이용 및 제공 사실을 조회할 수 있도록 하지 않은 경우	법 제52조 제4항제11호	800
소. 법 제35조제2항을 위반하여 개인신용정보의 이용 및 제공 사실을 통지하지 않거나 같은 조 제3항을 위반하여 통지를 요청할 수 있음을 알리지 않은 경우	법 제52조 제4항제11호	800
오. 법 제36조제1항을 위반하여 상거래관계의 설정을 거절 또는 중지한 근거를 고지하지 않은 경우	법 제52조 제2항제7호	2,000
조. 법 제37조제3항을 위반하여 고지나 사후고지를 하지 않은 경우	법 제52조 제2항제8호	2,000
초. 법 제38조제2항을 위반하여 신용정보를 삭제 또는 정정하지 않은 경우	법 제52조 제2항제9호	2,400
코. 법 제38조제3항을 위반하여 삭제하거나 정정한 내용을 알리지 않은 경우(법 제36조제3항에 따라 준용하는 경우를 포함한다)	법 제52조 제2항제7호 또는 제9호	2,000
토. 법 제38조제4항을 위반하여 처리결과를 알리지 않은 경우(법 제36조제3항에 따라 준용하는 경우를 포함한다)	법 제52조 제2항제7호 또는 제9호	800
포. 법 제38조제5항을 위반하여 시정명령을 이행하지 않은 경우	법 제52조 제2항제9호	2,400
호. 법 제38조제7항을 위반하여 시정조치 결과를 보고하지 않은 경우(법 제36조제3항에 따라 준용하는 경우를 포함한다)	법 제52조 제2항제7호 또는 제9호	1,000
구. 법 제38조의2제2항을 위반하여 정보제공을 중지하지 않은 경우	법 제52조 제2항제10호	2,000
누. 법 제38조의2제2항을 위반하여 정보제공의 중지 사실을 통지하지 않은 경우	법 제52조 제2항제10호	800

두. 법 제38조의3제2항을 위반하여 개인신용정보를 삭제하지 않은 경우	법 제52조 제2항제11호	2,400
루. 법 제38조의3제3항을 위반하여 분리보관하지 않은 경우	법 제52조 제2항제11호	1,000
무. 법 제38조의3제2항 및 제3항을 위반하여 신용정보주체에게 통지하지 않은 경우	법 제52조 제2항제11호	800
부. 법 제39조를 위반하여 무료로 제공하거나 열람토록 하지 않은 경우	법 제52조 제2항제12호	2,000
수. 법 제39조의2제1항을 위반하여 신용정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제52조 제2항제13호	2,400
우. 법 제39조의2제3항을 위반하여 조치 결과를 신고하지 않은 경우	법 제52조 제2항제14호	2,400
주. 법 제40조제7호를 위반하여 광고성 정보를 전송하는 행위에 개인신용정보 또는 개인식별정보를 이용한 경우	법 제52조 제2항제15호	2,400
추. 법 제41조의2제2항을 위반하여 모집업무수탁업자와 위탁계약을 해지하지 않은 경우	법 제52조 제1항제5호	3,000
쿠. 법 제41조의2제3항을 위반하여 위탁계약을 해지한 사실을 알리지 않은 경우	법 제52조 제4항제12호	1,000
투. 법 제45조제2항부터 제4항까지의 규정에 따른 명령에 따르지 않거나 검사 및 요구를 거부·방해 또는 기피한 경우	법 제52조 제4항제13호	1,000
푸. 법 제47조를 위반하여 보고서를 제출하지 않거나 사실과 다른 내용의 보고서를 제출한 경우	법 제52조 제4항제14호	1,000

신용정보의 이용 및 보호에 관한 법률 시행규칙

[시행 2015.9.12] [총리령 제01191호, 2015.9.11, 일부개정]

제1조(목적) 이 규칙은 「신용정보의 이용 및 보호에 관한 법률」 및 같은 법 시행령에서 위임된 사항과 그 시행에 필요한 사항을 규정함을 목적으로 한다.

제2조 삭제 <2011.8.18>

제3조(허가심사 절차 등) ① 「신용정보의 이용 및 보호에 관한 법률」(이하 "법"이라 한다) 제4조제3항에 따라 신용정보업 허가 신청서를 제출받은 금융위원회는 신청내용에 관한 사실 여부를 확인하고, 신청내용이 법 제6조에 따른 허가요건을 충족하는지를 심사하여야 한다. <개정 2011.8.18>

② 금융위원회는 신용정보업 허가의 신청내용에 대하여 이해관계자 등의 의견을 수렴하기 위하여 신청인, 신청일자, 신청내용, 의견제시의 방법 및 기간 등을 인터넷 홈페이지 등에 공고하여야 한다.

③ 금융위원회는 신용정보업의 허가를 함에 있어 제2항에 따른 의견 수렴 외에 필요하다고 인정되는 경우 허가신청에 대하여 관계기관 및 이해관계자의 의견을 요청하거나 「행정절차법」에 따른 공청회를 개최할 수 있다.<신설 2015.9.11>

④ 금융위원회는 제2항 및 제3항에 따라 수렴된 의견으로서 신용정보업 허가의 신청인에게 불리하다고 판단되는 의견이 있으면 신청인에게 그 의견을 알리고 일정한 기한을 정하여 소명자료를 제출하도록 할 수 있다.<신설 2015.9.11>

⑤ 금융위원회는 신용정보업의 허가를 함에 있어 제2항 및 제3항에 따라 수렴된 이해관계자 등의 의견과 제4항에 따라 신청인이 소명한 사항을 고려하여야 한다.<개정 2015.9.11>

⑥ 그 밖에 신용정보업 허가에 필요한 사항은 금융위원회가 정하여 고시한다.<개정 2015.9.11>

제4조(영업의 휴업 또는 폐업의 신고) 법 제10조제4항에 따라 영업의 전부 또는 일부를 일시적으로 중단하거나 폐업하려는 신용정보회사는 금융위원회가 정하여 고시하는 바에 따라 휴업 또는 폐업 업무범위 및 기간, 휴업 또는 폐업사유 등을 적은 휴·폐업신고서를 금융위원회에 제출하여야 한다.

제5조(겸업신고 등) ①신용정보회사(영리를 목적으로 신용정보업 외의 다른 업무를 겸업하려는 신용조회회사는 제외한다)는 법 제11조제1항에 따라 겸업을 하려는 경우 금융위원회가 정하여 고시하는 신고서에 제1호의 사항을 기재하고, 제2호 및 제3호의 서류를 첨부하여 금융위원회에 제출하여야 한다. <개정 2015.9.11>

1. 겸업업무의 예상 영업규모, 손익 전망 등에 비추어 해당 신용정보회사의 건전한 경영을 저해할 염려가 없고 수익기반 확충에 기여할 수 있는지 여부
2. 겸업업무가 관련 법령에 따라 행정관청의 인가·허가·등록 및 승인 등을 받아야 하는 경우 해당 인가·허가·등록 및 승인 등을 받았음을 증명할 수 있는 서류 또는 확약서
3. 겸업업무를 수행함에 따라 발생할 수 있는 이해상충 및 불공정행위를 방지하기 위하여 필요한 조직, 전문인력 및 적절한 업무체계를 갖췄음을 증명할 수 있는 서류 또는 확약서

② 신용조회회사는 법 제11조제2항 단서에 따라 겸업을 하려는 경우 금융위원회가 정하여 고시하는 승인신청서에 공공 목적의 조사·분석 등의 업무의 내용과 제1항제1호의 사항을 기재하고, 같은 항 제2호 및 제3호의 서류를 첨부하여 금융위원회에 제출하여야 한다.<신설 2015.9.11>

제6조(행정처분의 기준) 법 제14조제2항에 따른 행정처분의 기준은 별표와 같다.

제7조(위임직채권추심인 등록수수료) 법 제27조제10항에 따른 위임직채권추심인 등록수수료는 등록절차 및 등록절차의 관리에 필요한 인적·물적 비용을 고려하여 법 제44조제1항에 따른 신용정보협회의 장이 정한다. <개정 2015.9.11>

부칙 <제911호,2009.10.1>

이 규칙은 공포한 날부터 시행한다.

부칙 <제958호,2011.8.18>

이 규칙은 2011년 8월 20일부터 시행한다.

부칙 <제1191호,2015.9.11>

이 규칙은 2015년 9월 12일부터 시행한다.

[별표] <개정 2015.9.11.>

행정처분의 기준(제6조 관련)

위반행위	해당 법조문	업무정지 기간	업무정지 범위
1. 법 제6조제4항을 위반하여 허가의 요건을 계속 유지하지 않은 경우	법 제14조 제2항제1호	6개월	전부
2. 법 제9조제2항에 따른 명령을 위반하여 금융위원회의 승인 없이 취득한 주식을 처분하지 않은 경우	법 제14조 제2항제9호, 법 별표 제1호	6개월	전부
3. 법 제11조제1항을 위반하여 금융위원회에 미리 신고하지 않거나 거짓, 그 밖의 부정한 방법으로 신고하고 겸업을 한 경우	법 제14조 제2항제2호	3개월	일부
4. 법 제11조제2항을 위반하여 영리를 목적으로 다른 업무를 겸업한 경우 또는 금융위원회의 승인을 받지 않거나 거짓, 그 밖의 부정한 방법으로 승인을 받아 공공 목적의 조사·분석 등의 업무를 겸업한 경우	법 제14조 제2항제2호	6개월	전부
5. 법 제16조에 따른 수집·조사 등의 제한사항을 위반한 경우	법 제14조 제2항제3호	6개월	전부
6. 법 제17조제4항 또는 제19조를 위반하여 신용정보를 분실·도난·유출·변조 또는 훼손당한 경우	법 제14조 제2항제4호	3개월	전부
7. 법 제22조제1항을 위반하여 임원으로 채용·고용한 경우 또는 법 제27조제1항을 위반하여 임직원으로 채용·고용하거나 채권추심업무를 하게 한 경우	법 제14조 제2항제5호	3개월	일부
8. 신용조회회사가 법 제22조의3을 위반하여 계열회사 등에 개인신용정보를 제공한 경우	법 제14조 제2항제6호	1개월	전부
9. 법 제38조제5항에 따른 금융위원회의 시정명령에 따르지 않은 경우	법 제14조 제2항제9호, 법 별표 제3호	1개월	일부

10. 법 제40조제5호를 위반하여 정보원, 탐정, 그 밖에 이와 비슷한 명칭을 사용한 경우	법 제14조 제2항제7호	1개월	일부
11. 법 제42조제1항을 위반하여 개인비밀을 업무 목적 외에 누설하거나 이용한 경우 또는 법 제42조제3항을 위반하여 개인비밀을 타인에게 제공하거나 이용한 경우	법 제14조 제2항제8호	6개월	전부
12. 제42조제4항을 위반하여 개인신용정보를 타인에게 제공한 경우	법 제14조 제2항제8호	6개월	전부
13. 법 제45조제2항에 따른 업무 및 재산상황에 관한 보고 등의 명령에 따르지 않은 경우	법 제14조 제2항제9호, 법 별표 제4호	1개월	일부
14. 법 제45조제4항에 따른 자료의 제출, 관계자의 출석 및 의견의 진술을 하지 않은 경우	법 제14조 제2항제9호, 법 별표 제5호	1개월	일부
15. 법 제45조제7항제4호에 따른 임원에 대한 해임권고 또는 직무정지 요구 및 직원에 대한 면직 요구에 따르지 않은 경우	법 제14조 제2항제9호, 법 별표 제6호	1개월	일부
16. 법 제45조제7항제5호에 따른 위반행위에 대한 시정명령을 따르지 않은 경우	법 제14조 제2항제9호, 법 별표 제7호	1개월	일부
17. 법 제45조제7항제6호에 따른 신용정보 제공의 중지 조치에 따르지 않은 경우	법 제14조 제2항제9호, 법 별표 제8호	1개월	일부
18. 「채권의 공정한 추심에 관한 법률」 제12조제2호·제5호를 위반하여 채권추심 행위를 한 경우(채권추심업만 해당한다)	법 제14조 제2항제10호	1개월	일부
19. 그 밖에 법령 또는 정관을 위반하거나 경영상태가 건전하지 못하여 공익을 심각하게 해칠 우려가 있는 경우	법 제14조 제2항제11호	2개월	일부
20. 그 밖에 법령 또는 정관을 위반하거나 경영상태가 건전하지 못하여 공익을 심각하게 해친 경우	법 제14조 제2항제11호	3개월	전부

전자금융거래법

1. 전자금융감독규정
2. 전자금융감독규정시행세칙
3. 전자금융거래 기본약관
4. 전자금융거래법
5. 전자금융거래법 시행령

전자금융감독규정

[시행 2016.10.5] [고시 제2016 - 37호, 2016.10.5, 일부개정]

제1장 총칙

제1조(목적) 이 규정은 「전자금융거래법」(이하 "법"이라 한다) 및 동법 시행령(이하 "시행령"이라 한다)에서 금융위원회에 위임한 사항과 그 시행에 필요한 사항 및 다른 법령에 따라 금융감독원의 검사를 받는 기관의 정보기술부문 안전성 확보 등을 위하여 필요한 사항을 규정함을 목적으로 한다.

제2조(정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

1. "전산실"이라 함은 전산장비, 통신 및 보안장비, 전산자료 보관 및 출력장비가 설치된 장소를 말한다.
2. "전산자료"라 함은 전산장비에 의해 입력·보관·출력되어 있는 자료를 말하며 그 자료가 입력·출력되어 있는 자기테이프, 디스크, 디스켓, 콤팩트디스크(CD) 등 보조기억매체를 포함한다.
3. "정보처리시스템"이라 함은 전자금융업무를 포함하여 정보기술부문에 사용되는 하드웨어(hardware)와 소프트웨어(software)를 말하며 관련 장비를 포함한다.
4. "정보기술부문"이라 함은 컴퓨터 등 정보처리능력을 가진 장치를 이용하여 정보를 수집·가공·저장·검색·송신 또는 수신을 행하는 금융회사 또는 전자금융업자의 업무, 인력, 시설 및 조직을 말한다.
5. "정보보호" 또는 "정보보안"이라 함은 컴퓨터 등 정보처리능력을 가진 장치를 이용하여 수집·가공·저장·검색·송신 또는 수신되는 정보의 유출·위변조·훼손 등을 방지하기 위하여 기술적·물리적·관리적 수단을 강구하는 일체의 행위를 말하며 사이버안전을 포함한다.
6. "정보보호시스템"이라 함은 정보처리시스템내 정보를 유출·위변조·훼손하거나 정보처리시스템의 정상적인 서비스를 방해하는 행위로부터 정보 등을 보호하기 위한 장비 및 프로그램을 말한다.
7. "해킹"이라 함은 접근을 허가받지 아니하고 전자금융기반시설에 불법적으로 침투하거나 허가받지 아니한 권한을 불법적으로 갖는 행위 또는 전자금융기반시설을 공격하거나 해를 끼치는 행위를 말한다.

8. "컴퓨터악성코드"(이하 "악성코드"라 한다)라 함은 컴퓨터에서 이용자의 허락 없이 스스로를 복사하거나 변형한 뒤 정보유출, 시스템 파괴 등의 작업을 수행하여 이용자에게 피해를 주는 프로그램을 말한다.
9. "공개용 웹서버"라 함은 인터넷 이용자들이 웹페이지를 자유롭게 보고 웹서비스(월드 와이드 웹을 이용한 서비스를 말한다)를 이용할 수 있게 해주는 프로그램이 실행되는 장치를 말한다.
10. "정보통신망"(이하 "통신망"이라 한다)이라 함은 유·무선, 광선 등 정보통신 수단에 의하여 부호·문자·음향·영상 등을 처리·저장 및 송·수신할 수 있는 정보통신 조직형태를 말한다.
11. 삭제

제3조(전자금융보조업자의 범위) 법 제2조제5호에서 "금융위원회가 정하는 자"라 함은 다음 각 호의 어느 하나에 해당하는 자를 말한다.
1. 정보처리시스템을 통하여 「여신전문금융업법」 상 신용카드업자의 신용카드 승인 및 결제 그 밖의 자금정산에 관한 업무를 지원하는 사업자
2. 정보처리시스템을 통하여 은행업을 영위하는 자의 자금인출업무, 환업무 및 그 밖의 업무를 지원하는 사업자
3. 전자금융업무와 관련된 정보처리시스템을 해당 금융회사 또는 전자금융업자를 위하여 운영하는 사업자
4. 제1호 부터 제3호의 사업자와 제휴, 위탁 또는 외부주문(이하 "외부주문등"이라 한다)에 관한 계약을 체결하고 정보처리시스템을 운영하는 사업자

제2장 전자금융거래 당사자의 권리와 의무

제4조(확인에 필요한 구체적인 거래내용) 시행령 제7조제4항제6호에서 "금융위원회가 정하여 고시하는 사항"이란 다음 각 호를 말한다.
1. 법 제8조에 따른 오류정정 요구사실 및 처리결과에 관한 사항
2. 전자금융거래 신청, 조건변경에 관한 내용

제5조(전자금융사고 책임이행을 위한 보험 등의 가입에 관한 기준) ① 금융회사 또는 전자금융업자가 법 제9조제4항에 따라 전자금융사고 책임이행을 위한 보험 또는 공제에 가입하는 경우 보상한도는 다음 각 호에서 정하는 금액 이상이어야 한다.
1.「금융위원회의 설치 등에 관한 법률」 제38조제1호(다만, 「은행법」에 의한 지방금융회사 및 같은 법 제58조에 의해 인가를 받은 외국금융회사의 국내지점은 제외한다) 및 제7호의 회사, 「전자금융거래법 시행령」 제2조제2호의 회사 : 20억원
2.「금융위원회의 설치 등에 관한 법률」 제38조제8호의 회사, 「전자금융거래법」제2조제3호나목(신용카드업자에 한한다) 및 다목의 회사, 「전자금융거래법 시행령」 제2조제1호

의 회사, 「은행법」에 따른 지방금융회사 및 같은 법 제58조에 의해 인가를 받은 외국금융회사의 국내지점 : 10억원

3.「금융위원회의 설치 등에 관한 법률」 제38조제2호(다만, 명의개서대행업무를 수행하는 회사는 제외)의 회사 : 5억원

4. 제1호 부터 제3호 이외의 금융회사 : 1억원. 다만, 제1호 부터 제3호 이외의 금융회사들이 관련 법령에 의해 당해 금융회사를 구성원으로 하는 금융회사를 통해 전자금융거래 관련 정보기술부문의 주요부분을 공동으로 이용하는 경우, 정보기술부문의 주요부문을 제공하는 금융회사가 공동 이용 금융회사 전체의 사고를 보장하는 내용으로 제2호의 금액(시행령 제2조제5호의 금융회사는 제1호의 금액) 이상의 보험 또는 공제에 가입하면 공동 이용 금융회사는 본호의 보험 또는 공제에 가입한 것으로 본다.

5. 법 제28조제2항제1호 및 제2호의 전자금융업자 : 2억원

6. 법 제28조제2항제4호의 전자금융업자 중 제1호 또는 제2호에 속하는 금융회사가 발급한 신용카드, 직불카드 등 거래지시에 사용되는 접근매체의 정보를 저장하는 전자금융업자 : 10억원

7. 제5호, 제6호 이외의 전자금융업자 : 1억원 <종전의 제6호에서 이동>

② 금융회사 또는 전자금융업자가 전자금융사고 책임이행을 위한 준비금을 적립하는 경우에는 제1항 각 호에서 정한 금액 이상의 금액을 보유하고 책임이행이 신속히 이루어질 수 있도록 준비금 관리 및 지급에 관한 내부 절차를 수립하여 운영하여야 한다.

③ 금융회사 또는 전자금융업자가 보험 또는 공제 가입과 준비금 적립을 병행하는 경우 보험 또는 공제의 보상한도는 제1항에서 정한 금액에서 준비금 적립액을 차감한 금액 이상으로 한다.

④ 제1항 부터 제3항의 규정은 전자금융업무를 취급하지 않는 금융회사에 대하여는 적용하지 아니한다.

제6조(추심이체 출금 동의의 방법 등) ① 시행령 제10조제1호에서 "금융위원회가 정하여 고시하는 전자문서"라 함은 다음 각 전자문서을 말한다.

1. 「전자서명법」 제2조제2호에 따른 전자서명으로 다음 각 목의 요건을 구비된 전자서명을 한 전자문서

가. 전자서명을 생성하기 위하여 이용하는 전자적 정보(이하 "전자서명생성정보"라함)가 본인에게 유일하게 속할 것

나. 전자서명 당시 본인이 전자서명생성정보를 지배·관리하고 있을 것

다. 전자서명이 있은 후에 당해 전자서명에 대한 변경여부를 확인할 수 있을 것

라. 전자서명이 있은 후에 당해 전자문서의 변경여부를 확인할 수 있을 것

2. 「전자서명법」 제2조제2호에 따른 전자서명으로 다음 각 목의 요건을 구비된 전자서명을 한 전자문서

가. 서명 전 실명증표를 통해 본인확인

나. 전자문서가 생성된 이후 서명자가 지급인 본인임을 확인 가능
다. 전자서명 및 전자문서에 대한 위변조 여부 확인이 가능
라. 전자문서를 고객에게 전송한 이후 고객이 취소할 수 있는 충분한 기간 부여
3. 삭제
② 시행령 제10조제1호 및 제2호에서 "금융위원회가 정하는 방법"이라 함은 다음 각 호의 방법을 말한다.
1. 전화 녹취
2. 음성응답 시스템(Audio Response System : ARS)
③ 지급인(출금계좌의 실지명의인을 포함한다)이 출금의 동의를 해지하는 경우에도 제1항 및 제2항의 규정을 준용한다.
④ 금융회사·전자금융업자 또는 수취인은 제1항 각 호의 출금 동의의 방법을 운용함에 있어 다음 각 호의 어느 하나에 해당하는 사실을 확인하여야 한다.
1. 지급인과 추심이체 출금계좌 실지명의인이 동일인인 사실
2. 지급인과 추심이체 출금계좌 실지명의인이 동일인이 아닐 경우에는 지급인이 당해 계좌에서 출금할 수 있는 권한을 보유하고 있는 사실

제6조의2(정보보호최고책임자의 지정대상) ① 시행령 제11조의3제1항 후단에서 "금융위원회가 정하여 고시하는 상시 종업원 수의 산정방식"이란 「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 말한다.
② 시행령 <별표 1>의제3호나목 단서에서 "금융위원회가 정하여 고시하는 산정방식"이란 「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 말한다.

제3장 전자금융거래의 안전성 확보 및 이용자 보호

제1절 통칙

제7조(전자금융거래 종류별 안전성 기준) 법 제21조제2항의 "금융위원회가 정하는 기준"이라 함은 다음 각 호의 내용에 관하여 제8조 부터 제37조에서 정하는 기준을 말한다.
1. 인력, 조직 및 예산 부문
2. 건물, 설비, 전산실 등 시설 부문
3. 단말기, 전산자료, 정보처리시스템 및 정보통신망 등 정보기술부문
4. 그 밖에 전자금융업무의 안전성 확보를 위하여 필요한 사항

제2절 인력, 조직 및 예산 부문

제8조(인력, 조직 및 예산) ① 금융회사 또는 전자금융업자는 인력 및 조직의 운용에 관하여 다음 각 호의 사항을 준수하여야 한다.

1. 정보처리시스템 및 전자금융업무 관련 전담 조직을 확보할 것
2. 외부주문등에 관한 계약을 체결하는 때에는 계약내용의 적정성을 검토하고 자체적으로 통제가 가능하도록 회사내부에 조직과 인력을 갖출 것
3. 전산인력의 자질향상 및 예비요원 양성을 위한 교육 및 연수프로그램을 운영할 것
4. 정보보호최고책임자는 임직원이 정보보안 관련법규가 준수되고 있는지 정기적으로 점검하고 그 점검결과를 최고경영자에게 보고할 것
5. 최고경영자는 임직원이 정보보안 관련법규를 위반할 경우 그 제재에 관한 세부기준 및 절차를 마련하여 운영할 것

② 금융회사 또는 전자금융업자는 인력 및 예산에 관하여 다음 각 호의 사항을 준수하도록 노력하여야 한다.

1. 정보기술부문 인력은 총 임직원수의 100분의 5 이상, 정보보호인력은 정보기술부문 인력의 100분의 5 이상이 되도록 할 것
2. 정보보호예산을 정보기술부문 예산의 100분의 7 이상이 되도록 할 것

③ 제2항 각 호의 사항을 이행하지 못하는 금융회사 또는 전자금융업자는 그 사유 및 이용자 보호에 미치는 영향 등을 설명한 자료를 해당 금융회사 또는 전자금융업자가 운영하는 홈페이지 등을 통해 매 사업연도 종료 후 1개월 이내에 공시하여야 한다. 다만, 허가, 등록 또는 인가를 마친 후 1년이 지나지 않은 금융회사 또는 전자금융업자는 공시하지 아니할 수 있다.

④ 제2항제1호의 인력에 관한 기준은 <별표 1>과 같으며, 제2항제2호의 예산에 관한 기준은 <별표 2>와 같다.

제8조의2(정보보호위원회 운영) ① 금융회사 또는 전자금융업자는 중요 정보보호에 관한 사항을 심의·의결하는 정보보호위원회를 설치 운영하여야 한다.

② 정보보호위원회의 장은 정보보호최고책임자로 하며, 위원은 정보보호업무 관련 부서장, 전산운영 및 개발 관련 부서장, 준법업무 관련 부서의 장 등으로 구성한다.

③ 정보보호위원회는 다음 각 호의 사항을 심의·의결한다.

1. 법 제21조제4항에 따른 정보기술부문 계획서에 관한 사항
2. 법 제21조의2제4항제1호에 관한 사항
3. 법 제21조의3에서 정한 취약점 분석·평가 결과 및 보완조치의 이행계획에 관한 사항
4. 전산보안사고 및 전산보안관련 규정 위반자의 처리에 관한 사항
5. 기타 정보보호위원회의 장이 정보보안업무 수행에 필요하다고 정한 사항

④ 정보보호최고책임자는 정보보호위원회 심의·의결사항을 최고경영자에게 보고하여야 한다.

⑤ 최고경영자는 특별한 사정이 없는 한 정보보호위원회의 심의·의결사항을 준수하여야 한다.

제3절 시설부문

제9조(건물에 관한 사항) 금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 다음 각 호의 사항을 준수하여야 한다.

1. 건물 출입구는 경비원에 의하여 통제하고 출입통제 보안대책을 수립·운용할 것
2. 비상시 대피를 위한 비상계단 및 정전대비 유도등을 설치할 것
3. 번개, 과전류 등 고전압으로 인한 전산장비 및 통신장비 등의 피해 예방을 위하여 피뢰설비를 갖출 것
4. 서버, 스토리지(Storage) 등 전산장비 및 통신장비 등의 중량을 감안한 적재하중 안전대책을 수립·운용할 것
5. 화재발생 시 조기진압을 위한 소화기 및 자동소화설비 등을 갖추고, 화재전파방지를 위한 배연설비설치 등 화재예방 안전대책을 수립·운용할 것
6. 화재발생 위험이 높은 지역, 상습 침수지역 및 진동피해 발생지역 등 외부환경에 의하여 전산장비 등이 영향을 받을 수 있는 지역은 제외할 것

제10조(전원, 공조 등 설비에 관한 사항) 금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비에 관하여 다음 각 호의 사항을 준수하여야 한다.

1. 전원실, 공조실 등 주요 설비시설에 자물쇠 등 출입통제장치를 설치할 것
2. 전원, 공조, 방재 및 방범 설비에 대한 적절한 감시제어시스템을 갖출 것
3. 전산실의 전력공급 중단에 대비하여 자가발전설비를 갖출 것
4. 전력공급 장애 시 전력선 대체가 가능하도록 복수회선을 설치하고 전력공급의 연속성 유지를 위한 무정전전원장치(Uninterruptible Power Supply : UPS)를 갖출 것
5. 과전류, 누전에 의한 장애 방지를 위하여 과전류차단기, 누전경보기 등을 설치하고 일정한 전압 및 주파수 유지를 위한 정전압정주파수장치(Constant Voltage Constant Frequency : CVCF)를 갖출 것
6. 전산실에 공급되는 전원 및 공조 설비는 부하가 큰 설비부분과 분리하여 설치하고 공조 설비 상태 점검을 위한 압력계, 온도계 등을 갖출 것
7. 전산실에 24시간 동안 적정한 온도 및 습도를 유지하기 위해서 자동제어 항온·항습기를 갖출 것

제11조(전산실 등에 관한 사항) 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다.

1. 화재·수해 등의 재해 및 외부 위해(危害) 방지대책을 수립·운용할 것
2. 상시 출입문은 한 곳으로 정하며 상시 출입은 업무와 직접 관련이 있는 사전 등록자에 한하여 허용하고, 그 밖의 출입자에 대하여는 책임자의 승인을 받아 출입하도록 하며 출입자 관리기록부를 기록·보관할 것
3. 상시 출입이 허용된 자 이외의 출입자의 출입사항에 대하여는 전산실의 규모 및 설치장소 등을 감안하여 무인감시카메라 또는 출입자동기록시스템 설치 등 적절한 조치를 취하여 사

후 확인이 가능하도록 할 것

4. 출입문은 이중 안전장치로 보호하며 외벽이 유리인 경우 유리창문을 통하여 접근할 수 없도록 조치할 것
5. 천정、바닥、벽의 침수로 인한 정보처리시스템의 장애가 발생하지 않도록 외벽과 전산장비와의 거리를 충분히 유지하고 이중바닥설치 등 방안을 강구할 것
6. 적정수준의 온도、습도를 유지하기 위하여 온도、습도 자료 자동기록장치 및 경보장치 설치 등 적절한 조치를 취할 것
7. 케이블이 안전하게 유지되도록 전용 통로관 설치 등 적절한 보호조치를 강구할 것
8. 정전에 대비하여 조명설비 및 휴대용손전등을 비치할 것
9. 집적정보통신시설(Internet Data Center : IDC) 등과 같이 다수의 기관이 공동으로 이용하는 장소에 정보처리시스템을 설치하는 경우에는 미승인자가 접근하지 못하도록 적절한 접근통제 대책을 마련할 것
10. 다음 각 목의 중요 시설 및 지역을 보호구역으로 설정 관리할 것
    가. 전산센터 및 재해복구센터
    나. 전산자료 보관실
    다. 정보보호시스템 설치장소
    라. 그 밖에 보안관리가 필요하다고 인정되는 정보처리시스템 설치장소
11. 국내에 본점을 둔 금융회사의 전산실 및 재해복구센터는 국내에 설치할 것
12. 무선통신망을 설치하지 아니할 것

제4절 정보기술부문

제12조(단말기 보호대책) 금융회사 또는 전자금융업자는 단말기 보호를 위하여 다음 각 호의 사항을 준수하여야 한다.

1. 업무담당자 이외의 사람이 단말기를 무단으로 조작하지 못하도록 조치할 것
2. 정보처리시스템에 접속하는 단말기에 대해 정당한 사용자인가의 여부를 확인할 수 있는 기록을 유지할 것
3. 외부 반출, 인터넷 접속, 그룹웨어 접속의 금지 등 강화된 보호대책이 적용되는 중요단말기를 지정할 것
4. 정보유출, 악성코드 감염 등을 방지할 수 있도록 단말기에서 보조기억매체 및 휴대용 전산장비에 접근하는 것을 통제할 것
5. 삭제

제13조(전산자료 보호대책) ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립、운용하여야 한다.

1. 사용자계정과 비밀번호를 개인별로 부여하고 등록、변경、폐기를 체계적으로 관리할 것

2. 외부사용자에게 사용자계정을 부여하는 경우 최소한의 작업권한만 할당하고 적절한 통제장치를 갖출 것
3. 전산자료의 보유현황을 관리하고 책임자를 지정·운영할 것
4. 전산자료의 입력·출력·열람을 함에 있어 사용자의 업무별로 접근권한을 통제할 것
5. 전산자료 및 전산장비의 반출·반입을 통제할 것
6. 비상시에 대비하여 보조기억매체 등 전산자료에 대한 안전지출 및 긴급파기 계획을 수립·운용할 것
7. 정기적으로 보조기억매체의 보유 현황 및 관리실태를 점검하고 책임자의 확인을 받을 것
8. 중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하고 백업내역을 기록·관리할 것
9. 주요 백업 전산자료에 대하여 정기적으로 검증할 것
10. 이용자 정보의 조회·출력에 대한 통제를 하고 테스트 시 이용자 정보 사용 금지(다만, 법인인 이용자 정보는 금융감독원장이 정하는 바에 따라 이용자의 동의를 얻은 경우 테스트 시 사용 가능하며, 그 외 부하 테스트 등 이용자 정보의 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제하여야 한다)
11. 정보처리시스템의 가동기록은 1년 이상 보존할 것
12. 정보처리시스템 접속 시 5회 이내의 범위에서 미리 정한 횟수 이상의 접속 오류가 발생하는 경우 정보처리시스템의 사용을 제한할 것
13. 단말기에 이용자 정보 등 주요정보를 보관하지 아니하고, 단말기를 공유하지 아니할 것(다만, 불가피하게 단말기에 보관할 필요가 있는 경우 보관사유, 보관기간 및 관리 비밀번호 등을 정하여 책임자의 승인을 받아야 한다)
14. 사용자가 전출·퇴직 등 인사조치가 있을 때에는 지체 없이 해당 사용자 계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템에 대한 접근을 통제할 것

② 제1항제1호의 사용자계정의 공동 사용이 불가피한 경우에는 개인별 사용내역을 기록·관리하여야 한다.

③ 금융회사 또는 전자금융업자는 단말기를 통한 이용자 정보 조회 시 사용자, 사용일시, 변경·조회내용, 접속방법이 정보처리시스템에 자동적으로 기록되도록 하고, 그 기록을 1년 이상 보존하여야 한다.

④ 제1항제11호의 정보처리시스템 가동기록의 경우 다음 각 호의 사항이 접속의 성공여부와 상관없이 자동적으로 기록·유지되어야 한다.

1. 정보처리시스템에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록
2. 전산자료를 사용한 일시, 사용자 및 자료의 내용을 확인할 수 있는 접근기록
3. 정보처리시스템내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 액세스 로그 등 접근기록

⑤ 금융회사 또는 전자금융업자는 단말기와 전산자료의 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련·운용하여야 한다. 다만, 정보처리시스템 관리자의

주요 업무 관련 행위는 책임자가 제28조제2항에 따라 이중확인 및 모니터링을 하여야 한다.

제14조(정보처리시스템 보호대책) 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다.

1. 주요 정보처리시스템에 대한 구동, 조작방법, 명령어 사용법, 운용순서, 장애조치 및 연락처 등 시스템 운영매뉴얼을 작성할 것
2. 데이터베이스관리시스템(Database Management System : DBMS)·운영체제·웹프로그램 등 주요 프로그램에 대하여 정기적으로 유지보수를 실시하고, 작업일, 작업내용, 작업결과 등을 기록한 유지보수관리대장을 작성·보관할 것
3. 정보처리시스템의 장애발생 시 장애일시, 장애내용 및 조치사항 등을 기록한 장애상황기록부를 상세하게 작성·보관할 것
4. 정보처리시스템의 정상작동여부 확인을 위하여 시스템 자원 상태의 감시, 경고 및 제어가 가능한 모니터링시스템을 갖출 것
5. 시스템 통합, 전환 및 재개발 시 장애 등으로 인하여 정보처리시스템의 운영에 지장이 초래되지 않도록 통제 절차를 마련하여 준수할 것
6. 정보처리시스템의 책임자를 지정·운영할 것
7. 정보처리시스템의 운영체계, 시스템 유틸리티 등의 긴급하고 중요한 보정(patch)사항에 대하여는 즉시 보정 작업을 할 것
8. 중요도에 따라 정보처리시스템의 운영체제 및 설정내용 등을 정기 백업 및 원격 안전지역에 소산하고 백업자료는 1년 이상 기록·관리할 것
9. 정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Log in)할 경우 계정 및 비밀번호 이외에 별도의 추가인증 절차를 의무적으로 시행할 것
10. 정보처리시스템 운영체제(Operating System) 계정에 대한 사용권한, 접근 기록, 작업 내역 등에 대한 상시 모니터링체계를 수립하고, 이상 징후 발생 시 필요한 통제 조치를 즉시 시행할 것

제14조의2(비중요 정보처리시스템 지정) ① 금융회사 또는 전자금융업자는 자체적으로 수립한 정보자산 중요도 평가기준에 따라 전자금융거래의 안전성 및 신뢰성에 미치는 영향이 현저히 낮은 정보처리시스템을 비중요 정보처리시스템으로 지정할 수 있다. 다만, 개인의 고유식별정보 또는 「신용정보의 이용 및 보호에 관한 법률」에 따른 개인신용정보를 처리하는 정보처리시스템은 비중요 정보처리시스템으로 지정할 수 없다.

② 금융회사 또는 전자금융업자는 제1항에 따라 비중요 정보처리시스템 지정시 제8조의2에 따른 정보보호위원회의 심의·의결을 거쳐야 한다.

③ 금융회사 또는 전자금융업자는 제1항에 따라 비중요 정보처리시스템을 지정한 날로부터 7일 이내에 금융감독원장이 정하는 양식에 따라 정보자산 중요도 평가기준, 지정 결과, 관리방안 등을 포함한 보고서를 금융감독원에 제출하여야 한다.

④ 금융감독원장은 제3항에 따라 제출한 보고서를 검토한 결과, 평가 기준, 지정 결과, 관리 방안 등이 적합하지 않다고 판단되는 경우에는 금융회사 또는 전자금융업자에 대하여 개선·보완을 요구할 수 있다.

⑤ 제1항의 비중요 정보처리시스템만 위치한 전산실에 대해서는 제11조제11호 및 제12호, 제15조제1항제5호를 적용하지 아니한다.

제15조(해킹 등 방지대책) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.

1. 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영
2. 해킹 등 전자적 침해행위에 대비한 시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업 실시
3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다)
4. 내부통신망에서의 파일 배포기능은 통합 및 최소화하여 운영하고, 이를 배포할 경우에는 무결성 검증을 수행할 것
5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것(단, 업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.)

② 제1항제1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다.

1. 삭제
2. 최소한의 서비스번호(port)와 기능만을 적용하고 업무목적 이외의 기능 및 프로그램을 제거할 것
3. 보안정책의 승인·적용 및 보안정책의 등록, 변경 및 삭제에 대한 이력을 기록·보관할 것
4. 정보보호시스템 원격관리를 금지할 것. 다만, 원격관리가 불가피한 경우 전용회선(전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 포함한다) 사용, 접근통제 등을 포함한 원격 접속 보안 대책을 수립·운영할 것
5. 정보보호시스템의 작동 상태를 주기적으로 점검할 것
6. 시스템 장애, 가동중지 등 긴급사태에 대비하여 백업 및 복구 절차 등을 수립·시행할 것 <종전의 제5호에서 이동>

③ 제1항 각 호의 정보보호시스템에 대하여 책임자를 지정·운영하여야 하며, 운영결과는 1년 이상 보존하여야 한다.

④ 금융회사 또는 전자금융업자는 해킹 등 전자적 침해행위로 인한 피해 발생시 즉시 대처할 수 있도록 적절한 대책을 마련하여야 한다.

⑤ 삭제

⑥ 금융회사 또는 전자금융업자는 무선통신망을 설치·운용할 때에는 다음 각 호의 사항을 준수하여야 한다.

1. 무선통신망 이용 업무는 최소한으로 국한하고 법 제21조의2에 따른 정보보호최고책임자의 승인을 받아 사전에 지정할 것
2. 무선통신망을 통한 불법 접속을 방지하기 위한 사용자인증, 암호화 등 보안대책을 수립할 것
3. 금융회사 내부망에 연결된 정보처리 시스템이 지정된 업무 용도와 사용 지역(zone) 이외의 무선통신망에 접속하는 것을 차단하기 위한 차단시스템을 구축하고 실시간 모니터링체계를 운영할 것
4. 비인가 무선접속장비(Access Point : AP) 설치·접속여부, 중요 정보 노출여부를 주기적으로 점검할 것

제16조(악성코드 감염 방지대책) ① 금융회사 또는 전자금융업자는 악성코드 감염을 방지하기 위하여 다음 각 호를 포함한 대책을 수립·운용하여야 한다.

1. 응용프로그램을 사용할 때에는 악성코드 검색프로그램 등으로 진단 및 치료 후 사용할 것
2. 악성코드 검색 및 치료프로그램은 최신상태로 유지할 것
3. 악성코드 감염에 대비하여 복구 절차를 마련할 것
4. 제12조제3호에 따른 중요 단말기는 악성코드 감염여부를 매일 점검할 것

② 금융회사 또는 전자금융업자는 악성코드 감염이 발견된 경우 악성코드 확산 및 피해를 최소화하기 위하여 필요한 조치를 신속하게 취하여야 한다.

제17조(홈페이지 등 공개용 웹서버 관리대책) ① 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다.

1. 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 "DMZ구간"이라 한다)에 설치하고 네트워크 및 웹 접근제어 수단으로 보호할 것
2. 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 아이디·비밀번호 이외에 추가 인증수단을 적용할 것
3. 공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험·개발 도구 등의 사용을 제한할 것
4. DMZ구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니할 것(다만, 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화하여 저장·관리하여야 한다)

② 금융회사 또는 전자금융업자는 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다.

1. 게시자료에 대한 사전 내부통제 실시
2. 무기명 또는 가명에 의한 게시 금지

3. 홈페이지에 자료를 게시하는 담당자의 지정·운용
4. 개인정보의 유출 및 위·변조를 방지하기 위한 보안조치

③ 삭제

④ 금융회사 또는 전자금융업자는 공개용 웹서버가 해킹공격에 노출되지 않도록 대응 조치하여야 한다.

⑤ 금융회사 또는 전자금융업자는 단말기에서 음란, 도박 등 업무와 무관한 프로그램 또는 인터넷 사이트에 접근하는 것에 대한 통제대책을 마련하여야 한다.

제18조(IP주소 관리대책) 금융회사 또는 전자금융업자는 정보제공자 주소(이하 "IP주소"라 한다)의 안전한 사용을 위하여 다음 각 호를 포함하여 적절한 대책을 수립·운용하여야 한다.

1. 내부통신망에서 사용하는 IP주소의 경우 사설 IP주소 사용 등으로 보안을 강화하며 내부 IP주소체계의 외부유출을 금지할 것
2. 개인별로 내부 IP주소를 부여하여 유지·관리할 것
3. 내부 IP주소 및 외부 IP주소의 인터넷 접속내용을 1년 이상 별도로 기록·보관할 것
4. 정보처리시스템의 운영담당, 개발담당 및 외부직원 등 업무 특성별로 네트워크를 적절하게 분리하여 IP주소를 사용할 것. 다만, 외부직원 등과의 공동작업 수행 등 네트워크의 분리가 어렵다고 금융감독원장이 정하는 경우에는 업무특성별로 접근권한을 분리하여 IP주소를 사용할 수 있다.
5. 내부통신망은 다른 기관 내부통신망과 분리하여 사용할 것

제5절 정보기술부문 내부통제

제19조(정보기술부문 계획서 제출 절차 등) ① 시행령 제11조의2에 따라 금융위원회에 정보기술부문 계획서를 제출해야 하는 금융회사 또는 전자금융업자는 현실적이고 실현 가능한 장·단기 정보기술부문 계획을 매년 수립·운용하여야 한다.

② 금융위원장은 금융감독원장으로 하여금 정보기술부문 계획서의 적정성 등을 평가한 후 관련보고서를 제출하게 할 수 있다.

제19조의2(정보보호 교육계획의 수립 시행) ① 정보보호최고책임자는 임직원의 정보보호역량 강화를 위하여 필요한 교육프로그램을 개발하고, 다음 각 호의 기준에 따라 매년 교육계획을 수립·시행하여야 한다.

1. 임원 : 3시간 이상(단, 정보보호최고책임자는 6시간 이상)
2. 일반직원 : 6시간 이상
3. 정보기술부문업무 담당 직원 : 9시간 이상
4. 정보보호업무 담당 직원 : 12시간 이상

② 최고경영자는 정보보호교육을 실시한 이후 대상 임직원에 대해 평가를 실시하여야 한다.

③ 제1항의 교육프로그램 개발과 정보보호교육은 정보보호 전문 교육기관에 위탁할 수 있다.

제20조(정보처리시스템 구축 및 전자금융거래 관련 사업 추진) 금융회사 또는 전자금융업자는 정보처리시스템 및 전자금융거래와 관련된 사업을 추진하는 경우에 다음 각 호의 사항을 준수하여야 한다.

1. 조직에 미치는 영향이 크거나 내부직무전결기준에 따라 부서장 전결 금액 이상의 사업 추진 시에는 사전에 충분한 타당성 검토를 실시할 것
2. 정보처리시스템의 신규 사업 및 통합·전환·재개발 등과 같은 주요 추진사업에 대하여 비용 대비 효과분석을 실시할 것
3. 타당성 검토와 비용 대비 효과분석 결과는 전산운영위원회 등 독립적인 조직의 승인을 받을 것
4. 정보처리시스템의 안전성과 신뢰성을 확보하기 위하여 분석·설계 단계부터 보안대책을 강구할 것

제21조(정보처리시스템 구축 및 전자금융거래 관련 계약) 금융회사 또는 전자금융업자는 정보처리시스템 구축 및 전자금융거래와 관련된 계약 체결 시에 다음 각 호의 사항을 준수하여야 한다.

1. 적합한 업체를 공정하게 선정하기 위하여 객관적인 업체 선정 기준 및 절차를 마련·운용할 것
2. 정보처리시스템의 안전성과 신뢰성을 확보하기 위하여 제1호에 따른 기준 및 절차의 내용에는 정보보안 관련 사항을 포함할 것
3. 공정하고 합리적인 예정가격 산출 기준을 수립·적용할 것
4. 계약금액, 구축완료일자, 납품방법 및 대금지급방법 등 계약이행에 필요한 내용을 포함한 계약서 작성 기준을 수립·운용할 것
5. 구매 또는 개발한 제품의 소유권, 저작권 및 지적재산권 등의 귀속관계를 명확히 하여 사후 분쟁이 발생하지 않도록 할 것
6. 납품 또는 개발이 완료된 소프트웨어 등에 대하여 공급업체 파산 등 비상사태에 대비한 대책을 마련·운용할 것
7. 검수는 개발자, 계약자 등 이해당사자를 배제하여 공정하게 실시할 것
8. 계약조항을 이행하지 못하는 사유가 발생하였거나 계약조항을 변경할 경우에는 검사부서의 승인을 받을 것
9. 내부감사규정에 따라 감사가 정한 금액 이상의 계약에 대하여는 자체 감사를 실시하거나 검사부서의 승인을 받을 것

제22조(정보처리시스템 감리) 금융회사 또는 전자금융업자는 정보처리시스템의 안전성 및 효율성 확보를 위하여 다음 각 호의 사항을 포함한 정보처리시스템 감리 지침을 작성·운용하여야 한다.

1. 목적 및 대상, 시스템 감리인, 감리시기 및 계획 등 일반기준
2. 기획, 개발 및 운용의 감리 실시 기준
3. 지적사항 및 개선사항 등 감리 후 보고 기준
4. 전자금융업무와 관련된 외부주문등에 대한 감리 기준

제23조(비상대책 등의 수립·운용) ① 금융회사 또는 전자금융업자는 장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 각 호의 내용을 포함한 업무지속성 확보방안을 수립·준수하여야 한다.

1. 상황별 대응절차
2. 백업 또는 재해복구센터를 활용한 재해복구계획
3. 비상대응조직의 구성 및 운용
4. 입력대행, 수작업 등의 조건 및 절차
5. 모의훈련의 실시
6. 유관기관 및 관련업체와의 비상연락체제 구축
7. 보고 및 대외통보의 범위와 절차 등

② 제1항에 따른 업무지속성 확보대책에는 비상사태에 대비한 다음 각 호의 안전대책이 반영되어야 한다.

1. 파업 시 핵심전산업무 종사자의 근무지 이탈에 따른 정보처리시스템의 마비를 방지하기 위하여 비상지원인력을 확보·운영할 것
2. 비상사태 발생 시에도 정보처리시스템의 마비를 방지하고 신속히 원상복구가 될 수 있도록 정보처리시스템 운영에 대한 비상지원인력 또는 외부 전문업체를 활용하는 방안을 수립·운영할 것
3. 비상지원인력이 사용법을 충분히 이해하고 업무운용이 가능한 수준으로 전산시스템 운영지침서, 사용자매뉴얼 등을 쉽고 자세하게 작성하고 최신상태로 유지할 것
4. 핵심전산업무 담당자 부재 시에도 비상지원 인력이 업무를 수행할 수 있도록 비상지원인력에 대한 연수를 실시할 것

③ 금융회사 또는 전자금융업자는 제1항의 규정에 따른 업무지속성 확보대책의 실효성·적정성 등을 매년 1회 이상 점검하여 최신상태로 유지하고 관리하여야 한다.

④ 「국가위기관리기본지침」에 따라 금융위원회가 지정한 금융회사는 금융위원회의 「금융전산분야위기대응실무매뉴얼」에 따라 위기대응행동매뉴얼(이하 "행동매뉴얼"이라 한다)을 수립·준수하고 이를 금융위원회에 알려야 한다.

⑤ 금융위원회가 별도로 지정하지 아니한 금융회사 또는 전자금융업자는 자연 재해, 인적 재해, 기술적 재해, 전자적 침해 등으로 인한 전산시스템의 마비 방지와 신속한 복구를 위한 비상대책을 수립·운영하여야 한다.

⑥ 제4항에 따른 행동매뉴얼 또는 제5항에 따른 비상대책에는 제1항의 규정에 따른 업무지속성 확보대책이 반영되어야 한다.

⑦ 금융회사 또는 전자금융업자는 중앙처리장치, 데이터저장장치 등 주요 전산장비에 대하여 이중화 또는 예비장치를 확보하여야 한다.

⑧ 다음 각 호의 금융회사는 시스템 오류, 자연재해 등으로 인한 전산센터 마비에 대비하여 업무지속성을 확보할 수 있도록 적정 규모·인력을 구비한 재해복구센터를 주전산센터와 일정 거리 이상 떨어진 안전한 장소에 구축·운용하여야 한다.

1.「은행법」에 의해 인가를 받아 설립된 은행(다만,「은행법」제58조에 의해 인가를 받은 외국금융회사의 국내지점은 제외한다)

2.「한국산업은행법」에 의한 한국산업은행, 「중소기업은행법」에 의한 중소기업은행, 「농업협동조합법」에 의한 농협은행, 「수산업협동조합법」에 의한 수산업협동조합중앙회의 신용사업부문

3.「자본시장과 금융투자업에 관한 법률」에 의한 투자매매업자·투자중개업자(다만, 「자본시장과 금융투자업에 관한 법률」 제12조에 의해 인가를 받은 외국 투자매매업자·투자중개업자의 지점 등은 제외한다)

4.「자본시장과 금융투자업에 관한 법률」에 의한 증권금융회사 및 한국예탁결제원

5.「자본시장과 금융투자업에 관한 법률」에 의한 거래소

6.「여신전문금융업법」에 의한 신용카드업자(다만, 법인신용카드 회원에 한하여 신용카드업을 영위하는 자는 제외한다)

7.「보험업법」에 의한 보험요율산출기관

8.「상호저축은행법」에 의한 상호저축은행중앙회

9.「신용협동조합법」에 의한 신용협동조합중앙회

10.「보험업법」에 의한 보험회사

⑨ 제8항 각 호의 금융회사는 업무별로 업무지속성 확보의 중요도를 분석하여 핵심업무를 선정하여야 하며, 업무별 복구목표시간을 정하여야 한다. 이 경우 핵심업무의 복구목표시간은 3시간 이내로 하되, 「보험업법」에 의한 보험회사의 핵심업무의 경우에는 24시간 이내로 한다.

