정보보호 관리체계(ISMS) 인증 제도 안내서

2013. 6.

미래창조과학부 Ministry of Science, ICT & Future Planning

KISA 한국인터넷진흥원 Korea Internet & Security Agency

< 참 고 >

현재, 정보보호 관리체계 인증 관련 법률 소관부서는 정부조직법(2013.3.23. 공포 및 시행)에 따라 '방송통신위원회'에서 '미래창조과학부'로 변경되었음. 본 안내서의 법률과 시행령에는 변경된 소관부서명이 반영되었으나, 일부 고시 내용에는 반영되지 않음. 추후 업데이트 예정.

들 어 가 기

본 안내서는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조(정보보호 관리체계의 인증), 시행령, 고시 등에서 규정하고 있는 사항에 대하여 보다 구체적으로 설명함을 목적으로 한다.

본 안내서는 정보보호 관리체계(ISMS)를 구축하고 인증을 받기를 원하는 모든 기업이 활용할 수 있으며, 인증심사원, 보안컨설팅 업체, ISMS 구축에 관심이 있는 다양한 산업 분야에서도 본 안내서를 참고하여 인증심사, 컨설팅, ISMS 구축 및 운영 등에 이용이 가능하다.

본 안내서의 내용은 정보보호 관리체계(ISMS) 인증 제도의 개요, 인증 대상자, 인증 절차 및 기준, 주요 추진체계, 구축 및 운영 등의 내용으로 구성되어 있다.

기존의 정보보호 관리체계(ISMS) 구축 기업이 본 안내서를 참고할 경우, 변경된 내용을 확인하여 인증심사 준비에 차질이 없도록 유의해야 한다.

본 안내서의 내용은 기존의 정보보호 관리체계(ISMS) 관련 안내서(해설서) 내용을 개정한 것으로 지속적인 보완 작업을 통하여 변경될 수 있으므로 항상 최신 버전인지 여부를 확인 후 사용해야 한다.

본 안내서는 한국인터넷진흥원 홈페이지(http://www.kisa.or.kr) 및 ISMS 인증 제도 홈페이지(http://isms.kisa.or.kr)에 게재되어 있으며, 기타 문의 사항이 있으시면 아래로 문의해 주시기 바랍니다.

Tel : (02) 405-5233 E-mail : kisa_isms@kisa.or.kr

KISA 한국인터넷진흥원 Korea Internet & Security Agency

목 차

제 1 장 정보보호 관리체계(ISMS) 인증 제도 개요

1.1 인증 제도 도입 배경 ····· 5
1.2 인증 제도 추진 경과 ····· 7
1.3 인증 추진 체계 ····· 8
1.4 인증 프로세스·방법·인증대상자 요약 ····· 9
1.5 구축 기대 효과 ····· 10

제 2 장 정보보호 관리체계(ISMS) 인증대상자 및 절차·기준

2.1 인증대상자 ····· 11
2.2 인증 범위 ····· 23
2.3 인증 절차 ····· 26
2.4 인증 기준 ····· 37
2.5 기타 고려사항 ····· 43

제 3 장 정보보호 관리체계(ISMS) 인증 주요 추진체계

3.1 인증위원회 ····· 44
3.2 인증심사원 ····· 47
3.3 인증기관 ····· 53

제 4 장 정보보호 관리체계(ISMS) 구축 및 운영

4.1 정보보호 관리체계 구축 준비 및 전략 수립 단계 ····· 57
4.2 정보보호정책 수립 및 범위설정 단계 ····· 59
4.3 경영진 책임 및 조직 구성 단계 ····· 63
4.4 위험관리 단계 ····· 65
4.5 정보보호 대책 구현 단계 ····· 71
4.6 사후관리 단계 ····· 74
4.7 운영 단계 ····· 79

부 록

□ 인증 신청 제출 서류 및 작성 방법

[붙임 1] 정보보호 관리체계 인증신청서 ····· 82

[붙임 2] 정보보호 관리체계 명세서 ····· 83

□ 인증 심사 관련 문서

[붙임 3] 사전점검(심사) 체크리스트 ····· 142

[붙임 4] 보완조치 요청서 ····· 143

[붙임 5] 결함보고서 ····· 144

[붙임 6] 보완조치 내역서 ····· 146

□ 인증 관련 법령 및 인증 기준

[붙임 7] 정보보호 관리체계 인증 등에 관한 고시 전문 ····· 148

[붙임 8] ISMS 인증 관련 정보통신망법-시행령-하위고시(3단비교표) · 201

[붙임 9] 인증 기준 세부점검항목 ····· 225

제1장 정보보호 관리체계(ISMS) 인증 제도 개요

1.1 인증 제도 도입 배경

o 2009년 7·7 DDoS 공격, 2011년 은행 전산망 마비, 2012년 통신사 개인정보 대규모 유출 사고 등에서 보여지 듯, 사이버 공격은 기업의 기밀이나 개인정보 등의 특정 정보를 목표로 지능화, 고도화되고 있다.

- 이는 기업의 첨단 기술의 유출, 기업 신뢰도 하락과 고객 이탈, 주가 하락뿐만 아니라 집단소송과 대규모 피해보상 등 사회·경제적인 측면에서 큰 문제를 발생시켰다.

- 이러한 문제를 해소하기 위한 그동안의 기술적 대응 노력은 '일회성 관리', '부분적 보안' 등의 한계에 도달하였으며, 이로 인해 '지속적 관리', '전사적 보안'을 위한 보다 높은 수준의 보안관리 활동이 가능한 정보보호 관리체계(ISMS) 구축이 요구되었다.

※ ISMS : Information Security Management System

o 따라서, 기업의 경영진은 정보보호가 기업의 비즈니스 경영방침과 연계될 수 있도록 정보보호최고책임자 지정, 전사적 정보보호정책 수립, 인력 및 예산 등의 의사결정에 직접 참여할 수 있는 정보보호 관리체계의 구축을 무엇보다 시급하게 요구가 되었다.

- 또한, 그간의 정보보호정책 및 법제도의 한계에서 벗어나 기업 내 정보자산을 효과적으로 보호할 수 있는 새로운 접근방법과 위험관리 기반의 정보보호 관리체계 수립이 필요하게 되었다.

☞ 정보보호 관리체계

정보자산의 비밀성·무결성·가용성을 달성하기 위하여 각종 보안 대책을 관리하고, 위험기반 접근방법에 기초하여 구축·구현·운영·모니터링·검토·개선 등의 주기를 거쳐 정보보호를 관리하고 운영하는 체계

o 기업의 정보보호는 지출해야 하는 비용의 개념이 아니라, 비즈니스 기회를 예측하고 현재와 미래의 위험에 적절히 대응할 수 있는 핵심 경쟁력인 동시에, 예상하지 못한 위기상황에서 기업전반의 비즈니스 안정성을 유지하고 정보자산을 적절하게 보호하기 위한 경영활동의 일부로 보아야 한다.

- 정보보호에 대한 경영진의 관심과 의지가 무엇보다 중요하기 때문에 최근 주요 기업에서 발생한 대부분의 해킹사고는 내부관리 소홀 및 정보보호에 대한 경영진의 의사결정 지원 미흡 등이 원인이라 할 수 있다.

o 기업이 구축한 정보보호 관리체계의 적합성을 판단하여 인증을 부여하는 정보보호 관리체계 인증 제도는 기업의 정보보호에 대한 인식 및 수준을 제고 하는데 기여하고 있다.

☞ 정보보호 관리체계 인증 제도

어떤 조직이 정보보호 관리체계를 구축·운영하고 있을 때, 그 관리체계가 정보보호 관리체계의 인증기준에 적합한지를 인증기관이 객관적이고 독립적으로 평가하여 적합성 여부를 판단해 주는 제도

(그림1-1) 정보보호 관리체계의 필요성

1.2 인증 제도 추진 경과

o 국내 기업이 스스로 정보보호 관리체계를 구축·운영하는데 활용할 수 있도록 관리체계 모델을 개발하고, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 정보통신망법) 개정을 통하여 정보보호 관리체계 인증 제도를 도입하였다.('01.7월)

- 국내 기업의 실정을 반영한 관리체계를 도입하였으며, 이를 통해 기업 정보보호 수준을 제고하고자 하였다.

o 2003년 1.25 인터넷 대란 이후에 기업이 최소한의 보안조치를 하도록 의무화하여 시행하던 종전의 정보보호 안전진단 제도를 실효성 문제 등으로 폐지하고 보다 높은 수준의 정보보호 관리체계 인증 제도로 일원화 하였다.

- 또한, 주요정보통신서비스제공자를 정보보호 관리체계 인증 제도의 인증 의무대상자로 지정하여 운영하게 되었다.

※「정보통신망 이용촉진 및 정보보호 등에 관한 법률」개정 ('12.2.17)

[표1-1] 정보보호 관리체계 추진 경과

구분		내용
2001	1월	- 정보통신망법 개정
	7월	- 정보통신망법 시행 - 정보보호 관리체계 인증 제도 도입
2002	5월	- 인증기준 고시 (정보통신부고시 제2002-22호) - 인증업무지침 공포 (한국인터넷진흥원)
2004	1월	- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제46조의3(정보보호 안전진단) 개정으로 정보보호 안전진단 제도 도입
2012	2월	- 정보통신망법 개정 (정보보호 안전진단의 실효성 문제 등으로 더 높은 수준의 정보보호 관리체계 인증 제도로 일원화)
2013	2월	- 정보통신망법 개정에 따라 주요정보통신서비스제공자를 인증 의무대상자로 지정하여 운영 (정보보호 안전진단 제도 폐지)

1.3 인증 추진 체계

o 정보보호 관리체계(ISMS) 인증 추진체계는 미래창조과학부, 인증기관, 인증위원회, 인증심사원으로 구성된다.

- 현재 정보보호 관리체계의 인증 등의 사업을 하는 한국인터넷진흥원이 단일 인증(Certification) 기관으로써 인증에 관한 업무를 수행하고 있다.

관련근거

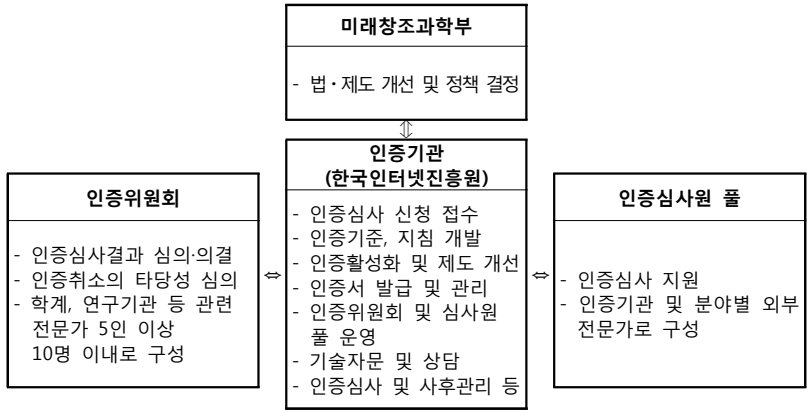
정보통신망 이용촉진 및 정보보호 등에 관한 법률

제47조(정보보호 관리체계의 인증)
⑤ 미래창조과학부장관은 한국인터넷진흥원 또는 미래창조과학부장관이 지정한 기관(이하 "정보보호 관리체계 인증기관"이라 한다)으로 하여금 제1항 및 제2항에 따른 인증에 관한 업무를 수행하게 할 수 있다.

관련근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률

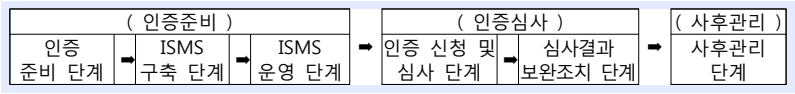
제52조(한국인터넷진흥원)
① 인터넷진흥원은 다음 각 호의 사업을 한다.
7. 정보보호 관리체계의 인증, 정보보호시스템 평가·인증 등 정보보호 인증·평가 등의 실시 및 지원



(그림1-2) 정보보호 관리체계 인증 추진체계

1.4 인증 프로세스・방법・인증대상자 요약

o 인증 프로세스는 인증준비 단계부터 사후관리 단계로 이루어진다.



(그림1-3) 정보보호 관리체계 인증 프로세스

- 인증준비 단계 : 관리체계 및 인증 이해, 전략적 목적의 명확화, 인증 취득 계획 구축, 경영자의 지원 설득
- 구축 단계 : 관리적・기술적・물리적 관리체계 구축
- 운영 단계 : 보안활동에 따른 증적자료 산출
- 인증 신청 및 심사단계 : 인증 신청 및 인증심사원 심사 수행
- 심사결과 보완조치 단계 : 심사결과에 따른 결함사항 보완
- 사후관리 단계 : 지속적인 운영을 위한 관리체계 점검

o 심사 방법은「서면심사 및 현장심사 → 보완조치 확인」을 통해 이루어진다.

- 서면심사 : 정보보호 정책, 지침, 절차 및 이행의 증적자료 검토, 정보보호 대책 적용 여부 확인 등의 방법으로 관리적 요소를 심사
- 현장심사 : 서면심사의 결과와 기술적・물리적 보호대책 이행 여부를 확인하기 위하여 담당자 면담, 관련 시스템 확인 및 취약점 점검 등의 방법으로 기술적 요소를 심사
- 보완조치 확인 : 인증심사에서 발견된 결함사항에 대한 조치 내역을 확인

o 인증대상자는 자율신청기업과 인증 의무대상자로 구분되며, 인증 의무대상자가 인증을 받지 않으면 과태료 1천만원이 부과된다.

- 자율신청기업 : 정보보호 관리체계를 구축・운영하여 적합성 여부의 판단을 원하는 모든 조직
- 인증 의무대상자 : 인터넷에 지대한 영향을 끼칠 수 있는 ISP・IDC・쇼핑몰 및 포털 등의 주요정보통신서비스제공자

1.5 구축 기대 효과

o 단순 일회성, 단편적 정보보호대책에서 벗어나 조직적이고 종합적인 정보보호 대책을 구현함으로써 기업의 정보보호관리 수준을 향상 시킬 수 있다.

o 기업은 지속적이고 체계적인 정보보호 관리체계 구축을 통해 해킹, DDoS 등의 침해사고 발생 시 신속하게 대응할 수 있으며, 피해에 대한 손실을 최소화 할 수 있다.

o 경영진 차원에서의 상시 모니터링 체계 구축이 가능하고, 경영진이 직접 정보보호 의사결정 지원에 참여함으로써 기업은 사이버 침해사고에 효율적으로 대처가 가능하다.

o 인증을 취득한 기업 입장에서는 입찰 시 가산점 부여 등의 인센티브를 얻을 수 있다.

[표1-2] 정보보호 관리체계 인증 취득에 따른 인센티브

구분	시행 기관	혜택 내용
가산점 부여	산업통상 자원부	- 소프트웨어 기술성 평가기준(지식경제부고시 제2010-53호) ※ 적용대상 : 공공부문 정보시스템 기획·구축·운영 사업자, SW개발 사업자 등 ※ 혜택 : 기술입찰서, 계약이행능력 심사, 제안서 등 평가항목(기밀보안)에 정보보호 관리체계 인증취득 시 만점 부여 - 업무수행능력 평가기준(지식경제부 공고 제2010-478호) ※ 적용대상 : 보안관제 전문업체 ※ 혜택 : 보안관제 전문업체 "업무수행능력 평가기준"의 신뢰도 항목에서 정보보호 인증기업에 5점 만점 부여
	한국 인터넷진흥원	- 정보보호大賞·입찰·과제선정 평가 시 가점 부여
	신용평가기관	- 한국신용평가정보 등의 경우 기업신용평가 시 가점 부여
	한국기업지배구조원	- 상장기업 ESG(환경, 사회, 지배구조) 평가 시, 소비자 항목에 가산점 부여(2010년 신설 혜택)
요금 할인	보험사 (11개)	- 정보보호관련 보험(개인정보보호배상책임보험 등) 가입 시 보험료 할인(AIG, LIG, 그린손해보험, 동부화재, 롯데손해보험, 메리츠화재, 삼성화재, 제일화재, 한화손해보험, 현대해상, 흥국화재)
권고	교육부	- 원격대학에 대하여 정보보호 관리체계 인증 취득 권고 ※ 교육과학기술부 고시 제2013-12호
	국토 교통부	- 유비쿼터스도시기반시설에 대하여 정보보호 관리체계 인증 취득 권고(유비쿼터스도시의 건설 등에 관한 법률 제22조)

제2장 정보보호 관리체계(ISMS) 인증대상자 및 절차·기준

2.1 인증대상자

o 자율신청기업은 정보통신망법 제47조제1항에 따라 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 '정보보호 관리체계'라 한다)를 수립·운영하고 있는 자를 말한다.

o 인증 의무대상자는 정보통신서비스 제공자로서 정보통신망법 제47조제2항에 따라 주요정보통신서비스제공자로 일정 규모 이상의 정보통신서비스제공자를 말한다.

- 기업은 스스로 인증 의무대상자 기준에 해당하는지를 판단해야 하며, 인증 의무대상자 기준에 해당할 경우 정보보호 관리체계의 구축·운영 및 인증심사를 통해 인증을 취득하면 된다.

2.1.1 자율신청기업

o 인증 의무대상자 기준에 해당하지 않으나 자발적으로 정보보호 관리체계를 구축·운영하는 기업은 자율신청기업으로 분류되며, 자율신청기업이 인증 취득을 희망할 경우 자율적으로 신청하여 인증심사를 받을 수 있다.

※ 의료, 교육, 금융 등 모든 산업 분야에서 신청 및 인증심사가 가능

관련근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제47조(정보보호 관리체계의 인증)
① 미래창조과학부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 구축·운영하고 있는 자에 대하여 제3항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.

2.1.2 인증 의무대상자

o 정보통신서비스제공자 중 인증 의무대상자는 ①정보통신망서비스를 제공하는 자(ISP), ②집적정보통신시설 사업자(IDC), ③연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자이다.

관련근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제47조(정보보호 관리체계의 인증)
② 정보통신서비스제공자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.
1. 「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자
2. 집적정보통신시설 사업자
3. 연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자

관련근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률

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>
3. "정보통신서비스 제공자"란 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

관련근거

전기통신사업법

제2조(정의)
이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2011.5.19>
6. "전기통신역무"란 전기통신설비를 이용하여 타인의 통신을 매개하거나 전기통신설비를 타인의 통신용으로 제공하는 것을 말한다.
8. "전기통신사업자"란 이 법에 따른 허가를 받거나 등록 또는 신고(신고가 면제된 경우를 포함한다)를 하고 전기통신역무를 제공하는 자를 말한다.

o 기업은 스스로 법에서 정한 인증 의무대상자 기준에 해당하는지 여부를 확인하여 인증을 받아야 한다.

- 인증 의무대상자의 서비스 별 분류는 [표2-1], [표2-2], [표2-3]을 참고한다.

[표2-1] 정보통신서비스 분류체계 (예시)

대분류	중분류	소분류	세분류
정보통신서비스	기간통신서비스	유선통신서비스	전화서비스
			전용회선서비스
			초고속망 서비스
			전신, 전보서비스
			기타 유선통신서비스
		무선통신서비스	이동통신서비스
			무선고정통신서비스 (B-WLL)
			위성통신서비스
	별정통신서비스	설비보유재판매	음성재판매
			인터넷전화
			국제콜백전화
			국제회선재판매
			고속접속서비스
			기타
		설비미보유재판매	재과금서비스
			호집중서비스
			인터넷전화
			무선재판매
			초고속접속서비스
		구내통신	
	부가통신서비스	네트워크서비스	
		인터넷접속 및 관리서비스	인터넷접속기반 서비스
			호스팅 및 관리 서비스
		부가통신 응용서비스	고도팩스서비스
			신용카드검색(CCIS)서비스
			컴퓨터예약(CRS)서비스
			전자문서교환(EDI)서비스
			원격통신서비스
			전자지불서비스
			온라인정보처리
			인터넷전자상거래(수수료)
			기타 부가통신응용 서비스
		콘텐츠제공서비스	콘텐츠제공서비스 (전화수수료)
			콘텐츠제공서비스 (인터넷·모바일)
			기타_콘텐츠서비스
		기타 부가통신서비스	
	방송서비스	지상파방송서비스	라디오방송
			TV방송
			지상 DMB
		유선방송서비스	종합유선방송
			중계유선방송
			음악유선방송
		위성방송서비스	위성방송
			위성 DMB
		프로그램 제작·공급	방송채널사용사업(PP)
			프로그램 제작업
		기타방송 서비스	

※ 한국정보통신기술협회(TTA)의 정보통신부문 상품 및 서비스 분류체계 참조(2007.12.26 개정)

※ 주요정보통신서비스제공자의 모든 서비스와 일치하지 않을 수 있음

[표2-2] 정보통신서비스 분류 (예시)

중분류	소분류	세분류	세세분류
통신업	우편업	우편업	우편업
	전기통신업	유선통신업	유선통신업
		무선통신업	무선통신업
		위성통신업	위성통신업
		기타 전기통신업	통신 재판매업
			그외 기타 전기 통신업
컴퓨터 프로그래밍, 시스템 통합 및 관리업	컴퓨터 프로그래밍, 시스템 통합 및 관리업	컴퓨터 프로그래밍 서비스업	컴퓨터 프로그래밍 서비스업
	컴퓨터시스템 통합 자문, 구축 및 관리업	컴퓨터시스템 통합 자문 및 구축 서비스업	
		컴퓨터시설 관리업	
	기타 정보기술 및 컴퓨터운영 관련 서비스업	기타 정보기술 및 컴퓨터운영 관련 서비스업	
정보서비스업	자료처리, 호스팅, 포털 및 기타 인터넷 정보매개서비스업	자료처리, 호스팅 및 관련 서비스업	자료 처리업
			호스팅 및 관련 서비스업
		포털 및 기타 인터넷 정보매개 서비스업	포털 및 기타 인터넷 정보매개 서비스업
	기타 정보 서비스업	뉴스 제공업	뉴스 제공업
		그외 기타 정보 서비스업	데이터베이스 및 온라인정보 제공업
			그외 기타 정보 서비스업

※ 통계청의 한국표준산업분류(9차 개정) 분류항목표 참조 (통계청 고시 제 2007-52호)

[표2-3] 인증 의무대상자 서비스 별 분류 (예시)

분야			
주요 정보통신 서비스 제공자	ISP		
집적 정보통신 시설 사업자	IDC		
쇼핑몰 등 정보통신서비스 제공자	인터넷 전자상거래	쇼핑몰 서비스	종합
			도서
			식품
			의류
			컴퓨터
			기타
		전자상거래 서비스	온라인 마켓플레이스
			게임 아이템
			네트워크 마케팅
			B2B/무역
		포털	
		인터넷 신문/방송	
		인터넷 게임	
		취업정보	
		정보제공	
		인터넷예약	
		카드조회/지불중계 등	
		인터넷 뱅킹, 온라인 증권 중개, 홈트레이딩 등	
		전문정보 제공서비스	음악
			교육
		기타	
	네트워크 제공	초고속 인터넷 서비스	Cable-SO
		VIDC	
		기타	

※ 인터넷 증권 중개, 인터넷 부동산 중개, 인터넷 인력 알선 등 인터넷을 통하여 특정한 산업 활동을 수행한다면 정보서비스업에 해당함

< 인증 의무대상자 기준① >

정보통신망서비스를 제공하는 자

관련근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제47조(정보보호 관리체계의 인증)
② 정보통신서비스제공자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.
1.「전기통신사업법」제6조제1항에 따른 허가를 받은 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자

※ 정보통신망서비스 제공자의 경우, 매출액과 이용자 수에 관계없이 인증 의무대상자에 해당함

o 정보통신망서비스를 제공하는 자(ISP)란「전기통신사업법」제6조제1항에 따른 기간통신사업 허가를 받고, 인터넷 서비스, 인터넷전화 서비스, 이동통신 서비스 등 정보통신망 서비스 제공 지역이 '서울특별시 및 모든 광역시'인 사업자를 말한다.

※ 모든 광역시 : 인천광역시, 대전광역시, 광주광역시, 대구광역시, 울산광역시, 부산광역시

관련근거

전기통신사업법

제6조(기간통신사업의 허가 등)
① 기간통신사업을 경영하려는 자는 미래창조과학부장관의 허가를 받아야 한다.

관련근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

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.

[표2-4] 정보통신망서비스

대분류	중분류	소분류	세분류
정보통신서비스	기간통신서비스	유선통신서비스	전화서비스
			전용회선서비스

			초고속망 서비스
			전신, 전보서비스
			기타 유선통신서비스
		무선통신서비스	이동통신서비스
			무선고정통신서비스(B-WLL)
			위성통신서비스

※ '서울특별시 및 모든 광역시'에서 서비스를 제공하지 않는 정보통신망서비스 제공자의 경우, 정보통신망법 제47조제2항제3호의 기준을 적용함

※ 인터넷 서비스를 위한 정보통신망이 아닐 경우, 인증 의무대상자에 해당되지 않음

< 인증 의무대상자 기준② >

집적정보통신시설 사업자

관련근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제47조(정보보호 관리체계의 인증)
② 정보통신서비스제공자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.
2. 집적정보통신시설 사업자

※ 집적정보통신시설 사업자의 경우, 매출액과 이용자 수에 관계없이 인증 의무대상자에 해당함

o 집적정보통신시설 사업자(IDC)란 정보통신망법 제46조제1항의 규정에 따라 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자를 말한다.

관련근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률

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.

- 정보통신서비스 제공을 위해 자체적으로 시설을 구축하여 운영하는 자로서, 공간 임대서비스(Co-location) 또는 서버 임대(서버호스팅) 서비스 및 네트워크 서비스 등을 제공하는 사업자를 말한다.

- 다만, 인증 의무대상자 중 타인에 의해 구축된 집적정보통신시설의 일부를 임대하여 서비스를 재판매하는 사업자(이하 VIDC)의 경우에는 정보통신망법 제47조제2항제3호에 따라 연간 매출액 또는 이용자 수 기준을 적용한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제49조(정보보호 관리체계 인증 대상자의 범위)
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.

[표2-5] 집적정보통신시설 서비스

대분류	중분류	소분류	세분류
정보통신서비스	부가통신서비스	네트워크서비스	
		인터넷 접속 및 관리서비스	인터넷접속기반 서비스
			호스팅 및 관리 서비스

< 인증 의무대상자 기준③ >

연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자

관련근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제47조(정보보호 관리체계의 인증)
② 정보통신서비스제공자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.
3. 연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자

o 쇼핑몰, 포털 등의 정보통신서비스를 제공하는 자는 연간 매출액 및 이용자 수 등 대통령령으로 정하는 기준(매출액 100억 이상 또는 일평균 이용자 100만명 이상)에 해당하는 자를 말한다.

관련근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

제49조(정보보호 관리체계 인증 대상자의 범위)
② 법 제47조제2항제3호에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.
1. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자
2. 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 100만명 이상인 자

(매출액 기준 : 전년도 매출액 100억 이상)

- 정보통신서비스 부문 매출액은 정보통신서비스 제공을 통해 발생하는 연간 총 매출액의 합으로 산정하며, 여러 가지 정보통신서비스를 제공할 경우에는 해당 서비스의 매출액을 모두 합하여 계산한다.

※ 매출액은 국세청 등에 신고된 금액으로 하며 이외에 내부적으로 결산자료 등을 마련하여 공인회계사 등의 검증을 거친 객관적 자료를 이용하며, 이러한 자료가 없으면 내부 회계자료에 대해 부서장의 승인을 거친 자료를 이용

[표2-6] 주요 정보통신서비스 매출액 구분 (예시)

구분	서비스 설명	정보통신서비스 부문 매출액 내역
신용카드 검색 (CCIS)서비스	인터넷으로 신용카드의 도난분실, 한도초과, 연체 등을 실시간으로 확인하는 서비스를 제공하는 사업자	카드조회수수료, 서비스매출, 회원수익매출, 부가수익 등
컴퓨터 예약 (CRS)서비스	인터넷을 통해 서비스나 상품에 대한 예약서비스를 제공하는 사업자	상품 및 서비스 판매매출, 수수료, 회원수익매출, 광고매출, 부가수익 등
전자문서교환 (EDI)서비스	인터넷을 통해 전자문서교환서비스를 제공하는 사업자	콘텐츠 판매매출, 수수료, 광고매출, 회원수익매출, 부가수익 등
전자지불 (PG)서비스	인터넷을 통해 지불중계역무를 제공하는 사업자	지불중계수수료, 서비스매출, 회원수익매출, 부가수익 등
인터넷 포털 서비스	인터넷 유·무선 포털 사이트를 제공하는 사업자	온라인 광고매출, 정보제공 수수료, 중계 수수료, 콘텐츠, 이용매출, 부가수익 등
인터넷 전자상거래	쇼핑몰 역무를 제공하는 사업자	판매 매출, 수수료, 광고매출, 부가수익 등
인터넷 방송	인터넷을 통해 신문기사나 방송프로그램을 제공하는 사업자	콘텐츠 판매매출, 수수료, 광고매출, 회원수익매출, 부가수익 등
인터넷 게임	인터넷게임서비스를 제공하는 사업자	게임이용매출, 아이템 판매매출, 광고매출, 수수료, 부가수익 등
금융 관련 서비스	인터넷을 통한 금융업, 연금업, 보험 관련 서비스업 등을 제공하는 사업자	인터넷 뱅킹 · 주식 거래 · 선물 거래 수수료, 인터넷 증권 중개, 홈트레이딩 기타 인터넷 금융 및 보험업 등
콘텐츠 제공 서비스	인터넷을 통한 교육서비스를 제공하는 사업자	콘텐츠 이용매출, 수수료, 광고매출, 회원수익매출, 부가수익 등
	인터넷을 통한 실시간 음악 감상 서비스를 제공하는 사업자	
	인터넷을 통한 기타 콘텐츠제공 서비스를 제공하는 사업자	
유선방송 서비스 (Cable-SO)	종합유선 방송서비스와 종합유선전송 서비스를 제공하는 사업자	방송중계서비스 매출을 제외한 초고속인터넷서비스 매출액 등
기타	인터넷을 통한 기타 정보통신서비스를 제공하는 사업자	

※ 정보통신서비스 온라인 판매, 광고, 콘텐츠 이용 등으로 발생한 매출액과 부가수익, 수수료, 세금 등을 포함한 총 합계액

※ 정보통신서비스 제공을 통해 직·간접으로 발생하는 연간 국내·외 매출액

[표2-7] 쇼핑몰 유형 별 매출 구분 (예시)

판매 유형	정보통신서비스 부문에 해당되는 매출액
자체쇼핑몰 운영	자체쇼핑몰을 통한 제품 판매액
중개쇼핑몰 이용	해당사항 없음
중개쇼핑몰 운영	판매 중개수수료 + 입점료(해당하는 경우)
자체쇼핑몰 운영 + 중개쇼핑몰 이용	자체쇼핑몰을 통한 제품판매액
중개쇼핑몰 운영 + 자체쇼핑몰 운영	판매 중개수수료 + 입점료(해당하는 경우) + 자체 쇼핑몰을 통한 제품 판매액
포인트 쇼핑몰	가맹점 수수료 + 고객 수수료 + 판매수수료 + 기프티콘

(이용자 수 : 전년도 말 기준 3개월 일일평균 이용자 수 100만명 이상)

- 일일평균 이용자 수는 일정 기간 동안의 주요정보통신서비스제공자의 홈페이지 방문자 수 등을 일평균으로 환산한 이용자 수를 말하며, 여러 가지 정보통신서비스를 제공할 경우에는 해당 서비스의 이용자 수를 모두 합하여 계산한다.

※ PC, 스마트폰 등이 네트워크 운영을 위해 이용하는 DNS query, 기지국 등록 등의 접속은 제외

※ 자체적 또는 공식적으로 이용자 수 확인이 어려운 경우, 민간 통계기관 등의 데이터 활용

※ 가능한 웹서버는 로그 분석도구 등을 이용하여 일일평균 이용자 수를 계산

[표2-8] 주요 정보통신서비스 이용자 수 구분 (예시)

구분	대상 이용자 수 기준	주요 서비스 예시
홈페이지 등	주요정보통신서비스제공자의 日평균 홈페이지 방문자수(PV)가 100만명 이상인 경우	인터넷 쇼핑몰, 포털 등

※ PV(Page View) : 홈페이지에 들어온 접속자가 둘러 본 페이지 수

2.1.3 인증 의무대상자 유의사항

o 인증 의무대상자 기준① 및 기준②에 해당하는 기업은 매출액 및 이용자 수에 관계없이 인증 의무대상자에 해당된다.

- 집적정보통신시설 사업자(IDC) 중 재판매 사업자(VIDC)는 기준③에 따라 매출액 및 이용자 수 기준에 따르게 된다.

[표2-9] 정보통신서비스 제공자 별 인증 의무대상자 구분

정보통신서비스 제공자	인증 의무대상자 여부
정보통신망서비스를 제공하는 자 (ISP) ※ 서비스 제공 지역이 '서울특별시 및 모든 광역시'인 사업자	- 매출액 및 방문자 수에 관계없이 인증 의무대상자에 해당
집적정보통신시설 사업자 (IDC)	
집적정보통신시설의 일부를 임대하여 서비스를 재판매하는 사업자 (VIDC)	- 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자 또는 - 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 100만명 이상인 자
연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자	

o 인증 의무대상자 기준 중에서 정보통신망법 제47조제2항의 어느 한가지 이상의 기준에 해당할 경우, 인증 의무대상자가 된다.

- 다만, 선정된 기준에 해당하는 서비스 범위를 합치거나 분할하여 인증의 범위를 정할 수 있다.

- 인증 범위를 분할할 경우, 각각의 인증범위에 대하여 별도의 인증계약으로 수수료 등 추가 비용이 발생할 수 있다.

o 인증 의무대상자는 스스로 법에서 정한 인증 의무대상자 기준에 적합한지 여부를 확인하여 인증을 받아야 하며, 만일 실태조사 등에서 인증 의무대상자이나 인증을 취득하지 안했을 경우에는 과태료 부과 대상이 될 수 있다.

o 구축 및 운영에 필요한 소요기간을 확인하여 인증심사에 차질이 없도록 준비해야 한다.

- 준비부터 인증까지는 약 6개월 이상이 소요되고, 인증 신청을 위해서는 최소 2개월 이상의 운영 기간이 필요하다.

[표2-10] 인증 절차 및 단계별 소요기간

인증 절차 내용	① 준비			② 심사					③ 인증	
	ISMS 구축	ISMS 운영	인증 신청	심사 준비	인증 심사	보완 조치	조치 확인	심사 결과보고서 작성	인증위원회 심의 준비	인증위원회 심의 및 인증서 교부
소요 시간	1~3개월	2개월 (최소)	5일	30일	5일	30일	5일	5일	30일	2일

o 정보보호 관리체계 인증 제도는 조직 내에서 발생할 수 있는 해킹 등 침해사고로부터 위험을 감소시키기 위한 최소한의 기본적인 정보보호 활동(프로그램)이다.

- 인증 취득이 침해사고를 완벽하게 방지하는 것은 아니며, 침해사고를 최소화하기 위해서는 대상자가 지속적으로 인증기준을 준수하여 일정 수준을 유지하고 향상시키는 노력이 가장 중요하다.

☞ 인증취득과 건강검진 비교

- 건강검진을 받고 예방접종을 맞아도 병에 걸릴 수 있음은 정보보호 관리체계를 수립하고 인증을 취득 이후에도 침해사고 발생 가능성은 충분히 존재한다는 의미로 인증취득이 침해사고의 모든 것을 해결해 주는 종합검사로 받아들여져서는 안 되며
- 건강검진 및 예방접종을 한 사람은 이를 실시하지 않은 사람보다 자신의 상태를 확인할 수 있으며 병에 대한 저항력이 높아 병에 걸릴 확률이 낮다는 의미라 할 수 있음
- 또한, 병에 걸리더라도 최악의 상황을 피할 수 있는 확률을 높일 수 있고, 타 병원과 결합되어 병이 확대될 수 있는 위험을 낮출 수 있음

o 정보보호 관리체계 인증 제도의 목적은 기업 스스로가 기업의 정보자산을 보호하기 위하여 기술적·관리적·물리적 보호조치를 포함하는 체계적이고 종합적인 정보보호 관리체계를 구축하는 것이다.

- 따라서, 단순히 인증 취득이 목적이 아니므로 위험 분석을 통해 보호조치를 취하는 등 정보보호 개선 활동을 지속적으로 추진해야 실효성 있는 보안관리 활동이 될 것이다.

2.2 인증 범위

< 인증 범위 개념 >

o 신청기관의 정보통신서비스를 포함하여 인증 범위를 설정해야 한다.

- 인증 범위는 신청기관이 제공하는 정보통신서비스를 기준으로, 해당 서비스에 포함되거나 관련 있는 자산(시스템, 설비, 시설 등), 조직 등을 모두 포함한다.

※ 해당 서비스와 관련이 없더라도, 그 서비스의 핵심정보자산에 직 · 간접적으로 접근한다면 포함

o 신청기관이 클라우드 서비스를 이용하여 정보통신서비스를 제공할 경우 클라우드 서비스 제공자의 설비, 시설, 서비스 제공을 위한 인프라 자산은 인증범위에서 제외된다.

o 클라우드 서비스 이용자가 클라우드 서비스를 활용하여 정보통신서비스를 제공하는 경우에 그 정보통신서비스는 인증범위에 포함된다.

[표2-11] 클라우드 서비스 관련 용어 정의

용어	정의
클라우드 서비스 제공자	인터넷 등 정보통신망을 통하여 시스템 자원, 소프트웨어, 응용프로그램, 정보 인프라 등을 가상화 또는 분산처리 하여 제공하는 자
클라우드 서비스 이용자	클라우드 서비스 제공자가 제공하는 클라우드 서비스를 이용하는 자

- 다만 클라우드 서비스 이용자는 클라우드 서비스의 신뢰성 및 안전성에 대한 관련 인증을 받은 클라우스 서비스 제공자의 서비스 사용을 권고한다.

< 인증 범위 설정 >

o 인증 범위를 설정하기 위해서는 신청기관이 제공하고 있는 정보통신서비스를 분류하고, 해당 서비스를 위한 자산 및 조직을 모두 식별해야 한다.

- 인증 범위 내의 모든 자산 및 조직에 대해「정보보호 관리체계 인증 등에 관한 고시」제18조에 따른 [별표 6] '정보보호 관리체계 인증기준'을 준수하여 보호조치를 취해야 한다.

(정보통신망서비스 제공자)

- 해당 서비스 : 전국망(서울특별시 및 모든 광역시)을 통한 인터넷 서비스

- 설비 : IP기반의 인터넷 연결을 위한 정보통신설비 및 관련 서비스를 제공하기 위한 정보통신설비

[표2-12] 정보통신망서비스 제공자 서비스 분류체계 (예시)

구분	서비스	기능
정보통신망서비스 제공자	기간통신서비스	인터넷 접속 서비스 (초고속망 서비스)
		인터넷 전화 서비스(VOIP)
		이동통신서비스 (셀룰라, PCS, 3G, 4G)

(집적정보통신시설 사업자)

- 해당 서비스 : 정보통신서비스를 제공하는 고객의 위탁을 받아 컴퓨터 장치 등 정보시스템을 구성하는 장비를 일정한 공간에 집중하여 시설을 운영·관리하는 서비스(공간임대서비스, 서버호스팅, 네트워크 서비스 등)

- 설비 : 집적정보통신시설의 관리·운영 용도로 설치된 컴퓨터 장치 및 네트워크 장비 등의 정보통신설비

[표2-13] 집적정보통신시설 사업자 서비스 분류체계 (예시)

구분	서비스	기능
집적정보통신시설 사업자 및 재판매 사업자	부가통신 서비스	서버 호스팅
		스토리지 호스팅
		코로케이션(Co-location)
		네트워크 제공 서비스 (회선 임대 포함)
		보안관리 서비스 (제공 시)
		도메인관리 서비스 (제공 시)

(연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자)

- 해당 서비스 : 정보통신망서비스 제공자 및 집적정보통신시설 사업자의 서비스를 제외한 쇼핑몰 등의 정보통신서비스

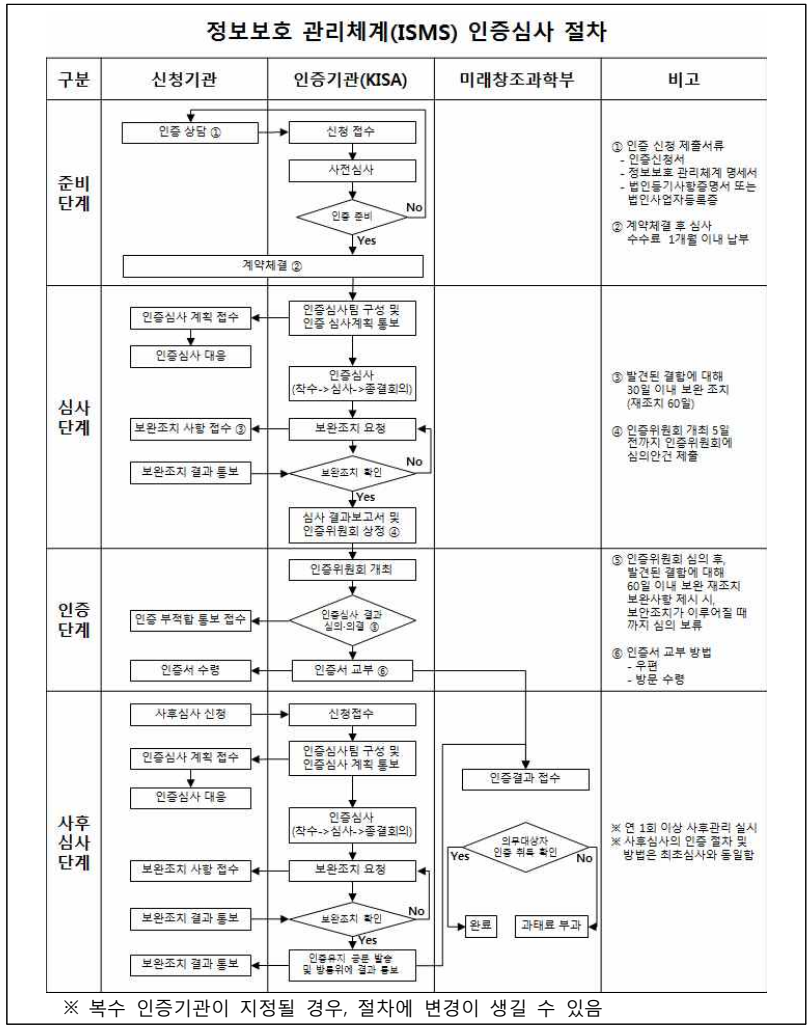
- 설비 : 쇼핑몰, 포털 등의 전자상거래업을 영위하기 위해서 필요한 정보통신설비

[표2-14] 정보통신서비스제공자 서비스 분류체계 (예시)

구분	서비스	기능	
쇼핑몰 등	부가통신 서비스	신용카드 검색(CCIS) 서비스	
		컴퓨터 예약(CRS) 서비스	
		전자문서교환(EDI) 서비스	
		전자지불서비스, 인터넷금융서비스	
		전화정보 서비스(ARS)	
		인터넷 정보제공 (유선, 무선)	인터넷 포털 서비스
			인터넷 전자상거래(수수료)
			인터넷 방송
			인터넷 게임
		콘텐츠 제공 서비스	
유선방송	방송서비스	유선방송서비스	

2.3 인증 절차

o 인증 절차는 (그림2-1)과 같으며, 준비단계, 심사단계, 인증단계, 사후심사 단계로 나누어진다.



(그림2-1) 인증 절차도

2.3.1 준비단계

< 인증 신청 >

o 인증 의무대상자는 인증을 신청하기 전에 인증기준에 따른 정보보호 관리체계를 구축하여 최소 2개월 이상 운영하여야 하며, 인증 신청 시 운영기간에 대한 증적자료를 포함하는 인증신청서류를 인증기관에 제출하여야 한다.

※ 정보보호 관리체계 구축 시, 모든 자산에 대해 취약점 점검을 실시하고 모든 자산별로 보호조치를 취하고 적용해야 한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제15조(신청기관의 사전 준비사항)
신청기관은 정보보호 관리체계 인증을 신청하기 전에 인증기준에 따른 정보보호 관리체계를 구축하여 최소 2개월 이상 운영하여야 한다.

- 심사팀이 현장심사 방문 시, 정보보호 관리체계를 2개월 이상 운영한 증적자료를 확인할 수 없을 경우에는 심사를 중단할 수 있다.

- 이 경우 신청기관은 심사 우선순위에서 최하위로 배정되고 재심사의 대상이 될 수 있다.

- 심사원의 인건비 등에 대한 추가비용을 부담하게 될 수 있다.

o 인증 의무대상자의 인증 신청 연말 쏠림현상을 방지하기 위해 신청기관의 사업자 등록일이 속한 분기가 끝나기 1개월 전에 인증 신청을 한 경우, 인증심사를 우선적으로 처리하도록 한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제16조(인증의 신청 등)
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.

- 분기 내 신청이 되지 않을 경우, 심사 우선순위에서 하위로 밀려날 수 있으며 이로 인해 인증을 취득하지 못할 경우 과태료 부과대상이 될 수 있음을 주의해야 한다.

o 신청기관은 인증신청서 등의 제출서류와 함께 공문(전자문서 포함)을 통하여 인증 신청을 해야 한다.

※ [붙임 1] : 정보보호 관리체계 인증신청서
※ [붙임 2] : 정보보호 관리체계 명세서

o 인증기관은 신청서류를 접수하고 접수증을 교부한 후 신청 서류의 기재사항을 검토하여 미비점이 있을 경우 보완을 요청할 수 있다.

- 신청기관은 보완 요청을 받은 날로부터 10일 이내에 이를 보완하고 신청서류를 재구비하여 신청하여야 한다.

o 인증신청서류는 정보보호 관리체계 인증신청서 및 정보보호 관리체계 명세서, 법인등기사항증명서(또는 법인사업자등록증)이다.