⑩ 제8항의 규정에 따른 재해복구센터를 운영하는 금융회사는 매년 1회 이상 재해복구센터로 실제 전환하는 재해복구전환훈련을 실시하여야 한다.

[제9항에서 이동 <2015.6.24.>]

제24조(비상대응훈련 실시) ① 금융회사 또는 전자금융업자는 제23조제4항에 따른 행동매뉴얼 또는 같은 조 제5항에 따른 비상대책에 따라 연 1회의 비상대응훈련을 실시하고 그 결과를 금융위원회에 보고하여야 한다. 이때, 제23조제10항에 따른 재해복구전환훈련을 포함하여 실시할 수 있다.

② 금융위원회는 금융분야의 비상대응능력을 강화하기 위하여 금융회사 또는 전자금융업자를 선별하여 금융분야 합동비상대응훈련을 실시할 수 있다.

③ 금융위원회는 제2항의 규정에 따른 합동비상대응훈련을 실시할 때, 다음 각 호의 기관에게 지원을 요청할 수 있다.

1.「정부조직법」 제15조에 따른 "국가정보원(국가사이버안전센터)"
2.「경찰법」 제2조에 따른 "경찰청(사이버테러대응센터)"
3. 침해사고대응기관
4. 그밖에 비상대응훈련의 실효성 확보를 위하여 금융위원회가 필요하다고 인정하는 기관

제25조(정보처리시스템의 성능관리) 금융회사 또는 전자금융업자는 정보처리시스템의 장애예방 및 성능의 최적화를 위하여 정보처리시스템의 사용 현황 및 추이 분석 등을 정기적으로 실시하여야 한다.

제26조(직무의 분리) 금융회사 또는 전자금융업자는 다음 각 호의 업무에 대하여 직무를 분리·운영하여야 한다.
1. 프로그래머와 오퍼레이터
2. 응용프로그래머와 시스템프로그래머
3. 시스템보안관리자와 시스템프로그래머
4. 전산자료관리자(librarian)와 그 밖의 업무 담당자
5. 업무운영자와 내부감사자
6. 내부인력과 전자금융보조업자 및 유지보수업자 등을 포함한 외부인력
7. 정보기술부문인력과 정보보호인력
8. 그 밖에 내부통제와 관련하여 직무의 분리가 요구되는 경우

제27조(전산원장 통제) ① 금융기관 또는 전자금융업자는 장애 또는 오류 등에 의한 전산원장의 변경을 위하여 별도의 변경절차를 수립·운용하여야 한다.
② 제1항의 절차에는 변경 대상 및 방법, 변경 권한자 지정, 변경 전후내용 자동기록 및 보존, 변경내용의 정당여부에 대한 제3자 확인 등이 포함되어야 한다.
③ 금융회사 또는 전자금융업자는 대차대조표 등 중요 자료의 계상액과 각종 보조부·거래기록·전산원장파일의 계상액에 대한 상호일치 여부를 전산시스템을 통하여 주기적으로 확인하여야 한다.
④ 금융회사 또는 전자금융업자는 제3항에 따른 확인 결과 불일치가 발견된 때에는 그 원인 및 조치 내용을 전산자료의 형태로 5년간 보존하여야 한다.
⑤ 금융회사 또는 전자금융업자는 이용자 중요원장에 직접 접근하여 중요원장을 조회·수정·삭제·삽입하는 경우에는 작업자 및 작업내용 등을 기록하여 5년간 보존하여야 한다.

제28조(거래통제 등) ① 금융회사 또는 전자금융업자는 사고위험도가 높은 거래에 대하여는 책임자 승인거래로 처리토록 하는 등 전산시스템에 의한 이중확인이 가능하도록 하여야 한다.
② 금융회사 또는 전자금융업자는 전산원장, 주요정보 또는 이용자 정보 등이 저장된 정보처리시스템에 대한 중요작업 수행 시 책임자가 이중확인을 해야 한다.

제29조(프로그램 통제) 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록·변경·폐기 절차를 수립·운용하여야 한다.

1. 적용대상 프로그램 종류 및 등록·변경·폐기 방법을 마련할 것
2. 프로그램 변경 전후 내용을 기록·관리할 것
3. 프로그램 등록·변경·폐기내용의 정당성에 대해 제3자의 검증을 받을 것
4. 변경 필요시 해당 프로그램을 개발 또는 테스트 시스템으로 복사 후 수정할 것
5. 프로그램에 대한 접근은 업무담당자에 한정할 것
6. 운영시스템 적용은 처리하는 정보의 기밀성·무결성·가용성을 고려하여 충분한 테스트 및 관련 책임자 승인 후 실시할 것
7. 프로그램 반출, 실행프로그램의 생성 및 운영시스템 등록은 전산자료 관리자 등 해당프로그램 담당자 이외의 자가 수행할 것
8. 운영체제, 데이터베이스관리프로그램 등의 시스템 프로그램도 응용프로그램과 동일한 수준으로 관리할 것
9. 프로그램 설명서, 입·출력 레코드 설명서, 프로그램 목록 및 사용자·운영자지침서 등 프로그램 유지보수에 필요한 문서를 작성·관리할 것
10. 전자 금융거래에 사용되는 전산프로그램은 실제 업무를 처리하는 정보처리시스템에 설치하기 전에 자체 보안성 검증을 실시할 것

제30조(일괄작업에 대한 통제) 금융회사 또는 전자금융업자는 안전하고 체계적인 일괄작업(batch)의 수행을 위하여 다음 각 호의 사항을 준수하여야 한다.

1. 일괄작업은 작업요청서에 의한 책임자의 승인을 받은 후 수행할 것
2. 일괄작업은 최대한 자동화하여 오류를 최소화할 것
3. 일괄작업 수행 과정에서 오류가 발생하였을 경우 반드시 책임자의 확인을 받을 것
4. 모든 일괄작업의 작업내용을 기록·관리할 것
5. 책임자는 일괄작업 수행자의 주요업무 관련 행위를 모니터링할 것

제31조(암호프로그램 및 키 관리 통제) ① 금융회사 또는 전자금융업자는 암호프로그램에 대하여 담당자 지정, 담당자 이외의 이용 통제 및 원시프로그램(source program) 별도 보관 등을 준수하여 유포 및 부당 이용이 발생하지 않도록 하여야 한다.

② 금융회사 또는 전자금융업자는 암호 및 인증시스템에 적용되는 키에 대하여 주입·운용·갱신·폐기에 대한 절차 및 방법을 마련하여 안전하게 관리하여야 한다.

제32조(내부사용자 비밀번호 관리) 금융회사 또는 전자금융업자는 내부사용자의 비밀번호 유출을 방지하지 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.

1. 담당업무 외에는 열람 및 출력을 제한할 수 있는 접근자의 비밀번호를 설정하여 운영할 것
2. 비밀번호는 다음 각 목의 사항을 준수할 것
   가. 비밀번호는 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정하고 분기별 1회 이상 변경

나. 비밀번호 보관 시 암호화

다. 시스템마다 관리자 비밀번호를 다르게 부여

3. 비밀번호 입력 시 5회 이내의 범위에서 미리 정한 횟수 이상의 입력오류가 연속하여 발생한 경우 즉시 해당 비밀번호를 이용하는 접속을 차단하고 본인 확인절차를 거쳐 비밀번호를 재부여하거나 초기화 할 것

제33조(이용자 비밀번호 관리) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 전산자료에 보관하고 있는 이용자의 비밀번호를 암호화하여 보관하며 동 비밀번호를 조회할 수 없도록 하여야 한다. 다만, 비밀번호의 조회가 불가피하다고 인정되는 경우에는 그 조회사유·내용 등을 기록·관리하여야 한다.

② 금융회사 또는 전자금융업자는 이용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다.

1. 주민등록번호, 동일숫자, 연속숫자 등 제3자가 쉽게 유추할 수 있는 비밀번호의 등록 불가
2. 통신용 비밀번호와 계좌원장 비밀번호를 구분해서 사용
3. 5회 이내의 범위에서 미리 정한 횟수 이상의 비밀번호 입력 오류가 발생한 경우 즉시 해당 비밀번호를 이용하는 거래를 중지시키고 본인 확인절차를 거친 후 비밀번호 재부여 및 거래 재개(이체 비밀번호 등 동일한 비밀번호가 다양한 형태의 전자금융거래에 공통으로 이용되는 경우, 입력오류 횟수는 이용되는 모든 전자금융거래에 대하여 통산한다)
4. 금융회사가 이용자로부터 받은 비밀번호는 거래전표, 계좌개설신청서 등에 기재하지 말고 핀패드(PIN pad) 등 보안장치를 이용하여 입력 받을 것
5. 신규 거래, 비밀번호 변경, 이체 신청과 같이 비밀번호를 등록·사용하는 경우 사전에 신청서 등에 기입하지 않고, 핀패드 등 보안장치를 이용하거나 이용자가 사후에 전자적 장치를 이용하여 직접 입력하는 방식으로 운영할 것

제6절 전자금융업무

제34조(전자금융거래 시 준수사항) 금융회사 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다.

1. 전화 등 거래수단 성격상 암호화가 불가능한 경우를 제외한 전자금융거래는 암호화 통신을 할 것(다만, 전용선을 사용하는 경우로서 제36조의 규정에 따라 자체 보안성심의를 실시한 경우에는 그러하지 아니하다)
2. 전자금융사고를 예방하기 위하여 비대면 전자금융거래를 허용하지 않는 계좌 개설, 중요거래정보에 대한 문자메시지 및 이메일(e-mail) 통지 등의 서비스를 이용자가 요청하는 경우, 동 서비스를 제공할 수 있도록 시스템을 갖출 것
3. 전자금융거래에 사용되는 접근매체를 발급받기 위해서는 반드시 실명확인 후 교부할 것.
4. 거래인증수단 채택시 안전성, 보안성, 이용편의성 등을 충분히 고려할 것

5. 금융회사 또는 전자금융업자는 전자금융거래에서 이용자에게 제공하거나 거래를 처리하기 위한 전자금융거래프로그램(거래전문포함)의 위·변조 여부 등 무결성을 검증할 수 있는 방법을 제공할 것

② 삭제

제35조(이용자 유의사항 공지) 금융회사 또는 전자금융업자는 전자금융거래의 안전한 수행을 위하여 이용자에게 다음 각 호의 사항을 준수하도록 공지하여야 한다.

1. 비밀번호 유출위험 및 관리에 관한 사항
2. 금융기관 또는 전자금융업자가 제공하고 있는 이용자 보호제도에 관한 사항
3. 해킹·피싱 등 전자적 침해 방지에 관한 사항
4. 본인확인 절차를 거쳐 비밀번호 변경이 가능하도록 정보처리시스템을 구축하고 비밀번호 변경 시 같은 번호를 재사용하지 않도록 할 것

제36조(자체 보안성심의) ① 금융회사 또는 전자금융업자는 다음 각 호의 행위를 하고자 하는 경우 금융감독원장이 정하는 기준과 절차에 따라 보안성심의를 실시하여야 한다.

1. 정보통신망을 이용하여 이용자를 대상으로 신규 전자금융업무를 수행
2. 복수의 금융회사 또는 전자금융업자가 공동으로 전자금융거래 관련 표준을 제정

② 금융회사 또는 전자금융업자는 제1항에 따른 심의(이하 "자체 보안성심의"라 한다)를 마친 후 제1항 각 호의 행위를 수행한 날로부터 7일 이내에 금융감독원장이 정하는 자체 보안성심의 결과보고서를 금융감독원에 제출하여야 한다. 다만, 제1항제1호에 따른 보안성심의의 경우 신규 전자금융업무가 제공 또는 시행된 날을 기준으로 과거 1년 이내에 전자금융사고가 발생하지 않은 기관으로서 금융감독원장이 정하는 기준에 해당하는 금융회사 또는 전자금융업자는 그러하지 아니하다.

③ 금융감독원장은 제2항에 따라 제출받은 자체 보안성심의 결과보고서를 검토한 결과, 보안수준이 충분하지 않다고 인정되는 경우에는 금융회사 또는 전자금융업자에 대하여 개선·보완을 요구할 수 있다.

④ 제2항 및 제3항에도 불구하고 다음 각 호의 기관은 제1항제1호에 따른 자체 보안성심의 결과보고서의 제출을 하지 아니할 수 있다.

1. 「우체국예금·보험에 관한 법률」에 의한 체신관서
2. 「새마을금고법」에 의한 새마을금고 및 새마을금고중앙회
3. 「한국수출입은행법」에 따른 한국수출입은행
4. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관

제37조(인증방법 사용기준) 금융회사 또는 전자금융업자는 전자금융거래의 종류·성격·위험수준 등을 고려하여 안전한 인증방법을 사용하여야 한다.

제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등) ① 전자금융기반시설의 취약점 분석·평가는 총자산이 2조원 이상이고, 상시 종업원 수(「소득세법」에 따른 원천징수의

무자가 근로소득세를 원천징수한 자를 기준으로 한다. 이하 같다) 300명 이상인 금융회사 또는 전자금융업자이거나 「수산업협동조합법」, 「산림조합법」, 「신용협동조합법」, 「상호저축은행법」 및 「새마을금고법」에 따른 중앙회의 경우 연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 실시하여야 한다.

② 금융회사 및 전자금융업자는 취약점 분석·평가를 위하여 정보보호최고책임자(정보보호최고책임자가 없는 경우 최고경영자가 지정한다)를 포함하여 5인 이상으로 자체전담반을 구성하여야 하며, 구성원 중 100분의 30 이상은 「정보보호산업의 진흥에 관한 법률 시행규칙」 제8조의 정보보호 전문서비스 기업 지정기준에서 정한 고급 기술인력 이상의 자격을 갖춘 자이어야 한다. 다만, 제37조의3제1항에 따른 평가전문기관에 위탁하는 경우에는 자체전담반을 구성하지 아니할 수 있다.

③ 제1항에 따른 금융회사 및 전자금융업자 이외의 자의 경우 연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 실시하되 자체전담반을 구성하지 아니할 수 있다. 이 경우 취약점 분석·평가의 내용은 금융감독원장이 정한다.

④ 금융회사 및 전자금융업자는 해당 주기 내에 평가 대상 시설과 평가기간을 나누어 평가할 수 있다.

⑤ 금융회사 또는 전자금융업자는 취약점 분석·평가에 따라 이행계획을 수립·시행하여야 하며 다음 각 호의 사항을 준수하여야 한다.

1. 취약점 분석·평가 결과에 따른 취약점의 제거 또는 이에 상응하는 조치의 시행
2. 취약점의 제거 또는 이에 상응하는 조치가 불가한 경우에는 최고경영자 승인을 득할 것
3. 이행계획의 시행 결과는 최고경영자에게 보고할 것

제37조의3(전자금융기반시설의 취약점 분석·평가 전문기관의 지정 등) ① 전자금융기반시설의 취약점 분석·평가를 위한 평가전문기관은 다음 각 호의 자로 한다.

1. 「정보통신기반 보호법」 제16조에 따라 금융분야 정보공유·분석센터로 지정된 자
2. 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호전문서비스 기업
3. 침해사고대응기관
4. 금융위원장이 지정하는 자

② 금융회사 및 전자금융업자는 시행령 제11조의5제3항에 따른 전자금융기반시설의 취약점 분석·평가 결과보고서를 금융위원장에게 제출하여야 하며, 금융감독원장은 결과보고서를 분석하여 매분기 1개월 이내에 금융위원장에게 보고하여야 한다.

③ 금융위원장은 취약점 분석·평가 결과보고서에 근거하여 필요시 금융회사 및 전자금융업자에 대하여 개선·보완을 요구할 수 있다.

제37조의4(침해사고대응기관 지정 및 업무범위 등) ① 침해사고에 대응하기 위한 침해사고대응기관은 다음 각 호의 자로 한다.

1. 금융보안원

2. 삭제
3. 금융위원장이 지정한 자

② 침해사고대응기관은 다음 각 호의 업무를 수행한다.

1. 침해사고에 관한 정보의 수집ㆍ전파를 위한 정보공유체계의 구축
2. 침해사고의 예보ㆍ경보 발령내용의 전파
3. 침해사고의 원인분석과 신속한 대응 및 피해 확산방지를 위해 필요한 조치
4. 금융회사 및 전자금융업자와 관련된 해킹 등 전자적 침해행위 정보를 탐지ㆍ분석하여 즉시 대응 조치를 하기 위한 기구(이하 "금융권 통합 보안관제센터"라 한다)의 운영

③ 금융위원장은 침해사고대응기관을 포함하여 침해사고조사단을 구성할 수 있다.

④ 금융위원장은 제2항에 따른 침해사고 긴급대응을 위한 침해사고대응기관의 업무 수행 또는 제3항에 따른 침해사고 원인분석 및 긴급조치를 위하여 금융회사 및 전자금융업자, 전자금융보조업자에 협조를 요청할 수 있다.

⑤ 금융회사 및 전자금융업자는 침해사고에 대한 대응능력 확보를 위하여 연 1회 이상 침해사고 대응 및 복구훈련 계획을 수립ㆍ시행하여야 하며 그 계획 및 결과를 침해사고대응기관의 장에게 제출하여야 한다. 다만 다음 각 호의 어느 하나에 해당하는 금융회사는 그러하지 아니한다.

1. 법 제2조제3호가목의 금융회사 중 신용협동조합
2. 법 제2조제3호다목ㆍ라목의 금융회사
3. 시행령 제2조제4호부터 제6호까지의 조합
4. 시행령 제5조제2항의 요건을 충족한 금융회사

⑥ 금융위원장은 침해사고대응기관의 장으로 하여금 침해사고 대응ㆍ복구 및 훈련결과를 점검하고 보완이 필요하다고 판단되는 경우 개선ㆍ보완을 요구할 수 있다.

⑦ 금융위원장은 침해사고대응기관의 장으로 하여금 시행령 제11조의6제1항제4호에 따른 보안취약점 통보를 위하여 금융회사 및 전자금융업자가 사용하고 있는 소프트웨어에 대한 조사ㆍ분석을 실시하게 할 수 있다.

제37조의5(정보보호최고책임자의 업무) 정보보호최고책임자는 정보보안점검의 날을 지정하고, 임직원이 금융감독원장이 정하는 정보보안 점검항목을 준수했는지 여부를 매월 점검하고, 그 점검 결과 및 보완 계획을 최고경영자에게 보고하여야 한다.

제38조(금융위원회가 정하는 보관자료 및 거래기록 등) 시행령 제12조제1항제2호다목에서 "금융위원회가 정하여 고시하는 거래기록"이라 함은 제4조제1호의 기록을 말한다.

제39조(전자지급수단의 이용한도) 시행령 제13조제2항 부터 제4항에 따라 금융위원회가 정하는 전자지급수단의 구체적인 이용한도는 <별표 3>과 같다.

제40조(약관교부 방법 등) ① 전자금융업무를 수행하는 금융회사 및 전자금융업자는 전자금융거래와 관련한 약관(이하 "약관"이라 한다)을 별도로 마련하여야 한다.

② 금융회사 또는 전자금융업자는 이용자와 전자금융거래의 계약을 체결함에 있어 이용자의 요청이 있는 경우 전자문서의 전송(전자우편을 이용한 전송을 포함한다), 모사전송, 우편 또는 직접 교부의 방식으로 전자금융거래 약관의 사본을 이용자에게 교부하여야 한다.

③ 금융회사 또는 전자금융업자는 이용자와 전자금융거래의 계약을 체결함에 있어 이용자가 약관의 내용에 대한 설명을 요청하는 경우 다음 각 호의 어느 하나의 방법으로 이용자에게 약관의 중요내용을 설명하여야 한다.

1. 약관의 중요내용을 이용자에게 직접 설명
2. 약관의 중요내용에 대한 설명을 전자적 장치를 통하여 이용자가 알기 쉽게 표시하고 이용자로부터 해당 내용을 충분히 인지하였다는 의사표시를 전자적 장치를 통하여 수령

④ 금융회사 또는 전자금융업자는 약관을 변경하는 때에는 그 시행일 1월 전에 변경되는 약관을 해당 전자금융거래를 수행하는 전자적 장치(해당 전자적 장치에 게시하기 어려울 경우에는 이용자가 접근하기 용이한 전자적 장치로서 당해 금융회사등이 지정하는 대체장치를 포함한다. 이하 이 조에서 같다)에 게시하고 이용자에게 통지하여야 한다. 다만, 이용자가 이의를 제기할 경우 금융회사 또는 전자금융업자는 이용자에게 적절한 방법으로 약관 변경내용을 통지하였음을 확인해 주어야 한다.

⑤ 금융회사 또는 전자금융업자가 법령의 개정으로 인하여 긴급하게 약관을 변경한 때에는 변경된 약관을 전자적 장치에 최소 1월 이상 게시하고 이용자에게 통지하여야 한다.

제41조(약관 제정 또는 변경에 따른 보고 등) ① 법 제25조제1항 단서에서 "금융위원회가 정하는 경우"란 다음 각 호와 같다.

1. 이용자의 권익을 확대하거나 의무를 축소하기 위한 약관의 변경
2. 금융감독원장에게 보고된 약관의 내용과 동일하거나 유사한 약관의 제정 또는 변경
3. 그 밖에 이용자의 권익이나 의무에 불리한 영향이 없는 경우로서 금융감독원장이 정하는 약관의 제정 또는 변경

② 금융회사 또는 전자금융업자가 전자금융거래 약관을 제정 또는 변경하고자 하는 경우에는 해당 약관 및 약관내용을 이해하는데 필요한 관련서류를 시행예정일 45일 전까지 금융감독원장에게 제출하여야 한다. 이 경우 약관 및 관련서류는 전자문서로 제출할 수 있다.

③ 금융감독원장은 제2항의 규정에 따라 제출받은 약관을 심사하고 건전한 금융거래질서의 유지를 위하여 약관내용의 변경이 필요하다고 인정하는 경우 해당 금융회사 또는 전자금융업자에 대하여 약관의 변경을 권고할 수 있다.

④ 제3항의 규정에 따라 변경권고를 받은 금융회사 또는 전자금융업자는 권고의 수락여부를 금융감독원장에게 보고하여야 한다.

제4장 전자금융업의 허가와 등록 및 업무

제1절 허가 및 등록의 대상과 절차

제42조(총발행잔액의 산정방법 등) ① 시행령 제15조제5항에 따른 선불전자지급수단 발행 시 총발행잔액은 등록신청일이 속하는 사업연도의 직전 사업연도 1분기(직전 사업연도 1분기말 이후에 사업을 개시한 경우에는 사업개시한 날이 속하는 분기를 말한다)부터 등록신청일 직전 분기까지 각 분기말 미상환 발행잔액의 단순평균으로 한다. 다만, 사업기간이 3월 미만인 경우에는 등록신청일 직전 월말 미상환 발행잔액으로 한다.

② 법 제28조제3항제1호다목에 따라 금융위원회에 등록하지 아니하고 선불전자지급수단을 발행하는 자는 매분기말 기준으로 선불전자지급수단의 미상환잔액을 평가하여 이를 시행령 제15조제6항에 따른 지급보증, 상환보증보험 또는 공제에 반영하여야 한다.

제42조의2(거래금액 기준) ① 법 제30조제3항제1호에서 "금융위원회가 정하는 기준"이라 함은 당해 전자금융업에 대한 분기별 결제대행금액(이용자가 지급한 재화 및 용역의 매출총액), 결제대금예치금액 또는 전자고지결제금액이 30억원 이하에 해당하는 경우를 말한다.

② 법 제30조제4항에서 "금융위원회가 정하는 기한"이라 함은 신고한 때로부터 6월 이내를 말한다.

③ 등록 자본금 초과시 신고와 관련한 절차 및 방법 등 세부사항은 금융감독원장이 정하는 바에 따른다.

제43조(허가등 절차의 구분) 다음 각 호의 허가 또는 인가(이하 "허가등"이라 한다)의 절차는 허가등 사항에 대한 사전심사 및 확실한 실행을 위하여 허가등의 이전에 예비적으로 행하는 의사표시(이하 "예비허가등"이라 한다)와 허가등으로 구분한다.

1. 법 제28조제1항의 규정에 의한 전자화폐의 발행 및 관리 업무의 허가
2. 법 제45조에 의한 합병 등의 인가

제44조(예비허가등) ① 예비허가등을 신청하고자 하는 자는 금융감독원장이 정하는 바에 따라 <별지 제3호 서식>에 따른 관련 신청서 및 첨부서류를 금융위원회에 제출하여야 한다.

② 금융위원회는 예비허가등의 심사를 위하여 필요하다고 인정하는 때에는 예비허가등의 신청에 대하여 이해관계인의 의견을 요청할 수 있고, 금융시장에 중대한 영향을 미칠 우려가 있다고 판단되는 경우 공청회를 개최할 수 있다.

③ 금융위원회는 제2항의 규정에 의하여 접수된 의견 중 신청인에게 불리한 의견에 대하여는 신청인에게 소명하도록 기한을 정하여 통보할 수 있다.

④ 금융감독원장은 예비허가등의 신청내용에 대한 진위여부를 확인하고 이해관계인, 일반인 및 관계기관 등으로부터 제시된 의견을 감안하여 신청내용이 관련 법령과 이 장 제2절에서 규정하는 허가등 세부기준에 부합되는지 여부를 심사하여야 한다.

⑤ 금융감독원장은 사업계획의 타당성을 평가하기 위하여 평가위원회를 구성·운영할 수 있으며 신청내용의 확인, 발기인 및 경영진과의 면담 등을 위하여 실지조사를 실시할 수 있다.

⑥ 금융위원회는 예비허가등의 신청에 대하여 관련 법령과 이 장 제2절에서 규정하는 허가의 세부기준을 감안하여 예비허가등의 여부를 결정한다.

⑦ 금융위원회는 예비허가등 시에 조건을 붙일 수 있으며 예비허가등을 거부하는 경우 이를 서면으로 신청인에게 통보하여야 한다.
⑧ 금융위원회는 합병, 영업양도 등 구조조정 및 이용자보호 등을 위하여 신속한 처리가 필요하거나 예비허가등의 신청 시 허가등의 요건을 갖추었다고 판단되는 때에는 예비허가등의 절차를 생략할 수 있다.

제45조(허가등) ① 신청인은 예비허가등의 내용 및 조건을 이행한 후 금융감독원장이 정하는 바에 따라 <별지 제4호 서식>에 따른 관련 신청서 및 첨부서류를 금융위원회에 제출하여야 한다.
② 금융위원회는 허가등의 신청에 대하여 관련 법령과 이 장 제2절에서 규정하는 허가의 세부기준에 따라 심사하여 허가여부를 결정한다.
③ 허가등에는 조건을 붙일 수 있으며 허가를 거부하는 경우에는 이를 서면으로 신청인에게 통보하여야 한다.
④ 금융위원회는 예비허가등의 내용 및 조건의 이행여부를 확인하기 위하여 실지조사를 실시할 수 있으며, 신청인은 이에 적극 협조하여야 한다.
⑤ 신청인은 예비허가등 또는 허가등 시에 부과된 조건이 있는 경우 그 이행상황을 이행기일 경과 후 지체 없이 금융위원회에 보고하여야 한다.

제46조(보완서류 등의 제출) 금융위원회는 예비허가등 또는 허가등의 심사 시 보완서류 등의 추가자료가 필요한 경우 신청인에게 기한을 정하여 그 자료의 제출을 요구할 수 있다.

제47조(허가등 사실의 공고) 금융위원회는 허가등의 신청을 승인한 경우에는 지체 없이 그 내용을 관보에 공고하고 인터넷 등을 이용하여 일반인들에게 알려야 한다.

제48조(등록) ① 법 제28조 및 제29조에 따라 등록을 신청하고자 하는 자는 금융감독원장이 정하는 바에 따라 <별지 제5호 서식>에 따른 등록신청서를 금융감독원에 제출하여야 하며 금융감독원장은 등록신청일로부터 20일 이내에 서면으로 등록여부를 통지한다. 다만, 제3항의 실지조사에 걸린 기간은 통지기간에 산입하지 아니한다.
② 금융감독원장은 신청인의 등록 신청에 대하여 이 장 제2절의 심사기준에 따라 등록 여부를 결정한다.
③ 금융감독원장은 등록의 내용 및 조건의 이행여부를 확인하기 위한 실지조사를 실시할 수 있다.
④ 금융감독원장은 등록 신청을 수리한 경우에는 지체 없이 그 내용을 관보에 공고하고 인터넷 등을 이용하여 일반인들에게 알려야 한다.

제49조(기재가 생략되는 출자자의 범위) 시행령 제20조제1항제3호에서 "금융위원회가 정하여 고시하는 소액출자자"라 함은 허가 또는 등록대상 전자금융업자가 되고자 하는 법인의 의결권 있는 발행주식총수의 100분의 1 이하의 주식을 소유하는 자를 말한다.

제2절 허가 및 등록의 세부요건

제50조(인력 및 물적 시설 세부요건) ① 법 제28조 및 제29조에 따라 허가를 받거나 등록을 하고자 하는 자는 인력과 물적 시설에 대한 다음 각 호의 요건을 모두 갖추어야 한다.

1. 신청 당시 전산업무 종사 경력이 2년 이상인 임직원을 5명 이상 확보하고 있거나 허가·등록 시점에 확보 가능할 것
2. 전자금융업을 원활히 영위하는데 필요한 전산기기를 보유할 것
3. 전산장애 발생 시 전산자료 손실에 대비한 백업(backup)장치를 구비할 것
4. 전자금융업의 원활한 영위를 위한 각종 프로그램을 보유할 것
5. 전산자료 보호 등을 위한 적절한 정보처리시스템 관리방안을 확보하고 정보보호시스템 등 감시운영체제를 구축할 것
6. 전산실 등의 구조 및 내장, 설비 등의 안전성을 확보하고 적절한 보안대책을 수립할 것

② 국외에서 주로 영업하는 국외 사이버몰("국외 사이버몰"이란 컴퓨터 등과 정보통신설비를 이용하여 재화 등을 거래할 수 있도록 설정된 가상의 영업장으로서 운용자의 사무소가 국외에 있는 경우를 말한다. 이하 같다)에서의 상거래에 수반한 전자지급결제대행업을 영위할 목적으로 전자금융업을 등록하고자 하는 자는 제50조제1항의 규정에도 불구하고 다음 각 호의 요건을 모두 충족한 경우 등록할 수 있다.

1. 국외에 소재한 계열사(「금융회사의 정보처리 및 전산설비 위탁에 관한 규정」 제2조제3항의 "계열사"를 말한다. 이하 같다)와 이용계약을 체결하였고, 계열사의 인력 및 물적 시설이 제50조제1항 각 호의 세부요건을 충족할 것
2. 제1호의 규정에도 불구하고 전자금융업을 등록하고자 하는 자는 신청 당시 법령 준수업무와 이용자 민원처리업무를 담당할 3명 이상의 임직원(전산업무 종사 경력이 2년 이상인 임직원 1명을 포함하여야 한다)은 직접 확보하고 있거나 등록시점에 확보 가능할 것
3. 신청 당시 계열사의 인력 또는 물적시설을 통해 5개국 이상의 국가에서 전자지급결제대행업무가 수행되고 있을 것

③ 제2항에 따라 등록을 하려는 자가 계열사의 인력 또는 물적시설의 이용계약을 체결하는 경우에는 「금융회사의 정보처리 및 전산설비 위탁에 관한 규정」을 적용한다. 다만, 동 규정의 제7조는 적용하지 아니한다.

제50조의2(국외 사이버몰을 위한 전자지급결제대행업) ① 제50조제2항에 따라 등록하고자 하는 경우 시행령 제20조제2항제8호에 따라 다음 각 호의 서류를 제출하여야 한다.

1. 「금융회사의 정보처리 및 전산설비 위탁에 관한 규정」 제7조제1항 각 호의 서류
2. 등록신청자 및 계열사의 수탁업무 수행 과정에서의 법·시행령 및 이 규정 등 준수에 대한 확약서
3. 신청 시점에 전자지급결제대행업무를 수행하고자 하는 국외 사이버몰에 대한 다음 각 목의 사항(해당 국가의 법령 등에서 이와 유사한 것으로 인정되는 사항을 포함한다)을 기재한 서

류

가. 「전자상거래 등에서의 소비자보호에 관한 법률」 제10조제1항 각 호의 서류

나. 신청일 직전연도에 사이버몰에서 체결된 전자상거래 중 국내에 소재한 소비자와 사업자 간 거래의 비중

② 제50조제2항에 따라 등록을 한 자는 국외에서 주로 영업하는 국외 사이버몰을 통한 상거래에 대해서만 전자지급결제대행업을 영위하여야 한다.

③ 금융감독원장은 국외에서 주로 영업하는 국외 사이버몰의 판단기준 등 필요한 사항을 정할 수 있다.

제51조(재무건전성 세부기준 및 계산방법 등) ① 시행령 제18조제1항 및 제2항에 따라 금융위원회가 정하는 재무건전성 기준은 다음 각 호와 같다.

1. 시행령 제18조제1항의 규정에 따른 기관 중 「금융산업의 구조개선에 관한 법률」 제2조제1호의 금융회사에 해당하는 기관은 그 기관의 설립·운영 등에 관한 법령상 경영개선권고, 경영개선요구 또는 경영개선명령 등의 요건이 되는 재무기준에 해당하지 아니할 것

2. 제1호 이외의 경우에는 다음 각 목의 요건을 충족할 것

가. 시행령 제18조제1항의 규정에 따른 금융회사 중 「금융산업의 구조개선에 관한 법률」 제2조제1호의 금융회사에 해당하지 않는 기관은 자기자본 대비 부채총액의 비율이 100분의 200 이내일 것. 다만, 금융회사 업무의 성격 및 재무 구조 등을 감안할 때 부채비율 기준을 적용하지 아니하고, 「금융산업의 구조 개선에 관한 법률」 제2조제1호 각 목 중 어느 하나의 금융회사(이하 "기준 금융회사"라 한다)의 재무건전성 기준을 적용하는 것이 적절하다고 금융위원회가 승인하는 경우에는, 기준 금융회사의 설립, 운영 등에 관한 법령에 따라 산출한 재무 비율이 같은 법령상의 경영개선권고, 경영개선요구 또는 경영개선명령 등의 요건이 되는 기준에 해당하지 아니할 것

나. 법 제28조제1항에 따른 허가대상 전자금융업일 경우에는 자기자본 대비 부채총액의 비율이 100분의 180 이내일 것

다. 법 제28조제2항 및 제29조에 따른 등록대상 전자금융업일 경우에는 자기자본·출자총액 또는 기본재산 대비 부채총액의 비율이 100분의 200 이내일 것

② 제1항제2호의 부채비율은 신청일이 속하는 사업연도의 직전 사업연도말 대차대조표(최근 대차대조표를 사용하고자 하는 경우에는 신청일 최근 분기말 대차대조표 또는 회계법인의 확인을 받은 신청일 최근 월말 대차대조표) 상의 자기자본 및 부채총액을 이용하여 산출한다. 이 경우 전자화폐·선불전자지급수단의 미상환잔액 및 전자자금이체·전자지급결제대행·결제대금예치·전자고지결제·「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제10호에 따른 통신과금서비스 등의 업무를 영위하는 자가 이용자와의 거래 관계에서 일시 보관하는 금액(이하 "미정산 잔액"이라 한다)은 부채총액에서 차감한다.

③ 제1항에도 불구하고 다음 각 호의 요건을 갖춘 신청인의 재무건전성 기준은 자기자본 대비 부채총액의 비율이 100분의 1500 이내일 것으로 한다.

1. 정부등이 자본금·출자총액 또는 기본재산의 100분의 10 이상을 소유하고 있거나 출자하고 있을 것
2. 신청인의 사업 수행이 곤란하게 되는 경우 정부등이 해당 사업을 인수할 것을 확약하는 등 그 사업의 연속성에 대하여 정부등이 보장하고 있을 것
3. 사업 개시 후 5년 이내 제1항의 재무건전성 기준을 충족하는 것을 내용으로 하는 실현가능한 재무구조개선계획을 수립하여 관련서류와 함께 제출할 것

제52조(사업계획에 관한 요건) 법 제28조에 따라 허가를 받고자 하는 자의 사업계획은 다음 각 호의 요건을 모두 갖추어야 한다.

1. 영업개시 후 3년간 추정재무제표 및 수익전망이 전자화폐 내지 선불전자지급수단 발행업계의 과거 수익상황 등에 비추어 타당성이 있고 그 내용이 해당 신청회사의 영업계획에 부합할 것
2. 전자화폐 발행업을 원활히 영위하는데 필요한 이용자 확보계획이 구체적이고 타당하며 실현가능성이 있을 것
3. 영위하고자 하는 영업의 내용이 법령에 위반되지 아니하고 투자자보호나 건전한 금융질서를 저해할 우려가 없을 것

제53조(주요출자자에 관한 요건) 주요출자자(시행령 제18조제3항에 따른 주요출자자를 말한다)는 <별표 4>에서 정한 요건을 충족하여야 한다.

제54조(허가 및 등록신청 결격자) 법 제32조제4호의 규정에서 "금융위원회가 정하는 자"라 함은「신용정보의 이용 및 보호에 관한 법률」제25조 제2항 제1호의 종합신용정보집중기관에 다음 각호 중 어느하나의 신용정보가 등록된 자를 말한다.

1. 어음·수표 거래정지처분 또는 부도거래정보
2. 대출금 등의 용도 외 유용 사실
3. 부정한 방법으로 대출을 받는 등 금융거래질서를 문란하게 한 사실

제55조(신청에 따른 등록말소 및 이용자 보호조치) ① 법 제34조에 따라 등록의 말소를 신청하고자 하는 전자금융업자는 <별지 제6호 서식>에 따른 등록말소신청서를 금융위원회에 제출하여야 한다.

② 법 제34조에 따라 등록의 말소를 신청하고자 하는 전자금융업자는 신청 이전에 이용자 보호조치 계획을 금융위원회에 제출하여야 한다.

③ 금융위원회는 제1항의 전자금융업자가 제출한 계획이 이용자 보호에 충분하지 않은 경우에 그 보완을 요구할 수 있다.

제3절 전자금융업의 업무

제56조(전자화폐 발행업자의 겸업가능 업무) 시행령 제22조제1항제3호에서 "금융위원회가 정하여 고시하는 업무"란 다음 각 호의 어느 하나에 해당하는 업무를 말한다.

1. 전자화폐 발행 및 관리를 위한 가맹점의 모집
2. 전자화폐 발행 및 관리를 위한 인터넷 홈페이지의 운영 및 이를 통한 통신판매 중개

제57조(수수료 및 준수사항 등의 고지방법) 법 제38조제3항 각 호의 사항은 다음 각 호의 방법 중 제1호의 방법을 포함한 둘 이상의 방법으로 가맹점에게 알려야 한다.

1. 가맹점에의 개별 통보
2. 전국적으로 보급되는 일간신문에의 공고
3. 해당 금융회사 또는 전자금융업자 영업장 및 인터넷 홈페이지에의 게시

제5장 전자금융업무의 감독

제58조(금융회사의 정보기술부문 실태평가 등) ① 금융감독원장은 금융회사의 정보기술부문의 건전성 여부를 감독하여야 한다.

② 금융감독원장은 업무의 성격 및 규모, 정보기술부문에 대한 의존도 등을 감안하여 <별표 5>에 규정된 금융회사(이하 이 조에서 '은행등'이라 한다)에 대하여 검사를 통해 정보기술부문 운영 실태를 평가하고 그 결과를 경영실태평가 등 감독 및 검사업무에 반영하여야 한다.

③ 제2항에 의한 실태평가는 1등급(우수), 2등급(양호), 3등급(보통), 4등급(취약), 5등급(위험)의 5단계 등급으로 구분한다.

④ 금융감독원장은 제2항에 따른 정보기술부문 실태평가 결과 종합등급이 4등급인 경우에는 해당 은행등에게 이의 개선을 위한 확약서 제출을 요구할 수 있으며, 종합등급이 5등급이거나 직전 정보기술부문 실태평가 결과에 비해 평가등급이 2등급 이상 하향된 경우에는 취약점 개선대책의 수립·이행을 내용으로 하는 양해각서를 체결할 수 있다.

⑤ 제4항의 확약서는 대표자의 승인을 받아 제출하고, 양해각서는 해당 은행등의 이사회 재적 이사 전원의 서명을 받아 체결한다.

⑥ 금융감독원장은 확약서 또는 양해각서의 이행상황을 점검하여 그 이행이 미흡하다고 판단되는 경우에는 확약서를 다시 제출받거나 양해각서를 다시 체결할 수 있다.

⑦ 확약서 또는 양해각서의 효력발생일자, 이행시한 및 이행상황 점검주기는 각 확약서 또는 양해각서에서 정한다. 다만, 이행상황 점검주기를 따로 정하지 않은 경우 은행등은 매분기 익월말까지 분기별 이행상황을 금융감독원장에게 보고하여야 한다.

⑧ 제2항에 따른 정보기술부문 실태평가 결과는 경영실태평가 세부 평가항목 중 경영관리 또는 위험관리 항목의 평가비중에서 최소 100분의 20 이상 반영되어야 하며, 금융감독원장은 정보기술부문 실태평가 결과가 4등급 이하인 은행등에 대해 경영실태평가 2등급 이상으로 평가할 수 없다.

⑨ 제2항에 의한 정보기술부문의 실태평가를 위한 세부 사항은 금융감독원장이 정한다.

제59조(검사결과의 보고방법) 금융감독원장은 법 제39조제5항에 따른 결과보고를 하는 경우 「금융기관 검사 및 제재에 관한 규정」 제3장부터 제4장을 준용한다.

제60조(외부주문등에 대한 기준) ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다.

1. 외부주문등에 의한 정보처리시스템의 개발업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치·운영
2. 금융회사와 이용자 간 암호화정보 해독 및 원장 등 중요 데이터 변경 금지
3. 계좌번호, 비밀번호 등 이용자 금융정보 무단보관 및 유출 금지
4. 접근매체 위·변조, 해킹, 개인정보유출 등에 대비한 보안대책 수립
5. 금융회사와 전자금융보조업자 간의 접속은 전용회선(전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 포함한다)을 사용
6. 정보처리시스템 장애 등 서비스 중단에 대비한 비상대책 수립
7. 외부주문등의 입찰·계약·수행·완료 등 각 단계별로 금융감독원장이 정하는 보안관리방안을 따를 것
8. 업무지속성을 위한 중요 전산자료의 백업(backup)자료 보존 및 백업설비 확보 등 백업대책 수립
9. 정보관리의 취약점을 최소화하고 보안유지를 위한 내부통제방안을 수립·운용하고, 통제는 제8조제1항제2호의 조직에서 수행
10. 전자금융보조업자에 대한 재무건전성을 연1회 이상 평가하여 재무상태 악화에 따른 도산에 대비하고 전자금융보조업자의 주요 경영활동에 대해 상시 모니터링을 실시
11. 전자금융보조업자가 제공하는 서비스의 품질수준을 연1회 이상 평가할 것
12. 전자금융보조업자가 사전 동의 없이 다시 외부주문등 계약을 체결하거나 계약업체를 변경하지 못하도록 하고, 사전 동의시 해당 계약서에 제7호의 사항을 기재하도록 통제
13. 업무수행인력에 대하여 사전 신원조회 실시 또는 대표자의 신원보증서 징구, 인력변경시 인수인계에 관한 사항 등을 포함한 업무수행인력 관리방안 수립
14. 외부주문등은 자체 보안성검토 및 정기(금융감독원장이 정하는 중요 점검사항에 대해서는 매일) 보안점검 실시

② 금융회사 또는 전자금융업자는 제1항제10호 및 제11호의 평가결과를 금융감독원장에게 보고하여야 한다.

③ 금융감독원장은 제2항의 규정에 따른 평가결과 보고를 접수하고, 그 평가실시 여부를 제58조제2항의 규정에 따른 정보기술부문 실태평가에 반영할 수 있다.

④ 법 제40조제6항 단서에서 "금융위원회가 인정하는 경우"란 전자금융거래정보의 보호와 관련된 전산장비·소프트웨어에 대한 개발·운영 및 유지관리 업무를 재위탁하는 경우로서 다음 각 호의 사항을 준수하는 경우를 말한다.

1. 재수탁업자가 재위탁된 업무를 처리함에 있어 금융거래 정보의 변경이 필요한 경우에는 위탁회사 또는 원수탁업자의 개별적 지시에 따라야 하며, 위탁회사 또는 원수탁업자는 변경된

정보가 지시 내용에 부합하는지 여부를 확인하여야 함

2. 위탁업무와 관련된 이용자의 금융거래정보는 위탁회사의 전산실 내에 두어야 함. 다만, 재수탁업자가 이용자의 이용자 정보를 어떠한 경우에도 알지 못하도록 위탁회사 또는 원수탁업자가 금융거래정보를 처리하여 제공한 경우에는 위탁회사의 관리·통제 하에 재수탁회사 등 제3의 장소로 이전 가능함

제61조(전자금융보조업자 자료제출 기준) ① 금융감독원장은 전자금융보조업자에 대해 외부주문등과 관련한 계약서, 계약서 부속자료 및 그 밖의 전자금융업무와 관련한 자료 등을 직접 요구할 수 있다.

② 제1항에 따른 자료제출 요구시 전자금융보조업자는 특별한 이유가 없는 한 자료제출에 응하여야 한다.

제62조(업무보고서의 제출) ① 법 제42조에 따라 금융회사 및 전자금융업자는 금융감독원장이 정하는 바에 따라 업무보고서를 금융감독원장에게 제출하여야 한다. 다만, 법 제2조제1호에 따른 전자금융업무를 하지 아니하는 금융회사는 그러하지 아니하다.

② 제1항에 따른 업무보고서 제출은 정보통신망(「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」 제2조의 규정에 의한 정보통신망을 말한다)을 이용한 전자문서의 방법에 의할 수 있다.

③ 제1항의 업무보고서 제출에 관한 세부적인 절차, 양식 등에 관해서는 금융감독원장이 별도로 정한다.

제63조(전자금융업자 경영지도기준) ① 법 제42조제2항에 따른 구체적인 경영지도기준은 다음과 같다.

1. 법 제30조 및 시행령 제17조에 따른 허가나 등록요건 상 최소자본금·출자총액 또는 기본재산 기준을 항상 충족할 것
2. 총자산에서 총부채를 감한 자기자본이 항상 0을 초과할 것
3. 미상환잔액 대비 자기자본 비율은 100분의 20 이상일 것(전자화폐 및 선불전자지급수단 발행자에 한한다)
4. 총자산 대비 투자위험성이 낮은 자산의 비율은 100분의 10 이상으로 유지하거나 미정산잔액 대비 투자위험성이 낮은 자산의 비율을 100분의 100 이상으로 유지할 것. 단, 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자 및 법 제28조제2항제3호의 규정에 따라 등록을 한 전자금융업자는 제외한다. 이 때 투자위험성이 낮은 자산은 <별표 6>와 같다.
5. 유동성 비율은 다음 각 목과 같이 유지할 것

가. 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자 : 100분의 60 이상

나. 법 제28조제2항제3호의 규정에 따라 등록을 한 전자금융업자 : 100분의 50 이상

다. 그 밖의 등록대상 전자금융업자 : 100분의 40 이상

② 제1항에서 정하는 비율의 구체적 산정기준은 금융감독원장이 정한다.

③ 금융감독원장은 제1항의 경영지도비율이 악화될 우려가 있거나 경영상 취약부문이 있다고 판단되는 전자금융업자에 대하여 이의 개선을 위한 계획 또는 약정서를 제출토록 하거나 해당 전자금융업자와 경영개선협약을 체결할 수 있다. 다만, 제64조 부터 제66조까지의 규정에 의한 경영개선권고, 경영개선요구 또는 경영개선명령을 받고 있는 전자금융업자의 경우에는 그러하지 아니하다.

제64조(경영개선권고) ① 금융위원회는 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자가 다음 각 호의 어느 하나에 해당되는 경우에는 해당 전자금융업자에 대하여 필요한 조치를 이행하도록 권고하여야 한다.

1. 제63조제1항제3호의 미상환잔액 대비 자기자본 비율이 100분의 20 미만인 경우
2. 거액의 금융사고 또는 부실채권의 발생으로 제1호의 기준에 해당될 것이 명백하다고 판단되는 경우

② 제1항에서 정하는 필요한 조치라 함은 다음 각 호의 일부 또는 전부에 해당하는 조치를 말한다.

1. 인력 및 조직운영의 개선
2. 경비절감
3. 고정자산투자, 신규업무영역에의 진출 및 신규출자의 제한
4. 부실자산의 처분
5. 자본금의 증액 또는 감액
6. 이익배당의 제한
7. 특별대손충당금의 설정

③ 금융위원회는 제1항에 의한 권고를 하는 경우 해당 전자금융업자 및 관련 임원에 대하여 주의 또는 경고조치를 취할 수 있다.

제65조(경영개선요구) ① 금융위원회는 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자가 다음 각 호의 어느 하나에 해당되는 경우에는 해당 전자금융업자에 대하여 필요한 조치를 이행하도록 요구하여야 한다.

1. 제63조제1항제3호의 미상환잔액 대비 자기자본 비율이 100분의 10 미만인 경우
2. 거액의 금융사고 또는 부실채권의 발생으로 제1호의 기준에 해당될 것이 명백하다고 판단되는 경우
3. 제64조제1항의 규정에 의해 경영개선권고를 받은 전자금융업자가 경영개선계획의 주요사항을 이행하지 않아 제69조제8항의 규정에 의해 이행촉구를 받았음에도 이를 이행하지 아니하는 경우

② 제1항에서 정하는 필요한 조치라 함은 다음 각 호의 일부 또는 전부에 해당하는 조치를 말한다.

1. 조직의 축소

2. 위험자산의 보유제한 및 처분
3. 자회사의 정리
4. 임원진 교체 요구
5. 영업의 일부정지
6. 합병, 제3자 인수, 영업의 전부 또는 일부 양도계획의 수립
7. 제64조제2항에서 정하는 사항

제66조(경영개선명령) ① 금융위원회는 법 제28조제1항의 규정에 따라 허가를 받은 전자금융업자가 다음 각 호의 어느 하나에 해당하는 경우에는 해당 전자금융업자에 대해 필요한 조치를 이행하도록 명령하여야 한다.

1. 제63조제1항제3호의 미상환잔액 대비 자기자본 비율이 100분의 5 미만인 경우
2. 제65조제1항의 규정에 의해 경영개선요구를 받은 전자금융업자가 경영개선계획의 주요사항을 이행하지 않아 제69조제8항의 규정에 의해 이행촉구를 받았음에도 이를 이행하지 아니하거나 이행이 곤란하여 정상적인 경영이 어려울 것으로 인정되는 경우

② 제1항에서 정하는 필요한 조치라 함은 다음 각 호의 일부 또는 전부에 해당하는 조치를 말한다. 다만, 영업의 전부정지, 영업의 전부양도, 계약의 전부이전 또는 주식의 전부소각의 조치는 제1항제1호의 기준에 미달하고 건전한 전자금융거래질서나 이용자의 권익을 해할 우려가 현저하다고 인정되는 경우에 한한다.

1. 주식의 전부 또는 일부 소각
2. 임원의 직무집행 정지 및 관리인의 선임
3. 6월 이내의 영업의 정지
4. 계약의 전부 또는 일부의 이전
5. 제65조제2항에서 정하는 사항

제67조(이유제시 등) 제64조 부터 제66조의 조치를 하는 경우 금융위원회는 해당 전자금융업자에게 그 근거와 이유를 제시하여야 한다.

제68조(적기시정조치의 유예) 제64조제1항, 제65조제1항 및 제66조제1항 각 호의 어느 하나에 해당하는 전자금융업자가 자본의 확충 또는 자산의 매각 등을 통하여 단기간 내에 그 기준에 해당되지 않을 수 있다고 판단되는 경우 또는 이에 준하는 사유가 있다고 인정되는 경우에는 금융위원회는 일정기간동안 조치를 유예할 수 있다.

제69조(경영개선계획 제출 및 평가 등) ① 제64조 부터 제66조에 의해 경영개선권고, 경영개선요구 또는 경영개선명령을 받은 전자금융업자는 동 조치를 받은 후 2월의 범위 내에서 금융위원회가 정하는 기한 내에 해당 조치의 내용이 반영된 계획(이하 "경영개선계획"이라 한다)을 금융감독원장에게 제출하여야 한다.

② 금융위원회는 제64조 부터 제66조에 의해 경영개선권고, 경영개선요구 또는 경영개선명령을 받은 전자금융업자가 제1항에 의해 제출한 계획에 대하여 1월 이내에 승인여부를 결정하여

야 한다. 다만, 제3항의 규정에 의한 경영평가위원회의 심의가 지연되는 경우에는 15일 이내에서 그 기한을 초과할 수 있다.

③ 금융감독원장은 제2항의 금융위원회의 승인여부 결정 이전에 해당 계획에 대하여 외부 전문가로 구성된 경영평가위원회의 심의를 거치도록 하여야 한다. 다만, 긴급을 요하거나 심의의 실익이 크지 아니하다고 금융감독원장이 인정하는 경우에는 그러하지 아니하다.

④ 제3항에 의해 경영평가위원회가 사전심의를 하는 경우에는 해당 전자금융업자를 출석시켜 의견을 청취할 수 있다.

⑤ 금융위원회는 제64조에 의해 경영개선권고를 받은 전자금융업자가 제1항의 규정에 의해 제출한 계획의 타당성이 인정되지 않을 경우 동 계획을 불승인하고, 제65조제2항 각 호의 일부 또는 전부에 해당하는 조치를 요구하며, 동 조치내용이 반영된 계획을 일정기간 내에 제출하도록 하여 승인여부를 결정한다.

⑥ 금융위원회는 제5항의 규정에 의해 제출한 계획 또는 제65조에 의해 경영개선요구를 받은 전자금융업자가 제1항의 규정에 의해 제출한 계획의 타당성이 인정되지 않을 경우 동 계획을 불승인한다. 이 경우 금융위원회는 제65조제2항 각 호의 일부 또는 전부에 해당하는 조치를 요구하고, 동 조치내용이 반영된 계획을 일정기간 내에 제출토록 하여야 하며 동 계획의 타당성이 인정되지 않을 경우에는 제66조제2항에서 규정한 조치의 일부 또는 전부를 이행하도록 명령하여야 한다.

⑦ 금융위원회는 제6항의 규정에 의해 제출된 계획 또는 제66조에 의해 경영개선명령을 받은 전자금융업자가 제1항의 규정에 의해 제출한 계획의 타당성이 인정되지 않을 경우 동 계획을 불승인한다. 이 경우 금융위원회는 제71조 각 호의 일부 또는 전부에 해당하는 조치를 할 수 있다.

⑧ 제2항의 규정에 따라 경영개선계획을 승인받은 전자금융업자는 매분기말 익월 10일까지 동 계획의 분기별 이행실적을 금융감독원장에게 제출하여야 하며, 금융감독원장은 그 이행실적이 미흡하거나 관련제도의 변경 등 여건변화로 인하여 이행이 곤란하다고 판단되는 경우에는 경영개선계획의 수정요구, 일정기간 내 이행촉구 등 필요한 조치를 취할 수 있다.

⑨ 제8항의 규정에 따라 금융감독원장이 경영개선권고, 경영개선요구 또는 경영개선명령을 받은 전자금융업자의 경영개선계획의 주요사항을 수정 요구하거나 일정기간 내 이를 이행토록 촉구하는 경우에는 그 내용을 금융위원회에 사전 보고하여야 한다.

⑩ 제8항의 규정에 따라 전자금융업자가 경영개선계획의 주요사항을 수정하여 제출한 경우에는 제2항부터 제7항을 준용할 수 있다.

⑪ 제3항의 경영평가위원회의 구성、운영과 관련된 세부사항은 금융감독원장이 정한다.

제70조(경영개선계획 이행기간 등) ① 제64조에 의하여 경영개선권고를 받은 전자금융업자의 경영개선계획 이행기간은 승인일로부터 6월 이내로 한다.

② 제65조에 의하여 경영개선요구를 받은 전자금융업자의 경영개선계획 이행기간은 승인일로부터 1년 이내로 한다. 이 경우 제64조에 의하여 경영개선권고를 받은 전자금융업자가 경영개선계획 이행 중 경영개선요구를 받은 경우의 이행기간은 경영개선권고에 따른 경영개선계

획의 승인일로부터 1년 이내로 한다.

③ 제69조제8항에 의하여 금융감독원장으로부터 경영개선계획의 수정요구 또는 일정기간 내 이행촉구를 받은 경우에는 제1항과 제2항의 기간을 초과할 수 있다. 다만, 그 초과기간은 제1항 또는 제2항에서 정하는 기간 이내이어야 한다.

④ 제66조에 의하여 경영개선명령을 받은 전자금융업자의 경영개선계획의 이행기간은 금융위원회가 정한다.

⑤ 제64조 부터 제66조까지의 규정에 의해 경영개선권고, 경영개선요구 또는 경영개선명령을 받은 전자금융업자가 자본 확충 또는 부실채권정리 등 경영개선계획의 주요사항을 조기에 달성하여 경영상태가 현저히 개선된 경우에는 금융위원회는 권고, 요구 또는 명령한 조치의 내용을 완화하거나 그 이행을 면제할 수 있다.

⑥ 제64조 부터 제66조까지의 규정에 의해 경영개선권고, 경영개선요구 또는 경영개선명령을 받은 전자금융업자의 경영개선계획 이행기간이 만료되어 경영상태가 충분히 개선되었다고 인정되는 경우에는 금융위원회는 당초의 조치가 종료되었음을 통지하여야 하며, 경영상태가 제64조제1항, 제65조제1항 또는 제66조제1항에 해당하는 경우에는 동 조항에 따라 별도의 경영개선권고, 경영개선요구 또는 경영개선명령을 하여야 한다.

제71조(경영개선계획의 불이행에 따른 조치) 금융위원회는 제66조에 의하여 경영개선명령을 받은 전자금융업자가 제70조에 의한 이행기한 내에 경영개선계획의 주요사항을 이행하지 아니하여 경영정상화가 이루어지지 아니하였다고 판단되는 경우 해당 전자금융업자에 대하여 다음 각 호의 일부 또는 전부에 해당하는 조치를 할 수 있다.

1. 제66조제2항에서 정한 조치
2. 허가의 취소
3. 임원의 해임 권고
4. 그 밖에 이용자 보호를 위하여 필요한 조치

제72조(과징금 수납기관 및 납부서식 등) ① 시행령 제27조제1항의 규정에 의하여 금융위원회가 과징금의 납부를 통지하는 경우에는 <별지 제2호 서식>에 따른다.

② 시행령 제27조제2항에 따른 수납기관은 은행법에 의한 금융회사와 우체국으로 한다.

제72조의2(과징금 과오납에 따른 환급가산금 이율) 금융위원장은 「은행법」 제8조에 따라 은행업 인가를 받은 국내은행의 1년 만기 정기예금 이자율을 감안하여 환급가산금 이자율을 정하여야 한다.

제6장 보칙

제73조(정보기술부문 및 전자금융 사고보고) ① 금융회사 및 전자금융업자는 다음 각 호와 관련된 중대한 사고가 발생한 경우에는 지체 없이 금융감독원장에게 보고하여야 한다.

1. 정보처리시스템 또는 통신회선 등의 장애로 10분 이상 전산업무가 중단 또는 지연된 경우
2. 전산자료 또는 프로그램의 조작과 관련된 금융사고가 발생한 경우
3. 전자적 침해행위로 인해 정보처리시스템에 사고가 발생하거나 이로인해 이용자가 금전적 피해를 입었다고 금융회사 또는 전자금융업자에게 통지한 경우
4. 법 제9조제1항의 규정에서 정하는 사고

② 금융회사 및 전자금융업자는 제1항에 따른 사고보고를 고의로 지연하거나 숨긴 자에 대하여 소정절차에 따라 징계 등 필요한 조치를 취하여야 한다.

③ 금융감독원장은 제1항에 따라 보고 받은 내용을 지체 없이 금융위원장에게 보고하여야 하며, 제1항제3호에 따른 사고 발생시에는 제37조의4제1항 각 호에 따른 침해사고대응기관에도 알려야 한다.

④ 제1항의 사고보고와 관련하여 사고보고 절차 및 방법 등 세부사항은 금융감독원장이 정하는 바에 따른다.

제74조(위탁업무의 처리 결과 보고) 금융감독원장은 시행령 제30조의 규정에 따라 금융위원회로부터 위탁받은 업무의 처리 결과를 매분기 금융위원회에 보고하여야 한다.

제75조(규제의 존속기한 및 재검토) ① 금융위원회는 행정규제기본법 제8조·제19조의2 및 훈령·예규 등의 발령 및 관리에 관한 규정(대통령훈령 제248호)에 따라 이 고시에 대하여 2014년 1월 1일을 기준으로 매 3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다. 다만, 제14조의2제1항에 대하여는 2017년 1월 1일을 기준으로 매 2년이 되는 시점(매 2년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

② 제8조제2항은 2020년 1월 1일까지 효력을 가진다.

부칙 <제2011-18호,2011.10.10>

제1조(시행일) 이 규정은 고시한 날부터 시행한다. 다만, 제15조제6항제2호 및 제3호, 제17조제1항제2호 단서 및 제34조제2항제7호의 개정규정은 이 규정 고시 후 6개월이 경과한 날부터 시행한다.

제2조(정보보호 인력 및 예산의 적용례) 제8조제2항의 개정규정은 이 규정 시행 후 최초로 개시되는 사업연도부터 적용한다.

부칙 <제2012-26호,2012.10.31>

이 규정은 고시한 날부터 시행한다. 다만, 제6조, 제44조, 제45조 및 제48조의 개정규정은 2012년 11월 8일부터 시행한다.

부칙 <제2013-39호,2013.12.3>

제1조(시행일) 이 규정은 고시한 날부터 시행한다. 다만, 제15조제1항제3호의 규정은 「은행법」에 따라 인가를 받아 설립된 은행은 2016년 1월 1일부터, 그 외의 자는 2017년 1월 1일부터 시행하고, 같은 항 제5호의 규정은 2015년 1월 1일부터 시행한다.

부칙 <제2013-44호,2013.12.31>

제1조(시행일) 이 규정은 2014년 1월 1일부터 시행한다.

부칙 <제2015-3호,2015.2.3>

제1조(시행일) 이 규정은 고시한 날부터 시행한다. 다만, 제37조의5조, 제60조 및 제73조의 개정규정은 2015년 4월 16일부터 시행한다.

부칙 <제2015-7호,2015.3.18>

제1조(시행일) 이 규정은 고시한 날부터 시행한다. 다만, 제37조의4의 개정규정은 같은 조 제1항제1호에 따른 금융보안원이 성립한 날부터 시행한다.

부칙 <제2015-18호,2015.6.24>

제1조(시행일) 이 규정은 고시한 날부터 시행한다.

부칙 <제2016-24호,2016.6.30>

이 규정은 2016년 6월 30일부터 시행한다.

부칙 <제2016-37호,2016.10.5>

제1조(시행일) 이 고시는 공포한 날부터 시행한다. 다만, 제5조제1항제6호 및 제5조제2항의 개정규정은 이 규정 고시 후 6개월이 경과한 날부터 시행한다.

제2조(인력, 조직 및 예산 기준 미준수 공시에 관한 적용례) 제8조제3항의 개정규정은 이 규정 시행 전에 허가, 등록 또는 인가를 마친 금융회사 또는 전자금융업자에 대하여도 적용한다.

<별표 1> <개정 2013.12.3., 2015.2.3.>

정보기술부문 및 정보보호 인력 산정기준

1. 총임직원 및 외주인력

가. 총임직원 수는 금융회사등의 상시 종업원(「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 기준으로 한다. 이하 같다)으로 하되, 1년 이상 장기휴직자와 외주(outsourcing)인력은 제외한다.

나. 외주인력이란 금융회사등과의 외부주문등에 따라 업무를 처리하는 업체에 소속된 자로서 다음 각 호의 기준에 따라 산정한다.

(1) 금융회사등의 정보기술부문 업무 수행을 위한 정보화 기획, 전자금융기반시설 운영, 정보보안 등의 IT(Information Technology, 정보통신기술)업무 종사자를 포함한다.

(2) 전자금융기반시설의 하드웨어 또는 소프트웨어 등의 유지보수를 수행하기 위한 제조사의 상시 운영 기술인력은 포함한다.

(3) 정보시스템 개발 프로젝트를 수행하기 위하여 상주하는 외주업체의 IT 업무 종사자는 제외한다.

(4) 외주인력 중 월·주 단위 등 부정기적이거나 일시적인 인력은 제외한다.

(5) 그 밖의 금융위원장이 외주인력에 포함 또는 제외하는 것이 필요하다고 인정한 인력은 해당인력을 외주인력에 포함시키거나 제외할 수 있다.

2. 정보기술부문 인력

정보기술부문 인력이란 다음 각 목에 해당되는 자를 말한다.

가. 금융회사의 총임직원 중 내부 규정에 따라 IT 기획·개발·운영·정보보호 등 정보기술부문의 업무를 처리하는 사람

나. 다음 각 호에 소속되어 IT업무를 담당하는 상시 종업원 중 해당 금융회사의 IT업무를 적법한 절차에 의해 수행하는 사람으로서, 이 규정 제60조제1항제13호에 의한 업무수행인력 관리방안에 따라 관리되고 있는 사람(이 경우, 해당 금융회사의 정보기술 인력 규모는 다음 각 호의 회사 또는 기관이 공동으로 위탁 받은 정보기술부문에 대한 운영비용 분담비율에 따라 산정한다)

(1) 「금융지주회사법」 제2조제1항에 의한 자회사 또는 손자회사로써 금융업을 영위하는 회사에 대한 전산·정보처리 등의 용역을 제공하는 회사

(2) 금융회사 또는 전자금융업자가 지분을 50%를 초과하여 소유하는 IT자회사 또는 IT손자회사로서 당해 금융회사 또는 전자금융업자에 대한 전산·정보처리 등의 용역 제공을 전업으로 하는 회사

(3) 「독점규제 및 공정거래에 관한 법률」 제2조제2호에 의한 기업집단에 속하는 금융회사들 또는 전자금융업자들이 합하여 지분을 50%를 초과하여 소유하는 IT자회사 또는 IT손자회사로서 당해 금융회사들 또는 전자금융업자들에 대한 전산·정보처리 등의 용역 제공을 전업으로 하는 회사

(4) ㈜코스콤, 상호저축은행중앙회, 신용협동조합중앙회, 농협중앙회, 수협중앙회, 산림조합중앙회, 새마을금고중앙회 등과 같이 회원사, 상호저축은행, 신용협동조합, 조합, 지역금고 등의 전자금융기반시설에 대한 운영을 공동수탁하는 기관

다. 나목을 제외한 외주인력 중 해당 금융회사 또는 전자금융업자의 IT업무를 적법한 절차에 의해 수행하는 사람으로서, 이 규정 제60조제1항제13호에 의한 업무수행인력 관리방안에 따라 관리되고 있는 사람(다만, 다목의 인력은 가목의 인력 규모 내에서 정보기술부문 인력으로 인정한다)

3. 정보보호 인력

정보보호 인력이란 다음 각 목에 해당되는 자를 말한다.

가. 금융회사의 총임직원 중 내부 규정에 따라 정보보호 업무를 처리하는 사람

나. 다음 각 호에 소속되어 정보보호 업무를 담당하는 상시 종업원 중 해당 금융회사의 정보보호 업무를 적법한 절차에 의해 수행하는 사람으

로서, 전자금융감독규정 제60조제1항제13호에 의한 업무수행인력 관리방안에 따라 관리되고 있는 사람(이 경우, 해당 금융회사의 정보보호 인력 규모는 다음 각 호의 회사 또는 기관이 공동으로 위탁 받은 정보보호 업무에 대한 운영비용 분담비율에 따라 산정한다)

(1) 「금융지주회사법」 제2조제1항에 의한 자회사 또는 손자회사로써 금융업을 영위하는 회사에 대한 전산·정보처리 등의 용역을 제공하는 회사

(2) 금융회사 또는 전자금융업자가 지분을 50%를 초과하여 소유하는 IT자회사 또는 IT손자회사로서 당해 금융회사 또는 전자금융업자에 대한 전산·정보처리 등의 용역 제공을 전업으로 하는 회사

(3) 「독점규제 및 공정거래에 관한 법률」 제2조제2호에 의한 기업집단에 속하는 금융회사들 또는 전자금융업자들이 합하여 지분을 50%를 초과하여 소유하는 IT자회사 또는 IT손자회사로서 당해 금융회사들 또는 전자금융업자들에 대한 전산·정보처리 등의 용역 제공을 전업으로 하는 회사

(4) ㈜코스콤, 상호저축은행중앙회, 신용협동조합중앙회, 농협중앙회, 수협중앙회, 산림조합중앙회, 새마을금고중앙회 등과 같이 회원사, 상호저축은행, 신용협동조합, 조합, 지역금고 등의 전자금융기반시설에 대한 운영을 공동수탁하는 기관

다. 나목을 제외한 외주인력 중 해당 금융회사 또는 전자금융업자의 정보보호 업무를 적법한 절차에 의해 수행하는 사람으로서, 이 규정 제60조제1항제13호에 의한 업무수행인력 관리방안에 따라 관리되고 있는 사람(다만, 다목의 인력은 가목의 인력 규모 내에서 정보보호 인력으로 인정한다)

<별표 2> 정보기술부문 및 정보보호 예산 기준

1. 정보기술부문 예산 기준

가. 정보기술부문 예산 개요

(1) 정보기술부문과 관련하여 기획·개발·운영·유지·보수 및 정보보호 등에 소요되는 모든 경비의 합계

(2) 정보기술부문 예산은 건물·시설 이용료, 건물·시설 공사비, 전기·전화 등 각종 세금과 공과금 및 사업성 경비는 제외

나. 정보기술부문 예산 항목

예산 항목	세부 내용
(1) 인건비	○정보기술부문과 관련하여 기획·개발·운영·유지·보수를 수행하는 내부 인력(정규직 및 계약직 포함)의 인건비 및 복리 후생비 등 관련 경비 일체 ○개인사무자동화기기(PC 등) 및 정보처리시스템을 단순 조회·이용하는 내부직원과 외부 주문·제휴에 따라 정보기술부문 관련 업무를 수행하는 외부 인력은 제외
(2) 정보처리시스템 구입비 및 임차료	○정보기술부문과 관련하여 하드웨어 및 소프트웨어를 구입 또는 임차(리스)하는데 소요되는 경비 일체 ○단순히 사무를 처리하기 위하여 사용하는 사무자동화기기(PC, 프린터, 팩스 등)는 제외
(3) 정보처리시스템 유지보수비	○정보처리시스템의 성능을 최적화하고 정상적 기능을 수행할 수 있도록 정기 또는 수시로 정보처리시스템을 유지하고 관리하는데 소요되는 경비 일체 ○정보처리시스템 관련 소모품 교체 비용 포함
(4) 정보기술 서비스이용료	○정보처리시스템 및 정보기술부문과 관련하여 필요한 서비스를 이용하는데 소요되는 경비 일체 ○S/W라이센스비용, 기술이전·이용료, 정보이용료, 특허 사용료, 정보보호관제·인증·재해복구 등 정보보호서비스 이용료 포함
(5) 정보기술 외주 용역비	○외부 주문 또는 제휴 등에 따라 정보처리시스템과 관련하여 기획·개발·운영·유지·보수의 일부 또는 전부의 업무를 외부업체에 위탁(아웃소싱)하여 수행하는데 소요되는 경비 일체
(6) 정보기술 컨설팅 비용	○정보처리시스템 및 정보기술부문과 관련하여 외부기관으로부터 자문, 점검, 분석, 평가, 인증, 심사, 연구, 조사에 소요되는 경비 일체 ○감리비, 자문료, 취약점 분석·평가 비용, 품질인증심사비, 국

예산 항목	세부 내용
	제표준인증심사비 포함
(7) 정보기술 교육·훈련비	○정보처리시스템 및 정보기술부문과 관련하여 임직원의 교육, 직무훈련·연수 및 회의·행사에 소요되는 경비 일체 ○도서▪교재 구입비, 교육자료인쇄비, 인쇄비, 세미나·워크샵·학술발표회 등 회의·행사개최·참가비, 강사료, 직무교육프로그램 참가비▪수강료, 직무훈련▪연수과정(대학포함) 수업료 포함
(8) 통신회선 이용료	○정보처리시스템과 관련하여 정보의 송신, 수신과 정보처리시스템간 접속·연계를 위하여 정보통신사업자(인터넷서비스제공자 포함)로부터 인터넷, 전용회선 등 통신회선을 이용하는데 소요되는 경비 일체 ○재해복구센터용 통신회선 이용료, 디도스공격대응용 통신회선 이용료 포함 ○직원의 정보검색, 이메일 송·수신 등 사무자동화용으로 사용하는 통신회선의 이용료는 제외

*상기 정보기술부문 예산 항목이외 제2조 제4호의 규정에서 정한 정보기술부문과 관련된 예산 항목을 포함할 수 있다.

2. 정보보호 예산 기준

가. 예산 개요

정보기술부문 예산중 정보보호와 관련하여 소요되는 모든 경비의 합계. 다만, 정보기술부문 예산에 포함되지 아니한 경비는 제외한다.

나. 예산 항목

예산 항목	세부 내용
(1) 정보보호 관련 인건비	○정보보호와 관련하여 기획·개발·운영·유지·보수를 수행하는 내부 인력(정규직 및 계약직 포함)의 인건비 및 복리 후생비 등 관련 경비 일체 ○외부 주문·제휴에 따라 정보보호 관련 업무를 수행하는 외주 인력과 관련된 경비는 제외
(2) 정보보호시스템 구입비 및 임차료	○정보보호와 관련하여 하드웨어 및 소프트웨어를 구입 또는 임차(리스)하는데 소요되는 경비 일체 ※다. 정보보호시스템 분류표 참고
(3) 정보보호시스템 유지보수비	○정보보호시스템의 성능을 최적화하고 정상적 기능을 수행할 수 있도록 정기 또는 수시로 정보보호시스템을 유지하고 관리하는데 소요되는 경비 일체 ○정보보호시스템 관련 소모품 교체 비용 포함
(4) 정보보호서비스 이용료	○정보보호와 관련하여 제공되는 서비스를 이용하거나 정보보호시스템와 관련하여 필요한 기술을 확보하는데 소요되는 경비 일체 ※ 라. 정보보호서비스 분류표 참고 ○정보보호S/W라이센스비용, 정보보호기술이전·이용료 포함
(5) 정보보호 관련 외주 용역비	○외부 주문 또는 제휴에 따라 정보보호시스템과 정보보호서비스와 관련하여 기획·개발·운영·유지·보수의 일부 또는 전부의 업무를 외부업체에 위탁(아웃소싱)하는데 소요되는 경비 일체
(6) 정보보호 관련 컨설팅 비용	○정보보호와 관련하여 외부기관으로부터 자문, 점검, 분석, 평가, 인증, 심사, 연구, 조사에 소요되는 경비 일체 ※마. 정보보호컨설팅 분류표 참고
(7) 정보보호 관련 교육·훈련비	○정보보호와 관련하여 임직원의 교육, 직무훈련·연수 및 회의·행사에 소요되는 경비 일체
(8) 정보보호 관련 통신회선 이용료	○재해복구센터용 통신회선 이용료 ○디도스공격대응용 통신회선 이용료

*상기 정보보호 예산 항목이외 제2조 제5호의 규정에서 정한 정보보호와 관련된 예산 항목을 포함할 수 있다.

다. 정보보호시스템 분류표

대분류	소분류	세부항목
(1) 컨텐츠 정보보호	①DB정보보호	○DB암호화

대분류	소분류	세부항목
		○DB접근통제
	②디지털저작권관리	○저작권관리(DRM) ○자료유출방지(DLP)
	③개인정보보호	○정보보호서버 ○개인정보필터링 S/W
	④데이터백업	◦데이터 백업·소산시스템 ○재해복구(DR)시스템
	⑤기타	○도청 및 감청 방지 제품
(2) 시스템 정보보호	①사용자 인증	○정보보호토큰(HSM) ○정보보호스마트카드 ○일회용 비밀번호(OTP) 생성시스템 ○생체(Bio)인식시스템
	②PC정보보호	○PC정보보호관리 ○정보보호USB ○키보드해킹방지프로그램
	③Anti-Virus/Spam	○바이러스백신(Vaccine) ○바이러스월(wall) ○안티 스파이웨어(Spyware) ○스팸(Spam) 차단 ○피싱(Phishing) 방지
	④접근통제	○정보보호운영체제(SecureOS) ○통합접근권한관리(EAM) ○싱글사인온(SSO) ○통합계정관리시스템(IM/IAM)
(3) 네트워크 정보보호	①침입차단시스템	○네트워크방화벽 ○시스템 방화벽 ○PC방화벽 ○웹방화벽 ○통합위협관리시스템(UTM)
	②침입방지시스템	○침입탐지(IDS) ○침입방지(IPS)
	③가상사설망	○VPN
	④전자서명	○공개키기반(PKI)
	⑤네트워크통제	○망접근제어(NAC)
	⑥무선·모바일정보보호	○무선랜정보보호 ○모바일정보보호
	⑦DDoS대응	○DDoS대응(탐지,차단)시스템
(4) 정보보호관리	①정보보호관리서비스	○네트워크정보보호관리(NMS) ○위협관리시스템(TMS) ○위험관리시스템(RMS) ○기업정보보호관리(ESM) ○패치관리시스템(PMS)

대분류	소분류	세부항목
		○ 로그(log) 관리·분석 툴 ○ 취약점 분석·포렌식 툴

* 상기 정보보호시스템이외 제2조 제6호의 규정에서 정한 정보보호시스템을 포함할 수 있다.

라. 정보보호서비스 분류표

대분류	소분류	세부항목
정보보호서비스	①인증서비스	○ 공인/사설인증서비스
	②정보보호관제서비스	○ 정보보호관제서비스
	③재해복구서비스	○ 재해복구서비스
	④위협정보제공서비스	○ 취약점, 대응방안 등 정보제공서비스

* 상기 정보보호서비스이외 제2조 제5호의 규정에서 정한 정보보호와 관련된 서비스를 포함할 수 있다.

마. 정보보호컨설팅 분류표

대분류	소분류	세부항목
정보보호컨설팅	①정보보호컨설팅	○ 정보보호계획 수립·자문 ○ 정보보호표준 인증 심사 ○ 정보보호제품 시험·평가 ○ 정보보호 연구·개발 ○ 정보기술부문 감리
	②취약점 분석	○ 취약점 분석·평가 ○ 모의 해킹 ○ 모의 훈련

*상기 정보보호컨설팅이외 제2조 제5호의 규정에서 정한 정보보호와 관련된 컨설팅을 포함할 수 있다.

<별표 3> 전자지급수단의 세부적 이용한도

가. 전자화폐 및 선불전자지급수단 발행권면 최고한도

(단위 : 만원)

구 분	발행권면 한도	
	무기명식[1]	기명식[2]
전자화폐	5	**200**
선불전자지급수단	50	**200**

1) 실지명의 확인이 없거나 예금계좌와 연결되지 않고 발행된 전자화폐 내지 선불전자지급수단

2) 실지명의가 확인되거나 예금계좌와 연결되어 발행된 전자화폐 내지 선불전자지급수단

나. 전자자금이체한도(지급이체의 경우)

(단위 : 억원)

구 분		1회 이체한도	1일 이체한도
현금카드[1]	인출한도	0.01	0.06
	이체한도	0.06	0.3
텔레뱅킹[2]	개인	0.5	2.5
	법인	1	5
인터넷뱅킹[3]	개인	1	5
	법인	10	50
모바일뱅킹[4]		1	5
메일뱅킹[5]		0.1	0.5

1) 금융회사의 자동화기기(CD/ATM)에서 현금을 인출하기 위해 사용하는 접근매체

2) 유선전화를 통하여 예금조회, 자금이체 등의 업무를 수행하는 전자금융방식

3) 유무선 인터넷을 통해 예금조회, 자금이체 등의 업무를 수행하는 전자금융방식

4) 이동통신용 기기에 IC칩을 넣거나 뱅킹용 프로그램을 다운로드하여 예금조회, 자금이체 등의 업무를 수행하는 전자금융방식

5) 예금계좌와 연결된 전자우편 주소(기타 전화번호)를 통해 자금이체 등의 업무를 수행하는 전자금융방식

*** 전자자금이체시 제34조 및 제37조의 규정에서 정한 사항을 준수하여야 한다.**

다. 직불전자지급수단 이용한도

(단위 : 만원)

구 분	1회 이용한도	1일 이용한도
직불전자지급수단	10000	10000
실명증표확인 외의 본인확인수단을 이용하여 발급된 직불전자지급수단	200	200

<별표 4> 주요출자자 요건

구 분	요 건
1. 주요출자자가 「금융위원회의 설치등에 관한 법률」 제38조의 규정에 의하여 금융감독원으로부터 검사를 받는 기관인 경우	가. 최근 사업연도말 현재 대차대조표상 자산총액에서 부채총액을 차감한 금액(이하 "자기자본"이라 한다)이 출자하고자 하는 금액의 **3배** 이상일 것 나. 그 금융기관의 재무상태가 다음 기준을 충족할 것 (가) 그 금융기관에 적용되는 「금융산업의 구조개선에 관한 법률」상 적기시정조치의 기준이 있는 경우에는 그 금융기관의 재무상태가 동 기준을 상회할 것 (나) 그 금융기관에 적용되는 「금융산업의 구조개선에 관한 법률」상 적기시정조치 기준이 없는 경우에는 그 금융기관의 재무상태가 그 금융기관과 유사업종을 영위하는 금융기관의 적기시정조치 기준을 상회할 것. 다만, 그 금융기관에 대하여 유사업종의 적기시정조치기준을 적용하는 것이 현저히 부적합한 경우에는 2호 나목의 기준을 충족할 것 다. 당해 금융기관이 「독점규제 및 공정거래에 관한 법률」에 의한 기업집단에 속하는 회사인 경우에는 당해 기업집단 (금융업 또는 보험업을 영위하는 회사는 제외)의 부채비율(최근 사업연도말 현재 대차대조표상 부채총액을 자본총액으로 나눈 비율을 말한다. 이하 같다)이 100분의 200 이하일 것 라. 자본금 납입자금은 주요출자자의 출자능력을 초과하여 금융기관 등으로부터 단순 차입(출자자가 법인인 경우 기업어음·회사채 발행 등 부채성 조달자금을 포함한다)에 의한 것이 아니며, 그 출처가 명확할 것 마. 「금융산업의 구조 개선에 관한 법률」 또는 금융관련 법령에 의하여 부실금융기관으로 결정된 당해 부실금융기관의 대주주(최대주주 또는 주요주주를 말하며, 특수관계인을 포함한다. 이하 이 호에서 같다)이었던 자 또는 부실금융기관에 준하는 금융기관으로서 인가취소 등의 처분을 받은 당해 금융기관의 대주주가 아닐 것. 다만, 그 대주주가 부실경영에 관하여 직접 또는 간접으로 책임이 없다는 것이 인정되거나 금융위원회가 정하는 부실금융기관 대주주의경제적책임부담기준에 의하여 경제적 책임부담의무를 이행 또는 면제받은 경우에는 그러하지 아니함 바. 최근 5년간 법, 영, 금융관계법령, 「독점규제 및 공정거래에 관한 법률」 및 「조세범 처벌법」을 위반하여 벌금이상의 처벌을 받은 사실이 없을 것. 다만, 그 사실이 영위하고자 하는 업무의 건전한 영위를 어렵게 한다고 볼 수 없는 경우에는 그러하지 아니함
2. 주요출자자가 제1호외의 내국법인인 경우	가. 최근 사업연도말 현재 자기자본이 출자하고자 하는 금액의 **3배** 이상일 것 나. 최근 사업연도말 현재 부채비율이 100분의 200 이하일 것 다. 기업집단에 속하는 회사인 경우에는 당해 기업집단(금융업 또는 보험업을 영위하는 회사는 제외)의 부채비율이 100분의 200 이하일 것 라. 제1호 라목 부터 바목의 요건을 충족할 것
3. 주요출자자가 내국인으로서 개인인 경우	가. 제1호 라목 부터 바목의 요건을 충족할 것
4. 주요출자자가 외국법령에 의하여 설립된 외국기업인 경우	가. 제1호 가목 및 마목의 요건을 충족할 것

<별표 5> <개정 2013.12.3>

정보기술부문 실태평가 대상 금융회사

1. 「은행법」에 의해 인가를 받아 설립된 은행. 다만, 「은행법」 제58조에 의해 인가를 받은 외국금융회사의 국내지점은 제외한다.

2. 「한국산업은행법」에 의한 한국산업은행, 「중소기업은행법」에 의한 중소기업은행, 「농업협동조합법」에 의한 농협은행, 「수산업협동조합법」에 의한 수산업협동조합중앙회의 신용사업부문

3. 「자본시장과 금융투자업에 관한 법률」에 의한 투자매매업자·투자중개업자(다만,「자본시장과 금융투자업에 관한 법률」제12조에 의해 인가를 받은 외국 투자매매업자·투자중개업자의 지점 등은 제외한다), 증권금융회사, 한국금융투자협회 및 한국예탁결제원

4. 「보험업법」에 의한 보험회사. 다만, 외국보험회사의 국내지점은 제외한다. 보험협회, 보험요율산출기관 및「화재로 인한 재해보상과 보험가입에 관한 법률」에 의한 한국화재보험협회

5. 「여신전문금융업법」에 의한 여신전문금융회사(다만, 신용카드사 이외 여신전문금융회사의 경우 직전 사업년도 기준 자산규모 2조원 이상인 회사에 한한다) 및 여신전문금융업협회

6. 「자본시장과 금융투자업에 관한 법률」에 의한 종합금융회사

7. 「자본시장과 금융투자업에 관한 법률」에 의한 거래소

8. 「상호저축은행법」에 의한 상호저축은행중앙회 및 상호저축은행(다만, 직전 사업년도 기준 자산규모 2조원 이상인 상호저축은행에 한한다)

9. 「신용협동조합법」에 의한 신용협동조합중앙회

10. 「신용정보의 이용 및 보호에 관한 법률」에 의한 종합신용정보집중기관

<별표 6> 투자위험성이 낮은 자산의 종류

1. 현금(OECD 국가의 통화, 금 포함), 은행예금 및 한은예치 지급준비자산
2. 기업신용평가기관에 의해 A등급 이상으로 분류된 회사채 및 A2등급 이상의 기업어음, 발행어음, 표지어음
3. 정부 및 한국은행이 발행하거나 보증한 유가증권 : 통안증권, 재정증권, 국채, 정부보증채
4. 「은행법」상 은행에 대한 채권(債權), 은행이 지급을 보증한 채권, 동 기관이 발행 또는 보증한 증권에 의해 담보된 채권
5. 다음 각호의 1에 해당하는 국내 공공기관에 대한 채권, 동 기관이 보증한 채권, 동 기관이 발행 또는 보증한 증권에 의해 담보된 채권
   ① 「지방자치법」 및 「정부투자기관 관리기본법」에 의한 기관
   ② 「지방공기업법」에 의한 기관
   ③ 특별법에 의한 특수공공 법인(신용보증기금 등)
   ④ 「금융기관 부실자산 등의 효율적 처리 및 자산관리 공사의 설립에 관한 법률」에 의한 자산관리공사(부실 채권 정리기금) 및 「예금자보호법」에 의한 예금보험공사. 다만, ② 및 ③의 기관은 결손이 발생하는 경우 정부 또는 지방자치단체로부터 제도적으로 결손보전이 이루어 질 수 있는 기관에 한한다.
6. 정부가 출자한 주택저당채권유동화회사로서 금융위원회로부터 업무감독과 건전성규제를 받는 회사가 발행한 주택저당증권, 주택저당채권담보부채권 또는 동사에 대한 채권
7. OECD국가의 중앙정부 및 중앙은행에 대한 채권 및 동 기관이 발행 또는 보증한 증권에 의해 담보된 채권

<별지 제1호 서식> 삭제

<별지 제2호 서식> 과징금 부과 통지서

과징금납부통지서
(수납기관보관용)

발행번호		
납부자	성 명 (대표자)	
	주 소 (상 호)	
위반일자		. . .
위반행위		
납부금액		원
납부기한		. . .
납부장소		국고수납은행, 우체국

전자금융거래법 제46조의 규정에 의하여 위와 같이 과징금 납부를 통지하오니 납부기한까지 납부하여 주시기 바랍니다.

<공지사항>

1. 위 과징금 처분에 불복이 있는 때에는 30일이내에 금융위원회위원장에게 이의를 제기할 수 있음
2. 30일이내에 이의를 제기하지 아니하거나 위 과징금을 납부하지 아니한 때에는 국세체납처분의 예에 의하여 이를 징수합니다.

년 월 일	수납인
금융위원회위원장 (인)	

과징금영수필통지서
(금융위원회보관용)

발행번호		
납부자	성 명 (대표자)	
	주 소 (상 호)	
위반일자		. . .
위반행위		
납부금액		원
납부기한		. . .
납부장소		국고수납은행, 우체국

위와 같이 납입하였기에 통지함

년 월 일

은행(우체국)

년 월 일	수납인
금융위원회위원장 귀하	

과징
(납

발행번호		
납부자	성 (대표	
	주 (상	
위반일자		
위반행위		
납부금액		
납부기한		
납부장소		

위와

년 월

<별지 제3호 서식>

<table>
<tr><td colspan="4">전자금융업 영위 예비허가 신청서</td></tr>
<tr><td>① 상호</td><td colspan="3"></td></tr>
<tr><td>② 본점 소재지</td><td></td><td>연 락 처</td><td>전화:
팩스:</td></tr>
<tr><td>③ 대표자</td><td></td><td>주민등록
번호</td><td></td></tr>
<tr><td>④ 자본금</td><td colspan="3">수권자본금 :　　억원
납입자본금 :　　억원</td></tr>
<tr><td>⑤ 주요출자자의 성명 또는 명칭과 지분율</td><td colspan="3"></td></tr>
<tr><td>⑥ 영위하고자 하는 전자금융업</td><td colspan="3"></td></tr>
<tr><td>⑦ 전자금융업 이외 사업을 영위하고 있는 경우 당해 사업의 내용</td><td colspan="3"></td></tr>
<tr><td colspan="4">「전자금융거래법」 제33조 및 동법 시행령 제20조에 의한 전자금융업 영위 예비허가를 위와 같이 신청합니다.

년　　월　　일

신청인 :　　서명 또는 인

금융위원회 위원장 귀하</td></tr>
<tr><td colspan="4">※ 첨부서류
1. 정관
2. 법인의 등기부 등본
3. 자본금 납입 증명서류
4. 재무제표와 그 부속서류
5. 주주구성
6. 업무개시 후 3년간 사업계획서, 추정재무제표, 예상 수지계산서
7. 전문인력, 시설현황 및 영업현황을 기재한 서류
8. 임원의 이력서 및 경력증명서</td></tr>
</table>

전자금융업 합병(양수·양도) 예비인가신청서				
신청인	회 사 명			
	주 소			
	대 표 자	(☎)	작성책임자	(☎)
합 병 대상회사	회 사 명			
	주 소			
	납입자본금			
	총 자 산			
	업 종			
합 병 방 법				
합 병 목 적				

「전자금융거래법」 제45조 및 동법 시행령 제25조에 의한 합병 예비인가를 위와 같이 신청합니다.

년 월 일

신청인 : 서명 또는 인

금융위원회 위원장 귀하

※ 첨부서류

1. 합병으로 존속될 전자금융업자 또는 합병으로 설립될 전자금융업자의 정관(안)
2. 주주총회 의사록
3. 합병계약서 또는 예약서 사본
4. 주주구성 및 경영지배구조 계획
5. 인력 및 조직체계
6. 이해관계인의 권익보호 계획
7. 합병회계년도를 포함한 3년간의 수지예상
8. 최근 사업연도의 재산목록, 재무제표
   (외부감사의 반기결산을 받은 경우 반기포함)

전자금융업 폐지(해산) 예비인가 신청서			
① 상호			
② 본점 소재지		연 락 처	전화: 팩스:
③ 대표자		주민등록번호	
④ 자본금	수권자본금 : 억원 납입자본금 : 억원		

「전자금융거래법」 제45조 및 동법 시행령 제25조에 의한 전자금융업 폐지(해산) 예비인가를 위와 같이 신청합니다.

년 월 일

신청인 : 서명 또는 인

금융위원회 위원장 귀하

※ 첨부서류

1. 정관
2. 법인의 등기부 등본
3. 이사회의사록 사본
4. 해산 및 청산절차에 관한 일정
5. 주주 및 임원명부
6. 최근 사업연도 재무제표와 그 부속서류
7. 회사(법인)의 재산목록 및 자산·부채 처리 계획
8. 채권자 및 이해관계자 보호절차 이행 계획

<별지 제4호 서식>

<table>
<tr><td colspan="4">전자금융업 영위 허가 신청서</td></tr>
<tr><td>① 상호</td><td colspan="3"></td></tr>
<tr><td>② 본점 소재지</td><td></td><td>연 락 처</td><td>전화:
팩스:</td></tr>
<tr><td>③ 대표자</td><td></td><td>주민등록번호</td><td></td></tr>
<tr><td>④ 자본금</td><td colspan="3">수권자본금 : 억원
납입자본금 : 억원</td></tr>
<tr><td>⑤ 주요출자자의 성명 또는 명칭과 지분율</td><td colspan="3"></td></tr>
<tr><td>⑥ 영위하고자 하는 전자금융업</td><td colspan="3"></td></tr>
<tr><td>⑦ 전자금융업 이외 사업을 영위하고 있는 경우 당해 사업의 내용</td><td colspan="3"></td></tr>
<tr><td colspan="4">「전자금융거래법」 제33조 및 동법 시행령 제20조에 의한 전자금융업 영위 허가를 위와 같이 신청합니다.

년 월 일

신청인 : 서명 또는 인

금융위원회 위원장 귀하</td></tr>
<tr><td colspan="4">※ 첨부서류

1. 정관
2. 법인의 등기부 등본
3. 자본금 납입 증명서류
4. 재무제표와 그 부속서류
5. 주주구성
6. 업무개시 후 3년간 사업계획서, 추정재무제표, 예상 수지계산서
7. 전문인력, 시설현황 및 영업현황을 기재한 서류
8. 임원의 이력서 및 경력증명서</td></tr>
</table>

전자금융업 합병(양수·양도) 인가신청서

신청인	회 사 명			
	주 소			
	대 표 자	(☎)	작성책임자	(☎)
합 병 대상회사	회 사 명			
	주 소			
	납입자본금			
	총 자 산			
	업 종			
합 병 방 법				
합 병 목 적				

「전자금융거래법」 제45조에 의한 합병 인가를 위와 같이 신청합니다.

년 월 일

신청인 : 서명 또는 인

금융위원회 위원장 귀하

※첨부서류

1. 합병으로 존속될 전자금융업자 또는 합병으로 설립될 전자금융업자의 정관(안)
2. 주주총회 의사록
3. 합병계약서 또는 예약서 사본
4. 주주구성 및 경영지배구조 계획
5. 인력 및 조직체계
6. 이해관계인의 권익보호 계획
7. 합병회계년도를 포함한 3년간의 수지예상
8. 최근 사업연도의 재산목록, 재무제표
   (외부감사의 반기결산을 받은 경우 반기포함)

전자금융업 폐지(해산) 인가 신청서			
① 상호			
② 본점 소재지		연 락 처	전화: 팩스:
③ 대표자		주민등록번호	
④ 자본금	수권자본금 : 억원 납입자본금 : 억원		

「전자금융거래법」 제45조, 동법 시행령 제25조에 의한 전자금융업 폐지(해산) 인가를 위와 같이 신청합니다.

년 월 일

신청인 : 서명 또는 인

금융위원회 위원장 귀하

※ 첨부서류

1. 정관
2. 법인의 등기부 등본
3. 이사회의사록 사본
4. 해산 및 청산절차에 관한 일정
5. 주주 및 임원명부
6. 최근 사업연도 재무제표와 그 부속서류
7. 회사(법인)의 재산목록 및 자산·부채 처리 계획
8. 채권자 및 이해관계자 보호절차 이행 계획

<별지 제5호 서식>

<table>
<tr><td colspan="4">전자금융업 등록 신청서</td></tr>
<tr><td>① 상호</td><td colspan="3"></td></tr>
<tr><td>② 본점 소재지</td><td></td><td>연 락 처</td><td>전화:
팩스:</td></tr>
<tr><td>③ 대표자</td><td></td><td>주민등록번호</td><td></td></tr>
<tr><td>④ 자본금(기본재산)</td><td colspan="3">수권자본금 :　　억원
납입자본금 :　　억원</td></tr>
<tr><td>⑤ 출자자의 성명 또는 명칭과 지분율</td><td colspan="3">※ 의결권 있는 발행주식총수의 100분의 1 이하의 주식을 소유하는 자는 기재 불요</td></tr>
<tr><td>⑥ 영위하고자 하는 전자금융업</td><td colspan="3"></td></tr>
<tr><td colspan="4">「전자금융거래법」 제33조 및 동법 시행령 제20조에 의한 전자금융업 등록을 위와 같이 신청합니다.

년　　월　　일

신청인 :　　서명 또는 인

금융위원회 위원장 귀하</td></tr>
<tr><td colspan="4">※ 첨부서류

1. 정관
2. 법인의 등기부 등본
3. 자본금 납입 증명서류
4. 재무제표와 그 부속서류
5. 업무개시 후 3년간 사업계획서, 추정재무제표, 예상 수지계산서
6. 전문인력, 시설현황을 기재한 서류
7. 임원의 이력서 및 경력증명서</td></tr>
</table>

<별지 제6호 서식>

<table>
<tr><td colspan="4">전자금융업 등록말소 신청서</td></tr>
<tr><td>① 상호</td><td colspan="3"></td></tr>
<tr><td>② 본점 소재지</td><td></td><td>연 락 처</td><td>전화:
팩스:</td></tr>
<tr><td>③ 대표자</td><td></td><td>주민등록번호</td><td></td></tr>
<tr><td>④ 등록말소 전자금융업</td><td colspan="3"></td></tr>
<tr><td colspan="4">「전자금융거래법」 제34조 및 동법 시행령 제21조에 의한 전자금융업 등록말소를 위와 같이 신청합니다.

년 월 일

신청인 : 서명 또는 인

금융위원회 위원장 귀하</td></tr>
<tr><td colspan="4">※ 첨부서류

1. 등록말소 사유(구체적으로 명기, 별지사용 가능)
2. 등록말소에 따른 가입자 보호조치 내역(구체적으로 명기, 별지사용 가능)</td></tr>
</table>

전자금융감독규정시행세칙

[시행 2016.11.11] [세칙 제9999호, 2016.11.10, 일부개정]

제1장 총칙

제1조(목적) 이 세칙은 「전자금융거래법」(이하 “ 법 ” 이라 한다) 및 동법 시행령(이하 “ 시행령 ” 이라 한다)과 「전자금융감독규정」(이하 “ 규정 ” 이라 한다)에서 금융감독원장(이하 “ 감독원장 ” 이라 한다)에게 위임한 사항과 그 시행에 필요한 사항을 규정함을 목적으로 한다.

[전문개정 2012.05.24]

제2조(정의) 이 세칙에서 별도로 정하지 아니한 용어는 법、시행령、규정에서 정하는 바에 따른다.

[전문개정 2012.05.24]

제2장 망분리 적용 예외 · 자체 보안성심의 기준 등

제2조의2 (망분리 적용 예외) ① 규정 제15조제1항제3호에서 금융감독원장의 확인을 받은 경우란 내부 업무용시스템을(규정 제12조의 중요단말기는 제외한다) 업무상 필수적으로 특정 외부기관과 연결해야 하는 경우를 말한다(다만, 이 경우 필요한 서비스번호(port)에 한하여 특정 외부기관과 연결할 수 있다).

② 규정 제15조제1항제5호에서 금융감독원장이 인정하는 경우란 다음 각 호와 같다.

1. 「금융회사의 정보처리 업무 위탁에 관한 규정」에 따라 정보처리 업무를 국외 소재 전산센터에 위탁하여 처리하는 경우(다만, 해당 국외 소재 전산센터에 대해서는 물리적 방식 외의 방법으로 망을 분리하여야 하며, 이 경우에도 국내 소재 전산센터 및 정보처리시스템 등은 물리적으로 망을 분리하여야 한다)
2. 업무상 외부통신망과 연결이 불가피한 다음의 정보처리시스템(다만, 필요한 서비스번호(port)에 한하여 연결할 수 있다)

   가. 전자금융업무의 처리를 위하여 특정 외부기관과 데이터를 송수신하는 정보처리시스템

   나. DMZ구간 내 정보처리시스템과 실시간으로 데이터를 송수신하는 내부통신망의 정보처리시스템

다. 다른 계열사(「금융회사의 정보처리 업무 위탁에 관한 규정」 제2조 제3항의 "계열사"를 말한다)와 공동으로 사용하는 정보처리시스템

3. 규정 제23조의 비상대책에 따라 원격 접속이 필요한 경우

4. 전산실 내에 위치한 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기와 외부통신망과의 연결 구간, 규정 제15조제1항제3호의 내부 업무용 시스템과의 연결 구간을 각각 차단한 경우<신설 2016.5.12>

③ 제1항 및 제2항의 규정은 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 <별표 7>에서 정한 망분리 대체 정보보호통제를 적용하고 정보보호위원회가 승인한 경우에 한하여 적용한다.