관련근거

정보통신망 이용 촉진 및 정보보호 등에 관한 법률 시행령

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 또는 미래창조과학부장관이 지정한 기관(이하 "정보보호 관리체계 인증기관"이라 한다)에 제출하여야 한다.
1. 정보보호 관리체계의 범위
2. 정보보호 관리체계의 범위에 포함되어 있는 주요 정보통신설비의 목록과 시스템 구성도
3. 정보보호 관리체계를 구축·운영하는 방법과 절차
4. 정보보호 관리체계와 관련된 주요 문서의 목록
5. 정보보호 관리체계와 관련된 국내외 품질경영체제의 인증을 취득한 경우에는 그 명세

< 계약 체결 >

o 인증기관은 인증신청서류 접수 여부 및 신청기관의 인증심사 준비현황을 파악한 후 신청기관과 인증심사 계약을 체결한다.

o 신청기관은 인증기관과 협의한 후 심사기간, 심사인원, 인증 수수료, 인증의 범위 등을 포함하는 인증심사계약을 체결하고, 인증심사 계약체결 후 인증심사 수수료를 1개월 이내에 납부해야 한다.

- 심사는 입금이 완료된 후에 진행된다.

o 수수료 납부 방법은 인증 심사 계약 시 신청기관과 협의하여 일괄 또는 분할 납부 방법으로 조정할 수 있다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

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.

o 인증 수수료는 직접인건비, 직접경비, 제경비, 기술료를 고려하여 산정한다.
※ 산정방식 : 직접인건비 + 직접경비(교통·출장비 등) + 제경비 + 기술료

- 직접인건비 : 인증심사에 투입되는 인증심사원에 대한 인건비로 산정한다.
※ 인건비는 SW사업 대가산정 가이드의 정보보안 컨설팅비를 준용

- 직접경비 : 인증심사업무의 수행에 따라 발생하는 교통비, 숙박비 및 식대 등 인증심사업무에 소요되는 직접적인 경비를 산정한다.

- 제경비 : 최대 (직접인건비×120%) 로 산정한다.

- 기술료 : 최대 {(직접인건비+제경비)×40%} 로 산정한다.

[표2-15] 인증 수수료 산정요소

산정요소	내용
직접인건비	선임심사원·심사원·심사원보 3~5명(기술자등급별단가 × 심사일수)
직접경비	여비 등 실제 소요비용 반영
제경비	직접인건비의 최대 120%
기술료	(직접인건비 + 제경비)의 최대 40%

o 중소기업법 제2조에 따른 중소기업이 인증을 신청하는 경우, 수수료 감면 혜택을 부여한다.
※ 수수료의 할인율에 대하여는 향후 공지 예정

관련근거

정보보호 관리체계 인증 등에 관한 고시

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.

2.3.2 심사단계

< 인증심사팀 구성 및 인증 심사계획 통보 >

o 인증기관에서 인증심사를 위한 인증심사팀 구성 시 인증심사 품질 제고 및 책임성 강화를 위해 심사팀장은 인증기관의 소속직원 중 심사원 이상으로 선정한다.

o 인증심사의 공정성, 객관성 확보를 위해 인증심사팀 구성 시 인증대상 기관의 컨설팅 참여직원은 배제한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제19조(인증심사팀 구성)
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.

[표2-16] 심사계획 통보 내용

구분	내용
심사 일정	- 착수회의 - 서면심사 - 현장심사 - 주요 시스템(업무지원 시스템, 정보보호시스템 등) 시연 - 현장실사 및 현장확인(담당자 인터뷰 및 현장실사) - 결과 확인 및 종결회의
심사팀 구성	- 심사팀장 - 심사팀 인원
심사 준비사항	- 심사 공간 및 비품 - 인증 심사 관련 자료 및 이행 증적자료심사 지원 - 담당자 지정

< 인증심사 대응 >

o 신청기관은 원활한 인증심사를 위하여 통보받은 계획에 따라 [표2-16]에 기재된 내용을 확인하여 심사 준비를 해야 한다.

- 신청기관은 인증 심사를 수행하기 위하여 필요한 장소와 세부 문서, 운영기록 등의 자료를 제공하고 담당자 면담을 주선하는 등 필요한 협조를 제공해야 한다.

[표2-17] 심사 준비사항

구분	내용
심사 공간	- 회의실 - 빔프로젝트
비품	- 전화 - 네트워크 회선 - 화이트 보드
인증 심사 관련 자료 및 이행 증적자료	- 상위 정책서, 직무기술서, 정보보호계획서, 정보보호 관리체계 범위정의서, 담당자 연락처 (사본 각 O부) - 정보보호대책명세서 (원본 O부, 사본 O부) ※ 운영현황/관련문서/증적자료는 상세하게 작성 - 각종 지침/절차/매뉴얼 (원본 O부, 사본 O부) - 위험분석 보고서, 내부 감사 결과보고서, 교육계획서 등 각종 보고서/계획서 (원본 O부, 사본 O부) - 각종 점검 및 관리대장 등 이행증적자료 (원본 O부)
심사 지원 담당자 지정	- 조직도 및 연락처 등 - 관련문서 열람 및 관계자 면담 등에 대한 협조

< 인증심사 >

o 인증심사는 관리체계의 인증기준인 관리과정과 관리적, 기술적, 물리적 보호조치로 구성된 정보보호대책 통제항목이 적절히 이행되고 있는지 확인한다.

o 인증심사 수행은 서면심사와 현장심사를 병행하여 실시한다.

- 서면심사에서는 신청기관이 정보보호 관리체계 관련 문서인 정책과 지침, 절차 등 내부규정을 갖추고 있는지, 해당 내부규정이 인증기준에서 제시하고 있는 요구사항(통제항목)을 충족하고 있는지 심사한다.

※ 각종 문서 및 이행 증적자료 검토, 보호대책 적용 여부 확인 등의 방법으로 관리적 요소를 심사

- 현장심사에서는 문서에서 명시한 통제사항들의 실행 여부 및 서면심사에서 발견된 문제점의 원인을 확인하고, 현장실사를 통해 기술적 대책, 물리적 대책이 이행되고 있는지 확인한다.

※ 이행에 따른 증적자료 또는 전자적 기록 점검 등

관련근거

정보보호 관리체계 인증 등에 관한 고시

제20조(인증심사 방법 및 보완조치)
① 인증심사는 신청기관을 방문하여 서면심사와 현장심사를 병행한다.
② 서면심사는 인증기준에 적합한지에 대하여 정보보호 관리체계 구축·운영 관련 정보보호정책, 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.

o 인증심사 후 심사원들은 서면심사 및 현장심사를 통하여 도출된 문제점에 대해 결함보고서를 작성하고, 최종적으로 신청기관의 담당자들과의 '결과확인 회의'를 통하여 결함 내용을 확인한다.

o 신청기관이 인증심사를 위한 심사원의 자료 요구, 인터뷰 등을 거부하여 더 이상 인증심사 진행이 어려울 경우, 인증기관은 심사를 중단하고 신청기관을 인증심사 최하위 순위로 배정하여 재심사 여부를 결정한다.

o 인증기관은 인증심사에서 알게 된 비밀을 타인에게 누설하거나 업무 외의 목적으로 사용하지 않는다.

관련근거

정보통신망 이용 촉진 및 정보보호 등에 관한 법률

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.
2. 제47조에 따른 정보보호 관리체계 인증 업무

※ 법 제66조를 위반하여 직무상 알게 된 비밀을 타인에게 누설하거나 직무 외의 목적으로 사용한 자 (3년 이하 징역 또는 3천만원 이하 벌금)

< 보완조치 요청 >

o 인증기관은 정보보호 관리체계 결함보고서를 신청기관에 전달하고, 결함보고서에 기술한 결함에 대해 신청기관에게 보완조치 요청서를 작성하여 통보한다.

- 신청기관은 보완조치 요청을 받은 날로부터 30일 이내에 보완조치를 수행하고 정보보호 관리체계 보완조치 내역서를 작성하여 인증기관에 제출해야 한다.

- 인증기관은 신청기관이 제출한 보완조치 결과에 대하여 현장 확인이 필요하다고 판단될 경우 현장을 방문하여 결과를 확인할 수 있다.

- 인증기관이나 인증위원회에서 보완조치결과가 미흡하다고 판단할 경우, 재조치를 요구할 수 있으며 추가적으로 60일 이내에서 보완조치 기간을 연장할 수 있다.

- 신청기관이 추가적으로 보완조치에 대한 요청을 받은 날로부터 60일 이내에 보완조치에 대한 결과물을 제출하지 못하는 경우, 보완이 이루어지지 않은 것으로 판단한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제20조(인증심사 방법 및 보완조치)
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.

< 심사 결과보고서 작성 및 인증위원회 상정 >

o 인증심사원은 서면심사 및 현장심사를 통하여 발견한 결함에 대한 보완조치의 결과 확인이 이루어지면, 심사 결과보고서를 작성한다.

o 인증심사팀이 수행한 심사결과에 대한 객관성과 공정성 확보 및 일정수준 이상의 품질 확보를 위하여 한국인터넷진흥원의 장이 구성·운영하는 인증위원회에 심사 결과보고서를 상정한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

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.

2.3.3 인증단계

< 인증심사 결과 심의·의결 >

o 위원장은 인증위원회의 업무를 통할하며 위원회를 대표하여 정보보호 관리체계 인증기관의 장에게 인증심사원이 실시한 인증심사 결과가 인증기준에 적합한지 여부를 심의하고 그 결과를 제출한다.

- 정보보호 관리체계 인증위원회를 운영함으로써 심사와 심의·의결을 분리하여 부실 논란을 없애고 실효성을 확보한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

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 정보보호 전문가, 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.

o 인증위원회 심의결과 보완조치가 발생하는 경우 고시 제20조제5항에 따라 30일 이내에 조치를 취하고 인증기관에 통보하여야 한다.

< 인증서 발급 >

o 인증위원회는 인증기관에서 수행한 인증심사결과(관리체계 인증 기준 적합 여부 등)를 심의·의결하고, 그 결과에 따라 인증기관은 인증서를 발급한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

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.

2.3.4 사후심사 단계

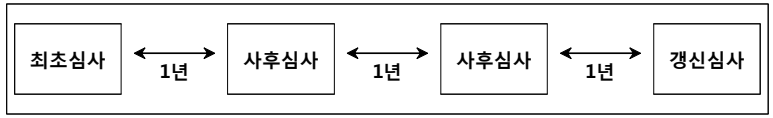
< 사후심사 >

o 정보보호 관리체계 인증을 받게 되면 그 인증은 3년간 유효하고 관리체계의 지속적인 유지운영을 위해 1년에 한번 이상 관리체계를 점검하는 사후심사를 받아야 한다.

관련근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제47조(정보보호 관리체계의 인증)
⑥ 한국인터넷진흥원 및 정보보호 관리체계 인증기관은 정보보호 관리체계의 실효성 제고를 위하여 연 1회 이상 사후관리를 실시하고 그 결과를 미래창조과학부장관에게 통보하여야 한다.



(그림2-2) 인증 심사 주기

o 인증기관은 인증취득 기관이 중대한 침해사고가 발생하였을 경우 사후관리를 위하여 사후심사를 할 수 있으며 인증취소 요건이 발생할 경우 인증을 취소할 수 있다.

2.3.5 인증취소

o 한국인터넷진흥원은 신청기관의 인증을 취소할 수 있다.

관련근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제47조(정보보호 관리체계의 인증)
⑧ 미래창조과학부장관은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 경우에는 인증을 취소할 수 있다.
1. 거짓이나 그 밖의 부정한 방법으로 정보보호 관리체계 인증을 받은 경우
2. 제3항에 따른 인증기준에 미달하게 된 경우
3. 제6항에 따른 사후관리를 거부 또는 방해한 경우

- 인증취소 사유에 대한 확인을 위하여 한국인터넷진흥원은 인증 취득 기업에 대해 수시점검을 수행할 수 있다.

2.4 인증 기준

o 정보보호 관리체계 인증 기준은 개정된 정보통신망법('13.2월) 시행에 따라 기존의 실효성이 낮은 점검항목의 통합 및 최신 보안관리 기준을 반영하여 변경되었다.

- 정보보호 관리체계 (구)인증 기준은 137개 통제항목 및 446개 세부점검항목으로, (신)인증 기준은 104개 통제항목 및 253개 세부점검항목으로 구성되어 있다.

[표2-18] 정보보호 관리체계 인증 기준 변경

통제영역	변경 전 항목 수	변경 후 항목 수	증감
관리과정	14	12	-2
문서화	3	0	-3
정보보호대책	120	92	-28
총계	**137**	**104**	**-33**

[표2-19] 정보보호 관리체계 인증 기준 주요 변경 내용

구분	주요 변경 내용
신규 항목 (14개)	- 경영진의 책임(예산 및 인력 지원, 의사결정 참여 등) 강화 - 정보보호최고책임자(CISO) 의무 지정 등 조직 구성 강화 - 최신기술 및 보안사고 반영
통합 또는 변경 항목 (128개 → 90개)	- 업무연속성관리, 물리적 보안, 전자거래보안, 검토, 모니터링 및 감사 영역 중심으로 중복 또는 유사항목 통합
삭제 항목 (9개)	- 적격심사, 물리적 위치 및 구조 조건, 입력 데이터/내부처리/출력 데이터 검증, 전자우편 등의 항목 실효성 부족(결함률 0)으로 삭제

o 변경된 인증 기준의 적용 시점은 기업의 혼란 발생을 최소화하기 위하여 시기 별 단계적으로 적용해 나간다.

[표2-20] 기준 변경 시점에 따른 인증 기준 적용 시점

최초·갱신	신청시점	2013.2.17 이전	2013.2.17 ~ 12.31	2014년 이후
사후	심사시점			
적용기준		변경 前 기준 적용	변경 前 기준 또는 변경 기준 선택 적용	변경 기준 적용

o (구)인증 기준은 정보보호 관리과정(5단계 14개 통제항목)·문서화(3개 분야, 3개 통제항목)·정보보호대책(15개 분야 120개 통제항목)으로, (신)인증 기준은 정보보호 관리과정(5단계 12개 통제항목)·정보보호대책(13개 분야 92개 통제항목)으로 구성되어 있다.

- 인증 취득을 계획하고 있는 인증대상자는 각각의 통제항목에 해당하는 세부점검항목을 확인하여 정보보호 관리체계를 구축하여야 한다.

※ [붙임 7] : 인증 기준 세부점검항목

[표2-21] 정보보호 관리체계 인증 기준

분야		(구)인증 기준		(신)인증 기준	
		통제항목 수	세부점검항목	통제항목 수	세부점검항목
정보보호 관리과정	정보보호 정책 수립	2	7	-	-
	관리체계 범위 설정	2	4	-	-
	정보보호정책수립 및 범위설정	-	-	2	4
	경영진 책임 및 조직구성	-	-	2	4
	위험 관리	5	19	3	11
	구현	2	7	-	-
	정보보호대책 구현	-	-	2	3
	사후 관리	3	10	3	6
	소계	**14**	**47**	**12**	**28**
문서화	문서 요건	1	1	-	-
	문서의 통제	1	1	-	-
	운영기록의 통제	1	1	-	-
	소계	**3**	**3**	**-**	**-**
정보보호 대책	정보보호 정책	5	10	6	13
	정보보호 조직	4	11	4	7
	외부자 보안	4	8	3	4
	정보자산 분류	4	7	3	7
	정보보호 교육 및 훈련	4	14	-	-
	정보보호교육	-	-	4	10
	인적 보안	5	18	5	11
	물리적 보안	12	36	9	21
	시스템 개발 보안	13	53	10	22
	암호 통제	3	6	2	8
	접근 통제	14	38	14	46
	운영 관리	22	99	-	-
	운영 보안	-	-	22	56
	전자거래 보안	5	21	-	-
	보안사고 관리	7	20	-	-
	침해사고 관리	-	-	7	14
	검토·모니터링·감사	11	37	-	-
	업무 연속성 관리	7	18	-	-
	IT재해복구	-	-	3	6
	소계	**120**	**396**	**92**	**225**
총계		**137**	**446**	**104**	**253**

< 정보보호 관리과정 인증 기준 >

o 정보보호 관리과정은 정보보호 관리체계 인증 심사 시 요구되는 필수 항목으로써 조직 내·외부 위협 요소의 변화 또는 새로운 취약성 발견 등에 대응하기 위하여 지속적으로 유지 관리되는 순환 주기의 형태를 가진다.

(그림2-3) 정보보호 관리과정

[표2-22] 정보보호 관리과정의 구체적인 요구사항

관리과정	요구사항	관련 문서
정보보호정책 수립 및 범위설정	- 조직 전반에 걸친 상위 수준의 정보보호정책 수립 - 정보보호 관리체계 범위 설정	- 정보보호정책서 - 정보보호 관리체계 범위서 - 정보자산 목록 (정보통신설비 목록) - 네트워크 및 시스템 구성도
경영진 책임 및 조직구성	- 정보보호를 수행하기 위한 조직 내 각 부문의 책임 설정 - 경영진 참여 가능하도록 보고 및 의사결정체계 구축	- 정보보호조직도
위험관리	- 위험관리 방법 및 계획 수립 - 위험 식별 및 위험도 평가 - 정보보호대책 선정 - 구현 계획 수립	- 위험관리지침서 - (00년)위험관리 계획서 - 위험 분석·평가 보고서
정보보호대책 구현	- 정보보호 대책 구현 및 이행 확인 - 내부 공유 및 교육	- 정보보호대책 명세서 - 정보보호계획서 - 정보보호계획 이행결과 보고서
사후관리	- 법적 요구사항 준수 검토 - 정보보호 관리체계 운영 현황 관리 - 정기적인 내부감사를 통해 정책 준수 확인	- 정보보호 관리체계 내부감사보고서 - 정보보호 관리체계 운영현황표

< 정보보호대책 인증 기준 >

o 정보보호대책은 정보보호 관리체계 인증 심사 시 요구되는 항목으로써 총 13개 분야 92개 통제항목으로 구성되어 있다.

- 미선정 통제항목이 있을 경우, 사유를 명시하고 정보보호책임자 등 경영진의 승인을 득하여 부주의 또는 의도적으로 통제항목 선정이 배제되지 않도록 하여야 한다.

[표2-23] 정보보호대책의 통제분야 및 통제항목

정보보호대책	통제분야	통제항목
정보보호정책	· 정책의 승인 및 공표	- 정책의 승인
		- 정책의 공표
	· 정책의 체계	- 상위 정책과의 연계성
		- 정책시행 문서수립
	· 정책의 유지관리	- 정책의 검토
		- 정책문서 관리
정보보호 조직	· 조직의 체계	- 정보보호 최고책임자 지정
		- 실무조직 구성
		- 정보보호위원회
	· 역할 및 책임	- 역할 및 책임
외부자 보안	· 보안요구사항 정의	- 외부자 계약 시 보안요구사항
	· 외부자 보안 이행	- 외부자 보안 이행 관리
		- 외부자 계약 만료 시 보안
정보자산 분류	· 정보자산 식별 및 책임	- 정보자산 식별
		- 정보자산별 책임할당
	· 정보자산의 분류 및 취급	- 보안등급과 취급
정보보호교육	· 교육 프로그램 수립	- 교육 계획
		- 교육 대상
		- 교육 내용 및 방법
	· 교육 시행 및 평가	- 교육 시행 및 평가
인적 보안	· 정보보호 책임	- 주요 직무자 지정 및 감독
		- 직무 분리
		- 비밀유지서약서
	· 인사규정	- 퇴직 및 직무변경 관리
		- 상벌규정
물리적 보안	· 물리적 보호구역	- 보호구역 지정
		- 보호설비
		- 보호구역 내 작업
		- 출입통제
		- 모바일기기 반출입
	· 시스템 보호	- 케이블 보안
		- 시스템 배치 및 관리
	· 사무실 보안	- 개인업무 환경 보안
		- 공용업무 환경 보안

정보보호대책	통제분야	통제항목
시스템개발보안	· 분석 및 설계 보안관리	- 보안 요구사항 정의
		- 인증 및 암호화 기능
		- 보안로그 기능
		- 접근권한 기능
	· 구현 및 이관 보안	- 구현 및 시험
		- 개발과 운영 환경 분리
		- 운영환경 이관
		- 시험데이터보안
		- 소스 프로그램 보안
	· 외주개발 보안	- 외주개발보안
암호통제	· 암호정책	- 암호 정책 수립
	· 암호키 관리	- 암호키 생성 및 이용
접근통제	· 접근통제 정책	- 접근통제 정책 수립
	· 접근권한 관리	- 사용자 등로곡 및 권한부여
		- 관리자 및 특수 권한 관리
		- 접근권한 검토
	· 사용자 인증 및 식별	- 사용자 인증
		- 사용자 식별
		- 사용자 패스워드 관리
		- 이용자 패스워드 관리
	· 접근통제 영역	- 네트워크 접근
		- 서버 접근
		- 응용 프로그램 접근
		- 데이터 베이스 접근
		- 모바일 기기 접근
		- 인터넷 접속
운영보안	· 운영 절차 및 변경 관리	- 운영절차 수립
		- 변경관리
	· 시스템 및 서비스 운영 보안	- 정보시스템 인수
		- 보안시스템 운영
		- 성능 및 용량관리
		- 장애관리
		- 원격운영관리
		- 스마트워크 보안
		- 무선네트워크 보안
		- 공개서버 보안
		- 백업관리
		- 취약점 점검
	· 전자거래 및 정보 전송 보안	- 전자거래 보안
		- 정보전송 정책 수립 및 협약 체결
	· 매체 보안	- 정보시스템 저장매체 관리
		- 휴대용 저장매체 관리
	· 악성코드 관리	- 악성코드 통제
		- 패치관리
	· 로그관리 및 모니터링	- 시각 동기화
		- 로그기록 및 보존
		- 접근 및 사용 모니터링
		- 침해시도 모니터링

정보보호대책	통제분야	통제항목
침해사고 관리	· 절차 및 체계	- 침해사고 대응절차 수립
		- 침해사고 대응체계 구축
	· 대응 및 복구	- 침해사고 훈련
		- 침해사고 보고
		- 침해사고 처리 및 복구
	· 사후관리	- 침해사고 분석 및 공유
		- 재발방지
IT재해복구	· 체계 구축	- IT 재해복구 체계 구축
	· 대책 구현	- 영향분석에 따른 복구대책 수립
		- 시험 및 유지관리

2.5 기타 고려사항

2.5.1 인증 쏠림 현상 방지

o 연말 인증신청 쏠림 현상을 방지하기 위하여 인증 신청기관이 사업자 등록일이 속한 분기가 끝나기 1개월 전에 인증 신청을 한 경우, 인증심사를 우선적으로 처리하도록 한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제16조(인증의 신청 등)
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.

- 연말에 인증신청이 집중되어 인증을 받지 못 할 수 있으며, 이로 인해 과태료가 부과될 수 있으므로 반드시 법인사업자 등록일이 속한 분기가 끝나기 1개월 전에 인증 신청을 해야 한다.

- 1분기 신청업체는 3월안에 인증을 신청하고, 4분기 신청업체는 보완조치 기간(60일)을 고려하여 매년 10월 초까지 신청을 하여야 하며, 보완조치가 이루어지지 않으면 인증을 취득한 것으로 볼 수 없다.

2.5.2 인증 소요기간 및 준비 사항

o 인증 의무대상자들은 단계별 소요기간을 확인하여 인증 취득을 준비해야 한다.

- 인증 소요기간은 내부 준비부터 인증까지 약 6개월 이상이 소요되므로, 연내 취득을 위해 일정을 역산하여 조기에 인증 준비를 하는 것이 필요하다.

※ 인증 신청을 위해서는 정보보호 관리체계 구축 후 최소 2개월 이상 운영 필요
※ 정보통신망법 개정 시 준비기간을 고려하여 1년간의 유예기간을 줌

관련근거

정보보호 관리체계 인증 등에 관한 고시

제15조(신청기관의 사전 준비사항)
신청기관은 정보보호 관리체계 인증을 신청하기 전에 인증기준에 따른 정보보호 관리체계를 구축하여 최소 2개월 이상 운영하여야 한다.

제3장 정보보호 관리체계(ISMS) 인증 주요 추진체계

3.1 인증위원회

o 한국인터넷진흥원의 장은 인증심사팀이 수행한 심사결과에 대한 객관성과 공정성, 일정수준 이상의 품질을 확보하기 위하여 인증위원회를 구성·운영한다.

- 인증위원회 운영함으로써 심사와 심의·의결을 분리하고 공정성을 확보하며, 부실 인증서를 남발하지 않도록 한다.

- 인증위원회의 위원은 정보보호전문가, 정보시스템감리사, 기술사 등 정보보호분야에 학식과 경험이 있는 전문가로 인증기관의 장이 위촉한 5인 이상 10인 이내의 위원으로 구성한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제21조(인증위원회의 구성)
② 인증위원회는 5인 이상 10인 이내의 위원으로 구성하되, 위원은 정보보호 전문가, 정보시스템감리사, 기술사, 대학교수 등 정보보호분야에 학식과 경험이 있는 자 중에서 인터넷진흥원 또는 인증기관의 장이 위촉하며, 위원장은 위원 중에서 호선한다.

o 인증위원회는 인증심사팀이 심의·의결을 요구하거나 위원장이 인증위원회의 개최가 필요하다고 인정하는 경우 개최할 수 있다.

- 회의는 위원 과반수의 출석으로 개의하며, 출석위원 2/3 이상의 찬성으로 의결한다.

- 정보보호 관리체계 인증기관의 장은 인증심사원이 실시한 심사결과를 위원회 개최 5일 전까지 인증위원회에 제출한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제22조(인증위원회의 운영)
① 인터넷진흥원 또는 인증기관의 장은 인증위원회의 심의안건을 검토하여 위원회 개최 5일 전까지 인증위원회에 제출한다.

- 인증위원회 위원장은 정보보호 관리체계 인증기관의 장에게 인증심사원이 실시한 인증심사 결과가 인증기준에 적합한지 여부를 심의하고 그 결과를 제출한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제22조(인증위원회의 운영)
② 인증위원회 위원장은 제21조제1항 각 호의 사항에 대한 심의·의결 결과를 인터넷진흥원 또는 인증기관의 장에게 제출한다.

o 인증위원회는 인증기관에서 수행한 인증심사결과가 인증 기준에 적합한지 등을 심의・의결하고, 그 결과에 따라 인증기관은 인증서를 발급한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

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.

o 한국인터넷진흥원 또는 인증기관은 발급된 인증서를 관리하여야 한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제24조(인증서 발급)
① 인터넷진흥원 또는 인증기관은 발급된 인증서의 인증번호, 발급일, 유효기간 등 인증서를 관리하여야 한다.

- 인증 취득기업이 인증서의 재발급 또는 인증서 기재사항의 변경을 요청할 경우에는 한국인터넷진흥원 또는 인증기관에 신청서를 제출하여야 한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제24조(인증서 발급)
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.

[표3-1] 위원회 구성 타법 사례

법	위원회	구성 방식	위원회 개최 방식
행정심판법	행정심판위원회	위원장 1명을 포함한 30명 이내의 위원으로 구성	위원장이 회의마다 8명 지정
개인정보 보호법	개인정보분쟁 조정위원회	위원장 1명을 포함한 20명 이내의 위원으로 구성	위원장이 지명하는 5명 이내의 위원으로 구성
국민건강 보험법	분쟁조정위원회	위원장을 포함하여 35명 이내의 위원으로 구성	회의는 위원장, 당연직위원 및 원장이 매 회의마다 지정하는 7명의 위원을 포함하여 총 9명으로 구성
지방공무원법	심사위원회	16명 이상 20명 이하의 위원으로 구성	위원장과 시·도지사 또는 교육감이 회의마다 지정하는 6명의 위원으로 구성

3.2 인증심사원

o 인증심사원은 한국인터넷진흥원에서 규정한 인증심사원의 자격요건, 자격 유지요건, 자격정지 및 취소 기준 등에 따라 풀로 관리되고 있다.

o 인증심사원 자격을 갖추기 위해서는 인증심사원 양성 교육을 수료 후, 최종 평가시험에 합격해야 한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제9조(인증심사원의 자격 요건 등)
② 인증심사원이 되려는 자는 별표 3의 학력 및 경력 요건을 갖추고 인터넷진흥원이 지정하는 기관에서 인증심사원 양성교육 과정을 수료하여야 한다.

- 최종 합격자는 인증심사원 자격신청서를 한국인터넷진흥원에 제출하고, 한국인터넷진흥원은 경력 요건의 적합 여부를 확인하여 통과한 자에게 자격을 부여한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제11조(인증심사원 자격 부여)
③ 인터넷진흥원은 인증심사원 자격의 적합 여부를 확인하여 통과한 자에게 별지 제9호서식의 인증심사원 자격 증명서를 발급하여야 한다.

- 인증심사원 자격심의를 통과한 자는 인증심사원 풀에 등록되며, 인증심사원 풀에 등록된 인증심사원은 정보보호 관리체계 인증심사에 참여 신청을 할 수 있다.

o 인증심사원의 자격은 심사원보, 심사원, 선임심사원 으로 구분된다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제9조(인증심사원의 자격 요건 등)
① 인증심사원은 심사원보, 심사원, 선임심사원으로 구분하며, 인증심사원 등급별 자격 요건은 별표 3과 같다.

[표3-2] 인증심사원 자격 구분

구 분	정 의
심사원보	인증심사원 학력 및 경력 요건을 만족하는 자로서 인터넷진흥원이 지정하는 기관에서 인증심사원 양성교육 과정을 수료한 자
심사원	심사원보 자격 취득자로서 인증심사 4회 이상 참여하고 심사일수의 합이 20일 이상인 자
선임심사원	심사원 자격 취득자로서 3회 이상 심사 총괄업무를 수행하고 심사일수의 합이 15일 이상인 자

< 자격요건 >

o 인증심사의 신뢰성을 확보하기 위하여 인증심사원이 공통적으로 만족하여야 할 자격요건은 다음과 같다.

- 공정하고 객관적인 심사를 수행할 수 있는 자질을 갖추어야 한다.
- 심사원칙, 절차 및 기법, 전문분야 및 관련법규 등 심사에 대한 지식 및 숙련도를 갖추어야 한다.
- 인증심사의 수행에서 취득한 정보를 관련 법령 또는 신청기관의 동의 없이 외부에 누설하지 말아야 한다.

o 인증심사원의 학력 및 경력 요건은 다음과 같다.

- 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)
- 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

- 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)

< 자격신청 >

o 인증심사원의 자격을 취득하기 위해서는 한국인터넷진흥원에 인증심사원 자격 신청을 하여, 한국인터넷진흥원 인증심사원 자격심의위원회의 심의를 통해 자격요건을 충족한 자로 판정받아야 한다.

o 인증심사원 자격취득을 위해서는 인증심사원 자격 요건을 갖췄음을 확인할 수 있는 서류를 제출해야 한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제10조(인증심사원의 자격 신청)
인증심사원의 자격을 신청하고자 하는 자는 제9조제2항에 따라 인증심사원 양성 교육 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)

< 자격유지 및 자격관리 >

o 인증심사원의 자격 유효기간은 자격 인증을 받은 날로부터 3년으로 한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제12조(인증심사원 자격 유지)
① 인증심사원의 자격 유효기간은 자격 부여를 받은 날로부터 3년으로 한다.

o 인증심사원은 자격 유지를 위해 유효기간 내에 인터넷진흥원이 지정하는 기관에서 시행하는 인증심사원 보수교육을 이수해야 하며, 다만 부득이한 사유로 보수교육을 받지 못한 경우에는 인터넷진흥원이 인정하는 대체 교육을 받아야 한다.

※ 보수교육을 이수한 자에 한하여 자격 유효기간이 3년간 연장됨

관련근거

정보보호 관리체계 인증 등에 관한 고시

제12조(인증심사원 자격 유지)
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.

< 자격정지 및 취소 >

o 인증심사원의 자격정지 여부와 자격정지기간은 인증심사원 자격심의위원회의 심의를 거쳐 결정한 후 해당 인증심사원에게 통보된다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

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.

- 인증심사원 자격이 취소된 자는 위촉장을 한국인터넷진흥원에 반납하여야 하며, 자격이 취소된 날로부터 3년이 경과하여야 인증심사원 자격을 다시 신청할 수 있다.

[표3-3] 인증심사원 자격정지 또는 자격취소 경우

구 분	해당 경우
자격정지	- 인증심사원이 자격갱신을 하지 않고 자격유효기간이 종료한 경우 - 인증심사원이 심사원 의무사항을 위반하여 직무를 수행한 경우

자격취소	- 인증심사원 자격 신청 시 제출한 서류가 허위로 판명된 경우 - 인증심사원이 자격갱신을 하지 않아 자격이 정지되고, 자격정지일로부터 3년이 경과하도록 자격을 갱신하지 않을 경우 - 인증심사원 자격이 정지된 상태에서 인증심사 등 심사원으로서의 업무를 수행한 경우 - 인증심사 수행 부적합조건에 해당하면서 인증심사에 참여한 경우 < 인증심사 수행 부적합 조건 > · 인증심사원이 피인증심사기관에 재직 중이거나 이직 후 1년이 경과하지 않은 경우 · 인증심사원 본인이나 인증심사원의 소속사가 인증심사수행 시작일로부터 과거 1년 이내에 피인증심사기관의 정보보호 관리체계와 관련된 컨설팅 등 보안컨설팅에 참여한 경우

< 심사원의 역할 >

o 인증심사원의 역할은 다음과 같다.

- 인증심사에 대한 요구사항을 명확히 한다.
- 인증심사결과는 명료하게 결론을 내리며, 부당하게 지체함이 없이 보고한다.
- 인증심사 결과보고서를 작성하고, 인증심사 내용의 효과성을 검증한다.

< 의무사항 >

o 인증심사원의 직무수행 시 준수해야 할 의무사항은 다음과 같다.

- 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 안 된다.
- 인증심사원은 인증업무지침을 성실히 준수한다.
- 인증심사원은 인증심사의 수행과 관련하여 상업적, 재정적 그리고 기타 모든 압력을 배제한다.

< 비밀유지 >

o 인증심사원은 인증심사 수행 중 취득한 정보에 대해 비밀유지를 해야 하며, 비밀을 누설하거나 직무 외의 목적으로 사용할 경우 3년 이하의 징역 또는 3천만원 이하의 벌금에 처해진다.

관련근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률

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.
2. 제47조에 따른 정보보호 관리체계 인증업무

관련근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제72조(벌칙)
① 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
5. 제66조를 위반하여 직무상 알게 된 비밀을 타인에게 누설하거나 직무 외의 목적으로 사용한 자

[표3-4] 유사 인증제도 심사원 분류 비교

구분	ISO 인증	정보시스템 평가 · 인증시스템	정보시스템 감리 제도
관리 기관	한국심사 자격인증원	국정원	지식경제부
심사원 분류	검증심사원 선임심사원 심사원 심사원보	선임평가자 주임평가자 수습평가자	수석감리원 감리원

3.3 인증기관

o 정보보호 관리체계를 구축·운영하고 있는 자의 정보보호 관리체계가 미래창조과학부가 고시한 기준에 적합한지에 관하여 인증을 해줄 수 있는 기관으로는 한국인터넷진흥원과 미래창조과학부가 지정한 정보보호 관리체계 인증기관이 있다.

- 현재 한국인터넷진흥원을 단일 인증기관으로 운영 중이다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제2조(용어의 정의)
1. "정보보호 관리체계 인증기관(이하 '인증기관'이라 한다)"이란 법 제47조제5항에 따라 방송통신위원회가 인증에 관한 업무를 수행할 수 있도록 지정한 기관을 말한다.

< 지정기준 >

o 정보보호 관리체계 인증기관으로 지정되기 위해서는 다음 기준에 적합함을 미래창조과학부의 정보보호 관리체계 인증기관 지정절차에 의해 인정받아야 한다.

관련근거

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

제53조(정보보호 관리체계 인증기관의 지정기준)
① 법 47조제5항에 따른 정보보호 관리체계 인증기관의 지정기준은 다음 각 호와 같다.
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

- 인증심사원을 5명 이상 보유해야 한다.

- 미래창조과학부가 실시하는 업무수행 능력 심사에서 적합하다고 인정받아야 한다.

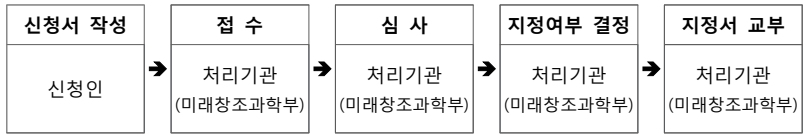
관련근거

정보보호 관리체계 인증 등에 관한 고시

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.

< 지정절차 >

o 미래창조과학부가 정보보호 관리체계 인증기관을 지정하는 절차는 인증기관 지정신청, 지정심사, 인증기관 지정으로 이루어진다.



(그림3-1) 정보보호 관리체계 인증기관 지정절차

(인증기관 지정신청)

- 미래창조과학부는 정보보호 관리체계 인증기관을 지정할 필요가 있을 경우 지정대상 기관의 수, 업무의 범위 및 신청요령 등을 정하여 관보 및 인터넷 홈페이지에 20일 이상 공고하여야 한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

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.

- 정보보호 관리체계 인증기관으로 지정을 받으려는 자는 정보보호 관리체계 인증기관 지정신청서에 서류를 첨부하여 미래창조과학부에 제출하여야 한다.

관련근거

정보보호 관리체계 인증 등에 관한 고시

제3조(인증기관의 지정 등)
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

[표3-5] 인증기관 지정신청 시 제출서류

구 분	제출서류
1. 일반	- 법인의 정관 또는 단체의 규약
2. 인증심사업무를 전담하는 직원의 보유현황과 이를 증명할 수 있는 서류	- 정보보호수행실적 명세서 및 이를 증빙할 수 있는 자료 (결과보고서 등) - 계약서 사본 및 세금계산서 등
3. 정보보호 업무를 수행한 경력이나 전문화 정도 등 업무수행능력 심사를 위하여 필요한 서류	- 총매출액대비 정보보호분야 매출액의 비율 계산 내역 (공인회계사 또는 회계담당자가 서명 날인한 서류) - 부채비율 및 자기자본 이익률의 계산내역 (회결산내역 등 관련 증빙자료) - 인증업무 운영체계 관련 규정 및 지침 등 · 인증기관의 운영체계 및 인증의 품질관리 · 인증업무를 수행하는 직원에 대한 운영관리 등의 내부규정 · 인증업무 수행 방법 및 절차

(인증기관 지정심사)

- 미래창조과학부는 인증기관의 지정신청을 받은 경우 인증기관 심사위원회를 개최하여 해당 기관의 적합성 여부에 대한 심사업무를 수행한다.

- 심사위원회 위원장은 심사위원회를 대표하여 미래창조과학부에 인증기관 지정 적합성 여부에 대한 심사결과를 제출한다.

(인증기관 지정)

- 미래창조과학부는 심사위원회의 결과를 기반으로 신청을 받은 날부터 3개월 이내에 그 지정결과를 신청인에게 통지한다.

- 인증기관으로 지정되는 신청인에게 정보보호 관리체계 인증기관 지정서를 교부한다.

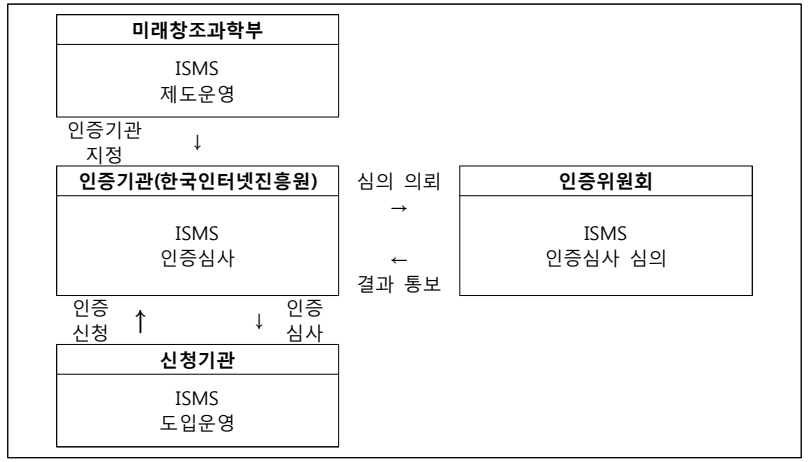
(인증기관 재지정)

- 인증기관 지정의 유효기간은 3년이며, 유효기간이 끝나기 전 6개월부터 끝나는 날까지 재지정 신청을 할 수 있으며, 이 경우 재지정의 신청에 대한 처리결과를 통지받을 때까지는 그 지정이 계속 유효한 것으로 본다.

- 인증기관 재지정 절차는 최초 지정절차와 동일한 절차를 준용한다.

[표3-6] 주요 추진체계 별 업무

주체	주요 업무
미래창조과학부	- 법제도 개선 및 정책 결정 - 인증기관 지정
한국인터넷진흥원	- 인증심사 신청 접수 - 인증심사 및 사후관리 - 인증서 발급 및 관리 - 인증위원회 운영 - 인증심사원 풀 구성 · 운영 - 기술자문 및 상담
신청기관	- 정보보호 관리체계 구축 및 운영 - 정보보호 관리체계 인증 취득



(그림3-2) 주요 추진체계 별 업무 흐름

제4장 정보보호 관리체계(ISMS) 구축 및 운영

4.1 정보보호 관리체계 구축 준비 및 전략 수립 단계

4.1.1 수행조직 구성

o 정보보호 관리체계 구축을 위해서는 전담 수행조직이 필요하며, 수행조직은 타부서와의 협업이 필요하다.

※ 정보보호 관리체계 구축은 수행조직의 단일 업무가 아닌 전사 차원의 업무임

- 처음 정보보호 관리체계를 구축할 경우, 수행조직의 구성 및 정보보호의 역할 할당이 어려우므로 전반적인 정보보호계획을 수립하기 위한 단기 작업반(TFT, Task Forced Team)이 구성될 수도 있다.

o 수행조직은 정보보호 관리체계에 대한 전반적인 이해 교육 등이 필요하다.

- 인증기관의 교육, 세미나 등의 참여를 통하여 정보보호 관리체계에 대한 이해도를 높이는 것이 좋다.

o 수행조직 내에 구축을 위한 전문가가 존재하지 않거나 조직 규모 등으로 인해 수행조직을 구성하기 어려울 경우, 외부전문가에게 자문을 구할 수 있다.

- 구축 담당자가 외부전문가의 지원을 받는 경우, 외부전문가가 구축의 주담당이 되지 않도록 해야 한다.

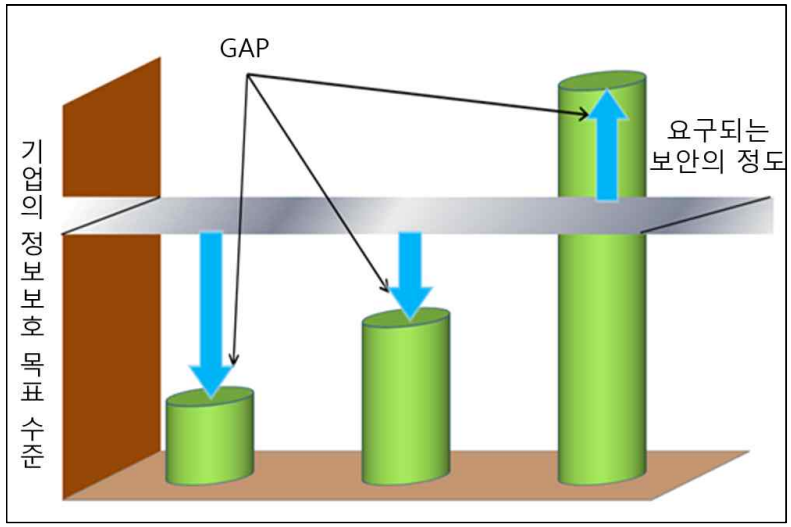
- 구축 담당자는 조직에 맞게 정보보호 관리체계를 구축해야 하며, 구축 완료 후에도 지속적인 개선을 통해 정보보호 관리체계를 보완해 나가야 한다.

4.1.2 정보보호 수준현황 분석

o 정보보호 관리체계를 효과적으로 구축하기 위해 정보보호 관리체계 수준 현황 분석(이하 “수준현황 분석”이라 한다)을 사전에 실시할 수도 있다.

- 수준현황 분석은 정보보호 관리체계 인증기준을 바탕으로 조직의 현재 정보보호 관리 수준을 확인하기 위한 절차이며, 관련 부서 인터뷰 및 문서 검토를 통해 수행할 수 있다.

o (그림4-1)은 조직이 현재 적용하고 있는 정보보호대책과 조직이 달성해야 하는 정보보호 목표 수준과의 차이를 보여주는 것이다.



(그림4-1) 정보보호 수준 분석

o 수준현황 분석 결과는 다음 사항을 검토하는데 활용할 수 있다.

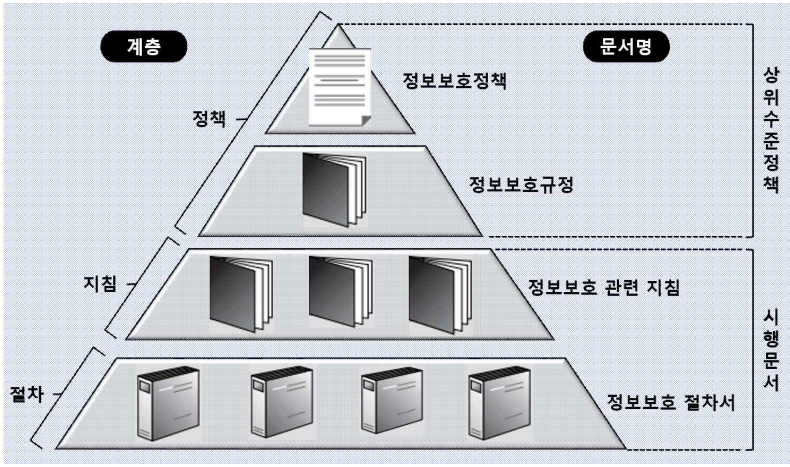
- 정보보호 관리체계 구축 소요 예산 산정

- 정보보호 관리체계 수행조직 구성

- 기타 정보보호 관리체계 구축을 위해 필요한 사항 등

4.2 정보보호정책 수립 및 범위설정 단계

4.2.1 정보보호정책의 수립



(그림4-2) 정보보호정책 체계 (예시)

o 정보보호정책의 수립의 요구사항은 다음과 같다.

관리과정		세부관리과정	관리과정 상세내용
정보보호정책 수립 및 범위설정	1.1	정보보호정책의 수립	조직이 수행하는 모든 정보보호 활동의 근거를 포함할 수 있도록 정보보호정책을 구축하고 동 정책은 국가나 관련 산업에서 정하는 정보보호 관련 법, 규제를 만족하여야 한다.

o 관리과정에서의 정보보호정책은 최상위 수준의 정보보호정책을 의미한다.

- 정보보호정책의 체계는 상위 정책과 하위 정책 시행문서로 구성하여야 한다.

o 정보보호 관리체계가 구축되기 이전의 조직은 정보보호 활동을 위한 최소한의 정책만을 정하고 있거나 별도의 정책없이 관행적으로 업무를 추진하고 있는 경우도 있다.

- 따라서 정보보호 관리체계를 구축하는 경우, 관리체계 관련 기준 및 법적요구사항 등을 만족하도록 정보보호정책을 수립하여야 한다.

o 정보보호정책에 포함되어야 할 항목은 다음과 같다.

- 최고 경영자 등 경영진의 정보보호에 대한 의지 및 방향 : 조직의 최고 책임자가 정책을 승인하고 지원의지를 알려야 한다.

- 조직의 정보보호 목적 : 조직의 중요한 정보자산 및 서비스를 식별하고 그 보호 목적(기밀성, 무결성, 가용성 등)을 명확하게 선언하여야 한다.

- 조직의 정보보호 범위 : 정책의 적용범위를 의미하며 전 조직을 대상으로 하고 정보자산에 접근하는 외부인을 포함하는 것이 가장 일반적이다.

- 조직의 정보보호 책임 : 정책을 수행하기 위해서는 기본적으로 책임 사항을 정의한다.

- 조직이 수행하는 관리적, 기술적, 물리적 정보보호 활동의 근거

o 상위 정보보호정책의 내용은 “정보는 비인가된 접근으로부터 보호하여야 한다.”는 정도로 간단하고 명료하게 작성한다.

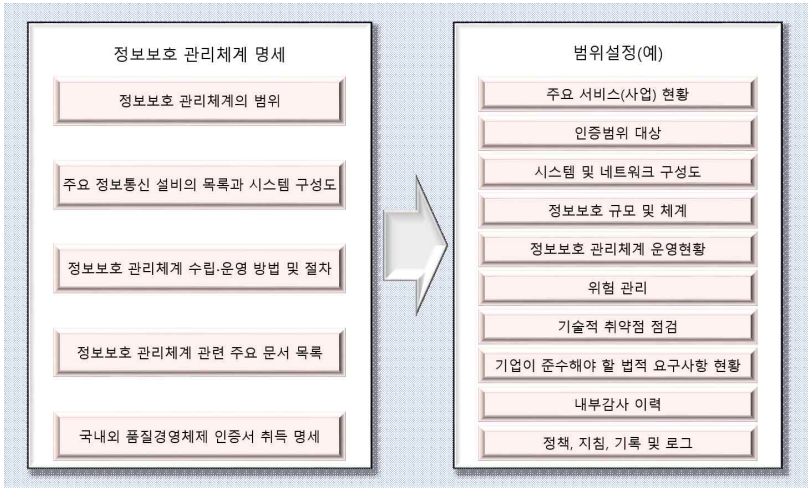
o 조직은 제공하고 있는 사업(서비스)에서 조직이 준수해야 하는 정보보호 관련 법적 요구사항을 분석하고 정보보호정책에 반영하여야 한다.

※ 정보보호 관련 법률 예시 : 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 개인정보보호법, 전자금융거래법, 부정경쟁방지 및 영업비밀보호에 관한 법률 등

o 상위 정보보호정책을 시행하기 위한 세부적인 수행주체, 방법, 절차 등은 정보보호 지침, 절차, 매뉴얼 등의 형식으로 수립하여야 한다.

o 정보보호정책은 지속적인 검토 및 개선이 필요하다.

4.2.2 범위설정



(그림4-3) 정보보호 관리체계 범위설정

o 범위설정의 요구사항은 다음과 같다.

관리과정		세부관리과정	관리과정 상세내용
정보보호정책 구축 및 범위설정	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.

o 정보보호 관리체계 범위에는 사업(서비스)와 관련된 임직원, 정보시스템, 정보, 시설 등 유·무형의 핵심자산이 누락 없이 포함되어야 한다.

- 범위 외의 다른 시스템, 조직, 제3자와의 관계 등 다른 부분과의 관계를 반드시 명시해야 한다.

o 정보보호 관리체계의 범위 내 서비스, 업무, 조직, 정보시스템, 설비 등을 명확하게 정의하여 정보보호 관리체계 범위를 충분하게 설명하여야 한다.

- 정보보호 관리체계 범위가 특정 영역에만 해당되는 경우, 범위 영역 경계를 식별하여 문서화하고 범위가 일부일 경우 전체사업 대비 해당 범위를 명확하게 식별할 수 있도록 하여야 한다.

- 조직 내에서 정보보호 관리체계의 범위에 포함되지 않는 부서, 인력, 사업, 정보자산 등이 있다면 이러한 제외 이유를 명확하고 타당성 있게 설명해야 한다.

o 정보보호 관리체계 범위에 포함되어야 할 내용의 예시는 다음과 같다.

- 정보보호 관리체계의 범위
  ※ 주요 서비스(사업) 현황 등
- 주요 정보통신 설비의 목록과 시스템 구성도
  ※ 인증범위 대상, 시스템 및 네트워크 구성도 등
- 정보보호 관리체계 수립·운영 방법 및 절차
  ※ 정보보호 규모 및 체계, 정보보호 관리체계 운영현황, 위험 관리, 기술적 취약점 점검, 기업이 준수해야 할 법적 요구사항 현황, 내부감사 이력 등
- 정보보호 관리체계 관련 주요 문서 목록
  ※ 정책, 지침, 절차, 기록 및 로그 등
- 국내외 품질경영체제 인증서 취득 명세

o 정보자산의 분류기준을 수립하고 정보보호 관리체계 범위 내 모든 정보자산을 식별해야 한다.

- 조직의 업무 특성에 적합한 분류기준을 정의해야 한다.
- 수립된 분류기준에 따라 정보보호 관리체계 범위 내 모든 정보자산을 식별해야 한다.

o 식별된 정보자산에 대한 정보자산명, 용도, 책임자 및 관리자, 관리부서, 보안등급 등의 정보자산 정보를 확인할 수 있도록 목록으로 관리하여야 한다.

※ 다만 목록은 자산관리시스템, 문서 등 다양한 형태로 관리 가능함

4.3. 경영진 책임 및 조직 구성 단계

4.3.1 경영진 참여

o 경영진 참여의 요구사항은 다음과 같다.

관리과정		세부관리과정	관리과정 상세내용
경영진 책임 및 조직구성	2.1	경영진 참여	정보보호 관리체계 구축 및 운영 등 조직이 수행하는 정보보호 활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 구축하여야 한다.

o 정보보호정책의 제·개정 승인 및 공표, 위험관리, 내부감사 등과 같은 중요한 사안에 대해 경영진이 참여하여 의사결정을 하여야 한다.

o 경영진의 책임과 역할의 정의가 상위 정보보호정책에 규정되어야 하고 그에 따른 보고체계를 갖추어야 한다.

4.3.2 정보보호 조직 구성 및 자원 할당

o 정보보호 조직 구성 및 자원 할당의 요구사항은 다음과 같다.

관리과정		세부관리과정	관리과정 상세내용
경영진 책임 및 조직구성	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.

o 최고경영자는 정보보호 관리체계의 지속적인 운영이 가능하도록 조직의 규모, 업무 중요도 등에 따라 요구되는 정보보호 조직을 구성하여야 한다.

※ 정보보호 조직 : CISO, 실무조직, 정보보호위원회 등

- 실무조직은 전담 또는 겸임조직으로 구성할 수 있으며 겸임조직으로 구성하더라도 정보보호 조직에 대한 공식적인 선언 또는 지정이 필요하다.

o 최고경영자는 정보보호 관리체계 구축 및 운영을 하는데 필요한 자원을 파악하여 예산 및 인력 운영계획에 대한 적절한 투자가 이루어지도록 지원하여야 한다.

4.4. 위험관리 단계

4.4.1 위험관리 방법 및 계획 수립

o 위험관리 단계(위험관리 방법 및 계획 구축)의 요구사항은 다음과 같다.

관리과정		세부관리과정	관리과정 상세내용
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.

< 위험관리 방법 선정 >

o 위험관리 방법론은 조직 전 영역(관리적, 기술적, 물리적, 법적 분야)에 대한 위험식별 및 평가가 가능하도록 각 영역별 특성을 반영한 방법을 선정하여야 한다.

※ 관리적, 물리적, 법적 분야의 방법론 예시 : 베이스라인 접근법
※ 기술적 분야의 방법론 예시 : 상세위험분석 또는 복합접근법

- 핵심자산에 대한 기술적 위험분석의 경우, 상세 위험분석(자산 중요도, 위협, 취약점)을 수행하는 것이 바람직하다.

- 외부 전문가를 활용할 경우 전문가별로 위험관리 방법론이 변경되는 것을 방지하기 위하여 조직 내 정의된 위험관리방법론에 따라 자문을 받는 것을 고려하여야 한다.

< 위험관리 계획 수립 >

o 위험관리 방법 및 절차에 따라 위험관리대상, 위험관리 수행 인력 등이 포함된 위험관리계획을 매년 수립하고 이행하여야 한다.

- 위험관리 대상에는 정보보호 관리체계 인증범위 내 핵심자산 및 서비스가 누락 없이 포함되어야 한다.

- 위험관리 수행 인력에는 위험관리 방법, 조직의 업무 및 시스템에 대한 전문성을 갖춘 인력뿐만 아니라 관련 부서 실무책임자도 포함하여야 하며 필요시 외부 전문가를 활용할 수 있다.

※ 외부 전문가 활용 시 정보자산별 위험분석 결과를 이해하기 위한 목적으로 조직 내 위험관리 책임자가 함께 참여하여야 한다.

- 매년 위험관리 수행 시 위험관리 방법론의 적정성도 함께 검토하여야 한다.

o 주기적인 위험관리 수행 이외에 조직의 정보자산 변화, 정보보호 환경의 변화 등이 조직의 정보보호 환경에 영향을 미치는 경우에도 위험분석을 재수행하는 것이 좋다.

4.4.2 위험식별 및 평가

o 위험관리 단계(위험식별 및 평가)의 요구사항은 다음과 같다.

관리과정		세부관리과정	관리과정 상세내용
위험관리	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.

o 정보보호 관리체계 범위 전 영역에 대하여 법적 준거성, 관리적, 운영적, 물리적, 기술적 관점에서 연 1회 이상 위험을 식별하고 평가하여야 한다.

- 정보보호 및 개인정보보호 관련 법적 요구사항 준수여부에 대한 위험을 식별하여야 한다.

- 관리적, 운영적, 물리적 위험은 정보보호 관리체계 통제항목이 적용되고 있는지 점검하여 통제적용이 이루어지지 않거나 미흡한 경우 위험으로 식별하여야 한다.

- 기술적 위험은 정보보호 관리체계 범위 내 정보시스템, 정보보호시스템 등에 대한 취약점 점검을 수행하여 발견된 취약점을 위험으로 식별하여야 한다.

o 위험관리담당자는 식별된 정보자산을 목록으로 관리하고 각 자산별 가치 산정 기준을 정의하여야 하며, 관련 부서 담당자의 의견을 반영하여 기준을 정의할 수 있다.

※ 자산별 가치 산정 기준의 예 : 서비스 영향/이익 손실/고객 상실/대외이미지 또는 기밀성/무결성/가용성 관점

- 만약 자산 중 용도, 사양(Specification), 관리부서, 자산가치 등이 모두 동일하다면 효율적인 위험분석 및 평가를 위하여 대상을 그룹핑(Grouping)을 하는 것도 좋은 방법이다.

< 수용 가능한 위험수준 설정 및 관리 >

o 식별된 위험과 각 위험도를 검토하여 수용 가능한 목표 위험수준(이하 DoA)을 정한 뒤 이를 초과하는 위험을 식별하여야 한다.

※ DoA : Degree of Assurance

- 수용 가능한 목표 위험수준은 논리적이거나 수리적인 방법을 통하여 계산될 필요는 없으나 반드시 정보보호 최고책임자 등 경영진의 의사결정에 의하여 결정되어야 한다.

- 식별된 위험에 대한 평가 보고서는 정보보호 최고책임자를 포함한 경영진의 검토 및 승인을 거쳐야 한다.

4.4.3 정보보호 대책 선정 및 이행계획 수립

o 위험관리 단계(정보보호대책 선정 및 이행계획 구축)의 요구사항은 다음과 같다.

관리과정		세부관리과정	관리과정 상세내용
위험관리	3.3	정보보호대책 선정 및 이행계획 구축	위험을 수용 가능한 수준으로 감소시키기 위해 정보보호대책을 선정하고 그 보호대책의 구현 우선순위, 일정, 담당부서 및 담당자 지정, 예산 등을 포함한 이행계획을 구축하여 경영진의 승인을 받아야 한다.

< 정보보호대책 선정 >

o 식별된 위험을 수용 가능한 위험 수준으로 감소시키기 위하여 정보보호 관리체계의 통제항목과의 연계성을 고려하여 정보보호대책을 선정하여야 한다.

- 위험수준 감소를 목표로 위험처리 전략을 수립하는 게 일반적이며 위험회피, 위험전가, 위험수용 등으로 고려할 수 있다.

[표4-1] 위험 처리 전략

구분	내용
위험수용	- 위험을 받아들이고 비용을 감수함
위험감소	- 위험을 감소시킬 수 있는 대책을 채택하여 구현함
위험회피	- 위험이 존재하는 프로세스나 사업을 포기함
위험전가	- 잠재적 비용을 제3자에게 이전하거나 할당함

- DoA를 초과하지 않은 위험 중 기업 및 외부 환경에 따라 위험 수준이 상승할 가능성이 높거나 조직이 중요하다고 판단하는 부분에 대해서는 필요시 보호대책 수립을 고려할 수 있다.

- 위험수용 전략의 선택은 경영진, 정보보호 관리체계 인증 심사팀 등 조직 내 · 외부에서 객관적으로 인정하는 경우에 가능하다.

- 기술적인 위험을 감소시키기 위한 취약점 제거 시 이를 이행하기 위한 시기와 소요예산을 함께 고려하는 것이 좋다.

o 정보보호대책은 법적 요구사항수준과 동일하거나 높은 수준으로 마련하여야 한다.

- 예를 들어, 외부에서 개인정보처리시스템 접근이 가능한 경우 '개인정보의 기술적 · 관리적 보호조치 기준(고시)'에 따라 공인인증서 등 안전한 인증수단을 적용하도록 명시하고 있으나 ID와 패스워드로 접근을 통제하는 경우 법적 요구사항을 준수하지 않은 것에 해당한다.

<정보보호대책 이행계획 수립>

o 정보보호대책 이행을 위한 계획을 수립하고 정보보호 최고책임자 등 경영진의 승인을 받아야 한다.

- 위험수준의 감소를 위하여 선정한 정보보호대책은 위험처리의 시급성, 예산 할당, 구현에 요구되는 기간에 따라 우선순위를 정하고 계획을 수립하여 지속적으로 관리하여야 한다.

- 정보보호 최고책임자 등 경영진은 정보보호 대책의 효과적인 이행을 위하여 이행계획을 승인하고 이행여부를 확인하기 위한 절차 및 방법도 함께 고려하여야 한다.

4.5. 정보보호 대책 구현 단계

4.5.1 정보보호대책의 효과적 구현

o 정보보호대책 구현 단계(정보보호대책의 효과적 구현)의 요구사항은 다음과 같다.

관리과정		세부관리과정	관리과정 상세내용
정보보호대책 구현	4.1	정보보호대책의 효과적 구현	정보보호대책 이행계획에 따라 보호대책을 구현하고 경영진은 이행결과의 정확성 및 효과성 여부를 확인하여야 한다.

< 정보보호대책 구현 >

o 식별된 위험에 대한 위험수준이 감소되었음을 보장하기 위하여 정보보호 책임자 등 경영진은 정보보호대책이 이행계획에 따라 빠짐없이 효과적으로 이행되었는지 여부를 검토 및 확인하여야 한다.

< 경영진의 이행결과 확인 >

o '정보보호 대책명세서'를 작성하여 정보보호 관리체계 인증기준에서 제시하는 통제항목별 운영현황을 확인할 수 있도록 하여야 한다.

- 미선정 통제항목이 있을 경우, 미선정 사유를 명확하게 명시하고 정보보호 최고책임자 등 경영진의 승인을 득하여 부주의 혹은 의도적으로 통제항목 선정에서 배제되지 않도록 하여야 한다.

4.5.2 내부 공유 및 교육

o 정보보호대책 구현 단계(내부 공유 및 교육)의 요구사항은 다음과 같다.

관리과정		세부관리과정	관리과정 상세내용
정보보호대책 구현	4.2	내부 공유 및 교육	구현된 정보보호대책을 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여야 한다.

< 운영 부서 및 담당자 파악 >

o 정보보호 관리체계 내재화를 위하여 다음과 같은 사항으로 정보보호 활동업무에 영향이 발생하는 경우, 관련부서 및 담당자를 파악하여 정보보호대책의 내용을 공유하고 교육을 수행하여야 한다.

- 정책(지침 및 절차 포함) 신규 제정 및 개정
- 정보시스템 신규 도입 및 개선 등

o 정보보호 관리체계 운영과 시행에 관련된 부서 및 담당자뿐만 아니라 조직의 임직원, 임시직원, 외주용역업체 직원 등 모든 인력을 대상으로 최소 연 1회 이상 정보보호 교육을 수행하여야 한다.

- 정보보호교육 연간 계획은 전년말도 혹은 당해 1/4분기 이내에 수립하여야 한다.
- IT 및 정보보호 조직 내 임직원은 정보보호 관련 직무별 전문성 제고를 위하여 정보보호 관련 컨퍼런스, 세미나, 교육 전문기관 등을 활용하여 별도의 교육을 받아야 한다.
- 정보보호(개인정보 포함)관련 법률 변경, 조직 내 정보보호 정책 및 절차 변경, 조직 내 · 외부 보안사고 발생, 업무 환경의 중대한 변화 발생 시 추가적인 교육을 수행하여야 한다.
- 출장, 휴가 등의 사정으로 정기 정보보호 교육을 받지 못한 인력에 대한 교육 방법을 마련하여야 한다.
- 채용으로 인해 신규 인력 발생 시 업무 시작 전 정보보호 교육을 시행

하여야 한다.

o 정보보호 교육 내용에는 정보보호의 기본 개요, 정보보호 관리체계 구축 절차 및 방법, 정보보호 관련 법률, 정보보호 규정 위반 시 상벌규정 및 책임 등을 포함하여야 한다.

o 정보보호 교육시행 후 교육 공지, 교육자료, 출석부 등과 같은 기록을 남기고 평가기준에 따라 설문 또는 테스트 등을 통하여 교육 내용의 적절성과 효과성을 평가하여야 한다.

- 교육평가 결과 내용에서 도출된 문제점에 대한 개선 대책을 마련하고 차기 교육 계획 수립 시 반영하여야 한다.

4.6 사후관리 단계

4.6.1 법적요구사항 준수검토

o 사후관리 단계(법적요구사항 준수검토)의 요구사항은 다음과 같다.

관리과정		세부관리과정	관리과정 상세내용
사후관리	5.1	법적요구사항 준수검토	조직이 준수해야 할 정보보호 관련 법적요구사항을 지속적으로 파악하여 최신성을 유지하고 준수여부를 지속적으로 검토하여야 한다.

o 정보보호 관리체계 구축 및 운영에 있어서 조직이 준수해야 하는 법령의 관련 조항, 세부 내용을 파악하고 준수여부를 주기적으로 검토할 수 있는 절차를 수립하여야 한다.

- 관련 법규의 제 · 개정 현황을 최소 연 1회 이상 검토하여 조직의 정책 및 절차에 반영하여 법규 미준수로 인한 과태료 부과 등과 같은 상황이 발생하지 않도록 대응하여야 한다.

- 법적 준수여부 검토는 독립적인 절차로 수행하거나 보안감사 계획에 포함하여 감사 수행 시 함께 수행하여도 된다.

- 법적 요구사항 준수 검토 활동의 증적자료(예 : 회의록 또는 보고서)를 작성 및 관리하는 것이 바람직하다.

[표4-2] 정보보호 관련 법률 예시

구분	법률명	주요 고려사항
산업보안	부정경쟁방지 및 영업비밀 보호에 관한 법률	영업비밀을 취급하는 모든 기업을 대상으로, 행위주체(인적)에 대한 비밀유지의무와 기업의 역할(비밀설정 및 보호조치) 고려
	산업기술의 유출방지 및 보호에 관한 법률	국가로부터 지정받은 산업기술 및 국가핵심기술을 보유한 국가기관/기업/연구기관 및 대학 등(이하 '기관")을 대상으로, 행위주체(인적)에 대한 비밀유지의무와 대상기관의 보호조치 고려
지적재산	저작권법	논문, 강연 등의 어문저작물과 컴퓨터프로그램 등을 저작한 저작자의 이익을 보호하기 위한 역할 고려

기반 시설	정보통신 기반보호법	국가안전보장, 행정, 국방, 치안, 금융, 통신, 운송, 에너지 등의 업무와 관련된 정보통신망을 운영하는 기업 및 국가 공공기관을 대상으로, 정보통신망 운용의 기반이 되는 시설을 보호하기 위한 역할과 보호조치 고려
정보 통신 보안	정보통신망이용촉진 및 정보보호 등에 관한 법률	정보통신망법에 따라 정보보호 관리체계 인증 획득이 요구되는 정보통신서비스제공자 등은 정보보호 관리체계 인증을 획득하는 정도의 정보보호 수준을 유지
	전자금융거래법	금융기관 및 전자금융업자가 전자금융거래의 안전성 확보 및 이용자 보호 이무사항 고려
개인 정보 보호	정보통신망이용촉진 및 정보보호 등에 관한 법률	개인정보를 취급하는 정보통신서비스제공자는 개인정보의 취급단계별 관리적, 기술적 보호조치 의무사항 고려
	신용정보의 이용 및 보호에 관한 법률	개인의 신용정보를 취급하는 금융회사(보험, 캐피탈, 카드사 등)를 대상으로, 신용정보의 취급 단계별 보호조치 의무사항 고려
	위치정보보호에 관한 법률	위치정보를 취급하는 사업자 및 공공기관 등은 수집, 이용, 파기 등에 대한 보호조치 의무사항을 고려
	개인정보보호법	일반법으로서 개인정보를 처리하는 모든 개인, 사업자, 공공기관 등에 대한 개인정보의 취급단계별 보호조치 및 정보주체의 권리 보장사항 고려

o 법적 준거성을 점검하기 위한 체크리스트는 최신 법규 사항을 반영하고 있어야 한다.

- 체크리스트를 통해 조직의 정책 및 정책시행 문서 등에 최신 법적 요구사항이 반영되어 있는 지 확인하여야 한다.

4.6.2 정보보호 관리체계 운영현황 관리

o 사후관리 단계(정보보호 관리체계 운영현황 관리)의 요구사항은 다음과 같다.

관리과정		세부관리과정	관리과정 상세내용
사후관리	5.2	정보보호 관리체계 운영현황 관리	정보보호 관리체계 범위 내에서 주기적 또는 상시적으로 수행해야 하는 활동을 문서화하고 그 운영현황을 지속적으로 관리하여야 한다.

< 수행업무의 문서화 >

o 정보보호 관리체계의 안정적 운영을 위해 필요한 수행업무를 목록화하여 문서화하고 그 운영현황과 이행여부를 지속적으로 관리하여야 한다.

o 정보보호 관리체계 운영활동을 식별하여 수행 주기, 수행 주체(담당부서, 담당자)를 정의한 운영현황표를 관리하고 최신성을 유지하여야 한다.

< 운영현황 관리 >

o 정보보호 관리체계 내 정보보호 활동을 효과적으로 운영하고 조직의 정보보호 목적을 달성하고 있는 지 여부를 확인하기 위하여 운영현황을 주기적으로 검토하여야 한다.

4.6.3 내부감사

o 사후관리 단계(내부감사)의 요구사항은 다음과 같다.

관리과정		세부관리과정	관리과정 상세내용
사후관리	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.

< 내부감사 수행 >

o 법적 요구사항 및 조직 내 수립된 정보보호정책에 따라 정보보호 관리체계 활동이 효과적으로 수행되는 지 여부를 검토하기 위한 지침을 수립하여야 한다.

- 지침에 내부감사 기준, 범위, 수행 주기, 감사인력 자격요건 등을 정의하여야 한다.

- 감사인력의 자격요건에서 감사의 객관성을 확보하기 위하여 독립적인 제3자가 감사를 수행하는 것이 원칙이나 불가피한 경우 제3자 인력을 포함하여 정보보호조직이 감사를 수행할 수 있다.

o 내부감사 지침에 따라 연 1회 이상 감사를 수행할 수 있도록 연간 계획을 수립하여야 한다.

- 연간 계획 수립 후 정보보호 최고책임자 등 경영진에게 보고하여 승인을 득한 후 계획에 따라 내부감사를 수행하여야 한다.

- 내부감사 수행기간, 중점 감사 분야 및 부서, 수행 감사 조직 구성, 감사에 필요한 체크리스트 등과 같은 세부적인 사항은 감사 수행 시점에서 감사 책임자가 결정하여 실행할 수 있다.

< 결과보고 >

o 내부감사 중 지적사항이 발견된 경우 일정 기간 동안 피감사 부서 혹은 담당자가 대책을 마련하여 보완하게끔 한 후 보완조치여부를 확인하여야 한다.

o 감사 수행 및 보완조치 완료 후 감사결과 보고서를 작성하여 정보보호 최고책임자 등 경영진 등에게 보고하여야 한다.

- 보고서에는 일정 및 범위, 감사 내용(감사 방법, 검토 문서, 면담자 등), 지적사항 및 보완조치 내용(보완조치 완료 여부, 대책 등) 등을 포함하여야 한다.

o 보고서는 발견사항, 결론과 권고사항, 그리고 감사인이 감사에 관련해서 갖고 있는 보류사항이나 한정사항을 기술해야 한다.

- 감사에 필요한 자료 중 특정 부문에 해당하는 자료를 감사 기간 내에 확보하지 못해 의견을 제출할 수 없는 경우, 또는 특정 시스템에 대해서만 감사를 수행하여 다른 시스템에 대해서는 이 감사 결과를 적용할 수 없는 경우에는 해당 사항들을 기술해야 한다.

4.7 운영 단계

4.7.1 운영 절차

o 정보보호 관리체계 구축이 완료되었으면 정보보호대책의 통제항목을 운영해야 한다.

- 정보보호대책은 총 13개 분야 92개 통제항목으로 구성되어 있다.

- 통제항목 중 정보보호대책 선택 시 선택하지 않은 항목은 식별되어 그 사유를 정보보호대책서에 명시하여야 한다.

o 정보보호 관리체계가 효과적으로 구현되고 각종 정책 및 절차가 안정적으로 적용되어 운영되는지를 판단하기 위해서는 최소 2개월 이상 운영하여야 한다.

- 인증 신청을 위해서는 최소 2개월 이상 운영을 하여야 하며, 운영기간에 대한 증적 자료를 제출해야 한다.

관련근거
정보보호 관리체계 인증 등에 관한 고시 제15조(신청기관의 사전 준비사항) 신청기관은 정보보호 관리체계 인증을 신청하기 전에 인증기준에 따른 정보보호 관리체계를 구축하여 최소 2개월 이상 운영하여야 한다.

- 제출한 증적 자료가 허위임이 증명될 경우, 심사를 중단할 수 있으며 심사 순위의 최하위 배정, 심사 인건비 부담 등과 같은 불이익이 발생할 수 있다.

o 정보보호 관리체계를 운영함에 있어 정보보호관리과정, 정보보호대책을 바탕으로 정책, 시행문서, 운영 증적 자료, 운영현황표 등을 문서화해야 한다.

- 이는 짧은 인증심사 기간 동안에 전반적인 정보보호 관리체계의 운영 현황과 적절성을 신뢰할 수 있도록 하기 위한 것이다. 문서화를 통해 전반적인 정보보호 관리체계 운영의 적정성과 현황을 확인할 수 있다.

[부록] 정보보호 관리체계(ISMS) 인증 관련 주요 문서 및 법령

□ 인증 신청 제출 서류 및 작성 방법

[붙임 1] 정보보호 관리체계 인증신청서
[붙임 2] 정보보호 관리체계 명세서

□ 인증 심사 관련 문서

[붙임 3] 사전점검(심사) 체크리스트
[붙임 4] 보완조치 요청서
[붙임 5] 결함보고서
[붙임 6] 보완조치 내역서

□ 인증 관련 법령

[붙임 7] 정보보호 관리체계 인증 등에 관한 고시 전문
[붙임 8] ISMS 인증 관련 정보통신망법-시행령-하위고시(3단비교표)
[붙임 9] 인증 기준 세부점검항목

< 인증 신청 제출 서류 >

1. 정보보호 관리체계 인증신청서

2. 정보보호 관리체계 명세서
   - 정보보호 관리체계의 범위
   - 주요 정보통신 설비의 목록과 시스템 구성도
   - 정보보호 관리체계 수립·운영 방법 및 절차
   - 정보보호 관리체계 관련 주요 문서 목록
   - 국내외 품질경영체제 인증서 취득 명세
   - [별지] 정보보호 관리체계 대책명세서 양식

3. 법인사업자등록증

[붙임 1] 정보보호 관리체계 인증신청서

■「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	*※ 종업원의 수 : 내부 및 외주 인력의 합산*
정보보호 관리체계의 범위에 포함되어 있는 서버의 수	*※ 서버(웹서버, DB서버 등), 네트워크 장비(라우터, L4이상 스위치 등), 보안장비(방화벽, IDS, IPS, DDos 대응시스템, 웹방화벽 등)을 포함하여 산정*

「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 관리체계 명세서 1부.	수수료 없음
담당공무원 확인사항	법인사업자등록증	

210㎜×297㎜[백상지(80g/㎡)]

[붙임 2] 정보보호 관리체계 명세서

정보보호 관리체계 명세서	
☐ 정보보호 관리체계 ☐ 개인정보보호 관리체계	
작성 항목	**기재 내용(요약)**
1. 정보보호 관리체계의 범위	※ 인증을 받고자하는 주요 서비스 명과 정의 등을 기재
2. 정보보호 관리체계의 범위에 포함되어 있는 주요 정보통신설비의 목록과 시스템 구성도	※ 인증범위 대상과 제외 대상을 적시하고 그 사유를 기재
3. 정보보호 관리체계를 수립·운영하는 방법과 절차	※ 정보보호 관리체계 운영현황, 자산식별 기준, 취약점 점검 등에 관한 내용을 기재
4. 정보보호 관리체계와 관련된 주요 문서의 목록	※ 정보보호 관리체계 관련 주요 문서 목록을 기재
5. 정보보호 관리체계와 관련된 국내외 품질경영체제의 인증을 취득한 경우에는 그 명세	※ 현재 국내외 품질경영체계 인증을 취득하였을 경우, 인증서 명, 인증기관, 취득일 등을 기재

※ 위 표에는 주요 내용만을 기재하고, 세부 사항은 이후 페이지부터 기재

Ⅰ 정보보호 관리체계의 범위(시행령 제47조제1항제1호)

☐ **주요 서비스(사업) 현황 (인증심사 희망일 : 2013.00.00 ~ 2013.00.00)**

※ 여러 신청기관이 같은 날짜에 심사를 희망할 경우, 실제 인증심사일이 희망하는 날짜와 다를 수 있음

① 현재 제공 중인 주요 서비스 (인증범위 외 서비스 포함)

☞ *인증범위 포함여부와 상관없이 기업이 제공하는 주요 서비스를 모두 기술*

② 인증을 받고자 하는 서비스

서비스명	*예) 포털 서비스, 통합정보관리서비스 등*		
인증희망 이유	☞ *법적요구, 고객요구, 내부 정책 등 고려사항을 기술*	**의무대상자 여부(Y/N)**	
이용자(고객)	☞ *개인(내국인, 외국인), 법인 등*	**이용자 수**	_____명
서비스 설명	☞ *각 서비스 별 상세 설명*		
홈페이지	☞ *홈페이지 및 관련 서비스 웹페이지 URL 기술*		
관련 외주업체 활용현황	☞ *위탁, 용역 수행업체 및 투입인력(xx명, 파견) 등 현황 기술* ☞ *서비스 관련 개발이나 운영 등을 위해 활용되는 외주업체 현황을 기술*		
기타	☞ *특이사항 기술*		

③ 종업원 수 및 사업장 위치

전체 종업원 수	xxx명(외주인력 포함)	인증범위 내 종업원 수	xxx명(외주인력 포함)
사업장 위치	*사업장명*	*위치*	
	사업장명	*위치*	
	사업장명	*위치*	

④ 기업 전체 조직도 및 정보보호 조직도

전체 조직도

☞ *인증 범위에 상관없이 기업 전체 조직도에 인증 범위에 해당하는 부서 표시, 부서별로 사업장 위치 등이 상이할 경우 상세 내용 기술*

정보보호 조직도

☞ *정보보호 관련 부서, 정보보호최고책임자, 정보보호책임자, 정보보호실무자 등을 표기*

II 주요 정보통신 설비의 목록과 시스템 구성도(시행령 제47조제1항제2호)

□ 인증범위 대상

o 운영기간 : ___년 ___개월 (○○○○년 ○월 ~ ○○○○년 ○월)

o 대상 부서(인력)

구분	부서명 (업체명)	업 무	규모
내부 인력	*네트워크 관리팀*	*네트워크 장비 및 보안장비 운영*	xxx명
	…	…	
	…	…	
외부 인력	*참조아라시스템즈*	*시스템유지보수 용역*	xxx명
	…	…	
	…	…	

o 자산 현황 요약 (서비스별 분류)

서비스	구분	자산명	수량	용도	자산 위치	관리 부서
원격교육 시스템	서버					
	네트워크					
	보안장비					
	PC					
	…					
	…					
…						

< 작성 時 주요 착안사항 >

※ 정보자산 현황은 정보자산 규모를 확인하고 수수료 산정 시 활용하기 위한 것임
※ 종류는 신청기관의 자산 분류기준에 따른 자산 유형과 일치해야 함

o 제외 부서·시스템 목록 및 사유

구분	부서명(시스템구분)	대상 제외 사유	규모
부서(인력)	*○○○팀*		xxx명
	…		
시스템	*서버*		xxx대
	…		

□ 시스템 및 네트워크 구성도

< 작성 時 주요 착안사항 >

※ 인증범위 서비스를 운영하는 시스템을 중심으로 시스템 구성도 제출 시 다음사항이 포함되도록 한다.
- o DB 서버, 웹서버, 로그 모니터링 시스템 등
- o IDC가 구분된 경우 해당 사항을 명시
- o 시스템간의 네트워크 연결을 간략히 명시

※ 인증범위 서비스를 연결하는 네트워크 구성도 제출 시 다음사항이 포함되도록 한다.
- o 네트워크 장비(예. 라우터, 스위치 등)
- o 정보보호 관련 장비 (예. 방화벽, 침입탐지 시스템, 침입방지 시스템 등)
- o DMZ 구역, VPN 구간 등 (해당시)

Ⅲ 정보보호 관리체계 수립·운영 방법 및 절차(시행령 제47조제1항제3호)

□ 정보보호 규모 및 체계

o 정보보호 인력 및 예산 규모

- 정보보호 인력

(단위 : 명)

총 인력	IT 인력	정보보호 인력
명	명	명

- 정보보호 예산

(단위 : %)

전체예산 대비 IT 예산	IT예산 대비 정보보호 예산
%	%

o 홈페이지 등을 통한 정보보호 활동 내역 공개 여부(Y/N) :

o 의사결정체계

※ 정보보호관련 정책 승인 또는 정보보호활동에 대한 의사결정체계를 도식화

□ 정보보호 관리체계 운영현황

o 주요 정보보호 활동 목록(구축 운영 순서대로 작성)

주요 활동	주기	담당자 (부서/성함)	실시유무 (O/X)	최근 실시
정보보호정책수립	*1회/3년*	*홍길동/보안관리팀*	*O*	*2012.12월*
백업훈련	*1회/1년*	*홍길동/보안관리팀*	*O*	*2013.1월*
…				

< 작성 時 주요 착안사항 >

※ 정보보호 관리체계를 지속적으로 운영하기 위해서 주기적 또는 상시적으로 수행하는 정보보호 활동을 목록화하여 기재(주기, 담당자, 실시유무 등)

o 2개월 이상 구축·운영 증빙자료

※ 증빙할 수 있는 승인문서, 계약서 등의 스캔 이미지 첨부
※ 문서명, 기관명, 주요내용 등이 포함되어야 하나, 모든 증빙자료 또는 증빙자료의 모두를 첨부할 필요는 없음

< 작성 時 주요 착안사항 >

※ 인증신청 2개월 전 운영날짜가 확인 가능한 관리적, 기술적 항목에 대한 운영증적(산출물) 1건씩 첨부 예)정보보호정책 또는 위험평가 승인문서, 백업정책 승인 문서 등
※ 컨설팅을 받은 경우, 인증신청 2개월 이전의 계약서 또는 결과보고서 사본
예) 결과보고서 승인 문서, 컨설팅계약서

o 심사항목 및 대책명세서 (아래 3개 중 해당하는 1개만 기재하시고 나머지는 삭제)

- 정보보호 관리체계(ISMS) 심사 항목(개정된 現기준 적용 時)

심사 영역		운영 현황		비고
		통제 항목	선택(심사) 항목	
관리과정(필수)		12	12 (필수)	
정보보호대책 (13개 분야)	1	6		
	2	4		
	3	3		
	4	3		
	5	4		
	6	5		
	7	9		
	8	10		
	9	2		
	10	14		
	11	22		
	12	7		
	13	3		
	계	92		
합계		104		

※ 상세 내용은 [별지1](p.97)에 기재

- 정보보호 관리체계(ISMS) 심사 항목(개정 전 舊기준 적용 時)

심사 영역		운영 현황		비고
		통제 항목	선택(심사) 항목	
관리과정(필수)		14	14 (필수)	
문서화(필수)		3	3 (필수)	
정보보호대책 (15개 분야)	1	5		
	2	4		
	3	4		
	4	4		
	5	4		
	6	5		
	7	12		
	8	13		
	9	3		
	10	14		
	11	22		
	12	5		
	13	7		
	14	11		
	15	7		
	계	120		
합계		137		

※ 상세 내용은 [별지2](p.109)에 기재
※ 개정 전 舊기준은 2013년 한시적으로 적용하고, 2014년부터는 개정된 現기준으로만 적용

- 개인정보보호 관리체계(PIMS) 심사 항목

심사 영역		운영 현황		비고
		통제 항목	선택(심사) 항목	
관리과정(필수)		13	13 (필수)	
보호대책 (8개 분야)	1	6		
	2	6		
	3	2		
	4	4		
	5	4		
	6	7		
	7	42		
	8	8		
	계	79		
생명주기(필수)		32	32 (필수)	
합계		124		

※ 상세 내용은 [별지3](p.126)에 기재

□ 위험 관리

o 자산분류 기준
※ 자산을 분류한 유형을 기재. 예) S/W, 서버, 네트워크, 시설, 인력 등

o 자산 중요도 산정방법
※ 자산 중요도 산정기준, 자산 등급 선정 계산방법 등을 기재 (자산 중요도 산정기준은 자산분류별로 상이할 수 있음)

o 위험평가 방법론
- 관리적, 기술적, 법적 위험 식별 방법

구분	방법	산출물
관리적 위험	*예) 베이스라인 접근법(체크리스트)*	*예) 분석결과*
기술적 위험	*예) 상세위험분석 방법*	
법적 위험	*예) 베이스라인 접근(체크리스트)*	

- 위험평가를 위한 위험도 산정기준

- 수용 가능한 위험수준(DoA) 선정 방법
예) 실무자 협의, CISO 최종 승인

o 위험관리 계획
※ 위험관리를 수행하기 위하여 인력 구성, 기간(단계별 구분), 대상, 방법, 예산 등을 구체화하여 기재

□ 기술적 취약점 점검

o 취약점 점검 대상 선정방법 및 그 사유
※ 정보자산 중 취약점 점검으로 선정한 방법 및 그 사유를 기재

o 취약점 점검 현황

기간 (○.○월~○월)	대상 서비스	대상 자산 및 규모		점검툴	취약점건수 (점검시)	잔여취약점 (현재)
5개월 (2012.7월~11월)	*웹서비스*	서버	대		건	건
		네트워크장비	대		건	건
		보안장비	대		건	건
		PC	대		건	건
		S/W	대		건	건
		…	…		…	…
…						

< 작성 時 주요 착안사항 >

※ 최근 3년간 외부 정보보호 컨설팅업체를 통하여 취약점 점검을 받은 내용을 기재
※ 취약점 발견 건수 : 취약점 점검 당시 발견된 취약점 건수
※ 잔여 취약점(현재) : 당시 발견한 취약점이 보완되지 않고 남아 있는 건수

□ ISMS 구축·운영 관련 외부업체 현황(최근 3년간)

※ ISMS를 구축 운영하기 위해 외부업체로부터 관련자문, 기술지원 등을 받은 현황을 모두 기재
(ISMS 인증범위에 포함되어 있는 외주업체 포함)

※ ISMS 신청기관과 이해관계가 없는 심사원을 선정하기 위함이며,
신청기관이 이해관계가 있는 업체 현황을 기재하지 않을 경우 인증심사에 차질이 발생할 수 있음

분류	외부업체명	기간	내용
ISMS 구축 컨설팅			
보안취약점 점검			
보안관제			
시스템유지보수			
출입관리 및 경비			
OOO 시스템 개발			
…			

□ 기업이 준수해야 할 법적 요구사항 현황

구분	관련 법적 요구사항	비 고
예) 데이터센터 운영 서비스	*예) 정보통신망법 제46조, 제47조 …*	
	예) 집적정보 통신시설 보호지침	
	…	
…		

< 작성 時 주요 착안사항 >

※ 국내·외 법규에 의거하여 신청기관이 의무로 시행하는 서비스를 기재

□ 내부감사 이력

No.	기간 (년.월.일~월.일)	수행 인력			감사결과 및 조치사항
		부서 (또는 외주업체명)	성명	수행업무	
1	*3개월 (2012.2.1일 ~2012.4.30일)*	*보안관리팀*	*홍길동*	*시스템개발 보안 점검*	…
		(조아컨설팅)	*아무개*	*보안취약점 점검*	…
		…	…	…	…
…	…	…	…	…	…

Ⅳ 정보보호 관리체계 관련 주요 문서 목록(시행령 제47조제1항제4호)

구분	문 서 명	관리 번호	주요 내용	제개정 주체 (부서/성명)
정책	*정보보호정책*			
	개인정보보호정책			
	...			
지침	*정보보호조직관리지침*			
	자산분류 및 관리지침			
	정보보호정책관리지침			
	서버보안관리지침			
	PC보안관리지침			
	사업연속성계획관리지침			
	아웃소싱보안지침			
	...			
절차	*보안성검토절차*			
	문서보안관리절차			
	침해사고대응절차			
	서버보안관리절차			
	PC보안관리절차			
	백업관리절차			
	암호관리절차			
	...			
기록 및 로그	*임직원 보안서약서*			
	출입 관리대장			
	정보보호 대책 명세서			
	...			

※ 신청기관이 보유한 정보보호 관리체계 관련 문서 및 기록을 최대한 기재

※ 위 표 "문서 명"은 단지 예시이며 해당 문서 명으로 존재해야 한다는 의미는 아님

Ⅴ 국내외 품질경영체제 인증서 취득 명세 (시행령 제47조제1항제5호)

인증 항목	예) ISO27001, BS7799, BS10012 등 ※ 1개 인증 항목 당, 개별 page를 할애하여 작성 요망		
인증 기관		**취득 일시**	**년 월 일**
인증 번호			
인증 목적	※ 해당 인증을 받은 목적에 대해 기술		
인증 범위	※ 인증을 받은 범위에 대해 자유롭게 기술 (보호 자산이 명확하게 드러나도록 기술)		
인증 혜택	※ 인증을 받은 후 혜택 사항(세금 감면, 우선 입찰 선정 등)		
인증 결과	※ 인증 전과 비교하여 개선된 사항(긍정적인 내부 변화 등)		
비고			

[별지1] 정보보호 관리체계 대책명세서 양식A(신청기관이 개정된 現기준으로 정보보호 관리체계를 수립·운영한 경우)

1. 정보보호관리과정

< 작성 時 주요 착안 사항 >

정보보호관리과정은 필수적인 항목으로 해당 인증기준을 모두 선택하여야 한다. 운영여부와 운영내용을 확인할 수 있도록 다음 항목을 상세히 작성하여야 한다. 항목별 설명은 다음과 같다.

o 상세내용 : 신청기관 참고사항. 각 통제항목별로 의미하는 바를 기재하였음 (운영현황 등의 작성 공란이 부족할 경우 상세내용 삭제)

o 수립여부 : 정보보호관리과정은 필수적으로 수립 및 구축해야 하므로 자가진단을 통해 Y/N으로 수립 및 구축을 확인

o 운영현황 : 각 인증기준의 요구사항에 대해 어떻게 대응한 것인지 작성하는 것으로 누가, 언제, 무엇을, 어떻게 적용하고 있는지 상세히 작성

o 관련문서 : 인증기준을 만족하는 내용이 포함되어있는 기관의 문서 제목을 작성하되 문서 내 부분에 해당할 경우 장, 절, 조 등을 표시. 문서번호가 있다면 문서번호도 표시

o 기록(증적자료) : 인증기준을 만족하는 내용이 포함되어있는 기관의 기록(증적자료) 제목 및 번호를 작성

통제항목		상세내용	수립 여부	운영현황	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
1. 정보보호정책수립 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.				

통제항목		상세내용	수립 여부	운영현황	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
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.				
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.				