[본조신설 2015.9.17]

제2조의3 (비중요 정보처리시스템의 보고) 규정 제14조의2 제3항에 따라 감독원장이 정하는 양식은 별지 제6호 서식에 따른다.

[본조신설 2016.11.10]

제2조의4 (법인 이용자 정보의 사용에 대한 동의) 규정 제13조 제1항 제10호에 따라 동의를 얻는 경우 다음 각 호의 사항을 정보주체에게 사전에 알려야 한다.

1. 테스트의 목적 및 기간

2. 사용되는 이용자 정보의 항목

3. 테스트 기간 중 정보유출 방지를 위한 통제 계획

4. 테스트 종료 후 테스트에 사용된 이용자 정보의 파기 계획

[본조신설 2016.11.10]

제3조(자체 보안성심의 기준 등) ① 규정 제36조제1항에 따른 금융감독원장이 정하는 기준과 절차란 다음 각 호를 말한다.

1. 정보통신망을 이용하여 신규전자금융업무를 수행하는 경우 <별표 1>의 기준에 따라 보안성심의를 실시한 후 정보보호최고책임자의 승인을 받을 것

2. 공동으로 전자금융거래 관련 표준을 제정하는 경우 <별표 1의2>의 기준에 따라 보안성심의를 실시할 것(다만, 이 경우 특정 금융회사 또는 전자금융업자가 다른 금융회사등을 대표하여 규정 제36조제2항에 따른 자체 보안성심의 결과보고서를 제출할 수 있음).<개정 2014.3.31, 2016.7.27>

② 금융회사 또는 전자금융업자가 규정 제36조제2항에 따라 제출하는 자체 보안성심의 결과보고서의 양식은 제1항제1호의 경우 별지 제3호 서식에, 제1항제2호의 경우 별지 제4호 서식에 각각 따른다.[전문개정 2012.05.24.]<개정2014.3.31, 2016.7.27>

③ 금융회사 또는 전자금융업자는 제1항에 따른 자체 보안성심의를 수행함에 있어 필요한 경우 규정 제37조의4제1항의 침해사고대응기관, 「정보통신기반보호법」 제16조제1항의 정보공유·분석센터 등 외부기관에 보안대책의 적정성 여부 등에 대한 검토를 의뢰할 수 있다.<신설 2014.3.31>

④ 규정 제36조 제2항 단서에서 "금융감독원장이 인정하는 기준"이란 다음 각 호에서 정하는 요건을 충족하는 것을 말한다.<신설 2016.5.12>

1. 전자금융업자 : 법 제28조에 따라 금융위원회로부터 허가를 받았거나 금융위원회에 등록한 날 및 전자금융업무를 신규로 수행한 날로부터 1년이 경과하였을 것.
2. 금융회사 : 전자금융업무를 신규로 수행한 날로부터 1년이 경과하였을 것

[전문개정 2015.9.17]

제4조 삭제 <2015.9.17>

제5조 삭제 <2015.9.17>

제6조 삭제 <2015.9.17>

제7조 삭제 <2015.9.17>

제7조의2(전자금융기반시설의 취약점 분석·평가의 내용) 규정 제37조의2제3항에 따라 감독원장이 정하는 취약점 분석·평가의 내용는 별표 3과 같다. <신설 2014.3.31>

제7조의3(정보보호최고책임자의 업무) 규정 제37조의5에 따라 감독원장이 정하는 정보보안 점검항목은 별표 3 - 2와 같다. <신설 2015.4.8>

제8조(약관의 제정 또는 변경) 규정 제41조제1항제3호에 따른 감독원장이 정하는 약관의 제정 또는 변경이란 다음 각 호의 어느 하나를 말한다.

1. 법령의 개정 또는 금융위원회의 명령에 따른 약관의 변경
2. 이용자의 권익이나 의무사항을 제외한 사항으로서 단순히 업무편의를 위한 약관의 변경
3. 사업자단체의 표준약관을 원용하는 약관의 제정 또는 변경

[전문개정 2012.05.24]

제8조의2(국외에서 주로 영업하는 국외 사이버몰의 판단기준) 규정 제50조의2제3항에 따라 감독원장은 국외에서 주로 영업하는 국외 사이버몰을 판단하는데 있어 다음 각 호의 사항 등을 고려한다. <신설 2014.3.31>

1. 사이버몰 운용자의 사무소, 인적·물적 시설의 소재지
2. 사이버몰에서 이루어지는 상거래 대상 국가의 수
3. 사이버몰에 대한 국외 감독당국, 규제기관의 감독·규제여부
4. 사이버몰에서 체결된 전자상거래 중 국내에 소재한 소비자와 사업자간 거래의 비중
5. 규정 제50조의2제2항에 따른 제한을 회피하기 위한 사이버몰 여부

제8조의3(거래금액 기준 초과시 신고 등) ①법 제30조제3항제1호에 해당하는 전자금융업자는 분기별 거래 총액(결제대행금액, 결제대금예치금액 또는 전자고지결제금액)이 규정 제42조의2제1항에 따른 거래금액 기준을 초과한 경우 해당 분기 종료 후 45일 이내에 별지 제5호 서식에 따라 감독원장에게 초과 내역 및 자본금 증액 계획을 신고하여야 한다.

②제1항에 따른 신고를 마친 자는 법 제30조제4항에 따른 자본금 요건을 갖춘 후, 신고한 때부터 6개월 이내에 자본금 납입 증명서류 등 관련 서류를 감독원장에게 제출하여야 한다.

[본조신설 2016.7.27]

제3장 정보기술부문 실태평가 등

제9조(정보기술부문 실태평가 방법 등) ① 규정 제58조에 따른 정보기술부문 실태평가는 검사기준일 현재 평가대상기관의 정보기술부문 실태를 IT감사, IT경영, 시스템 개발、도입、유지보수, IT서비스 제공 및 지원, IT보안 및 정보보호의 부문별로 구분 평가하고 부문별 평가결과를 감안하여 종합평가한다. <개정 2014.3.31>

② 제1항의 규정에 따른 부문별 세부 평가 항목은 별표 4와 같다.<개정 2014.3.31>

③ 규정 제58조제3항의 평가등급별 정의는 별표 5와 같다.<개정 2014.3.31>

[전문개정 2012.05.24]

제9조의2(외부주문등에 대한 기준) ① 규정 제60조제1항제7호에 따라 감독원장이 정하는 보안관리방안은 별표 5 - 2와 같다.

② 규정 제60조제1항제14호에 따라 감독원장이 정하는 중요 점검사항은 별표 5 - 3과 같다.

<신설 2015.4.8>

제10조(업무보고서의 제출) ① 금융회사 또는 전자금융업자는 규정 제62조에 따른 업무보고서를 분기말 현재로 작성하여 매분기 종료 후 45일 이내에 감독원장에게 제출하여야 한다. <개정 2014.3.31>

② 업무보고서 양식 및 기재사항은 별지 제1호서식에 따른다.

[전문개정 2012.05.24]

제11조(경영지도비율 산정기준) 규정 제63조제2항에 따른 경영지도비율의 구체적 산정기준은 별표 6과 같다.

[전문개정 2012.05.24] <개정 2014.3.31>

제4장 보칙

제12조(정보기술부문 사고보고) ① 금융회사 및 전자금융업자는 규정 제73조에 따른 정보기술부문 및 전자금융 사고가 발생한 경우 별지 제2호서식에 따라 즉시 보고하여야 한다. <개정 2014.3.31>

② 제1항에 따른 사고보고는 최초보고, 중간보고 및 종결보고로 구분한다.

1. 최초보고 : 사고를 인지 또는 발견한 즉시 감독원의 전자금융사고 대응시스템(Electronic Financial Accident Response System : EFARS), 서면, 팩시밀리 또는 전화로 보고하되, 전화로 보고한 경우에는 즉시 전자금융사고 대응시스템, 서면 또는 팩시밀리로 보고한다.

<개정 2015.4.8>

2. 중간보고 : 제1호의 즉시보고 후 제3호의 조치완료 시까지 2월 이상 소요될 경우에는 인지·발견일로부터 2월 이내 및 종결 시까지 매 6월마다 제1호의 방법에 따라 보고한다. 다만, 즉시보고 후 조치완료 시까지 2월 미만이 소요될 경우에는 중간보고를 생략할 수 있다.

3. 종결보고 : 피해금액에 대한 배상조치가 완료되거나 사고조치 등이 완료되어 정상적인 업무를 수행하게 된 때 제1호의 방법에 따라 보고한다.

③ 감독원장은 금융회사 및 전자금융업자 정보기술부문의 사고보고 등을 전담할 비상연락 담당자를 회사별로 지정할 수 있다.<개정 2014.3.31, 2015.4.8>

④ 금융회사 및 전자금융업자는 비상연락 담당자가 제3항에 따라 지정되거나 변경된 경우에는 제2항제1호에서 정한 보고방법에 따라 감독원장에게 즉시 보고하여야 한다.<개정 2014.3.31, 2015.4.8>

[전문개정 2012.05.24]

부칙 <제9999호,2012.5.24>

제1조(시행일) 이 세칙은 2012년 5월 29일부터 시행한다.

부칙 <제9999호,2013.2.6>

제1조(시행일) 이 세칙은 2013년 2월 6일부터 시행한다.

제2조(적용례) 제5조제4항의 개정규정은 이 세칙 개정 후 제5조제1항에 따라 위촉된 위원에 대하여 적용한다.

부칙 <제9999호,2015.4.8>

제1조(시행일) 이 세칙은 2015년 4월 16일부터 시행한다.

부칙 <제9999호,2015.9.17>

제1조(시행일) 이 세칙은 2015년 9월 21일부터 시행한다.

부칙 <제9999호,2016.5.12>

제1조(시행일) 이 세칙은 2016년 5월 18일부터 시행한다.

부칙 <제9999호,2016.7.27>

이 세칙은 2016년 7월 29일부터 시행한다.

부칙 <제9999호,2016.11.10>

제1조(시행일) 이 세칙은 2016년 11월 11일부터 시행한다.

<별표 1> 자체 보안성심의 기준 <개정 2015.9.17>

	심의기준
1	거래 당사자 인증
2	거래정보의 기밀성 및 무결성
3	정보처리시스템 보호대책
4	고객 단말기 보호대책
5	정보유출 방지대책
6	이상금융거래 방지대책
7	시스템 가용성 확보 및 비상대책
8	시스템 설치장소에 대한 물리적 접근통제

※ 전자금융업무 유형에 따라 자체적으로 심의기준 추가·수정 가능

<별표 1의2> 자체 보안성 심의 기준 <신설 2016.7.27>

	심의기준
1	컴플라이언스 준수
2	사용자 접근성
3	호환성 지원
4	서비스 품질 보장(안정성)
5	불필요한 기능 제거(간결성)
6	표준화 그룹 체계 관리

※ 공동 표준안의 유형에 따라 자체적으로 심의기준 추가·수정

<별표 2> <삭제 2015.9.17>

<별표 3> 전자금융기반시설의 취약점 분석·평가의 내용

평가 부문	평가 항목
관리적 보안	- 정보보호 정책 - 정보보호 조직 및 인력 - 내부통제 - 정보보호 교육 및 훈련 - 자산관리 - 업무연속성 관리 - 사고관리 - 정보시스템 도입·개발·유지보수
물리적 보안	- 전산설비 보안 - 전산센터 보안
기술적 보안	- 인터넷 전자금융 보안 - 모바일 전자금융 보안 - 접근통제 - 전산자료 보안 - 서버 보안 - 데이터베이스 보안 - 웹 서비스 보안 - 단말기 보안 - 네트워크 보안 - 정보보호시스템 보안

<별표 3-2> 정보보안 점검항목 <신설 2015.4.8>

	점검항목
전산실	상시출입자외 출입자에 대한 책임자 승인 및 출입자관리기록부 기록·보관 여부
	무인감시카메라 또는 출입자동기록시스템 등의 정상 작동 여부
단말기	업무담당자 이외의 단말기 무단조작 금지 조치 여부
	정보처리시스템 접속 단말기의 정당한 사용자인가를 확인할 수 있는 기록 유지 여부
	중요 단말기의 외부 반출 금지 여부
	중요 단말기의 인터넷 접속 금지 여부
	중요 단말기의 그룹웨어 접속 금지 여부
	단말기에서 보조기억매체 및 휴대용 전산장비 접근 통제 여부
전산자료	개인별 사용자계정과 비밀번호 부여 여부
	사용자계정과 비밀번호 등록·변경·폐기의 체계적 관리 여부
	이용자 정보 조회·출력 통제 여부
	테스트시 이용자 정보 사용 금지 및 불가피한 경우 이용자정보를 변환하여 사용하고 테스트 종료 즉시 삭제 여부
	단말기에 이용자 정보 등 주요정보 보관을 금지하고 불가피한 경우 책임자의 승인을 받고 있는지 여부
	단말기 공유 금지 여부
	전산자료 및 전산장비의 반출·반입 통제 여부
	사용자 인사 조치시 지체 없이 해당 사용자계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템 접근을 통제하고 있는지 여부
정보처리시스템	내부통신망의 비인가 전산장비·무선통신 접속 통제 여부
해킹 등 방지대책	해킹 등을 방지하기 위한 정보보호시스템의 정상 작동 여부
	정보보호시스템에 최소한의 서비스번호와 기능만을 적용하고 있는지 여부
	정보보호시스템에 업무목적이외 기능 및 프로그램 제거 여부
	정보보호시스템의 원격관리 금지 여부
	시스템프로그램 등 긴급하고 중요한 보정사항에 대한 즉시 보정작업 실시 여부
	무선통신망 이용 업무에 대한 승인 및 사전 지정 여부
악성코드	악성코드 검색 및 치료프로그램의 최신상태 유지 여부
	중요 단말기의 악성코드 감염여부를 매일 점검하고 있는지 여부
공개용 웹서버	사용자계정에 아이디·비밀번호 이외 추가 인증수단 적용 여부
	DMZ구간 내 이용자 정보 등 주요정보를 저장, 관리하지 않는지 여부
내부사용자 비밀번호	접근자 비밀번호 설정·운영 여부
	비밀번호 보관시 암호화 여부
이용자 비밀번호 관리	정보처리시스템 및 전산자료에 보관하고 있는 이용자 비밀번호 암호화 보관 여부
이용자 유의사항	비밀번호 유출위험 및 관리에 관한 사항의 공지 여부
	제공하고 있는 이용자보호 제도에 관한 사항의 공지 여부
	해킹·피싱 등 전자적 침해방지에 관한 사항의 공지 여부
전자금융 사고보고	전자적 침해행위에 대한 보고 및 조치 여부

<별표 4> 정보기술부문 실태평가 부문별 평가항목

평가 부문	평가 항목
1. IT 감사	- IT감사조직 및 요원 - IT감사 실시 내용 - IT감사 사후관리 및 기타
2. IT 경영	- IT부서 조직 및 요원 - IT관련 내규(규정, 지침, 절차, 편람 등) - IT계획 및 방향제시 - 비상계획 - 경영정보시스템(MIS) 등 - IT 인력 및 예산의 적정성
3. 시스템 개발, 도입 및 유지보수	- 시스템 개발, 도입 및 유지보수 관련 조직 및 요원 - 시스템 개발, 도입 및 유지보수 관련 내규(규정, 지침, 절차 등) - 시스템 개발, 도입, 유지보수 현황 - 내부통제용 시스템, 시스템통합 등
4. IT서비스 제공 및 지원	- IT서비스 제공/지원 관련 조직 및 요원 - IT서비스 제공/지원 관련 내규(규정, 지침, 절차 등) - 시설 및 장비 - 운영통제 - 통신망 - 최종사용자 컴퓨팅 - 전자금융거래 등
5. IT보안 및 정보보호	- IT보안 절차 - IT보안 리스크 평가 - IT보안 및 정보보호 전략 - IT보안 통제 구현 - IT보안 모니터링

<별표 5> 평가등급별 정의

가. IT 감사 부문에 대한 평가등급별 정의

평가등급	정 의
1 등급 (우수:Strong)	감사업무가 독립적으로 정확하게 이루어지고 감사내용 및 결과처리가 적절하며 특별한 문제점이 없어 감독상 주의를 기울일 필요가 거의 없음
2 등급 (양호:Satisfactory)	감사업무가 독립적으로 비교적 정확하게 이루어지나 감사내용 및 결과처리에 경미한 문제점이 있어 감독상 최소의 주의를 요함
3 등급 (보통:Less than satisfactory)	감사활동의 독립성과 감사내용 및 감사결과처리가 다소 미흡하여 개선이 요망되며 업무의 정확성 및 적시성이 부족하여 적정수준의 감독이 요구됨
4 등급 (취약:Deficient)	감사활동의 독립성과 감사내용 및 감사결과처리가 현저하게 미흡하고 업무수행이 부적절하여 적절한 통제 및 시정이 요구됨
5 등급 (위험:Critically deficient)	감사활동 및 감사결과처리가 크게 미흡하여 감사업무 전반에 대한 신뢰성이 없음

나. IT 경영 부문에 대한 평가등급별 정의

평가등급	정 의
1 등급 (우수:Strong)	경영전략 및 비상대책이 우수하고 이를 효율적으로 추진할 수 있는 조직과 경영정보시스템 등이 적절히 구축되어 정보기술부문의 취약점이나 문제점에 대해 효과적으로 대응할 수 있음
2 등급 (양호:Satisfactory)	경영전략 및 비상대책이 양호하고 이를 추진하는 조직과 경영정보시스템 등이 비교적 효율적으로 구축되어 정보기술부문의 취약점이나 문제점에 대해 적절히 대응할 수 있음
3 등급 (보통:Less than satisfactory)	경영전략 및 비상대책이 다소 미흡하고 이를 추진하는 조직과 경영정보시스템 등에 대한 개선이 요망되며 정보기술부문의 취약점이나 문제점에 대한 대응이 약간 부족함
4 등급 (취약:Deficient)	경영전략 및 비상대책 및 이를 추진하는 조직과 경영정보시스템 등이 전반적으로 부족하여 이에 대한 개선이 요망됨
5 등급 (위험:Critically deficient)	경영전략 및 비상대책 및 이를 추진하는 조직과 경영정보시스템 등이 전반적으로 크게 부족하여 긴급대책이 요구됨

다. 시스템 개발, 도입 및 유지보수 부문에 대한 평가등급별 정의

평가등급	정 의
1 등급 (우수:Strong)	시스템이 효율적으로 구축되고 사용목적에 부합하며 시스템 및 프로그램의 변경과정에 대한 효과적인 통제제도 등이 수립되어 있음
2 등급 (양호:Satisfactory)	시스템이 비교적 효율적으로 구축되고 시스템 및 프로그램의 변경과정에 대한 통제제도 등이 건전하나 사용목적에 다소 부합하지 않고 경미한 문제점이 발견됨
3 등급 (보통:Less than satisfactory)	시스템에 일부 결함이 발견되고 시스템 및 프로그램의 변경과정에 대한 통제제도 등이 다소 미흡하며 사용목적에 부합하기 위해서는 개선이 요망됨
4 등급 (취약:Deficient)	시스템이 심각한 취약점을 내포하고 사용목적에 부합하지 않으며 시스템 및 프로그램의 변경과정에 대한 통제제도가 미흡하여 금융회사의 건전성에 손해를 초래할 우려가 있음
5 등급 (위험:Critically deficient)	시스템과 시스템 및 프로그램의 변경과정에 대한 통제제도가 극히 취약하며 중대한 결함을 갖고 있고 사용목적을 전혀 고려하지 못하여 금융회사의 존립이 위태로움

라. IT 서비스 제공 및 지원 부문에 대한 평가등급별 정의

평가등급	정 의
1 등급 (우수:Strong)	IT 서비스 부문이 효율적이고 일상적인 운영상황에 특별한 문제점이 없음
2 등급 (양호:Satisfactory)	IT 서비스 부문이 비교적 효율적이고 일상적인 운영상황에 경미한 문제점이 있으나 정상적인 운영과정에서 적절히 대응할 수 있음
3 등급 (보통:Less than satisfactory)	IT 서비스 부문의 효율성이 다소 미흡하고 일상적인 운영상의 취약점이나 문제점에 대한 대응이 부족하여 개선이 요구됨
4 등급 (취약:Deficient)	IT 서비스 부문의 효율성이 취약하고 일상적인 운영상의 취약점이나 문제점이 현저하게 드러나 동 부문의 안전성 및 건전성에 위험을 초래할 가능성이 큼
5 등급 (위험:Critically deficient)	IT 서비스 부문이 비효율적이고 일상적인 운영상의 취약점이나 문제점이 크게 심각하여 동 부문의 안전성 및 건전성 확보가 위태로움

마. IT보안 및 정보보호 부문에 대한 평가등급별 정의

평가등급	정 의
1 등급 (우수Strong)	IT보안 및 정보보호가 우수하고 이를 효율적으로 추진할 수 있는 조직과 정보보호시스템 등이 적절히 구축되어 보안부문의 취약점이나 문제점에 대해 효과적으로 대응할 수 있음
2 등급 (양호Satisfactory)	IT보안 및 정보보호가 양호하고 이를 추진하는 조직과 정보보호시스템 등이 비교적 효율적으로 구축되어 보안부문의 취약점이나 문제점에 대해 적절히 대응할 수 있음
3 등급 (보통Less than satisfactory)	IT보안 및 정보보호가 다소 미흡하고 이를 추진하는 조직과 정보보호시스템 등에 대한 개선이 요망되며 보안부문의 취약점이나 문제점에 대한 대응이 약간 부족함
4 등급 (취약Deficient)	IT보안 및 정보보호를 추진하는 조직과 이를 지원하는 정보보호시스템 등이 전반적으로 부족하여 이에 대한 개선이 요망됨
5 등급 (위험Critically deficient)	IT보안 및 정보보호를 추진하는 조직과 이를 추진하는 정보보호시스템 등이 전반적으로 크게 부족하여 긴급대책이 요구됨

바. 종합평가등급의 정의

평가등급	정 의
1 등급 (우수:Strong)	- 전자금융업무와 정보기술부문 전반에 걸쳐 운영상태가 건전하며 정상적인 감독상의 주의만 요구됨 - 약간의 적출사항은 있으나 그 정도가 경미하여 통상적인 방법으로 해결이 가능함
2 등급 (양호:Satisfactory)	- 전자금융업무와 정보기술부문 전반에 걸쳐 운영상태가 근본적으로 건전하나, 약간의 취약점을 내포하고 있으며 필요시 제한된 범위내의 감독조치가 요구됨
3 등급 (보통:Less than satisfactory)	- 전자금융업무와 정보기술부문 전반에 걸쳐 즉각적인 시정을 요하는 다양한 취약점을 내포하고 있어 이를 시정하기 위해 통상적인 수준 이상의 감독상의 주의가 요구됨
4 등급 (취약:Deficient)	- 전자금융업무와 정보기술부문 전반에 걸쳐 즉각적인 시정을 요하는 다양한 취약점을 내포하고 있어 감독당국의 면밀한 주의 및 문제점을 시정하기위한 조치가 필요함 - 전자금융업무와 정보기술부문 전반에 걸친 취약점이 심각하여 장래 동 업무처리 자체가 위험하게 될 가능성이 있으므로 감독당국의 면밀한 주의 및 문제점을 시정하기 위한 조치가 필요함
5 등급 (위험:Critically deficient)	- 전자금융업무와 정보기술부문 전반에 걸쳐 취약점이 매우 심각하여 정상적인 업무처리를 할 수 없는 상황임

<별표 5-2> 보안관리방안 <신설 2015.4.8> <개정 2016.11.10>

단계	세부사항
입찰	ㅇ 입찰 공고 이전에 투입이 예상되는 자료·장비 가운데 보안관리가 필요한 사항에 대하여 금융회사 또는 전자금융업자의 내부관리기준과 관련 법규를 검토하고 필요한 보안요구 사항을 마련 ㅇ 입찰 공고시에 금융회사 또는 전자금융업자가 자체 작성한 중요정보, 부정당업자 제재조치, 기밀유지 의무 및 위반시 불이익 등을 정확히 공지 ㅇ 제안서 평가요소에 자료·장비·네트워크 보안대책 및 중요정보 관리 방안 등 보안관리 계획의 평가항목 및 배점기준 마련 ㅇ 업체가 입찰제안서에 제시한 용역사업 전반에 대한 보안관리 계획이 타당한지를 검토하여 사업자 선정시에 이를 반영
계약	ㅇ 계약서 작성 초기 단계부터 정보보안사항 포함여부에 대한 검토 실시 ㅇ 용역사업에 투입되는 자료·장비 등에 대해 대외보안이 필요한 경우 보안의 범위·책임을 명확히 하기 위해 사업수행 계약서와 별도로 비밀유지계약서 작성 ㅇ 비밀유지계약서에는 비밀정보의 범위, 보안준수 사항, 위반시 손해배상 책임, 지적재산권 문제, 자료의 반환 등이 포함되도록 명시 ㅇ 용역사업 참여인원은 금융회사 또는 전자금융업자의 사전 동의 없이 용역업체가 임의로 교체할 수 없도록 명시 ㅇ 금융회사 또는 전자금융업자의 요구사항을 사업자에게 명확히 전달키 위하여 작성하는 과업지시서·계약서(입찰 공고 포함)에 인원·장비·자료 등에 대한 보안조치 사항과 정보유출 및 부정당업자에 대한 손해배상 내용 등을 정확히 기술 ㅇ 용역업체가 사업에 대한 하도급 계약을 체결할 경우 원래 사업계약 수준의 비밀 유지 조항을 포함토록 조치 ㅇ 규정 제7조 각호에 규정한 사항의 준수를 위하여 외부주문업체 등의 협조가 요구되는 사항
수행	[인력] ㅇ 용역사업 참여인원에 대해서는 '정보 유출' 방지 조항 및 개인의 자필 서명이 들어간 보안서약서 징구 ㅇ 용역사업 수행前 참여인원에 대해 법적 또는 금융회사 또는 전자금융업자의 규정에 따른 비밀유지 의무 준수 및 위반시 처벌내용 등에 대한 보안교육 실시 * 유출 금지 대상정보 및 정보 유출시 부정당업자 제재조치 등에 대한 교육 병행 ㅇ 금융회사 또는 전자금융업자는 사업 수행 중 업체 인력에 대한 보안점검 실시, '유출금지 대상정보' 외부 유출여부 확인 [자료] ㅇ 계약서 등에 명시한 중요정보를 업체에 제공할 경우 자료관리 대장을 작성, 인계자·인수자가 직접 서명한 후 제공하고 사업완료시 관련자료 회수 ㅇ 용역사업 관련자료 및 사업과정에서 생산된 모든 산출물은 금융회사 또는 전자금융업자의 파일서버에 저장하거나 금융회사 또는 전자금융업자가 지정한 PC에 저장관리 ㅇ 용역사업 관련 자료는 인터넷 웹하드·P2P 등 인터넷 자료공유사이트 및 개인메일함에 저장을 금지하고 금융회사 또는 전자금융업자와 용역업체간 전자우편을 이용해 전송이 필요한 경우에는 자체 전자우편을 이용하고, 첨부자료 중 중요정보 포함자료는 암호화 후 수발신

	ㅇ 금융회사 또는 전자금융업자가 제공한 사무실에서 업체가 용역사업을 수행할 경우, 유출금지 대상 정보가 포함된 자료는 매일 퇴근시 시건장치가 된 보관함에 보관 ㅇ 용역사업 수행으로 생산되는 산출물 및 기록은 금융회사 또는 전자금융업자가 인가하지 않은 비인가자에게 제공·대여·열람을 금지 [사무실·장비] ㅇ 용역사업 수행장소는 금융회사 또는 전자금융업자 전산실 등 중요시설과 분리하고 CCTV·시건장치 등 비인가자의 출입통제 대책을 마련 ㅇ 용역업무를 수행하는 공간에 대한 보안점검을 정기적으로 실시 ㅇ 용역직원이 노트북 등 관련 장비를 외부에서 반입하여 내부망에 접속시 악성코드 감염여부 및 반출시마다 자료 무단반출 여부 확인 ㅇ 인가받지 않은 USB메모리 등의 휴대용 저장매체 사용을 금지하며 산출물 저장을 위하여 휴대용 저장매체가 필요한 경우 금융회사 또는 전자금융업자의 승인하에 사용 [내·외부망 접근시] ㅇ 금융회사 또는 전자금융업자는 개발시스템과 운영시스템을 분리하고, 용역업체는 업무상 필요한 서버에만 제한적 접근 허용 ㅇ 용역사업 수행시 금융회사 또는 전자금융업자 전산망 이용이 필요한 경우 -사업 참여인원에 대한 사용자계정(ID)은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근 권한을 차등 부여하되 허용되지 않은 금융회사 또는 전자금융업자의 내부문서 접근 금지 -계정별로 부여된 접속권한은 불필요시 즉시 해지하거나 계정을 폐기 -참여인원에게 부여한 계정은 별도로 기록 관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력 확인 -금융회사 또는 전자금융업자는 내부서버 및 네트워크 장비에 대한 접근기록 이상 여부를 정기 점검 ㅇ 용역업체에서 사용하는 PC는 인터넷 연결을 금지하되, 사업수행상 연결이 필요한 경우에는 금융회사 또는 전자금융업자의 보안통제하에 제한적 허용 ㅇ 용역업체 사용 전산망에서 P2P, 웹하드 등 인터넷 자료공유사이트로의 접속을 원천 차단
완료	ㅇ 사업 완료 후 생산되는 최종 산출물 등 대외보안이 요구되는 자료는 대외비 이상으로 작성관리하고 불필요한 자료는 삭제 및 폐기 ㅇ 용역업체에 제공한 자료, 장비와 중간·최종 산출물 등 용역과 관련된 제반자료는 전량 회수하고 업체에 복사본 등 별도 보관 금지 ㅇ 용역사업 완료 후 업체 소유 PC·서버의 하드디스크·휴대용 저장매체 등 전자기록 저장매체는 복원이 불가능한 방법으로 완전 삭제 후 반출 ㅇ 용역사업 관련자료 회수 및 삭제조치 후 업체에게 복사본 등 용역사업관련 자료를 보유하고 있지 않다는 대표자 명의의 확약서 징구

<별표 5-3> 중요 점검사항 <신설 2015.4.16, 개정 2015.9.17>

	점검 항목
1	이용자 정보의 조회·출력에 대한 통제 및 이용자 정보 조회시 사용자, 사용일시, 변경·조회내역, 접속방법 기록·관리
2	테스트시 이용자 정보 사용금지(부하 테스트 등 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제)
3	운영시스템 접속·사용 통제
4	내부통신망의 비인가 전산장비·무선통신 접속 통제(정보처리시스템을 이용한 통제장치 마련시 통제 장치에 대한 일일점검으로 대체 가능)
5	전산자료 및 전산장비 반출·반입 통제
6	전산실 등 출입자 관리기록부 기록·보관
7	인터넷(무선통신망 포함) 사용 통제(정보처리시스템을 이용한 통제 장치 마련시 통제장치에 대한 일일점검으로 대체 가능)
8	운영체제 및 악성코드 치료프로그램을 최신으로 유지
9	USB 등 보조기억매체 사용 통제
10	단말기에 이용자 정보 등 중요정보 보관 금지

<별표 6> 경영지도비율 산정기준

1. 자본적정성

$$\text{미상환잔액 대비 자기자본비율} = \frac{\text{자기자본}}{\text{미상환잔액}} \times 100$$

2. 자산건전성

$$\text{총자산 대비 투자위험성이 낮은 자산의 비율} = \frac{\text{투자 위험성이 낮은 자산}}{\text{총자산}} \times 100$$

※ 투자 위험성이 낮은 자산 : 규정 〈별표 6〉 참조

3. 유동성

$$\text{유동성비율} = \frac{\text{유동자산}}{\text{유동부채}} \times 100$$

<별표 7> 망분리 대체 정보보호통제 <신설 2015.9.17>

대책	세부사항
내부망 보안 강화	- 업무망에 반입되는 전산자료 대상으로 악성코드 감염여부 진단·치료 대책 수립
외부망 보안 강화	- 지능형 해킹(APT)차단 대책 수립 - 외부망을 통해 전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링 대책 수립
메일 시스템 보안 강화	- 본문과 첨부파일 포함하여 메일을 통한 악성코드 감염 예방 대책 수립 - 메일을 통한 전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링 대책 수립
단말기 보안 강화	- PC 사용자의 관리자 권한 제거 - 승인된 프로그램만 설치·실행토록 대책 수립 - 단말기 전산 자료 암호화 저장
원격 접속 통제 수립	- 원격접속 기준 및 절차가 포함된 보안정책 수립 - 불법 원격접속을 방지하기 위한 사용자인증, 암호화 등의 보안대책을 수립 - 원격접속은 책임자의 승인을 받은 사전 등록자에 한하여 허용하며 원격접속 관리 기록부를 기록·보관 - 원격에서 접속하는 외부 단말기와 내부 업무용 시스템 구간의 암호화 통신 - 원격접속 사용자는 아이디·비밀번호 이외에 추가 인증수단을 적용 - 원격에서 접속하는 외부 단말기의 악성코드 감염 예방 대책 수립·적용 - 원격접속 가능한 내부 업무용 시스템의 접근 통제 수립·적용 - 원격으로 접속하여 수행한 모든 작업 내역 기록하고 매일 이상여부 점검 실시 및 책임자가 확인

<별지 제1호 서식>

- 업무보고서 양식 및 기재사항(엑셀파일 참고) -

<별지 제2호 서식> <개정 2015.4.8>

작 성 자 : (직 위)
전화번호 :

정보기술부문 및 전자금융 사고보고서

문서번호 20 . . .

수 신

참 조

제 목 정보기술부문 및 전자금융 사고보고

전자금융감독규정 제73조에 따라 붙임과 같이 사고를 보고합니다.

붙 임 사고내용 1부. 끝.

○ ○ 금융회사 사장 (인)

<별첨>

정보기술부문 및 전자금융 사고내용

보고형태	□ 최초 □ 중간 □ 완료					
최초 인지	□ 금융회사 □ 고객(민원인) □ 기타: ( )					
사고인지일시						
발생일시 및 지속시간						
발생 장소						
피해자 정보 및 피해금액 (전자금융사기사고 보고에 한함)	피해자 성명		생년월일		피해금액	
사고유형	IT보안사고		정보기술장애		전자금융사기사고	
	□ 전산자료/프로그램조작 □ 정보유출사고 □ 내부망 해킹 □ 시스템 위변조 □ DDoS 공격 □ 원인미정(파악중)		□ 천재지변에 의한 장애 □ 시스템/설비 장애 □ 프로그램 오류 □ 인적 재해 □ 외부요인으로 인한 장애 □ 원인미정(파악중)		□ 피싱/파밍(인터넷) □ 피싱/파밍(모바일) □ 피싱/파밍(텔레뱅킹) □ 전자상거래 위변조 □ 매체위변조 □ 신종 전자금융사기사고 □ 원인미정(파악중)	
사고내용						
사고원인						
파급영향						
처리결과						
대 책						

<선택 입력사항> 금융회사 공격자의 정보 제공

공격 유형	□ DDoS □ 파밍악성코드 □ C&C서버 □ 기타
공격방법	
공격자IP	
공격자 MAC	
Domain정보	
상세내용	

<별지 제3호 서식> 자체 보안성심의 결과보고서 <신설 2015.9.17> <개정 2016.7.27>

작 성 자 :	(직 위)
전화번호 :	

자체 보안성심의 결과보고서(신규 전자금융서비스)

20 . . .

문서번호

수 신

참 조

제 목 자체 보안성심의 결과보고서

전자금융감독규정 제36조에 따라 붙임과 같이 자체 보안성심의 결과보고서를 제출합니다.

붙 임 자체 보안성심의 개요 1부.
자체 보안성심의 결과 1부. 끝.

OO 금융회사 대표이사 (인)

(붙임1)

자체 보안성심의 개요

1. 업무명 :

2. 업무적용일 : 20 년 월 일 완료

3. 업무개요

※ *서비스 목적, 대상 및 주요 내용을 기재*

4. 업무처리 절차

※ *가입절차, 이용절차 등을 기재*

5. 자체 보안성심의 결과

□ 20 년 월 일 완료 ('붙임2. 자체 보안성심의 결과' 참조)

※ *자체 보안성심의 결과(자율양식)를 붙임2로 첨부*

6. 담당자

소 속	직 위	이 름	담당업무	연락처	e-mail

(붙임2)

자체 보안성심의 결과

※ 보안성심의 기준별 심의 결과 및 판단근거 등을 상세하게 기재

<별지 제4호> <신설 2016.7.27>

작 성 자 :	(직위)
전화번호 :	

자체 보안성심의 결과보고서(공동 표준안)

20 . . .

문서번호

수 신

참 조

제 목 자체 보안성심의 결과보고서

전자금융감독규정 제36조에 따라 붙임과 같이 자체 보안성심의 결과보고서를 제출합니다.

붙 임 자체 보안성심의 개요 1부.
자체 보안성심의 결과 1부. 끝.

OO 금융회사 대표이사 (인)

(붙임1)

자체 보안성심의 개요

1. 표준명 :

2. 표준 제정일 : 20 년 월 일 제정

3. 개요

※ *참여 회사, 서비스 목적, 대상 및 주요 내용을 기재*

4. 업무처리 방안

※ *공동 표준안 관리 방안, 각 개별회사에 대한 적용 방안 등을 기재*

5. 자체 보안성심의 결과

□ 20 년 월 일 완료 ('붙임2. 자체 보안성심의 결과' 참조)

※ *자체 보안성심의 결과(자율양식)를 붙임2로 첨부*

6. 표준화 그룹 담당자

회사명[1]	직 위	이 름	담당업무	연락처	e-mail

1) 보안성심의 진행과 관련하여 대표자(또는 회사)가 있다면 회사명 앞에 별도 표기

(붙임2)

자체 보안성심의 결과

※ 보안성심의 기준별 심의 결과 및 판단근거 등을 상세하게 기재

<별지 제5호 서식> <신설 2016.7.27>

전자금융 거래금액 기준 초과 신고서

문서번호 20 . . .

수 신

참 조

제 목 전자금융 거래금액 기준 초과 관련 신고서 제출

전자금융감독규정 제42조의2 제3항 및 동 시행세칙 제8조의3 제1항에 따라 붙임과 같이 전자금융 거래금액 기준을 초과한 사실을 신고합니다.

붙 임 전자금융 거래금액 기준 초과 내역 및 자본금 증액 계획 1부. 끝.

ㅇ ㅇ ㅇ ㅇ 대표이사 (인)

(붙임)

전자금융 거래금액 기준 초과 내역 및 자본금 증액 계획

1. 거래금액 기준 초과 내역

(단위: 원)

	전전기	전기	당기
연도 및 분기[1]	*(예시) 2016년 4분기*	*(예시) 2017년 1분기*	*(예시) 2017년 2분기*
거래금액[2]	*(예시) 2,000,000,000*	*(예시) 4,000,000,000*	*(예시) 5,000,000,000*

[작성요령]

1) 연도 및 분기
- 당기 : 분기 거래총액이 2분기 연속 30억원을 초과한 경우의 두번째 분기
- 전기 : 분기 거래총액이 2분기 연속 30억원을 초과한 최초 분기
- 전전기 : '전기'의 전분기

2) 거래금액
- 전자지급결제대행 : 결제시(신용카드, 계좌이체, 가상계좌, 기타(상품권 등) 포함) 이용자가 지불한 재화나 용역의 가격을 말하며, 분기중 누적금액으로 작성
- 결제대금예치 : 이용자가 결제대금예치 서비스 제공업자와 거래한 총액으로서, 분기중 누적금액으로 작성
- 전자고지결제 : 이용자가 전자고지결제 서비스 제공업자와 거래한 총액으로서, 분기중 누적금액으로 작성

2. 자본금 증액 계획

(단위: 원)

	등록시 자본금[1]	변경 후 자본금[2]	자본금 변경 신고 예정일[2]
자본금	*(예시) 300,000,000*	*(예시) 1,000,000,000*	*(예시) 2017.12.31.*

[작성요령]

1) 전자지급결제대행에 관한 업무 : 3억원 이상
결제대금예치업 : 3억원 이상
전자고지결제업 : 3억원 이상
2) 전자지급결제대행에 관한 업무 : 10억원 이상
결제대금예치업 : 10억원 이상
전자고지결제업 : 5억원 이상

2) 자본금 변경 신고 예정일 : 거래금액이 2분기 연속 30억원을 초과한 시점부터 6월 이내에 금융감독원에 제출해야 함

<별지 제6호 서식> <신설 2016.11.10>

작 성 자 : (직 위)
전화번호 :

비중요 정보처리시스템 지정결과 보고

문서번호 20 . . .

수 신

참 조

제 목 비중요 정보처리시스템 지정결과 보고

전자금융감독규정 **제14조의2 제3항**에 따라 붙임과 같이 비중요 정보처리시스템 지정결과를 제출합니다.

붙 임 비중요 정보처리시스템 지정결과 보고서 1부. 끝.

○ ○ ○ ○ 대표이사 (인)

(붙임)

비중요 정보처리시스템 지정결과 보고서

1. 시스템명 :

2. 업무 개요 :

3. 업무처리 절차

※ 업무 단계별 이용자 및 데이터 흐름 표시

4. 시스템 개요

가. 시스템의 용도

나. 처리 데이터

다. 시스템 이용자

라. 타 시스템과의 연계성

마. 시스템 구성도 및 정보통신망 구성도

5. 정보자산 중요도 평가 기준

6. 비중요 정보처리시스템 지정결과

별첨 : 정보보호위원회 회의록

7. 정보처리 업무위탁 여부

위탁 여부	수탁사	위탁업무 보고 (예정)일*

* 금융회사의 정보처리 업무 위탁에 관한 규정 제7조에 따름

8. 비중요 정보처리시스템 관리 방안

9. 시스템 책임자

소 속	직 위	이 름	담당업무	연락처	e-mail

전자금융거래 기본약관

[시행 2012.9.28] [표준약관 제10028호, 2012.9.28, 전부개정]

제1조(목적) 이 약관은 OO 은행(이하 "은행"이라 한다)과 거래처 사이의 전자금융거래에 관한 기본적인 사항을 정함으로써, 거래의 신속하고 효율적인 처리를 도모하고 거래당사자 상호간의 이해관계를 합리적으로 조정하는 것을 목적으로 한다.

제2조(용어의 정의) 이 약관에서 사용하는 용어의 의미는 다음 각호와 같다.

1. "거래처"라 함은 전자금융거래를 이용하는 고객을 말한다.
2. "전자금융거래"라 함은 은행이 전자적 수단을 통하여 제공하는 조회, 입금·출금, 계좌이체 등을 거래처가 직접 이용하는 거래를 말한다.
3. "전자적 수단"이라 함은 현금자동지급기, 현금자동입·출금기, 컴퓨터, 전화기, 직불카드거래단말기 기타 전자금융거래를 처리하는데 이용되는 전자적 장치를 말한다.
4. "거래지시"라 함은 거래처가 전자금융거래에 관한 계약에 의하여 은행에 개별적인 전자금융거래의 처리를 의뢰하는 것을 말한다.
5. "지급인"이라 함은 전자금융거래에 의하여 자금이 출금되는 계좌(이하 "출금계좌"라 한다)의 명의인을 말한다.
6. "수취인"이라 함은 전자금융거래에 의하여 자금이 입금되는 계좌(이하 "입금계좌"라 한다)의 명의인을 말한다.
7. "계좌이체"라 함은 지급인의 거래지시에 따라 은행이 특정계좌에서 자금을 출금하여 같은 은행 또는 다른 은행의 계좌에 입금하는 것을 말한다.
8. "예약에 의한 계좌이체"라 함은 계좌이체가 장래의 특정일자에 이루어지도록 거래처가 미리 거래지시하고 은행이 이를 해당일자에 처리하는 것을 말한다.
9. "계좌송금"이라 함은 거래처가 현금자동입·출금기를 통하여 자기 또는 타인의 계좌에 자금을 입금하는 것을 말한다.
10. "영업일"이라 함은 통상 은행이 점포에서 정상적인 영업을 하는 날을 말한다.
11. "접근수단"이라 함은 전자금융거래의 방식을 통하여 거래지시를 하는데 필요한 카드, 인증서, 비밀번호, 이용자번호 등을 말한다.

제3조 (적용되는 거래) 이 약관은 은행과 거래처사이에 이루어지는 다음 각호의 전자금융거래에 적용된다.

1. 현금자동지급기, 현금자동입·출금기에 의한 거래
2. 컴퓨터에 의한 거래
3. 전화기에 의한 거래
4. 직불카드단말기에 의한 거래
5. 기타 전자적 수단에 의한 거래

제4조(거래계약의 체결) 거래처가 전자금융거래를 하고자 하는 경우에는 사전에 은행과 별도의 거래계약을 체결하여야 한다. 다만, 다음 각호의 1에 해당하는 경우에는 그러하지 아니하다.

1. 단순조회(예금잔액, 예금입·출금내역 등)
2. 단순히 이용수수료를 납부하고 처리하는 거래
3. 현금자동지급기, 현금자동입·출금기에 의한 거래
4. 기타 은행이 정하는 거래

제5조(이용시간) ① 거래처는 은행이 정한 시간 이내에서 전자금융거래를 이용할 수 있다.

② 이용시간은 은행의 사정에 따라 달라질 수 있으며, 이용시간을 변경하고자 할 경우에는 3영업일전 영업점 및 게시 가능한 전자적 수단을 통하여 게시한다. 다만, 시스템 장애복구, 긴급한 프로그램 보수, 외부요인 등 불가피한 경우에는 예외로 한다.

제6조(계좌이체 한도) 거래처는 은행이 정한 최고한도 및 지정방법에 따라 이체한도를 설정하여야 한다.

제7조(비밀번호 등록) 거래계약을 체결하고 거래처가 거래비밀번호를 전자적 수단으로 직접 등록할 경우에는 계약일 포함 3영업일 이내에 등록하여야 한다.

제8조(거래의 성립) 거래처가 전자금융거래를 하고자 하는 경우에는 다음 각 호의 시기에 거래가 성립한다.

1. 계좌이체의 경우에는 거래처가 입력한 거래지시의 내용을 은행이 확인하고 출금자금(수수료를 포함한다. 이하같다)을 출금계좌원장에 출금기록 한 때
2. 현금출금의 경우에는 거래처가 입력한 거래지시의 내용을 은행이 확인하고 출금자금을 출금계좌원장에 출금기록 한 때
3. 계좌송금의 경우에는 은행이 거래처가 입력한 거래지시의 내용 및 입금자금을 모두 확인한 때
4. 예약에 의한 계좌이체의 경우는 은행이 거래처의 거래지시 내용을 확인한 때. 다만, 이체시점에 자금이 출금계좌에 입금되어 있을 것을 조건으로 한다.

제9조(거래지시의 처리기준) ① 은행은 거래처의 거래지시에 포함된 계좌번호, 비밀번호, 이용자번호 등을 신고된 것과 대조하여 그 일치여부를 확인한 후에 거래지시를 처리한다.

② 은행은 거래처의 거래지시에 따라 출금계좌에서 자금을 인출할 때 예금거래기본약관에 불구하고 통장이나 지급청구서 또는 수표없이 인출한다.

③ 대량계좌이체, 타행계좌이체 등과 같이 거래의 특성상 수취인의 명의를 확인할 수 없는 경우에는 수취인의 계좌번호를 기준으로 하여 거래를 처리한다.
④ 타행계좌이체는 당일 중에 처리한다. 다만 당일 중 처리가 불가능한 경우에는 제20조 제4항에서 정한 바에 따라 처리한다.
⑤ 예약에 의한 계좌이체의 경우 이체시점에 출금계좌의 자금이 거래처가 거래지시한 금액 이상일 때 처리한다.
⑥ 예약에 의한 계좌이체의 경우 이체지정일이 은행 휴무일로 정해질 때에는 익영업일에 거래를 처리한다.

제10조(거래의 제한) ① 다음 각호의 1에 해당하는 경우에는 전자금융거래의 당해 지시에 따른 거래를 제한할 수 있다.
1. 전자금융거래의 처리시점에 출금계좌의 자금이 출금자금에 미달하는 때. 다만, 전자금융거래에 관한 개별약관에 따로 정한 경우에는 그에 따른다.
2. 입금 또는 출금계좌가 해지되었거나 거래중지계좌에 편입되었을 때
3. 이체일에 입금 또는 출금계좌의 잔액증명서가 발급되었을 때
4. 거래처가 설정한 이체한도를 초과하여 계좌이체 거래지시를 할 때
5. 입금계좌를 지정하여 계좌이체를 이용하기로 한 거래처가 지정하지 않은 계좌로 계좌이체 거래지시를 할 때
6. 법적 지급제한 등으로 거래제공이 부적합하다고 은행이 인정했을 때

② 다음 각호의 1에 해당하는 경우에는 해당 전자적 수단을 통한 계좌이체의 전부를 제한할 수 있다.
1. 인증서 유효기간이 만료되었거나 인증서가 취소되었을 때
2. 컴퓨터 또는 전화기로 전자금융거래를 이용하는 거래처가 6개월이상 계좌이체 이용실적이 없을 때

③ 은행이 제1항 및 제2항에 의해 전자금융거래를 제한한 경우에는 거래처의 거래지시가 있을 때 해당 전자적 수단을 통하여 그 사유를 알려야 한다.
④ 제2항의 경우에 거래처는 은행이 정한 인증서 재발급·유효기간의 연장 또는 계속 사용의사 확인 등의 절차를 거쳐 전자금융거래를 이용할 수 있다.

제11조(거래의 완료) ① 계좌이체 및 계좌송금의 경우에는 수취인의 계좌원장에 입금기록을 마친 때에 거래가 완료된다.
② 현금출금의 경우에는 거래처에게 현금이 지급된 때에 거래가 완료된다.

제12조(수수료) ① 은행은 전자금융 수수료를 거래처의 계좌에서 출금하거나 거래처로부터 직접 현금으로 받을 수 있으며, 수납방법은 개별약관에 따른다.
② 수수료는 은행의 수수료율 계산방법에 따르며, 은행이 수수료율을 변경하고자 하는 때에는 그 내용을 영업점 및 게시 가능한 전자적 수단에 변경일 1주일전에 게시하여 1개월간 알린다.

제13조(거래지시의 취소·변경) ① 제8조에 의하여 거래가 성립한 이후에는 이를 취소 또는 변경하지 못한다. 다만 예약에 의한 계좌이체는 이체일 전영업일까지 해당 전자적 수단을 통하여 거래지시를 취소할 수 있다.

② 거래처의 요청에 따라 출금계좌를 해지할 때에는 해당 계좌에 등록된 예약에 의한 계좌이체 거래지시도 취소된다.

③ 거래처의 사망·한정치산선고·금치산 선고나 거래처 또는 은행의 해산·합병·파산은 그 자체로는 거래지시를 취소 또는 변경하는 것으로 되지 아니하며 은행의 권한에도 영향을 미치지 아니한다

제14조(신고사항의 변경) ① 거래처가 계좌번호, 비밀번호, 이용자번호, 상호, 주소, 전화번호 등 은행에 신고한 사항을 변경하고자 할 경우에는 전자금융거래에 관한 개별약관에 정한 바에 따라 신고하여야 한다.