2. 정보보호대책

< 작성 時 주요 착안 사항 >

정보보호 대책은 기업의 정보보호 운영현황에 따라 선택할 수 있다. 선택하지 않은 통제항목의 경우 미선택 사유를 작성하여야 한다. 선택한 경우에는 선택이유 및 구현내용을 확인할 수 있도록 선택사유, 적용내용, 관련문서, 기록(증적자료)을 상세히 작성하여야 한다.

o 상세내용 : 신청기관 참고사항. 각 통제항목별로 의미하는 바를 기재하였음 (운영현황 등의 작성 공란이 부족할 경우 상세내용 삭제)

o 선택여부 : 정보보호 대책의 선택여부에 대해 Y(Yes) / N(No)로 표시 (N은 해당통제사항이 기업의 운영환경 상 적용되지 않는 경우에 선택)

o 운영현황(또는 미선택사유) : 해당 통제사항에 대한 구축 및 실제 운영내용을 요약하여 작성하되 구축의 특성 및 정당성을 파악할 수 있도록 인증기준보다 상세히 작성. 통제사항을 선택하지 않은 경우 위험관리(위험평가 및 처리)의 결과 및 분석에 따른 미선택의 사유를 반드시 작성.

o 관련문서(정책 또는 매뉴얼) : 인증기준을 만족하는 내용이 포함되어있는 기관의 문서(정책, 규정, 지침, 절차, 매뉴얼 등)의 제목을 작성하되 문서 내 부분에 해당할 경우 장, 절, 조 등을 상세하게 표시. 선택하지 않을 경우, 해당 근거를 확인할 수 있는 문서 및 문서 내 부분을 작성. 문서번호가 있다면 문서번호도 표시.

o 기록(증적자료) : 인증기준을 만족하는 내용이 포함되어있는 기관의 운영기록(증적자료)의 제목(파일명) 및 번호를 작성. 통제사항에 관련된 위험분석결과, 계획, 취약점분석관련 자료도 기록하여 대책명세서를 통해 관련내용을 확인할 수 있도록 함. 관련증적이 시스템으로 관리되는 경우 해당 시스템 위치, 시스템명 및 관련 메뉴를 작성.

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
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						

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
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.				
2.1.2	**실무조직 구성**	최고경영자는 정보보호 최고책임자의 역할을 지원하고 조직의 정보보호활동을 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 계약만료, 업무종료, 담당자변경 시 조직이 외부자에게 제공한 정보자산의 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 업무 수행 시 알게 된 정보의 비밀유지확약서 등의 내용을 확인하여야 한다.				
4 정보자산 분류						

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
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	**교육계획**	교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 정보보호교육 계획을 수립하여야 한다.				
5.1.2	**교육대상**	교육 대상에는 정보보호 관리체계 범위 내 임직원 및 외부자를 모두 포함하여야 한다.				
5.1.3	**교육내용 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.				
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 인적자원 부족 등 불가피하게 직무분리가 어려운 경우 별도의 보완통제를 마련하여야 한다.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
6.1.3	**비밀유지서약서**	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.				
7 물리적 보안						
7.1 물리적 보호구역						
7.1.1	**보호구역지정**	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.				
7.3 사무실 보안						

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
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.				
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	시험데이터 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 외주개발보안						

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
8.3.1	외주개발보안	정보시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리.감독하여야 한다.				
9 암호통제						
9.1 암호 정책						
9.1.1	암호 정책 수립	조직의 중요정보 보호를 위하여 암호화 대상, 암호 강도(복잡도), 키관리, 암호사용에 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. 접근통제						
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.				
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.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
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 접근통제리스트, 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.				
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 운영절차 및 변경관리						
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.				
11.2 시스템 및 서비스 운영보안						

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
11.2.1	정보시스템 인수	새로운 정보시스템 도입 또는 개선 시 필수 보안요구사항을 포함한 인수 기준을 수립하고 인수 전 기준 적합성을 검토하여야 한다.				
11.2.2	보안시스템 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	원격운영관리	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	스마트워크 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.				
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						

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
11.4.1	정보시스템 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.				
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	시각동기화	로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 정보시스템 시각을 공식 표준시각으로 정확하게 동기화 하여야 한다.				
11.6.2	로그기록 및 보존	정보시스템, 응용프로그램, 보안시스템, 네트워크 장비 등 기록해야 할 로그유형을 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 모니터링 하기 위한 체계 및 절차를 수립하여야 한다.				
12. 침해사고 관리						
12.1 절차 및 체계						
12.1.1	침해사고대응 절차 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.				
12.2.2	침해사고 보고	침해사고 징후 또는 사고 발생을 인지한 때에는 침해사고 유형별 보고절차에 따라 신속히 보고하고 법적 통지 및 신고 의무를 준수하여야 한다.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
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.				

[별지2] 정보보호 관리체계 대책명세서 양식B(신청기관이 개정 전 舊기준으로 정보보호 관리체계를 수립·운영한 경우)

1. 정보보호관리과정

< 작성 時 주요 착안 사항 >

정보보호관리과정은 필수적인 항목으로 해당 인증기준을 모두 선택하여야 한다. 운영여부와 운영내용을 확인할 수 있도록 다음 항목을 상세히 작성하여야 한다. 항목별 설명은 다음과 같다

o 상세내용 : 신청기관 참고사항. 각 통제항목별로 의미하는 바를 기재하였음 (운영현황 등의 작성 공란이 부족할 경우 상세내용 삭제)

o 수립여부 : 정보보호관리과정은 필수적으로 수립 및 구축해야 하므로 자가진단을 통해 Y/N으로 수립 및 구축을 확인

o 운영현황 : 각 인증기준의 요구사항에 대해 어떻게 대응한 것인지 작성하는 것으로 누가, 언제, 무엇을, 어떻게 적용하고 있는지 상세히 작성

o 관련문서 : 인증기준을 만족하는 내용이 포함되어있는 기관의 문서 제목을 작성하되 문서 내 부분에 해당할 경우 장, 절, 조 등을 표시. 문서번호가 있다면 문서번호도 표시

o 기록(증적자료) : 인증기준을 만족하는 내용이 포함되어있는 기관의 기록(증적자료) 제목 및 번호를 작성

통제항목		상세내용	수립 여부	운영현황	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
1. 정보보호 정책 수립						
1.1	**정보보호 정책의 수립**	신청기관의 경영목표를 지원할 수 있도록 정보보호의 법적, 규제적 요건과, 전략적이고 조직적인 위험관리를 기술한 정보보호정책을 수립하여야 한다.				
1.2	**조직 및 책임 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. 관리체계 범위설정						
2.1	**정보보호 관리체계 범위 설정**	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						

통제항목		상세내용	수립 여부	운영현황	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
3.1	**위험관리 전략 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.				
3.2	**위험분석**	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 우선 순위의 확보를 지원하여야 한다.				
3.4	**정보보호 대책 수립**	신청기관의 정보보호정책과 목적에 부합하도록 위험을 수용 가능한 수준으로 감소시키기 위해, 위험분석 및 평가에 의거하여, 위험처리, 위험수용, 위험회피, 위험전가 등의 전략을 설정하고, 기준에서 제시하는 통제사항을 선택한다. 기준에서 제시되지 않은 통제사항을 추가할 경우에는, 정보보호관리과정의 각 단계간 일관성을 유지하도록 한다. 정보보호대책의 선택은 비용·효과 분석에 의해 정당화될 필요가 있다.				
3.5	**정보보호 계획 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.				
4. 구현						
4.1	**정보보호 대책의 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	**정보보호 관리체계의 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.				

통제항목		상세내용	수립 여부	운영현황	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
5.2	정보보호 관리체계의 모니터링 및 개선	정보보호관리체계가 신청기관의 정보보호정책과 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 결과 보고, 기록 유지 및 이행 모니터링에 대한 책임과 요구사항을 문서화된 절차에 의해 규정하여야 한다. 피감사분야의 관리자는 발견된 보완조치 사항을 처리하고, 검증・보고됨을 보장하여야 한다.				

2. 문서화

< 작성 時 주요 착안 사항 >

작성 방법은 "1. 정보보호관리과정"과 동일

통제항목	상세내용	수립 여부	운영현황	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
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.				

3. 정보보호대책

< 작성 時 주요 착안 사항 >

정보보호 대책은 기업의 정보보호 운영현황에 따라 선택할 수 있다. 선택하지 않은 통제항목의 경우 미선택 사유를 작성하여야 한다. 선택한 경우에는 선택이유 및 구현내용을 확인할 수 있도록 선택사유, 적용내용, 관련문서, 기록(증적자료)을 상세히 작성하여야 한다.

o 상세내용 : 신청기관 참고사항. 각 통제항목별로 의미하는 바를 기재하였음 (운영현황 등의 작성 공란이 부족할 경우 상세내용 삭제)

o 선택여부 : 정보보호 대책의 선택여부에 대해 Y(Yes) / N(No)로 표시 (N은 해당통제사항이 기업의 운영환경 상 적용되지 않는 경우에 선택)

o 운영현황(또는 미선택사유) : 해당 통제사항에 대한 구축 및 실제 운영내용을 요약하여 작성하되 구축의 특성 및 정당성을 파악할 수 있도록 인증기준보다 상세히 작성. 통제사항을 선택하지 않은 경우 위험관리(위험평가 및 처리)의 결과 및 분석에 따른 미선택의 사유를 반드시 작성.

o 관련문서(정책 또는 매뉴얼) : 인증기준을 만족하는 내용이 포함되어있는 기관의 문서(정책, 규정, 지침, 절차, 매뉴얼 등)의 제목을 작성하되 문서 내 부분에 해당할 경우 장, 절, 조 등을 상세하게 표시. 선택하지 않을 경우, 해당 근거를 확인할 수 있는 문서 및 문서 내 부분을 작성. 문서번호가 있다면 문서번호도 표시

o 기록(증적자료) : 인증기준을 만족하는 내용이 포함되어있는 기관의 운영기록(증적자료)의 제목(파일명) 및 번호를 작성. 통제사항에 관련된 위험분석결과, 계획, 취약점분석관련 자료도 기록하여 대책명세서를 통해 관련내용을 확인할 수 있도록 함. 관련증적이 시스템으로 관리되는 경우 해당 시스템 위치, 시스템명 및 관련 메뉴를 작성.

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
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						

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
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 조직의체계						
2.1.1	**조직의 구성**	신청기관내 정보보호관리 활동을 계획, 관리하는 정보보호관리자가 있어야 하며, 필요에 따라 정보보호위원회를 구성할 수 있다.				
2.1.2	**외부의 전문가 활용**	정보보호정책 수립, 위험분석·평가, 통제사항의 선택과 구현, 보안사고 대응 등 중요한 정보보호관리 활동에 도움을 받기 위하여 외부 전문가의 조언을 받을 수 있다.				
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	**외부위탁 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.				
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.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
4 정보자산분류						
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 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.				
5. 정보보호 교육 및 훈련						
5.1 교육 및 훈련 프로그램 수립						
5.1.1	**교육 및 훈련 계획**	정보보호 인식제고 및 실제 운영에 필요한 교육·훈련 계획을 종합적으로 수립하여 이행하여야 한다				
5.1.2	**교육 및 훈련 대상**	교육 및 훈련의 대상에는 신청기관의 임직원 및 관련 외부자를 포함하여야 한다.				
5.1.3	**교육 및 훈련 내용**	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. 인적보안						
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.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
6.1.2	**인사규정**	인사규정에는 정보보호에 대하여 직원이 지켜야 할 책임 및 관련 법규상의 책임을 명시하여야 한다. 특히, 정보보호업무를 담당하는 자와 정보시스템 사용자 및 관리자에 대해서는 보다 명확한 책임을 명시하여야 하며, 직원이 책임을 이행하지 않는 경우를 대비한 적절한 처벌규정을 포함하여야 한다.				
6.2 적격심사 및 주요 직무담당자 관리						
6.2.1	**적격심사**	계약직 및 임시직원은 물론 정식직원 채용 시 신원, 업무능력, 교육정도, 경력 등에 대한 적격심사가 이루어져야 한다. 직원들이 용역회사를 통하여 충원되는 경우에는 용역회사와의 계약서에 적격심사에 따르는 책임사항을 명문화하여야 한다.				
6.2.2	**주요직무담당자 관리**	정보시스템 접근 권한을 포함하는 업무가 새로이 할당될 때, 특히 재무정보나 비밀정보와 같이 중요한 정보를 처리하는 담당자에 대해서는 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 보안 대책						
7.1.1	**물리적 보호 구역**	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 접근 통제**	보호구역을 출입하는 자를 감시·통제하고 권한 없는 자의 출입을 방지하기 위하여 수립된 보안 절차에 따라 필요한 조치를 수행하고 주기적으로 검토하여야 한다.				
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 기록대장은 정기적으로 점검하여야 한다.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
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 유지·보수를 하여야 하고 유지·보수에 대한 기록을 남겨야 한다.				
7.3.6	장비의 안전한 폐기 및 사용	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 개발 보안						
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.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
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.				
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				
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.				
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.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
8.3.3	소프트웨어 패키지 변경	소프트웨어 패키지는 가능한 수정하지 않고 사용하고, 패키지 변경 시에는 공급자의 동의를 얻으며, 수정이 가능한지 확인하여야 한다. 모든 변경사항은 시험하고 문서화하여야 한다.				
9. 암호통제						
9.1	암호정책	암호사용에 대한 정책을 수립하여야 한다.				
9.2	암호사용	암호 정책에 따른 암호 사용시 적절한 알고리즘의 유형, 신뢰성 및 키 길이를 결정하여야 한다.				
9.3	키관리	암호 키에 대한 관리지침, 절차 및 방법을 마련하고 필요시 복구 방안을 마련하여야 한다.				
10. 접근통제						
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	접근통제 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.				
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	특수 권한 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.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
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 접근 정책을 수립하고 이행하여야 한다.				
10.3.2	운영체제 접근	안전한 로그온 절차, 식별 및 인증관리, 필요시 터미널 자동확인 등을 포함하여 시스템의 운영체제 접근을 통제하여야 한다.				
10.3.3	응용 프로그램 접근	사용자 접근이 허가되지 않은 응용 프로그램의 기능들에 대한 정보제공을 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 운영절차와 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	직무분리	부주의에 의한 또는 고의적인 시스템 오용의 위험을 감소시키기 위해 직무를 분리하고, 직무 분리가 어려운 특수한 경우 별도의 관리 감독 대책을 수립하여야 한다.				
11.1.4	개발과 운영 환경의 분리	원칙적으로 개발, 테스트, 운영 환경을 분리하여야 한다. 또한 응용 프로그램을 개발환경으로부터 운영환경으로 이전하는 절차를 정의하고 문서화하여야 한다.				
11.1.5	외부 운영 설비의 관리	외부계약자가 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.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
11.2.2	시스템 인수	새로운 정보시스템의 설치 또는 업그레이드에 따른 인수기준을 수립하고, 시스템 구매 계약서에 반영하여야 한다. 또한 시스템은 이 기준에 의해 테스트 한 후 인수하여야 한다.				
11.2.3	성능관리	조직에서 요구되는 성능 요구사항을 충족시킬 수 있도록 성능관리를 수행하여야 한다.				
11.2.4	용량관리	조직에서 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	보안시스템 운영	보안시스템에 대해서는 그 유형별로 설치, 운영에 대한 절차를 수립하고, 절차이행을 주기적으로 검토하여야 한다.				
11.3 네트워크 운영						
11.3.1	네트워크 운영 대책	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 통해 접근통제를 수행하여야 하며, 필요시 침입탐지시스템 등을 활용하여 접근을 모니터링 하여야 한다.				
11.3.3	원격운영관리	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.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
11.4.3	시스템 문서의 보안	보안절차, 운영매뉴얼, 운영기록 등 중요 시스템 문서들은 안전하게 보관하고 적절한 폐기절차에 따라 폐기하여야 한다.				
11.5	악성소프트웨어 통제	바이러스 등의 악성 소프트웨어로부터 시스템을 보호하기 위해 악성 소프트웨어들을 예방하고 탐지, 대응하는 대책을 수립하여야 한다.				
11.6 원격컴퓨터 및 원격작업						
11.6.1	이동컴퓨팅	휴대용 정보통신기기의 사용 시에 사업 정보를 보호하기 위한 보안정책을 수립하고, 내부 네트워크으로의 연결 및 공공 장소에서의 사용에 대한 정책을 수립하여야 한다.				
11.6.2	원격작업	재택 근무와 같은 원격 작업 수행시 이에 대한 물리적, 논리적 보호를 위한 정책과 절차를 마련하여야 한다.				
12. 전자거래보안						
12.1	교환합의서	조직간의 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	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 게시절차가 수립되어야 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 권고한다.				
13. 보안사고관리						
13.1 대응계획 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·시행하여야 한다.				
13.1.2	보안사고 대응체계 구축	보안사고의 대응이 신속하게 이루어질 수 있도록 중앙집중적인 대응체계를 구축하고, 대응체계에는 내부직원뿐 아니라 외부기관 및 전문가들과의 협조체계를 반영하여야 한다.				
13.2 대응 및 복구						

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
13.2.1	보안사고 대응교육 및 훈련	보안사고 대응 계획, 절차 및 방법에 대하여 정기적으로 교육을 실시하여야 하며 사고 처리 후 재발 방지를 위하여 필요한 교육·훈련을 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 수행하여야 한다.				
13.3 사후관리						
13.3.1	보안사고 분석 및 정보의 공유	보안사고가 처리되고 종결된후 이에 대한 분석이 수행되어야 하며, 그 결과가 보고되어야 한다. 또한 사고에 대한 정보와 발견된 취약성들이 관련조직과 인력에 공유되어야 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 변경도 이루어져야 한다.				
14. 검토, 모니터링 및 감사						
14.1 법적요구사항 준수검토						
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	준수검토	정보통신망이용촉진및 정보보호등에관한법률, 신용정보등의보호에관한법률 등의 개인정보보호 관련법 및 저작권법, 컴퓨터 프로그램보호법 등 지적재산권법 등의 관련 법규의 준수여부를 검토해야 한다.				
14.1.3	증거자료 수집	보안사고 처리 및 계약 증빙을 위하여 조직이나 개인에 대한 소송을 지원하기 위한 적정한 증거 자료를 확보하여야 한다.				
14.2 정보보호정책 및 대책 준수검토						
14.2.1	검토계획	검토의 대상, 주기, 방법, 범위, 절차, 검토자를 포함한 검토계획 및 정책이 수립되어야 한다. 이를 근거로 보안요구사항에 대한 통제와 책임의 준수에 대한 적정성이 검토되어야 한다.				
14.2.2	정책의 준수	모든 정보보호 정책, 절차의 준수여부를 검토하여야 한다.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
14.2.3	기술적 점검	정보시스템이 정보보호표준 및 절차에 따라 운영 관리되고 있는지 정기적으로 기술적 점검을 실시한다. 이에 따라 취약성들을 발견한 후 필요한 조치를 취한다.				
14.3 모니터링						
14.3.1	접근 및 사용 모니터링	사용자의 시스템 및 네트워크 사용 및 접근이 명확하게 허용된 범위 안에 있는지를 확인하기 위해 모니터링 절차를 수립하고 시행하여야 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	시각동기화	감사 기록의 명확성을 보장하고 법적인 자료나 징계 자료로서 효력을 갖기 위해서는 시스템 시각을 정확히 설정하여야 한다.				
14.4 보안감사						
14.4.1	보안감사계획 및 이행	보안 감사 대상, 범위, 주기, 방법, 절차, 감사자, 감사도구를 포함한 보안감사 계획을 수립하고 시행하여야 한다.				
14.4.2	감사결과 및 사후관리	감사의 결과에 따라 감사보고서를 작성하고 적정한 책임자에게 보고하며, 감사 지적 내용이 이행되도록 사후관리 하여야 한다.				
15. 업무연속성 관리						
15.1 업무연속성 관리 체계수립						
15.1.1	업무연속성 관리과정 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.				
15.1.2	업무연속성계획 프레임워크 수립	업무별 연속성 계획의 이행에 필요한 조건, 응급절차, 대체절차 등을 고려하여 연속성 계획들이 일관성을 유지할 수 있도록 프레임워크를 수립하여야 한다.				
15.2 업무연속성계획 수립과 구현						
15.2.1	업무영향분석	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.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
15.2.2	업무연속성계획 수립	업무복구목표 및 최소 요구사항을 구현하기 위한 여러 대안들을 평가하여 업무연속성을 위한 전략을 수립하고 대책 구현을 위한 계획을 수립하여야 한다.				
15.2.3	업무연속성계획 구현	업무연속성계획에서 수립한 위험감소 조치 및 재해복구를 위한 설비를 구현하며 필요한 계획 및 절차 등을 문서화하여야 한다.				
15.3 업무연속성계획 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 유지관리	업무연속성계획에 대해 정기적인 교육 및 훈련을 실시하고 지속적인 검토와 평가 및 변경관리를 수행하여야 한다.				

[별지3] 개인정보보호 관리체계 대책명세서 양식

1. 개인정보보호 관리과정

< 작성 時 주요 착안 사항 >

정보보호관리과정은 필수적인 항목으로 해당 인증기준을 모두 선택하여야 한다. 운영여부와 운영내용을 확인할 수 있도록 다음 항목을 상세히 작성하여야 한다. 항목별 설명은 다음과 같다

o 상세내용 : 신청기관 참고사항. 각 통제항목별로 의미하는 바를 기재하였음 (운영현황 등의 작성 공란이 부족할 경우 상세내용 삭제)

o 수립여부 : 정보보호관리과정은 필수적으로 수립 및 구축해야 하므로 자가진단을 통해 Y/N으로 수립 및 구축을 확인

o 운영현황 : 각 인증기준의 요구사항에 대해 어떻게 대응한 것인지 작성하는 것으로 누가, 언제, 무엇을, 어떻게 적용하고 있는지 상세히 작성

o 관련문서 : 인증기준을 만족하는 내용이 포함되어있는 기관의 문서 제목을 작성하되 문서 내 부분에 해당할 경우 장, 절, 조 등을 표시. 문서번호가 있다면 문서번호도 표시

o 기록(증적자료) : 인증기준을 만족하는 내용이 포함되어있는 기관의 기록(증적자료) 제목 및 번호를 작성

통제항목		상세내용	수립 여부	운영현황	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
1. 개인정보보호 정책수립 및 범위설정						
1.1	개인정보보호정책 수립	조직이 수행하는 모든 개인정보보호 활동의 근거를 포함할 수 있도록 개인정보보호정책을 수립하고 동 정책은 국가나 관련 산업에서 정하는 개인정보보호 관련 법, 규제를 만족하여야 한다.				
1.2	범위설정	조직에 미치는 영향을 고려하여 중요한 업무, 서비스, 조직, 자산 등을 포함할 수 있도록 개인정보보호 관리체계 범위를 설정하고 범위 내 모든 자산을 식별하여 문서화하여야 한다.				
1.3	개인정보 흐름 파악	조직의 개인정보 관련 서비스 및 업무에서 개인정보 흐름을 파악하여 개인정보 흐름도를 작성해야 한다. 개인정보 흐름도는 취급상의 변화 등을 반영하여 주기적으로 검토하고 최신성을 유지해야 한다.				
2. 경영진 책임 및 조직구성						
2.1	경영진 참여	개인정보보호 관리체계 수립 및 운영 등 조직이 수행하는 개인정보보호 활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여야 한다.				
2.2	개인정보보호	최고경영자는 조직의 규모, 업무 중요도 분석을 통해 개인정보보호 관리체계의				

통제항목		상세내용	수립 여부	운영현황	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
	조직 구성 및 자원 할당	지속적인 운영이 가능하도록 개인정보보호관리책임자(CPO), 실무조직 등 개인정보보호 조직을 구성하고 개인정보보호 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 개인정보보호 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	위험 식별 및 평가	위험관리 방법 및 계획에 따라 개인정보보호 전 영역에 대한 위험 식별 및 평가를 연 1회 이상 수행하고 그 결과에 따라 조직에서 수용 가능한 위험수준을 설정하여 관리하여야 한다.				
3.3	개인정보보호대책 선정 및 이행계획 수립	위험을 수용 가능한 수준으로 감소시키기 위해 개인정보보호대책을 선정하고 그 보호대책의 구현 우선순위, 일정, 담당부서 및 담당자 지정, 예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.				
4. 개인정보보호대책 구현						
4.1	개인정보보호대책의 효과적 구현	개인정보보호대책의 이행계획에 따라 대책을 구현하고 경영진은 이행결과의 정확성 및 효과성 여부를 확인하여야 한다.				
4.2	내부 공유 및 교육	구현된 개인정보보호 대책을 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여야 한다.				
5. 사후관리						
5.1	법적요구사항 준수검토	개인정보보호법, 위치정보보호법 등 조직이 준수해야 할 개인정보보호 관련 법적요구사항을 지속적으로 파악하여 최신성을 유지하고 준수여부를 지속적으로 검토하여야 한다.				
5.2	개인정보보호 관리체계 운영현황 관리	개인정보보호 관리체계 범위 내에서 주기적 또는 상시적으로 수행해야 하는 활동을 문서화하고 그 운영현황을 지속적으로 관리하여야 한다.				
5.3	내부감사	개인정보보호 관리체계 정책 및 법적 요구사항의 이행여부를 확인하기 위해 독립성 및 전문성을 확보할 수 있는 보안감사 조직의 구성, 감사 대상, 범위, 방법 등을 포함한 보안감사계획을 수립한다. 연 1회 이상 내부감사를 수행하고, 발견된 문제점은 보완조치를 완료하여 경영진 및 관련 책임자에게 보고하고 사후관리를 수행해야 한다.				

2. 보호대책

< 작성 時 주요 착안 사항 >

정보보호 대책은 기업의 정보보호 운영현황에 따라 선택할 수 있다. 선택하지 않은 통제항목의 경우 미선택 사유를 작성하여야 한다. 선택한 경우에는 선택이유 및 구현내용을 확인할 수 있도록 선택사유, 적용내용, 관련문서, 기록(증적자료)을 상세히 작성하여야 한다.

o 상세내용 : 신청기관 참고사항. 각 통제항목별로 의미하는 바를 기재하였음 (운영현황 등의 작성 공란이 부족할 경우 상세내용 삭제)

o 선택여부 : 정보보호 대책의 선택여부에 대해 Y(Yes) / N(No)로 표시 (N은 해당통제사항이 기업의 운영환경 상 적용되지 않는 경우에 선택)

o 운영현황(또는 미선택사유) : 해당 통제사항에 대한 구축 및 실제 운영내용을 요약하여 작성하되 구축의 특성 및 정당성을 파악할 수 있도록 인증기준보다 상세히 작성. 통제사항을 선택하지 않은 경우 위험관리(위험평가 및 처리)의 결과 및 분석에 따른 미선택의 사유를 반드시 작성.

o 관련문서(정책 또는 매뉴얼) : 인증기준을 만족하는 내용이 포함되어있는 기관의 문서(정책, 규정, 지침, 절차, 매뉴얼 등)의 제목을 작성하되 문서 내 부분에 해당할 경우 장, 절, 조 등을 상세하게 표시. 선택하지 않을 경우, 해당 근거를 확인할 수 있는 문서 및 문서 내 부분을 작성. 문서번호가 있다면 문서번호도 표시.

o 기록(증적자료) : 인증기준을 만족하는 내용이 포함되어있는 기관의 운영기록(증적자료)의 제목(파일명) 및 번호를 작성. 통제사항에 관련된 위험분석결과, 계획, 취약점분석관련 자료도 기록하여 대책명세서를 통해 관련내용을 확인할 수 있도록 함. 관련증적이 시스템으로 관리되는 경우 해당 시스템 위치, 시스템명 및 관련 메뉴를 작성.

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
1. 개인정보보호 정책						
1.1 정책의 승인 및 공표						
1.1.1	정책의 승인	개인정보보호정책은 이해관련자의 검토와 최고경영자의 승인을 받아야 한다.				
1.1.2	정책의 공표	개인정보보호정책은 모든 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.				
1.2 정책의 체계						
1.2.1	상위 정책과의 연계성	개인정보보호정책은 상위조직 및 관련 기관의 정책과 연계성을 유지하여야 한다.				
1.2.2	정책시행 문서수립	개인정보보호정책의 구체적 시행을 위한 지침, 절차, 표준 등을 수립하고 관련 문서간의 일관성을 유지해야 한다.				
1.3 정책의 유지관리						

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
1.3.1	정책 검토	정기적으로 개인정보보호정책 및 시행문서의 타당성을 검토하고, 중대한 보안사고 발생, 새로운 위협 또는 취약성의 발견, 시스템 환경에 중대한 변화 등이 개인정보보호정책에 미치는 영향을 분석하여 필요한 경우 제·개정하여야 한다.				
1.3.2	정책문서 관리	개인정보보호정책 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. 개인정보보호 조직						
2.1 조직 체계						
2.1.1	개인정보보호 관리책임자 (CPO) 지정	이용자의 개인정보보호 및 개인정보와 관련한 고충 처리를 위해 개인정보관리책임자를 지정하여야 한다. 개인정보관리책임자는 조직의 임원이나 개인정보와 관련하여 이용자의 고충처리를 담당하는 부서의 장이 수행할 수 있다.				
2.1.2	실무조직 구성	최고경영자는 개인정보보호관리책임자(CPO)의 역할을 지원하고 조직의 개인정보보호활동을 체계적으로 이행하기 위한 실무조직을 구성하고 조직 구성원의 정보보호 전문성을 고려하여야 한다.				
2.1.3	부서별 개인정보취급 책임자 및 담당자 지정	개인정보 취급부서의 개인정보보호 관련 의무 및 법 규정 준수 여부 등 감독.관리할 책임자 및 담당자를 지정하여야 한다.				
2.1.4	개인정보보호 의사결정 기구 구성 및 운영	조직 전반에 걸친 개인정보보호 관련 중요한 의사결정을 할 수 있는 의사결정 기구를 구성.운영하여야 한다.				
2.2 역할 및 책임						
2.2.1	역할 및 책임	개인정보관리책임자 및 개인정보를 취급하는 각 부서의 책임자, 담당자에 대한 역할과 책임을 정의하고, 그 활동을 평가할 수 있는 체계를 마련하여야 한다.				
2.2.2	보고 및 의사소통 체계	개인정보관리책임자 및 각 부서의 개인정보취급자, 담당자가 상호 의사소통할 수 있는 보고체계, 방법 및 절차를 정의하여야 한다.				
3. 개인정보 자산분류						
3.1 개인정보의 식별 및 책임						
3.1.1	개인정보 식별 및 관리 자산별 책임할당	조직의 개인정보 및 개인정보 관리자산을 식별하고 관리 자산별로 업무 영향, 법적 준수사항 등을 고려하여 중요도를 결정해야 한다. 또한, 소유자, 관리자, 개인정보취급자를 확인하고, 적절한 통제를 유지하기 위해 책임 소재를 명확히 정의하여야 한다.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
3.2 개인정보의 분류 및 취급						
3.2.1	개인정보 및 자산별 보안등급과 취급	개인정보 및 개인정보 관리 자산에 대하여 보안등급을 부여하고 관리해야 한다. 또한, 보안등급에 따라 취급 절차를 정의.이행하여야 한다.				
4. 개인정보 보호교육						
4.1 교육 프로그램 수립						
4.1.1	교육 계획	교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 개인정보보호 교육 계획을 수립.이행해야 한다.				
4.1.2	교육 대상	교육 대상에는 개인정보보호 관리체계 범위 내 임직원 및 외부자를 모두 포함하여야 한다.				
4.1.3	교육 내용 및 방법	교육에는 개인정보보호 및 개인정보보호 관리체계 개요, 보안사고 사례, 내부 규정 및 절차, 법적 책임 등의 내용을 포함하고 일반 임직원, 책임자, IT 및 개인정보보호 담당자 등 각 직무별 전문성 제고에 적합한 교육내용 및 방법을 정하여야 한다.				
4.2 교육 시행 및 평가						
4.2.1	교육 시행 및 평가	개인정보보호 관리체계 범위 내 임직원 및 외부자를 대상으로 연 1회 이상 교육을 시행하고 개인정보보호정책 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.				
5. 인적보안						
5.1 개인정보 취급자 관리						
5.1.1	개인정보 취급자 지정 및 감독	업무상 개인정보 취급하는 임직원의 경우 개인정보취급자로 지정하고 개인정보취급자 지정을 최소화 하는 등 관리할 수 있는 보호대책을 수립하여야 한다.				
5.1.2	개인정보보호 서약	개인정보취급자에게 이용자 개인정보 취급에 대한 보안서약서를 받아야 한다. 임시직원이나 제3자에게 개인정보에 대한 접근권한을 부여할 경우에도 개인정보보호 취급에 대한 보안서약서에 서명을 받아야한다.				
5.1.3	퇴직 및 직무변경 관리	퇴직 및 직무변경 시 인사부서와 개인정보보호 및 시스템 운영 부서 등 관련 부서에서 이행해야 할 자산반납, 접근권한 회수.조정, 결과 확인 등의 절차를 수립하여야 한다.				
5.1.4	상벌규정	인사규정에 직원이 개인정보보호 책임을 충실히 이행하거나 이행하지 않는 경우 등 정보보호 활동 수행에 따른 상벌 규정을 포함하여야 한다.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
6 침해사고 관리						
6.1 절차 및 체계						
6.1.1	침해사고 대응절차 수립	개인정보의 노출, 변경, 삭제에 대응하기 위한 긴급 연락체계, 개인정보 침해사고 발생 시 보고 및 대응, 사고 대응 조직의 구성 등을 포함한 개인정보 침해사고 대응절차를 수립하여야 한다.				
6.1.2	침해사고 대응체계 구축	개인정보 침해사고 대응이 신속하게 이루어질 수 있도록 중앙 집중적인 대응체계를 구축하고 외부기관 및 전문가들과의 협조체계를 수립하여야 한다.				
6.2 대응 및 복구						
6.2.1	침해사고 대응훈련	개인정보 침해사고 대응 절차를 임직원들이 숙지할 수 있도록 시나리오에 따른 모의훈련을 실시하여야 한다.				
6.2.2	침해사고 보고	개인정보 침해사고 징후 또는 사고 발생을 인지한 때에는 침해사고 유형별 보고절차에 따라 신속히 보고하고 법적 통지 및 신고 의무를 준수하여야 한다.				
6.2.3	침해사고 처리 및 복구	개인정보 침해사고 대응절차에 따라 처리와 복구를 신속하게 수행하여야 한다.				
6.3 사후관리						
6.3.1	침해사고 분석 및 정보공유	개인정보 침해사고가 처리되고 종결된 후 이에 대한 분석을 수행하고 그 결과를 보고하여야 한다. 또한 개인정보 침해사고에 대한 정보와 발견된 취약점들을 관련 조직 및 임직원들과 공유하여야 한다.				
6.3.2	침해사고 재발방지	개인정보 침해사고로부터 얻은 정보를 활용하여, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하고 이를 위해 필요한 경우 정책, 절차, 조직 등의 대응체계를 변경하여야 한다.				
7 기술적 보호조치						
7.1 접근통제						
7.1.1	접근통제 정책 수립	개인정보보호 요구사항을 기반으로 비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 개인정보취급자의 접근통제 정책을 수립하여야 한다.				
7.1.2	개인정보취급자 등록	개인정보 및 개인정보처리시스템의 접근을 통제하기 위한 공식적인 개인정보취급자 등록 및 해지 절차를 마련하고 업무 필요성에 따라 개인정보취급자 접근권한을 최소한으로 부여하여야 한다.				
7.1.3	개인정보취급자 권한관리	개인정보처리시스템의 접근권한은 최소한의 업무수행자에게만 부여하고 관련 내역을 관리해야 한다.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
7.1.4	개인정보취급자 접근 권한 검토	개인정보 및 개인정보처리시스템을 사용하는 개인정보취급자에게 부여된 접근권한 현황을 정기적으로 점검해야 한다.				
7.1.5	개인정보취급자 인증 및 식별	개인정보처리시스템의 접근을 개인정보취급자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 인증 절차에 따라 통제하고, 필요한 경우 법적요구사항 등을 고려하여 개인정보처리시스템 접근 시 강화된 인증방식을 적용해야 한다. 또한, 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.				
7.1.6	개인정보 취급자 책임	법적요구사항, 외부 위협요인 등을 고려하여 개인정보처리시스템 및 개인정보에 대한 접근이 허용된 PC의 보안책임은 개인정보 취급자 자신에게 있음을 주지시키고 관리지침을 제공하여야 한다.				
7.1.7	개인정보취급자 및 사용자 패스워드 관리	법적요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도, 초기 패스워드 변경, 변경주기 등 사용자 패스워드 관리절차를 수립하고 패스워드 관리 책임이 사용자에게 있음을 주지시켜야 한다. 특히, 개인정보취급자 패스워드는 별도 보호대책을 수립하여 관리하여야 한다.				
7.1.8	특수권한 관리	개인정보 및 개인정보처리시스템에 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.				
7.1.9	네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 접근통제리스트, 네트워크 식별자 등에 대한 관리절차를 수립하고 서비스, 사용자 그룹, 개인정보 자산의 중요도에 따라 내·외부 네트워크를 분리하여야 한다.				
7.1.10	서버 접근	서버별로 접근이 허용되는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 적용하여야 한다.				
7.1.11	응용 프로그램 접근	사용자의 업무 또는 직무에 따라 개인정보를 취급하는 응용프로그램 접근권한을 제한하고 불필요한 개인정보의 노출을 최소화하여야 한다.				
7.1.12	데이터베이스 접근	데이터베이스 접근을 허용하는 응용프로그램 및 사용자 직무를 명확하게 정의하고 응용프로그램 및 직무별 접근통제 정책을 수립하여야 한다. 또한 개인정보를 저장하고 있는 데이터베이스의 경우 사용자 접근내역을 기록하고 접근의 타당성을 정기적으로 검토하여야 한다.				
7.1.13	모바일 기기 접근	모바일기기를 업무 목적으로 내.외부 네트워크에 연결하여 활용하는 경우 개인정보 유출 및 침해사고 예방을 위해 기기 인증 및 승인, 접근 범위, 기기 보안설정, 오남용 모니터링 등의 접근통제 대책을 수립하여야 한다.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
7.1.14	인터넷 접속 통제	개인정보처리시스템에 접근 가능한 개인정보취급자의 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.				
7.2 암호통제						
7.2.1	암호 정책 수립 및 이행	조직의 개인정보보호를 위한 암호화 대상, 암호 강도(복잡도), 키관리, 암호사용 대한 정책을 수립하고 이행하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.				
7.2.2	암호키 생성 및 이용	암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고 필요 시 복구방안을 마련하여야 한다.				
7.3 운영통제						
7.3.1	운영절차 수립	개인정보처리시스템 동작에 문제 발생 시 재 동작 및 복구, 오류 및 예외사항 처리 등 시스템 운영을 위한 절차를 수립하여야 한다.				
7.3.2	직무 분리	고의적이거나 부주의로 인한 개인정보처리시스템의 오남용 예방을 위해 직무를 분리하고, 직무 분리가 어려운 특수한 경우 별도의 관리감독 대책을 수립 한다.				
7.3.3	변경관리	권한 오남용 등 고의적인 행위로 인해 발생할 수 있는 잠재적인 피해를 줄이기 위하여 직무 분리 기준을 수립하고 적용하여야 한다. 다만 인적자원 부족 등 불가피하게 직무분리가 어려운 경우 별도의 보완통제를 마련하여야 한다.				
7.3.4	원격운영 관리	내부 네트워크를 통하여 개인정보처리시스템을 관리하는 경우 특정 단말에서만 접근을 할 수 있도록 제한하고, 원격지에서 인터넷 등 외부 네트워크를 통하여 개인정보시스템을 관리하는 것은 원칙적으로 금지한다. 부득이한 사유로 인해 허용하는 경우에는 책임자 승인, 접속 단말 및 사용자 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등의 보호대책을 수립하여야 한다.				
7.3.5	스마트워크 보안	재택근무, 원격협업 등과 같은 원격 업무 수행 시 이에 대한 관리적.기술적 보호대책을 수립하고 이행하여야 한다.				
7.3.6	무선 네트워크 보안	무선랜 등을 통해 무선인터넷을 사용하는 경우 무선 네트워크 구간에 대한 보안을 강화하기 위해 사용자 인증, 송수신 데이터 암호화 등의 보호대책을 수립하여야 한다.				
7.3.7	공개서버 보안	웹사이트 등에 정보를 공개하는 경우 정보 수집, 저장, 공개에 따른 허가 및 게시절차를 수립하고 공개서버에 대한 물리적, 기술적 보호대책을 수립하여야 한다.				
7.3.8	악성코드 통제	바이러스, 웜, 트로이목마 등의 악성코드로부터 정보시스템을 보호하기 위해 악성코드 예방, 탐지, 대응 등의 보호대책을 수립하여야 한다.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
7.3.9	패치관리	소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인해 발생할 수 있는 침해사고를 예방하기 위해 최신 패치를 정기적으로 적용하고 필요한 경우 시스템에 미치는 영향을 분석하여야 한다.				
7.3.10	백업관리	데이터의 무결성 및 개인정보처리시스템의 가용성을 유지하기 위해 백업 대상, 주기, 방법 등의 절차를 수립하고 침해사고 발생 시 바로 복구할 수 있도록 관리하여야 한다.				
7.3.11	취약점 점검	개인정보처리시스템이 알려진 취약점에 노출되어 있는지 여부를 확인하기 위하여 정기적으로 기술적 취약점 점검을 수행하고 발견된 취약점들은 조치하여야 한다.				
7.4 매체 보안						
7.4.1	개인정보처리 시스템 저장매체 관리	개인정보처리시스템 폐기 또는 재사용 시 개인정보를 담고 있는 하드디스크, 스토리지, 테잎 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 개인정보는 복구 불가능하도록 완전히 삭제하여야 한다.				
7.4.2	휴대용 저장매체 관리	조직의 개인정보 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.				
7.5 시스템 개발보안						
7.5.1	분석 및 설계 보안	개인정보처리시스템을 신규 개발하거나 구매, 기존 시스템 개선 등 환경에 의한 변경이 있을 경우, 개인정보 영향평가를 수행하고 평가 결과에 따른 보안요구사항을 포함하여 개발해야 한다.				
7.5.2	구현 및 시험	안전한 코딩방법에 따라 개인정보처리시스템을 구현하고, 분석 및 설계과정에서 도출한 보안요구사항이 개인정보처리시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다. 또한 알려진 기술적 보안 취약성에 대한 노출여부를 점검하고 이에 대한 보안대책을 수립하여야 한다.				
7.5.3	개발과 운영 환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경 위험의 감소를 위해 원칙적으로 분리하여야 한다.				
7.5.4	운영 환경 이관	개인정보처리시스템 운영 관련 프로그램의 수정은 적절한 권한을 부여받은 직원만이 수행해야 한다. 개인정보처리시스템은 실행코드만을 갖고, 성공적인 시험절차와 개인정보취급자 인수 후에 실행해야 한다.				
7.5.5	시험 데이터 보안	시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험 데이터 생성, 이용 및 관리, 파기, 기술적 보호조치 관한 절차를 수립.이행하여야 한다.				
7.5.6	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.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
7.5.7	외주 개발 보안	개인정보처리시스템의 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리.감독하여야 한다.				
7.6 접속기록 관리 및 모니터링						
7.6.1	시각동기화	로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 정보시스템 시각을 공식 표준시각으로 정확하게 동기화 하여야 한다.				
7.6.2	개인정보처리 시스템 접속기록 저장	응용프로그램, DB 등 개인정보처리시스템에 대한 개인정보취급자의 접속기록(식별자, 접속일시, 개인정보 열람.수정.삭제.출력 등의 작업내역)을 저장하여야 한다.				
7.6.3	개인정보처리 시스템 접속 기록의 위.변조 방지	개인정보처리시스템의 접속기록은 위변조되지 않도록 접근권한 통제, 별도의 물리적인 저장장치 보관 등의 보안통제가 적용되어야 한다.				
7.6.4	개인정보 처리활동 모니터링 및 점검	개인정보보호 업무의 수행과 관련하여 오류 및 부정행위가 발생하지 하지 않도록 개인정보처리 활동에 대한 모니터링 및 정기적 점검활동에 대한 지침, 절차를 수립.이행해야 한다. 또한 모니터링 및 점검결과에 따라 사후조치가 적시에 이루어져야 한다.				
7.7 출력, 복사 통제						
7.7.1	개인정보 출력 용도의 특정 및 보호대책	개인정보 출력시 용도를 특정하고 용도에 따라 출력 항목을 최소화한다. 또한, 개인정보 출력방법(테이프, 디스크, 인쇄, 휴대용 저장매체 등)에 따라 출력 일시, 방법 등 필요한 사항의 기록.관리 등 보호대책을 수립하여야 한다.				
7.8 개인정보표시 제한						
7.8.1	개인정보 마스킹	업무를 목적으로 개인정보 조회, 출력 등을 수행할 경우, 마스킹 기술 등을 통해 개인정보 표시를 제한하여야 한다.				
8. 물리적 보호조치						
8.1 보호구역						
8.1.1	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.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
8.1.2	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 개인정보처리시스템을 외부 집적정보통신시설에 위탁.운영하는 경우 관련 요구사항을 계약서에 반영하고 주기적으로 검토를 수행하여야 한다.				
8.1.3	보호구역 내 작업	유지보수 등 주요 설비 및 시스템이 위치한 보호구역 내의 작업 절차를 수립하고 작업에 대한 기록을 주기적으로 검토하여야 한다.				
8.1.4	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.				
8.1.5	모바일 기기 반.출입	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.				
8.2 사무실 보호						
8.2.1	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.				
8.2.2	공용업무 환경 보안	사무실에서 공용으로 사용하는 사무처리 기기, 문서고, 공용 PC, 파일서버 등을 통해 중요정보 유출이 발생하지 않도록 보호대책을 마련하여야 한다.				
8.3 영상정보처리기기 보안						
8.3.1	영상정보처리 기기 이용제한, 안내판 설치, 관리	영상정보처리기기를 운영 하는 경우 설치 목적에 따라 법적 요구사항(안내판 설치, 안전성 확보에 필요한 조치 등)을 준수하여야 한다.				

3. 생명주기

< 작성 時 주요 착안 사항 >

정보보호 대책은 기업의 정보보호 운영현황에 따라 선택할 수 있다. 선택하지 않은 통제항목의 경우 미선택 사유를 작성하여야 한다. 선택한 경우에는 선택이유 및 구현내용을 확인할 수 있도록 선택사유, 적용내용, 관련문서, 기록(증적자료)을 상세히 작성하여야 한다.

o 상세내용 : 신청기관 참고사항. 각 통제항목별로 의미하는 바를 기재하였음 (운영현황 등의 작성 공란이 부족할 경우 상세내용 삭제)

o 선택여부 : 정보보호 대책의 선택여부에 대해 Y(Yes) / N(No)로 표시 (N은 해당통제사항이 기업의 운영환경 상 적용되지 않는 경우에 선택)

o 운영현황(또는 미선택사유) : 해당 통제사항에 대한 구축 및 실제 운영내용을 요약하여 작성하되 구축의 특성 및 정당성을 파악할 수 있도록 인증기준보다 상세히 작성. 통제사항을 선택하지 않은 경우 위험관리(위험평가 및 처리)의 결과 및 분석에 따른 미선택의 사유를 반드시 작성.

o 관련문서(정책 또는 매뉴얼) : 인증기준을 만족하는 내용이 포함되어있는 기관의 문서(정책, 규정, 지침, 절차, 매뉴얼 등)의 제목을 작성하되 문서 내 부분에 해당할 경우 장, 절, 조 등을 상세하게 표시. 선택하지 않을 경우, 해당 근거를 확인할 수 있는 문서 및 문서 내 부분을 작성. 문서번호가 있다면 문서번호도 표시.

o 기록(증적자료) : 인증기준을 만족하는 내용이 포함되어있는 기관의 운영기록(증적자료)의 제목(파일명) 및 번호를 작성. 통제사항에 관련된 위험분석결과, 계획, 취약점분석관련 자료도 기록하여 대책명세서를 통해 관련내용을 확인할 수 있도록 함. 관련증적이 시스템으로 관리되는 경우 해당 시스템 위치, 시스템명 및 관련 메뉴를 작성.

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
1. 개인정보수집에 따른 조치						
1.1 최소한의 정보수집						
1.1.1	서비스 제공을 위해 필요한 최소한의 정보수집	서비스 제공을 위해 필요한 최소한의 정보만을 수집해야 한다. 개인정보 수집 시 필수와 선택 사항으로 구분하여 기재할 수 있도록 하여야 하며, 선택 사항의 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하여서는 아니 된다.				
1.1.2	중요 개인정보 수집 제한	개인의 사생활을 현저하게 침해할 우려가 있거나 개인을 식별할 수 있는 민감하고 중요한 개인정보를 수집하지 않아야 하며, 수집이 필요한 경우 이용자의 별도 동의를 받아야 한다.				
1.1.3	간접 수집 시 조치	시스템에 의한 수집 또는 개인정보 처리를 통해 생성하여 간접 수집한 개인정보에 대하여 적절한 보호대책을 수립.이행해야 한다.				
1.1.4	주민등록번호 수집.이용 제한	법령에서 이용자의 주민등록번호 수집·이용을 허용한 경우를 제외하고 주민등록번호를 수집·이용하면 아니 된다.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
1.1.5	주민등록번호 대체수단	법령에서 이용자의 주민등록번호 수집·이용을 허용한 경우에도 공인인증서, 아이핀 등 주민등록번호 대체수단을 제공해야 한다.				
1.2 개인정보수집 시 고지 및 동의 획득						
1.2.1	이용자 동의	개인정보는 이용자의 동의를 얻은 후에 수집해야 한다.				
1.2.2	법정대리인 동의 획득 및 고지	만14세 미만의 아동의 개인정보를 수집 할 경우 법정대리인에게 필요한 사항을 고지해야 한다.				
1.2.3	동의기록 보관	이용자 동의 기록은 이용자가 탈퇴하여 관련 기록을 파기.폐기 전까지 안전하게 보관해야 한다.				
1.2.4	고유식별번호 별도 동의	고유식별번호를 수집하게 될 경우에는 다른 개인정보 동의와는 별도로 추가 동의를 얻은 후 수집해야 된다.				
1.3 개인정보취급방침						
1.3.1	개인정보취급 방침 마련 및 게시	개인정보취급방침을 마련하고 이용자가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개해야 한다.				
2. 개인정보이용 및 제공에 따른 조치						
2.1 동의 범위 내 개인정보 사용						
2.1.1	목적 내 개인정보 이용	개인정보는 이용자에게 고지하고 동의 받은 범위를 벗어나 이용하지 않아야 하고, 만약 동의 범위를 벗어나 이용할 경우, 이용자로부터 추가적으로 동의를 받아야 한다.				
2.2 역할 및 책임						
2.2.1	이용자의 불만 처리	개인정보와 관련한 이용자의 의견 및 불만을 접수.처리하기 위하여 상담창구를 운영해야 한다.				
2.2.2	열람정정 요구권 보장 및 처리	이용자가 자신의 개인정보에 대한 열람 또는 이용 및 제공 내역을 요청할 경우 이에 대해 지체 없이 대응.조치해야한다.				
2.2.3	동의철회	이용자가 개인정보 수집·이용·제공 등의 동의 철회를 요청하면 지체 없이 대응.조치해야한다.				
2.2.4	개인정보 이용내역 통지	수집한 이용자의 개인정보 이용내역을 주기적으로 이용자에 통지해야 한다.				
2.2.5	개인정보 누출 등 통지.신고 절차 및 방법	개인정보의 분실·도난·누출 사실은 지체 없이 이용자에 고지하고 소관 부처 및 전문기관에 신고해야 하며, 개인정보 누출에 따른 통지 및 신고 방법.절차를 수립.이행해야 한다.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
2.2.6	개인정보 누출 등 대책 마련	개인정보 누출에 따른 통지 및 신고의 방법·절차를 수립.이행해야 한다.				
2.3 외부 위탁 시 개인정보보호						
2.3.1	이용자 고지 및 동의	개인정보 누출에 따른 통지 및 신고의 방법·절차를 수립.이행해야 한다.				
2.3.2	위탁자 책임	제3자에게 이용자의 개인정보를 처리할 수 있도록 업무를 위탁하는 경우에는 수탁자, 수탁목적 등의 사항을 이용자에게 알리고 동의를 얻어야 한다.				
2.3.3	외부위탁 관리 감독	위탁자는 개인정보의 위탁 시 수탁자가 안전하게 개인정보를 취급하도록 관리.감독해야 하고, 수탁자가 법.규정 위반한 경우를 대비하여 처리절차를 수립.이행해야 한다.				
2.3.4	외부위탁계약 시 보안 요구사항	외부위탁 업체가 계약서 및 서비스 수준 협약에 명시된 사항을 충분히 이행하는지 상시 관리 감독하고 주기적으로 점검 또는 감시를 해야한다.				
2 개인정보이용 및 제공에 따른 조치						
2.4 제3자 제공시 개인정보보호						
2.4.1	제3자 제공시 동의	이용자의 개인정보를 제3자에게 제공하는 경우, 제공받는 자, 제공목적 등 관련 내용을 이용자에게 알리고 동의를 얻어야 한다.				
2.4.2	제공받은 개인정보의 관리	개인정보를 제공받은 경우 제공받은 목적 외의 용도로 이용하지 않고, 제3자에게 제공하지 않아야 한다.				
2.4.3	제3자 보안	제3자에게 개인정보의 접근을 허용하는 경우 개인정보를 안전하게 보호하기 위한 보호절차에 따라 통제해야 한다.				
2.5 개인정보이전 시 개인정보보호						
2.5.1	개인정보 이전 시 보호조치	영업의 양도, 합병 등으로 개인정보를 이전하는 경우 적절한 보호대책을 수립.이행해야 한다.				
2.5.2	해외 이전 시 보호조치	개인정보를 해외로 이전하는 경우 개인정보 항목 등에 대한 이용자 동의를 얻고 적절한 보호대책을 수립.이행해야 한다.				
3. 개인정보관리 및 파기에 따른 조치						
3.1 개인정보관리 및 파기						
3.1.1	개인정보의 저장 및 관리	수집된 개인정보는 안전하게 저장 및 관리 하여야 하며 정확성을 유지 하여야 한다.				
3.1.2	파기규정	개인정보의 보유기간 및 파기 관련 내부 규정이 마련되어야 한다.				

통제항목		상세내용	선택 여부	운영현황 (또는 미선택사유)	관련문서 (정책, 지침 등 세부조항번호까지)	기록(증적자료)
3.1.3	파기시점	개인정보가 저장된 매체, 문서 등은 서비스 이용계약 해지 등 개인정보의 수집 목적이 달성된 경우 이를 지체 없이 파기해야 한다.				
3.1.4	파기방법	개인정보는 안전한 방법으로 파기하여야 한다.				
3.1.5	목적 달성 후 보유	개인정보의 수집목적 달성 후에도 개인정보를 관련 법령 등에 의해 일부 또는 전부를 보유한다면 정보주체에게 보유근거, 목적, 보유기간 및 항목에 대해 고지하거나 약관에 명시하고 최소한의 항목으로 제한하여야 한다.				
3.1.6	휴면 이용자의 개인정보 파기	일정기간 동안 이용하지 않는 휴먼 이용자의 개인정보를 보호하기 위해 개인정보 삭제 예정고지와 삭제조치 및 안내를 등 보호조치를 취해야 한다.				

< 인증 심사 관련 문서 >

[붙임 3] 사전점검(심사) 체크리스트

[붙임 4] 보완조치 요청서

[붙임 5] 결함보고서

[붙임 6] 보완조치 내역서

[붙임 7] 인증 기준 세부점검항목

사전점검(심사) 체크리스트

항목	체크	메모
홈페이지	□	
- 홈페이지 서버, 네트워크, 정보보호시스템 수 ※ 서버운영 : IDC 이용 or 자체전산센터 이용 - 홈페이지 운영 범위 - 메인 홈페이지에 링크된 홈페이지 개수, 관리주체(소유주체), 로그인 시 프로세스 - 외부업체(협력업체) 업무수행 범위		
인증심사	□	
- 심사일정 확정 - 심사 시작회의 시간 협의 ※ 월~화: 문서심사 , 수~금: 기술심사 위주 안내 - 심사범위의 담당자 미리 알려줄 것 - 인터뷰는 하루 전, 반나절 전에 요청할 것임		
준비사항	□	
- 상위 규정 및 정책(방침)서, 정보보호 정책/지침/절차서/매뉴얼(원본 O부, 사본 O부) - 인증범위정의서, 자산목록, 위험분석보고서, 취약점 분석결과 등 (원본 O부, 사본 O부) - 정보보호계획서, 직무기술서, 내부심사결과 등 각종 계획서 및 보고서(원본 O부, 사본 O부) - 각종 점검 및 관리대장 등 이행증적 자료(O부) - 정보보호대책명세서(O부) - 업무관련 조직도, 심사지원 담당자 연락처(O부) ※ 심사지원을 위한 담당자 지정 필요		
문서 현행화 및 송부	□	
- 대책명세서, 범위정의서 현행화 및 송부 ※ 조직개편, 신청범위 재설정 시, 실무운영위원 등 내용포함 - 내부심사 결과 및 이행여부 문서에 반영 - 교육결과 (최근날짜 수정)		
요청사항	□	
- 시작회의 참석자 명단(이름, 직급, 부서명) - 주요보안시스템, 업무시스템 실무자 설명(시연) 요청 - 외주업체, 협력업체, 유지보수업체 등 상주인력 인원 포함한 목록정리 요청		
기타	□	
- 심사장소 및 심사일자 확정		

※ 정보보호 관리체계 구축 후 인증 신청을 하기 전에 스스로 점검하거나, 인증기관이 사전점검(심사) 시 점검에 활용하는 체크리스트

※ 인증기관이 사전점검(심사)을 실시하지 않을 경우, 자체 점검내역을 신청서류와 함께 제출 필요

[붙임 4] 보완조치 요청서

보완조치 요청서		
인증심사 신청내역	신청기관	
	대 표 자	
	신청구분	□ 정보보호 관리체계 □ 개인정보보호 관리체계 □ 최초심사 □ 사후심사 □ 갱신심사
	심사범위	
	적용규격	□ 정보보호 관리체계 인증심사기준(정보보호 관리체계 인증 등에 관한 고시) □ 개인정보보호 관리체계 인증심사기준(방통위 의결(제2010-66-272호))

□ 보완조치요청사항 : 총 건

중결함 (건) 결함 (건)

□ 건별 정보보호관리체계 결함보고서 및 보완조치요청사항은 별도로 첨부

위와 같이 결함보고서 및 보완조치요청사항을 통보하오니 기한 내에 보완조치에 대한 결과를 제출하여 주시기 바랍니다.

년 월 일

한국인터넷진흥원 (심사팀장 : (인))

1. 이 인증심사는 샘플링 심사기법에 의하여 수행된 것으로 발견되지 않은 부적합이 존재할 수 있습니다.
2. 이 보고서의 내용은 비밀로 취급되며 신청기관의 사전 동의 없이는 공개되지 않습니다. 다만 법원의 요구가 있거나 법률로 정한 경우 예외로 합니다.

※ 인증 심사 후, 결함 사항에 대하여 인증기관이 신청기관에 보완조치를 요청

[붙임 5] 결함보고서

결함보고서				
기록일자	년 월 일		신청기관	
인증심사 구분	□ 정보보호 관리체계 □ 개인정보보호 관리체계 □ 최초심사 □ 사후심사 □ 갱신심사			
심사범위				
인증심사원	성명	(인)		
신청기관 확 인 자	성명	(인)	소속 및 직급	/
문 제 점	□ 중결함 □ 결 함			

해당부서	
관련조항	(적용항목)
문제점	□ (결함사항 요약) o 기준/지침/절차는 ~하도록 되어있음 (인증기준) - 이에 대해 신청기관에서는 ~명시하고 있음 (반영된 정책/지침 내용) o 그러나 ~되고/하고 있지 않음 (현황) o 따라서 ~해야 함 (요구사항)
근거목록	-

※ 심사원 별로 인증기준 미준수 사항에 대하여 개별 결함 사항을 작성하여 보완조치 요청서와 함께 신청기관에 통보

<결함보고서 예시>

결함보고서				
기록일자	2011년 11월 25일		신청기관	ABC(주)
인증심사 구분	■ 정보보호 관리체계		□ 개인정보보호 관리체계	
	■ 최초심사	□ 사후심사	□ 갱신심사	
심사범위	ABC(주), 『인터넷 쇼핑몰 서비스』			
인증심사원	성명	홍 길 동 (인)		
신청기관 확 인 자	성명	이 개 인 (인)	소속 및 직급	정보보호실 / 실장 (정보보호책임자)
문 제 점	□ 중결함	■ 결 함		

해당부서	전부서
관련조항	4. 정보자산분류 4.2.2 보안등급과 취급
문제점	□ **ABC(주) 른 정보(문서, 파일)자 산 식별** ○ 심사기 등급을 부여하고 보안등급 에 따른 - 또한 AI 용표준)"에는 정보를 공개(Public), 대외비(Internal), 기밀(Confidential), 제한(Restricted)로 분류하도록 하고 있으며 등급별 취급기준(표기방법, 저장, 폐기, 외부전송 등)을 정의하고 있음 ○ 그러나 주요 정보 취급부서(재무부문, 인사부문, CTO 부문 등) 인터뷰 결과 다음과 같은 문제점이 발견됨 - 내부직원의 정보분류체계(공개, 대외비, 기밀, 제한)에 대한 인지 미흡 - 각 부서별로 인사기록카드, 회계전표, 권리침해신고서, 영업비밀(통계, 분석 자료), 연봉정보 등 주요정보에 대한 등급부여(대외비, 기밀, 제한) 및 식별 미흡 ※ 각 팀별로 정보(문서, 파일 등)에 대한 식별이 명확하게 되어 있지 않음 - 정보등급 따른 취급기준 준수 미흡 : 팀별로 임의적 관리 수행 ※ 기밀이상의 문서로 판단되는 인사기록카드, 권리침해신고서 등 시건장치가 되지 않는 공간에 보관, PC 또는 파일서버 팀별 저장 시 암호화 적용 미흡, 등급표기 누락 등 ○ 따라서 상기 문제점에 대한 보완이 필요함 - 내부직원에 대한 정보분류체계 및 취급기준 교육 수행(인식제고) - 각 부서별 주요정보(문서, 파일 등) 등급 식별 - 정보등급 부여에 따른 취급기준 준수
근거목록	-『정보보호 준거 이행 표준』

[붙임 6] 보완조치 내역서

보완조치 내역서						
□ 정보보호 관리체계 □ 개인정보보호 관리체계 □ 전자정부 정보보호 관리체계						
관련조항 : 통제항목번호 및 제목						
□ 중결함(부적합) □ 결함						
보완조치 결과	※ 결함(부적합)보고서의 결함(부적합)사항에 대한 보완 조치 내용 작성 □ 결함(부적합)내용 □ 보완내역 □ 관련근거					
	작성자	(인)	확인자	(인)	작성일	년 월 일
보완조치 결과확인	확인자 (심사팀장)	(인)	확인일	년 월 일		
			결과	□ 완료 □ 미완료 □ 현장확인		
현장확인	확인자 (심사팀장)	(인)	확인일	년 월 일		
			결과	□ 완료 □ 미완료		

※ 인증기관이 요청한 보완조치 요청에 대하여 보완조치를 완료하고, 신청기관이 인증기관에 제출하는 문서

< 인증 관련 법령 >

[붙임 7] 정보보호 관리체계 인증 등에 관한 고시 전문

[붙임 8] ISMS 인증 관련 정보통신망법-시행령-하위고시(3단비교표)

[붙임 9] 인증 기준 세부점검항목

[붙임 7] 정보보호 관리체계 인증 등에 관한 고시 전문

정보보호 관리체계 인증 등에 관한 고시

제정 2008. 05. 19. 방송통신위원회고시 제2008-11호
개정 2009. 11. 05. 방송통신위원회고시 제2009-27호
개정 2010. 02. 03. 방송통신위원회고시 제2010- 3호
개정 2012. 03. 15. 방송통신위원회고시 제2012-23호
전부개정 2013. 01. 17. 방송통신위원회고시 제2013- 4호

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 보유 현황과 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 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 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 변경 신청서를 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) 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령 훈령 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<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 시행 당시 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<제2013-00호, 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 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="4">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>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 장소</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)

※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></td><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>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></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 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></td><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 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	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 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 대가 산정 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 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	정보자산 별 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	데이터 베이스 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 인수기준을 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	무선네트 워크 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	처 리 기 관 (방송통신위원회)	처 리 기 관 (방송통신위원회)	처 리 기 관 (방송통신위원회)	처 리 기 관 (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.

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 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

210㎜×297㎜[백상지(120g/㎡)]

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/㎡]

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)

210㎜×297㎜[백상지(80g/㎡)]

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

(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

(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	

(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 안 된다.
- 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

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				

실적사항	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

210㎜×297㎜[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 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

210㎜×297㎜[백상지(120g/㎡)]

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/㎡)]

[붙임 8] ISMS 인증 관련 정보통신망법-시행령-하위고시(3단비교표)

정보통신망법	정보통신망법 시행령	하위고시
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> 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. "정보보호산업"이란 정보보호제품을 개발·생산 또는 유통하는 사업이나 정보보호에 관한 컨설팅 등과 관련된 산업을 말한다. 9. "게시판"이란 그 명칭과 관계없이 정보통신망을 이용하여 일반에게 공개할 목적으로 부호·문자·음성·음향·화상·동영상 등의 정보를 이용자가 게재할 수 있는 컴퓨터 프로그램이나 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	**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.	

정보통신망법	정보통신망법 시행령	하위고시
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. ② 이 법에서 사용하는 용어의 뜻은 제1항에서 정하는 것 외에는 「정보화촉진기본법」으로 정하는 바에 따른다. <개정 2008.6.13> **제45조(정보통신망의 안정성 확보 등)** ① 정보통신서비스제공자는 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 정보통신서비스제공자에게 이를 지키도록 권고할 수 있다. <개정 2012.2.17> ③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다. 1. 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치 2. 정보의 불법 유출·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 계획구축 등 관리적 보호조치 **[시행일 : 2013.2.18] 제45조**		**<정보보호조치에 관한 지침> 전부개정안** **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

정보통신망법	정보통신망법 시행령	하위고시
		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. **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)** 정보통신서비스제공자는 매년 별표 1의 정보보호조치의 이행여부를 자체적으로 점검하거나 외부 전문기관으로 하여금 점검하게 할 수 있다. **제5조(재검토 기한)** 「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 2016년 2월 17일까지로 한다. **부칙<제2008-12호, 2008.5.19.>**

정보통신망법	정보통신망법 시행령	하위고시
		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<제2013-4호, 2013. 1.17.>** 이 고시는 2013년 2월 18일부터 시행한다.
제45조의2(정보보호 사전점검) ① 정보통신서비스제공자는 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. 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		**<정보보호 사전점검에 관한 고시> 제정안** **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. **부칙<제2013-4호, 2013. 1.17.>** **제1조(시행일)** 이 고시는 2013년 2월 18일부터 시행한다. **제2조(재검토 기한)** 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 고시 발령 후 법령이나 현실여건

정보통신망법	정보통신망법 시행령	하위고시
③ 제2항에 따른 정보보호 사전점검의 기준·방법·절차·수수료 등 필요한 사항은 대통령령으로 정한다. **[본조신설 2012.2.17] [시행일 : 2013.2.18] 제45조의2**	**제36조의2(정보보호 사전점검기준)** 법 제45조의2제2항에 따른 정보보호 사전점검기준은 다음 각 호의 사항을 고려하여 미래창조과학부장관이 정하여 고시한다. 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]**	의 변화 등을 검토하여 이 고시의 폐지, 개정 등 조치를 하여야 하는 기한은 2016년 2월 17일까지로 한다. **제18조(사전점검 기준)** 영 제36조의2에 따른 사전점검기준은 별표 3과 같다.
	제36조의3(정보보호 사전점검 권고 대상) ① 법 제45조의2제2항 제1호에서 "대통령령으로 정하는 정보통신서비스 또는 전기통신사업"이란 정보시스템 구축에 필요한 투자금액이 5억원 이상(하드웨어·소프트웨어의 단순한 구입비용을 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. **[본조신설 2012.8.17]**	**제4조(사전점검 실시 우대)** 방송통신위원회는 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.
	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.	**제6조(사전점검 수행기관 지정 공고)** ① 방송통신위원회는 영 제36조의4제3항에 따라 사전점검을 수행하는 외부 전문기관(이하 "사전점검 수행기관"이라 한다)을 지정할 수 있다. ② 방송통신위원회는 사전점검 수행기관을 지정할 필요가 있을 때에는 미리 접수 신청기간과 신청요령 등을 정하여 관보 및 인터넷 홈페이지에 20일 이상 공고하여야 한다.

정보통신망법	정보통신망법 시행령	하위고시
		제7조(사전점검 수행기관 지정 요건) ① 사전점검 수행기관으로 지정받으려는 자는 시스템, 네트워크, 데이터베이스, 소프트웨어 개발, 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 구축·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 방송통신위원회에 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 방송통신위원회는 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 방송통신위원회는 심사위원회의 심사결과를 검증하여야 한다. ② 방송통신위원회는 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)** 방송통신위원회는 수행기관이 제7조제3항 각호에 따른 보호대책의 준수 여부를 점검할 수 있다.

정보통신망법	정보통신망법 시행령	하위고시
	④ 제1항부터 제3항까지에서 규정한 사항 외에 정보보호 사전점검의 방법 및 절차에 관하여 필요한 세부사항은 미래창조과학부장관이 정하여 고시한다. **[본조신설 2012.8.17]**	**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 방송통신위원회는 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 방송통신위원회에 제출하여야 한다. **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. **제3조(사전점검 실시 시기)** 사전점검은 대상자가 새로이 정보통신망을 구축하거나 정보통신서비스를 제공하고자 하는 때에는 그 계획 또는 설계 단계부터 실시한다. **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. **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.

정보통신망법	정보통신망법 시행령	하위고시
	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. ② 미래창조과학부장관은 다음 각 호의 사항을 고려하여 정보보호 사전점검 수수료의 산정기준을 정하여 고시한다. 1. 정보보호 사전점검을 받는 정보통신서비스 또는 전기통신사업의 규모 2. 정보보호 사전점검에 참가하는 자의 전문성	**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 구축하고 정보통신망 또는 정보통신서비스의 운영과정에 반영한다. ② 사전점검 과정에서 심각한 위험이 발견된 경우 그에 대한 보호대책을 구현한 이후에 정보통신망 또는 정보통신서비스를 운영하여야 한다. **제25조(안내서)** 한국인터넷진흥원장은 이 고시에 대한 안내서를 마련하여 방송통신위원회 위원장의 승인을 받아 공표할 수 있다. **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

정보통신망법	정보통신망법 시행령	하위고시
	3. 정보보호 사전점검에 필요한 기간 **[본조신설 2012.8.17]**	
제45조의3(정보보호 최고책임자의 지정 등) ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정할 수 있다. ② 정보보호 최고책임자는 다음 각 호의 업무를 총괄한다. 1. 정보보호 관리체계의 구축 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 ③ 정보통신서비스제공자는 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. ④ 정부는 제3항에 따른 정보보호 최고책임자 협의회의 활동에 필요한 경비의 전부 또는 일부를 지원할 수 있다. **[본조신설 2012.2.17] [시행일 : 2013.2.18] 제45조의3**	**제36조의6(정보보호 최고책임자 협의회의 사업 범위)** 법 제45조의3제3항에서 "대통령령으로 정하는 공동의 사업"이란 다음 각 호의 사업을 말한다. 1. 정보통신서비스제공자의 정보보호 강화를 위한 정책의 조사, 연구 및 구축 지원 2. 정보통신서비스 이용에 따른 침해사고 분석 및 대책 연구 3. 정보보호 최고책임자 교육 등 정보통신서비스제공자의 정보보호 능력 및 전문성 향상 4. 정보통신서비스 보안 관련 국제 교류 및 협력 5. 그 밖에 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 필요한 사업 **[본조신설 2012.8.17]**	
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.	**제37조(집적정보통신시설사업자의 보호조치)** ① 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자(이하 "집적정보통신시설사업자"라 한다)가 법 제46조 제1항에 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	**<집적정보 통신시설 보호지침, 제2012-29호, '12.3.15>** **제3조(출입자의 접근제어 및 감시)** ①집적정보통신시설을 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 ②사업자는 제1항에 따른 보호조치를 효율적으로 수행하기 위하

정보통신망법	정보통신망법 시행령	하위고시
	4. 정보통신시설의 안정적 운영을 위한 내부 관리계획(비상시 계획을 포함한다)의 구축 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. ③ 미래창조과학부장관은 제1항에 따른 보호조치의 이행확인을 하는 과정에서 다른 기관이 수행하는 업무와 관계되는 때에는 해당 기관과 미리 협의하여야 한다.	여 중앙감시실을 설치·운용하여야 한다. **제4조(각종 재난에 대비한 보호조치)** ①사업자는 집적정보통신시설에 안정적으로 전원을 공급하고 지진, 수해 및 화재 등으로 인한 전원공급이 중단되는 경우에 대비하기 위하여 다음 각 호에 해당하는 조치를 하여야 한다. 1. 전력관련시설(축전지설비, 자가발전설비, 수변전설비)의 상황 파악 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 ②사업자는 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 ③사업자는 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 ④사업자는 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, 철근콘크리트 및 내화 건축자재를 사용하고 방화문을 설치할 것 3. 누수에 의한 피해를 예방하기 위하여 주요시설의 천장 및 바닥은 방수시공을 할 것 **제5조(관리인원의 선발 및 배치)** ①사업자는 24시간 경비가 가능하도록 상근 경비원을 두어야 한다. ②사업자는 주요시설의 유지·관리를 수행하는 관련분야 2년이상의 경험이 있는 전문인력을 두어야 한다. ③사업자는 집적정보통신시설의 효율적 관리·운영을 위하여

정보통신망법	정보통신망법 시행령	하위고시
		제2항에 따른 전문인력과 소속 인력에 대한 교육·훈련을 실시하여야 한다. ④사업자는 집적정보통신시설의 보호를 위하여 다음 각 호에 해당하는 업무를 수행하는 관리책임자를 두어야 한다. 1. 집적정보통신시설 보호계획의 구축 2. 집적정보통신시설에 대한 물리적·기술적, 인적·제도적 안전성 점검 ·지도 3. 제3항에 따라 의한 교육·훈련의 실시 4. 기타 집적정보통신시설의 보호를 위하여 사업자가 지시하는 관리·감독 업무 **제6조(시설보호계획의 구축 및 시행)** ①사업자는 해킹·컴퓨터 바이러스 유포 등의 전자적 침해행위와 정전·화재 기타 각종 재난으로부터 집적정보통신시설을 보호하기 위하여 다음 각 호의 사항을 포함하는 계획(이하 "시설보호계획"이라 한다)을 구축·시행하여야 한다. 1. 시설 보호의 목적 및 범위 2. 시설보호 조직·인력의 구성 및 운영에 관한 사항 3. 시설보호를 위한 교육·훈련에 관한 사항 4. 침해사고 예방·대응 및 복구 대책 5. 기타 시설의 안전한 운영·관리를 위한 지침 ②사업자는 제1항에 따른 시설보호계획을 성실히 준수하여야 하며 업무환경의 변화 등으로 인하여 계획의 수정·보완이 필요한 경우에는 지체없이 검토·보완하여야 한다. **제7조(관리용 정보시스템 장비의 보호)** ①사업자는 집적정보통신시설의 관리·운영을 위하여 설치된 컴퓨터장치 및 네트워크 장비(이하 "관리용 정보시스템 장비"라 한다)를 보호하기 위하여 권한 없는 자의 접근을 제한하는 조치를 하여야 한다. ②사업자는 관리용 정보시스템 장비를 해킹·컴퓨터바이러스 유포 등의 전자적 침해행위로부터 보호하기 위하여 침입차단조치 등 필요한 조치를 하여야 한다. **제8조(세부기준)** 제3조부터 제7조까지에 따라 사업자가 의무적으로 준수하여야 하는 보호조치의 세부적인 기준은 별표와 같다. **제9조(검사의 실시)** ①방송통신위원회는 사업자가 제3조부터 제8조까지에 따른 보호조치 의무를 성실히 이행하였는지 여부를 확인하기 위하여 법 제64조제3항에 따른 검사(이하 "검사"라 한다)를 실시한다. ②방송통신위원회가 검사를 실시하는 때에는 법 제64조제10항에 따라 한국인터넷진흥원장(이하 "인터넷진흥원장"이라 한다)에게 필요한 지원을 요청할 수 있다. ③인터넷진흥원장은 제2항에 따라 검사를 지원하는 때에는 건축·전기설비에 관한 전문지식을 지닌 자, 정보보호에 관한 전

정보통신망법	정보통신망법 시행령	하위고시
		문지식을 지닌 자가 참여하는 전담반을 구성하여야 한다. ④인터넷진흥원장은 검사를 효율적으로 지원하기 위하여 전담반의 구성·운영, 지원 절차 및 방법에 관하여 필요한 사항을 정하여야 한다. **제10조(검사결과의 처리)** ①인터넷진흥원장은 제9조에 따라 검사를 지원한 때에는 그 결과를 방송통신위원회에 통지하여야 한다. **제11조(평가)** ①방송통신위원회는 사업자가 희망하는 때에는 인터넷진흥원장으로 하여금 사업자의 신청을 받아 집적정보통신시설의 안전·신뢰성에 대한 평가를 실시하게 할 수 있다. ②인터넷진흥원장은 제1항에 따른 평가를 실시하는 경우에는 평가기준, 절차 및 방법 등에 관하여 필요한 사항을 정하여야 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> 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]**	**제38조(보험가입)** ① 집적정보통신시설사업자는 법 제46조제2항에 따라 사업 개시와 동시에 책임보험에 가입하여야 한다. ② 제1항에 따라 사업자가 가입하영야 하는 책임보험의 최저보험금액은 별표 1과 같다. <개정 2011.8.29>	
제46조의3(정보보호 안전진단) 삭제 **[본조삭제 2012.2.17] [시행일 : 2013.2.18] 제46조의3**	**제39조(정보보호 안전진단의 방법 및 절차 등)** 삭제 **제40조(정보보호 안전진단의 수수료)** 삭제 **제41조(안전진단대상자의 범위)** 삭제 **제42조(정보보호 안전진단 확인증의 발급)** 삭제 **제43조(정보보호 안전진단 결과의 제출)** 삭제 **제44조(정보보호 기술인력의 자격기준)** 삭제	

정보통신망법	정보통신망법 시행령	하위고시
	제45조(정보보호컨설팅 수행실적) 삭제 **제46조(안전진단수행기관의 지정절차 등)** 삭제	
제47조(정보보호 관리체계의 인증) ① 미래창조과학부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 구축·운영하고 있는 자에 대하여 제3항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다. <개정 2012.2.17> ② 정보통신서비스제공자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다. <신설 2012.2.17> 1. 「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자 2. 집적정보통신시설 사업자 3. 연간 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자 ③ 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> ④ 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> ⑤ 미래창조과학부장관은 한국인터넷진흥원 또는 미래창조과학부장관이 지정한 기관(이하 "정보보호 관리체계 인증기관"이라 한다)으로 하여금 제1항 및 제2항에 따른 인증에 관한 업무를 수행하게 할 수 있다. <신설 2012.2.17> ⑥ 한국인터넷진흥원 및 정보보호 관리체계 인증기관은 정보보호 관리체계의 실효성 제고를 위하여 연 1회 이상 사후관리를 실시하고 그 결과를 미래창조과학부장관에게 통보하여야 한다. <신설 2012.2.17> ⑦ 제1항 및 제2항에 따라 정보보호 관리체계의 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다. <개정 2012.2.17> ⑧ 미래창조과학부장관은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 경우에는 인증을 취소할 수 있다.<신설 2012.2.17> 1. 거짓이나 그 밖의 부정한 방법으로 정보보호 관리체계 인증을 받은 경우 2. 제3항에 따른 인증기준에 미달하게 된 경우 3. 제6항에 따른 사후관리를 거부 또는 방해한 경우		**<정보보호 관리체계 인증 등에 관한 고시> 전부개정** **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 구축하여 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 구축하여 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 구축·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 구축·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.

정보통신망법	정보통신망법 시행령	하위고시
		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. **제28조(인증업무 지침)** 인터넷진흥원 또는 인증기관은 인증업무 수행을 위해 필요한 경우 인증업무에 관한 지침을 마련하여 시행할 수 있다. **제29조(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 2016년 2월 17일까지로 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 시행 당시 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.
⑨ 제1항 및 제2항에 따른 인증의 방법·절차·범위·수수료, 제6항에 따른 사후관리의 방법·절차, 제8항에 따른 인증취소의 방법·절차, 그 밖에 필요한 사항은 대통령령으로 정한다. <개정 2012.2.17>	**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 포함	

정보통신망법	정보통신망법 시행령	하위고시
[시행일 : 2013.2.18] 제47조	된 정보보호 관리체계 명세서(전자문서를 포함한다)를 첨부하여 인터넷진흥원 또는 미래창조과학부장관이 지정한 기관(이하 “정보보호 관리체계 인증기관”이라 한다)에 제출하여야 한다. 1. 정보보호 관리체계의 범위 2. 정보보호 관리체계의 범위에 포함되어 있는 주요 정보통신설비의 목록과 시스템 구성도 3. 정보보호 관리체계를 구축·운영하는 방법과 절차 4. 정보보호 관리체계와 관련된 주요 문서의 목록 5. 정보보호 관리체계와 관련된 국내외 품질경영체제의 인증을 취득한 경우에는 그 명세	
	② 인터넷진흥원 또는 정보보호 관리체계 인증기관은 제1항에 따른 신청을 받은 때에는 법 제47조제3항에 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.	**제18조(인증기준)** 인증기준은 별표 6과 같다.
	③ 법 제47조제1항 및 제2항에 따른 정보보호 관리체계 인증심사는 관리체계인증고시에 따라 서면심사 또는 현장심사의 방법으로 실시한다. ④ 제3항에 따른 심사는 제53조제1항제1호에 따른 인증심사원만 수행할 수 있다. ⑤ 인터넷진흥원 또는 정보보호 관리체계 인증기관은 제3항에 따른 인증심사의 결과를 심의하기 위하여 정보보호에 관한 학식과 경험이 풍부한 자를 위원으로 하는 인증위원회를 설치·운영하여야 한다. ⑥ 인터넷진흥원 또는 정보보호 관리체계 인증기관은 제5항에 따른 인증위원회의 심의 결과 관리체계인증고시에 적합한 때에는 그 인증신청을 한 자에게 정보보호 관리체계 인증서를 발급하여야 한다.	
	⑦ 제1항부터 제6항까지에서 규정한 사항 외에 인증신청, 인증심사, 인증위원회의 설치·운영 및 인증서의 발급 등에 필요한 세부사항은 미래창조과학부장관이 정하여 고시한다. **[전문개정 2012.8.17, 종전 제47조를 제53조로 이동하고, 종전 제50조를 제47조로 이동]**	**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 인증신청서를 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

정보통신망법	정보통신망법 시행령	하위고시
		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. **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 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 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 **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

정보통신망법	정보통신망법 시행령	하위고시
		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.
		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.
	제48조(정보보호 관리체계 인증의 수수료) ① 제47조제1항에 따라 인증을 신청하는 자는 인터넷진흥원 또는 정보보호 관리체계 인증기관에 수수료를 납부하여야 한다. ② 미래창조과학부장관은 인증심사에 투입되는 인증심사원의 수, 인증심사에 필요한 일수 등을 고려하여 정보보호 관리체계 인증 수수료 산정을 위한 구체적인 기준을 정하여 고시한다. **[본조신설 2012.8.17, 종전 제48조를 제53조의2로 이동]**	**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

정보통신망법	정보통신망법 시행령	하위고시
		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.
	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. 1. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자 2. 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 100만명 이상인 자 **[본조신설 2012.8.17, 종전 제49조를 제53조의3으로 이동]** ※ 규제심사에서 영세 VIDC 면제조항 삭제(고시에 반영)	**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.
	제50조 삭제 **[본조삭제 2012.8.17, 종전 제50조를 제47조로 이동]** ※ 법제처 심사시 제50조(정보보호 관리체계 인증에 관한 업무의 범위) 신설조문 삭제(고시에 반영)	
	제51조(인증의 사후관리) ① 법 제47조제6항에 따른 사후관리는 서면심사 또는 현장심사의 방법으로 실시한다. ② 인터넷진흥원 또는 정보보호 관리체계 인증기관은 제1항에 따른 사후관리를 실시한 결과 법 제47조제8항 각 호의 사유를 발견한 경우에는 제47조제5항에 따른 인증위원회의 심의를 거쳐 그 결과를 미래창조과학부장관에게 통보하여야 한다. **[전문개정 2012.8.17, 종전 제51조(인증의 유효기간)를 삭제하고 종전 제52조를 제51조로 이동]**	
	제52조(인증표시 및 홍보) 법 제47조제1항 및 제2항에 따라 정보보호 관리체계 인증을 받은 자는 같은 조 제7항에 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. **[전문개정 2012.8.17, 종전 제52조를 제51조로 이동하고, 종전 제53조를 제52조로 이동]**	**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.
	제53조(정보보호 관리체계 인증기관의 지정기준) ① 법 제47조	

정보통신망법	정보통신망법 시행령	하위고시
	제5항에 따른 정보보호 관리체계 인증기관의 지정기준은 다음 각 호와 같다. 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. **[전문개정 2012.8.17, 종전 제53조를 제52조로 이동하고, 종전 제47조를 제53조로 이동]**	**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 기준

정보통신망법	정보통신망법 시행령	하위고시
		을 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. **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 지정신청을 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.
⑩ 정보보호 관리체계 인증기관 지정의 기준·절차·유효기간 등에 필요한 사항은 대통령령으로 정한다.<개정 2012.2.17> **[전문개정 2008.6.13]** **[시행일 : 2013.2.18] 제47조**	**제53조의2(정보보호 관리체계 인증기관의 지정절차 등)** ① 법 제47조제5항에 따라 정보보호 관리체계 인증기관으로 지정을 받으려는 자는 정보보호 관리체계 인증기관 지정신청서(전자문서로 된 신청서를 포함한다)에 다음 각 호의 서류(전자문서를 포함한다)를 첨부하여 미래창조과학부장관에게 제출하여야 한다. 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. ③ 미래창조과학부장관은 제1항에 따른 지정신청을 받은 경우에는 제53조제1항에 따른 지정기준 충족 여부를 심사하여 신청을 받은 날부터 3개월 이내에 그 결과를 신청인에게 통지하고, 정보보호 관리체계 인증기관으로 지정되는 신청인에게 정보보호 관리체계 인증기관 지정서를 발급하여야 한다. 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.	**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 인증심사원의 보유현황과 이를 증명할 수 있는 서류 3. 영 제53조의2제1항제3호에 따른 별표 1의 업무수행 요건·능력 심사를 위하여 필요한 서류 **제6조(인증기관 지정서)** 영 제53조의2제3항에 따른 정보보호 관리체계 인증기관 지정서는 별지 제3호서식과 같다.

정보통신망법	정보통신망법 시행령	하위고시
	⑤ 삭제 **<'12.6.25, 행안부 정부위원회 정비계획>** **[전문개정 2012.8.17, 종전 제48조를 제53조의2로 이동]**	
	제53조의3(정보보호 관리체계 인증기관 지정의 유효기간) ① 제53조의2에 따른 정보보호 관리체계 인증기관 지정의 유효기간은 3년으로 한다.	
	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.	**제8조(인증기관 재지정)** ① 인증기관은 유효기간이 끝나기 전 6개월부터 끝나는 날까지 별지 제1호서식에 따라 방송통신위원회에 재지정 신청을 할 수 있다.
	③ 제2항에 따른 재지정에 관하여는 제53조, 제53조의2 및 제1항을 준용한다.	② 제1항에 따른 재지정의 심사, 재지정 결과 통지, 재지정서 교부 등에 관하여는 영 제53조의2제3항을 준용한다.
	[전문개정 2012.8.17, 종전 제49조를 제53조의3으로 이동]	
	제53조의4(정보보호 관리체계 인증기관의 사후관리) ① 정보보호 관리체계 인증기관은 전년도 인증실적 보고서를 매년 1월 31일까지 미래창조과학부장관에게 제출하여야 한다.	**제7조(인증기관의 사후관리)** 영 제53조의4제1항에 따른 인증기관의 전년도 인증실적 보고서는 별지 제4호서식과 같다.
	② 미래창조과학부장관은 법 제47조의2제1항 각 호에 해당하는지를 확인하기 위하여 필요한 경우 정보보호 관리체계 인증기관에 대하여 자료의 제출을 요구하거나 현장실사를 할 수 있다. **[본조신설 2012.8.17]**	
제47조의2(정보보호 관리체계 인증기관의 지정취소 등) ① 미래창조과학부장관은 제47조에 따라 정보보호 관리체계 인증기관으로 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. 1. 거짓이나 그 밖의 부정한 방법으로 정보보호 관리체계 인증기관의 지정을 받은 경우 2. 업무정지기간 중에 인증을 한 경우 3. 정당한 사유 없이 인증을 하지 아니한 경우 4. 제47조제9항을 위반하여 인증을 한 경우 5. 제47조제10항에 따른 지정기준에 적합하지 아니하게 된 경우 ② 제1항에 따른 지정취소 및 업무정지 등에 필요한 사항은 대통령령으로 정한다.	**제54조(지정취소 등의 기준)** 법 제47조의2에 따른 지정취소 및 업무정지에 관한 행정처분의 기준은 별표 4와 같다.	
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 구축·운영하고 있는 자에 대하여 제2항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.	**제54조의2(개인정보보호 관리체계의 인증)** 법 제47조의3에 따른 개인정보보호 관리체계 인증의 방법·절차·범위·수수료·사후관리 및 인증기관 지정의 기준·절차·유효기간·취소 등에 대해서는 제47조, 제48조, 제51조부터 제53조까지, 제53조의2부터 제53조의4까지 및 제54조를 준용한다. **[본조신설 2012.8.17]**	**<개인정보보호 관리체계 인증 등에 관한 고시> 별도제정**

정보통신망법	정보통신망법 시행령	하위고시
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 제47조제5항부터 제10항까지의 규정을 준용한다. 이 경우 "제1항 및 제2항"은 "제1항"으로 본다. ④ 개인정보보호 관리체계 인증기관의 지정취소 등에 대하여는 제47조의2를 준용한다. **[본조신설 2012.2.17] [시행일 : 2013.2.18]** **[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 주요정보통신서비스제공자는 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. **[제47조의3에서 이동 <2012.2.17>] [시행일 : 2012.8.18]**	**제55조(이용자 보호조치의 요청에 관한 약관사항)** 법 제47조의4제4항에 따라 이용자에 대한 보호조치의 요청에 관하여 이용약관으로 정하여야 하는 사항은 다음 각 호와 같다. 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	
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. ② 미래창조과학부장관은 한국인터넷진흥원으로 하여금 제1항에 따른 등급 부여에 관한 업무를 수행하게 할 수 있다. 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.	**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. **[본조신설 2012.8.17]**	**<정보보호 관리등급 부여에 관한 고시> 추후 제정**
	제55조의3(정보보호 관리등급 부여의 방법 및 절차) ① 법 제47조의5제1항에 따라 정보보호 관리등급을 부여받으려는 자는 정보보호 관리등급 신청서(전자문서로 된 신청서를 포함한다)에 정	

정보통신망법	정보통신망법 시행령	하위고시
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] [시행일 : 2013.2.18] 제47조의5**	보보호 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. **[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]**	
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]		
제72조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다. 5. 제66조를 위반하여 직무상 알게 된 비밀을 타인에게 누설하거나 직무 외의 목적으로 사용한 자 ② 제1항제1호의 미수범은 처벌한다. [전문개정 2008.6.13]		
제76조(과태료) ③ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.	**제74조(과태료의 부과기준)** 법 제76조제1항부터 제3항까지의 규정에 따른 과태료의 부과기준은 별표 9와 같다.	