② 신고사항의 변경은 은행이 제1항의 신고를 접수하고 전산입력에 요구되는 합리적인 시간이 지난 후에 그 효력이 생긴다.

제15조(거래계약의 해지) 전자금융거래에 관한 계약을 해지하고자 할 때에는 거래처 본인이 전자금융거래에 관한 개별약관에 정한 바에 따라 서면 또는 해당 전자적 수단에 의하여 은행에 해지신청을 하여야 한다.

제16조(거래내용의 확인) ① 거래처는 거래지시와 제21조 제1항에 의한 처리결과가 일치하는지 여부를 확인하여야 한다.

② 거래처는 거래지시와 은행의 처리결과가 일치하지 않음을 알게 된 때에는 이를 즉시 은행에 통지하여야 하며, 은행은 통지를 받은 때에는 이를 즉시 조사하여 처리하고 통지를 받은 후 2주 이내에 오류의 원인과 처리결과를 거래처에게 알려야 한다.

제17조(오류의 처리) ① 은행은 전자금융거래가 거래지시와 달리 처리된 사실을 확인한 때에는 이를 즉시 조사하여 처리하여야 한다.

② 은행은 제1항에 오류가 있음을 안날부터 2주 이내에 오류의 원인과 처리결과를 거래처에게 통지하여야 한다.

제18조(거래내용 녹음) 은행은 거래의 정확성을 기하기 위해 직원과의 전화통화에 의한 거래내용을 녹음할 수 있다. 다만, 녹음된 내용은 해당거래에 관한 분쟁이 발생할 경우의 증거자료로만 사용할 수 있으며, 이 경우 거래처는 은행에 녹음된 내용의 개시를 요구할 수 있다.

제19조(거래기록의 보존 및 자료 등의 제공) ① 은행은 전자금융거래로 인한 입출금내역을 5년간 유지, 보전하여야 한다.

② 은행은 거래처의 요청이 있을 경우 금융실명거래및비밀보장에관한법률 등 다른 법률에 저촉되지 않는 범위 내에서 은행이 보존·관리하고 있는 전자금융거래 관련 기록·자료를 요청을 받은 날부터 2주 이내에 거래처에 제공하여야 한다.

제20조(사고·장애시의 처리) ① 거래처는 거래계좌에 관한 접근수단의 도난·분실·위조 또는 변조의 사실을 알았거나 기타 거래절차상 비밀을 요하는 사항이 누설되었음을 알았을 때에는 지체없이 이를 은행에 신고하여야 한다.

② 은행은 제1항의 신고를 받은 때부터 제3자가 그 접근수단을 사용함으로써 거래처에게 발생한 손해를 배상할 책임을 진다.

③ 제1항의 신고를 철회할 경우에는 거래처 본인이 은행에 서면으로 신청하여야 한다.

④ 은행은 통신장애 및 기타의 사유로 인하여 거래지시된 전자금융거래가 처리 불가능할 경우 출금계좌로 입금처리하고 거래처의 신고된 연락처로 이를 통지하여야 한다.

⑤ 은행은 거래처의 요청이 있을 때에는 사고 또는 장애의 사유를 지체 없이 조사하여 그 결과를 거래처에게 통지하여야 한다.

제21조(통지방법 및 효력) ① 은행은 제11조의 처리결과를 즉시 해당 전자적 수단을 통하여 알린다. 다만, 타행계좌이체 및 예약에 의한 계좌이체의 경우에는 접수결과를 즉시 해당 전자적 수단을 통하여 알린다.

② 은행은 제17조제2항, 제20조제4항 및 제5항 등 전자금융거래에서 발생하는 사항을 통지하는 경우에는 거래처가 신고한 연락처로 전화, 서면 또는 기타 전자적 수단으로 통지하여야 한다.

③ 은행이 서면으로 통지했을 때에는 천재지변 등 불가항력적인 경우 외에는 보통의 우송기간이 지났을 때 도달한 것으로 추정한다.

④ 거래처가 제14조에 의한 변경신고를 게을리함에 따라 제3항에 의하여 발송한 서면통지가 거래처에게 연착하거나 도달하지 아니한 때에는 보통의 우송기간이 경과한 때에 도달한 것으로 본다.

제22조(접근수단의 관리) ① 거래처는 전자금융거래에 필요한 접근수단을 제3자에게 대여, 위탁 또는 양도하지 못한다.

② 거래처는 접근수단을 본인 이외의 제3자에게 누설해서는 안되며, 접근수단의 도용이나 위조 또는 변조를 방지하기 위한 관리에 충분한 주의를 기울여야 한다.

제23조(손실부담 및 면책) ① 은행은 거래처로부터 제20조에 의한 신고를 받은 후에 발생하는 부정이체 금액에 대하여는 그 금액과 1년 만기 정기예금 이율로 계산한 경과이자를 보상한다. 다만, 부정이체 결과로 당해 계좌에서 발생한 손실액이 1년 만기 정기예금 이율로 계산한 금액을 초과하는 경우에는 당해 손실액을 보상한다.

② 은행은 접근매체의 위조나 변조로 발생한 사고계약체결 또는 거래지시의 전자적 전송이나 처리과정에서 발생한 사고로 인하여 이용자에게 손해가 발생한 경우에는 그 손해를 배상할 책임을 진다.

③ 제2항의 규정에도 불구하고 은행은 다음 각 호의 어느 하나에 해당하는 경우에는 그 책임의 전부 또는 일부를 거래처가 부담하게 할 수 있다.

1. 천재지변, 전쟁, 테러 또는 은행의 귀책사유 없이 발생한 정전, 화재, 건물의 훼손 등 불가항력으로 인한 경우
2. 거래처가 접근매체를 제3자에게 대여하거나 사용을 위임하거나 양도 또는 담보목적으로 제공한 경우
3. 제3자가 권한 없이 거래처의 접근매체를 이용하여 전자금융거래를 할 수 있음을 알았거나 알 수 있었음에도 불구하고 거래처가 자신의 접근매체를 누설 또는 노출하거나 방치한 경우
4. 법인(「중소기업기본법」 제2조 제2항에 의한 소기업을 제외한다)인 거래처에게 손해가 발생한 경우로 은행이 사고를 방지하기 위하여 보안절차를 수립하고 이를 철저히 준수하는 등 합리적으로 요구되는 충분한 주의의무를 다한 경우

④ 은행은 제2항의 규정에 따른 책임을 이행하기 위해서는 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 한다.

제24조(비밀보장의무) 은행은 법령에 정한 경우를 제외하고는 전자금융거래업무를 수행함에 있어서 알게 된 거래처 관련 정보를 거래처 본인의 동의 없이는 다른 사람에게 제공하지 못한다. 다만, 은행의 관리소홀로 인한 거래처 관련 정보 도난 및 유출시에는 은행이 책임을 진다.

제25조(약관의 변경) ① 은행이 이 약관을 변경하고자 할 경우, 은행은 변경예정일 직전 1개월간 회사의 영업점 및 홈페이지에 변경내용을 게시한다.

② 제1항의 변경내용이 거래처에게 불리한 경우 은행은 이를 서면 등 거래처와 사전에 합의한 방법으로 변경 전 최소 30일전까지 개별 통지한다. 다만 기존 거래처에게 변경 전 내용이 그대로 적용되는 경우 또는 거래처가 변경내용에 대한 통지를 받지 아니하겠다는 의사를 명시적으로 표시한 경우에는 그러하지 아니하다.

③ 은행은 제2항의 통지를 할 경우 "거래처가 변경에 동의하지 아니한 경우 통지를 받은 날로부터 30일 이내에 계약을 해지할 수 있으며, 계약해지의 의사표시를 하지 아니한 경우에는 변경에 동의한 것으로 본다."라는 취지의 내용을 통지하여야 한다.

④ 거래처가 제3항의 통지를 받은 날로부터 30일 이내에 계약해지의 의사표시를 하지 아니한 경우에는 변경에 동의한 것으로 본다.

⑤ 은행은 약관을 영업점에 비치 또는 게시하여 거래처가 요구할 경우 이를 교부하여야 한다.

제26조(약관적용의 우선순위) ① 은행과 거래처 사이에 개별적으로 합의한 사항이 이 약관에 정한 사항과 다를 때에는 그 합의사항을 이 약관에 우선하여 적용한다.

② 전자금융거래에 관하여 이 약관에 정하지 않은 사항은 개별약관이 정하는 바에 따른다.

③ 이 약관과 전자금융거래에 관한 개별약관에 정하지 않은 사항에 대하여는 다른 약정이 없으면 관계 법령, 은행수신거래약관 및 은행여신거래약관을 적용한다.

제27조(이의제기) 거래처는 전자금융거래의 처리에 관하여 이의가 있을 때에는 은행의 분쟁처리기구에 그 해결을 요구하거나 금융감독원 금융분쟁조정위원회, 한국소비자보호원 소비자분쟁조정위원회 등을 통하여 분쟁조정을 신청할 수 있다.

제28조(준거법) 이 약관의 해석·적용에 관하여는 대한민국법을 적용한다.

전자금융거래법

[시행 2016.1.27] [법률 제13929호, 2016.1.27, 일부개정]

제1장 총칙

제1조(목적) 이 법은 전자금융거래의 법률관계를 명확히 하여 전자금융거래의 안전성과 신뢰성을 확보함과 아울러 전자금융업의 건전한 발전을 위한 기반조성을 함으로써 국민의 금융편의를 꾀하고 국민경제의 발전에 이바지함을 목적으로 한다.

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2007.4.27, 2008.2.29, 2012.3.21, 2012.6.1, 2013.5.22>

1. "전자금융거래"라 함은 금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공(이하 "전자금융업무"라 한다)하고, 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말한다.
2. "전자지급거래"라 함은 자금을 주는 자(이하 "지급인"이라 한다)가 금융회사 또는 전자금융업자로 하여금 전자지급수단을 이용하여 자금을 받는 자(이하 "수취인"이라 한다)에게 자금을 이동하게 하는 전자금융거래를 말한다.
3. "금융회사"란 다음 각 목의 어느 하나에 해당하는 기관이나 단체 또는 사업자를 말한다.
   가. 「금융위원회의 설치 등에 관한 법률」 제38조제1호부터 제5호까지, 제7호 및 제8호에 해당하는 기관
   나. 「여신전문금융업법」에 따른 여신전문금융회사
   다. 「우체국예금·보험에 관한 법률」에 따른 체신관서
   라. 「새마을금고법」에 따른 새마을금고 및 새마을금고중앙회
   마. 그 밖에 법률의 규정에 따라 금융업 및 금융 관련 업무를 행하는 기관이나 단체 또는 사업자로서 대통령령이 정하는 자
4. "전자금융업자"라 함은 제28조의 규정에 따라 허가를 받거나 등록을 한 자(금융회사는 제외한다)를 말한다.
5. "전자금융보조업자"라 함은 금융회사 또는 전자금융업자를 위하여 전자금융거래를 보조하거나 그 일부를 대행하는 업무를 행하는 자 또는 결제중계시스템의 운영자로서 「금융위원회의 설치 등에 관한 법률」제3조에 따른 금융위원회(이하 "금융위원회"라 한다)가 정하는 자를 말한다.

6. "결제중계시스템"이라 함은 금융회사와 전자금융업자 사이에 전자금융거래정보를 전달하여 자금정산 및 결제에 관한 업무를 수행하는 금융정보처리운영체계를 말한다.
7. "이용자"라 함은 전자금융거래를 위하여 금융회사 또는 전자금융업자와 체결한 계약(이하 "전자금융거래계약"이라 한다)에 따라 전자금융거래를 이용하는 자를 말한다.
8. "전자적 장치"라 함은 전자금융거래정보를 전자적 방법으로 전송하거나 처리하는데 이용되는 장치로서 현금자동지급기, 자동입출금기, 지급용단말기, 컴퓨터, 전화기 그 밖에 전자적 방법으로 정보를 전송하거나 처리하는 장치를 말한다.
9. "전자문서"라 함은 「전자문서 및 전자거래 기본법」 제2조제1호에 따른 작성, 송신·수신 또는 저장된 정보를 말한다.
10. "접근매체"라 함은 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 다음 각 목의 어느 하나에 해당하는 수단 또는 정보를 말한다.
    가. 전자식 카드 및 이에 준하는 전자적 정보
    나. 「전자서명법」 제2조제4호의 전자서명생성정보 및 같은 조제7호의 인증서
    다. 금융회사 또는 전자금융업자에 등록된 이용자번호
    라. 이용자의 생체정보
    마. 가목 또는 나목의 수단이나 정보를 사용하는데 필요한 비밀번호
11. "전자지급수단"이라 함은 전자자금이체, 직불전자지급수단, 선불전자지급수단, 전자화폐, 신용카드, 전자채권 그 밖에 전자적 방법에 따른 지급수단을 말한다.
12. "전자자금이체"라 함은 지급인과 수취인 사이에 자금을 지급할 목적으로 금융회사 또는 전자금융업자에 개설된 계좌(금융회사에 연결된 계좌에 한한다. 이하 같다)에서 다른 계좌로 전자적 장치에 의하여 다음 각 목의 어느 하나에 해당하는 방법으로 자금을 이체하는 것을 말한다.
    가. 금융회사 또는 전자금융업자에 대한 지급인의 지급지시
    나. 금융회사 또는 전자금융업자에 대한 수취인의 추심지시(이하 "추심이체"라 한다)
13. "직불전자지급수단"이라 함은 이용자와 가맹점간에 전자적 방법에 따라 금융회사의 계좌에서 자금을 이체하는 등의 방법으로 재화 또는 용역의 제공과 그 대가의 지급을 동시에 이행할 수 있도록 금융회사 또는 전자금융업자가 발행한 증표(자금을 융통받을 수 있는 증표를 제외한다) 또는 그 증표에 관한 정보를 말한다.
14. "선불전자지급수단"이라 함은 이전 가능한 금전적 가치가 전자적 방법으로 저장되어 발행된 증표 또는 그 증표에 관한 정보로서 다음 각 목의 요건을 모두 갖춘 것을 말한다. 다만, 전자화폐를 제외한다.
    가. 발행인(대통령령이 정하는 특수관계인을 포함한다) 외의 제3자로부터 재화 또는 용역을 구입하고 그 대가를 지급하는데 사용될 것
    나. 구입할 수 있는 재화 또는 용역의 범위가 2개 업종(「통계법」 제22조제1항의 규정에 따라 통계청장이 고시하는 한국표준산업분류의 중분류상의 업종을 말한다. 이하 이 조에

서 같다)이상일 것

15. "전자화폐"라 함은 이전 가능한 금전적 가치가 전자적 방법으로 저장되어 발행된 증표 또는 그 증표에 관한 정보로서 다음 각 목의 요건을 모두 갖춘 것을 말한다.
    가. 대통령령이 정하는 기준 이상의 지역 및 가맹점에서 이용될 것
    나. 제14호 가목의 요건을 충족할 것
    다. 구입할 수 있는 재화 또는 용역의 범위가 5개 이상으로서 대통령령이 정하는 업종 수 이상일 것
    라. 현금 또는 예금과 동일한 가치로 교환되어 발행될 것
    마. 발행자에 의하여 현금 또는 예금으로 교환이 보장될 것
16. "전자채권"이라 함은 다음 각 목의 요건을 갖춘 전자문서에 기재된 채권자의 금전채권을 말한다.
    가. 채무자가 채권자를 지정할 것
    나. 전자채권에 채무의 내용이 기재되어 있을 것
    다. 「전자서명법」 제2조제3호의 공인전자서명이 있을 것
    라. 금융회사를 거쳐 제29조제1항의 규정에 따른 전자채권관리기관(이하 "전자채권관리기관"이라 한다)에 등록될 것
    마. 채무자가 채권자에게 가목 내지 다목의 요건을 모두 갖춘 전자문서를 「전자문서 및 전자거래 기본법」 제6조제1항에 따라 송신하고 채권자가 이를 같은 법 제6조제2항의 규정에 따라 수신할 것
17. "거래지시"라 함은 이용자가 전자금융거래계약에 따라 금융회사 또는 전자금융업자에게 전자금융거래의 처리를 지시하는 것을 말한다.
18. "오류"라 함은 이용자의 고의 또는 과실 없이 전자금융거래가 전자금융거래계약 또는 이용자의 거래지시에 따라 이행되지 아니한 경우를 말한다.
19. "전자지급결제대행"이라 함은 전자적 방법으로 재화의 구입 또는 용역의 이용에 있어서 지급결제정보를 송신하거나 수신하는 것 또는 그 대가의 정산을 대행하거나 매개하는 것을 말한다.
20. "가맹점"이라 함은 금융회사 또는 전자금융업자와의 계약에 따라 직불전자지급수단이나 선불전자지급수단 또는 전자화폐에 의한 거래에 있어서 이용자에게 재화 또는 용역을 제공하는 자로서 금융회사 또는 전자금융업자가 아닌 자를 말한다.
21. "전자금융기반시설"이란 전자금융거래에 이용되는 정보처리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망을 말한다.
22. "전자적 침해행위"란 해킹, 컴퓨터 바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 전자금융기반시설을 공격하는 행위를 말한다.

제3조(적용범위) ①이 법은 다른 법률에 특별한 규정이 있는 경우를 제외하고 모든 전자금융거래에 적용한다. 다만, 금융회사 및 전자금융업자간에 따로 정하는 계약에 따라 이루어지는 전자금융거래 가운데 대통령령이 정하는 경우에는 이 법을 적용하지 아니한다. <개정 2013.5.22>

②제5장의 규정은 제2조제3호 다목 및 라목의 금융회사에 대하여는 이를 적용하지 아니한다. <개정 2013.5.22>

③ 금융회사 중 전자금융거래의 빈도, 회사의 규모 등을 고려하여 대통령령으로 정하는 금융회사에 대하여는 다음 각 호를 적용하지 아니한다.<신설 2013.5.22>

1. 제21조제2항의 인력, 시설, 전자적 장치 등의 정보기술부문 및 전자금융업무에 관하여 금융위원회가 정하는 기준 준수
2. 제21조제4항의 정보기술부문의 계획수립 및 제출
3. 제21조의2의 정보보호최고책임자 지정
4. 제21조의3의 전자금융기반시설의 취약점 분석·평가

제4조(상호주의) 외국인 또는 외국법인에 대하여도 이 법을 적용한다. 다만, 대한민국 국민 또는 대한민국 법인에 대하여 이 법에 준하는 보호를 하지 아니하는 국가의 외국인 또는 외국법인에 대하여는 그에 상응하여 이 법 또는 대한민국이 가입하거나 체결한 조약에 따른 보호를 제한할 수 있다.

제2장 전자금융거래 당사자의 권리와 의무

제1절 통칙

제5조(전자문서의 사용) ①전자금융거래를 위하여 사용되는 전자문서에 대하여는 「전자문서 및 전자거래 기본법」 제4조부터 제7조까지, 제9조 및 제10조를 적용한다. <개정 2012.6.1>

②금융회사 또는 전자금융업자가 거래지시와 관련하여 수신한 전자문서는 각 문서마다 독립된 것으로 본다. 다만, 금융회사 또는 전자금융업자와 이용자 사이에 전자금융거래계약에 따라 확인절차를 거치는 경우에는 그 절차에 따른다.<개정 2013.5.22>

제6조(접근매체의 선정과 사용 및 관리) ①금융회사 또는 전자금융업자는 전자금융거래를 위하여 접근매체를 선정하여 사용 및 관리하고 이용자의 신원, 권한 및 거래지시의 내용 등을 확인하여야 한다. <개정 2013.5.22>

②금융회사 또는 전자금융업자가 접근매체를 발급할 때에는 이용자의 신청이 있는 경우에 한하여 본인임을 확인한 후에 발급하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 이용자의 신청이나 본인의 확인이 없는 때에도 발급할 수 있다.<개정 2013.5.22>

1. 선불전자지급수단 또는 제16조제1항 단서의 규정에 따른 전자화폐인 경우
2. 접근매체의 갱신 또는 대체발급 등을 위하여 대통령령이 정하는 바에 따라 이용자의 동의를 얻은 경우

③ 누구든지 접근매체를 사용 및 관리함에 있어서 다른 법률에 특별한 규정이 없는 한 다음 각 호의 행위를 하여서는 아니 된다. 다만, 제18조에 따른 선불전자지급수단이나 전자화폐의 양도 또는 담보제공을 위하여 필요한 경우(제3호의 행위 및 이를 알선하는 행위는 제외한다)에는 그러하지 아니하다.<개정 2008.12.31, 2015.1.20, 2016.1.27>

1. 접근매체를 양도하거나 양수하는 행위
2. 대가를 수수(授受)·요구 또는 약속하면서 접근매체를 대여받거나 대여하는 행위 또는 보관·전달·유통하는 행위
3. 범죄에 이용할 목적으로 또는 범죄에 이용될 것을 알면서 접근매체를 대여받거나 대여하는 행위 또는 보관·전달·유통하는 행위
4. 접근매체를 질권의 목적으로 하는 행위
5. 제1호부터 제4호까지의 행위를 알선하거나 광고하는 행위

제6조의2(불법 광고에 이용된 전화번호의 이용중지 등) ① 검찰총장, 경찰청장 또는 금융감독원장(「금융위원회의 설치 등에 관한 법률」 제29조에 따른 금융감독원장을 말한다. 이하 같다)은 제6조제3항제5호에 따른 불법광고에 이용된 전화번호를 확인한 때에는 미래창조과학부장관에게 해당 전화번호에 대한 전기통신역무 제공의 중지를 요청할 수 있다.

② 제1항에 따른 요청으로 전기통신역무 제공이 중지된 사람은 전기통신역무 제공의 중지를 요청한 자에게 이의신청을 할 수 있다.

③ 제2항에 따른 이의신청의 절차 등에 필요한 사항은 대통령령으로 정한다.

[본조신설 2016.1.27]

제7조(거래내용의 확인) ①금융회사 또는 전자금융업자는 이용자가 전자금융거래에 사용하는 전자적 장치(금융회사 또는 전자금융업자와 이용자 사이에 미리 약정한 전자적 장치가 있는 경우에는 그 전자적 장치를 포함한다)를 통하여 거래내용을 확인할 수 있도록 하여야 한다. <개정 2013.5.22>

②금융회사 또는 전자금융업자는 이용자가 거래내용을 서면(전자문서를 제외한다. 이하 같다)으로 제공할 것을 요청하는 경우에는 그 요청을 받은 날부터 2주 이내에 거래내용에 관한 서면을 교부하여야 한다.<개정 2013.5.22>

③제1항 및 제2항의 규정에 따라 제공하는 거래내용의 대상기간, 종류 및 범위 등에 관한 사항은 대통령령으로 정한다.

제8조(오류의 정정 등) ①이용자는 전자금융거래에 오류가 있음을 안 때에는 그 금융회사 또는 전자금융업자에게 이에 대한 정정을 요구할 수 있다. <개정 2013.5.22>

②금융회사 또는 전자금융업자는 제1항의 규정에 따른 오류의 정정요구를 받은 때에는 이를 즉시 조사하여 처리한 후 정정요구를 받은 날부터 2주 이내에 오류의 원인과 처리 결과를 대통령령으로 정하는 방법에 따라 이용자에게 알려야 한다.<개정 2008.12.31, 2013.5.22>

③금융회사 또는 전자금융업자는 스스로 전자금융거래에 오류가 있음을 안 때에는 이를 즉시 조사하여 처리한 후 오류가 있음을 안 날부터 2주 이내에 오류의 원인과 처리 결과를 대통령령으로 정하는 방법에 따라 이용자에게 알려야 한다.<개정 2008.12.31, 2013.5.22>

제9조(금융회사 또는 전자금융업자의 책임) ①금융회사 또는 전자금융업자는 다음 각 호의 어느 하나에 해당하는 사고로 인하여 이용자에게 손해가 발생한 경우에는 그 손해를 배상할 책임을

진다. <개정 2013.5.22>

1. 접근매체의 위조나 변조로 발생한 사고
2. 계약체결 또는 거래지시의 전자적 전송이나 처리 과정에서 발생한 사고
3. 전자금융거래를 위한 전자적 장치 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망에 침입하여 거짓이나 그 밖의 부정한 방법으로 획득한 접근매체의 이용으로 발생한 사고

②제1항의 규정에 불구하고 금융회사 또는 전자금융업자는 다음 각 호의 어느 하나에 해당하는 경우에는 그 책임의 전부 또는 일부를 이용자가 부담하게 할 수 있다.<개정 2013.5.22>

1. 사고 발생에 있어서 이용자의 고의나 중대한 과실이 있는 경우로서 그 책임의 전부 또는 일부를 이용자의 부담으로 할 수 있다는 취지의 약정을 미리 이용자와 체결한 경우
2. 법인(「중소기업기본법」 제2조제2항에 의한 소기업을 제외한다)인 이용자에게 손해가 발생한 경우로 금융회사 또는 전자금융업자가 사고를 방지하기 위하여 보안절차를 수립하고 이를 철저히 준수하는 등 합리적으로 요구되는 충분한 주의의무를 다한 경우

③제2항제1호의 규정에 따른 이용자의 고의나 중대한 과실은 대통령령이 정하는 범위 안에서 전자금융거래에 관한 약관(이하 "약관"이라 한다)에 기재된 것에 한한다.

④금융회사 또는 전자금융업자는 제1항의 규정에 따른 책임을 이행하기 위하여 금융위원회가 정하는 기준에 따라 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다.<개정 2008.2.29, 2013.5.22>

[제목개정 2013.5.22]

제10조(접근매체의 분실과 도난 책임) ①금융회사 또는 전자금융업자는 이용자로부터 접근매체의 분실이나 도난 등의 통지를 받은 때에는 그 때부터 제3자가 그 접근매체를 사용함으로 인하여 이용자에게 발생한 손해를 배상할 책임을 진다. 다만, 선불전자지급수단이나 전자화폐의 분실 또는 도난 등으로 발생하는 손해로서 대통령령이 정하는 경우에는 그러하지 아니하다. <개정 2013.5.22>

②제1항 및 제9조의 규정에 불구하고 다른 법령에 이용자에게 유리하게 적용될 수 있는 규정이 있는 경우에는 그 법령을 우선 적용한다.

제11조(전자금융보조업자의 지위) ①전자금융거래와 관련하여 전자금융보조업자(전자채권관리기관을 포함한다. 이하 이 장에서 같다)의 고의나 과실은 금융회사 또는 전자금융업자의 고의나 과실로 본다. <개정 2013.5.22>

②금융회사 또는 전자금융업자는 전자금융보조업자의 고의나 과실로 인하여 발생한 손해에 대하여 이용자에게 그 손해를 배상한 경우에는 그 전자금융보조업자에게 구상할 수 있다.<개정 2013.5.22>

③이용자는 금융회사 또는 전자금융업자와의 약정에 따라 금융회사 또는 전자금융업자에게 행하는 각종 통지를 전자금융보조업자에게 할 수 있다. 이 경우 전자금융보조업자에게 한 통지는 금융회사 또는 전자금융업자에게 한 것으로 본다.<개정 2013.5.22>

제2절 전자지급거래 등

제12조(전자지급거래계약의 효력) ①금융회사 또는 전자금융업자는 지급인 또는 수취인과 전자지급거래를 하기 위하여 체결한 약정에 따라 수취인이나 수취인의 금융회사 또는 전자금융업자에게 지급인 또는 수취인이 거래지시한 금액을 전송하여 지급이 이루어지도록 하여야 한다. <개정 2013.5.22>

②금융회사 또는 전자금융업자는 제1항의 규정에 따른 자금의 지급이 이루어질 수 없게 된 때에는 전자지급거래를 하기 위하여 수령한 자금을 지급인에게 반환하여야 한다. 이 경우 지급인의 과실로 인하여 지급이 이루어지지 아니한 때에는 그 전송을 하기 위하여 지출한 비용을 공제할 수 있다.<개정 2013.5.22>

제13조(지급의 효력발생시기) ①전자지급수단을 이용하여 자금을 지급하는 경우에는 그 지급의 효력은 다음 각 호의 어느 하나에서 정한 때에 생긴다. <개정 2013.5.22, 2014.10.15>

1. 전자자금이체의 경우 : 거래지시된 금액의 정보에 대하여 수취인의 계좌가 개설되어 있는 금융회사 또는 전자금융업자의 계좌의 원장에 입금기록이 끝난 때
2. 전자적 장치로부터 직접 현금을 출금하는 경우 : 수취인이 현금을 수령한 때
3. 선불전자지급수단 및 전자화폐로 지급하는 경우 : 거래지시된 금액의 정보가 수취인이 지정한 전자적 장치에 도달한 때
4. 그 밖의 전자지급수단으로 지급하는 경우 : 거래지시된 금액의 정보가 수취인의 계좌가 개설되어 있는 금융회사 또는 전자금융업자의 전자적 장치에 입력이 끝난 때

② 총자산 등을 감안하여 대통령령으로 정하는 금융회사 또는 전자금융업자는 이용자가 원하는 경우 대통령령으로 정하는 절차와 방법에 따라 이용자가 거래지시를 하는 때부터 일정 시간이 경과한 후에 전자자금이체의 지급 효력이 발생하도록 하여야 한다.<신설 2014.10.15>

제14조(거래지시의 철회) ①이용자는 제13조제1항 각 호의 규정에 따라 지급의 효력이 발생하기 전까지 거래지시를 철회할 수 있다. <개정 2014.10.15>

②제1항의 규정에 불구하고 금융회사 또는 전자금융업자와 이용자는 대량으로 처리하는 거래 또는 예약에 따른 거래 등의 경우에는 미리 정한 약정에 따라 거래지시의 철회시기를 달리 정할 수 있다.<개정 2013.5.22>

③금융회사 또는 전자금융업자는 제1항의 규정에 따른 거래지시의 철회방법 및 절차와 제2항의 규정에 따른 약정에 관한 사항을 약관에 기재하여야 한다.<개정 2013.5.22>

제15조(추심이체의 출금 동의) ①금융회사 또는 전자금융업자는 추심이체를 실행하기 위하여 대통령령이 정하는 바에 따라 미리 지급인으로부터 출금에 대한 동의를 얻어야 한다. <개정 2013.5.22>

②지급인은 수취인의 거래지시에 따라 지급인의 계좌의 원장에 출금기록이 끝나기 전까지 금융회사 또는 전자금융업자에게 제1항의 규정에 따른 동의의 철회를 요청할 수 있다.<개정

2013.5.22>

③제2항의 규정에 불구하고 금융회사 또는 전자금융업자는 대량으로 처리하는 거래 또는 예약에 따른 거래 등의 경우에는 미리 지급인과 정한 약정에 따라 동의의 철회시기를 달리 정할 수 있다.<개정 2013.5.22>

④금융회사 또는 전자금융업자는 제2항 및 제3항의 규정에 따른 동의의 철회방법 및 절차와 약정에 관한 사항을 약관에 기재하여야 한다.<개정 2013.5.22>

제16조(전자화폐의 발행과 사용 및 환금) ①전자화폐를 발행하는 금융회사 또는 전자금융업자(이하 "전자화폐발행자"라 한다)는 전자화폐를 발행할 경우 접근매체에 식별번호를 부여하고 그 식별번호와 「금융실명거래 및 비밀보장에 관한 법률」 제2조제4호에서 규정한 이용자의 실지명의(이하 "실지명의"라 한다) 또는 예금계좌를 연결하여 관리하여야 한다. 다만, 발행권면 최고한도가 대통령령이 정하는 금액 이하인 전자화폐의 경우에는 그러하지 아니하다. <개정 2013.5.22>

②전자화폐발행자는 현금 또는 예금과 동일한 가치로 교환하여 전자화폐를 발행하여야 한다.

③전자화폐발행자는 전자화폐보유자가 전자화폐를 사용할 수 있도록 발행된 전자화폐의 보관 및 사용 등에 필요한 조치를 하여야 한다.

④전자화폐발행자는 전자화폐보유자의 요청에 따라 전자화폐를 현금 또는 예금으로 교환할 의무를 부담한다.

⑤제1항 내지 제4항의 규정에 따른 전자화폐의 발행·교환의 방법 및 절차에 관하여는 대통령령으로 정한다.

제17조(전자화폐에 의한 지급의 효력) 전자화폐보유자가 재화를 구입하거나 용역을 제공받고 그 대금을 수취인과의 합의에 따라 전자화폐로 지급한 때에는 그 대금의 지급에 관한 채무는 변제된 것으로 본다.

제18조(전자화폐 등의 양도성) ①선불전자지급수단 보유자 또는 전자화폐 보유자는 발행자와의 약정에 따라 선불전자지급수단 또는 전자화폐를 타인에게 양도하거나 담보로 제공할 수 있다.

②제1항의 규정에 따라 선불전자지급수단 또는 전자화폐를 양도하거나 담보로 제공하는 경우에는 반드시 발행자의 중앙전산시스템을 경유하여야 한다. 다만, 실지명의가 확인되지 아니하는 선불전자지급수단 또는 제16조제1항 단서의 규정에 따른 전자화폐의 경우에는 그러하지 아니하다.

제19조(선불전자지급수단의 환급) ①선불전자지급수단을 발행한 금융회사 또는 전자금융업자는 선불전자지급수단보유자가 선불전자지급수단에 기록된 잔액의 환급을 청구하는 경우에는 미리 약정한 바에 따라 환급하여야 한다. <개정 2013.5.22>

②금융회사 또는 전자금융업자는 제1항의 규정에 따른 환급과 관련된 약정을 약관에 기재하고, 다음 각 호의 어느 하나에 해당하는 경우에는 선불전자지급수단에 기록된 잔액의 전부를 지급한다는 내용을 약관에 포함시켜야 한다.<개정 2013.5.22>

1. 천재지변 등의 사유로 가맹점이 재화 또는 용역을 제공하기 곤란하여 선불전자지급수단을 사용하지 못하게 된 경우
2. 선불전자지급수단의 결함으로 가맹점이 재화 또는 용역을 제공하지 못하는 경우
3. 선불전자지급수단에 기록된 잔액이 일정비율 이하인 경우. 이 경우 일정비율은 100분의 20 미만으로 정할 수 없다.

제20조(전자채권양도의 대항요건) ①전자채권의 양도는 다음 각 호의 요건을 모두 갖춘 때에 「민법」 제450조제1항의 규정에 따른 대항요건을 갖춘 것으로 본다.

1. 양도인의 채권양도의 통지 또는 채무자의 승낙이 「전자서명법」제2조제3호의 공인전자서명을 한 전자문서에 의하여 이루어질 것
2. 제1호의 규정에 따른 통지 또는 승낙이 기재된 전자문서가 전자채권관리기관에 등록될 것

②제1항의 규정에 따른 통지 또는 승낙이 기재된 전자문서에 「전자서명법」 제20조의 규정에 따른 시점확인이 있고 제1항의 요건을 모두 갖춘 때에 「민법」 제450조제2항의 규정에 따른 대항요건을 갖춘 것으로 본다.

제3장 전자금융거래의 안전성 확보 및 이용자 보호

제21조(안전성의 확보의무) ①금융회사·전자금융업자 및 전자금융보조업자(이하 "금융회사등"이라 한다)는 전자금융거래가 안전하게 처리될 수 있도록 선량한 관리자로서의 주의를 다하여야 한다. <개정 2013.5.22>

②금융회사등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치, 소요경비 등의 정보기술부문, 전자금융업무 및 「전자서명법」에 의한 인증서의 사용 등 인증방법에 관하여 금융위원회가 정하는 기준을 준수하여야 한다.<개정 2008.2.29, 2013.5.22, 2014.10.15>

③ 금융위원회는 제2항의 기준을 정할 때 특정 기술 또는 서비스의 사용을 강제하여서는 아니되며, 보안기술과 인증기술의 공정한 경쟁이 촉진되도록 노력하여야 한다.<개정 2014.10.15>

④ 대통령령으로 정하는 금융회사 및 전자금융업자는 안전한 전자금융거래를 위하여 대통령령으로 정하는 바에 따라 정보기술부문에 대한 계획을 매년 수립하여 대표자의 확인·서명을 받아 금융위원회에 제출하여야 한다.<신설 2013.5.22>

제21조의2(정보보호최고책임자 지정) ① 금융회사 또는 전자금융업자는 전자금융업무 및 그 기반이 되는 정보기술부문 보안을 총괄하여 책임질 정보보호최고책임자를 지정하여야 한다. <개정 2013.5.22>

② 총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 금융회사 또는 전자금융업자는 정보보호최고책임자를 임원(「상법」 제401조의2제1항제3호에 따른 자를 포함한다)으로 지정하여야 한다.<개정 2013.5.22>

③ 총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 금융회사 또는 전자금융업자의 정보보호최고책임자는 제4항의 업무 외의 다른 정보기술부문 업무를 겸직할 수 없다.<신설 2014.10.15>

④ 제1항에 따른 정보보호최고책임자는 다음 각 호의 업무를 수행한다.<개정 2014.10.15>

1. 제21조제2항에 따른 전자금융거래의 안정성 확보 및 이용자 보호를 위한 전략 및 계획의 수립
2. 정보기술부문의 보호
3. 정보기술부문의 보안에 필요한 인력관리 및 예산편성
4. 전자금융거래의 사고 예방 및 조치
5. 그 밖에 전자금융거래의 안정성 확보를 위하여 대통령령으로 정하는 사항

⑤ 정보보호최고책임자의 자격요건 등에 필요한 사항은 대통령령으로 정한다.<개정 2014.10.15>

[본조신설 2011.11.14]

제21조의3(전자금융기반시설의 취약점 분석·평가) ① 금융회사 및 전자금융업자는 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 전자금융기반시설에 대한 다음 각 호의 사항을 분석·평가하고 그 결과(「정보통신기반 보호법」 제9조에 따른 취약점 분석·평가를 한 경우에는 그 결과를 말한다)를 금융위원회에 보고하여야 한다.

1. 정보기술부문의 조직, 시설 및 내부통제에 관한 사항
2. 정보기술부문의 전자적 장치 및 접근매체에 관한 사항
3. 전자금융거래의 유지를 위한 침해사고 대응조치에 관한 사항
4. 그 밖에 대통령령으로 정하는 사항

② 금융회사 및 전자금융업자는 제1항에 따른 전자금융기반시설의 취약점 분석·평가 결과에 따른 필요한 보완조치의 이행계획을 수립·시행하여야 한다.

③ 금융위원회는 소속 공무원으로 하여금 제1항에 따른 전자금융기반시설의 취약점 분석·평가 결과 및 제2항에 따른 보완조치의 이행실태를 점검하게 할 수 있다.

④ 제1항에 따른 전자금융기반시설의 취약점 분석·평가의 내용 및 절차와 제2항에 따른 이행계획의 수립·시행, 그 밖에 필요한 사항은 대통령령으로 정한다.

[본조신설 2013.5.22]

제21조의4(전자적 침해행위 등의 금지) 누구든지 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.

1. 접근권한을 가지지 아니하는 자가 전자금융기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 넘어 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위
2. 전자금융기반시설에 대하여 데이터를 파괴하거나 전자금융기반시설의 운영을 방해할 목적으로 컴퓨터 바이러스, 논리폭탄 또는 메일폭탄 등의 프로그램을 투입하는 행위

3. 전자금융기반시설의 안정적 운영을 방해할 목적으로 일시에 대량의 신호, 고출력 전자기파 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 전자금융기반시설에 오류 또는 장애를 발생하게 하는 행위

[본조신설 2013.5.22]

제21조의5(침해사고의 통지 등) ① 금융회사 및 전자금융업자는 전자적 침해행위로 인하여 전자금융기반시설이 교란·마비되는 등의 사고(이하 "침해사고"라 한다)가 발생한 때에는 금융위원회에 지체 없이 이를 알려야 한다.

② 금융회사 및 전자금융업자는 침해사고가 발생하면 그 원인을 분석하고 피해의 확산을 방지하기 위하여 필요한 조치를 하여야 한다.

[본조신설 2013.5.22]

제21조의6(침해사고의 대응) ① 금융위원회는 침해사고에 대응하기 위하여 다음 각 호의 업무를 수행한다.

1. 침해사고에 관한 정보의 수집·전파
2. 침해사고의 예보·경보
3. 침해사고에 대한 긴급조치
4. 그 밖에 침해사고 대응을 위하여 대통령령으로 정하는 사항

② 제1항에 따른 업무를 수행하는 데 필요한 절차·방법 등은 대통령령으로 정한다.

[본조신설 2013.5.22]

제22조(전자금융거래기록의 생성·보존 및 파기) ①금융회사등은 전자금융거래의 내용을 추적·검색하거나 그 내용에 오류가 발생할 경우에 이를 확인하거나 정정할 수 있는 기록(이하 이 조에서 "전자금융거래기록"이라 한다)을 생성하여 5년의 범위 안에서 대통령령이 정하는 기간동안 보존하여야 한다. <개정 2013.5.22, 2014.10.15>

② 금융회사등은 제1항에 따라 보존하여야 하는 기간이 경과하고 금융거래 등 상거래관계가 종료된 경우에는 5년 이내에 전자금융거래기록(「신용정보의 이용 및 보호에 관한 법률」에 따른 신용정보는 제외한다. 이하 이 항에서 같다)을 파기하여야 한다. 다만, 다음 각 호의 경우에는 그러하지 아니하다.<신설 2014.10.15>

1. 다른 법률에 따른 의무를 이행하기 위하여 불가피한 경우
2. 그 밖에 전자금융거래기록을 보관할 필요성이 있는 경우로서 금융위원회가 정하는 경우

③제1항 및 제2항에 따라 금융회사등이 보존하여야 하는 전자금융거래기록의 종류, 보존방법, 파기절차·방법 및 상거래관계가 종료된 날의 기준 등은 대통령령으로 정한다.<개정 2013.5.22, 2014.10.15>

[제목개정 2014.10.15]

제23조(전자지급수단 등의 발행과 이용한도) ① 금융위원회는 전자지급수단의 특성을 감안하여 대통령령이 정하는 바에 따라 금융회사 또는 전자금융업자에게 다음 각 호에 규정된 한도를

제한하거나 그 밖에 필요한 조치를 할 수 있다. <개정 2008.2.29, 2013.5.22>

1. 전자화폐 및 선불전자지급수단의 발행권면 최고한도
2. 전자자금이체의 이용한도
3. 직불전자지급수단의 이용한도

② 금융위원회는 대통령령으로 정하는 바에 따라 금융회사 또는 전자금융업자에게 전자적 장치로부터의 현금 출금 최고한도를 제한하거나 그 밖에 필요한 조치를 할 수 있다.<신설 2013.5.22>

[제목개정 2013.5.22]

제24조(약관의 명시와 변경통지 등) ①금융회사 또는 전자금융업자는 이용자와 전자금융거래의 계약을 체결함에 있어서 약관을 명시하여야 하고, 이용자의 요청이 있는 경우에는 금융위원회가 정하는 방법에 따라 그 약관의 사본을 교부하고 그 약관의 내용을 설명하여야 한다. <개정 2008.2.29, 2013.5.22>

②금융회사 또는 전자금융업자는 제1항의 규정을 위반하여 계약을 체결한 때에는 당해 약관의 내용을 계약의 내용으로 주장할 수 없다.<개정 2013.5.22>

③금융회사 또는 전자금융업자는 약관을 변경하는 때에는 변경되는 약관의 시행일 1월 전에 금융위원회가 정하는 방법에 따라 이를 게시하고 이용자에게 알려야 한다. 다만, 법령의 개정으로 인하여 긴급하게 약관을 변경하는 때에는 금융위원회가 정하는 방법에 따라 이를 즉시 게시하고 이용자에게 알려야 한다.<개정 2008.2.29, 2013.5.22>

④이용자는 제3항의 규정에 따른 약관의 변경내용이 게시되거나 통지된 후부터 변경되는 약관의 시행일 전의 영업일까지 전자금융거래의 계약을 해지할 수 있다. 전단의 기간 안에 이용자가 약관의 변경내용에 대하여 이의를 제기하지 아니하는 경우에는 약관의 변경을 승인한 것으로 본다.

제25조(약관의 제정 및 변경) ①금융회사 또는 전자금융업자가 전자금융거래에 관한 약관을 제정하거나 변경하고자 하는 경우에는 미리 금융위원회에 보고하여야 한다. 다만, 이용자의 권익이나 의무에 불리한 영향이 없는 경우로서 금융위원회가 정하는 경우에는 약관의 제정 또는 변경 후 10일 이내에 금융위원회에 보고할 수 있다. <개정 2008.2.29, 2013.5.22>

②금융위원회는 건전한 전자금융거래질서를 유지하기 위하여 필요한 경우에는 금융회사 또는 전자금융업자에 대하여 제1항의 규정에 따른 약관의 변경을 권고할 수 있다.<개정 2008.2.29, 2013.5.22>

③금융위원회는 제1항의 규정에 따른 약관의 제정 또는 변경에 대한 보고의 시기·절차 그 밖에 필요한 사항을 정할 수 있다.<개정 2008.2.29>

④제1항 내지 제3항의 규정은 제2조제3호 다목 및 라목의 금융회사에 대하여는 이를 적용하지 아니한다.<개정 2013.5.22>

제26조(전자금융거래정보의 제공 등) 전자금융거래와 관련한 업무를 수행함에 있어서 다음 각 호의 어느 하나에 해당하는 사항을 알게 된 자는 이용자의 동의를 얻지 아니하고 이를 타인에

게 제공·누설하거나 업무상 목적 외에 사용하여서는 아니된다. 다만, 「금융실명거래 및 비밀보장에 관한 법률」 제4조제1항 단서의 규정에 따른 경우 그 밖에 다른 법률에서 정하는 바에 따른 경우에는 그러하지 아니하다.

1. 이용자의 인적 사항
2. 이용자의 계좌, 접근매체 및 전자금융거래의 내용과 실적에 관한 정보 또는 자료

제27조(분쟁처리 및 분쟁조정) ①금융회사 또는 전자금융업자는 대통령령이 정하는 바에 따라 전자금융거래와 관련하여 이용자가 제기하는 정당한 의견이나 불만을 반영하고 이용자가 전자금융거래에서 입은 손해를 배상하기 위한 절차를 마련하여야 한다. <개정 2013.5.22>

②이용자는 전자금융거래의 처리에 관하여 이의가 있을 때에는 제1항에서 정한 절차에 따라 손해배상 등 분쟁처리를 요구하거나 금융감독원 또는 한국소비자원 등을 통하여 분쟁조정을 신청할 수 있다.<개정 2013.5.22>

③제1항 및 제2항의 규정에 따른 분쟁처리 및 분쟁조정의 신청을 위한 구체적인 절차와 방법 등은 대통령령으로 정한다.

④금융회사 또는 전자금융업자는 전자금융거래의 계약을 체결하는 때에는 제1항 내지 제3항의 규정에 따른 절차를 명시하여야 한다.<개정 2013.5.22>

제4장 전자금융업의 허가와 등록 및 업무

제28조(전자금융업의 허가와 등록) ①전자화폐의 발행 및 관리업무를 행하고자 하는 자는 금융위원회의 허가를 받아야 한다. 다만, 「은행법」에 따른 은행 그 밖에 대통령령이 정하는 금융회사는 그러하지 아니하다. <개정 2008.2.29, 2010.5.17, 2013.5.22>

②다음 각 호의 업무를 행하고자 하는 자는 금융위원회에 등록하여야 한다. 다만, 「은행법」에 따른 은행 그 밖에 대통령령이 정하는 금융회사는 그러하지 아니하다.<개정 2008.2.29, 2010.5.17, 2013.5.22>

1. 전자자금이체업무
2. 직불전자지급수단의 발행 및 관리
3. 선불전자지급수단의 발행 및 관리
4. 전자지급결제대행에 관한 업무
5. 그 밖에 대통령령이 정하는 전자금융업무

③제2항의 규정에 불구하고 다음 각 호의 어느 하나에 해당하는 자는 금융위원회에 등록하지 아니하고 같은 항 각 호의 업무를 행할 수 있다.<개정 2008.2.29>

1. 다음 각 목의 어느 하나의 경우에 해당하는 선불전자지급수단을 발행하는 자
   가. 특정한 건물 안의 가맹점 등 대통령령이 정하는 기준에 해당하는 가맹점에서만 사용되는 경우
   나. 총발행잔액이 대통령령이 정하는 금액 이하인 경우

다. 이용자가 미리 직접 대가를 지불하지 아니한 선불전자지급수단으로서 이용자에게 저장된 금전적 가치에 대한 책임을 이행하기 위하여 대통령령이 정하는 방법에 따라 상환보증보험 등에 가입한 경우

2. 자금이동에 직접 관여하지 아니하고 전자지급거래의 전자적 처리를 위한 정보만을 전달하는 업무 등 대통령령이 정하는 전자지급결제대행에 관한 업무를 수행하는 자

④제3항제1호 다목의 규정에 따라 등록이 면제된 선불전자지급수단을 발행하는 자에 대하여는 제4조, 제2장(제19조는 제외한다) 및 제3장(제21조제4항, 제21조의2, 제21조의3, 제23조 및 제25조는 제외한다), 제37조, 제38조, 제39조제1항·제6항, 제41조제1항, 제43조제2항·제3항, 제46조, 제46조의2 및 제47조의 전자금융업자에 관한 규정을 준용한다. 다만, 소속 임직원의 위법·부당한 행위로 지급불능 상태가 되는 등 대통령령이 정하는 금융사고가 발생하는 경우에는 제25조, 제39조제2항 내지 제5항 및 제40조제2항·제3항을 준용한다. <개정 2013.5.22, 2014.10.15>

⑤금융위원회는 제1항의 규정에 따른 허가에 조건을 붙일 수 있다.<개정 2008.2.29>

제29조(전자채권관리기관의 등록) ①전자채권의 등록 및 관리업무를 행하고자 하는 자는 금융위원회에 등록하여야 한다. <개정 2008.2.29>

②제21조, 제22조, 제39조, 제41조 및 제43조의 규정은 제1항의 규정에 따라 전자채권의 등록 및 관리업무를 행하기 위하여 등록한 전자채권관리기관에 대하여 이를 준용한다.

③전자채권관리기관의 전자채권 등록에 관한 절차와 방법 그 밖에 필요한 사항은 대통령령으로 정한다.

제30조(자본금) ①제28조제1항의 규정에 따라 허가를 받고자 하는 자는 주식회사로서 자본금이 50억원 이상이어야 한다.