정보통신망법	정보통신망법 시행령	하위고시
6. 제47조제2항을 위반하여 정보보호 관리체계 인증을 받지 아니한 자 7. 제47조제7항 및 제47조의3제3항을 위반하여 인증받은 내용을 거짓으로 홍보한 자 **[전문개정 2008.6.13]** **[시행일 : 2013.2.18] 제76조제3항제6호,제76조제3항제7호**	**별표 9 과태료의 부과기준(제74조 관련)** 2. 개별기준 (단위: 만원) 위반행위 / 근거 법조문 / 위반횟수별 과태료 금액 (1회 / 2회 / 3회 이상) 어. 법 제47조제2항을 위반하여 정보보호 관리체계 인증을 받지 않은 경우 / 법 제76조제3항제6호 / 1,000 / 1,000 / 1,000 저. 법 제47조제7항 및 제47조의3제3항을 위반하여 인증받은 내용을 거짓으로 홍보한 경우 / 법 제76조제3항제7호 / 300 / 600 / 1,000 **<개정 2012.8.17> [시행일:2013.2.18] 제2호어목·저목**	
부칙 <법률 제11322호, 2012.2.17> **제3조(정보보호 안전진단의 폐지에 따른 경과조치)** 이 법 시행 당시 종전의 규정에 따라 정보보호 안전진단을 받은 사업자는 정보보호 안전진단을 받은 해당 연도에는 제47조제2항의 개정 규정에 따른 정보보호 관리체계 인증을 받은 사업자로 본다.		

[붙임 9] 인증 기준 세부점검항목

< 정보보호관리과정 >

No	관리과정	No	세부관리과정	관리과정 상세내용	점검항목	설명
1	정보보호정책수립 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.	조직이 수행하는 모든 정보보호 활동의 근거가 될 수 있는 최상위 수준의 정보보호정책이 있는가?	ㅇ 조직이 수행하는 모든 정보보호 활동의 근거가 될 수 있도록 다음과 같은 항목이 포함된 최상위 수준의 정보보호정책을 수립하여야 한다. - 최고경영자 등 경영진의 정보보호에 대한 의지 및 방향 - 조직의 정보보호 목적, 범위, 책임 - 조직이 수행하는 관리적, 기술적, 물리적 정보보호 활동의 근거 ㅇ 정보보호 상위 정책을 시행하기 위한 세부적인 수행주체, 방법, 절차 등은 정보보호 지침, 절차, 매뉴얼 등의 형식으로 수립하여야 한다.
					정보보호정책은 조직이 제공하고 있는 사업 등에 관련된 정보보호 관련 법적 요구사항을 반영하여 수립하고 있는가?	ㅇ 제공하는 사업(서비스)에서 조직이 준수해야 하는 정보보호 관련 법적 요구사항을 분석하고 정보보호정책에 반영하여야 한다. - 정보보호정책에 조직이 준수하여야 하는 법령 및 관련조항을 명시하여야 함 - 정보보호정책에 법적 요구사항이 반영될 경우 법률적 지식이 있는 조직 내 관련 부서 또는 관련자의 검토를 거치는 것이 좋다. ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 - 개인정보보호법 - 신용정보의 이용 및 보호에 관한 법률 - 위치정보보호에 관한 법률 - 전자금융거래법 - 신용정보 이용 및 보호에 대한 법률 - 전자상거래 등에서의 소비자보호에 대한 법률 - 저작권법 - 정보통신 기반보호법

No	관리과정	No	세부관리과정	관리과정 상세내용	점검항목	설명
						- 산업기술의 유출방지 및 영업비밀보호에 관한 법률 - 부정경쟁방지 및 영업비밀보호에 관한 법률 등
		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.	조직의 사업(서비스)에 영향을 줄 수 있는 핵심자산을 포함하도록 범위를 선정하고 있는가?	ㅇ 정보보호 관리체계 범위에는 사업(서비스)와 관련된 임직원, 정보시스템, 정보, 시설 등 유·무형의 핵심자산이 누락 없이 포함되어야 한다.
					정보보호 관리체계 범위를 설명하기 위하여 다음과 같은 내용이 포함된 문서를 작성하고 있는가? - 주요 서비스 및 업무 현황 - 서비스 제공과 관련된 조직 - 정보보호 조직, 주요 설비 목록 - 정보시스템 목록 및 네트워크 구성도 - 문서 목록 (예 : 정책, 지침, 매뉴얼, 대책명세서 등) - 정보보호 관리체계 수립 방법 및 절차 등	ㅇ 정보보호 관리체계의 범위 내 서비스, 업무, 조직, 정보시스템, 설비 등을 명확하게 정의하여 정보보호 관리체계 범위를 충분하게 설명하여야 한다. ㅇ 정보보호 관리체계 범위가 특정 영역에만 해당되는 경우, 범위 영역 경계를 식별하여 문서화하고 범위가 일부일 경우 전체사업 대비 해당 범위를 명확하게 식별할 수 있도록 하여야 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.	경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 등의 책임과 역할을 문서화하고 있는가?	ㅇ 정보보호 관리체계 수립 및 운영을 위한 정보보호정책의 제·개정 승인 및 공표, 위험관리, 내부감사 등과 같은 중요한 사안에 대해 경영진이 참여하여 의사결정을 할 수 있도록 경영진의 책임과 역할을 정보보호정책에 명시하여야 한다.
					경영진 또는 경영진의 권한을 위임받은 자가 정보보호 관리체계 내 중요한 활동 내용을 보고 받고 의사결정에 참여하고 있는가?	ㅇ 정보보호 관리체계에서 경영진이 참여하는 중요한 활동을 정의하고 그에 따른 보고체계를 갖추어야 한다. ㅇ 정보보호 관리체계 내 중요한 활동에 대해 경영진은 직접 또는 권한 위임을 통해 보고를 받고 의사결정에 참여하여야 한다.
		2.2	정보보호 조직 구성 및 자원 할당	최고경영자는 조직의 규모, 업무 중요도 분석을 통해 정보보호 관리체계의 지속적인 운영이 가능하도록 정보보호 최고책임자, 실무조	조직의 규모, 업무 중요도 등의 특성을 고려하여 정보보호 관리체계 구축·운영 활동을 지속적으로 수행할 수 있는 정보보호 조직(CISO, 실무조직, 정보보호위원회 등)을 구성하고 있는가?	ㅇ 최고경영자는 정보보호 관리체계의 지속적인 운영이 가능하도록 조직의 규모, 업무 중요도 등에 따라 요구되는 정보보호 조직을 구성하여야 한다.

No	관리과정	No	세부관리과정	관리과정 상세내용	점검항목	설명
				직 등 정보보호 조직을 구성하고 정보보호 관리체계 운영 활동을 수행하는데 필요한 자원(예산 및 인력)을 확보하여야 한다.	최고경영자는 정보보호 관리체계 구축 · 운영에 소요되는 자원을 평가하여 필요한 예산과 인력을 승인하고 있는가?	ㅇ 최고경영자는 정보보호 관리체계 구축 및 운영을 하는데 필요한 자원을 파악하여 예산 및 인력운영계획을 승인하여야 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.	정보보호 및 개인정보보호를 위한 관리적, 물리적, 기술적, 법적 분야 등 다양한 측면에서 발생할 수 있는 위험을 식별하고 평가할 수 있는 방법을 정의하여 문서화하고 있는가?	ㅇ 관리적, 기술적, 물리적, 법적 분야 등 조직 전 영역에 대한 위험식별 및 평가가 가능하도록 각 영역별 특성을 반영한 위험관리 방법을 선정하여야 하며 그 방법과 절차를 지침으로 규정하여야 한다. ※ 참고 ※ - 관리적, 물리적, 법적분야 : 베이스라인 접근법 - 기술적분야 : 상세위험분석 또는 복합접근법 ㅇ 핵심자산에 대한 기술적 위험분석의 경우 상세위험분석(자산 중요도, 위협, 취약점)을 수행하는 것이 바람직하다.
					매년 위험관리를 수행하기 위하여 전문인력 구성, 기간, 대상, 방법, 예산 등을 구체화한 위험관리계획을 수립 · 이행하고 있는가?	ㅇ 위험관리 방법 및 절차에 따라 매년 위험관리 계획을 수립하고 이행하여야 하며 계획에는 다음과 같은 내용을 포함하여야 한다. - 위험관리 대상 : 정보보호 관리체계 인증범위 내 핵심자산 및 서비스를 누락 없이 포함 - 위험관리 수행인력 : 위험관리 방법, 조직의 업무 및 시스템에 대한 전문성을 갖춘 인력과 관련 부서 실무책임자가 참여 (위험관리 전문가, 정보보호관리자, IT 실무 책임자, 현업부서 실무 책임자 등) - 위험관리 기간 등
		3.2	위험 식별 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.	정보보호 관리체계 범위 전 영역에 대한 위험식별 및 평가를 연 1회 이상 수행하고 있는가?	ㅇ 매년 정보보호 관리체계 범위 전체를 대상으로 위험식별과 평가를 수행하여야 하며 기 적용된 정보보호대책의 실효성 검토도 함께 이루어져야 한다.
					정보보호 및 개인정보보호 관련 법적 준거성 위험을 식별하고 있는가?	ㅇ 정보보호 및 개인정보 관련 법적 요구사항 준수여부에 대한 위험을 식별하여야 한다.

No	관리과정	No	세부관리과정	관리과정 상세내용	점검항목	설명
						※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 - 전자금융거래법 - 개인정보보호법 - 부정경쟁방지 및 영업비밀보호에 관한 법률 등
					정보보호 관리체계 통제항목 또는 별도의 기준으로 관리적, 운영적, 물리적 위험을 식별하고 있는가?	ㅇ 관리적, 운영적, 물리적 위험은 정보보호 관리체계 통제항목이 적용되고 있는지 점검하여 통제적용이 이루어지지 않거나 미흡한 경우 위험으로 식별하여야 한다.
					정보보호 관리체계 인증범위 내의 정보시스템 자산에 대해 취약점 점검을 통한 기술적 위험을 식별하고 있는가?	ㅇ 기술적 위험은 정보보호 관리체계 범위 내의 정보시스템(서버, 네트워크 장비, 응용 프로그램 등), 정보보호시스템 등에 대한 취약점 점검(점검툴 사용, 체크리스트 사용, 침투시험 등)을 수행하여 발견된 취약점을 위험으로 식별하여야 한다.
					식별된 위험에 대한 위험도를 산정하고 있는가?	ㅇ 식별된 위험이 실제 조직에 미치는 영향(잠재적 손실)을 고려하여 위험도를 산정하여야 하며 이를 위하여 위험도 산정기준을 마련하여야 한다.
					조직에서 수용 가능한 목표 위험수준을 정하고 그 수준을 초과하는 위험을 식별하고 있는가?	ㅇ 식별된 위험과 각 위험도를 검토하여 수용 가능한 목표 위험수준(DoA : Degree of Assurance)을 정한 뒤 이를 초과하는 위험을 식별하여야 한다. 이 수준은 논리적이거나 수리적인 방법을 통해 계산될 필요는 없으나 반드시 정보보호 최고책임자 등 경영진의 의사결정에 의해 설정되어야 한다.
					위험 식별 및 평가 결과를 정보보호 최고책임자 등 경영진이 이해하기 쉽게 작성하여 보고하고 있는가?	ㅇ 식별된 위험에 대한 평가 보고서를 정보보호 최고책임자를 포함한 경영진이 손쉽게 이해할 수 있도록 작성하여 보고하여야 한다.
		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 이행	식별된 위험에 대한 처리 전략(위험감소, 위험회피, 위험전가, 위험수용 등)을 수립하고 위험처리를 위한 정보보호대책을 선정하고 있는가?	ㅇ 위험 식별 및 평가 결과에 근거하여 정보보호대책을 선정하고 정보보호 관리체계 인증 기준에서 제시하는 정보보호 대책 통제항목(92개)과의 연계성도 함께 고려하여야 한다. ㅇ 위험수준 감소를 목표로 위험처리 전략을 수립하는 게 일반적이며 위험회피, 위험전가, 위험수용 등으로 고려할 수 있다.

No	관리과정	No	세부관리과정	관리과정 상세내용	점검항목	설명
				계획을 수립하여 경영진의 승인을 받아야 한다.		ㅇ 수용 가능한 위험 수준을 초과하지 않은 위험 중 기업 및 외부 환경에 따라 위험 수준이 상승할 가능성이 높거나 조직이 중요하다고 판단하는 부분에 대해서는 필요시 보호대책 수립을 고려할 수 있다. ㅇ 특별한 사유(예 : 대책 적용 대상 자산 無)로 인해 위험수용 전략을 선택하는 경우 경영진, 정보보호 관리체계 인증 심사 팀 등 조직 내·외부에서 객관적으로 인정하는 경우에 가능하다.
					정보보호대책 구현의 우선순위를 정한 후에 일정, 담당부서 및 담당자, 예산 등의 항목을 포함한 정보보호대책 이행계획을 수립하고 정보보호 최고책임자 등 경영진의 승인을 받고 있는가?	ㅇ 위험수준의 감소를 위하여 선정한 정보보호대책은 위험처리의 시급성, 예산 할당, 구현에 요구되는 기간에 따라 이행 우선순위를 정하고 계획을 수립하여야 한다. ㅇ 정보보호 대책의 효과적인 이행을 위하여 이행계획을 정보보호 최고책임자 등 경영진의 승인을 얻고 이행여부를 확인하기 위한 절차 및 방법도 함께 고려하여야 한다.
4	정보보호대책 구현	4.1	정보보호대책의 효과적 구현	정보보호대책 이행계획에 따라 보호대책을 구현하고 경영진은 이행결과의 정확성 및 효과성 여부를 확인하여야 한다.	정보보호대책 이행계획에 따라 정보보호대책을 구현하고 그 이행결과를 정보보호 최고책임자 등 경영진에게 보고하고 있는가?	ㅇ 식별된 위험에 대한 위험수준이 감소되었음을 보장하기 위하여 정보보호 최고책임자 등 경영진은 정보보호대책이 이행계획에 따라 빠짐없이 효과적으로 이행되었는지 여부를 검토 및 확인하여야 한다.
					정보보호 관리체계 인증기준 통제항목별(관리과정 및 정보보호 대책 총 104 개)로 정보보호대책 구현 및 운영 현황을 기록한 '정보보호 대책명세서'를 작성하고 있는가?	ㅇ '정보보호 대책명세서'는 정보보호 관리체계 인증기준에서 제시하는 통제항목별 운영현황을 확인할 수 있도록 다음과 같은 내용을 포함하여야 한다. - 통제항목 선정여부(Yes/No) 확인 : 관리과정 12 개 통제항목은 필수사항 - 운영 현황 - 관련문서 (정책, 지침 등) - 기록 (증적자료) - 통제항목 미선정 시 사유

No	관리과정	No	세부관리과정	관리과정 상세내용	점검항목	설명
						ㅇ 미선정 통제항목이 있을 경우, 미선정 사유를 명확하게 명시하고 정보보호 최고책임자 등 경영진의 승인을 득하여 부주의 또는 의도적으로 통제항목 선정이 배제되지 않도록 하여야 한다.
		4.2	내부 공유 및 교육	구현된 정보보호대책을 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여야 한다.	구현된 정보보호대책 운영 및 시행부서 담당자를 대상으로 관련내용 공유 및 교육을 수행하고 있는가?	ㅇ 정보보호 관리체계를 내재화하기 위하여 다음과 같은 사항으로 정보보호 활동업무에 영향이 발생하는 경우, 관련부서 및 담당자를 파악하여 정보보호대책의 내용을 공유하고 교육을 수행하여야 한다. - 정책(지침 및 절차 포함) 신규 제정 및 개정 - 정보시스템 신규 도입 및 개선 등
5	사후관리	5.1	법적요구사항 준수검토	조직이 준수해야 할 정보보호 관련 법적요구사항을 지속적으로 파악하여 최신성을 유지하고 준수여부를 지속적으로 검토하여야 한다.	조직이 준수해야 하는 개인정보 및 정보보호 관련 법적 요구사항(법규명, 관련 조항, 세부내용 등)의 준수여부를 주기적(최소 연 1 회 이상)으로 검토하고 있는가?	ㅇ 정보보호 관리체계 구축 및 운영에 있어서 조직이 준수해야 하는 법령의 관련 조항, 세부내용을 파악하고 준수여부를 주기적으로 검토할 수 있는 절차를 수립하여야 한다. (관리과정 1.1 정보보호정책의 수립, 3.2 위험 식별 및 평가 참고) ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 - 전자금융거래법 - 개인정보보호법 - 부정경쟁방지 및 영업비밀보호에 관한 법률 등 ㅇ 관련 법규의 제·개정 현황을 최소 연 1 회 이상 검토하여 조직에 미치는 영향을 분석하고 조직의 정책 및 절차에 바로 반영하여 법규 미준수로 인한 과태료 부과 등과 같은 상황이 발생하지 않도록 대응하여야 한다.
					조직이 준수해야 할 법적 요구사항은 최신성을 유지하고 있는가?	ㅇ 조직이 준수해야 할 법규가 존재하는 경우 법적 요구사항을 명시한 문서(지침 등), 해당 법규 준거성을 점검하기 위한 체크리스트는 최신 법규 사항을 반영하고 있어야 한다.

No	관리과정	No	세부관리과정	관리과정 상세내용	점검항목	설명
		5.2	정보보호 관리체계 운영현황 관리	정보보호 관리체계 범위 내에서 주기적 또는 상시적으로 수행해야 하는 활동을 문서화하고 그 운영현황을 지속적으로 관리하여야 한다.	정보보호 관리체계 운영을 위한 정보보호 활동의 수행 주기를 손쉽게 확인할 수 있도록 문서화하고 최신성 여부를 주기적으로 검토하고 있는가?	ㅇ 조직 내 정책, 지침, 절차 등에 규정화 되어 있는 정보보호 관리체계 운영활동을 식별하고 그 운영현황을 확인할 수 있도록 수행 주기, 수행 주체(담당부서, 담당자)를 정의한 문서(운영현황표)를 관리하고 최신성을 유지하여야 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.	법적 요구사항 및 수립된 정책에 따라 정보보호 관리체계가 효과적으로 운영되는지 여부를 검토하기 위한 내부감사를 수행하기 위하여 감사기준, 범위, 주기, 감사인력 자격요건 등을 정의하고 있는가?	ㅇ 법적 요구사항 및 조직 내 수립된 정보보호정책에 따라 정보보호 관리체계 활동이 효과적으로 수행되는 지 여부를 검토하기 위하여 다음과 같은 항목이 정의된 내부감사 지침을 수립하여야 한다. - 내부감사 기준 - 내부감사 범위 - 내부감사 수행 주기 (예 : 연 1회 이상) - 감사인력 자격요건 : 감사의 객관성을 확보하기 위해 제3자가 감사를 수행하는 것이 원칙임. 다만, 불가피한 경우 제3자 인력을 포함하여 정보보호조직이 감사를 수행할 수 있음
					내부감사 지침에 따라 연 1회 이상의 내부감사 계획을 수립하여 정보보호 최고책임자 등 경영진에게 보고한 후 계획에 따라 내부감사를 수행하고 있는가?	ㅇ 내부감사 지침에 따라 연 1회 이상 감사가 수행될 수 있도록 연간 계획을 수립한 후 정보보호 최고책임자 등 경영진에게 보고하여 승인을 득한 후 계획에 따라 내부감사를 수행하여야 한다.
					내부감사에서 발견된 지적사항에 대해 보완조치 여부를 확인하여 정보보호 최고책임자 등 경영진에 보고하고 있는가?	ㅇ 내부감사 중 지적사항이 발견된 경우 일정 기간 동안 피감사 부서 혹은 담당자가 대책을 마련하여 보완하게끔 한 후 보완조치여부를 확인하여야 한다. ㅇ 감사결과 보고서에 다음과 같은 내용을 작성하여 정보보호 최고책임자 등 경영진 등에게 보고하여야 한다. - 일정 및 범위 - 감사 내용 (감사 방법, 검토 문서, 면담자 등) - 지적사항 및 보완조치 내용 (보완조치 완료 여부, 대책 등 포함) 등

< ***정보보호대책_1. 정보보호정책*** >

No	통제분야	No	통제항목	통제목적	점검항목	설명
1.1	정책의 승인 및 공표	1.1.1	정책의 승인	정보보호정책은 이해관련자의 검토와 최고경영자의 승인을 받아야 한다.	정보보호정책 및 정책시행 문서(지침, 절차 등)의 제·개정 시 이해관련자의 검토를 받고 있는가?	ㅇ 정책은 정보보호 활동을 규정한 상위 정보보호정책과 상위 정책 시행을 위한 문서(지침, 절차, 매뉴얼 등)로 구분하여 제정할 수 있다. ㅇ 문서의 제 · 개정 시에는 이해 관련자의 검토(협의 및 조정 등)를 통해 조직 내에서 실제 수행하고 있는 정보보호 활동이 내용에 반영될 수 있도록 하여야 한다. - 또한, 실무협의회를 운영하고 있는 경우 이 협의회를 통해 검토할 수 있다. ㅇ 이해관련자는 상위정책과 정책시행 문서의 시행주체가 되는 부서 및 담당자(정보보호부서, 정보시스템 운영 및 개발 부서, 현업부서)를 의미한다.
					정보보호정책 제 · 개정 시 최고경영자의 승인을 받고 있는가?	ㅇ 정보보호 활동에 대한 최고경영자 등 경영진의 참여와 지원을 보장하기 위하여 상위 수준의 정보보호정책은 최종적으로 최고경영자의 승인을 받아야 한다.
					지침, 절차 등 정책시행 문서 제 · 개정 시 최고경영자의 위임을 받은 책임자(CISO 등)의 승인을 받고 있는가?	ㅇ 정책시행을 위하여 필요한 세부 방법, 절차, 주기 등을 규정한 정보보호 지침, 절차, 매뉴얼의 제·개정 시 최고경영자의 위임 규정에 따라 정보보호 최고책임자 등의 승인을 받아야 한다.
		1.1.2	정책의 공표	정보보호정책 문서는 모든 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.	정보보호정책 및 정책시행 문서의 제 · 개정 시 그 내용을 관련 임직원에게 공표하고 있는가?	ㅇ 정보보호정책 및 정책시행 문서의 제 · 개정 시 그 내용과 시행사실을 관련 임직원이 알 수 있도록 공표(교육, 메일, 게시판 등 활용)하여야 한다.
					정보보호정책 및 정책시행 문서를 관련 임직원에게 이해하기 쉬운 형태로 전달하고 최신본으로 제공하고 있는가?	ㅇ 정보보호정책 및 정책시행 문서를 관련 임직원이 용이하게 참고할 수 있는 형태(예 : 전자게시판, 책자, 교육자료 등)로 전달하여야 하며 최신 정책 및 정책시행 문서를 언제든지 확인할 수 있도록 하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
1.2	정책의 체계	1.2.1	상위 정책과의 연계성	정보보호정책은 상위조직 및 관련 기관의 정책과 연계성을 유지하여야 한다.	정보보호정책이 상위 조직 및 관련기관의 정책과 연계성이 있는 지 검토하고 있는가?	ㅇ 정보보호정책이 상위조직 및 관련 기관 정보보호정책과의 연계성이 있는 지 분석하여 내용상 상호 부합되지 않은 요소가 있는 지 확인하고 정책간 상하체계가 적절한 지 여부를 검토하여야 한다. (예 : 자회사의 경우 본사 정책과의 연계성 검토 등)
		1.2.2	정책시행 문서수립	정보보호정책의 구체적인 시행을 위한 정보보호지침, 절차를 수립하고 관련 문서간의 일관성을 유지하여야 한다.	정보보호정책의 시행을 위하여 필요한 세부적인 방법, 절차, 주기 등을 규정한 정보보호 지침, 절차, 매뉴얼 등을 수립하고 있는가?	ㅇ 임직원이 상위 정보보호정책에서 정한 정보보호 활동을 일관성 있게 수행하기 위해서는 시행주체(책임과 역할 정의), 방법, 주기 등을 구체적으로 정한 정보보호 지침, 절차, 매뉴얼 등을 수립하여야 하며 필요한 경우 서비스별, 시스템별 지침, 절차를 별도로 마련하여야 한다. ㅇ 담당자에 의한 임의적, 임기응변식 정보보호 활동 수행은 지양하여야 하며 정보보호 활동은 관련 근거 규정을 반드시 제시할 수 있어야 한다.
					정보보호정책과 지침, 절차 등과 같은 정책시행 문서 간 내용의 일관성 여부를 검토하고 유지하고 있는가?	ㅇ 정책, 지침, 절차에서 정하고 있는 정보보호 활동의 주기, 수준, 방법 등을 일관성 있게 유지하여야 한다. (예 : 시스템 대상 패스워드 복잡도 기준이 각 문서별로 다르게 기술되어 있을 경우 문서 간 일관성이 결여되어 있다고 할 수 있음)
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.	정보보호정책 및 정책시행 문서의 정기적 타당성 검토 절차를 수립하고 있는가?	ㅇ 다음과 같은 상황이 발생한 경우를 포함하여 주기적으로 정보보호정책 및 정책시행 문서의 타당성을 검토하여 제·개정을 통해 관련 문서에 반영하여야 한다. - 내부감사 수행 결과 - 중대한 보안사고 발생 - 개인정보 및 정보보호 관련 법령 제·개정 - 새로운 위협 또는 취약점 발견 - 정보보호 환경의 중대한 변화 - 조직 사업 환경의 변화 (예 : 신규 사업)

No	통제분야	No	통제항목	통제목적	점검항목	설명
						- 정보시스템 환경의 중대한 변화 (예 : 차세대 시스템 구축) ㅇ 보안점검, 내부감사 결과 분석 등을 통해 정책, 정책시행 문서에서 규정하고 있는 정보보호 활동의 주기, 방법 등이 적절한 지 정기적으로 검토하여야 하며 필요한 경우 제·개정을 통해 문서에 반영하여야 한다.
					중대한 환경 변화 시 정보보호정책 및 정책시행 문서에 미치는 영향을 분석하고 제·개정 필요성 여부를 검토하고 있는가?	ㅇ 다음과 같은 상황이 발생한 경우 정보보호정책 및 정책시행 문서에 미치는 영향을 분석하고 필요 시 문서에 반영하여야 한다. - 중대한 보안사고 발생 - 정보보호 및 개인정보 관련 법률 제·개정 - 새로운 위협 또는 취약성의 발견 - 비즈니스 환경의 변화 (신규 사업 영역 진출 등) - 정보보호 및 IT 환경의 중대한 변화 등
		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.	정보보호정책 및 정책시행 문서의 제정, 개정, 배포, 폐기 등의 이력을 확인할 수 있도록 관리절차를 수립 · 이행하고 있는가?	ㅇ 정보보호정책 및 정책시행 문서의 제정, 개정, 폐기 시 이력(일자, 내용, 작성자, 승인자 등)을 확인할 수 있는 관리절차를 수립하고 이행하여야 한다. - 제·개정으로 인한 문서의 효력 발생일은 일반적으로 최고경영자 혹은 정보보호책임자의 승인일 혹은 공표일로 하여야 한다.
					정보보호정책 및 정책시행 문서는 최신본으로 관리하고 있는가?	ㅇ 정보보호정책 및 정책시행 문서는 최신본으로 유지하여야 한다.
					정보보호정책 및 정책시행 문서에서 정한 정보보호 활동 수행에 관한 운영 기록을 생성하여 유지하고 있는가?	ㅇ 정보보호 활동 수행 과정에서 생성된 각종 양식, 대장, 로그, 결재문서 등 운영기록의 보관방법, 보호대책, 유지기간, 접근통제 등 관리절차를 마련하여야 한다. ㅇ 운영기록 확인을 통해 관련 활동의 정상적인 이행 여부를 확인할 수 있어야 하며 정보보호 관리체계 인증기준(104 개)의 이행 확인이 가능하도록 운영기록(증적)을 확보하고 있어야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
2.1	조직 체계	2.1.1	정보보호 최고책임자 지정	최고경영자는 임원급의 정보보호 최고책임자를 지정하고 정보보호 최고책임자는 정보보호정책 수립, 정보보호 조직 구성, 위험관리, 정보보호위원회 운영 등의 정보보호에 관한 업무를 총괄 관리하여야 한다.	최고경영자는 조직의 정보보호 관련 업무를 총괄 관리할 수 있는 임원급의 정보보호 최고책임자(CISO)를 지정하고 있는가?	ㅇ 최고경영자는 조직 내에서 정보보호 관리활동을 효과적으로 추진하기 위하여 이를 총괄 관리할 수 있는 임원급의 정보보호 최고책임자(CISO)를 지정하여야 하며 인사발령 등의 공식적인 지정절차를 거쳐야 한다. ㅇ 정보보호 최고책임자 지정 시 다음과 같은 법률을 참고할 수 있다. - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 45 조의 3(정보보호 최고책임자의 지정 등) - 전자금융거래법 제 21 조의 2(정보보호 최고책임자의 지정)
		2.1.2	실무조직 구성	최고경영자는 정보보호 최고책임자의 역할을 지원하고 조직의 정보보호활동을 체계적으로 이행하기 위해 실무조직을 구성하고 조직 구성원의 정보보호 전문성을 고려하여 구성한다.	최고경영자는 정보보호 최고책임자(CISO)의 역할을 지원하고 조직의 정보보호활동을 체계적으로 이행하기 위한 실무조직을 구성하고 있는가?	ㅇ 최고경영자는 조직의 규모 및 정보보호 관리체계 범위 내 서비스의 중요도에 따라 필요인력, 예산 등을 분석하여 정보보호 실무조직을 구성하여야 한다. ㅇ 실무조직은 전담 또는 겸임조직으로 구성할 수 있으며 겸임조직으로 구성하더라도 정보보호 조직에 대한 공식적인 선언 또는 지정이 필요하다.
					정보보호 전문성을 고려하여 실무조직 구성원을 임명하고 있는가?	ㅇ 조직의 정보보호활동을 원활하게 수행하기 위하여 다음과 같은 항목을 고려하여 실무조직 구성원을 임명하여야 한다. - 전문적 지식 보유 여부 (예 : 정보보호 관련 학위 또는 자격증 보유) - 정보보호 관련 실무 경력 - 정보보호 관련 직무교육 이수 등

No	통제분야	No	통제항목	통제목적	점검항목	설명
		2.1.3	정보보호위원회	정보보호 자원할당 등 조직 전반에 걸친 중요한 정보보호 관련사항에 대한 검토 및 의사결정을 할 수 있도록 정보보호위원회를 구성하여 운영하여야 한다.	정보보호위원회 구성, 운영, 역할 및 책임 등을 정한 규정을 마련하고 있는가?	ㅇ 정보보호위원회의 주기적인 운영이 가능하도록 위원회의 구성, 역할, 책임, 주기 등을 정의한 규정을 마련하여야 한다. ㅇ 정보보호위원회의 역할과 책임은 다음과 같다. - 조직 전반에 걸친 중요한 정보보호 관련 사항 검토 및 의사결정 - 정보보호 실무조직 구성 및 정보보호 활동을 위한 위한 자원할당 등
					정보보호위원회는 중요한 정보보호 관련 사항에 대해 검토 및 의사결정을 할 수 있는 인원으로 구성하고 있는가?	ㅇ 정보보호위원회는 정보보호 관련하여 조직 내 이해관계를 대변할 수 있는 경영진, 부서장, 정보보호 최고책임자 등 주요 임직원으로 구성하여야 한다. 즉, 조직 내 정보보호위원회의 위상은 조직의 정보보호 의지를 나타내는 것이므로 정보보호 관련 중요한 사안에 대해 검토, 의사결정, 집행 권한이 부여된 인원으로 구성하여야 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.	정보보호 최고책임자와 정보보호 관련 담당자의 역할 및 책임을 정의하고 있는가?	ㅇ 정보보호 최고책임자가 총괄 관리하여야 할 정보보호 관련 업무는 다음과 같다. - 정보보호정책 및 정책시행 문서 수립 - 정보보호 조직 구성 - 정보보호 관리체계 수립 및 운영 - CERT 구성 등 침해사고 예방, 대응, 복구 - 정보보호 취약점 분석, 평가 및 개선 등을 포함한 위험관리 활동 - 임직원 대상 정보보호 교육 - 정보보호위원회 운영 - 그 밖에 법에서 정한 정보보호 조치 이행 등 ㅇ 정보보호관리자, 정보보호담당자 등 정보보호실무자는 정보보호 최고책임자의 관리 업무를 실무적으로 이행할 수 있도록 직무기술서 등을 통해 책임과 역할을 구체적으로 정의하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
					정보보호 최고책임자와 정보보호 관련 담당자의 활동을 평가할 수 있는 체계를 수립하고 있는가?	ㅇ 조직 내 KPI, MBO, 인사평가와 같은 평가 체계 내 정보보호 활동의 책임과 역할을 평가할 수 있는 항목을 포함하여 주기적으로 정보보호 최고책임자와 정보보호 관련 담당자의 활동을 평가하여야 한다. ※ KPI (Key Performance Indicator) : 핵심성과지표 ※ MBO (Management By Objectives) : 목표관리

< *정보보호대책_3. 외부자보안* >

No	통제분야	No	통제항목	통제목적	점검항목	설명
3.1	보안요구사항 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.	조직의 정보처리 업무를 외부자에게 위탁하는 경우 다음과 같은 보안요구사항을 정의하여 계약 시 반영하고 있는가? - 정보보호 관련 법률 준수 (개인정보 처리 관련 등) - 정보보호서약서 제출 (비밀유지, 정보보호 책임 등) - 위탁 업무 수행 직원 대상 주기적인 정보보호 교육 수행 - 업무수행 관련 취득한 중요정보 유출 방지 대책 - 외부자 내부네트워크(업무망) 연결 시 인터넷접속 제한 - 외부자 사무실 공간에 대한 물리적 보호조치 (장비 및 매체 반출입, 출입통제 등) - 외부자 직원 PC 등 단말 보안 (백신설치, 안전한 패스워드 설정 및 주기적 변경, 화면보호기 설정 등) - 조직 중요정보시스템 접근 허용 시 과도한 권한이 부여되지 않도록 접근권한 부여 및 해지 절차 - 주기적 보안점검 수행 - 무선네트워크 구축 및 사용 제한 (필요 시 위험분석을 통한 대책 마련 후 책임자 승인) - 재위탁 하도급 계약 시 본 계약 수준의 보안요구사항 정의 - 보안요구사항 위반 시 처벌, 손해배상 책임 - 보안사고발생에 따른 보고 의무 등	ㅇ 조직의 업무 중 서비스 제공을 위한 시스템 통합(SI : System Integration), 운영(SM : System Maintenance), 유지보수, 고객상담 등 외부자에게 업무를 위탁하거나 클라우드 서비스를 이용하는 경우 외부자 업무형태(자사 건물 상주, 독립된 공간 근무 등)에 따라 준수하여야 할 보안요구사항을 정의하고 계약과정에서 명확하게 반영하여야 한다. - 이는 위탁업무 수행과정에서 외부자가 접근하는 중요정보(시스템 및 네트워크 구성도, 개인정보, 산출물, 산업기밀 등)의 유출, 침해사고를 예방하기 위한 것이다. - 다만 외부자 업무형태에 따라 세부점검 항목에서 제시하고 있는 보안요구사항을 계약서에 반영하지 못하는 경우 타당한 사유가 있어야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
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.	외부자가 계약서에 명시한 보안요구사항을 준수하고 있는 지 주기적으로 점검 또는 감사를 수행하고 문제점 발견 시 개선할 수 있는 보호대책을 수립 · 이행하고 있는가?	○ 조직의 외부자 관리 직무를 맡은 담당자는 외부자와 계약 시 정의한 보안요구사항을 준수하고 있는 지 주기적으로 점검 또는 감사를 수행하여야 한다. 또한 외부자가 자체적으로 정보보호책임자를 지정하여 보안점검을 수행한 경우 그 결과를 주기적으로 보고하고 문제점 발생 시 유사한 문제가 재발하지 않도록 추가적인 보호대책을 수립하고 이행하여야 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.	외부자가 위탁 업무 수행과정에서 담당자 퇴직 등의 변경사항이 발생할 경우 위탁사 관련부서에 보고하고 공식적인 절차에 따라 정보자산 반납, 접근계정 삭제 등의 조치를 하고 있는가?	○ 위탁 업무 수행과정에서 외부자의 관련 업무 담당자가 변경될 수 있으며 변경이력에 대한 보고 및 적절한 보호조치가 지체 없이 이루어질 수 있도록 관리하여야 한다.
					외부자와의 계약 만료, 업무 종료 시 공식적인 절차에 따라 정보자산의 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 물리적 출입권한 삭제 업무 수행 시 알게 된 정보의 비밀유지서약서 작성 등을 확인하고 있는가?	○ 외부자와의 계약 만료, 업무 종료에 따른 공식적인 정책 및 절차가 수립되어야 하며 이 정책 및 절차를 통해 정보시스템 자산 반납 및 업무 중 사용하였던 모든 접근계정 삭제 확인보장되어야 한다.

< 정보보호대책_4. 정보자산분류 >

No	통제분야	No	통제항목	통제목적	점검항목	설명
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.	정보자산(정보시스템, 정보보호시스템, 정보)의 분류기준을 수립하고 정보보호 관리체계 범위 내 모든 정보자산을 식별하고 있는가?	○ 다음의 정보자산에 대해 조직의 업무 특성에 적합한 분류기준을 정의하여야 한다. ※ 정보자산 ※ - 정보시스템 : 서버, PC 등 단말기, 보조저장매체, 네트워크 장비, 응용 프로그램 등 정보의 수집, 가공, 저장, 검색, 송수신에 필요한 하드웨어 및 소프트웨어 - 정보보호시스템 : 정보의 훼손, 변조, 유출 등을 방지하기 위하여 구축된 시스템으로 침입차단시스템, 침입탐지시스템, 침입방지시스템, 개인정보유출방지시스템 등을 포함 - 정보 : 문서적 정보와 전자적 정보 모두를 포함 ○ 수립된 분류기준에 따라 정보보호 관리체계 범위 내 모든 정보자산을 식별하여야 한다.
					식별된 정보자산을 다음 항목이 포함된 별도 목록으로 관리하고 있는가? - 정보자산명, 자산번호, 모델명, 용도 - 정보자산별 책임자, 관리자, 관리부서 - 정보자산에 대한 보안등급 등	○ 식별된 정보자산에 대한 정보자산명, 용도, 책임자 및 관리자, 관리부서, 보안등급 등의 정보자산 정보를 확인할 수 있도록 목록으로 관리하여야 한다. ○ 다만 목록은 자산관리시스템, 문서 등 다양한 형태로 관리할 수 있다.
					정기적으로 정보자산 현황을 조사하고 정보자산목록을 최신으로 유지하고 있는가?	○ 신규 도입, 변경, 폐기되는 정보자산 현황을 확인 할 수 있도록 정기적으로 정보자산 조사를 수행하고 정보자산목록을 최신으로 유지하여야 한다.
		4.1.2	정보자산별 책임할당	식별된 정보자산에 대한 책임자 및 관리자를 지정하여 책임소재를 명확히 하여야 한다.	식별된 정보자산에 대한 책임자 및 관리자(또는 담당자)를 지정하고 있는가?	○ 정보자산 도입, 변경, 폐기, 반출입 등의 책임을 질 수 있는 책임자 및 정보자산을 실제 관리 · 운영하는 관리자(또는 담당자)를 지정하여 책임소재를 명확하게 하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
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.	기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 정보자산의 중요도를 평가하기 위한 기준을 수립하고 있는가?	ㅇ 정보자산의 유출, 장애 및 침해 발생 시 조직의 업무에 미치는 영향을 고려하여 식별된 정보자산의 중요도를 평가할 수 있도록 기준을 수립하여야 한다. 일반적으로 기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 평가기준을 마련할 수 있다. 그 외에 서비스 영향, 이익손실, 고객상실, 대외 이미지 등도 추가적으로 고려할 수 있다. ㅇ 이는 정보자산에 미치는 위험을 분석(관리과정 3.2 위험분석 참고)하기 위한 첫번째 단계로 정보자산의 중요도가 높을수록 발견된 위험의 위험도가 높아지며 이 과정을 통해 비용효과적으로 우선 적용하여야 하는 정보보호대책을 선정할 수 있다.
					정보자산별로 중요도를 평가하고 각 자산별 특성에 적합한 보안등급 부여하고 보안등급을 쉽게 확인할 수 있도록 하고 있는가?	ㅇ 정보자산 중요도 평가기준에 따라 정보자산별로 중요도를 평가하여야 한다. 또한 정보자산별 특성에 따라 보안등급을 부여하고 다음과 같이 임직원이 보안등급을 쉽게 식별할 수 있도록 하여야 한다. - (전자)문서 : 기밀, 대외비, 일반 표시 - 서버 등 하드웨어 자산 : 자산번호 또는 바코드 표시를 통한 보안등급 확인
					정보자산의 보안등급에 따른 취급절차(생성, 저장, 이용, 파기 등)를 정의하고 이행하고 있는가?	ㅇ 정보자산의 등급에 따라 취급절차(생성, 저장, 이용, 파기 등)를 정의하고 이에 따라 접근통제 등 적절한 보안통제를 이행하여야 한다. (예 : 문서자산의 경우 각 보안등급별(기밀, 대외비, 일반)로 생성, 저장, 이용, 파기 등에 대한 보안통제를 마련하여 이행)

< 정보보호대책_5. 정보보호교육 >

No	통제분야	No	통제항목	통제목적	점검항목	설명
5.1	교육 프로그램 수립	5.1.1	교육 계획	교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 정보보호교육 계획을 수립하여야 한다.	정보보호 교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 정보보호교육 계획을 수립하고 있는가?	ㅇ 정보보호교육을 시행할 수 있도록 다음과 항목이 포함된 정보보호 교육 계획을 전년도말 혹은 당해 1/4 분기 이내에 수립하여야 한다. - 교육 시기 (예 : 분기별, 반기별 등) - 시기별 교육 기간 - 교육 대상 - 교육 내용 - 교육 방법 (예 : 온라인, 집합교육 등)
					정보보호교육 시행을 책임질 수 있는 경영진(최고경영자 등)이 정보보호 교육 계획을 검토하여 승인하고 있는가?	ㅇ 예산 배정 및 집행 권한을 보유하고 있는 경영진(최고경영자)은 연간 정보보호 교육 계획을 검토하고 승인하여 정보보호 교육이 계획에 따라 이행될 수 있도록 적극 지원하여야 한다.
		5.1.2	교육 대상	교육 대상에는 정보보호 관리체계 범위 내 임직원 및 외부자를 모두 포함하여야 한다.	정보보호 교육대상에 정보보호 관리체계 범위 내 정보자산에 직 · 간접적으로 접근하는 임직원 및 외부자를 모두 포함하고 있는가?	ㅇ 정보보호 교육대상에는 정보보호 관리체계 범위 내 정보자산에 직 · 간접적으로 접근하는 정규직 임직원, 임시직원, 외주용역업체 직원 등 모든 인력을 포함하여야 한다. ㅇ 정보자산이 위치한 장소에 접근할 수 있는 청소원, 경비원 등에게도 기본적인 정보보호 인식교육을 수행하여야 한다. ㅇ 교육대상이 하도급에 의해 파견된 직원인 경우 해당 용역업체 담당자가 정보보호 교육을 수행할 수 있도록 관련 자료를 제공하고 지원하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
		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.	임직원 대상 기본 정보보호교육에 다음의 내용을 포함하고 있는가? - 정보보호 및 정보보호 관리체계 개요 - 정보보호 정책, 지침, 절차 등 정보보호 관련 내부규정 - 정보보호 관련 법률 - 침해사고 사례 및 대응방안 - 정보보호 규정 위반 시 법적 책임 등	ㅇ 기본 정보보호교육에는 다음과 같은 내용을 포함하여야 한다. - 정보보호의 기본 개요 - 정보보호 관리체계 구축 절차 및 방법 - 정보보호 관련 법률의 이해 : 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 개인정보보호법, 전자금융거래법, 신용정보의 이용 및 보호에 관한 법률, 전자상거래 등에서의 소비자보호에 관한 법률 등 - 침해사고 대응 절차 등 임직원이 준수하여야 할 정보보호 관련 내부규정 - 최근 침해사고 사례 및 정보보호 관련 국내외 동향 - 정보보호 규정 위반 시 상벌규정, 법적 책임 등 ㅇ 교육을 효과적으로 시행하기 위하여 집합교육, 온라인교육, 전달교육 등 다양한 교육방법을 정할 수 있다. ㅇ 교육의 대상, 내용, 기간 등에 따라 효과적으로 교육을 수행할 수 있는 방법 (예 : 집합교육, 온라인 교육, 전달 교육 등)을 선택하여야 한다. ㅇ 정보보호 인식제고 위하여 보안의 날 지정, 포스터 또는 뉴스레터를 제작할 수도 있다.
					IT 및 정보보호 조직 내 임직원은 정보보호와 관련하여 직무별 전문성 제고를 위하여 필요한 별도의 교육을 받고 있는가?	ㅇ IT 직무자(운영, 개발), 정보보호 직무자는 일반 직원과 별도로 직무별 업무 수행에 필요한 정보보호교육을 받아야 한다. 직무별 교육은 다음과 같은 교육과정을 활용할 수 있다. - 정보보호 관련 컨퍼런스, 세미나, 워크샵 참가 - 정보보호 관련 교육 전문기관 내 교육 수료 - 외부 전문가 초빙을 통한 내부 교육 및 세미나

No	통제분야	No	통제항목	통제목적	점검항목	설명
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.	정보보호 관리체계 범위 내 임직원 및 외부자를 대상으로 연 1회 이상 기본 정보보호 교육을 수행하고 있는가?	ㅇ 경영진(최고경영진)의 승인을 받은 정보보호 교육 계획에 따라 정규직 임직원, 임시직원, 외주용역, 외부자 등을 대상으로 연 1회 이상 기본 정보보호 교육을 시행하여야 한다. ㅇ IT 및 정보보호 직무자는 기본 정보보호 교육 이외에 직무별 정보보호 교육을 별도로 연 1회 이상 이수하여야 한다. ㅇ 개인정보관리책임자 및 개인정보취급자는 연 2회 이상 개인정보보호 교육을 이수하여야 한다. (기본 정보보호 교육에 개인정보보호 내용을 포함할 수 있다.) ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적·관리적 보호조치 기준(고시)' 제3조(내부관리계획의 수립·시행) 2항
					정보보호 정책 및 절차의 중대한 변경, 조직 내·외부 보안사고 발생, 정보보호 관련 법률 변경 등 발생 시 이에 대한 추가 교육을 수행하고 있는가?	ㅇ 기본 정보보호 교육 이외에 다음과 같은 상황이 발생할 경우 추가적인 정보보호 교육을 수행하여야 한다. - 정보보호(개인정보 포함) 관련 법률 변경 - 조직 내 정보보호 관련 정책 및 절차 변경 - 조직 내·외부 보안사고 발생 - 업무 환경의 중대한 변화 발생 (예 : 정보보호 관리체계 범위 변경)
					출장, 휴가 등의 사정으로 정기 정보보호 교육을 받지 못한 인력에 대한 교육 방법을 마련하고 시행하고 있는가?	ㅇ 출장, 휴가 등으로 인해 정기 정보보호 교육에 불참한 인력에 대해 전달교육, 추가교육, 온라인 교육 등의 방법으로 정보보호 교육을 시행하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
					임직원 및 외부자 신규 채용 계약 시, 업무 시작 전에 정보보호 교육을 시행하고 있는가?	ㅇ 채용으로 인해 신규 인력 발생 시, 업무 투입 전에 정보보호 교육을 실시하여 조직 내 정보보호 관련 사전 지식이 없는 데 따른 보안규정 위반, 보안사고 발생의 위험수준을 낮추도록 하여야 한다.
					교육시행에 대한 기록을 남기고 교육 효과와 적정성을 평가하여 다음 교육 계획에 반영하고 있는가?	ㅇ 교육 시행 후, 교육 공지, 교육자료, 출석부 등과 같은 기록을 남기고 미리 마련된 평가 기준에 따라 설문 또는 테스트 등을 통해 교육 내용의 적절성과 효과성을 평가하여야 한다. ㅇ 교육평가 결과 내용에서 도출된 문제점에 대해 개선 대책을 마련하고 차기 교육 계획 수립 시 반영하여야 한다.

< *정보보호대책_6. 인적보안* >

No	통제분야	No	통제항목	통제목적	점검항목	설명
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.	조직 내 중요 정보자산(정보, 시스템 등)을 취급하는 직무를 정의하고 해당 직무를 수행하는 주요 직무자를 지정하고 있는가?	ㅇ 다음을 주요직무로 분류할 수 있으며 이 업무를 수행하는 임직원을 주요 직무자로 지정하여야 한다. - 중요정보(개인정보, 인사정보, 영업비밀, 산업기밀, 재무정보 등)를 취급 - 주요 정보시스템(서버, DB, 응용 프로그램 등) 운영 및 개발 - 정보보호시스템 운영 - 정보보호관리업무 수행
					중요정보를 취급하는 주요 직무자는 최소한으로 지정하고 주기적으로 주요 직무자 현황을 관리하고 있는가?	ㅇ 중요정보를 취급하는 주요 직무자의 경우 업무 범위 및 목적에 벗어나는 정보 처리 권한을 부여하지 않도록 관련 직무자를 최소한으로 지정하여야 한다. ㅇ 중요정보 처리 권한이 부여된 주요 직무자의 현황을 주기적으로 관리하여 직무자별 업무 성격에 따라 적정한 권한이 부여되었는지 여부를 검토하여야 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 인적자원 부족 등 불가피하게 직무분리가 어려운 경우 별도의 보완통제를 마련하여야 한다.	직무의 권한 오남용을 예방하기 위하여 정보보호 관련 주요 직무 분리 기준을 수립하고 직무별 역할과 책임을 명확하게 기술하고 있는가?	ㅇ 직무별 권한과 책임을 분산시켜 직무간 상호견제를 할 수 있도록 직무 분리 기준을 수립하여야 한다. - 개발과 운영 직무 분리 (필수) - 정보시스템(서버, DB, 네트워크 등)간 운영직무 분리 - 정보보호 관리와 정보시스템 운영직무 분리 - 정보보호 관리와 정보시스템 개발직무 분리 등

No	통제분야	No	통제항목	통제목적	점검항목	설명
					직무분리가 어려운 경우 직무자간 상호 검토, 상위관리자 정기 모니티링 및 변경 사항 승인, 책임추적성 확보 방안 등의 보완통제를 마련하고 있는가?	ㅇ 조직 규모가 작거나 인적 자원 부족 등의 사유로 인해 불가피하게 직무 분리가 어려운 경우, 직무자간의 상호 검토, 상위관리자의 주기적인 직무수행 모니터링 및 변경 사항 검토/승인, 직무자의 책임추적성 확보 등의 보완통제를 마련하여야 한다.
		6.1.3	비밀유지서약서	임직원으로부터 비밀유지 서약서를 받아야 하고 임시직원이나 외부자에게 정보시스템에 대한 접근권한을 부여할 경우에도 비밀유지서약서를 받아야 한다.	신규 인력 채용 시 정보보호 책임이 명시된 정보보호서약서를 받고 있는가?	ㅇ 신규로 채용된 인력은 조직의 중요정보 취급 및 관리 시 정보보호의 필요성과 책임에 대해 명시된 정보보호서약서에 서명하고 조직에 제출하여야 한다. ㅇ 정보보호서약서의 제출 의무에 대해 신규 인력 채용 절차 중 기본적인 사항으로 인식하고 관리 부서를 지정하여 정보보호서약서를 관리하여야 한다. (일반적으로 신규 인력 채용 시 인력관리부서에서 정보보호서약서를 수집 및 관리하고 있다.)
					임시직원 혹은 외주용역과 같은 외부자에게 정보자산에 대한 접근권한을 부여할 경우, 정보보호에 대한 책임을 계약서에 명시하고 이에 대한 정보보호서약서를 받고 있는가?	ㅇ 임시직원 혹은 외주용역업체직원과 같은 외부자에게 정보자산에 대한 접근권한을 부여할 경우 정보보호 책임, 조직 내 정보보호 규정 준수 의무, 정보보호 의무에 미준수로 인한 사건 · 사고 발생 시 손해배상 책임 등의 내용을 정보보호서약서에 명시하고 서명을 받아야 한다.
					임직원 퇴직 시 별도의 비밀유지에 관련한 서약서를 받고 있는가?	ㅇ 직무 상 알게 된 조직의 중요정보에 대한 퇴사 후 누출 방지를 위하여 인력 퇴사 절차 내 비밀유지서약서를 받고 누출 발생 시 그에 따르는 법적 책임이 있음을 상기시켜야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
						ㅇ 직무변경과 같이 인력의 고용조건에 변화가 발생한 경우 이전에 습득한 비밀정보를 누출하지 않도록 정보보호서약서의 내용을 환기시키는 것 좋다.
					정보보호서약서 및 비밀유지서약서는 법적 분쟁 발생 시 증거자료로 사용할 수 있도록 안전하게 보존하고 용이하고 찾아볼 수 있도록 관리하고 있는가?	ㅇ 정보보호서약서 및 비밀유지서약서는 법적 분쟁 발생 시 법률적 책임에 대한 증거자료로 사용할 수 있기 때문에 필요 시 용이하게 찾아볼 수 있는 형태로 보관하여야 한다. ㅇ 정보보호서약서 및 비밀유지서약서에 개인정보가 포함될 경우 비인가된 제3자에게 누출되지 않도록 물리적으로 안전한 장소에 보관하여야 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.	부서 및 직무변경, 휴직, 퇴직 등으로 인한 인사변경 내용이 인사부서, 정보보호부서, 정보시스템 운영부서 간에 공유되고 있는가?	ㅇ 부서 및 직무변경, 휴직, 퇴직 등 인사변경 발생 시 정보자산 반납, 접근권한의 변경 · 회수 조치가 신속하게 이루어질 수 있도록 인사부서는 변경내용을 정보보호부서, 정보시스템 운영부서 등에 공유하여야 한다.
					조직 내 인력(정규직 임직원, 임시직원, 외주용역업체 직원 등)의 직무변경 혹은 퇴직 시 정보자산 반납, 접근권한 조정 · 회수, 결과 확인 등 수립된 절차에 따라 지체 없이 이행하고 있는가?	ㅇ 조직 내 인력(정규직 임직원, 임시직원, 외주용역업체 직원 등)의 직무 변경 혹은 퇴직 발생 시 정보자산 반납, 접근권한의 조정 · 회수 등을 수립된 절차에 따라 시행하고 결과를 확인하여야 한다. ㅇ 직무변경자 혹은 퇴직자가 불가피하게 정보시스템 및 정보보호시스템 계정을 공유 사용하고 있었다면 계정의 비밀번호를 즉시 변경하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
		6.2.2	상벌규정	인사규정에 직원이 정보보호 책임과 의무를 충실히 이행했는지 여부 등 정보보호 활동 수행에 따른 상벌 규정을 포함하여야 한다.	인사규정에 임직원이 정보보호 책임과 의무를 충실히 수행했는지 여부에 따른 상벌규정이 문서로 명시화 되어 있는가?	ㅇ 임직원이 정보보호 관련 조직 내부 규정(예 : 정책, 지침, 절차 등) 및 비밀유지서약서에 명시된 정보보호 책임을 충실히 이행하지 않고 조직 내 중요정보를 훼손, 누출한 경우, 관계 법령상의 책임 및 처벌규정을 인사규정에 포함하고 아울러 정보보호 책임을 충실히 이행한 경우에 대한 보상 방안도 함께 마련하여야 한다.

< 정보보호대책_7. 물리적보안 >

No	통제분야	No	통제항목	통제목적	점검항목	설명
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.	주요 설비 및 시스템을 보호하기 위하여 물리적 보호구역을 다음과 같이 정의하고 구역별 보호대책을 수립 · 이행하고 있는가? - 접견구역 : 외부인 접견 구역 - 제한구역 : 사무실 지역 등 - 통제구역 : 주요 정보처리 설비 및 시스템 구역 등	ㅇ 전산실, 시스템 운영 및 개발 공간, 통신장비실, 관제센터 등 업무의 중요도 및 정보자산 위치에 따라 물리적 보호 구역을 다음과 같이 구분하고 구역별 보호대책을 수립하고 이행하여야 한다. - 접견구역 : 외부인이 별다른 출입증 없이 출입이 가능한 구역(예 : 접견장소 등) - 제한구역 : 비인가된 접근을 방지하기 위하여 별도의 출입통제 장치 및 감시 시스템이 설치된 장소로 출입 시 직원 카드와 같은 출입증이 필요한 장소(예 : 부서별 사무실 등) - 통제구역 : 제한구역의 통제항목을 모두 포함하고 출입자격이 최소인원으로 유지되며 출입을 위하여 추가적인 절차가 필요한 곳(예 : 전산실, 통신장비실, 관제실, 공조실, 발전실, 전원실 등) ㅇ 통제구역은 조직 내부에서도 출입 인가자를 최소한으로 제한하고 있으므로 통제구역임을 표시하여 접근시도 자체를 원천적으로 차단하고 불법적인 접근시도여부를 주기적으로 검토하여야 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.	각 보호구역의 중요도 및 특성에 따라 화재, 전력 이상 등 인재 및 자연재해 등에 대비하여 필요한 설비를 갖추고 운영절차를 수립 · 관리하고 있는가?	ㅇ 보호구역의 중요도와 특성에 따라 화재, 전력이상, 비인가된 외부침입 등을 방지하기 위하여 보호구역별 필요한 다음과 같은 설비를 갖추고 운영절차를 마련하여야 한다. - 온습도 조절기(항온항습기 또는 에어컨) - 화재감지 및 소화설비 - 누수감지기 - UPS,비상발전기, 전압유지기

No	통제분야	No	통제항목	통제목적	점검항목	설명
						- CCTV, 외부침입감지 및 경보, 출입통제 시스템(예 : 지문인식, 출입카드시스템 등) - 전력선 이중화 - 파손방지(예 : 정보시스템기기의 rack 설치 등) 등 o 특히 통제구역에 해당하는 전산실의 경우 상기설비를 갖추고 화재, 전력이상, 장애 등의 비상 시 신속한 복구 및 대응이 가능하도록 운영절차를 마련하여야 한다. ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '집적정보 통신시설 보호지침(고시)'
					보호구역 내 주요 시스템 및 인력을 화재로부터 보호하기 위하여 필요한 설비를 설치하고 지속적으로 운영 · 관리하고 있는가?	o 화재 감지기를 적절한 간격으로 설치하고 충분한 용량의 소화기를 비치하여야 한다. - 보호구역 면적에 대비하여 화재 감지기(예 : 열감지, 연기감지) 및 소화기를 설치하여야 하며 주기적으로 화재감지기 및 소화기 상태를 점검하여야 한다. ※ 참고 ※ - 소방시설 설치 · 유지 및 안전관리에 관한 법률
					보호구역 내 주요 시스템을 수해로부터 보호할 수 있도록 누수를 탐지할 수 있는 설비를 설치하고 지속적으로 운영 · 관리하고 있는가?	o 전산실과 같이 주요 시스템이 위치한 보호구역의 경우 누수 발생 시 탐지가 가능하도록 누수감지기를 설치하고 정상적인 작동유무를 주기적으로 점검하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
					보호구역 내 주요 정보시스템이 안정적인 환경에서 동작할 수 있도록 적절한 온도와 습도를 유지시키는 항온항습 또는 에어컨을 설치하여 운영 · 관리하고 있는가?	o 전산실과 같이 주요 시스템이 위치한 보호구역의 경우 온도 16~26 도, 습도 40~70%를 항시 유지하기 위하여 전산실 규모에 따른 적정한 규모의 항온항습기 또는 에어컨을 설치하고 주기적으로 항온항습기 또는 에어컨 상태를 점검하여야 한다.
					보호구역 내 주요 시스템이 전력을 안정적으로 공급받을 수 있도록 시설을 설치하고 지속적으로 운영 · 관리하고 있는가?	o 정전, 전기사고 등 갑작스러운 전력공급 중단 시 주요 정보시스템이 전력을 안정적으로 공급받을 수 있도록 전산실 및 시스템 규모를 고려하여 다음과 같은 설비를 구축하고 주기적으로 상태를 점검하여야 한다. - 무정전전원장치 (UPS) - 비상발전기 - 이중전원선 - 전압유지기 - 접지시설 등 ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '집적정보 통신시설 보호지침(고시)'
					화재 등의 재해 발생 시 임직원이 대피절차에 따라 안전하게 대피할 수 있도록 비상벨, 비상등, 비상통로 안내표지 등을 설치하고 있는가?	o 화재 등의 재해 발생 시 임직원이 대피할 수 있도록 대피절차를 별도로 마련하고 절차에 따라 신속하게 대피할 수 있도록 비상벨, 비상등, 비상로 안내표지 등을 설치하여야 한다.
					주요 정보시스템을 외부 집적정보통신시설(IDC)에 위탁운영하는 경우, 물리적보호에 필요한 요구사항을 계약서에 반영하고 운영상태를 주기적으로 검토하고 있는가?	o 주요 정보시스템을 외부 집적정보통신시설(IDC)에 위탁운영하는 경우 화재, 수재, 전력이상, 온도, 습도, 환기 등의 환경적 위협 및 파손, 도난 등 물리적 위협으로부터 보호되도록 보안요구사항을 계약서에 반영하고 운영상태를 주기적으로 검토하여야 한다 - 온습도 조절기(항온항습기 또는 에어컨)

No	통제분야	No	통제항목	통제목적	점검항목	설명
						- 화재감지 및 소화설비 - 누수감지기 - UPS,비상발전기, 전압유지기 - CCTV, 외부침입감지 및 경보, 출입통제 시스템(예 : 지문인식, 출입카드시스템 등) - 전력선 이중화 - 파손방지(예 : 정보시스템기기의 rack 설치 등) 등 - 구조의 안전성 (설비 하중을 견딜 수 있는 구조) - IDC 의 책임보험 가입여부 (미가입 시 1천만원 이하의 과태료 부과) ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 46 조(집적된 정보통신시설의 보호) - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제 38 조(보험가입)
		7.1.3	보호구역 내 작업	유지보수 등 주요 설비 및 시스템이 위치한 보호구역 내에서의 작업 절차를 수립하고 작업에 대한 기록을 주기적으로 검토하여야 한다.	정보시스템 도입, 유지보수 등으로 보호구역 내 작업이 필요한 경우 작업신청 및 수행 관련 절차를 수립하고 작업기록을 주기적으로 검토하고 있는가?	ㅇ 주요 시설 및 정보시스템이 위치한 통제구역(전산실 등)에서 정보시스템 도입 및 폐기, 유지보수(정기점검 포함) 등의 사유로 임직원 및 외부인이 작업을 수행할 경우 다음 사항을 고려하여 작업신청 및 승인, 작업기록 작성, 모바일 기기 반출입 통제 등의 절차를 마련하고 그 기록을 정기적으로 검토하여야 한다. - 작업신청 시 관련자(예 : 보호구역 출입통제 담당자, 작업신청부서장 등) 검토 · 승인 필요 - 작업기록에는 작업일자, 작업시간, 작업목적, 작업내용, 작업업체 및 담당자명, 검토자 승인자 등 포함 - 작업 수행을 위한 보호구역 출입 절차 마련 및 출입기록의 주기적 검토

No	통제분야	No	통제항목	통제목적	점검항목	설명
						- 작업 수행을 위한 모바일기기 반출입 및 모바일 기기 안전성 확보 절차(백신 설치 등) 마련 ㅇ 주요 시설 및 시스템이 위치한 통제구역 내 모바일기기(노트북, 스마트기기 등) 사용은 원칙적으로 금지하는 것이 바람직하다. 다만 작업의 원활한 수행을 위하여 불가피하게 모바일기기를 사용해야 하는 경우 사전 승인 및 모바일 기기의 보안성 검토를 수행한 후 사용하여야 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.	각 보호구역별 내 · 외부자 출입통제 절차를 마련하고 출입 가능한 임직원 현황을 관리하고 있는가?	ㅇ 각 보호구역별로 출입 가능한 부서, 직무, 업무를 정의하고 출입권한이 부여된 임직원을 식별하여 그 현황을 관리하여야 한다. ㅇ 공식적인 출입절차(출입신청, 책임자 승인, 출입권한부여 및 회수, 출입내역 기록, 출입기록 정기적 검토 등)를 마련하고 인가된 사람만이 출입할 수 있도록 하여야 한다. ㅇ 또한 주요 시설 및 시스템이 위치하고 있는 통제구역의 경우 업무목적에 따라 최소한의 인원만 출입할 수 있도록 통제하여야 한다. ㅇ 특히 보호구역에 외부인 출입이 필요한 경우 내부 임직원 출입절차와는 별도의 절차(방문객 출입증 발급 및 패용, 방문장소로 출입권한 제한, 담당자 동행, 출입대장 작성 등)를 마련하여 출입을 통제하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
					각 보호구역에 대한 내 · 외부자 출입기록을 일정기간 보존하고 출입기록 및 출입권한을 주기적으로 검토하고 있는가? - 업무 목적에 적합한 출입권한 부여 - 절차에 따른 출입권한 부여 - 퇴직자 또는 직무변경자 출입권한 삭제·조정 및 출입증 회수 - 업무시간 외 출입 - 비인가자의 출입 시도 등	ㅇ 각 보호구역 출입의 책임추적성을 확보할 수 있도록 출입기록을 일정기간 보존하고 출입의 적정성을 확인하기 위하여 다음과 같은 기준으로 출입기록을 주기적으로 검토하여야 한다. - 업무 목적에 적합한 출입권한 부여 : 업무 목적에 비해 과도한 출입권한 부여 시 권한 조정, 장기간 미출입 시 권한 회수 등 조치 - 절차에 따른 출입권한 부여 : 보호구역 출입절차에 따른 권한 부여 여부 확인 (임의적 출입권한 생성 확인) - 퇴직자 또는 직무변경자 출입권한 삭제 · 조정 및 출입증 회수 : 퇴직자 출입증 회수 및 출입권한을 삭제, 직무변경에 따른 출입권한 조정 - 업무시간 외 출입 : 일상 업무시간 이외 출입 시 출입사유 확인 - 비인가자의 출입 시도 : 중요한 보호구역인 통제구역의 비인가자 출입시도를 확인하여 그 사유를 확인하고 조치 - 외부자 출입기록 : 유지보수, 비상 시 외부자 출입 적정성 검토 상기 검토 기준 이외에도 조직의 업무특성에 따른 기준을 별도로 마련하여 보호구역 출입 적정성을 검토하는 것이 좋다. ㅇ 또한 시스템적으로 출입로그를 남기지 않는 단순 잠금장치(자물쇠)를 사용하는 경우에는 반드시 출입대장을 작성하여 출입기록을 확인할 수 있도록 하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
					보호구역 내 중요한 장비, 문서, 매체 등에 대한 반출입 관련 정책 및 절차를 수립 · 이행하고 있는가?	ㅇ 보호구역 내 다음 항목에 대한 반출입 통제 정책 및 절차를 수립하고 이행하여야 한다. - 장비(예 : 서버, 네트워크 장비, 항온항습기 등) - 문서(예 : 업무관련 대외비 이상의 문서) - 저장매체 (예 : CD, 테이프 등) ㅇ '반출입관리대장'을 별도로 마련하여 일시, 품명 및 수량, 반출입 담당자, 반출입장소, 반출입 사유, 관리부서 확인 및 서명 등과 내용이 포함되어 이력관리를 하고 책임자가 주기적으로 관리대장 내용의 적정성을 확인하여야 한다.
		7.1.5	모바일기기 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.	노트북, 패드 등 모바일 기기 반출입 시 반출입 통제 및 보안사고 예방 절차를 수립하고 있는가?	ㅇ 보호구역별로 모바일기기(노트북, 탭, 패드 등)의 반출입에 대한 통제절차를 다음과 같이 마련하여야 한다. - 보호구역 출입통제 책임자 사전승인 - 반출입 관리대장 기록 - 모바일 기기 보안 점검 수행 - 모바일 기기 반출입내역 주기적 점검 등 ㅇ 모바일기기 반출입을 통한 중요정보 유출, 내부망 악성코드 감염 등의 보안사고 예방절차 수립 시 다음과 같은 사항을 고려하여야 한다. - (반입시) 안티바이러스 S/W 통한 악성코드 감염여부 점검 - (반입시) USB 포트 차단 및 USB 반입 금지 - (반입시) 모바일 기기 장착된 카메라 렌즈 봉인 등 - (반출시) 중요정보 저장 여부 확인 ㅇ 주요 시설 및 정보자산이 위치한 통제구역 내 모바일기기(노트북, 탭, 패드 등)의 반입은 원칙적으로 금지하는 것

No	통제분야	No	통제항목	통제목적	점검항목	설명
						이 바람직하며 업무목적으로 작업의 원활한 수행을 위하여 불가피하게 모바일 기기를 사용하여야 하는 경우 사전 승인을 받고 상기 모바일 기기 보안사고 예방절차를 이행한 후 사용하는 것이 좋다. - 다만, 개인용 스마트폰의 경우 예외정책을 적용할 수 있으나 내부 네트워크에 연결하여 사용하지 않도록 하여야 한다.
					모바일 기기 반출입 절차에 따라 반출입 대장을 작성하고 관리자는 주기적으로 모바일 기기 반출입 이력을 점검하고 있는가?	ㅇ 보호구역 내 임직원 혹은 외부자가 업무목적을 위한 모바일 기기를 반출입하는 경우, 모바일기기 반출입 통제 절차에 따라 허가를 받고 '반출입대장' 이력을 기록하여야 한다. - 반출입 관리대장에 포함될 내용 : 일시, 사용자, 기종(모델), 기기식별번호(MAC, 시리얼 번호 등), 사유, 반출입 장소, 보안점검 결과, 관리자 확인서명 등 ㅇ 모바일 반출입대장은 관리자가 주기적으로 점검하여 반출입이 적정한 절차에 따라 이루어졌는지 검토하여야 한다.
7.2	시스템 보호	7.2.1	케이블 보안	데이터를 송수신하는 통신케이블이나 전력을 공급하는 전력 케이블은 손상을 입지 않도록 보호하여야 한다.	전력 및 통신케이블이 외부로부터의 물리적 손상이나 전기적 영향(예 : 간섭)으로부터 보호되고 있는가?	ㅇ 전력 및 통신케이블 등이 외부의 영향 없이 안정적으로 전력 및 데이터 전송이 이루어질 수 있도록 다음과 같은 보호조치를 취하여야 한다. - 전력 및 통신케이블은 물리적으로 구분하여 배선 - 전력 및 통신케이블에 대한 식별(어느 시스템에 연결되어 있는 지 확인 필요) - 전력 및 통신케이블 사이의 상호간섭을 방지하기 위한 거리유지 - 케이블을 지지하고 보호할 수 있는 설비 설치 (예 : 케이블 트레이) - 도청이나 손상이 일어나지 않도록 케이블을 보이지 않게 매설할 것

No	통제분야	No	통제항목	통제목적	점검항목	설명
						- 약전실, 강전실, 배전반 등에 대한 접근통제 등 ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '집적정보 통신시설 보호지침(고시)' - 방송통신설비의 기술기준에 관한 규정
		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.	정보시스템의 특성을 고려하여 배치 장소를 분리하고 있는가?	ㅇ 서버, 네트워크 장비, 정보보호시스템, 백업장치 등 정보시스템 특성에 따라 분리하여 배치하고 전산랙(Rack)등을 이용하여 시스템을 외부로부터 보호하여야 한다. ㅇ 개인정보 또는 사내 기밀정보 등 중요 정보를 저장하고 있는 서버나 중요 네트워크 장비(백본 등)의 경우 전산랙에 잠금장치를 설치하는 등 인가된 자에 한해 접근이 가능하도록 관리하여야 한다.
					정보시스템의 실제 물리적 위치를 손쉽게 확인할 수 있는 방안(배치도, 자산목록 등)을 마련하고 있는가?	ㅇ 장애 또는 보안사고 발생 시 신속한 조치를 위하여 시스템의 위치를 담당자가 즉시 확인할 수 있도록 물리적 배치도(시설 단면도, 배치도 등) 또는 목록을 마련하여 최신본으로 관리하여야 한다. - 또한 시스템 정보자산목록에 물리적 위치 항목을 포함하여 목록에서 언제든지 물리적 배치를 확인 가능하도록 하여야 한다.
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.	개인업무 환경에서의 정보보호에 대한 정책을 수립 · 이행하고 있는가? - 자리 이석 시 중요문서 및 저장매체 방치 금지 - 자리 이석 시 컴퓨터 화면보호기 및 패스워드 설정 - 개인용컴퓨터 보안설정	ㅇ 일상업무를 수행하는 사무실 환경에 대해 다음과 같은 보호대책이 명시된 정책을 수립하고 이행하여야 한다. - 일정시간 자리 이석, 퇴근, 휴가 시 책상 위에 중요문서, 저장매체방치 금지 - 중요 문서가 보관된 서랍장, 캐비넷 잠금장치 사용

No	통제분야	No	통제항목	통제목적	점검항목	설명
					- 중요문서 파기대책 등	- 일정시간 컴퓨터 미사용 시 화면보호기를 설정, 재시작 시 로그인 설정, 장기간 자리 이석 시 컴퓨터 로그오프 - 안전한 로그인 비밀번호 사용 및 주기적 변경 - 개인용컴퓨터 백신설치, 최신 패치, 공유폴더 설정 제한 - 개인용컴퓨터 및 업무시스템 안전한 로그인 비밀번호 사용 및 주기적 변경, 로그인정보(ID, 비밀번호) 노출 금지 (포스트잇 기록 부착 등) - 중요 정보가 포함된 문서 폐기 시 세절기를 이용한 파쇄 등
					개인업무 환경에서의 정보보호 준수여부를 주기적으로 점검하고 있는가?	ㅇ 임직원으로 하여금 개인업무환경에서의 정보보호 준수여부를 자가진단하게 하고 주기적으로 관리부서에서 정보보호 준수여부를 점검하여야 한다. - 또한 개인업무 환경보안 미준수자는 상벌규정에 따라 관리되어야 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.	팩스, 복사기, 프린터, 공용 PC, 파일서버, 문서고 등 공용으로 사용하는 사무장비 및 시설에 대한 보호대책을 수립・이행하고 있는가?	ㅇ 공용으로 사용하는 사무기기, PC, 파일서버, 문서고 등에 대해 다음과 같은 보호대책을 수립하고 이행하여야 한다. - 공용사무기기 : 팩스, 복사기, 프린트 등의 공용사무기기 주변에 중요정보문서 방치 금지 - 공용 PC : 일정기간 미사용 시 화면보호기를 설정, 재 시작 시 로그인 암호설정, 공용패스워드 사용 시 주기적으로 패스워드 변경, 중요정보 저장 제한 - 파일서버 : 파일서버 접근권한을 부서별, 업무별 등으로 부여하여 불필요한 정보공개 최소화, 사용자 별도 접근계정 발급, 공용 PC 보안대책 적용 - 문서고 : 문서고에 대한 접근권한을 부서별 혹은 업무별로 부여하여 출입가능

No	통제분야	No	통제항목	통제목적	점검항목	설명
						인원을 최소화하고 CCTV 혹은 출입통제시스템을 설치하여 출입이력 관리 - 공용 사무실 : 회의실, 프로젝트룸, 화상회의실 등 공용사무실 내 중요정보 문서 방치 금지 - 기타 공용업무환경에 대한 보안대책 수립
					공용업무 환경 보안에 대한 관리자를 지정하고 준수여부를 주기적으로 검토하고 있는가?	ㅇ 공용업무 환경 보안을 담당하는 관리자를 지정하고 각 사무기기, 파일서버, 문서고 등에 적용해야 할 보호대책 준수여부를 주기적을 점검하여야 한다. 또한 미준수 사항 발견 시 관련 내용을 임직원들에게 공고 또는 교육을 수행하여 주의를 환기시켜야 한다. (예 : 복사기 주변 프린트물 방치 발견 시, 관련 내용을 사내메일 등을 통해 공고하여 주의 환기를 통한 재발방지 유도)

No	통제영역	No	통제항목	통제내용	점검항목	설명
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 보안 요구사항을 명확히 정의하고 이를 적용하여야 한다.	신규 정보시스템 개발 및 기존 시스템 변경 시 법적 요구사항을 포함한 보안 요구사항을 정의하고 설계 단계에서부터 반영하고 있는가?	ㅇ 신규 정보시스템 개발 및 기존 시스템 변경 시 (개인)정보 영향 평가 결과, 정보보호 기본요소, 최신 보안취약점 등을 고려하여 다음과 같은 항목이 포함된 보안 요구사항을 정의하여 설계 단계에서부터 구현, 시험, 이관까지 일관성있게 적용될 수 있도록 하여야 한다. - 개인정보처리에 관련된 법적 요구사항 (예 : 개인정보 취급자 권한 부여 기록, 접속기록, 암호화 대상 정보 등) - 사용자 부서 및 기관의 정보보호 요구사항 (예 : 접근권한 정의 및 통제 원칙, 암호화 대상 선정 등) - 정보보호 관련 기술적인 요구사항 등 (예 : 개발보안, 인증, 암호화 등) ※ 참고 ※ - 홈페이지 SW(웹) 개발보안 가이드 (KISA) - 웹서버구축 보안점검 안내서(KISA) - 웹어플리케이션 보안 안내서(KISA) - 홈페이지 개발보안 안내서(KISA) - 소프트웨어 개발보안(시큐어 코딩) 관련 가이드(JAVA, C, Android-JAVA)(안전행정부)
		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.	정보시스템 설계 시 사용자 인증에 대한 보안 요구사항을 정의하여 반영하고 있는가?	ㅇ 정보시스템 설계 시 사용자 인증에 대해 다음과 같은 사항을 고려하여야 한다.(인증기준 10. 접근통제 참고) - 패스워드 관련 : 패스워드 잠김 임계치 설정, 패스워드 암호화 - 접근관련 : 동일사용자 동시세션 제한 등 - 추가적인 사용자 인증 절차 : 중요한 정보시스템(예 : 개인정보처리스시템)의

No	통제영역	No	통제항목	통제내용	점검항목	설명
						경우 추가적인 인증(예 : OTP, 공인 인증서 등) 요구 ※ 참고 ※ - 정보통신 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적 · 관리적 보호조치 기준(고시)' 제 4 조(접근통제) - 정보통신 이용촉진 및 정보보호 등에 관한 법률 제 23 조의 2(주민등록번호의 사용 제한)
					중요정보에 대하여 암호화가 요구되는 경우 법적 요구사항을 고려한 적절한 암호화 방법을 사용하고 있는가?	ㅇ 법적 요구사항을 고려하여 중요정보에 대해 안전성이 입증된 알고리즘과 키 길이를 사용하여 암호화하여야 한다. (인증기준 9.1.1 암호 정책 수립 참고) - 법적 요구사항이외에 조직에 특성에 따라 암호화 대상을 정의한 경우 암호화를 고려하여야 한다. ※ 참고 ※ ㅇ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제 15 조(개인정보의 보호조치) - 비밀번호 일방향 암호화 저장 - 주민등록번호 및 계좌번호 등 금융정보의 암호화 저장 ㅇ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적 · 관리적 보호조치 기준(고시)' 제 6 조(개인정보의 암호화) - 주민등록번호, 신용카드번호, 계좌번호의 암호화 저장 - 정보통신서비스 제공자의 개인용컴퓨터(PC)상에 저장된 이용자의 개인정보 암호화

No	통제영역	No	통제항목	통제내용	점검항목	설명
						ㅇ 개인정보보호법 '개인정보의 안전성 확보조치 기준(고시)' 제 7 조(개인정보의 암호화) - 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록증번호) 암호화 - 비밀번호 및 바이오정보 암호화(비밀번호는 일방향 암호화) - 개인정보처리자 개인용컴퓨터(PC)상에 저장된 고유식별번호 ㅇ KISA 안내서 - 암호기술 구현 안내서 (http://seed.kisa.or.kr) - 암호이용 안내서 - 암호정책 수립기준 안내서 등
					개인정보 및 인증정보 등의 중요한 정보 전송 시 SSL 보안서버 구축 등을 통하여 암호화하고 있는가?	ㅇ 정보통신망을 통해 중요정보를 송 · 수신하는 경우, 법적 요구사항을 고려하여 보안서버 구축 등의 조치를 통한 암호화 통신이 이루어져야 한다. (인증기준 9.1.1 암호 정책 수립 참고) ※ 참고 ※ ㅇ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적 · 관리적 보호조치 기준(고시)' 제 6 조(개인정보의 암호화) - 정보통신서비스 제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송수신할때에 안전한 보안서버 구축 등의 조치 필요 (예 : SSL, 암호화 응용프로그램을 설치하여 전송정보 암호화) ㅇ 개인정보보호법 '개인정보의 안전성 확보조치 기준 고시 및 해설서' 제 7 조(개인정보의 암호화) - 개인정보처리자는 주민등록번호, 비밀번호, 바이오정보 등 정보통신망을 통

No	통제영역	No	통제항목	통제내용	점검항목	설명
						하여 송수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 암호화 필요(보안서버 활용가능) ㅇ 보안서버구축 안내서 (KISA)
		8.1.3	보안로그 기능	정보시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 하여야 한다.	정보시스템 설계 시 보안관련 로그, 감사증적 등을 확보할 수 있는 기능을 반영하고 있는가?	ㅇ 보안사고 발생 시 책임 추적을 위하여 정보시스템에 다음과 같은 감사증적(로그)을 확보할 수 있도록 설계하여야 한다. (인증기준 11.6 로그관리 및 모니터링 참고) - 사용자 및 관리자의 접속기록 (로그인 및 로그아웃) - 사용자 권한 부여, 변경, 말소 기록 - 정보시스템 시작 및 중지 - 특수 권한으로의 접근 기록 - 주요업무관련 행위에 대한 로그 등
					정보시스템 설계 시 보안로그를 보호하기 위한 대책을 마련하고 있는가?	ㅇ 정보시스템 설계 시 보안로그의 비인가된 변조 및 삭제를 방지하기 위한 대책을 마련하여야 한다. (예 : 로그에 대한 접근통제 등)
		8.1.4	접근권한 기능	정보시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다.	정보시스템 설계 시 시스템 사용자의 업무 목적, 기능, 중요도에 따라 접근권한이 부여될 수 있도록 접근권한 부여 기능을 보안 요구사항 및 설계에 반영하고 있는가?	ㅇ 정보시스템 설계 시 업무 성격, 프로세스, 보안 요구사항에 따라 다음과 같은 기준을 고려하여 접근권한 부여 기능을 마련하여야 한다. (인증기준 10.2.1 사용자 등록 및 권한 부여, 10.2.3 접근권한 검토 참고) - 사용자별 - 사용자 업무역할별 - 기능별 - 메뉴별 등

No	통제영역	No	통제항목	통제내용	점검항목	설명
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.	정보시스템의 안전한 구현을 위한 코딩 표준이 마련되어야 하며 이에 따라 구현하고 있는가?	ㅇ 정보시스템에서 알려진 기술적 보안 취약점으로 인한 위협을 최소화하기 위하여 안전한 코딩 표준 및 규약을 마련하여야 하며 이에 따라 정보시스템을 구현하여야 한다.
					기술적 보안취약점 점검을 하고 있는가?	ㅇ 코딩 완료 후 안전한 코딩 표준 및 규약 준수 여부를 점검하고 기술적 보안 취약점이 존재하는 지 확인하여 취약점 발견 시 재코딩을 하여야 한다. - 시스템이 안전한 코딩표준에 따라 구현하는 지 소스코드 검증 (소스코드 검증 도구 활용 등) - 코딩이 완료된 프로그램은 운영환경과 동일한 환경에서 취약점 점검도구 또는 모의진단을 통한 취약점 노출 여부를 점검
					구현된 기능이 사전 정의된 보안 요구사항을 충족하는 지 시험을 수행하고 있는가?	ㅇ 정보시스템 구현 완료 후 사전 정의된 보안 요구사항(인증기준 8.1.1 보안 요구사항 정의 참고)을 충족하는 지 확인하기 위하여 시험 시나리오, 체크리스트 등을 작성하여 시험을 수행하여야 한다.
		8.2.2	개발과 운영 환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다.	정보시스템의 개발 및 시험 시스템을 운영 시스템과 분리하고 있는가?	ㅇ 개발과 운영 환경을 분리하지 않은 경우 개발로 인해 운영환경의 성능 및 용량에 영향을 미칠 수 있고 개발자의 비인가된 운영환경으로의 접근이 발생할 수 있다. - 조직 규모가 작거나 인적 자원 부족 등의 사유로 인해 불가피하게 개발과 운영 직무 분리가 어려운 경우, 직무자간의 상호 검토, 상위관리자의 주기적인 직무수행 모니터링 및 변경 사항 검토/승인, 직무자의 책임추적성 확보 등의 보완통제를 마련하여야 한다. (인증기준 6.1.2 직무분리 참고)

No	통제영역	No	통제항목	통제내용	점검항목	설명
		8.2.3	운영환경 이관	운영환경으로의 이관은 통제된 절차에 따라 이루어져야 하고 실행코드는 시험과 사용자 인수 후 실행하여야 한다.	운영환경으로의 이관 절차를 수립 · 이행하고 있는가?	ㅇ 다음과 같은 내용을 고려하여 운영환경으로의 이관 절차를 수립하고 이행하여야 한다. - 개발자 이외의 이관담당자 지정 - 시험완료여부 확인 - 이관 전략 (단계적 이관, 일괄적 이관 등) - 이관 시 문제 대응 방안 - 이관에 대한 책임자 승인
					운영환경으로의 이관 시 발생할 수 있는 문제 대응 방안을 마련하고 있는가?	ㅇ 운영환경으로의 정보시스템 이관이 원활하게 이루어지지 않았을 경우 복귀(rollback) 방안, 이전 버전의 시스템 보관 방안(소프트웨어, 소프트웨어정보, 부가적인 관련 프로그램, 구성파일, 절차, 파라미터 등)등을 마련하여야 한다.
					운영환경에는 서비스 실행에 필요한 파일만을 설치하고 있는가?	ㅇ 운영환경에는 승인되지 않은 개발도구(컴파일러, 편집기 등)와 소스코드(백업본 포함)가 있어서는 안되며 승인된 실행파일만 설치하여야 한다.
		8.2.4	시험데이터보안	시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다.	시스템 시험 과정에서 실제 운영 데이터 사용을 제한하고 있는가?	ㅇ 개인정보를 포함한 회사의 중요한 정보가 시스템 시험과정에서 유출되는 것을 방지하기 위하여 시험데이터는 임의의 데이터를 생성하거나 운영데이터를 가공하여 사용하여야 한다.
					불가피하게 운영데이터를 시험 환경에서 사용할 경우 책임자 승인 등의 인가 절차를 수립 · 이행하고 있는가?	ㅇ 실제 운영 데이터가 시험 환경에서 사용될 경우, 다음과 같은 절차를 수립하고 이행하여야 한다. - 운영 데이터 사용 승인 절차 : 데이터 중요도에 따른 보고 및 승인체계 정의 - 시험용 운영 데이터 사용 기한 및 기한 만료 후 폐기 절차 (예 : 사용 만료 후 즉시 폐기 확인) - 중요 데이터 사용에 대한 시험 환경에서의 접근 권한 및 통제 수립 (예 : 운영환경과 동일한 접근 통제 권고) - 운영데이터 복제 및 사용에 대한 모니터링 및 감사

No	통제영역	No	통제항목	통제내용	점검항목	설명
		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.	소스 프로그램에 대한 변경이력을 관리하고 있는가?	ㅇ 소스 프로그램의 변경(예 : 변경 · 구현 · 이관 일자, 변경 요청 사유 등)을 통제하고 변경된 소스 프로그램에 맞춰서 시스템 관련 문서(예 : 요구사항정의서, 설계서 등)에 대한 변경통제도 함께 수행하여야 한다.
					시스템 운영 장애 등 비상시를 대비하여 이전 시스템의 소스 프로그램을 보관하고 있는가?	ㅇ 신규 시스템 개발 및 기존 시스템 개선 완료 후 시스템 운영 장애 등 비상시를 대비하여 이전 시스템 소스 프로그램을 다음 항목과 함께 보관하여야 한다. - 이전 시스템 환경에 필요한 운영 소프트웨어 (OS) - 이전 시스템 지원 소프트웨어 - 이전 시스템 관련 문서 (예 : 기능적, 기술적 설계서, DB 설계 및 데이터 정의서 등)
					비인가된 자의 소스프로그램의 접근을 통제하기 위하여 절차를 수립 · 이행하고 있는가?	ㅇ 소스 프로그램은 운영 환경이 아닌 별도의 환경에 저장하여야 하며 인가된 담당자에게만 접근을 허용하여야 한다.
8.3	외주개발 보안	8.3.1	외주개발보안	정보시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리 · 감독하여야 한다.	정보시스템 개발을 외주 위탁하는 경우 개발 시 준수해야할 보안 요구사항을 제안요청서에 기재하고 계약시에 반영하고 있는가?	ㅇ 정보시스템을 외주 위탁하는 경우 SW 개발보안을 위한 적절한 개발절차 방법, SW 보안 취약점 진단도구 사용여부 확인에 대하여 제안요청서에 기재하여야 한다. ㅇ 정보시스템을 외주 위탁하여 개발하는 경우 분석부터 설계, 구현에 이르기까지 보안 요구사항을 계약서 상에 분명히 명시하여야 한다.