② 제28조제2항제1호부터 제3호까지의 규정에 따라 등록할 수 있는 자는 다음 각 호의 어느 하나에 해당하는 자로 하되, 업무의 종류별로 자본금 또는 출자총액이 20억원 이상으로서 대통령령으로 정하는 금액 이상이어야 한다.<개정 2013.5.22>

1. 「상법」 제170조에서 정한 회사

2. 특별법에 따라 설립된 법인(해당 법률에서 정한 업무를 수행하기 위하여 행하는 제28조제2항제3호의 선불전자지급수단의 발행 및 관리업무로 한정한다)

③제28조제2항제4호·제5호 및 제29조의 규정에 따라 등록할 수 있는 자는 「상법」 제170조에서 정한 회사 또는 「민법」 제32조에서 정한 법인으로서 업무의 종류별로 자본금·출자총액 또는 기본재산이 다음 각 호의 구분에 따른 금액 이상이어야 한다.<개정 2016.3.29>

1. 분기별 전자금융거래 총액이 30억원 이하의 범위에서 금융위원회가 정하는 기준 이하로 운영하고자 하는 자(제29조에 따라 등록을 하고자 하는 자는 제외한다): 3억원 이상으로 대통령령으로 정하는 금액

2. 제1호 외의 자: 5억원 이상으로 대통령령으로 정하는 금액

④ 제3항제1호에 해당하는 자가 제28조에 따라 등록을 한 후 2분기 이상 계속하여 제3항제1호의 금융위원회가 정하는 기준을 초과하는 경우에는 그 내용을 금융위원회에 신고하고 금융위원회가 정하는 기한 내에 제3항제2호에서 정하는 자본금요건을 갖추어야 한다.<신설 2016.3.29>

제31조(허가 및 등록의 요건) ①제28조 및 제29조의 규정에 따라 허가를 받거나 등록을 하고자 하는 자는 다음 각 호의 요건을 모두 갖추어야 한다. 제4호 및 제5호는 허가의 경우에 한한다.

1. 제30조의 규정에 의한 자본금 또는 기본재산을 보유할 것
2. 이용자의 보호가 가능하고 행하고자 하는 업무를 수행함에 있어서 충분한 전문인력과 전산설비 등 물적 시설을 갖추고 있을 것
3. 대통령령이 정하는 재무건전성 기준을 충족할 것
4. 사업계획이 타당하고 건전할 것
5. 대통령령이 정하는 주요출자자가 충분한 출자능력, 건전한 재무상태 및 사회적 신용을 갖추고 있을 것

②제1항의 규정에 따른 허가 및 등록의 세부요건에 관하여 필요한 사항은 금융위원회가 정한다.<개정 2008.2.29>

제32조(허가와 등록의 결격사유) 다음 각 호의 어느 하나에 해당하는 자는 제28조 및 제29조의 규정에 따른 허가를 받거나 등록을 할 수 없다. <개정 2008.2.29>

1. 제34조의 규정에 따라 등록이 말소된 날부터 1년이 지나지 아니한 법인 및 그 등록이 말소될 당시 그 법인의 대주주(대통령령이 정하는 출자자를 말한다. 이하 같다)이었던 자로서 그 말소된 날부터 1년이 지나지 아니한 자
2. 제43조제1항의 규정에 따른 허가 또는 등록의 취소가 있은 날부터 3년이 지나지 아니한 법인 및 그 취소 당시 그 법인의 대주주이었던 자로서 그 취소가 있은 날부터 3년이 지나지 아니한 자
3. 「채무자 회생 및 파산에 관한 법률」에 따른 회생절차 중에 있는 회사 및 그 회사의 대주주
4. 금융거래 등 상거래에 있어서 약정한 기일 내에 채무를 변제하지 아니한 자로서 금융위원회가 정하는 자
5. 허가 또는 등록 신청일을 기준으로 최근 3년간 대통령령이 정하는 금융관계법령을 위반하여 벌금형 이상의 처벌을 받은 사실이 있는 자
6. 제1호 내지 제5호에 해당하는 자가 대주주인 법인

제33조(허가·등록 및 인가의 신청 등) ①제28조, 제29조 및 제45조에 따라 허가·인가를 받거나 등록을 하고자 하는 자는 대통령령이 정하는 바에 따라 신청서를 금융위원회에 제출하여야 한다. <개정 2008.2.29, 2013.5.22>

②금융위원회는 제1항의 규정에 따라 신청서를 접수한 때에는 대통령령이 정하는 바에 따라 허가, 등록 또는 인가를 하고 그 결과를 신청인에게 통보하여야 한다.<개정 2008.2.29, 2013.5.22>

③금융위원회는 제28조, 제29조 및 제45조에 따라 허가, 등록 또는 인가를 한 때에는 지체 없이 그 내용을 관보에 공고하고 컴퓨터통신 등을 이용하여 일반인에게 알려야 한다.<개정 2008.2.29, 2013.5.22>

[제목개정 2013.5.22]

제33조의2(예비허가) ① 제28조제1항에 따른 허가(이하 이 조에서 "본허가"라 한다)를 받으려는 자는 미리 금융위원회에 예비허가를 신청할 수 있다.

② 금융위원회는 제1항에 따른 예비허가 여부를 결정할 때에는 예비허가를 받으려는 자가 본허가 요건을 모두 충족할 수 있는지를 확인하여야 한다.

③ 금융위원회는 제2항에 따른 예비허가에 조건을 붙일 수 있다.

④ 금융위원회는 예비허가를 받은 자가 본허가를 신청하는 경우에는 제3항에 따른 예비허가 조건을 이행하였는지와 본허가 요건을 모두 충족하는지를 확인한 후 본허가 여부를 결정하여야 한다.

⑤ 예비허가에 관하여는 제33조제1항 및 제2항을 준용한다.

[본조신설 2013.5.22]

제34조(신청에 따른 등록의 말소) ①제28조제2항 및 제29조의 규정에 따라 등록을 한 자는 대통령령이 정하는 바에 따라 그 등록의 말소를 신청할 수 있다.

②금융위원회는 제1항의 규정에 따른 신청이 있는 때에는 지체 없이 그 등록을 말소한다.<개정 2008.2.29>

③금융위원회는 제2항의 규정에 따라 등록을 말소한 때에는 지체 없이 그 내용을 관보에 공고하고 컴퓨터통신 등을 이용하여 일반인에게 알려야 한다.<개정 2008.2.29>

제35조(겸업제한) ①제28조제1항의 규정에 따라 허가를 받은 전자금융업자는 다음 각 호의 업무가 아닌 업무는 이를 겸영하지 못한다.

1. 제28조제2항 각 호의 업무(등록한 경우에 한한다)
2. 제28조제1항의 규정에 따라 허가를 받은 업무 및 제1호의 업무를 행하기 위하여 필요한 업무로서 대통령령이 정하는 업무

②제1항의 규정에 불구하고 제28조제1항의 규정에 따라 허가를 받은 전자금융업자는 전자화폐 미상환잔액 전부에 대하여 대통령령이 정하는 금융회사로부터 지급보증을 받거나 상환보증보험에 가입한 경우에는 제1항 각 호의 규정에서 정한 업무 아닌 업무를 행할 수 있다.<개정 2013.5.22>

제36조(유사명칭의 사용금지) ①제2조제15호의 전자화폐가 아닌 것에는 전자화폐라는 명칭을 사용하지 못한다.

②제28조제1항의 규정에 따라 허가를 받지 아니한 자는 그 상호 중에 전자화폐라는 명칭을 사용하지 못한다.

제37조(가맹점의 준수사항 등) ①가맹점은 직불전자지급수단이나 선불전자지급수단 또는 전자화폐(이하 "전자화폐등"이라 한다)에 의한 거래를 이유로 재화 또는 용역의 제공 등을 거절하거나 이용자를 불리하게 대우하여서는 아니된다.

②가맹점은 이용자로 하여금 가맹점수수료를 부담하게 하여서는 아니 된다.

③가맹점은 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.

1. 재화 또는 용역의 제공 등이 없이 전자화폐등에 의한 거래를 한 것으로 가장(假裝)하는 행위
2. 실제 매출금액을 초과하여 전자화폐등에 의한 거래를 하는 행위
3. 다른 가맹점 이름으로 전자화폐등에 의한 거래를 하는 행위
4. 가맹점의 이름을 타인에게 빌려주는 행위
5. 전자화폐등에 의한 거래를 대행하는 행위

④가맹점이 아닌 자는 가맹점의 이름으로 전자화폐등에 의한 거래를 하여서는 아니 된다.

제38조(가맹점의 모집 등) ①금융회사 또는 전자금융업자가 가맹점을 모집하는 경우에는 가맹점이 되고자 하는 자의 영업여부 등을 확인하여야 한다. 다만, 「여신전문금융업법」 제16조의2의 규정에 따라 이미 확인을 한 가맹점인 경우에는 그러하지 아니하다. <개정 2013.5.22>

②금융회사 또는 전자금융업자는 다음 각 호의 어느 하나에 해당하는 거래에 따른 손실을 가맹점에 떠넘길 수 없다. 다만, 금융회사 또는 전자금융업자가 그 거래에 대하여 그 가맹점의 고의 또는 중대한 과실을 증명하는 경우에는 그 손실의 전부 또는 일부를 가맹점의 부담으로 할 수 있다는 취지의 계약을 가맹점과 체결한 경우에는 그러하지 아니하다.<개정 2013.5.22>

1. 분실되거나 도난된 전자화폐등에 의한 거래
2. 위조되거나 변조된 전자화폐등에 의한 거래

③금융회사 또는 전자금융업자는 다음 각 호의 사항을 금융위원회가 정하는 방법에 따라 가맹점에 알려야 한다.<개정 2008.2.29, 2013.5.22>

1. 가맹점수수료
2. 제2항의 규정에 따른 가맹점에 대한 책임
3. 제37조의 규정에 따른 가맹점의 준수사항

④금융회사 또는 전자금융업자는 가맹점이 제37조의 규정을 위반하여 형의 선고를 받거나 관계 행정기관으로부터 위반사실에 대하여 서면통보를 받는 등 대통령령이 정하는 사유에 해당하는 때에는 특별한 사유가 없는 한 지체 없이 가맹점계약을 해지하여야 한다.<개정 2013.5.22>

제5장 전자금융업무의 감독

제39조(감독 및 검사) ①금융감독원(「금융위원회의 설치 등에 관한 법률」 제24조제1항의 규정에 따른 "금융감독원"을 말한다. 이하 같다)은 금융위원회의 지시를 받아 금융회사 및 전자금융업자에 대하여 이 법 또는 이 법에 의한 명령의 준수여부를 감독한다. <개정 2008.2.29,

2013.5.22>

②금융감독원장은 제1항의 규정에 따른 감독을 위하여 필요한 때에는 금융회사 또는 전자금융업자로 하여금 그 업무 및 재무상태에 관한 보고를 하게 할 수 있다.<개정 2008.2.29, 2013.5.22, 2016.1.27>

③금융감독원장은 금융회사 및 전자금융업자의 전자금융업무와 그와 관련된 재무상태를 검사하고, 검사를 위하여 필요하다고 인정하는 때에는 금융회사 및 전자금융업자에 대하여 업무와 재무상태에 관한 자료의 제출 또는 관계인의 출석을 요구할 수 있다.<개정 2013.5.22>

④제3항의 규정에 따라 검사를 하는 자는 그 권한을 표시하는 증표를 지니고 이를 관계인에게 내보여야 한다.

⑤금융감독원장은 제3항의 규정에 따라 검사를 한 때에는 그 결과를 금융위원회가 정하는 바에 따라 금융위원회에 보고하여야 한다.<개정 2008.2.29>

⑥금융위원회는 금융회사 또는 전자금융업자가 이 법 또는 이 법에 따른 명령을 위반하여 금융회사 또는 전자금융업자의 건전한 운영을 해할 우려가 있다고 인정하는 때에는 금융감독원장의 건의에 따라 다음 각 호의 어느 하나에 해당하는 조치를 하거나 금융감독원장으로 하여금 제1호 내지 제3호에 해당하는 조치를 하게 할 수 있다.<개정 2008.2.29, 2013.5.22>

1. 위반행위에 대한 시정명령
2. 금융회사 또는 전자금융업자에 대한 주의 또는 경고
3. 임원과 직원에 대한 주의, 경고 또는 문책의 요구
4. 임원의 해임권고 또는 직무정지의 요구

제40조(외부주문등에 대한 감독 및 검사) ①금융회사 및 전자금융업자는 전자금융거래와 관련하여 전자금융보조업자와 제휴, 위탁 또는 외부주문(이하 이 조에서 "외부주문등"이라 한다)에 관한 계약을 체결하거나 변경하는 때(전자금융보조업자가 다른 전자금융보조업자와 외부주문등에 관한 계약을 체결하거나 변경하는 때를 포함한다)에는 전자금융거래의 안전성 및 신뢰성과 금융회사 및 전자금융업자의 건전성을 확보할 수 있도록 금융위원회가 정하는 기준을 준수하여야 한다. <개정 2008.2.29, 2013.5.22>

②금융위원회는 제1항의 규정에 따른 계약 내용이 금융회사 또는 전자금융업자의 경영의 건전성 및 이용자의 권익을 침해하는 것이라고 인정하는 때에는 그 금융회사 또는 전자금융업자에 대하여 관련 계약 내용의 시정 또는 보완을 지시할 수 있다.<개정 2008.2.29, 2013.5.22>

③금융감독원장은 제1항의 규정에 따른 외부주문등과 관련하여 금융회사 또는 전자금융업자에 대한 검사를 하는 경우에는 금융위원회가 정하는 기준에 따라 그 전자금융보조업자에 대한 자료제출을 요구할 수 있다.<개정 2008.2.29, 2013.5.22>

④ 금융감독원장은 전자금융보조업자가 제3항에 따른 자료를 제출하지 아니하거나 부실한 자료를 제출한 경우에는 해당 전자금융보조업자에 대하여 조사를 할 수 있다.<신설 2013.5.22>

⑤ 금융감독원장은 제4항에 따른 조사를 위하여 필요하다고 인정하는 경우에는 전자금융보조업자에게 다음 각 호의 사항을 요구할 수 있다.<신설 2013.5.22>

1. 조사사항에 관한 진술서의 제출
2. 조사에 필요한 장부·서류, 그 밖의 물건의 제출
3. 관계인의 출석

⑥ 정보기술부문의 정보보호와 관련된 업무를 위탁받은 전자금융보조업자는 해당 업무를 제3자에게 재위탁하여서는 아니 된다. 다만, 전자금융거래정보의 보호 및 안전한 처리를 저해하지 아니하는 범위에서 금융위원회가 인정하는 경우에는 그러하지 아니하다.<신설 2014.10.15>

⑦ 제4항에 따른 조사에 관하여는 제39조제4항을 준용한다.<신설 2013.5.22, 2014.10.15>

[제목개정 2013.5.22]

제41조(한국은행의 자료제출 요구 등) ①한국은행은 금융통화위원회가 전자지급거래와 관련하여 통화신용정책의 수행 및 지급결제제도의 원활한 운영을 위하여 필요하다고 인정하는 때에는 금융회사 및 전자금융업자에 대하여 자료제출을 요구할 수 있다. 이 경우 요구하는 자료는 금융회사 및 전자금융업자의 업무부담을 고려하여 필요한 최소한의 범위로 한정하여야 한다.<개정 2013.5.22>

②한국은행은 금융통화위원회가 통화신용정책의 수행을 위하여 필요하다고 인정하는 때에는 전자화폐발행자 및 제28조제2항제1호의 업무를 행하기 위하여 등록한 금융회사 및 전자금융업자에 대하여 금융감독원에 검사를 요구하거나 한국은행과의 공동검사를 요구할 수 있다.<개정 2013.5.22>

③제1항 및 제2항의 요구 방법 및 절차는 「한국은행법」 제87조 및 제88조의 규정과 「금융위원회의 설치 등에 관한 법률」 제62조의 규정을 준용한다.<개정 2008.2.29>

제42조(회계처리 구분 및 건전경영지도) ①금융회사 및 전자금융업자는 자금운용과 전자금융거래와 관련한 업무의 성과를 분석할 수 있도록 제28조제1항 및 제2항에 규정된 업무별로 다른 업무와 구분하여 회계처리하고, 금융위원회가 정하는 바에 따라 전자금융거래와 관련한 업무 및 경영실적에 관한 보고서를 작성하여 금융위원회에 제출하여야 한다. <개정 2008.2.29, 2013.5.22, 2014.10.15>

②금융위원회는 전자금융거래와 관련한 업무를 수행하는 금융회사 또는 전자금융업자의 건전경영을 지도하고 전자금융사고를 예방하기 위하여 대통령령이 정하는 바에 따라 다음 각 호의 사항에 관한 경영지도기준을 정할 수 있다.<개정 2008.2.29, 2013.5.22>

1. 자본의 적정성에 관한 사항
2. 자산의 건전성에 관한 사항
3. 유동성에 관한 사항
4. 그 밖에 경영의 건전성 확보를 위하여 필요한 사항

③금융위원회는 제28조제1항의 규정에 따라 허가를 받은 금융회사 또는 전자금융업자가 제2항의 경영지도기준을 충족하지 못하는 등 경영의 건전성을 크게 해할 우려가 있다고 인정하는 때에는 자본금의 증액, 이익배당의 제한 등 경영개선을 위하여 필요한 조치를 요구할 수 있다.<개정 2008.2.29, 2013.5.22>

④제28조제1항의 규정에 따라 허가를 받은 금융회사 또는 전자금융업자의 재무상태가 제2항의 경영지도기준에 미달하거나 거액의 금융사고 또는 부실채권의 발생으로 인하여 제2항의 경영지도기준에 미달하게 될 것이 명백하다고 판단되는 때에 필요한 조치 등에 관하여는 「금융산업의 구조개선에 관한 법률」 제10조, 제11조제1항·제4항·제5항, 제13조의2, 제14조, 제14조의2부터 제14조의4까지, 제14조의7, 제15조부터 제19조까지, 제27조 및 제28조를 준용한다.<개정 2013.5.22>

제43조(허가와 등록의 취소 등) ①금융위원회는 금융회사 또는 전자금융업자가 다음 각 호의 어느 하나에 해당하는 때에는 제28조의 규정에 따른 허가 또는 등록을 취소할 수 있다. <개정 2008.2.29, 2013.5.22>

1. 허위 그 밖의 부정한 방법으로 제28조의 규정에 따른 허가를 받거나 등록을 한 때
2. 제32조제1호 내지 제5호에 해당하는 때
3. 제2항의 규정에 따른 업무의 정지명령을 위반한 때
4. 정당한 사유 없이 1년 이상 계속하여 영업을 하지 아니한 때
5. 법인의 합병이나 파산이나 영업의 폐지 등으로 사실상 영업을 종료한 때

②금융위원회는 금융회사 또는 전자금융업자가 다음 각 호의 어느 하나에 해당하는 때에는 6월의 범위 안에서 기간을 정하여 관련 업무의 전부 또는 일부의 정지를 명할 수 있다.<개정 2008.2.29, 2013.5.22, 2016.3.29>

1. 제6조제1항·제2항, 제16조제1항부터 제4항까지, 제19조제1항, 제21조제1항·제2항, 제21조의5제2항, 제35조, 제36조 또는 제38조제3항·제4항의 규정을 위반한 때
2. 제8조제2항 및 제3항을 위반하여 오류를 조사하여 처리를 하지 아니한 때
3. 제23조, 제39조제6항, 제40조제2항 또는 제42조제3항의 규정에 따른 금융위원회의 조치나 지시 또는 명령을 어긴 때
4. 제30조제4항에서 정한 신고를 하지 아니하거나 기한 내 요건을 갖추지 아니한 때

③금융회사 또는 전자금융업자는 제1항 및 제2항의 규정에 따라 업무의 전부 또는 일부가 정지되거나 허가 또는 등록이 취소된 경우에도 그 처분 전에 행하여진 전자금융거래의 지급 및 결제를 위한 업무를 계속하여 행할 수 있다.<개정 2013.5.22>

④금융위원회는 제1항의 규정에 따라 허가 또는 등록을 취소한 때에는 지체 없이 그 내용을 관보에 공고하고 컴퓨터통신 등을 이용하여 일반인에게 알려야 한다.<개정 2008.2.29>

제44조(청문) 금융위원회는 제43조제1항의 규정에 따라 허가 또는 등록을 취소하고자 하는 경우에는 청문을 실시하여야 한다. <개정 2008.2.29>

제45조(합병·해산·폐업 등의 인가) ①제28조제1항의 규정에 따라 허가를 받은 전자금융업자가 다음 각 호의 어느 하나에 해당하는 행위를 하고자 하는 때에는 대통령령이 정하는 바에 따라 금융위원회의 인가를 받아야 한다. <개정 2008.2.29, 2013.5.22>

1. 다른 금융회사 또는 전자금융업자와의 합병

2. 해산 또는 전자금융업무의 폐지
3. 영업의 전부 또는 일부의 양도와 양수

②금융위원회는 제1항의 규정에 따른 인가에 조건을 붙일 수 있다.<개정 2008.2.29>

제45조의2(예비인가) ① 제45조제1항에 따른 인가(이하 이 조에서 "본인가"라 한다)를 받으려는 자는 미리 금융위원회에 예비인가를 신청 할 수 있다.

② 금융위원회는 제1항에 따른 예비인가 여부를 결정할 때에는 예비인가를 받으려는 자가 본인가 요건을 모두 충족할 수 있는지를 확인하여야 한다.

③ 금융위원회는 제2항에 따른 예비인가에 조건을 붙일 수 있다.

④ 금융위원회는 예비인가를 받은 자가 본인가를 신청하는 경우에는 제3항에 따른 예비인가 조건을 이행하였는지와 본인가 요건을 모두 충족하는지를 확인한 후 본인가 여부를 결정하여야 한다.

⑤ 예비인가에 관하여는 제33조제1항 및 제2항을 준용한다.

[본조신설 2013.5.22]

제46조(과징금) ① 금융위원회는 금융회사 또는 전자금융업자가 제21조제1항 또는 제2항을 위반하여 전자금융거래정보를 타인에게 제공 또는 누설하거나 업무상 목적 외에 사용한 경우에는 50억원 이하의 과징금을 부과할 수 있다. <신설 2014.10.15>

②금융위원회는 금융회사 또는 전자금융업자가 제43조제2항 각 호의 어느 하나(제1항에 따라 과징금을 부과하는 경우는 제외한다)에 해당하게 된 때에는 대통령령이 정하는 바에 따라 업무정지명령에 갈음하여 5천만원 이하의 과징금을 부과할 수 있다.<개정 2008.2.29, 2013.5.22, 2014.10.15>

③제1항 또는 제2항에 따른 과징금을 부과하는 위반행위의 종별과 정도 등에 따른 과징금의 금액 그 밖에 필요한 사항은 대통령령으로 정한다.<개정 2014.10.15>

④금융위원회는 제1항 또는 제2항에 따른 과징금을 기한 이내에 납부하지 아니하는 때에는 국세체납처분의 예에 따라 이를 징수한다.<개정 2008.2.29, 2014.10.15>

⑤금융위원회는 대통령령이 정하는 바에 따라 과징금의 징수 및 체납처분에 관한 업무를 국세청장에게 위탁할 수 있다.<개정 2008.2.29, 2014.10.15>

제46조의2(과오납금의 환급) ① 금융위원회는 과징금납부의무자가 이의신청의 재결 또는 법원의 판결 등의 사유로 과징금 과오납금의 환급을 청구하는 경우에는 지체 없이 환급하여야 하며, 과징금납부의무자의 청구가 없는 경우에도 금융위원회가 확인한 과오납금은 환급하여야 한다.

② 금융위원회는 제1항에 따라 과오납금을 환급하는 경우 환급받을 자가 금융위원회에 납부하여야 하는 다른 과징금이 있으면 환급하는 금액을 그 과징금에 충당할 수 있다.

③ 금융위원회가 제1항에 따라 과오납금을 환급하는 경우에는 과징금을 납부한 날의 다음 날부터 환급하는 날까지의 기간에 대하여 대통령령으로 정하는 가산금 이율을 적용하여 산정한 환급가산금을 환급받을 자에게 지급하여야 한다.

[본조신설 2013.5.22]

제6장 보칙

제47조(전자금융거래 통계조사) ①한국은행은 전자금융거래의 현황 파악과 효과적인 통화신용정책의 수립 및 시행을 위하여 전자금융업 및 전자금융거래에 관한 통계조사를 할 수 있다. 이 경우 필요한 자료를 정부기관, 금융회사등과 전자금융거래 관련 법인과 단체에 요구할 수 있다. <개정 2013.5.22>

②제1항의 규정에 따라 자료의 제출을 요구받은 정부기관, 금융회사등과 전자금융거래 관련 법인과 단체는 정당한 사유가 없는 한 이에 응하여야 한다.<개정 2013.5.22>

③제1항의 규정에 따른 통계조사의 대상과 방법 및 절차에 관하여 필요한 사항은 대통령령으로 정한다.

제48조(권한의 위탁) 금융위원회는 이 법에 따른 권한의 일부를 대통령령이 정하는 바에 따라 금융감독원장에게 위탁할 수 있다. <개정 2008.2.29>

제7장 벌칙

제49조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다. <신설 2014.10.15>

1. 제21조의4제1호를 위반하여 전자금융기반시설에 접근하거나 저장된 데이터를 조작·파괴·은닉 또는 유출한 자
2. 제21조의4제2호를 위반하여 데이터를 파괴하거나 컴퓨터 바이러스, 논리폭탄 또는 메일폭탄 등의 프로그램을 투입한 자
3. 제21조의4제3호를 위반하여 일시에 대량의 신호, 고출력 전자기파 또는 데이터를 보내거나 전자금융기반시설에 오류 또는 장애를 발생시킨 자
4. 제26조를 위반하여 전자금융거래정보를 타인에게 제공 또는 누설하거나 업무상 목적 외에 사용한 자(제28조제4항에 따라 이를 준용하는 선불전자지급수단을 발행하는 자를 포함한다)

②다음 각 호의 어느 하나에 해당하는 자는 7년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.<개정 2013.5.22, 2014.10.15>

1. 접근매체를 위조하거나 변조한 자
2. 위조되거나 변조된 접근매체를 판매알선·판매·수출 또는 수입하거나 사용한 자
3. 분실되거나 도난된 접근매체를 판매알선·판매·수출 또는 수입하거나 사용한 자
4. 전자금융기반시설 또는 전자금융거래를 위한 전자적 장치에 침입하여 거짓이나 그 밖의 부정한 방법으로 접근매체를 획득하거나 획득한 접근매체를 이용하여 전자금융거래를 한 자

5. 강제로 빼앗거나, 횡령하거나, 사람을 속이거나 공갈하여 획득한 접근매체를 판매알선ㆍ판매ㆍ수출 또는 수입하거나 사용한 자
6. 삭제 <2014.10.15>

③전자화폐는 「형법」 제214조 내지 제217조에 정한 죄의 유가증권으로 보아 각 그 죄에 정한 형으로 처벌한다.<개정 2014.10.15>

④다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.<개정 2008.12.31., 2015.1.20, 2016.1.27>

1. 제6조제3항제1호를 위반하여 접근매체를 양도하거나 양수한 자
2. 제6조제3항제2호 또는 제3호를 위반하여 접근매체를 대여받거나 대여한 자 또는 보관ㆍ전달ㆍ유통한 자
3. 제6조제3항제4호를 위반한 질권설정자 또는 질권자
4. 제6조제3항제5호를 위반하여 알선하거나 광고하는 행위를 한 자
5. 제28조 또는 제29조의 규정에 따라 허가를 받거나 등록을 하지 아니하고 그 업무를 행한 자
6. 허위 그 밖의 부정한 방법으로 제28조 또는 제29조의 규정에 따라 허가를 받거나 등록을 한 자
7. 제37조제3항제3호의 규정을 위반하여 다른 가맹점의 이름으로 전자화폐등에 의한 거래를 한 자
8. 제37조제3항제5호의 규정을 위반하여 전자화폐등에 의한 거래를 대행한 자
9. 제37조제4항의 규정을 위반하여 가맹점의 이름으로 전자화폐등에 의한 거래를 한 자
10. 허위 그 밖의 부정한 방법으로 전자금융거래정보를 열람하거나 제공받은 자

⑤다음 각 호의 어느 하나에 해당하는 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

1. 삭제 <2008.12.31>
2. 삭제 <2013.5.22>
3. 제37조제1항의 규정을 위반하여 전자화폐등에 의한 거래를 이유로 재화 또는 용역의 제공을 거절하거나 이용자를 불리하게 대우한 자
4. 제37조제2항의 규정을 위반하여 이용자에게 가맹점수수료를 부담하게 한 자
5. 제37조제3항제4호의 규정을 위반하여 가맹점의 이름을 타인에게 빌려준 자
6. 제45조제1항의 규정에 따른 인가를 받지 아니하고 동항 각 호의 어느 하나에 해당하는 행위를 한 자

⑥ 제1항제1호ㆍ제2호 및 제3호와 제2항제1호ㆍ제2호 및 제4호의 미수범은 처벌한다.<개정 2014.10.15>

⑦제1항 내지 제6항의 징역형과 벌금형은 병과할 수 있다.

제50조(양벌규정) ① 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제49조제1항, 제2항, 제3항(「형법」 제216조에서 정한 형

으로 처벌하는 경우로 한정한다), 제4항부터 제6항까지의 어느 하나에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형을 과(科)한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다. <개정 2014.10.15>

② 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제49조제3항(「형법」 제214조, 제215조 또는 제217조에서 정한 형으로 처벌하는 경우로 한정한다)의 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인을 5천만원 이하의 벌금에 처한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.<개정 2014.10.15>

[전문개정 2011.11.14]

제51조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다. <개정 2014.10.15>

1. 제21조제1항 또는 제2항을 위반하여 선량한 관리자로서의 주의를 다하지 아니하거나 금융위원회가 정하는 기준을 준수하지 아니한 자
2. 제36조를 위반하여 전자화폐의 명칭을 사용한 자

② 다음 각 호의 어느 하나에 해당하는 자(제3호의 경우에는 제28조제4항에 따라 해당 규정을 준용하는 선불전자지급수단을 발행하는 자를 포함한다)에게는 2천만원 이하의 과태료를 부과한다.<개정 2014.10.15>

1. 제13조제2항을 위반하여 전자자금이체의 지급 효력이 발생하도록 하지 아니한 자
2. 제21조의3제1항을 위반하여 전자금융기반시설의 취약점을 분석·평가하지 아니한 자
3. 제21조의3제2항을 위반하여 보완조치의 이행계획을 수립·시행하지 아니한 자
4. 제22조제2항을 위반하여 전자금융거래기록을 파기하지 아니한 자
5. 제40조제6항을 위반하여 제3자에게 재위탁을 한 자

③ 다음 각 호의 어느 하나에 해당하는 자(제1호, 제6호부터 제8호까지, 제10호 및 제11호의 경우에는 제28조제4항에 따라 해당 규정을 준용하는 선불전자지급수단을 발행하는 자를 포함한다)에게는 1천만원 이하의 과태료를 부과한다.

1. 제7조제2항을 위반하여 거래내용에 관한 서면을 교부하지 아니한 자
2. 제8조제2항 및 제3항을 위반하여 오류의 원인과 처리 결과를 알리지 아니한 자
3. 제18조제2항을 위반하여 선불전자지급수단 또는 전자화폐를 양도하거나 담보로 제공한 자
4. 제21조제4항을 위반하여 정보기술부문에 대한 계획을 제출하지 아니한 자
5. 제21조의3제1항을 위반하여 전자금융기반시설의 취약점 분석·평가의 결과를 보고하지 아니한 자
6. 제21조의5제1항을 위반하여 침해사고를 알리지 아니한 자
7. 제22조제1항(제29조제2항에서 준용하는 경우를 포함한다)을 위반하여 기록을 생성하거나 보존하지 아니한 자

8. 제24조제1항 또는 제3항을 위반하여 약관의 명시, 설명, 교부를 하지 아니하거나 게시 또는 통지하지 아니한 자
9. 제25조제1항을 위반하여 금융위원회에 보고하지 아니한 자
10. 제27조제1항을 위반하여 분쟁처리 절차를 마련하지 아니한 자
11. 제39조제3항(제29조제2항에서 준용하는 경우를 포함한다) 및 제40조제3항·제4항에 따른 검사, 자료제출 및 조사를 거부 또는 방해하거나 기피한 자
12. 제42조제1항을 위반하여 회계처리의 구분을 하지 아니한 자 또는 보고서를 제출하지 아니하거나 허위의 보고서를 제출한 자

④ 제1항부터 제3항까지의 규정에 따른 과태료는 금융위원회가 부과·징수한다.

[전문개정 2013.5.22]

부칙 <제7929호,2006.4.28>

제1조 (시행일) 이 법은 2007년 1월 1일부터 시행한다.

제2조 (접근매체 등에 관한 경과조치) 이 법 시행당시 발행된 접근매체 및 전자지급수단은 이 법에 따라 발행된 것으로 본다.

제3조 (허가 및 등록에 관한 경과조치) ①이 법 시행당시 전자화폐를 발행하거나 관리하고 있는 자는 이 법 시행일부터 3월 이내에 제28조제1항의 규정에 따라 금융감독위원회의 허가를 받아야 한다.

②이 법 시행당시 전자자금이체업무, 직불전자지급수단 또는 선불전자지급수단의 발행 및 관리, 전자지급결제대행에 관한 업무 등을 수행하고 있는 자는 이 법 시행일부터 6월 이내에 제28조제2항의 규정에 따라 금융감독위원회에 등록하여야 한다.

③이 법 시행당시 전자채권관리기관의 업무를 행하고 있는 자는 이 법 시행일부터 3월 이내에 제29조의 규정에 따라 금융감독위원회에 등록하여야 한다.

제4조 (다른 법률의 개정) 「여신전문금융업법」 일부를 다음과 같이 개정한다.

제17조제1항제1호중 "신용카드 또는 직불카드"를 "신용카드"로 한다.

제17조제1항제2호중 "신용카드등"을 "신용카드"로 한다.

제19조제3항중 "신용카드회원등"을 "신용카드회원"으로 한다.

제19조제4항제3호 및 제5호중 "신용카드등"을 각각 "신용카드"로 한다.

제22조를 삭제한다.

제57조제1항제2호중 "제21조·제22조"를 "제21조"로 한다.

제70조제2항제4호·제5호중 "신용카드등"을 각각 "신용카드"로 한다.

제70조제3항제3호중 "신용카드회원등"을 "신용카드회원"으로 한다.

부칙 <제8387호,2007.4.27>

제1조 (시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다.

제2조부터 제7조 생략

제8조 (다른 법률의 개정) ①부터 ⑨생략

⑩전자금융거래법 일부를 다음과 같이 개정한다.

제2조제14호나목 중 "「통계법」 제17조제1항"을 "「통계법」 제22조제1항"으로 한다.

⑪부터 ⑭생략

제9조 생략

부칙 <제8863호,2008.2.29>

제1조(시행일) 이 법은 공포한 날부터 시행한다.

제2조부터 제4조까지 생략

제5조(다른 법률의 개정) ① 부터 <36> 까지 생략

<37> 전자금융거래법 일부를 다음과 같이 개정한다.

제2조제3호가목 중 "「금융감독기구의 설치 등에 관한 법률」"을 "「금융위원회의 설치 등에 관한 법률」"로 하고, 같은 조 제5호 중 "「금융감독기구의 설치 등에 관한 법률」제3조의 규정에 따른 금융감독위원회(이하 "금융감독위원회"라 한다)"를 "「금융위원회의 설치 등에 관한 법률」제3조에 따른 금융위원회(이하 "금융위원회"라 한다)"로 한다.

제39조제1항 중 "금융감독원(「금융감독기구의 설치 등에 관한 법률」제24조제1항"을 "금융감독원(「금융위원회의 설치 등에 관한 법률」제24조제1항"으로, "금융감독위원회의"를 "금융위원회의"로 하고, 같은 조 제2항 중 "금융감독원장(「금융감독기구의 설치 등에 관한 법률」 제29조제1항"을 "금융감독원장(「금융위원회의 설치 등에 관한 법률」 제29조제1항"으로 한다.

제41조제3항 중 "「금융감독기구의 설치 등에 관한 법률」 제62조"를 "「금융위원회의 설치 등에 관한 법률」 제62조"로 한다.

제9조제4항, 제21조제2항·제3항, 제23조 각 호 외의 부분, 제24조제1항·제3항, 제25조제1항부터 제3항까지, 제28조제1항부터 제3항까지·제5항, 제29조제1항, 제31조제2항, 제32조제4호, 제33조제1항부터 제3항까지, 제34조제2항·제3항, 제38조제3항 각 호 외의 부분, 제39조제5항·제6항, 제40조제1항부터 제3항까지, 제42조제1항부터 제3항까지, 제43조제1항·제2항·제4항, 제44조, 제45조제1항 각 호 외의 부분, 같은 조 제2항, 제46조제1항·제3항·제4항, 제48조 및 제51조제2항부터 제4항까지 중 "금융감독위원회"를 각각 "금융위원회"로 한다.

<38> 부터 <85> 까지 생략

부칙 <제9325호,2008.12.31>

이 법은 공포 후 3개월이 경과한 날부터 시행한다.

부칙 <제10303호,2010.5.17>

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다. <단서 생략>

제2조부터 제8조까지 생략

제9조(다른 법률의 개정) ① 부터 <58> 까지 생략

<59> 전자금융거래법 일부를 다음과 같이 개정한다.

제28조제1항 단서 및 같은 조 제2항 각 호 외의 부분 단서 중 "「은행법」에 따른 금융기관"을 각각 "「은행법」에 따른 은행"으로 한다.

<60> 부터 <86> 까지 생략

제10조 생략

부칙 <제11087호,2011.11.14>

이 법은 공포 후 6개월이 경과한 날부터 시행한다.

부칙 <제11407호,2012.3.21>

제1조(시행일) 이 법은 공포한 날부터 시행한다. <단서 생략>

제2조 생략

제3조(다른 법률의 개정) ① 및 ② 생략

③ 전자금융거래법 일부를 다음과 같이 개정한다.

제2조제3호가목을 다음과 같이 한다.

가. 「금융위원회의 설치 등에 관한 법률」 제38조제1호부터 제5호까지, 제7호 및 제8호에 해당하는 기관

부칙 <제11461호,2012.6.1>

제1조(시행일) 이 법은 공포 후 3개월이 경과한 날부터 시행한다.

제2조부터 제9조까지 생략

제10조(다른 법률의 개정) ①부터 ⑭까지 생략

⑮ 전자금융거래법 일부를 다음과 같이 개정한다.

제2조제9호 중 "「전자거래기본법」 제2조제1호의 규정"을 "「전자문서 및 전자거래 기본법」 제2조제1호"로 한다.

제2조제16호마목 중 "「전자거래기본법」 제6조제1항의 규정"을 "「전자문서 및 전자거래 기본법」 제6조제1항"으로 한다.

제5조제1항 중 "「전자거래기본법」 제4조 내지 제7조, 제9조 및 제10조의 규정을"을 "「전자문서 및 전자거래 기본법」 제4조부터 제7조까지, 제9조 및 제10조를"로 한다.

<16>부터 <25>까지 생략

부칙 <제11814호,2013.5.22>

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다.

제2조(정보기술부문에 대한 계획의 제출에 관한 적용례) 제21조제4항의 개정규정에 따른 정보기술부문에 대한 계획의 제출은 이 법 시행 후 개시되는 사업연도부터 적용한다.

제3조(벌칙 및 과태료에 관한 경과조치) 이 법 시행 전의 위반행위에 대하여 벌칙 및 과태료를 적용할 때에는 종전의 규정에 따른다.

부칙 <제12837호,2014.10.15>

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다. 다만, 제13조제2항과 제21조제2항 및 제3항의 개정규정은 공포 후 1년이 경과한 날부터 시행한다.

제2조(정보보호최고책임자의 겸직금지에 관한 적용례) 제21조의2제3항의 개정규정은 이 법 시행 후 선임(재선임되는 경우를 포함한다)되는 정보보호최고책임자부터 적용한다.

제3조(정보보호와 관련된 업무의 재위탁 금지에 관한 적용례) 제40조제6항의 개정규정은 이 법 시행 후 재위탁하거나 재위탁 기간을 연장하는 것부터 적용한다.

제4조(과징금의 부과에 관한 적용례) 제46조제1항의 개정규정은 이 법 시행 후 위반행위를 한 금융회사 또는 전자금융업자부터 적용한다.

제5조(벌칙 및 과태료에 관한 경과조치) 이 법 시행 전의 행위에 대하여 벌칙 및 과태료를 적용할 때에는 종전의 규정에 따른다.

부칙 <제13069호,2015.1.20>

제1조(시행일) 이 법은 공포한 날부터 시행한다.

제2조(벌칙에 관한 경과조치) 이 법 시행 전의 행위에 대하여 벌칙을 적용할 때에는 종전의 규정에 따른다.

부칙 <제13929호,2016.1.27>

이 법은 공포한 날부터 시행한다. 다만, 제6조의2의 개정규정은 공포 후 6개월이 경과한 날부터 시행한다.

부칙 <제14132호,2016.3.29>

이 법은 공포 후 3개월이 경과한 날부터 시행한다.

전자금융거래법 시행령

[시행 2016.9.30] [대통령령 제27205호, 2016.5.31, 타법개정]

제1조(목적) 이 영은 「전자금융거래법」에서 위임된 사항과 그 시행에 관하여 필요한 사항을 규정함을 목적으로 한다.

제2조(금융회사의 범위) 「전자금융거래법」(이하 "법"이라 한다) 제2조제3호마목에서 "대통령령이 정하는 자"라 함은 다음 각 호의 어느 하나에 해당하는 자를 말한다. <개정 2008.7.29, 2009.5.29, 2009.10.1, 2013.11.22, 2016.5.31>

1. 「한국산업은행법」에 따른 한국산업은행

1의2. 삭제 <2014.12.30>

2. 「중소기업은행법」에 따른 중소기업은행
3. 「한국수출입은행법」에 따른 한국수출입은행
4. 「산림조합법」에 따른 조합과 그 중앙회의 신용사업부문
5. 「농업협동조합법」에 따른 조합
6. 「수산업협동조합법」에 따른 조합
7. 「자본시장과 금융투자업에 관한 법률」에 따른 거래소
8. 「자본시장과 금융투자업에 관한 법률」에 따른 한국예탁결제원
9. 「금융지주회사법」에 따른 금융지주회사와 「금융지주회사법 시행령」 제2조제2항제1호에 해당하는 회사
10. 「보험업법」에 따른 보험협회와 보험요율산출기관
11. 「화재로 인한 재해보상과 보험가입에 관한 법률」에 따른 한국화재보험협회
12. 「자본시장과 금융투자업에 관한 법률」에 따른 한국금융투자협회
13. 삭제 <2008.7.29>
14. 「신용정보의 이용 및 보호에 관한 법률」에 따른 신용정보회사와 종합신용정보집중기관
15. 「금융회사부실자산 등의 효율적 처리 및 한국자산관리공사의 설립에 관한 법률」에 따른 한국자산관리공사
16. 「한국주택금융공사법」에 따른 한국주택금융공사
17. 「신용보증기금법」에 따른 신용보증기금
18. 「기술보증기금법」에 따른 기술보증기금

[제목개정 2013.11.22]

제3조(선불전자지급수단의 요건) 법 제2조제14호가목에서 "대통령령이 정하는 특수관계인"이라 함은 발행인과 다음 각 호의 어느 하나에 해당하는 관계에 있는 자를 말한다.

1. 「상법」 제342조의2에 따른 모회사 또는 자회사
2. 「독점규제 및 공정거래에 관한 법률」 제2조제1호의2 또는 제1호의3에 따른 지주회사 또는 자회사
3. 「금융지주회사법」 제2조제1항제1호에 따른 금융지주회사 또는 동항제2호에 따른 자회사

제4조(전자화폐의 범용성 요건) ①법 제2조제15호가목에서 "대통령령이 정하는 기준 이상의 지역 및 가맹점"이라 함은 2개 이상의 광역지방자치단체(「지방자치법」 제2조제1항제1호에 따른 지방자치단체를 말한다. 이하 같다) 및 500개 이상의 가맹점을 말한다.
②법 제2조제15호다목에서 "대통령령이 정하는 업종 수"라 함은 5개 업종을 말한다.

제5조(적용범위의 예외) ①법 제3조제1항 단서에서 "대통령령이 정하는 경우"라 함은 다음 각 호의 어느 하나에 해당하는 경우를 말한다. <개정 2013.11.22>
1. 법 제2조제6호에 따른 결제중계시스템을 이용하는 전자금융거래
2. 「한국은행법」 제81조제1항에 따라 한국은행이 운영하는 지급결제제도를 이용하는 전자금융거래

② 법 제3조제3항 각 호 외의 부분에서 "대통령령으로 정하는 금융회사"란 다음 각 호의 어느 하나에 해당하는 금융회사로서 법 제2조제1호에 따른 전자금융업무를 하지 아니하는 금융회사를 말한다.<신설 2013.11.22>
1. 법 제2조제3호가목부터 라목까지의 금융회사
2. 제2조제4호부터 제6호까지의 금융회사
3. 제2조제14호에 따른 신용정보회사

제6조(접근매체의 갱신 또는 대체발급) 금융회사 또는 전자금융업자는 법 제6조제2항 각 호 외의 부분 단서 및 같은 항 제2호에 따라 다음 각 호의 어느 하나에 해당하는 경우에는 이용자의 신청이나 본인의 확인이 없는 때에도 접근매체를 갱신 또는 대체발급할 수 있다. <개정 2013.11.22>
1. 갱신 또는 대체발급 예정일 전 6월 이내에 사용된 적이 없는 접근매체는 이용자로부터 갱신 또는 대체발급에 대하여 서면동의[「전자서명법」 제2조제3호에 따른 공인전자서명(이하 "공인전자서명"이라 한다)이 있는 전자문서에 의한 동의를 포함한다]를 얻은 경우
2. 갱신 또는 대체발급 예정일 전 6월 이내에 사용된 적이 있는 접근매체는 그 예정일부터 1월 이전에 이용자에게 발급 예정사실을 알린 후 20일 이내에 이용자로부터 이의 제기가 없는 경우

제6조의2(이의신청의 절차 등) ① 법 제6조의2제1항에 따른 요청으로 전기통신역무 제공이 중지된 사람이 같은 조 제2항에 따라 이의신청을 하려면 전기통신역무 제공이 중지된 날부터 30일 이내에 다음 각 호의 사항을 적은 문서를 같은 조 제1항에 따른 전기통신역무 제공의 중지를 요청한 기관(이하 이 조에서 "제공중지요청기관"이라 한다)에 제출하여야 한다.

1. 이의신청인의 명칭 또는 성명과 주소 및 연락처
2. 이의신청의 사유
3. 전기통신역무 제공이 중지된 날

② 제공중지요청기관은 제1항에 따라 이의신청을 받은 날부터 15일 이내에 그 이의신청에 대하여 결정을 하고 그 결과를 이의신청인에게 문서로 통지하여야 한다. 다만, 부득이한 사유로 그 기간 이내에 결정을 할 수 없을 때에는 15일의 범위에서 그 기간을 연장할 수 있으며, 연장 사유와 연장기간을 이의신청인에게 통지하여야 한다.

③ 제공중지요청기관은 제1항에 따라 제출된 문서에 흠결이 있거나 추가적인 사실 확인이 필요한 경우 보완을 요청할 수 있다. 이 경우 그 보완에 소요된 기간은 제2항 본문의 기간에 산입(算入)되지 아니한다.

④ 제공중지요청기관은 법 제6조의2제2항에 따른 이의신청이 이유가 있다고 인정할 때에는 지체 없이 미래창조과학부장관에게 해당 전기통신역무 제공의 중지를 해제하도록 요청하여야 한다.

[본조신설 2016.6.28]

제7조(거래내용의 확인 등) ①금융회사 또는 전자금융업자는 법 제7조제1항에 따라 이용자가 전자적 장치를 통하여 거래내용을 확인할 수 있도록 하는 경우에 전자적 장치의 운영장애, 그 밖의 사유로 거래내용을 확인하게 할 수 없는 때에는 인터넷 등을 이용하여 즉시 그 사유를 알리고, 그 사유가 종료된 때부터 이용자가 거래내용을 확인할 수 있도록 하여야 한다. <개정 2013.11.22>

②금융회사 또는 전자금융업자는 법 제7조제2항에 따라 이용자로부터 거래내용을 서면(전자문서를 제외한다. 이하 같다)으로 제공할 것을 요청받은 경우 전자적 장치의 운영장애, 그 밖의 사유로 거래내용을 제공할 수 없는 때에는 그 이용자에게 즉시 이를 알려야 한다. 이 경우 법 제7조제2항의 거래내용에 관한 서면의 교부기간을 산정함에 있어서 전자적 장치의 운영장애, 그 밖의 사유로 거래내용을 제공할 수 없는 기간은 산입하지 아니한다.<개정 2013.11.22>

③법 제7조제3항에 따른 거래내용의 대상기간은 제12조제1항 각 호에 따른 전자금융거래기록의 보존기간으로 한다.<개정 2015.4.14>

④법 제7조제3항에 따른 거래내용의 종류(조회거래를 제외한다. 이하 이 조에서 같다) 및 범위는 다음 각 호와 같다.<개정 2008.2.29, 2013.11.22>

1. 전자금융거래의 종류(보험계약의 경우에는 보험계약의 종류를 말한다) 및 금액, 전자금융거래의 상대방에 관한 정보
2. 전자금융거래의 거래일시, 전자적 장치의 종류 및 전자적 장치를 식별할 수 있는 정보
3. 전자금융거래가 계좌를 통하여 이루어지는 경우 거래계좌의 명칭 또는 번호(보험계약의 경우에는 보험증권번호를 말한다)
4. 금융회사 또는 전자금융업자가 전자금융거래의 대가로 받은 수수료
5. 법 제15조제1항에 따른 지급인의 출금 동의에 관한 사항

6. 그 밖에 이용자의 전자금융거래내용 확인에 필요한 사항으로서 금융위원회가 정하여 고시하는 사항

⑤금융회사 또는 전자금융업자는 법 제7조제2항에 따른 거래내용의 서면 제공과 관련하여 그 요청의 방법·절차, 접수창구의 주소(전자우편주소를 포함한다) 및 전화번호 등을 전자금융거래와 관련한 약관(이하 "약관"이라 한다)에 규정하여야 한다.<개정 2013.11.22>

제7조의2(오류의 정정 통지 방법) 법 제8조제2항 및 제3항에서 "대통령령으로 정하는 방법"이란 문서, 전화 또는 전자우편으로 알리는 것을 말한다. 다만, 이용자가 문서로 알려줄 것을 요청하는 경우에는 문서로 알려야 한다. <개정 2013.11.22>

[본조신설 2009.3.31]

제8조(고의나 중대한 과실의 범위) 법 제9조제3항에 따른 고의나 중대한 과실의 범위는 다음 각 호와 같다 <개정 2013.11.22>

1. 이용자가 접근매체를 제3자에게 대여하거나 그 사용을 위임한 경우 또는 양도나 담보의 목적으로 제공한 경우(법 제18조에 따라 선불전자지급수단이나 전자화폐를 양도하거나 담보로 제공한 경우를 제외한다)
2. 제3자가 권한 없이 이용자의 접근매체를 이용하여 전자금융거래를 할 수 있음을 알았거나 쉽게 알 수 있었음에도 불구하고 접근매체를 누설하거나 노출 또는 방치한 경우
3. 금융회사 또는 전자금융업자가 법 제6조제1항에 따른 확인 외에 보안강화를 위하여 전자금융거래 시 요구하는 추가적인 보안조치를 이용자가 정당한 사유 없이 거부하여 법 제9조제1항제3호에 따른 사고가 발생한 경우
4. 이용자가 제3호에 따른 추가적인 보안조치에 사용되는 매체·수단 또는 정보에 대하여 다음 각 목의 어느 하나에 해당하는 행위를 하여 법 제9조제1항제3호에 따른 사고가 발생한 경우

가. 누설·노출 또는 방치한 행위

나. 제3자에게 대여하거나 그 사용을 위임한 행위 또는 양도나 담보의 목적으로 제공한 행위

제9조(선불전자지급수단이나 전자화폐의 분실과 도난 책임) 법 제10조제1항 단서에서 "대통령령이 정하는 경우"라 함은 선불전자지급수단이나 전자화폐의 분실 또는 도난의 통지를 하기 전에 저장된 금액에 대한 손해에 대하여 그 책임을 이용자의 부담으로 할 수 있다는 취지의 약정이 금융회사 또는 전자금융업자와 이용자 간에 미리 체결된 경우를 말한다. <개정 2013.11.22>

제9조의2(전자자금이체의 지급 효력 발생시기의 지연) ① 법 제13조제2항에서 "대통령령으로 정하는 금융회사 또는 전자금융업자"란 법 제28조제2항에 따라 같은 항 제1호의 전자자금이체업무를 수행하는 금융회사 또는 전자금융업자를 말한다.

② 제1항에 따른 금융회사 또는 전자금융업자는 법 제13조제2항에 따라 거래지시를 하는 때부터 일정 시간이 경과한 후에 전자자금이체의 지급 효력이 발생(이하 이 항에서 "지연이체

"라 한다)하기를 원하는 이용자가 컴퓨터, 전화기, 그 밖에 금융위원회가 정하여 고시하는 전자적 장치를 통하여 지연이체가 되는 거래지시를 할 수 있도록 하여야 한다.

[본조신설 2015.4.14]

제10조(출금 동의의 방법) 법 제15조제1항에 따라 지급인으로부터 출금에 대한 동의를 얻는 방법은 다음 각 호와 같다. <개정 2008.7.9, 2012.5.7, 2013.11.22>

1. 금융회사 또는 전자금융업자가 지급인으로부터 서면(금융위원회가 정하여 고시하는 전자문서를 포함한다. 이하 이 조에서 같다) 또는 녹취 등 금융위원회가 정하는 방법으로 출금 동의를 받는 방법
2. 수취인이 지급인으로부터 서면 또는 녹취 등 금융위원회가 정하는 방법으로 출금 동의를 받아 금융회사 또는 전자금융업자에게 전달(전자적 방법으로 출금의 동의내역을 전송하는 것을 포함한다)하는 방법

제11조(전자화폐의 발행 및 환금방법) ①법 제16조제1항 단서에서 "대통령령이 정하는 금액"이라 함은 5만원을 말한다.

②전자화폐발행자는 법 제16조제1항·제2항 및 제4항에 따라 전자화폐를 발행하거나 현금 또는 예금과 교환하는 경우에는 그 전자화폐발행자의 중앙전산시스템을 경유하여야 하며, 다음 각 호의 사항을 기록·관리하여야 한다. 다만, 법 제16조제1항 단서에 따른 전자화폐의 경우에는 전자화폐발행자의 중앙전산시스템을 경유하지 아니할 수 있으며, 제2호의 사항을 기록·관리하지 아니할 수 있다.

1. 전자화폐의 발행 또는 교환의 일시와 금액
2. 전자화폐의 발행신청인 또는 교환신청인
3. 전자화폐 접근매체의 식별번호
4. 그 밖에 전자화폐의 발행 또는 교환에 관한 사항

③전자화폐발행자는 전자화폐보유자가 전자화폐를 현금 또는 예금으로 교환하여 줄 것을 요청하는 경우에는 이를 발행하는 모든 장소에서 그 교환에 응하여야 한다. 다만, 법 제16조제1항 단서에 따른 전자화폐의 경우 교환의 편의성을 해치지 아니하는 범위에서 그 이용자에게 교환장소를 별도로 정하여 알린 경우에는 그 장소에서만 교환에 응할 수 있다.

④전자화폐발행자는 전자화폐보유자가 교환을 요구하면 교환요구금액 전부를 즉시 현금으로 지급하거나 전자화폐보유자의 예금계좌로 지급하여야 한다. 다만, 전자화폐의 파손 등으로 인하여 교환요구금액을 확인할 수 없으면 교환을 요구받은 날부터 15일 이내에 해당 전자화폐 가맹점의 대금청구와 이에 따른 결제내역 등을 확인한 후 즉시 그 금액을 지급하여야 한다.

제11조의2(정보기술부문 계획수립의 대상 금융회사 등) ① 법 제21조제4항에서 "대통령령으로 정하는 금융회사 및 전자금융업자"란 다음 각 호의 자를 말한다.

1. 법 제2조제3호가목·나목·마목의 금융회사
2. 전자금융업자

② 법 제21조제4항에 따른 정보기술부문에 대한 계획에는 다음 각 호의 사항이 포함되어야 한다.

1. 정보기술부문의 추진목표 및 추진전략
2. 정보기술부문의 직전 사업연도 추진실적 및 해당 사업연도 추진계획
3. 정보기술부문의 조직 등 운영 현황
4. 정보기술부문의 직전 사업연도 및 해당 사업연도 예산
5. 그 밖에 안전한 전자금융거래를 위하여 정보기술부문에 필요한 사항으로서 금융위원회가 정하여 고시하는 사항

③ 법 제21조제4항에 따른 정보기술부문에 대한 계획은 매 사업연도 초일(初日)부터 3개월 이내에 금융위원회에 제출하여야 한다.

④ 제2항에 따라 정보기술부문에 대한 계획에 포함되어야 하는 사항의 세부내용이나 제출방법 등에 관하여 필요한 사항은 금융위원회가 정하여 고시한다.

[본조신설 2013.11.22]

[종전 제11조의2는 제11조의3으로 이동 <2013.11.22>]

제11조의3(정보보호최고책임자 지정대상 금융회사 등) ① 법 제21조의2제2항에서 "대통령령으로 정하는 금융회사 또는 전자금융업자"란 직전 사업연도 말을 기준으로 총자산이 2조원 이상이고, 상시 종업원 수가 300명 이상인 금융회사 또는 전자금융업자를 말한다. 이 경우 상시 종업원 수의 산정방식은 금융위원회가 정하여 고시한다. <개정 2013.11.22>

② 법 제21조의2제3항에서 "대통령령으로 정하는 금융회사 또는 전자금융업자"란 직전 사업연도 말을 기준으로 총자산이 10조원 이상이고, 상시 종업원 수가 1,000명 이상인 금융회사를 말한다. 이 경우 상시 종업원 수의 산정방식은 제1항 후단을 준용한다.<신설 2015.4.14>

③ 법 제21조의2제4항제5호에서 "대통령령으로 정하는 사항"이란 다음 각 호의 사항을 말한다.<신설 2013.11.22, 2015.4.14>

1. 전자금융업무 및 그 기반이 되는 정보기술부문 보안을 위한 자체심의에 관한 사항
2. 정보기술부문 보안에 관한 임직원 교육에 관한 사항

④ 법 제21조의2제5항에 따른 정보보호최고책임자의 자격요건은 별표 1과 같다.<개정 2013.11.22, 2015.4.14>

[본조신설 2012.5.7]

[제목개정 2013.11.22]

[제11조의2에서 이동 <2013.11.22>]

제11조의4(전자금융기반시설 취약점 분석·평가의 내용) 법 제21조의3제1항제4호에서 "대통령령으로 정하는 사항"이란 다음 각 호의 사항을 말한다.

1. 정보기술부문과 연계된 전자금융보조업자의 정보처리시스템 등에 관한 사항
2. 그 밖에 전자금융거래의 안정성과 신뢰성을 확보하기 위하여 필요한 사항으로서 금융위원회가 정하여 고시하는 사항

[본조신설 2013.11.22]

제11조의5(전자금융기반시설 취약점 분석·평가의 절차 및 방법 등) ① 금융회사 및 전자금융업자는 법 제21조의3제1항에 따라 전자금융기반시설의 취약점 분석·평가를 하려는 경우에는 자체전담반을 구성하여 실시하거나 전문성을 갖춘 외부 기관에 의뢰하여 실시하여야 한다. 이 경우 자체전담반의 구성기준과 의뢰할 수 있는 외부 기관의 기준은 금융위원회가 정하여 고시한다.

② 법 제21조의3제1항에 따른 전자금융기반시설의 취약점 분석·평가는 사업연도마다 1회 이상 하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 지체 없이 취약점 분석·평가를 하여야 한다.

1. 법 제21조의5제1항에 따른 침해사고가 발생하여 그 피해 및 피해 확산을 방지하기 위한 긴급한 조치가 필요한 경우
2. 정보처리시스템이나 인터넷 홈페이지 구축 등 정보기술부문 관련 사업을 실시하였거나 정보기술부문의 기능개선·변경을 수행한 경우

③ 금융회사 및 전자금융업자는 법 제21조의3제1항에 따라 전자금융기반시설의 취약점 분석·평가를 하였을 때에는 다음 각 호의 사항이 포함된 결과보고 및 보완조치 이행계획서를 그 취약점 분석·평가 종료 후 30일 이내에 금융위원회에 제출하여야 한다.

1. 취약점 분석·평가의 사유, 대상, 기간 등 실시개요
2. 취약점 분석·평가의 세부 수행방법
3. 취약점 분석·평가 결과
4. 취약점 분석·평가 결과에 따른 필요한 보완조치의 이행계획
5. 그 밖에 취약점 분석·평가의 적정성을 확보하기 위하여 필요한 사항으로서 금융위원회가 정하여 고시하는 사항

④ 제1항부터 제3항까지의 규정에도 불구하고 금융위원회는 전자금융거래의 빈도, 총자산 및 상시 종업원 수 등을 고려하여 금융위원회가 정하여 고시하는 기준에 미달하는 금융회사 및 전자금융업자에 대하여 다음 각 호의 사항을 완화하여 적용할 수 있는 기준을 정하여 고시할 수 있다.

1. 제1항에 따른 취약점 분석·평가의 방법
2. 제2항 각 호 외의 부분 본문에 따른 취약점 분석·평가의 실시 주기
3. 제3항에 따른 결과보고 및 보완조치 이행계획서의 제출 시기 및 제출 시 포함되어야 하는 사항

[본조신설 2013.11.22]

제11조의6(침해사고 대응을 위한 금융위원회의 업무 등) ① 법 제21조의6제1항제4호에서 "대통령령으로 정하는 사항"이란 다음 각 호의 사항을 말한다.

1. 침해사고 대응을 총괄·관리하는 침해사고 대책본부의 운영 및 침해사고 긴급대응을 위한 침해사고 대응기관의 지정에 관한 사항

2. 침해사고 대응을 위한 비상계획의 수립 및 훈련 등에 관한 사항
3. 침해사고 조사 및 관련 금융회사·전자금융업자·전자금융보조업자 등에 대한 정보제공 등 요청에 관한 사항
4. 금융회사 및 전자금융업자가 사용하고 있는 소프트웨어 중 침해사고와 관련 있는 소프트웨어를 제작한 자 및 관계 행정기관 등에 대한 보안취약점 통보 등에 관한 사항

② 금융위원회는 법 제21조의6제1항에 따른 업무를 수행하기 위하여 필요한 경우 관계 행정기관 등에 관련 정보제공 등의 협조를 요청할 수 있다.

[본조신설 2013.11.22]

제12조(전자금융거래기록의 보존기간·보존방법 및 파기 절차·방법 등) ①법 제22조제1항 및 제3항에 따른 전자금융거래기록의 종류별 보존기간은 다음 각 호와 같다. <개정 2008.2.29, 2015.4.14>

1. 다음 각 목의 전자금융거래기록은 5년간 보존하여야 한다.
   가. 제7조제4항제1호 내지 제5호에 관한 사항
   나. 해당 전자금융거래와 관련한 전자적 장치의 접속기록
   다. 전자금융거래의 신청 및 조건의 변경에 관한 사항
   라. 건당 거래금액이 1만원을 초과하는 전자금융거래에 관한 기록
2. 다음 각 목의 전자금융거래기록은 1년간 보존하여야 한다.
   가. 건당 거래금액이 1만원 이하인 전자금융거래에 관한 기록
   나. 전자지급수단의 이용과 관련된 거래승인에 관한 기록
   다. 그 밖에 금융위원회가 정하여 고시하는 전자금융거래기록

②금융회사 또는 전자금융업자와 동일한 전자금융거래기록을 생성·보존하는 전자금융보조업자가 제1항제1호 각 목의 전자금융거래기록을 보존하여야 하는 기간은 같은 호에도 불구하고 3년으로 한다.<개정 2013.11.22, 2015.4.14>

③금융회사·전자금융업자 및 전자금융보조업자(이하 "금융회사등"이라 한다)는 제1항 및 제2항의 전자금융거래기록을 서면, 마이크로필름, 디스크 또는 자기테이프, 그 밖의 전산정보처리조직을 이용한 방법으로 보존하여야 한다.<개정 2013.11.22, 2015.4.14>

④금융회사등은 제3항에 따라 전자금융거래기록을 디스크, 자기테이프, 그 밖의 전산정보처리조직을 이용하여 보존하는 경우에는 「전자문서 및 전자거래 기본법」 제5조제1항 각 호의 요건을 모두 갖추어야 한다.<개정 2012.8.31, 2013.11.22, 2015.4.14>

⑤ 금융회사등이 법 제22조제2항에 따라 전자금융거래기록을 파기할 때 그 절차와 방법에 관하여는 「개인정보 보호법 시행령」 제16조를 준용한다.<신설 2015.4.14>

⑥ 법 제22조제3항에 따른 상거래관계가 종료된 날의 기준은 금융회사등과 거래상대방 간의 상거래관계가 관계 법령, 약관 또는 합의 등에 따라 계약기간의 만료, 해지권·해제권·취소권의 행사, 소멸시효의 완성, 변제 등으로 인한 채권의 소멸, 그 밖의 사유로 종료된 날을 그 기준으로 한다.<신설 2015.4.14>

[제목개정 2015.4.14]

제13조(이용한도 등) ① 법 제23조제1항제1호에 따른 전자화폐의 발행권면 최고한도는 200만원으로, 선불전자지급수단의 발행권면 최고한도는 50만원으로 한다. 다만, 「금융실명거래 및 비밀보장에 관한 법률」 제2조제4호에 따른 실지명의로 발행된 선불전자지급수단의 발행권면 최고한도는 200만원으로 한다. <개정 2008.7.9, 2013.11.22>

②법 제23조제1항제2호에 따른 전자자금이체의 이용한도는 100억원의 범위에서 금융위원회가 정하여 고시한다. 다만, 금융회사 또는 전자금융업자와 이용자 간에 별도의 계약이 있는 경우에는 그 이용한도를 달리 정할 수 있다.<개정 2008.2.29, 2008.7.9, 2013.11.22>

③법 제23조제1항제3호에 따른 직불전자지급수단의 이용한도는 1억원의 범위에서 금융위원회가 정하여 고시한다. 다만, 금융회사 또는 전자금융업자와 이용자 간에 별도의 계약이 있는 경우에는 그 이용한도를 달리 정할 수 있다.<개정 2008.2.29, 2008.7.9, 2013.11.22>

④ 법 제23조제2항에 따른 전자적 장치로부터의 현금 출금 최고한도는 1천만원의 범위에서 금융위원회가 정하여 고시한다. 다만, 금융회사 또는 전자금융업자와 이용자 간에 별도의 계약이 있는 경우에는 그 최고한도를 달리 정할 수 있다.<신설 2013.11.22>

⑤제2항 본문 및 제3항 본문에 따른 이용한도와 제4항 본문에 따른 최고한도의 구체적인 사항은 전자자금이체의 방법, 이용횟수나 이용기간 등을 고려하여 금융위원회가 정하여 고시한다. <개정 2008.2.29, 2008.7.9, 2013.11.22>

제14조(분쟁처리 및 분쟁조정 신청절차 등) ①금융회사 또는 전자금융업자는 법 제27조제1항에 따라 손해배상 등의 분쟁처리를 위한 분쟁처리책임자 및 담당자를 지정하고, 그 연락처(전화번호·모사전송번호·전자우편주소 등을 말한다)를 인터넷 등을 통하여 이용자에게 알려야 한다. <개정 2013.11.22>

②이용자는 법 제27조제2항에 따라 손해배상 등의 분쟁처리를 요구하는 경우에는 서면(전자문서를 포함한다) 또는 전자적 장치를 이용하여 금융회사 또는 전자금융업자의 본점이나 영업점에 분쟁의 처리를 신청할 수 있다. 이 경우 금융회사 또는 전자금융업자는 15일 이내에 손해배상 등 분쟁처리에 대한 조사 또는 처리 결과를 이용자에게 알려야 한다.<개정 2013.11.22>

③이용자는 법 제27조제2항에 따라 「금융위원회의 설치 등에 관한 법률」에 따른 금융감독원의 금융분쟁조정위원회 또는 「소비자기본법」에 따른 한국소비자원의 소비자분쟁조정위원회에 분쟁조정을 신청할 수 있다.<개정 2007.3.27, 2008.2.29>

제15조(허가 또는 등록면제 등) ①법 제28조제1항 단서에서 "대통령령이 정하는 금융회사"란 다음 각 호의 어느 하나에 해당하는 금융회사를 말한다. <개정 2008.2.29, 2009.5.29, 2013.11.22>

1. 법 제2조제3호다목 및 라목에 따른 금융회사
2. 「금융위원회의 설치 등에 관한 법률」 제38조제4호·제5호·제7호 및 제8호에 따른 기관

3. 「여신전문금융업법」에 따른 여신전문금융회사 중 신용카드사업자
4. 제2조제1호, 제1호의2, 제2호부터 제6호까지의 기관
5. 삭제 <2009.5.29>

②법 제28조제2항 각 호 외의 부분 단서에서 "대통령령이 정하는 금융회사"란 다음 각 호의 어느 하나에 해당하는 금융회사를 말한다.<개정 2007.6.28, 2008.2.29, 2008.7.9, 2008.7.29, 2009.3.31, 2013.11.22>

1. 제1항 각 호의 어느 하나에 해당하는 금융회사. 다만, 제1항제3호의 자는 법 제28조제2항제1호의 전자자금이체업무를 금융위원회에 등록하지 아니하고 행할 수 있는 금융회사에서 제외한다.
2. 다음 각 목의 어느 하나에 해당하는 금융회사(법 제28조제2항제1호에 따른 전자자금이체업무로 제한한다)
   가. 「자본시장과 금융투자업에 관한 법률」에 따른 투자매매업자·투자중개업자 및 증권금융회사
   나. 삭제 <2008.7.29>
   다. 「자본시장과 금융투자업에 관한 법률」에 따른 종합금융회사
   라. 「보험업법」에 따른 보험회사

③법 제28조제2항제5호에서 "대통령령이 정하는 전자금융업무"라 함은 전자금융거래와 관련하여 자금을 수수(授受)하거나 수수를 대행하는 전자금융업무로서 다음 각 호의 어느 하나에 해당하는 업무를 말한다.

1. 「전자상거래 등에서의 소비자보호에 관한 법률」 제13조제2항제10호에 따라 결제대금을 예치받는 업무
2. 수취인을 대행하여 지급인이 수취인에게 지급하여야 할 자금의 내역을 전자적인 방법으로 지급인에게 고지하고, 자금을 직접 수수하며 그 정산을 대행하는 업무

④법 제28조제3항제1호가목에서 "대통령령이 정하는 기준"이라 함은 다음 각 호의 어느 하나에 해당하는 것을 말한다.<개정 2013.6.28>

1. 가맹점이 1개의 기초자치단체(「지방자치법」 제2조제1항제2호에 따른 지방자치단체를 말하며, 제주특별자치도의 경우에는 행정시를 말한다) 안에만 위치할 것
2. 가맹점 수가 10개 이하일 것
3. 가맹점이 1개의 건축물(「건축법」 제2조제1항제2호에 따른 건축물을 말한다) 안에만 위치할 것
4. 가맹점이 1개의 사업장(「부가가치세법 시행령」 제8조 및 제10조에 따른 사업장을 말한다) 안에만 위치할 것

⑤법 제28조제3항제1호나목에서 "대통령령이 정하는 금액"이라 함은 30억원을 말한다. 이 경우 법 제28조제3항제1호나목에 따른 총발행잔액의 구체적인 산정방법은 금융위원회가 정하여 고시한다.<개정 2008.2.29>

⑥법 제28조제3항제1호다목에서 "대통령령이 정하는 방법에 따라 상환보증보험 등에 가입한 경우"라 함은 선불전자지급수단의 미상환잔액 전부에 대하여 제22조제2항 각 호의 어느 하나에 해당하는 금융회사로부터 지급보증을 받거나 상환보증보험(이에 상당하는 공제를 포함한다)에 가입한 경우를 말한다.<개정 2013.11.22>

⑦법 제28조제3항제2호에서 "대통령령이 정하는 전자지급결제대행에 관한 업무"라 함은 전자금융거래와 관련된 자금을 수수하거나 수수를 대행하지 아니하고 전자지급거래에 관한 정보만을 단순히 전달하는 업무를 말한다.

⑧법 제28조제4항 단서에서 "대통령령이 정하는 금융사고가 발생한 경우"라 함은 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 해당 법인 임직원의 위법하거나 부당한 행위로 이용자 또는 가맹점에 대한 환급 또는 정산이 사실상 불가능하게 된 경우
2. 해당 전자금융업무와 관련된 접근매체의 위조 또는 변조로 이용자 또는 가맹점에 손해가 발생한 경우
3. 해당 지급수단의 관리를 위한 정보처리시스템의 장애로 이용자 또는 가맹점에 손해가 발생한 경우
4. 해당 법인의 임직원 또는 가맹점이 이용자의 전자금융거래정보를 노출하거나 그 밖에 다른 법령에 따른 개인정보 또는 신용정보보호 관련 규정을 위반한 것이 명백한 경우

제16조(전자채권 등록에 관한 절차와 방법 등) ①전자채권을 전자채권관리기관(법 제29조제1항에 따라 전자채권의 등록 및 관리업무를 행하기 위하여 등록한 자를 말한다. 이하 이 조에서 같다)에 등록하려는 자는 미리 금융회사와 전자채권의 발행 및 채무의 이행을 위한 계좌개설약정을 체결하여야 한다. <개정 2013.11.22>

②전자채권관리기관은 금융회사를 거쳐 전자채권의 등록을 신청받은 때에는 그 전자채권의 발행 내역의 이상 유무를 확인하고, 이상이 없으면 전자채권등록원장에 등록한 후 이를 채권자에게 통지하여야 한다.<개정 2013.11.22>

③전자채권관리기관이 제2항에 따라 전자채권을 등록하는 경우 그 등록사항은 다음 각 호와 같다.<개정 2013.11.22>

1. 전자채권의 채권번호와 종류(보증채권인지 무보증채권인지 여부)
2. 채권자 및 채무자와 그 거래 금융회사에 관한 사항
3. 전자채권의 발행일 및 변제기
4. 전자채권의 발행한도 및 발행금액
5. 그 밖에 전자채권의 등록에 필요한 사항

④전자채권관리기관은 등록된 전자채권에 대하여 다음 각 호의 사항을 관리하여야 한다.<개정 2013.11.22>

1. 전자채권의 변제기와 관련된 사항의 채무자에 대한 통지
2. 전자채권의 변제내역 및 미변제내역

3. 전자채권의 양도내역
4. 금융회사 간 전자채권 관련 결제내역
5. 전자채권 관련 거래의 정지에 관한 사항
6. 그 밖에 전자채권의 관리와 관련된 사항

제17조(자본금 요건) ①법 제30조제2항 각 호 외의 부분에서 "대통령령으로 정하는 금액"이란 다음 각 호의 구분에 따른 금액을 말한다. <개정 2013.11.22>

1. 법 제28조제2항제1호의 전자자금이체업무의 경우 : 30억원
2. 법 제28조제2항제2호의 직불전자지급수단의 발행 및 관리의 경우 : 20억원
3. 법 제28조제2항제3호의 선불전자지급수단의 발행 및 관리의 경우 : 20억원

② 법 제30조제3항제1호에서 "대통령령으로 정하는 금액"이란 다음 각 호의 구분에 따른 금액을 말한다.<신설 2016.6.28>

1. 법 제28조제2항제4호의 전자지급결제대행에 관한 업무의 경우: 3억원
2. 제15조제3항제1호의 업무의 경우: 3억원
3. 제15조제3항제2호의 업무의 경우: 3억원

③법 제30조제3항제2호에서 "대통령령으로 정하는 금액"이란 다음 각 호의 구분에 따른 금액을 말한다.<개정 2016.6.28>

1. 법 제28조제2항제4호의 전자지급결제대행에 관한 업무의 경우 : 10억원
2. 제15조제3항제1호의 업무의 경우 : 10억원
3. 제15조제3항제2호의 업무의 경우 : 5억원
4. 법 제29조의 전자채권의 등록 및 관리업무의 경우 : 30억원

④법 제28조 및 법 제29조에 따른 업무를 둘 이상 영위하려는 경우에는 제1항부터 제3항까지의 구분에 따른 금액의 합계액을 자본금·출자총액 또는 기본재산으로 한다. 다만, 그 합계액이 50억원 이상이면 50억원으로 한다.<개정 2016.6.28>

제18조(재무건전성 기준 등) ①법 제28조 및 법 제29조에 따른 허가를 받거나 등록을 하려는 자(이하 이 조에서 "신청인"이라 한다)가 「금융위원회의 설치 등에 관한 법률」 제38조에 규정된 금융감독원의 검사대상기관인 경우에는 그 기관의 설립·운영 등에 관한 법령에서 정하는 경영건전성에 관한 기준 등을 감안하여 금융위원회가 정하여 고시하는 재무건전성 기준에 적합하여야 한다. <개정 2008.2.29>

②신청인이 제1항의 검사대상기관이 아닌 경우에는 신청인[신청인의 대주주가 「독점규제 및 공정거래에 관한 법률」 제2조제2호에 따른 기업집단(동법 시행령 제17조제1항제1호 및 제2호에 해당하는 기업집단을 제외한다. 이하 이 조에서 "기업집단"이라 한다)에 속하는 기업이면 금융업 또는 보험업을 영위하는 회사를 제외한 그 기업집단을 포함한다]의 자기자본·출자총액 또는 기본재산에 대한 부채총액의 비율이 100분의 200의 범위 안에서 금융위원회가 정하여 고시하는 비율 이하이어야 한다. 다만, 다음 각 호의 요건을 모두 갖춘 신청인에 대하여는 금융위원회가 그 비율을 달리 정하여 고시할 수 있다.<개정 2008.2.29>

1. 정부 또는 광역지방자치단체(이하 "정부등"이라 한다)가 자본금ㆍ출자총액 또는 기본재산의 100분의 10 이상을 소유하고 있거나 출자하고 있을 것
2. 신청인의 사업 수행이 곤란하게 되는 경우 정부등이 해당 사업을 인수할 것을 확약하는 등 그 사업의 연속성에 대하여 정부등이 보장하고 있을 것
3. 금융위원회가 정하여 고시하는 요건에 맞추어 재무구조개선계획을 제출할 것

③법 제31조제1항제5호에서 "대통령령이 정하는 주요출자자"라 함은 다음 각 호와 같다.<개정 2008.7.9, 2008.7.29>

1. 의결권 있는 발행주식총수 또는 출자총액을 기준으로 본인 및 그와 「자본시장과 금융투자업에 관한 법률 시행령」 제8조 각 호의 어느 하나에 해당하는 관계에 있는 자(이하 "특수관계인"이라 한다)가 소유하는 주식의 수 또는 출자지분이 가장 많은 경우의 그 본인(이하 "최대주주"라 한다). 다만, 최대주주가 법인인 경우에는 다음 각 목의 어느 하나에 해당하는 자를 포함한다.
   가. 최대주주인 법인의 최대주주(최대주주인 법인을 사실상 지배하는 자가 그 법인의 최대주주와 다른 경우에는 그 사실상 지배하는 자를 포함한다)
   나. 최대주주인 법인의 대표자
2. 최대주주의 특수관계인인 주주 또는 출자자
3. 누구의 명의로 하든지 자기의 계산으로 소유한 주식 또는 출자지분의 합계액이 의결권 있는 발행주식총수 또는 출자총액의 100분의 10 이상에 해당하는 자
4. 임원의 임면(任免) 등 해당 법인의 주요 경영사항에 대하여 사실상 영향력을 행사하고 있는 주주 또는 출자자

제19조(대주주인 출자자 등) ① 법 제32조제1호에서 "대통령령이 정하는 출자자"란 제18조제3항에 따른 주요출자자를 말한다. <개정 2008.7.9>

②법 제32조제5호에서 "대통령령이 정하는 금융관계법령"이라 함은 별표 1의2 각 호의 법령을 말한다.<개정 2012.5.7>

제20조(허가와 등록의 신청방법 등) ①법 제28조 및 법 제29조에 따라 허가를 받거나 등록을 하려는 자는 다음 각 호의 사항을 기재한 허가 또는 등록신청서를 금융위원회에 제출하여야 한다. <개정 2008.2.29>

1. 상호 및 주된 사무소의 소재지
2. 임원에 관한 사항
3. 자본금 및 출자자(금융위원회가 정하여 고시하는 소액출자자를 제외한다)의 성명 또는 명칭과 그 지분율
4. 영위하려는 전자금융업무
5. 전자금융업무 외의 사업을 영위하고 있거나 영위하려는 자의 경우에는 해당 사업의 내용(허가의 경우에 한한다)

② 제1항에 따른 신청서에는 다음 각 호의 서류를 첨부하여야 한다. 이 경우 금융위원회는 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 법인 등기사항증명서(신청인이 법인인 경우로 한정한다)를 확인하여야 한다.<개정 2008.2.29, 2010.5.4, 2010.11.2>

1. 정관 및 자본금 납입 증명서류
2. 재무제표와 그 부속서류
3. 주주의 구성(허가의 경우만 해당한다)
4. 업무개시 후 3년 간의 사업계획서(추정 재무제표 및 예산수지 계산서를 포함한다)
5. 전문인력 및 시설현황을 기재한 서류
6. 영업현황(허가의 경우만 해당한다)을 기재한 서류
7. 삭제 <2012.5.7>
8. 그 밖에 허가 또는 등록에 필요한 서류로서 금융위원회가 정하여 고시하는 서류

③금융위원회는 제1항에 따라 허가신청서를 제출받은 날부터 3월 이내에 허가 여부를 결정하고, 신청인에게 통보하여야 한다.<개정 2008.2.29>

④금융위원회는 제1항에 따라 등록신청서를 제출한 자가 법 제31조의 등록요건을 갖춘 경우에는 지체 없이 등록을 하고, 그 사실을 신청인에게 통보하여야 한다.<개정 2008.2.29>

⑤금융위원회는 제1항 및 제2항에 따라 제출받은 서류에 흠결이 있는 경우에는 서류를 제출받은 날부터 10일 이내에 보완할 것을 요청할 수 있다. 이 경우 보완에 걸린 기간은 제3항에 따른 기간에 산입하지 아니한다.<개정 2008.2.29>

⑥ 금융위원회는 제1항에 따른 신청서류의 서식을 정하여 고시한다.<신설 2012.5.7>

제21조(등록말소신청) ①법 제34조제1항에 따라 등록의 말소를 신청하려는 자는 금융위원회가 정하여 고시하는 바에 따라 이용자 보호조치를 마친 후, 다음 각 호의 사항을 기재한 등록말소신청서를 금융위원회에 제출하여야 한다. <개정 2008.2.29, 2012.5.7>

1. 상호 및 주된 사무소 소재지
2. 등록을 말소하려는 전자금융업무의 종류
3. 등록말소의 사유
4. 등록말소에 따른 이용자 보호조치내역

② 금융위원회는 제1항에 따른 등록말소신청서류의 서식을 정하여 고시한다.<신설 2012.5.7>

제22조(겸업가능 업무 등) ①법 제35조제1항제2호에서 "대통령령이 정하는 업무"라 함은 다음 각 호의 어느 하나에 해당하는 업무를 말한다. <개정 2008.2.29, 2013.11.22>

1. 전자금융업과 관련된 정보처리시스템 및 소프트웨어의 개발·판매·대여
2. 금융회사 및 전자금융업자를 위한 전자금융업무의 일부 대행
3. 그 밖에 법 제28조 또는 법 제29조에 따른 허가를 받거나 등록을 한 업무를 수행하기 위하여 필요한 업무로서 금융위원회가 정하여 고시하는 업무

②법 제35조제2항에서 "대통령령이 정하는 금융회사"란 다음 각 호의 어느 하나에 해당하는 금융회사를 말한다.<개정 2008.2.29, 2013.11.22, 2016.5.31>

1. 「금융위원회의 설치 등에 관한 법률」 제38조제1호·제2호(종합금융회사만 해당한다)·제7호 및 제8호의 기관
2. 「신용보증기금법」에 따른 신용보증기금
3. 「기술보증기금법」에 따른 기술보증기금
4. 「보험업법」에 따른 보험회사
5. 제2조제1호 및 제2호의 금융회사

제23조(전자금융업 가맹점계약 해지 사유) 법 제38조제4항에서 "대통령령이 정하는 사유"라 함은 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 가맹점이 법 제26조 또는 법 제37조제3항제3호 내지 제5호를 위반하여 형을 선고받은 경우
2. 가맹점이 법 제37조제1항·제2항 또는 제3항제3호 내지 제5호를 위반한 사실에 관하여 관계 행정기관으로부터 서면통보가 있는 경우
3. 관계 행정기관으로부터 해당 가맹점의 폐업사실을 서면으로 통보받은 경우

제24조(경영지도의 기준) 법 제42조제2항에 따른 경영지도의 기준에는 다음 각 호의 사항이 포함되어야 한다. <개정 2012.5.7>

1. 법 제28조 또는 법 제29조에 따른 허가 또는 등록의 요건인 자본금의 유지에 관한 사항
2. 자기자본의 보유기준에 관한 사항
3. 유동성부채에 대한 유동성자산의 보유기준에 관한 사항
4. 총자산 대비 투자위험성이 낮은 자산의 비율에 관한 사항(선불전자지급수단의 발행인 및 전자화폐발행자의 경우는 제외한다)
5. 미상환잔액 대비 자기자본의 비율에 관한 사항(선불전자지급수단의 발행인 및 전자화폐발행자에 한한다)

제25조(합병·해산·폐업 등의 인가) ①금융위원회는 법 제45조제1항에 따라 합병·해산 또는 폐지의 인가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다. <개정 2008.2.29, 2008.7.29, 2013.11.22>

1. 법 제45조제1항제1호에 따른 합병의 경우
   가. 전자금융산업의 효율화와 신용질서의 유지에 지장을 주지 아니할 것
   나. 합병에 따른 영업계획 및 조직운영계획이 적정할 것
   다. 합병으로 인하여 설립되는 회사 또는 합병 후 존속하는 회사 등이 법 제30조 내지 제32조를 위반하지 아니할 것
   라. 「상법」과 「자본시장과 금융투자업에 관한 법률」, 그 밖의 관계 법령에 따른 절차이행에 하자가 없을 것
2. 법 제45조제1항제2호에 따른 해산 또는 폐지의 경우
   가. 해당 금융회사의 경영 및 재무상태 등에 비추어 부득이한 사정이 있을 것

나. 전자화폐 이용자 및 가맹점 보호와 신용질서유지에 지장을 주지 아니할 것

다. 「상법」과 「자본시장과 금융투자업에 관한 법률」, 그 밖에 관계 법령에 따른 절차이행에 하자가 없을 것

②법 제45조제1항제3호에 따른 영업의 전부 또는 일부의 양수 인가에 관하여는 제1항제1호를, 영업의 전부 또는 일부의 양도 인가에 관하여는 제1항제2호를 각각 준용한다.

③금융위원회는 법 제45조제1항에 따른 인가의 세부요건, 신청서류, 그 밖에 필요한 사항을 정하여 고시할 수 있다.<개정 2008.2.29>

제26조(업무정지 및 과징금부과의 기준 등) ①법 제43조제2항에 따라 업무정지를 명하거나 법 제46조제1항 또는 제2항에 따라 과징금을 부과할 수 있는 위반행위의 종별에 따른 업무정지의 기간 및 과징금의 금액은 별표 2와 같다. <개정 2015.4.14>

②금융위원회는 위반행위의 정도 및 위반횟수 등을 참작하여 제1항에 따른 업무정지의 기간 또는 과징금의 금액의 2분의 1의 범위 안에서 가중하거나 감경할 수 있다. 다만, 가중하는 경우에도 업무정지의 기간은 6개월을, 과징금의 총액은 다음 각 호의 구분에 따른 금액을 초과할 수 없다.<개정 2008.2.29, 2015.4.14>

1. 법 제46조제1항에 따라 과징금을 부과하는 경우: 50억원
2. 법 제46조제2항에 따라 과징금을 부과하는 경우: 5천만원

제27조(과징금의 부과 및 납부) ①금융위원회는 법 제46조제1항 또는 제2항에 따라 과징금을 부과하려는 때에는 그 위반행위의 종별과 해당 과징금의 금액 등을 명시하여 납부할 것을 서면으로 통지하여야 한다. <개정 2008.2.29, 2015.4.14>

②제1항에 따라 통지를 받은 자는 20일 이내에 과징금을 금융위원회가 정하여 고시하는 수납기관에 납부하여야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 그 기간 안에 과징금을 납부할 수 없을 때에는 그 사유가 없어진 날부터 7일 이내에 납부하여야 한다.<개정 2008.2.29>

③제2항에 따라 과징금을 납부받은 수납기관은 영수증을 납부자에게 교부하고, 지체 없이 수납한 사실을 금융위원회에 통보하여야 한다.<개정 2008.2.29>

④과징금은 이를 분납할 수 없다.

제28조(체납처분의 위탁) ①금융위원회는 법 제46조제5항에 따라 체납처분에 관한 업무를 국세청장에게 위탁하는 때에는 다음 각 호의 서류를 첨부한 서면으로 하여야 한다. <개정 2008.2.29, 2015.4.14>

1. 금융위원회 의결서
2. 세입징수결의서 및 고지서
3. 납부독촉장

②국세청장은 제1항에 따라 위탁받은 체납처분 업무를 종료한 경우에는 그 업무 종료 일시, 그 밖에 필요한 사항을 종료일부터 30일 이내에 금융위원회에 서면으로 통보하여야 한다.<개정 2008.2.29>

제28조의2(환급가산금의 이율) 법 제46조의2제3항에서 "대통령령으로 정하는 가산금 이율"이란 은행(「은행법」에 따라 은행업의 인가를 받은 은행을 말한다)의 정기예금 이자율을 고려하여 금융위원회가 정하여 고시하는 이율을 말한다.

[본조신설 2013.11.22]

제29조(통계조사의 대상과 방법 등) 법 제47조제1항에 따라 한국은행이 실시하는 전자금융업 및 전자금융거래에 관한 통계조사는 다음 각 호의 사항을 대상으로 한다.

1. 전자금융업무를 영위하거나 이를 보조하는 기관 또는 단체나 사업자의 자산·부채 및 자본금, 전자금융거래에 관련된 매출·비용 및 수익에 관한 사항
2. 전자금융거래를 처리하는 정보처리시스템 현황에 관한 사항
3. 전자지급수단의 발행 및 이용과 전자자금이체, 전자지급결제대행 및 전자채권거래 등 전자금융거래의 현황에 관한 사항
4. 그 밖에 전자금융업 및 전자금융거래에 관한 현황파악 또는 통화신용정책의 수행에 필요한 사항

제30조(권한의 위탁) ①금융위원회는 법 제48조에 따라 다음 각 호의 업무를 금융감독원장에게 위탁한다. <개정 2008.2.29, 2008.7.9, 2012.5.7, 2013.11.22, 2015.4.14, 2016.6.28>

1. 법 제21조제2항에 따른 인증방법에 관한 기준의 설정
1의2. 법 제21조제4항에 따른 정보기술부문에 대한 계획의 접수
1의3. 법 제21조의3제1항에 따른 취약점 분석·평가 결과의 접수
1의4. 법 제25조에 따른 약관의 제정 및 변경 보고의 접수, 약관 변경의 권고
2. 법 제28조·제29조·제33조 및 제34조에 따른 등록 및 등록 말소
2의2. 법 제30조제4항에 따른 기준을 초과하는 경우 그 내용에 관한 신고의 접수
2의3. 법 제33조제2항에 따른 허가·인가를 하기 위한 검토
2의4. 법 제33조의2제2항 및 제45조의2제2항에 따른 본허가·본인가의 요건을 충족할 수 있는지의 확인
2의5. 법 제33조의2제4항 및 제45조의2제4항에 따른 예비허가·예비인가의 조건 이행 여부 확인 및 본허가·본인가의 요건을 충족하는지의 확인
3. 법 제40조에 따른 제휴, 위탁 또는 외부주문에 관한 계약에 대한 시정 또는 보완 지시
4. 법 제42조제1항에 따른 업무 및 경영실적보고서의 제출방법 및 절차의 결정, 보고서의 접수
5. 법 제42조제2항에 따른 경영지도기준의 구체적 산정방법의 설정

②금융감독원장은 제1항에 따라 위탁받은 업무의 처리결과를 금융위원회가 정하여 고시하는 바에 따라 금융위원회에 보고하여야 한다.<개정 2008.2.29>

제31조(민감정보 및 고유식별정보의 처리) ① 금융위원회(제30조에 따라 금융위원회의 권한을 위탁받은 자를 포함한다)는 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제18조제2호에 따른 범죄경력자료에 해당하는 정보, 같은 영 제19조제1호,

제2호 또는 제4호에 따른 주민등록번호, 여권번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다. <개정 2013.11.22>

1. 법 제25조에 따른 약관의 제정 및 변경에 관한 사무
2. 법 제28조, 제29조, 제33조에 따른 허가와 등록 등에 관한 사무

2의2. 법 제33조의2에 따른 예비허가에 관한 사무

3. 법 제34조에 따른 등록의 말소에 관한 사무
4. 법 제39조제1항부터 제5항까지, 제40조에 따른 감독·검사 또는 자료제출 및 이에 따른 사후 조치 등에 관한 사무
5. 법 제39조제6항 및 제44조에 따른 조치, 청문 등에 관한 사무
6. 법 제41조제2항에 따른 공동검사에 관한 사무
7. 법 제42조에 따른 회계처리 구분 및 건전경영지도에 관한 사무
8. 법 제45조에 따른 인가에 관한 사무
9. 법 제45조의2에 따른 예비인가에 관한 사무

② 금융감독원장 또는 한국소비자원(제1호의 사무만 해당한다)은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 제1항 각 호 외의 부분에 따른 개인정보가 포함된 자료를 처리할 수 있다.

1. 법 제27조에 따른 분쟁처리 및 분쟁조정에 관한 사무
2. 법 제39조제1항부터 제5항까지, 제40조에 따른 감독·검사 또는 자료제출 및 이에 따른 사후 조치 등에 관한 사무
3. 법 제39조제6항에 따른 조치에 관한 사무

③ 금융회사 또는 전자금융업자는 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법 시행령」 제19조제1호, 제2호 또는 제4호에 따른 주민등록번호, 여권번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.<신설 2014.8.6>

1. 법 제6조제2항에 따른 접근매체의 발급에 관한 사무
2. 법 제28조제2항제2호에 따른 직불전자지급수단의 발행에 관한 사무
3. 법 제28조제2항제3호에 따른 선불전자지급수단의 발행에 관한 사무

[본조신설 2012.1.6]

제32조(규제의 재검토) ① 금융위원회는 제5조제2항에 따른 금융회사의 범위에 대하여 2016년 1월 1일을 기준으로 3년마다(매 3년이 되는 해의 1월 1일 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 하여야 한다. <개정 2015.12.30>

② 금융위원회는 다음 각 호의 사항에 대하여 다음 각 호의 기준일을 기준으로 2년마다(매 2년이 되는 해의 기준일과 같은 날 전까지를 말한다) 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.<신설 2014.12.9, 2015.4.14>

1. 제11조의3제1항에 따른 정보보호최고책임자 지정대상 금융회사 등의 기준: 2015년 1월 1일

2. 제11조의3제4항에 따른 정보보호최고책임자의 자격요건: 2015년 1월 1일

[본조신설 2013.11.22]

부칙 <제19783호,2006.12.29>

①(시행일) 이 영은 2007년 1월 1일부터 시행한다.

②(다른 법령의 개정) 전자상거래 등에서의 소비자보호에 관한 법률 시행령 일부를 다음과 같이 개정한다.

제19조의2제1항을 다음과 같이 하고, 동조제2항을 삭제하며, 동항제3항 각 호 외의 부분중 "제1항제10호의 규정에 따른 사업자가 동항동호 라목의 규정에 따라"를 "제1항제1호에 따른 사업자가 동항동호가목에 따라"로 한다.

①법 제13조제2항제10호에서 "대통령령이 정하는 제3자"라 함은 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 법 제13조제2항제10호의 결제대금예치업무를 하기 위하여 「전자금융거래법」 제28조제2항제5호 및 동법 시행령 제15조제3항제1호에 따라 금융감독위원회에 등록한 자로서 다음 각 목의 요건을 모두 갖춘 사업자

가. 법 제24조제1항에 따른 소비자피해보상보험계약 등(이하 "소비자피해보상보험계약등"이라 한다)을 체결할 것

나. 「금융감독기구의 설치 등에 관한 법률」 제38조에 따른 금융기관 또는 「우체국예금·보험에 관한 법률」에 따른 체신관서에 결제대금의 예치만을 위한 계좌로 개설·통보한 계좌에 소비자의 결제대금을 예치할 것

2. 「전자금융거래법」 제28조제2항 단서에 따른 금융기관

부칙 <제19958호,2007.3.27>(소비자기본법 시행령)

제1조 (시행일) 이 영은 2007년 3월 28일부터 시행한다. <단서 생략>

제2조 내지 제6조 생략

제7조 (다른 법령의 개정) ①내지 ⑨생략

⑩전자금융거래법 시행령 일부를 다음과 같이 개정한다.

제14조제3항 중 "「소비자보호법」에 따른 한국소비자보호원"을 "「소비자기본법」에 따른 한국소비자원"으로 한다.

⑪내지 <16> 생략

제8조 생략

부칙 <제20112호,2007.6.28>

이 영은 2007년 7월 1일부터 시행한다.

부칙 <제20653호,2008.2.29>(금융위원회의 설치 등에 관한 법률 시행령)

제1조(시행일) 이 영은 공포한 날부터 시행한다. 다만, 부칙 제2조에 따라 개정되는 대통령령 중 이 영의 시행 전에 공포되었으나 시행일이 도래하지 아니한 대통령령을 개정한 부분은 각각 해당 대통령령의 시행일부터 시행한다.

제2조(다른 법령의 개정) ① 부터 <31> 까지 생략

<32> 전자금융거래법 시행령 일부를 다음과 같이 개정한다.

제7조제4항제6호, 제12조제1항제2호다목, 제13조제2항 본문、제3항、제4항, 제15조제2항제1호 단서、제5항 후단, 제18조제1항、제2항 각 호 외의 부분 본문、단서、제3호, 제20조제1항 각 호 외의 부분、제3호、제2항제7호、제3항、제4항、제5항 전단, 제21조 각 호 외의 부분, 제22조제1항제3호, 제25조제1항 각 호 외의 부분、제3항, 제26조제2항 본문, 제27조제1항、제2항 본문、제3항, 제28조제1항 각 호 외의 부분、제1호, 제28조제2항, 제30조제1항 각 호 외의 부분、제2항, 제31조제1항、제2항 전단、제3항 및 별표 2 제6호、제9호 중 "금융감독위원회"를 각각 "금융위원회"로 한다.

제14조제3항, 제15조제1항제2호, 제18조제1항 및 제22조제2항제1호 중 "「금융감독기구의 설치 등에 관한 법률」"을 각각 "「금융위원회의 설치 등에 관한 법률」"로 한다.

제20조제2항을 다음과 같이 한다.

② 제1항에 따른 신청서에는 다음 각 호의 서류를 첨부하여야 한다. 이 경우 담당 공무원은 「전자정부구현을 위한 행정업무 등의 전자화촉진에 관한 법률」 제21조제1항에 따른 행정정보의 공동이용을 통하여 법인등기부 등본(신청인이 법인인 경우만 해당한다)을 확인하여야 하며, 신청인이 확인에 동의하지 아니하는 경우에는 해당 서류를 첨부하도록 하여야 한다.

1. 정관 및 자본금 납입 증명서류
2. 재무제표와 그 부속서류
3. 주주의 구성(허가의 경우만 해당한다)
4. 업무개시 후 3년 간의 사업계획서(추정 재무제표 및 예산수지 계산서를 포함한다)
5. 전문인력 및 시설현황을 기재한 서류
6. 영업현황(허가의 경우만 해당한다)을 기재한 서류
7. 임원의 이력서 및 경력증명서
8. 그 밖에 허가 또는 등록에 필요한 서류로서 금융위원회가 정하여 고시하는 서류

별표 1 제25호를 다음과 같이 한다.

25. 「금융위원회의 설치 등에 관한 법률」

<33> 부터 <49> 까지 생략

부칙 <제20913호,2008.7.9>

이 영은 공포한 날부터 시행한다.

부칙 <제20947호,2008.7.29>(자본시장과 금융투자업에 관한 법률 시행령)

제1조(시행일) 이 영은 2009년 2월 4일부터 시행한다. <단서 생략>

제2조부터 제25조까지 생략

제26조(다른 법령의 개정) ① 부터 <87> 까지 생략

<88> 전자금융거래법 시행령 일부를 다음과 같이 개정한다.

제2조제7호·제8호 및 제12호를 각각 다음과 같이 하고, 같은 조 제13호를 삭제한다.

7. 「자본시장과 금융투자업에 관한 법률」에 따른 한국거래소

8. 「자본시장과 금융투자업에 관한 법률」에 따른 한국예탁결제원

12. 「자본시장과 금융투자업에 관한 법률」에 따른 한국금융투자협회

제15조제2항제2호가목 중 "「증권거래법」에 따른 증권회사"를 "「자본시장과 금융투자업에 관한 법률」에 따른 투자매매업자·투자중개업자"로 하고, 같은 호 나목을 삭제하며, 같은 호 다목 중 "「종합금융회사에 관한 법률」"을 "「자본시장과 금융투자업에 관한 법률」"로 한다.

제18조제3항제1호 각 목 외의 부분 본문 중 "「증권거래법 시행령」 제2조의8"을 "「자본시장과 금융투자업에 관한 법률 시행령」 제8조"로 한다.

제25조제1항제1호라목 및 같은 항 제2호다목 중 "「증권거래법」"을 각각 "「자본시장과 금융투자업에 관한 법률」"로 한다.

별표 1 제8호를 다음과 같이 하고, 같은 표 제9호부터 제11호까지 및 제24호를 각각 삭제한다.

8. 「자본시장과 금융투자업에 관한 법률」

<89> 부터 <113> 까지 생략

제27조 및 제28조 생략

부칙 <제21404호,2009.3.31>

이 영은 2009년 4월 1일부터 시행한다.

부칙 <제21518호,2009.5.29>(한국정책금융공사법 시행령)

제1조(시행일) 이 영은 2009년 6월 1일부터 시행한다.

제2조 생략

제3조(다른 법령의 개정) ① 부터 <21> 까지 생략

<22> 전자금융거래법 시행령 일부를 다음과 같이 개정한다.

제2조에 제1호의2를 다음과 같이 신설한다.

1의2. 「한국정책금융공사법」에 따른 한국정책금융공사

제15조제4호를 다음과 같이 하고, 같은 조 제5호를 삭제한다.

4. 제2조제1호, 제1호의2, 제2호부터 제6호까지의 기관

제25조제2항제5호를 다음과 같이 한다.

5. 제2조제1호, 제1호의2 및 제2호의 금융기관

<23> 부터 <25> 까지 생략

부칙 <제21590호,2009.6.30>

제1조(시행일) 이 영은 2009년 7월 1일부터 시행한다. 다만, 제8조 및 제9조의 개정규정은 2010년 1월 1일부터 시행한다.

제2조(「농지법 시행령」 개정에 따른 유효기간 등) ① 「농지법 시행령」 별표 2 제46호란의 개정규정은 2011년 6월 30일까지 효력을 가진다.

② 「농지법 시행령」 별표 2 제46호란의 개정규정은 이 영 시행 후 최초로 농지전용허가(변경허가의 경우와 다른 법률에 따라 농지전용허가 또는 그 변경허가가 의제되는 인가 또는 허가 등의 경우를 포함한다. 이하 이 항에서 같다)를 신청하거나 농지전용신고(변경신고를 포함한다. 이하 이 항에서 같다)를 하는 것부터 적용하고, 2011년 6월 30일까지 농지전용허가를 신청하거나 농지전용신고를 하는 것에 대하여도 이를 적용한다.

제3조(「관광진흥법 시행령」개정에 따른 적용례) 「관광진흥법 시행령」 제32조제1호의 개정규정은 이 영 시행 전에 법 제15조에 따른 사업계획의 승인을 받거나 승인을 신청한 자에 대하여도 적용한다.

제4조(「산업입지 및 개발에 관한 법률 시행령」의 개정에 따른 적용례 등) ① 「산업입지 및 개발에 관한 법률 시행령」 제40조제2항의 개정규정은 이 영 시행 후 최초로 분양계획서를 작성하는 분부터 적용한다.

② 「산업입지 및 개발에 관한 법률 시행령」 제40조제2항의 개정규정에 따라 조례에 위임된 사항은 해당 조례가 제정 또는 개정될 때까지 종전의 규정에 따른다.

제5조(「고용보험법 시행령」의 개정에 따른 경과조치) 「고용보험법 시행령」 제13조제1항제2호의 개정규정은 이 영 시행 후 최초로 「고용보험법 시행령」 제13조제1항에 따라 근로시간을 단축한 사업장부터 적용한다.

제6조(「부동산개발업의 관리 및 육성에 관한 법률 시행령」의 개정에 따른 경과조치) 이 영 시행 전의 행위에 대한 과태료의 적용은 종전의 규정에 따른다.

제7조(「신항만건설촉진법 시행령」의 개정에 따른 경과조치) 이 영 시행 당시 종전의 규정에 따라 신항만건설사업실시계획 승인 신청기간의 연장을 받아 그 기간 중에 있는 자에 대하여는 「신항만건설촉진법 시행령」 제9조제5항 후단의 개정규정을 적용하되, 같은 개정규정에 따라 1회의 연장을 받은 것으로 본다.

제8조(「자원의 절약과 재활용촉진에 관한 법률 시행령」의 개정에 따른 경과조치) 이 영 시행 전의 행위에 대한 과태료의 적용은 종전의 규정에 따른다.

제9조(「하수도법 시행령」의 개정에 따른 경과조치) ① 「하수도법 시행령」 제38조제2항제2호가목의 개정규정에 따른 최초의 재교육은 이 영 시행 전에 실시한 가장 최근의 재교육 완료일부터 기산하여 5년이 되는 날이 속하는 해에 실시한다.

② 「하수도법 시행령」 제38조제2항제2호나목의 개정규정은 이 영 시행 후 최초로 해당 영업정지처분을 받은 경우부터 적용한다.

부칙 <제21765호,2009.10.1>

제1조(시행일) 이 영은 공포한 날부터 시행한다.

제2조 및 제3조 생략

제4조(다른 법령의 개정) ① 부터 <23> 까지 생략

<24> 전자금융거래법 시행령 일부를 다음과 같이 개정한다.

제2조제14호 중 "신용정보업자"를 "신용정보회사"로 한다.

<25> 부터 <31> 까지 생략

제5조 생략

부칙 <제22151호,2010.5.4>

제1조(시행일) 이 영은 2010년 5월 5일부터 시행한다.

제2조 및 제3조 생략

제4조(다른 법령의 개정) ① 부터 <143> 까지 생략

<144> 전자금융거래법 시행령 일부를 다음과 같이 개정한다.

제20조제2항 각 호 외의 부분 후단 중 "「전자정부구현을 위한 행정업무 등의 전자화촉진에 관한 법률」 제21조제1항"을 "「전자정부법」 제36조제1항"으로 한다.

<145> 부터 <192> 까지 생략

부칙 <제22467호,2010.11.2>

이 영은 공포한 날부터 시행한다.

부칙 <제23488호,2012.1.6>

제1조(시행일) 이 영은 공포한 날부터 시행한다. <단서 생략>

제2조 생략

부칙 <제23776호,2012.5.7>

이 영은 공포 후 6개월이 경과한 날부터 시행한다. 다만, 제11조의2, 제19조, 별표 1 및 별표 1의2의 개정규정은 2012년 5월 15일부터 시행한다.

부칙 <제24076호,2012.8.31>

제1조(시행일) 이 영은 2012년 9월 2일부터 시행한다. <단서 생략>

제2조 생략

제3조(다른 법령의 개정) ①부터 ⑩까지 생략

⑪ 전자금융거래법 시행령 일부를 다음과 같이 개정한다.

제12조제4항 중 "「전자거래기본법」"을 "「전자문서 및 전자거래 기본법」"으로 한다.

⑫부터 <16>까지 생략

제4조 생략

부칙 <제24638호,2013.6.28>

제1조(시행일) 이 영은 2013년 7월 1일부터 시행한다. <단서 생략>

제2조부터 제15조까지 생략

제16조(다른 법령의 개정) ①부터 <26>까지 생략

<27> 전자금융거래법 시행령 일부를 다음과 같이 개정한다.

제15조제4항제4호 중 "「부가가치세법 시행령」 제4조 및 제4조의2"를 "「부가가치세법 시행령」 제8조 및 제10조"로 한다.

<28>부터 <37>까지 생략

제17조 생략

부칙 <제24880호,2013.11.22>

제1조(시행일) 이 영은 2013년 11월 23일부터 시행한다.

제2조(전자금융기반시설 취약점 분석·평가에 관한 적용례) 제11조의5제2항 각 호 외의 부분 본문의 개정규정은 이 영 시행 후 개시되는 사업연도부터 적용한다.

제3조(정보보호최고책임자의 자격에 관한 특례) 별표 1 제3호나목의 개정규정에도 불구하고 이 영 시행 당시 조합·신용협동조합·지역금고의 장이나 그 장이 지정한 사람은 같은 개정규정에 따른 교육을 이수하지 아니하였어도 정보보호최고책임자의 자격을 가진다. 다만, 이 영 시행 후 1년 이내에 같은 개정규정에 따른 교육을 이수하여야 한다.

제4조(오류의 정정 통지 방법에 관한 경과조치) 이 영 시행 당시 법 제8조제2항 또는 제3항에 따라 오류의 정정요구를 받았거나 오류가 있음을 안 경우에는 제7조의2의 개정규정에도 불구하고 종전의 규정에 따른다.

부칙 <제25279호,2014.3.24>

제1조(시행일) 이 영은 공포한 날부터 시행한다.

제2조(다른 법령의 개정) ①부터 <29>까지 생략

<30> 전자금융거래법 시행령 일부를 다음과 같이 개정한다.

별표 1의2 제34호를 다음과 같이 한다.

34. 「금융회사부실자산 등의 효율적 처리 및 한국자산관리공사의 설립에 관한 법률」

<31>부터 <34>까지 생략

제3조 생략

부칙 <제25532호,2014.8.6>

이 영은 2014년 8월 7일부터 시행한다.

부칙 <제25840호,2014.12.9>

제1조(시행일) 이 영은 2015년 1월 1일부터 시행한다.

제2조부터 제16조까지 생략

부칙 <제25945호,2014.12.30>

제1조(시행일) 이 영은 법률 제12663호 한국산업은행법 전부개정법률 부칙 제4조제6항에 따른 합병의 등기를 한 날부터 시행한다.

제2조 및 제3조 생략

제4조(다른 법령의 개정) ①부터 <31>까지 생략

<32> 전자금융거래법 시행령 일부를 다음과 같이 개정한다.

제2조제1호의2를 삭제한다.

<33>부터 <37>까지 생략

제5조 생략

부칙 <제26199호,2015.4.14>

이 영은 2015년 4월 16일부터 시행한다. 다만, 제9조의2 및 제30조제1항제1호의 개정규정은 2015년 10월 16일부터 시행한다.

부칙 <제26817호,2015.12.30>

이 영은 공포한 날부터 시행한다.

부칙 <제27205호,2016.5.31>

제1조(시행일) 이 영은 2016년 9월 30일부터 시행한다. <단서 생략>

제2조(다른 법령의 개정) ①부터 <46>까지 생략

<47> 전자금융거래법 시행령 일부를 다음과 같이 개정한다.

제2조제18호를 다음과 같이 한다.

18. 「기술보증기금법」에 따른 기술보증기금

제22조제2항제3호를 다음과 같이 한다.

3. 「기술보증기금법」에 따른 기술보증기금

별표 1의2 제19호를 다음과 같이 한다.

19. 「기술보증기금법」

<48>부터 <59>까지 생략

제3조 생략

부칙 <제27292호,2016.6.28>

이 영은 2016년 6월 30일부터 시행한다. 다만 제6조의2의 개정규정은 2016년 7월 28일부터 시행한다.

[별표 1] <개정 2015.4.14.>

정보보호최고책임자의 자격(제11조의3제4항 관련)

1. 정보보호 또는 정보기술(IT) 분야의 학력 또는 기술자격을 가진 사람으로서 다음 각 목의 어느 하나에 해당하는 사람은 정보보호최고책임자의 자격을 가진다.
   가. 정보보호 또는 정보기술(IT) 분야의 전문학사학위를 취득한 후 4년 이상 정보보호 분야 업무 또는 5년 이상 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람
   나. 정보보호 또는 정보기술(IT) 분야의 학사학위 또는 다음 전문자격을 취득한 후 2년 이상 정보보호 분야 또는 3년 이상 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람
      1) 「전자정부법」 제2조제15호에 따른 감리원
      2) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제5항에 따른 정보보호 관리체계 인증기관의 인증 심사원
      3) 「자격기본법」에 따라 공인을 받은 정보보호전문가(Specialist for Information Security)
      4) 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 정보시스템감사사(Certified Information Systems Auditor)
      5) 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 정보시스템보호전문가(Certified Information System Security Professional)
   다. 정보보호 또는 정보기술(IT) 분야의 석사학위를 취득한 후 1년 이상 정보보호 분야 업무 또는 2년 이상 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람
2. 다음 각 목의 어느 하나에 해당하는 사람은 정보보호최고책임자의 자격을 가진다.
   가. 8년 이상 정보보호 분야 업무 또는 10년 이상 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람
   나. 전문학사학위를 취득한 후 6년 이상 정보보호 분야 업무 또는 7년 이상 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람
   다. 학사학위를 취득한 후 4년 이상 정보보호 분야 업무 또는 5년 이상 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람
   라. 석사학위를 취득한 후 2년 이상 정보보호 분야 업무 또는 3년 이상 정보기술

(IT) 분야 업무를 수행한 경력이 있는 사람

3. 「농업협동조합법」에 따른 조합, 「수산업협동조합법」에 따른 조합, 「산림조합법」에 따른 조합, 「신용협동조합법」에 따른 신용협동조합 및 「새마을금고법」에 따른 지역금고의 경우에는 제1호 및 제2호에도 불구하고 다음 각 목의 어느 하나에 해당하는 사람도 정보보호최고책임자의 자격을 가진다.

가. 정보보호 또는 정보기술(IT) 분야의 학력 또는 기술자격을 가진 사람으로서 6년 이상 금융업에 종사한 사람

나. 금융위원회가 정하여 고시하는 교육을 이수한 사람으로서 조합·신용협동조합·지역금고의 장이나 그 장이 지정한 사람. 다만, 상시 종업원 수(금융위원회가 정하여 고시하는 산정방식에 따라 계산된 상시 종업원 수를 말한다)가 20명 이하인 조합·신용협동조합·지역금고의 경우로 한정한다.

비고

1. "정보보호 또는 정보기술(IT) 분야 학력"이란 「고등교육법」에 따른 해당 학교에서 다음 각 목에 해당하는 학과의 과정을 이수하고 졸업하거나 그 밖의 관계법령에 따라 국내 또는 외국에서 이와 같은 수준 이상으로 인정되는 학력을 말한다.

가. 전자 관련 학과: 전기전자, 전기전자정보, 전기전자제어, 전자, 전자계산, 전자전기정보, 전자정보, 전자제어, 전자재료, 전자컴퓨터, 전자컴퓨터전기제어, 정보전자, 반도체, 메카트로닉스, 제어계측, 컴퓨터과학

나. 정보통신 관련 학과: 통신, 국제정보통신, 무선통신, 방송통신, 이동통신, 전기전자통신, 전기전자정보통신, 정보통신, 전자통신, 전자정보통신, 전자제어통신, 전파통신, 컴퓨터통신, 항공통신정보, 전기통신설비, 전자정보통신반도체, 전파, 전기전자전파, 방송설비, 통신컴퓨터, 컴퓨터네트워크, 컴퓨터정보기술

다. 정보보호 또는 정보처리기술 관련 학과: 전산, 전산통계, 정보전산, 정보처리, 시스템, 정보시스템, 구조시스템, 컴퓨터응용, 컴퓨터응용설계, 컴퓨터제어, 컴퓨터응용제어, 컴퓨터정보, 멀티미디어

라. 그 밖에 교육부장관이나 해당 교육기관의 장으로부터 전자, 정보통신, 정보보호 또는 정보처리기술 관련 학과로 인정받은 학과

2. "정보보호 또는 정보기술(IT) 분야 기술자격"이란 「국가기술자격법」 제2조제3호, 제8조의2제2항 및 같은 법 시행규칙 별표 2의 전기·전자 직무분

야 중 전자계산기 종목의 자격과 정보통신 직무분야 중 기술·기능 분야의 자격을 말한다.

3. "정보보호 분야 업무"란 공공기관, 민간기업, 교육기관 등에서 수행하는 다음 각 목에 해당하는 분야의 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 말한다.

가. 정보보호를 위한 공통기반기술 분야: 암호 기술, 인증 기술 등

나. 시스템·네트워크 보호 분야: 시스템 보호, 해킹·바이러스 대응, 네트워크 보호 등

다. 응용서비스 보호 분야: 전자거래 보호, 응용서비스 보호, 정보보호 표준화 등

4. "정보기술(IT) 분야 업무"란 공공기관, 민간기업, 교육기관 등에서 수행하는 다음 각 목에 해당하는 분야의 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 말한다.

가. 정보통신서비스 분야: 기간통신, 별정통신, 부가통신, 방송서비스 등

나. 정보통신기기 분야: 정보기기, 방송기기, 부품 등

다. 소프트웨어 및 컴퓨터 관련 서비스 분야: 범용 패키지 소프트웨어, 특정 업무용 프로그램, 디지털콘텐츠, 데이터베이스의 개발·구축·운영·활용 및 컴퓨터 관련 서비스

5. 정보보호업무를 수행한 기간과 정보기술(IT)업무를 수행한 기간은 서로 중복하여 인정되지 아니한다. 다만, 정보기술(IT)업무를 수행한 기간이 인정요건에 미달하는 경우에는 정보보호업무를 수행한 기간을 다음 산식의 비율로 환산하여 정보기술(IT)업무를 수행한 기간으로 합산할 수 있다.

정보보호업무 수행기간 : 정보기술업무 수행기간 = 2 : 3

6. 외국에서 취득한 기술자격, 학력 또는 경력은 제1호부터 제5호까지의 기준에 따라 산정한다.

[별표 1의2] <개정 2016. 5. 31.>

허가 및 등록의 결격사유와 관련된 금융관계법령(제19조제2항 관련)

1. 「은행법」
2. 「한국은행법」
3. 「예금자보호법」
4. 「한국산업은행법」
5. 「중소기업은행법」
6. 「장기신용은행법」
7. 「한국수출입은행법」
8. 「자본시장과 금융투자업에 관한 법률」
9. 삭제 <2008.7.29>
10. 삭제 <2008.7.29>
11. 삭제 <2008.7.29>
12. 「보험업법」
13. 「자산유동화에 관한 법률」
14. 「주택저당채권 유동화회사법」
15. 「산업발전법」
16. 「상호저축은행법」
17. 「여신전문금융업법」
18. 「신용보증기금법」
19. 「기술보증기금법」
20. 「신용협동조합법」
21. 「새마을금고법」
22. 「중소기업 창업지원법」
23. 「신용정보의 이용 및 보호에 관한 법률」
24. 삭제 <2008.7.29>
25. 「금융위원회의 설치 등에 관한 법률」
26. 「농업협동조합법」
27. 「수산업협동조합법」
28. 「산림조합법」
29. 「외국환거래법」
30. 「외국인투자촉진법」
31. 「금융산업의 구조개선에 관한 법률」
32. 「금융실명거래 및 비밀보장에 관한 법률」
33. 「금융지주회사법」
34. 「금융회사부실자산 등의 효율적 처리 및 한국자산관리공사의 설립에 관한 법률」
35. 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」
36. 「한국주택금융공사법」
37. 「유사수신행위의 규제에 관한 법률」
38. 「대부업의 등록 및 금융이용자보호에 관한 법률」

[별표 2] <개정 2015.4.14.>

위반행위별 업무정지의 기간 및 과징금의 금액(제26조제1항 관련)

위반행위	근거 법조문	업무정지 기간	과징금 금액
1. 금융회사 또는 전자금융업자가 법 제6조제1항·제2항 또는 제38조제3항·제4항을 위반한 때	법 제43조제2항제1호 법 제46조제2항	3개월	3천만원
2. 금융회사 또는 전자금융업자가 법 제8조제2항 및 제3항을 위반하여 오류를 조사하여 처리를 하지 아니한 때	법 제43조제2항제2호 법 제46조제2항	1개월	1천만원
3. 전자화폐발행자가 법 제16조제1항을 위반한 때	법 제43조제2항제1호 법 제46조제2항	6개월	5천만원
4. 전자화폐발행자가 법 제16조제2항부터 제4항까지의 규정을 위반한 때	법 제43조제2항제1호 법 제46조제2항	3개월	3천만원
5. 금융회사 또는 전자금융업자가 법 제19조제1항 또는 제21조의5제2항을 위반한 때	법 제43조제2항제1호 법 제46조제2항	1개월	1천만원
6. 금융회사 또는 전자금융업자가 법 제21조제1항 또는 제2항을 위반하여 전자금융거래정보를 타인에게 제공 또는 누설하거나 업무상 목적 외에 사용한 때	법 제43조제2항제1호 법 제46조제1항	6개월	50억원
7. 금융회사 또는 전자금융업자가 법 제21조제1항 또는 제2항을 위반한 때. 다만, 제6호에 해당하는 경우는 제외한다.	법 제43조제2항제1호 법 제46조제2항	1개월	1천만원
8. 금융회사 또는 전자금융업자가 법 제23조 또는 제39조제6항에 따른 금융위원회의 조치를 어긴 때	법 제43조제2항제3호 법 제46조제2항	3개월	3천만원
9. 전자금융업자가 법 제35조를 위반한 때	법 제43조제2항제1호 법 제46조제2항	6개월	5천만원
10. 금융회사 또는 전자금융업자가 법 제36조를 위반한 때	법 제43조제2항제1호 법 제46조제2항	6개월	5천만원
11. 금융회사 또는 전자금융업자가 법 제40조제2항 또는 제42조제3항에 따른 금융위원회의 지시 또는 명령을 어긴 때	법 제43조제2항제3호 법 제46조제2항	1개월	1천만원

IT위탁

1. 금융기관의 업무위탁 등에 관한 규정
2. 금융회사의 정보처리 업무 위탁에 관한 규정

금융기관의 업무위탁 등에 관한 규정

[시행 2015.7.1] [고시 제2015 - 20호, 2015.6.30, 타법개정]

제1조(목적) 이 규정은 금융기관이 인가ㆍ허가 또는 등록 등(이하 "인가등"이라 한다)에 따른 업무를 수행함에 있어 당해 업무의 위탁 등에 관한 사항(정보처리 및 전산설비 위탁에 관한 사항은 제외한다)을 정함을 목적으로 한다. <개정 2013.6.25>

제2조(정의) ① 이 규정에서 "금융기관"이라 함은 다음 각호와 같다. <개정 2005. 7. 27>

1. 은행법에 의해 설립된 금융기관
2. 농업협동조합법에 의한 농협협동조합중앙회의 신용사업부문
3. 수산업협동조합법에 의한 수산업협동조합중앙회의 신용사업부문
4. 중소기업은행법에 의한 중소기업은행
5. 신탁업법에 의한 신탁회사
6. 주택저당채권유동화회사법에 의한 주택저당채권유동화회사
7. 상호저축은행법에 의한 상호저축은행 및 그 중앙회
8. 종합금융회사에관한법률에 의한 종합금융회사
9. 여신전문금융업법에 의한 여신전문금융회사
10. 보험업법에 의한 보험회사
11. 증권거래법에 의한 증권회사
12. 선물거래법에 의한 선물업자
13. 신용협동조합법에 의한 신용협동조합 및 그 중앙회, 동법 제95조의 규정에 의한 각 조합 및 그 중앙회의 상호금융부문
14. 기타 금융업 또는 금융관련업무를 영위하는 자로서 금융감독원장(이하 "감독원장"이라 한다)이 정하는 자

② 이 규정에서 "업무위탁"이라 함은 금융기관이 인가등을 받은 금융업을 영위하기 위하여 제3자(개인을 포함한다)의 용역 또는 시설 등을 계속적으로 활용하는 행위를 말한다. 다만, 금융업 영위와 직접적으로 관계되지 아니하는 시설관리 등 단순한 구매ㆍ용역계약은 제외한다. <신설 2005. 7. 27>

③ 이 규정에서 "업무수탁"이라 함은 금융기관이 제3자가 영위하는 업무를 위탁받아 계속적으로 처리하는 행위를 말한다. <신설 2005. 7. 27>

④ 제2항 및 제3항의 규정에 불구하고 외국 금융기관 국내지점의 국내외 본지점간의 용역 또는 시설 등의 공급계약은 이 규정에 의한 업무위탁 또는 수탁으로 간주한다. <신설 2005. 7. 27>

제3조(업무위탁 등) ① 금융기관은 인가등을 받은 업무를 영위함에 있어 제3자에게 업무를 위탁하거나 제3자의 업무를 수탁할 수 있다. 다만, 다음 각호의 1에 해당하는 사항은 그러하지 아니하다. <개정 2005. 7. 27>

1. 인가 등을 받은 금융업의 본질적 요소를 포함하는 업무를 위탁하는 경우 <본호 신설 2005. 7. 27>
2. 관련 법령에서 금융기관이 수행하도록 의무를 부여하고 있는 경우 <본호 신설 2005. 7. 27>
3. 업무의 위탁 또는 수탁으로 인하여 당해 금융기관의 건전성 또는 신인도를 크게 저해하거나 금융질서의 문란 또는 금융이용자의 피해 발생이 심히 우려되는 경우 <본호 신설 2005. 7. 27>

② 제1항 제1호의 본질적 요소에 해당하는 사항은 <별표 1>과 같다. <개정 2005. 7. 27>

1. <본호 삭제 2005. 7. 27>
2. <본호 삭제 2005. 7. 27>
3. <본호 삭제 2005. 7. 27>
4. <본호 삭제 2005. 7. 27>

③ 금융기관이 제1항의 규정에 따라 제3자에게 업무를 위탁하거나 제3자로부터 업무를 수탁하는 경우에는 다음 각호의 사항을 고려하여 동 업무가 적정하게 처리될 수 있도록 하여야 한다. <개정 2005. 7. 27>

1. 업무위탁 또는 수탁에 따른 비용·편익분석 <개정 2005. 7. 27>
2. 금융이용자 피해발생 및 금융질서 문란 여부 <개정 2005. 7. 27>
3. 제3자가 관련 법규에 따라 업무위탁 또는 수탁이 가능한지의 여부 <개정 2005. 7. 27>
4. 제3자가 수탁업무를 적절히 수행할 수 있는지의 여부 <개정 2005. 7. 27>
5. 금융실명거래및비밀보장에관한법률 등 관련법령에의 저촉여부

제3조의2(업무위수탁기준) 금융기관은 제3조에서 정한 업무위탁 등에 따른 리스크의 체계적 관리를 위하여 <별표2>에서 정하는 업무위수탁기준에 따라 금융권역 및 위탁대상자의 특성 등을 감안하여 자체 업무위수탁 운영기준을 마련하고 이를 준수하여야 한다. <신설 2005. 7. 27>

제4조(보고) ① 금융기관이 제3조제1항의 규정에 따라 제3자와 업무위탁 계약을 체결하거나 제3자(금융기관 제외)와 업무수탁계약을 체결하고자 하는 경우에는 그 사실을 동 계약체결 예정일로부터 7영업일 이전에 <별지 제1호 서식>에 따라 다음 각호의 서류를 첨부하여 감독원장에게 보고하여야 한다. <개정 2005. 7. 27>

1. 위탁 또는 수탁 관련 계약서(안) 사본 <개정 2005. 7. 27>
2. 제3조제3항 각호의 고려사항에 대한 검토의견 및 관련자료 사본
3. 위탁 또는 수탁의 필요성 및 기대효과 <개정 2005. 7. 27>
4. 위탁 또는 수탁에 따른 업무처리절차의 주요변경내용 <개정 2005. 7. 27>

② 금융기관은 제1항의 규정에 불구하고 다음 각호의 1에 해당하는 경우에는 제1항에 의한 사전보고를 생략하고, <별지 제2호 서식>에 따라 반기현황을 당해연도 7월말 또는 익년 1월말까지 감독원장에게 보고하여야 한다. 이 경우 관련 협회 등이 회원 금융기관의 현황을 종합하여 보고할 수 있다. <개정 2005. 7. 27>

1. 당해 금융기관 또는 동일한 금융업을 영위하는 다른 금융기관이 감독원장에게 보고한 내용과 동일한 경우로서 위탁 또는 수탁 상대방의 주된 업종이 동일한 경우 <개정 2005. 7. 27>
2. 금융기관이 약관 등을 보고하면서 당해 약관 등의 내용과 관련된 위탁 또는 수탁예정업무를 보고한 경우(제1항에 의한 첨부서류를 제출한 경우에 한한다) <개정 2005. 7. 27>
3. 이미 보고한 내용을 일부 변경하는 경우로서 변경되는 내용이 경미한 경우

③ 감독원장은 제1항 및 제2항의 규정에 의하여 금융기관이 보고한 업무위탁 또는 수탁현황을 매반기 금융위에 보고하여야 한다. <개정 2005. 7. 27>

제5조(변경권고등) 감독원장은 업무위탁 또는 수탁이 제3조의 규정에 적합하지 아니하다고 판단하는 경우에는 당해 금융기관에 대하여 그 내용의 변경권고 등 필요한 조치를 할 수 있다. 이 경우 감독원장은 그 조치결과를 지체없이 금융위에 보고하여야 한다. <개정 2005. 7. 27>

제6조(적용배제) 금융관련법령에서 정하는 바에 따라 금융기관이 제3자에게 업무를 위탁하거나 제3자로부터 업무를 수탁하는 경우에는 이 규정을 적용하지 아니한다. <개정 2005. 7. 27>

제7조 <삭제 2005. 7. 27>

제8조(재검토기한) 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 규정 발령 후의 법령이나 현실여건의 변화 등을 검토하여 이 규정의 유지, 폐지, 개정 등의 조치를 하여야 하는 2015년 7월 1일을 기준으로 매 2년이 되는 시점(매 2년째의 6월 30일까지를 말한다)으로 한다.[개정 2015.6.30]

부칙 <제9999호,2000.1.14>

①(시행일자)이 규정은 2000.1.17.부터 시행한다

②(경과조치)이 규정 시행전에 금융기관이 이 규정에서 정한 업무위탁 또는 수탁을 한 경우 이는 이 규정에 따라 행한 것으로 본다.

③(폐지규정)이 규정의 시행과 동시에 다음 각호의 규정은 폐지한다.

1. 은행감독규정 제16조 및 동 시행세칙 제12조
2. 여신전문금융회사등감독업무시행세칙 제80조

부칙 <제2005 - 39호,2005.7.27>

제1조(시행일) 이 규정은 공고한 날부터 시행한다.

제2조(경과조치) 이 규정 시행당시 금융기관이 제3자에게 업무를 위탁한 경우 또는 제3자로부터 업무를 수탁한 경우에는 계약기간이 종료한 때부터 이 규정을 적용한다.

부칙 <제2008 - 3호,2008.4.4>

이 규정은 고시한 날부터 시행한다.

부칙 <제2012 - 12호,2012.6.26>

이 규정은 고시한 날부터 시행한다.

부칙 <제2013 - 18호,2013.6.25>

제1조(시행일) 이 규정은 고시한 날부터 시행한다.

부칙 <제2015 - 20호,2015.6.30>

이 규정은 2015년 7월 1일부터 시행한다.

【별표1】<개정 2005. 7. 27>

인가등을 받은 금융업의 본질적 요소

구분	본질적 요소
◦ 예금	◦ 예금계약 체결행위 ◦ 채무부담 증명행위 - 자기앞수표 발행, 예금잔액 증명서 발급 등
◦ 대출	◦ 대출심사 및 승인행위 (단, 금융지주회사내 자회사간 전산시스템에 의한 대출심사행위는 제외) ◦ 대출실행
◦ 환거래	◦ 환거래관련 심사 및 승인
◦ 채무보증 또는 어음인수	◦ 채무자에 대한 보증또는 어음 인수의 결정(또는 승인행위) ◦ 채무보증을 위하여 채권자와 보증계약을 체결
◦ 금전(또는 재산) 신탁	◦ 신탁의 인수 ◦ 신탁해지
◦ 유가증권의 위탁매매등	◦ 계좌개설시 고객의 투자목적, 투자성향, 자금력 등 투자 상담 권유에 필요한 고객정보 확인 ◦ 계좌개설계약 체결행위 ◦ 투자권유 및 투자상담(투자권유자료 생산 제외) ◦ 주문 접수, 전달, 집행 및 확인

구분	본질적 요소
◦ 유가증권 인수	◦ 총액인수, 잔액인수 및 모집 매출의 주선 ◦ 공모유가증권의 매수청약 권유 또는 매도 청약 ◦ 기업실사 ◦ 수요예측의 실시 ◦ 공모유가증권의 청약사무 수행 ◦ 공모가 결정 ◦ 공모유가증권의 배정
◦ 유가증권의 자기매매업	◦ 고객을 상대로 한 호가의 제시 및 매매거래의 집행
◦ 보험업	◦ 보험모집 및 계약체결(보험 상품 판매) - 청약서 작성 - 고지사항 수령등 ◦ 보험회사 공시(경영공시 및 상품공시 등) ◦ 보험계약인수(underwriting) 여부에 대한 심사·결정 ◦ 보험계약의 유지 및 관리 - 해지, 실효 및 부활처리 등 - 보험료 영수증(청약서포함) 관리 ◦ 재보험 출 · 수재(해외 포함) - 재보험 계약체결 - 재보험 정산 등 ◦ 재공제(농,수,축협 등) ◦ 보험금 지급여부 심사 및 결정
◦ 기업의 인수·합병 등의 중개, 주선업무	◦ 인수·합병전략 및 영업 전략에 관한 컨설팅 ◦ 가격 협상 및 가격결정 지원

구분	본질적 요소
◦ 어음의 발행, 할인, 매매, 중개, 인수, 및 보증 ◦ CMA	◦ 어음의 발행, 할인, 매매, 중개, 인수, 보증 및 CMA 계약체결 행위 ◦ 채무부담증명 행위 - 어음발행 등의 증명서 발급
◦ 선물거래업	◦ 선물거래제도 및 위험등에 관한 설명 ◦ 선물거래 주문 수탁 및 거래의 체결 ◦ 선물거래 일일 정산 ◦ 증거금 관리 ◦ 청산 ◦ 현금결제 및 실물인수도
◦ 신용카드업	◦ 회원자격 심사 및 발급승인 - 단, 신용리스크를 직접 수반하지 않는 단순업무(모집, 기재사항 확인 등)는 제외 ◦ 이용한도 부여 및 변경 ◦ 신용카드 이용관련 대금결제 ◦ 거래승인 - 단, 전산장애, 해외거래 등 기술적으로 불가피한 경우 제외
◦ 시설대여업	◦ 리스심사 및 승인 ◦ 리스계약체결 ◦ 변경리스계약 체결
◦ 할부금융업	◦ 공급자 및 할부금융이용자와 할부금융계약 ◦ 할부금융 심사 및 승인

구분	본질적 요소
◦ 신기술사업	◦ 투자 및 융자대상 물건에 대한 심사·승인 ◦ 투자 및 융자 계약 체결 - 직접투자(지분인수), 간접투자(사채인수) 및 조건부대출 등 ◦ 이익환수 - 주식상장(코스닥등록 포함) 및 지분매각 ◦ 신기술투자조합설립 및 자금의 관리·운용
◦ 주택저당채권 유동화 업무	◦ 채권유동화계획의 수립 및 등록 ◦ 주택저당채권양수도 등록 ◦ 주택저당채권명세와 그 현황에 대한 서류작성 및 비치 ◦ 채권유동화증권발행 ◦ 주택저당증권에 대한 지급보증

【별표2】<신설 2005. 7. 27>

업무 위수탁 기준

금융회사가 업무 위수탁을 추진하는 경우 다음 각호의 사항을 참고로 하여 업무위수탁운영기준을 제정·운영하여야 한다.

1. 위수탁계약에 따른 리스크 평가 및 관리대책

2. 위수탁계약의 결정·해지 절차 및 재위탁에 관한 사항

3. 위탁업무의 모니터링에 관한 사항

   - 위탁업무 수행관련 주요사항(수탁자의 재무상태 및 리스크, 비상계획 및 그 테스트 결과 등)에 대한 모니터링 절차, 모니터링 담당직원의 지정, 경영진에 대한 보고체계 등에 관한 사항

4. 고객정보의 보호에 관한 사항

   - 위탁금융회사 고객자료의 별도 관리, 인가된 자에게만 접근권 부여 및 비밀보호 위반시 위탁금융회사의 조치권 등 안전장치 확보

5. 비상계획에 관한 사항

   - 수탁자의 부도 또는 통신문제 등 우발상황 발생시 대책에 관한 사항

6. 위탁업무관련 자료에 대한 접근권 확보에 관한 사항

   - 감독당국 또는 내외부 감사인의 자료접근권 보장

7. 위수탁 계약서 주요 기재사항

   - 위수탁업무의 범위(공급주기, 내용, 형태 등)
   - 업무수행의 수단
   - 정보제공 책임(수탁자 내부의 영업상 중요정보 포함)
   - 수탁자에 대한 감사 권한
   - 업무위수탁에 대한 수수료 및 보상금
   - 위탁업무에서 발생하는 자료에 대한 위탁금융회사의 소유권과 당해 금융회사의 물적설비 및 지적재산권 등의 이용조건
   - 고객정보의 보호 및 비밀유지에 관한 사항
   - 업무의 연속성을 확보하기 위한 백업시스템 확보 등 비상계획
   - 면책조항, 보험가입, 분쟁해결(중재, 조정 등) 방법
   - 수탁자의 책임한계
   - 계약의 파기 또는 종료(위탁금융회사의 계약해지권, 자료의 복구방법 등)에 관한 규정
   - 감독당국의 검사 수용의무
   - 수탁자가 업무 재위탁시 원계약 준수 명시
   - 준거법 및 관할법원(업무위수탁 상대방이 외국에 소재하는 경우)
   - 기타 업무위수탁에 따른 리스크관리 등을 위하여 필요한 사항 등

8. 기타 고려사항
   - 금융회사는 금융권역 및 위탁대상자의 특성 등을 감안하여 상기 각호의 사항을 가감하여 반영할 수 있다.

<별지 제1호 서식> <신설 2005. 7. 27>

업무 위수탁 보고

문서번호 :　　20 . . .

수　　신 : 금융감독원장

참　　조 : 해당 감독국장

「금융기관의업무위탁등에관한규정」 제4조제1항에 따라 업무 위수탁 계획을 아래와 같이 보고합니다.

계약건명	
계약상대방 (개인인 경우 계약당사자수)	
계약기간	
계약내용	

※ 첨부서류

1. 계약상대방에 관한 사항(상호, 자본금규모, 소재지, 주된 업종, 개인의 경우 대표자 인적사항 등) 1부
2. 업무 위수탁 관련 계약(안) 사본 1부
3. 동 규정 제3조제3항 각호의 고려사항에 대한 검토의견 및 관련자료 1부
4. 업무 위수탁의 필요성 및 기대효과 1부
5. 업무 위수탁에 따른 업무처리절차의 주요변경내용 1부
6. 기타 관련 또는 참고 서류 각 1부

대표이사　　(인)

작 성 자 : (직 위)	(성명)
연 락 처 :	

<별지 제2호 서식> <신설 2005. 7. 27>

20××년도 상(하)반기 업무위수탁 현황 보고

문서번호 20 . . .

수 신 금융감독원장

참 조 해당 감독국장

「금융기관의업무위탁등에관한규정」 제4조제2항에 따라 20××년 상(하)반기 중 업무위수탁 현황(제4조제1항에 의한 사전보고사항 제외)에 대해 아래와 같이 보고합니다.

계약건명	
계약상대방 (개인인 경우 계약당사자수)	
계약기간	
계약내용	
계약의 필요성 및 기대효과	
사전보고대상에서 제외한 사유	

대표이사 (인)

작 성 자 : (직 위)	(성명)
연 락 처 :	

금융회사의 정보처리 업무 위탁에 관한 규정

[시행 2015.7.22] [고시 제2015 - 27호, 2015.7.22, 일부개정]

제1조(목적) 이 규정은 금융회사가 인가ㆍ허가 또는 등록 등(이하 "인가등"이라 한다)을 받은 금융업을 영위함에 있어 정보처리 업무의 위탁 등에 관한 사항을 규정함을 목적으로 한다. <개정 2015.7.22.>

제2조(정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다. ① "금융회사"라 함은 다음 각 호와 같다.

1. 「은행법」에 따른 은행<개정 2015.7.22.>
2. 「한국산업은행법」에 따른 한국산업은행
3. 「중소기업은행법」에 따른 중소기업은행
4. 「한국수출입은행법」에 따른 한국수출입은행
5. 「자본시장과 금융투자업에 관한 법률」에 따른 금융투자업자, 종합금융회사
6. 「보험업법」에 따른 보험회사
7. 「상호저축은행법」에 따른 상호저축은행
8. 「신용협동조합법」에 따른 신용협동조합
9. 「여신전문금융업법」에 따른 여신전문금융회사
10. 「농업협동조합법」에 따른 농협은행
11. 「수산업협동조합법」에 따른 수산업협동조합중앙회의 신용사업부문
12. 「전자금융거래법」에 따라 허가를 받거나 등록한 전자금융업자

② "외국계 금융회사"라 함은 외국법령에 따라 설립되어 외국에서 금융업을 경영하는 자의 국내 지점 또는 계열사인 전항의 금융회사를 말한다.

③ "계열사"라 함은 해당 금융회사와 주식보유 등을 통하여 하나 이상의 법인이 개재되어 있고, 이들이 모두 상법상의 모회사 또는 자회사의 출자관계로 연결된 경우를 말한다(다만, 상장된 회사의 경우 소유지분 요건을 발행주식 총수의 100분의 30 이상으로 한다).

④ "금융거래정보"라 함은 금융회사(제2조제2항의 외국계 금융회사를 포함한다. 이하 같다)가 인가등을 받은 금융업을 영위하기 위하여 고객과 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제2조제2호 가목 및 나목에 규정된 금융거래행위를 함으로써 거래상대방인 고객으로부터 수집한 해당 고객의 정보 및 금융거래행위의 결과로 생성된 고객의 거래내역 정보를 의미한다.<개정 2015.7.22.>

⑤ "정보처리"라 함은 금융회사가 전산설비를 활용하여, 정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 및 기타 이와 유사한 행위를 하는 것을 말한다.<개정 2015.7.22.>

⑥ "정보처리의 위탁"이라 함은 금융회사가 자신의 정보처리 업무를 제3자로 하여금 계속적으로 처리하도록 하는 행위를 말한다.<개정 2015.7.22.>

⑦ "전산사고"라 함은 정보처리 및 전산설비의 장애, 재해, 파업, 테러 등의 사유로 발생하는 업무의 중단 또는 지연 및 해킹 등 전자적 침해행위가 발생하는 경우를 말한다.

⑧ 이 규정에서 사용하는 용어의 정의는 특별히 정한 경우 외에는 관련법령에서 정하는 바에 따른다.

제3조(적용범위 등) ① 금융회사의 정보처리 위탁과 관련해서는 다른 법령에 특별한 규정이 있는 경우를 제외하고는 이 규정에서 정하는 바에 따른다. <개정 2015.7.22.>

② 금융관련 법령에 따라 금융업의 인가등을 신청한 자에게도 이 규정을 적용한다.<개정 2015.7.22.>

③ 삭제<2015.7.22.>

제4조(정보처리의 위탁) ① 금융회사는 인가등을 받은 업무를 영위함에 있어 정보처리가 요구되는 경우 이를 제3자에게 위탁할 수 있다. <개정 2015.7.22.>

② 제1항의 규정에도 불구하고 다음 각 호의 어느 하나에 해당하는 경우는 정보처리를 위탁할 수 없다. 다만, 다음 제2호의 경우 금융감독원장이 허용하는 방식에 따라 코스콤 또는 저축은행중앙회에 원장 등의 관리를 위탁하는 경우는 제외한다.

1. 관련 법령에서 해당 업무의 위탁을 금지하고 있는 경우
2. 최근 3년 이내에 금융이용자의 정보관리, 감독관련 자료 제출 등 감독기관의 검사와 관련한 사항으로 기관경고 이상의 제재 또는 형사처벌을 2회 이상 받은 경우<개정 2015.7.22.>
3. 기타 업무의 위탁으로 인하여 당해 금융회사의 건전성 또는 신인도를 크게 저해하거나, 금융질서의 문란 또는 금융이용자의 피해 발생이 심히 우려되는 경우

③ 금융회사는 제1항에 따른 정보처리 위탁계약을 체결할 경우 데이터에 대한 접근통제, 전산사고 등에 따른 이용자 피해에 대한 위·수탁회사간의 책임관계, 수탁회사에 대한 감독당국의 감독·검사 수용의무, 수탁회사의 분쟁해결 과정에서의 재판관할 등을 계약 내용에 반드시 포함하여 위탁에 따라 발생할 수 있는 책임관계를 명확히 하여야 한다.<개정 2015.7.22.>

④ 제1항에 따라 정보처리를 위탁받은 자는 위탁받은 업무를 제3자에게 재위탁할 수 있다. 이 경우 본조 제2항·제3항·제5항·제6항, 제5조, 제7조, 제8조를 준용한다.<개정 2015.7.22.>

⑤ 제1항에 따라 정보처리를 위탁받은 자는 정보처리 과정에서 이전받은 정보를 당초 위탁의 범위를 초과하여 다른 목적으로 활용할 수 없다. 다만, 해당 정보 주체의 동의를 얻은 경우는 동의의 범위 내에서 활용할 수 있다.

⑥ 제1항에 따라 정보처리를 위탁하는 경우 위탁된 처리와 관련한 전산설비 및 인력 등은 관련 법령상 인허가를 위한 전산설비 및 인력 구비 요건 등의 충족 여부를 판단시 고려한다.<개

정 2015.7.22.>

⑦ 제1항에 따라 정보처리를 위탁하는 경우(제4항에 따라 재위탁하는 경우를 포함한다) 위탁회사는 수탁회사가 이 규정 등 관계법령 및 제3항에 따른 위탁계약 내용상의 의무를 위반하여 발생하는 정보주체 및 이용자의 손해에 대하여 수탁회사와 연대하여 책임을 진다.<개정 2015.7.22.>

제5조(특정정보의 보호) ① 제4조에 따라 정보처리를 위탁하는 경우 금융회사는 각 관련 법령상의 안전성 확보조치를 충실히 이행하여야 한다. 이 때 개인고객의 고유식별정보는 암호화 등의 보호 조치를 하여야 하며, 특히 국외로 이전되지 않도록 하여야 한다. <개정 2015.7.22.>

② 금융회사는 위탁 처리되는 정보의 보호를 위한 안전성 확보조치의 구체적 내용을 홈페이지 등을 통해 공시하여야 한다. 또한 민감정보의 처리를 위탁할 경우에는 정보주체에게 금융감독원장이 정하는 방법에 따라 개별 고지하여야 한다.

제6조 삭제 <2015.7.22.>

제7조(보고) ① 금융회사가 제4조제1항에 따라 개인고객의 금융거래정보(금융거래의 내용이 누구의 것인지를 알 수 없는 경우를 제외한다) 처리업무를 위탁하고자 하는 경우로서 업무를 수탁받는 자가 국외에 소재하는 경우에는 그 사실을 동 위탁계약의 체결예정일로부터 30영업일 이전에 다음 각 호의 서류를 첨부하여 금융감독원장에게 보고하여야 한다. <개정 2015.7.22.>

1. 위탁계약서(안) 사본
2. 「금융기관의 업무위탁 등에 관한 규정」 제3조의2에 따라 금융기관이 마련하고 준수하여야 할 ‘업무위탁 운영기준’
3. 업무위탁 계약이 이 규정 등 관련법령에 위배되지 아니한다는 준법감시인(준법감시인이 없는 경우, 감사 등 이에 준하는 자)의 검토의견 및 관련자료 사본
4. 위탁의 필요성 및 기대효과
5. 위탁에 따른 업무처리절차의 주요 변경내용
6. 정보처리업무 운영에 대한 감독기관의 실질적 감독가능성을 확인할 수 있는 서류
7. 위탁계약 상대방(재위탁 예정시 재위탁계약 상대방 포함)에 관한 사항(상호, 자본금 규모, 소재지, 주된 업종, 개인의 경우 대표자 인적사항 등)

[본호신설 2015.7.22.]

8. 전산사고 및 정보유출 등 발생시 피해자 구제절차

[본호신설 2015.7.22.]

② 금융회사가 제4조제1항에 따라 개인고객의 금융거래정보(금융거래의 내용이 누구의 것인지를 알 수 없는 경우를 제외한다) 처리업무를 위탁하고자 하는 경우로서 업무를 수탁받는 자가 국내에 소재하는 경우에는 그 사실을 동 위탁계약의 체결예정일로부터 7영업일 이전에 제1항 각 호의 서류를 첨부하여 금융감독원장에게 보고하여야 한다.<개정 2015.7.22.>

③ 금융회사가 제1항 및 제2항에 따른 보고의 대상이 되는 금융거래정보를 제외한 금융거래정보의 처리를 위탁하는 경우에는 그 사실을 동 위탁계약의 체결일로부터 10영업일 이내에 제1항 각 호의 서류를 첨부하여 금융감독원장에게 보고하여야 한다.
[본항신설 2015.7.22]
④ 금융회사는 다음 각 호의 구분에 따라 정보처리 위탁에 관한 반기 현황을 해당 연도 7월말 또는 이듬해 1월말까지 금융감독원장에게 보고하여야 한다. 이 때 금융감독원장은 관련 협회 등이 회원 금융회사의 현황을 종합하여 보고하게 할 수 있다.
1. 제2조제4항에 따른 금융거래정보의 처리업무를 위탁하는 경우로서 다음 각 목에 해당하는 경우
가. 해당 금융회사 또는 동일한 금융업을 영위하는 다른 금융회사가 금융감독원장에게 보고한 내용과 동일한 경우로서, 위탁 상대방의 업종이 동일한 경우
나. 이미 보고한 내용을 일부 변경하는 경우로서, 변경되는 내용이 경미한 경우
2. 제2조제4항에 따른 금융거래정보 이외의 정보 처리업무를 위탁하는 경우
[본항신설 2015.7.22]
⑤ 금융감독원장은 이 규정에 따른 보고 절차 등과 관련하여 필요한 경우 「금융기관의 업무위탁 등에 관한 규정」의 서식을 사용하도록 할 수 있다.
[종전 제3항에서 이동]

제8조(감독 및 검사) ① 위탁 금융회사 및 해당 업무의 수탁회사는 제4조에 따라 위탁 운영되는 정보처리 업무와 관련하여 금융감독원장의 자료 제출 등 감독 및 검사를 위한 요구에 응하여야 한다. <개정 2015.7.22.>
② 삭제<2015.7.22.>
③ 금융감독원장은 이 규정에 따른 금융회사의 업무 위탁 현황을 매 반기 금융위원회에 보고하여야 한다.
④ 금융감독원장은 위탁회사 또는 수탁회사의 정보처리 위탁행위 또는 위탁된 업무의 수행과 관련된 행위가 이 규정 등 관계법령, 제7조제1항제2호의 ‘업무위탁 운영기준’에 적합하지 아니하다고 판단하는 경우에는 위탁회사 또는 수탁회사에 대하여 그 내용의 자료제출 및 보완요구, 변경권고 등 필요한 조치를 할 수 있다.<개정 2015.7.22.>

제9조(재검토기한) 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제334호)에 따라 이 규정 발령 후의 법령이나 현실여건의 변화 등을 검토하여 이 규정의 유지, 폐지, 개정 등의 조치를 하여야 하는 기한은 2018년 6월 30일까지로 한다. <개정 2015.7.22.>

부칙 <제2013-17호,2013.6.25>
제1조(시행일) 이 규정은 고시한 날부터 시행한다.

제2조(경과조치) 이 규정은 최초 시행시, 관련 법령에 따라 적법하게 위탁?운용되고 있는 정보처리 및 전산설비와 관련하여 추가적인 의무나 제약을 부담하게 하는 것으로는 해석되지 아니한다.

부칙 <제2015 - 27호,2015.7.22>

제1조(시행일) 이 규정은 고시한 날부터 시행한다.

전자금융 및 개인정보 관련 법규

제 작 자 : 멋진사람
기관/부서 : 좋은회사
전화번호 : 000-0000-0000
메일주소 : cissp74@gmail.com
주 소 : 서울시 땡땡구 땡땡동
제작일자 : 2017.3.8

법제처 국가법령정보센터