No	통제영역	No	통제항목	통제내용	점검항목	설명
					외주 위탁업체가 계약서에 명시된 보안요구사항을 준수하는 지 여부를 관리 · 감독하고 있는가?	ㅇ 정보시스템 개발주기(분석-설계-구현-시험)별로 보안요구사항 준수여부를 관리하고 감독하여야 한다. - 기능적, 기술적 요구사항의 반영 여부 - 개발 보안 가이드 준수 여부(시큐어 코딩 등) - 테스트 시 보안요구사항 준수여부 확인 절차 포함 - 개발완료된 시스템에 대한 취약점 점검 등 - 개발인력 대상 SW 개발보안 관련교육
					정보시스템 개발 완료 후 SW 보안취약점 제거여부 진단, SW 보안취약점 발견사항 조치 여부 등을 확인 후 검수 · 인수하고 있는가?	ㅇ 정보시스템 개발 완료 후 보안 요구사항 반영 여부, SW 보안취약점 제거 여부, SW 보안취약점 발견사항 조치여부, 개발자 계정 및 권한 삭제 여부 등을 확인한 후 검수 또는 인수하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
9.1	암호 정책	9.1.1	암호 정책 수립	조직의 중요정보 보호를 위하여 암호화 대상, 암호 강도(복잡도), 키관리, 암호사용에 대한 정책을 수립하고 이행하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.	개인정보 등 중요정보의 전송 및 저장 시 안전한 보호를 위한 암호 정책을 수립·이행하고 있는가?	ㅇ 조직 내 개인정보, 기밀정보, 영업정보, 인사정보와 같은 중요정보에 대해 전송 및 저장 시 다음과 같은 내용이 포함된 암호정책을 수립하여야 한다. - 암호대상 : 취급 정보 민감도 및 중요도에 따라 정의 - 암호화 대상별 암호화 방식과 알고리즘 강도 정의 - 암호키 관리 대책 - 정보 전송 및 저장 시 암호화 방안 - 암호화 관련 시스템 운영 담당자 역할 및 책임 정의 - 암호화 관련 법적 요구사항 반영 (개인정보보호 관련 법률 등) ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제 15 조(개인정보의 보호조치) - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적·관리적 보호조치 기준(고시)' 제 6 조(개인정보의 암호화) - 개인정보보호법 '개인정보의 안전성 확보조치 기준(고시)' 제 7 조(개인정보의 암호화) - 전자금융거래법 '전자금융감독규정(고시)' 제 15 조(해킹 등 방지대책) 및 제 17 조(홈페이지 등 공개용 웹서버 관리대책) - 위치정보의 보호 및 이용에 관한 법률 제 16 조(위치정보의 보호조치 등)

No	통제분야	No	통제항목	통제목적	점검항목	설명
					서비스 이용자 및 내부 사용자(임직원 등) 비밀번호 저장 시 암호화 정책을 수립·이행하고 있는가?	ㅇ 관련 법률에 따라 이용자 및 내부 사용자(임직원 등)의 비밀번호는 안전한 알고리즘(예 : 128 비트 이상. SHA 256, SHA384 등)을 통해 일방향 암호화하여야 한다. - 법률에 따른 대상 이외의 서비스 및 시스템 비밀번호도 일방향 암호 알고리즘을 이용하여 암호화하는 것이 바람직하다. ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제 15 조(개인정보의 보호조치) - 개인정보보호법 '개인정보의 안전성 확보조치 기준(고시)' 제 7 조(개인정보의 암호화) - 전자금융거래법 '전자금융감독규정(고시)' 제 32 조(내부사용자 비밀번호 관리) 및 제 33 조(이용자 비밀번호 관리)
					중요정보 저장 시 암호화 정책을 수립·이행하고 있는가?	ㅇ 다음과 같은 법적 요구사항에 따라 개인정보 저장 시 암호화를 하여야 한다. - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적·관리적 보호조치 기준(고시)' : 주민등록번호, 신용카드번호, 계좌번호를 안전한 알고리즘(128 비트 이상 보안강도 권고 : SEED, AES128 등)으로 암호화하도록 하고 있음 - 개인정보보호법 '개인정보의 안전성 확보조치 기준(고시)' : 인터넷구간 및 인터넷구간과 내부망의 중간지점(DMZ)에 저장하는 고유식별정보(주민등록번호, 여권번호, 면허번호, 외국인등록번호)는 반드시 암호화하여야 하며 내부망에 고유식별정보를 저장할 경우에는 별도의 개인정보 영향평가, 위험도 분석을 시행하여 암호화 적용 여부를 정하도록 하고 있음

No	통제분야	No	통제항목	통제목적	점검항목	설명
						ㅇ 법률에서 정한 대상 이외의 개인정보(휴대폰 번호, 이메일 등), 기밀정보, 영업비밀과 같은 중요정보에 대해서도 저장 시 암호화를 고려하여야 한다. ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제 15 조(개인정보의 보호조치) - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적 · 관리적 보호조치 기준(고시)' 제 6 조(개인정보의 암호화) - 개인정보보호법 '개인정보의 안전성 확보조치 기준(고시)' 제 7 조(개인정보의 암호화)
					정보통신망을 통해 중요정보를 송 · 수신하는 경우 암호화 정책을 수립 · 이행하고 있는가?	ㅇ 다음과 같은 법적 요구사항에 따라 이용자의 개인정보 및 인증정보를 정보통신망을 통해 송 · 수신 할 경우 암호화를 하여야 한다. - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적 · 관리적 보호조치 기준(고시)' : 정보통신망을 통해 이용자의 모든 개인정보 및 인증정보를 송 · 수신 할 경우 보안서버 구축(SSL 인증서 등) 등의 암호화를 하도록 하고 있음 - 개인정보보호법 '개인정보의 안전성 확보조치 기준(고시)' : 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호), 비밀번호, 바이오정보를 정보통신망을 통해 내외부로 송 · 수신하거나 보조저장매체를 통해 전달하는 경우 암호화 하도록 하고 있음

No	통제분야	No	통제항목	통제목적	점검항목	설명
						ㅇ 법률에서 정한 대상 이외의 중요정보를 정보통신망을 통해 송 · 수신 및 보조저장매체를 통한 전달 시 암호화를 고려하여야 한다. ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제 15 조(개인정보의 보호조치) - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적 · 관리적 보호조치 기준(고시)' 제 6 조(개인정보의 암호화) - 개인정보보호법 '개인정보의 안전성 확보조치 기준(고시)' 제 7 조(개인정보의 암호화)
					조직 내 중요정보를 개인용 컴퓨터(PC 등)에 저장할 경우 암호화 정책을 수립 · 이행하고 있는가?	ㅇ 다음과 같은 법적 요구사항에 따라 개인정보를 개인용 컴퓨터(PC 등)에 저장할 경우 암호화를 하여야 한다. - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적 · 관리적 보호조치 기준(고시)' : 서비스 이용자의 개인정보를 개인용컴퓨터(PC)에 저장할 때 암호화 하도록 하고 있음 - 개인정보보호법 '개인정보의 안전성 확보조치 기준(고시)' : 업무용 컴퓨터에 고유식별정보를 저장할 경우 암호화하도록 하고 있음 ㅇ 법률에서 정한 대상 이외의 중요정보를 개인용 컴퓨터(PC 등)에 저장할 경우 암호화를 고려하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
						※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제 15 조(개인정보의 보호조치) - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적 · 관리적 보호조치 기준(고시)' 제 6 조(개인정보의 암호화) - 개인정보보호법 '개인정보의 안전성 확보조치 기준(고시)' 제 7 조(개인정보의 암호화) - 상용소프트웨어에서의 암호기능 이용 안내서 (KISA)
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.	암호키 생성, 이용, 보관, 배포, 복구, 파기 등에 관한 절차를 수립 · 이행하고 있는가?	ㅇ 암호키 생성, 이용, 보관, 배포, 파기에 대해 다음과 같은 항목이 포함된 정책 및 절차를 수립하고 이행하여야 한다. - 암호키 관리 담당자 지정 - 암호키 생성, 보관(소산 백업 등) 방법 - 암호키 배포 대상자 정의 및 배포방법 (복호화 권한 부여 포함) - 암호키 사용 유효기간 (변경주기) - 복구 및 폐기 절차 및 방법 등
					암호키 생성 후 암호키는 별도의 안전한 장소에 소산 보관하고 암호키 사용에 관한 접근권한 부여를 최소화하고 있는가?	ㅇ 생성된 암호키는 암호키 손상 시 시스템 또는 암호화된 정보의 복구를 위하여 별도의 매체에 저장 후 안전한 장소에 보관(소산 백업 포함)하여야 한다. ㅇ 암호키는 암호키를 이용하는 시스템(웹서버 또는 DB 서버 등)에 저장할 수 있으나 물리적으로 분리된 서버에 저장하는 것이 좋다. - 다만 암호키는 하드코딩 방식으로 구현하여서는 안된다. ㅇ 암호키에 대한 접근권한 부여는 최소화하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
					암호키 변경에 관한 정책을 수립 · 이행하고 있는가?	ㅇ 암호기술 구현 안내서(KISA)에서 암호키의 사용기간은 최대 2 년 유효기간은 최대 5 년을 권고하고 있으나 암호키 변경 시 비용과 기업의 정보자산 및 업무 중요도를 고려하여 자체적으로 정하여 적용할 수 있다. ㅇ 다만 암호키 유출, 암호시스템 해킹이 의심되는 경우, 즉시 암호키를 변경하여야 한다. ※ 참고 ※ - 암호기술 구현 안내서 (KISA, http://seed.kisa.or.kr)

No	통제분야	No	통제항목	통제목적	점검항목	설명
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.	접근 통제영역을 정의하고 접근 통제영역별로 접근통제 정책을 수립하고 있는가? - 접근통제 영역별 통제 규칙, 방법, 절차 등 - 예외사항에 대한 안전한 관리절차	ㅇ 접근통제 정책은 네트워크, 서버, 응용프로그램, DB, 모바일기기 등 영역별 접근통제 규칙, 방법, 절차 등을 포함하여야 한다. ㅇ 업무상 불가피하게 접근통제 정책 예외사항이 발생할 경우 이를 보완할 수 있는 통제방안(허가기간, 단말기, 접근위치 등)을 마련한 후 한시적으로 허용하여야 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.	정보시스템의 사용자 계정 등록 · 삭제(비활성화) 및 접근권한 등록 · 변경 · 삭제에 관한 공식적인 절차를 수립 · 이행하고 있는가?	ㅇ 정보시스템 영역별(네트워크장비, 서버, 응용프로그램, DB 등)로 사용자 계정 등록 · 삭제(비활성화) 및 접근권한 등록 · 변경 · 삭제에 관한 공식적인 검토 · 승인절차를 수립하여 이행하여야 한다. ㅇ 정보시스템의 사용자 계정 등록 · 삭제(비활성화) 및 접근권한 등록 · 변경 · 삭제를 담당자가 임의대로 수행하여서는 안되며 수립된 절차에 따라 책임자의 승인이 완료된 후 이루어져야 한다. ㅇ 사용자 계정 발급 및 접근권한 부여의 적정성 검토를 위하여 정보시스템에 등록된 사용자 계정 및 접근권한 부여 현황을 문서 또는 시스템으로 기록 · 관리하여야 한다. (인증기준 10.2.3 접근권한 검토 참고)
					정보시스템의 사용자 계정 생성 및 변경 시 직무별 접근권한 분류 체계 따라 업무상 필요한 최소한의 권한만을 부여하고 있는가?	ㅇ 직무별 또는 역할별 정보시스템 접근권한을 정의한 접근권한 분류 체계를 관리하여야 한다. ㅇ 정보시스템에 대한 접근권한은 업무 수행에 필요한 최소한으로 할당하여야 하며, 업무 담당자 직무에 따라 차등 부여하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
					사용자 계정 등록 · 삭제(비활성화) 및 접근권한 등록 · 변경 · 삭제 권한을 한 사람에게 집중되지 않도록 하고 불가피한 경우, 접근권한 활동의 적정성을 주기적으로 검토하고 있는가?	ㅇ 사용자 계정 등록 · 삭제(비활성화) 및 접근권한 등록 · 변경 · 삭제 권한을 한 사람에게 집중 부여하여서는 안되며 사용자 접근권한 변경이력에 대한 감사추적이 될 수 있도록 이력을 기록하여야 한다. - 다만 불가피하게 계정관리 및 권한부여 권한이 한 사람에게 집중될 경우 권한 부여 활동의 적정성을 주기적으로 검토하여야 한다. ㅇ 또한 아웃소싱 업체에게 접근권한 설정 권한을 주는 경우 중요 권한부여 시에는 내부 조직 책임자의 승인을 득하도록 하여야 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.	관리자 및 특수 권한은 최소한의 인원에게만 부여하고 권한 부여 시 책임자 승인 절차를 수립하고 있는가?	ㅇ 관리자(root, administrator, admin 등 최종 권한) 및 특수 권한(배치나 모니터링을 위하여 부여받은 권한, 계정 및 접근 설정 권한 등) 할당 및 사용 시에는 책임자의 승인을 포함한 인가 절차를 따라야 한다.
					관리자 권한 및 특수 권한을 식별하여 별도 목록으로 관리하고 있는가?	ㅇ 관리자 권한을 식별하여 사용자를 최소한으로 제한하고 관리자 권한의 계정은 별도의 목록으로 관리하는 등 통제절차를 수립하여야 한다. ㅇ 특수 권한은 반드시 필요한 경우에만 할당하도록 하며 특수 권한을 부여 받은 계정은 식별이 가능하도록 관리하여야 한다. ㅇ 정보보호시스템(침입차단시스템 등), 응용프로그램 등의 관리자 계정 또한 특수 목적을 위한 계정으로 인식하고 관리하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
					외부자에게 부여하는 계정은 한시적으로 부여하고 사용이 끝난 후에는 즉시 삭제 또는 정지하고 있는가?	ㅇ 정보시스템 유지보수를 위하여 방문하는 외부자에게 부여하는 계정은 필요시에만 생성하고 유지보수 완료 후 즉시 삭제 또는 정지하는 절차를 적용하여야 한다. (3.2.2 외부자 계약 만료 시 보안 참고)
		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.	직무별 또는 역할별 정보시스템 접근권한을 정의한 접근권한 분류 체계를 수립하고 있는가?	ㅇ 접근권한 분류체계(권한분류표 등)를 마련하여 분류체계를 기반으로 권한부여에 대한 적정성 여부를 검토할 수 있도록 하여야 한다. - 접근권한 분류체계는 직무별 또는 역할별로 구분하여 수립할 수 있다. - 예를 들어 개인정보처리시스템의 경우에는 개인정보처리(조회, 변경, 삭제, 다운로드 등) 권한 구분이 가능하도록 권한관리를 하여야 한다.
					정보시스템 및 중요정보에 대한 접근권한 검토 기준, 검토주체, 검토방법, 주기 등을 정하여 정기적 검토를 이행하고 있는가?	ㅇ 다음과 같은 항목을 기준으로 접근권한 부여의 적정성을 검토하여야 한다. - 공식적인 절차에 따른 접근권한 부여 여부 - 접근권한 분류체계의 업무목적(직무) 및 보안정책 부합 여부 - 접근권한 부여 승인자에 대한 적절성 - 직무변경 시 기존 권한 회수 후 신규업무에 적합한 권한부여 여부 - 업무 목적 이외의 과도한 전급권한 부여 ㅇ 또한 장기 미사용, 직무변경, 휴직, 퇴직, 업무시간 외 사용 등의 경우에도 접근권한 사용 현황을 검토하여 다음과 같은 조치를 취해야 한다. - 장기 미사용(3 개월 권고) 계정 및 접근권한 삭제 - 직무변경 시 기존 권한을 회수하고 신규업무에 적합한 권한을 부여 - 휴직(병가, 출산 등) 시 계정 및 권한 회수

No	통제분야	No	통제항목	통제목적	점검항목	설명
						- 퇴직 시 지체없이 계정을 삭제 (단, 계정삭제가 어려운 경우 권한 회수 한 후 계정을 정지) ※ 계정 정지 또는 비활성화를 하는 경우에는 계정 활성화가 불가능하도록 조치 필요 ㅇ 접근권한 검토 기준별로 검토주체, 검토방법, 주기(최소 분기 1회 이상 권고) 등을 구체적으로 정의하여 이행하여야 한다. ㅇ 접근권한 검토 대상은 개인정보처리시스템 등 서비스 및 업무에 영향을 줄 수 있는 주요 정보시스템 및 정보보호시스템으로 정할 수 있다. (인증기준 4.2.1 보안등급과 취급 참고)
					접근권한의 검토 결과 접근권한 오남용 등의 이상징후가 발견된 경우 그에 따른 조치절차를 수립 · 이행하고 있는가?	ㅇ 접근권한 검토 결과 권한의 과다 부여, 오남용 등 의심스러운 상황이 발견된 경우, 원인 분석, 보완대책 마련, 보고체계 등이 포함된 절차를 수립하고 이행하여야 한다. ㅇ 접근권한 검토 후 변경 적용된 권한에 대해서는 사용자 및 관련자에게 통지하여야 한다.
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.	정보시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하고 있는가?	ㅇ 정보시스템(네트워크 장비, 서버, 응용프로그램, DB 등) 및 정보보호시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하여야 한다. ㅇ 공개 인터넷망을 통하여 접속을 허용하는 주요 정보시스템의 경우 아이디, 패스워드 기반의 사용자 인증 이외의 강화된 인증수단(OTP, 공인인증서 등)적용을 고려하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
						ㅇ 특히 법적 요구사항에 따른 강화된 인증방식 사용이 필요한 경우 해당 정보시스템 접근 시 강화된 인증방식을 적용하여야 한다. ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적 · 관리적 보호조치 기준 (고시)' 제 4 조(접근통제)
					싱글사인온 등의 인증 방법을 사용하는 경우 이에 대한 별도의 보호대책을 수립하고 있는가?	ㅇ 싱글사인온 등 다양한 정보시스템에 대한 사용자 인증을 용이하게 하는 시스템을 운영하는 경우 병목 및 침투(인증 도용 등) 시 피해 확대 가능성이 있으므로 별도의 보안대책(주요 정보시스템 재인증 등)을 마련하여야 한다. ※ 싱글사인온(SSO : Single Sign-On) : 하나의 아이디로(단 한번의 로그인) 조직의 각종 정보시스템에 접속할 수 있는 응용프로그램을 의미
		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.	정보시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자의 사용을 제한하고 있는가?	ㅇ 정보시스템에서 사용자를 유일하게 구분할 수 있는 식별자(아이디)를 할당하여 모든 사용자의 책임추적성을 보장하여야 한다. ㅇ 관리자 및 특수권한 계정의 경우 추측 가능한 식별자(root, admin, administrator 등)의 사용을 제한하여야 한다. - 시스템 설치 후 제조사 또는 판매사의 기본계정 및 시험계정 등은 제거 또는 추측이 어려운 계정으로 변경하여야 한다.
					동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받고 있는가 ?	ㅇ 정보시스템 환경 상 혹은 업무상 불가피하게 사용자 계정을 공유하여 사용할 경우, 사유와 타당성을 검토하여 책임자의 승인을 받아야 하며 책임추적성을 보장할 추가적인 통제 방안을 적용하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
		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.	정보시스템 및 정보보호시스템에 대한 안전한 사용자 패스워드 관리절차를 수립 · 이행하고 있는가?	ㅇ 조직 내부 주요 정보시스템 및 정보보호시스템에 대한 사용자의 안전한 패스워드 사용 및 관리절차(작성규칙 등)를 다음과 같이 수립하고 이행하여야 한다. - 사전공격(Dictionary attack)에 취약하지 않도록 문자(영문 대소문자), 숫자, 특수문자 등을 일정 자리수 이상으로 조합하도록 패스워드 작성규칙을 수립하고 주기적으로 변경 (분기 1 회 이상 권고) - 연속 숫자, 생일, 전화번호, 아이디 등 추측하기 쉬운 개인 신상정보를 활용한 취약 패스워드사용 제한 - 정보시스템 도입 시 초기/임시 패스워드 로그인 시 지체 없이 변경 - 패스워드 처리(입력, 변경) 시 마스킹 처리 - 종이, 파일, 포켓용 소형기기 등에 패스워드 기록·저장을 제한하고 부득이하게 기록 · 저장해야 하는 경우 암호화 등의 보호대책 적용 - 정보시스템 침해사고가 발생 또는 패스워드의 노출 징후가 의심될 경우 지체없이 패스워드 변경 - 패스워드 자동 저장 금지 - 개인정보취급자의 경우, 패스워드 작성 규칙에 대해 법적 요구사항 반영 등 ㅇ 응용프로그램인 경우 안전한 패스워드 작성규칙, 추측하기 쉬운 패스워드 사용 제한, 발급받은 초기/임시 패스워드 최초 로그인 시 변경, 패스워드 주기적 변경 유도, 패스워드 입력 시 마스킹 처리 등의 규칙은 기술적 기능으로 반영하여야 한다. ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적 · 관리적 보호조치 기준(고시)' 제 4 조(접근통제)

No	통제분야	No	통제항목	통제목적	점검항목	설명
						: 영문 대문자, 영문 소문자, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성 - 개인정보보호법 '개인정보 안전성 확보조치 기준 제5조(비밀번호관리)'에 대한 해설서 : 영문 대문자, 영문 소문자, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성
					정보시스템 관리자 패스워드는 별도 목록(문서 또는 파일)으로 유지 · 관리하고 비밀등급에 준하는 보호대책을 적용하고 있는가?	ㅇ 정보시스템의 관리자 패스워드는 일반 사용자 패스워드와 별도로 관리하여야 하며 관리자 패스워드를 기록한 문서 또는 저장장치(보안 USB 등)는 비밀등급에 준하여 취급하고 내화 금고 등 잠금장치로 비인가자의 접근을 통제할 수 있는 안전한 곳에 보관하여야 한다.
					패스워드 관리 책임이 사용자에게 있음을 주지시키고 있는가?	ㅇ 교육, 홍보, 안내 등을 통해 사용자 계정 및 패스워드의 안전한 관리 절차에 대해 충분하게 공지하고 그에 따른 책임이 사용자에게 있음을 주지시켜야 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.	고객, 회원 등 서비스 이용자가 접근하는 정보시스템 또는 웹서비스의 안전한 이용을 위하여 계정 및 패스워드 관리절차를 수립 · 이행하고 있는가?	ㅇ 서비스 이용자 계정 및 패스워드의 도용을 방지하기 위하여 다음과 같은 항목이 포함된 관리절차를 수립하고 이행하여야 한다. -안전한 패스워드 작성규칙 수립 (패스워드 복잡도 등) - 연속 숫자, 생일, 전화번호, 아이디 등 추측하기 쉬운 개인 신상정보를 활용한 취약 패스워드사용 제한 - 초기/임시 패스워드를 발급할 경우 최초 로그인 시 변경 - 주기적인 패스워드 변경 유도 - 패스워드 처리(입력, 변경) 시 마스킹 처리 - 이용자 패스워드 분실 · 도난 시 안전한 재발급 절차(본인인증 등)를 수립하여 재발

No	통제분야	No	통제항목	통제목적	점검항목	설명
						급을 통한 도용 방지 등 (임시 패스워드 발급 시 안전한 전송 및 로그인 후 변경) ㅇ 안전한 패스워드 작성규칙, 추측하기 쉬운 패스워드 사용 제한, 발급받은 초기/임시 패스워드 최초 로그인 시 변경, 패스워드 주기적 변경 유도, 패스워드 입력 시 마스킹 처리 등의 규칙은 기술적 기능으로 반영하여야 한다.
					이용자 계정 및 패스워드 관리절차 관련 내용을 홈페이지 또는 메일 등을 통하여 사용자가 쉽게 확인하고 이해할 수 있도록 공지하고 있는가?	ㅇ 고객, 회원 등 서비스 이용자가 접근하는 정보시스템 또는 웹서비스의 안전한 이용을 위하여 계정 및 패스워드의 관리절차를 마련하고 관련 내용을 홈페이지 또는 메일 등을 통하여 사용자가 쉽게 확인하고 이해할 수 있도록 공지하여야 한다.
10.4	접근통제 영역	10.4.1	네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 접근통제리스트, 네트워크 식별자 등에 대한 관리절차를 수립하고 서비스, 사용자 그룹, 정보자산의 중요도에 따라 내 · 외부 네트워크를 분리하여야 한다.	접근통제 정책에 따라 인가된 사용자만이 네트워크에 접근할 수 있도록 네트워크 식별자(IP) 할당 등을 통제하고 있는가?	ㅇ 정보시스템, PC 등에 IP를 부여하는 경우 승인 절차에 따라 부여하고 허가되지 않은 IP의 사용은 통제하여야 하며 인가된 사용자/단말만이 네트워크에 접근할 수 있도록 하여야 한다. ㅇ 특별히 업무를 위하여 필요하지 않은 경우 네트워크 장비에 설치된 포트, 서비스를 제거 또는 차단하여야 한다.
					네트워크 구성 변경 시에는 공식적인 변경 관리 절차를 준수하고 자체적인 보안성 검토를 수행하고 있는가?	ㅇ 네트워크 신규 생성 및 변경은 조직의 정보보호 환경에 많은 영향을 미치기 때문에 주요 변경에 대해서는 보안성을 검토하고 책임자의 승인을 받아야 한다. (인증기준 11.1.2 변경관리 참고)
					네트워크를 구성하는 주요자산 목록, 구성도, IP 현황을 최신으로 유지하고 안전하게 관리하고 있는가?	ㅇ 네트워크를 구성하는 주요자산목록, 구성도, IP 현황 등을 최신으로 유지하고 외부에 유출되지 않도록 대외비 이상으로 안전하게 관리하여야 한다. - 최소한의 인력만 접근, 전자 문서 형태로 관리할 경우 암호 설정 등

No	통제분야	No	통제항목	통제목적	점검항목	설명
					내부 네트워크 IP 주소는 사설 IP로 할당하고 국제권고표준을 따르고 있는가?	○ 내부망에서의 주소 체계는 사설 IP 주소 체계를 사용하고 내부 주소체계를 외부에 유출되지 않도록 하여야 하며 외부 네트워크와의 연결지점에 NAT(Network Address Translation) 기능을 적용하여야 한다. ○ 사설 IP 주소를 할당하는 경우 국제표준에 따른 사설IP 주소대역을 사용하여야 한다. ※ 사설 IP 주소대역 ※ - 10.0.0.0~10.255.255.255 - 172.16.0.0~172.31.255.255 - 192.168.0.0~192.168.255.255)
					서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 있는가?	○ 핵심 업무영역의 네트워크는 위험평가를 통해 물리적 또는 논리적으로 영역을 분리하고 영역간 접근통제를 하여야 한다. - (DMZ)외부로부터의 접근이 불가피한 웹서버, 메일서버 등의 공개용 서버는 DMZ 영역에 위치시키고 공개서버를 경유하여 내부 업무망으로의 접근이 이루어지지 않도록 접근통제를 수행하여야 한다. - (서버팜) 서버들이 위치하는 영역(서버팜)은 다른 네트워크 영역과 구분되고 인가받은 내부사용자의 접근만을 허용하도록 접근통제 정책을 적용하여야 한다. - (DB 팜) 조직의 중요정보가 저장된 DB가 위치한 네트워크 영역은 다른 네트워크 영역과 분리하여야 한다. - (운영환경) 서버, 보안장비, 네트워크장비 등을 운영하는 인력이 사용하는 네트워크 영역은 별도로 분리하여야 한다. - (개발환경) 개발업무(개발자 PC, 개발서버, 테스트서버 등)에 사용되는 네트워크는 별도망으로 구성하여 운영에 사용되는 네트워크와 분리하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
						- (외부자) 외부 사용자에게 서비스를 제공하는 네트워크(외주용역, 민원실, 교육장 등)는 내부 업무용 네트워크와 분리하여야 한다. - (기타) 업무망의 경우 업무의 특성, 중요도에 따라 네트워크 대역 분리기준을 수립하여 운영하여야 한다. ※ 다만 기업의 규모 등을 고려하여 서버팜/DB 팜을 세부적으로 분리하기 어려운 경우 추가적인 보완대책을 마련하여야 한다. (호스트 기반 접근통제 등)
					접근통제 정책에 따라 분리된 네트워크 영역간에 침입차단시스템 등을 통한 접근통제를 하고 있는가?	○ 침임차단시스템, ACL(Access Control List) 설정이 가능한 네트워크 장비 등을 활용하여 네트워크 영역 간 업무수행에 필요한 서비스의 접근만 허용하도록 통제하여야 한다. - 특히 외부(인터넷)로부터의 불법적인 접근 및 침해시도를 방지하기 위해 침입차단시스템 등을 통하여 내부 네트워크 접근은 더욱 엄격하게 통제하여야 한다.
					물리적으로 떨어진 IDC 센터, 지사, 대리점 등과의 네트워크 연결 시 전용회선을 구축하고 전용선 구축이 불가능한 경우 VPN(가상사설망) 등의 대책을 마련하고 있는가?	○ 물리적으로 떨어진 장소와 네트워크 연결이 필요한 경우 전용회선 또는 VPN을 활용하여 보안성을 강화하여야 한다.
		10.4.2	서버 접근	서버별로 접근이 허용되는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 적용하여야 한다.	서버별로 접근이 허용된 사용자를 명확하게 식별·인증하고 안전한 접근수단을 적용하고 있는가?	○ 서버별로 접근이 허용된 사용자를 명확하게 식별하여 접속 시 인증하고 원격 접근 시 암호화된 통신 수단(ssh 등)을 사용하여야 한다.
					중요 서버의 연결시간을 제한하고 있는가?	○ 서버 사용자 접속 후 일정시간 사용이 없으면 연결을 종료(세션 타임아웃 시간 설정)하여야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
					서버의 사용목적과 관계없는 서비스를 제거하고 있는가?	○ 서버의 사용목적과 관련이 없거나 침해사고를 유발할 수 있는 서비스 또는 포트를 확인하여 제거 또는 차단하여야 한다. ○ 시스템관리를 위한 프로그램의 설치 및 사용에 대해서는 인가 및 통제 절차를 수립하여야 한다.
					자체 DNS 를 사용하는 경우 DNS 서버의 과부하 및 침해사고를 예방하기 위한 보호대책을 수립 · 이행하고 있는가?	○ DNS 서버의 부하분산 방안(DNS 서버 이중화 또는 공개된 외부 DNS 서버)을 수립하여 적용하여야 한다. ○ DNS 서버의 환경변수 설정 및 설정 파일 정보에 대한 기록을 정기적으로 백업하고 DNS 스푸핑, DDoS 공격 등을 예방하기 위한 보호대책을 수립하여야 한다.
					주요서비스를 제공하는 서버는 독립된 서버로 운영하고 있는가?	○ 외부에 서비스를 제공하는 웹, 민감한 정보를 보관 · 처리하고 있는 DB 와 응용프로그램 등은 공용 장비로 사용하지 않고 독립된 서버를 사용하여야 한다.
		10.4.3	응용 프로그램 접근	사용자의 업무 또는 직무에 따라 응용프로그램 접근권한을 제한하고 불필요한 중요정보 노출을 최소화해야 한다.	응용프로그램 및 중요정보 접근을 통제하기 위하여 사용자의 업무에 따라 접근권한을 차등 부여하고 있는가?	○ 사용자의 업무(직무)에 따라 응용프로그램 접근권한을 분류하여 업무(직무)별 권한의 차등 부여가 가능하여야 하며 업무 목적에 맞게 접근권한 부여를 최소화하여야 한다.
					중요정보의 노출(조회, 출력, 다운로드 등)을 최소화 하도록 응용 프로그램을 구현하고 있는가?	○ 사용자 권한과 법적 요구사항에 따라 중요정보의 필요한 부분만 표시되도록 하는 기능을 구현하여 중요정보의 노출을 통제하여야 한다. ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적 · 관리적 보호조치 기준(고시)' 제 8 조(출력 · 복사시 보호조치) 및 제 9 조(개인정보 표시 제한 보호조치)

No	통제분야	No	통제항목	통제목적	점검항목	설명
					일정 시간동안 입력이 없는 세션은 자동 차단하고, 동일 사용자의 동시 세션 수를 제한하고 있는가?	○ 일정시간 동안 입력이 없는 세션은 타임아웃 설정을 통해 연결을 차단하여야 한다. 단, 세션 타임아웃의 예외가 있는 경우 충분히 타당성을 검토하고 관련 책임자의 승인을 받아야 한다. ○ 주요 응용프로그램은 동일 사용자가 동시 접속할 수 없도록 하여야 한다.
					관리자 전용 응용프로그램(관리자 웹페이지, 관리콘솔 등)을 외부에 오픈되지 않도록 접근통제하고 있는가?	○ 관리자 전용 응용프로그램(관리자 웹페이지, 관리콘솔 등)은 외부 오픈을 차단하고 특정 위치의 단말에서만 접근 가능하도록 접근을 통제하고 로깅하여야 한다.
		10.4.4	데이터 베이스 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.	데이터베이스 관리자 및 사용자의 직무별 접근 통제 정책을 수립하고 이에 따라 운영하고 있는가?	○ DB 서버 및 DBMS 접속에 대한 권한은 데이터베이스 관리자(DBA : Database Administrator), 사용자 등으로 구분하고 직무별 접근 통제 정책을 수립하여 이행하여야 한다. ○ 데이터베이스 관리자(DBA) 및 사용자의 활동을 감사추적할 수 있도록 유일한 식별자를 할당하여야 한다. (인증기준 10.3.2 사용자 식별 참고)
					중요정보를 저장하고 있는 데이터베이스는 별도의 네트워크 영역으로 구분하고 있는가?	○ 중요정보(개인정보, 기밀정보 등)를 저장하고 있는 데이터베이스 및 WAS(WebApplication Server)는 외부에 서비스를 제공하는 공개 네트워크 영역(DMZ)에 위치하여서는 안된다. (웹서버와 분리) - 단 WAS 가 웹서버와 일체형으로 구성되어 분리가 어려운 경우에는 예외로 할 수 있다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
					데이터베이스 접근을 허용하는 IP, 포트, 응용프로그램을 통제하고 있는가?	ㅇ 일반 사용자는 응용프로그램을 통해서만 데이터베이스에 접근 가능하도록 하여야 하며 DBMS 에 직접 접속하는 경우 DB 관리용 프로그램(DB 툴 등) 및 사용자(데이터베이스 관리자(DBA) 등)를 통제하여야 한다. ㅇ DMZ 구간에 위치한 웹서버에서 내부 네트워크 DB 로 접근할 경우 관련 포트 이외의 서비스포트(ftp, telnet, 터미널 등)는 차단하여야 한다.
					중요정보를 포함하고 있는 데이터베이스의 경우 데이터베이스 계정 또는 오브젝트(테이블, 뷰 또는 컬럼 등)수준에서 사용자 접근을 통제하고 있는가?	ㅇ 중요정보(개인정보, 인사정보, 급여정도 등)가 포함된 테이블 또는 컬럼에 대해서는 업무상 취급 권한이 있는 자(개인정보취급자 등)만이 사용할 수 있도록 제한하여야 한다. ㅇ DBMS 관리를 위한 계정은 데이터베이스 관리자(DBA)만이 사용할 수 있도록 하여야 한다. ㅇ 사용하지 않는 계정, 테스트 계정, 기본 계정 등은 삭제 또는 접근이 불가능하도록 조치하여야 한다. ㅇ 응용프로그램(웹 등)용으로 부여된 데이터베이스 계정의 경우 데이터베이스 관리자(DBA), 사용자 등이 공용으로 사용하지 않아야 한다.

No	통제분야	No	통제항목	통제목적	점검항목	설명
					중요정보를 저장하고 있는 데이터베이스의 경우 사용자 접속내역을 기록하고 접근의 타당성을 정기적으로 검토하고 있는가? - 최소 월 1 회 이상 검토 - 검토 후 이상여부에 대한 적절한 조치 여부 - 법적 요구사항 준수 여부 - 개인정보 등 중요정보를 대량으로 조회, 변경, 삭제와 관련된 이상징후	ㅇ DB 접근의 타당성을 최소 월 1 회 이상 주기적으로 검토하는 것이 바람직하다. 개인정보처리시스템(DB)의 경우 개인정보취급자가 접속한 기록을 월 1 회 정기적으로 확인감독하도록 하고 있다. (인증기준 11.6.3 접근 및 사용 모니터링 참고)
		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, 접근범위, 기기 보안설정, 오남용 모니터링 등의 접근통제 대책을 수립하여야 한다.	모바일기기에 대한 보안 통제 정책을 마련하고 이에 따라 이행하고 있는가? - 모바일 기기 허용기준 - 모바일 기기를 통한 업무 사용범위 - 모바일 기기 사용시 승인 절차 및 방법 - 모바일 기기 인증(MAC 인증 등) - 모바일 기기 이용에 따른 보안 설정 정책 및 오남용 모니터링 대책	ㅇ 모바일 기기를 업무 목적으로 사용하는 경우 다음을 고려하여 모바일기기 허용기준을 마련하고 모바일기기정보(MAC, 시리얼번호, 사용자 등)을 목록화하여 관리하여야 한다. - 내 · 외부 자산(법인스마트폰, 개인스마트폰 등) - 기기종류(노트북, 스마트패드, 스마트폰 등) ㅇ 모바일기기를 통한 업무를 허용할 경우 범위를 명확히 하고 접근을 통제하여야 한다. ㅇ 모바일기기를 통한 업무를 허용할 경우 기기이용에 대한 승인절차를 거쳐야 하며 접속시 기기인증을 수행하는 방안을 마련하고 이행하여야 한다. ※ 기기인증 : 네트워크 장비를 통한 인증, 전용장비(NAC 등)을 통한 인증, AP 인증 등 ㅇ 모바일 기기 이용에 따른 보안정책 및 모니터링 대책을 마련하여야 한다. - 모바일 기기에 대한 이용자 보안 설정 정책 (백신설치, 보안패치, 공공장소에서의 사용주의, 분실시 데이터초기화 등)

No	통제분야	No	통제항목	통제목적	점검항목	설명
						- 내부자료 유출 방지를 위한 정책, 교육, 책임부여, 처벌기준 - 모바일 기기의 오남용 여부를 파악할 수 있는 모니터링 대책 - 모바일 장비에 설치되는 소프트웨어의 안전성을 점검대책
		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.	다음과 같은 인터넷 접속에 대한 정책을 수립하고 있는가? - 인터넷 연결시 네트워크 구성 정책 - 이메일, 인터넷 사이트의 접속, 소프트웨어 다운로드 및 전송 등의 사용자 접속정책	ㅇ 인터넷 접속에 대한 보안정책을 수립하여야 한다. 보안정책에는 인터넷 연결 시의 네트워크 구성 정책, 사용자 접속정책을 포함하여야 한다.
					중요정보를 취급 · 운영하는 주요 직무자를 식별하여 인터넷 접속을 제한하고 있는가?	ㅇ 중요정보를 취급·운영하는 주요 직무자(개인정보취급자, 시스템관리자 등)의 경우 인터넷 접속 또는 서비스(P2P, 웹하드, 웹메일, 메신저 등)를 제한하는 등의 보호대책을 수립하고 이에 따라 이행하여야 한다. (인증기준 6.1.1 주요 직무자 지정 및 감독 참조) - 다만 일정규모 이상의 정보통신서비스제공자는 개인정보를 처리(다운로드, 파기, 접근권한 설정)하는 개인정보취급자 컴퓨터의 외부 인터넷 접속을 차단하여야 한다. ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제 15 조(개인정보의 보호조치) - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적 · 관리적 보호조치 기준(고시)' 제 4 조(접근통제)

No	통제분야	No	통제항목	통제목적	점검항목	설명
					내부 직원의 업무용 PC 에서 유해사이트 등의 접속을 차단하고 있는가?	ㅇ 외부로부터의 악성코드 유입을 방지하기 위하여 내부 업무용 PC 의 유해사이트(P2P, 웹하드 등) 접속에 대한 차단조치를 수행하여야 한다.
					내부 서버에서 외부 인터넷접속을 제한하고 있는가?	ㅇ 악성코드 유입, 리버스커넥션이 차단되도록 내부 서버(DB 서버, 파일서버, 패치서버 등)에서 외부 인터넷 접속을 제한하여야 한다. 부득이하게 허용할 필요가 있는 경우 관련 위험 분석을 통해 보호대책을 마련하고 정보보호책임자의 승인을 얻어야 한다.
					인터넷 PC 와 내부 업무용 PC 를 분리하고 있는 경우 PC 간의 자료전송을 통제하고 있는가?	ㅇ 원칙적으로 인터넷망과 내부망 PC 간의 자료전송은 차단하여야 하며 필요한 경우 별도의 통제절차를 거쳐 전송하고 해당 로그를 주기적으로 검토하여야 한다.

No	통제영역	No	통제항목	통제내용	점검항목	설명
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.	정보시스템 운영을 위한 운영절차(또는 매뉴얼)를 수립하고 있는가?	ㅇ "정보시스템"은 정보의 수집 · 가공 · 저장 · 검색 · 송신 · 수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 의미한다. 즉 서버, PC 등 단말기, 보조기억매체, 네트워크 장치, 응용프로그램 등 정보의 수집 · 가공 · 저장 · 검색 · 송신 · 수신에 필요한 하드웨어 및 소프트웨어를 말한다. ㅇ 각 정보시스템 특성에 적합한 운영절차(또는 매뉴얼)를 수립하여야 한다. 이는 담당자 부재 시 혹은 신입직원 등이 긴급 상황에서 별다른 인수인계 없이도 정의된 절차에 따라 대응이 가능하도록 하기 위한 것이다. ㅇ 정보시스템 운영절차에는 다음과 같은 내용을 포함하여야 한다. - 정보시스템 환경설정(접근통제 : ACL, 패스워드 등) 방법 - 정보시스템 변경 절차 - 정보시스템 보안설정 방법 (인증기준 11.2.1 정보시스템 인수 참고) - 접근권한 설정 방법 - 오류 및 예외 사항 처리 방법 - 문제 발생 시 긴급종료/재동작/복구 방법 - 시스템 모니터링 방안 : 보안감사로그, 각종 이벤트 로그 확인방법 - 긴급상황 발생 시 비상연락망 등

No	통제영역	No	통제항목	통제내용	점검항목	설명
					각종 정보시스템 운영절차(또는 매뉴얼)를 목록으로 관리하고 주기적인 내용 검토를 하고 있는가?	ㅇ 신규 정보시스템 도입, 유지보수업체 변경 등 정보시스템 관련 환경 변화가 있을 경우 운영절차 내용을 검토하여 변경 사항을 반영하여야 한다. 또한 운영절차(매뉴얼)의 작성일자, 변경일자, 검토 및 승인자 등에 대한 이력도 함께 관리하여야 한다. ㅇ 운영절차(또는 매뉴얼)는 정보시스템 운영과 관련된 중요 자료이므로 조직의 민감한 정보(IP 등 시스템 정보)가 포함된 경우 대외비 문서로 지정(인증기준 4.2.1 보안등급과 취급 참고)하여 해당 업무 관련자만 접근할 수 있도록 통제하고 업무상 재해에 대비하여 복사본을 별도로 마련하여 소산 보관하는 것이 좋다. (인증기준 13. 재해복구 참고)
					정보시스템 운영을 외부 위탁하는 경우 운영절차(매뉴얼) 수립 여부를 확인하고 있는가?	ㅇ 정보시스템 운영을 외부 위탁하는 경우 외부 아웃소싱 업체가 정보시스템 운영절차(매뉴얼)를 수립하고 있는지 확인하고 운영절차에 따라 정보시스템 운영을 보장하도록 계약서에 관련 내용을 명시하여야 한다. - 운영절차(매뉴얼)은 외부 아웃소싱 업체가 자체 수립하거나 위탁사의 절차를 준용하여 수립할 수 있다. ㅇ 운영 점검항목 등을 통해 외부 아웃소싱 업체가 운영절차를 준수하고 있는지 주기적으로 확인하여야 한다. (인증기준 3.외부자 보안 참고)

No	통제영역	No	통제항목	통제내용	점검항목	설명
		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.	정보시스템 관련 자산(하드웨어, 운영체제, 상용 소프트웨어 패키지 등) 변경에 관한 절차를 수립 · 이행하고 있는가?	o 운영체제 업그레이드, 상용 소프트웨어 설치, 운영 중인 응용프로그램 기능 개선, 네트워크 구성 변경, CPU/메모리/저장장치 증설 등 정보시스템 관련 자산 변경이 필요한 경우 변경요청, 책임자 검토 · 승인, 변경확인, 변경이력관리 등의 공식적인 절차를 수립하고 이행하여야 한다.
					정보시스템 관련 자산 변경을 수행하기 전 성능 및 보안에 미치는 영향을 분석하고 있는가?	o 정보시스템 관련 정보자산 변경이 필요한 경우 변경에 따른 보안, 성능, 업무 등에 미치는 영향을 분석하여 변경에 따른 영향을 최소화 할 수 있도록 변경을 이행하고 변경 실패에 따른 복구방안을 사전에 고려하여야 한다. - 변경의 규모를 고려하여 영향 분석 대상 기준을 자체적으로 정할 수 있다.
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.	정보시스템 도입 또는 개선 계획을 수립하고 있는가?	o 새로운 정보시스템(서버, 네트워크 장비, 상용 소프트웨어 패키지) 및 보안시스템 도입 시 도입 타당성 분석 등의 내용이 포함된 도입계획을 수립하여야 한다. - 현재 시스템 자원의 이용률, 사용량, 능력한계에 대한 분석 - 추가 자원의 필요성 및 시기에 대한 예상 - 성능, 안전성, 신뢰성, 보안성, 법규 등을 포함한 시스템 자원의 기능적, 운영적 요구사항 - 기존 시스템과의 호환성, 상호운영성, 기술표준에 따른 확장성 o 이 기준(11.2.1 정보시스템 인수)에서 적용되는 "정보시스템" 범위는 서버, 네트워크 장비, 상용 소프트웨어 패

No	통제영역	No	통제항목	통제내용	점검항목	설명
						키지에 해당하며 "보안시스템" 도입 및 인수 시에도 적용하여야 한다. - 다만 응용프로그램 신규 개발 및 개선 시 보안요구사항 정의, 구현 및 시험 등에 관한 내용은 "8. 시스템 개발 보안"을 참고하여 적용하면 된다.
					정보시스템 인수 여부를 판단하기 위한 시스템 인수기준을 수립하고 있는가?	o 정보시스템 인수 여부를 판단하기 위하여 정보시스템 및 보안시스템의 기본 보안설정 등이 반영된 인수 승인 기준을 수립하여야 한다. 또한 시스템 구매계약서 등에 반영하여 도입 과정에서 인수기준을 준수하도록 함으로써 기본 보안 설정 미흡으로 발생할 수 있는 보안취약점을 최대한 제거한 후 인수할 수 있어야 한다. ※ 기본 보안 설정 : 불필요한 시스템 계정, 디폴트 계정, 임시 계정 등 삭제, 불필요한 서비스 및 포트 차단, 백신 프로그램 설치 등
					정보시스템 인수 전 인수기준 적합성 여부를 확인하기 위하여 테스트를 수행하고 있는가?	o 정보시스템을 인수하기 전 사전 정의한 인수기준과의 적합성 여부를 테스트 등을 통해 확인한 후 인수여부를 결정하여야 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.	조직에서 운영하고 있는 보안시스템 운영절차를 수립하고 있는가?	o 보안시스템(정보보호시스템)은 정보통신망을 통하여 수집 · 저장 · 검색 및 송 · 수신되는 정보의 훼손 · 변조 · 유출 등을 방지하기 위한 장치로서 침입차단시스템(FW), 침입탐지시스템(IDS), 침입방지시스템(IPS), 웹방화벽, DB 접근통제시스템, 내부정보유출방지시스템(DLP), 가상사설망(VPN), 패치관리시스템(PMS) 등을 포함할 수 있다.

No	통제영역	No	통제항목	통제내용	점검항목	설명
						ㅇ 외부침입 탐지 및 차단, 내외부자에 의한 정보유출 방지 등을 위하여 도입·운영하고 있는 보안시스템에 대한 운영절차를 수립하여야 한다. - 보안시스템 유형별 책임자 및 관리자 지정 - 보안시스템 정책(룰셋 등) 적용(등록, 변경, 삭제 등) 절차 - 최신 정책 업데이트 : IDS, IPS 등의 보안시스템의 경우 새로운 공격기법을 탐지하기 위한 최신 패턴(시그너쳐) 및 엔진 지속적 업데이트, 시그너쳐 - 보안시스템 이벤트 모니터링 절차 : 정책에 위배되는 이상징후 탐지 및 확인 등 (인증기준 11.6.4 침해시도 모니터링 참고) - 보안시스템 접근통제 정책 - 보안시스템 운영현황 주기적 점검 등
					보안시스템 관리자 등 접근이 허용된 인원을 최소화하고 비인가자 접근을 엄격하게 통제하고 있는가?	ㅇ 사용자 인증, 관리자 단말 IP 또는 MAC 접근통제 등의 보호대책을 적용하여 보안시스템 관리자 등 접근이 허용된 인원 이외의 비인가자 접근을 엄격히 통제하여야 한다. 또한 주기적인 보안시스템 접속로그 분석을 통해 비인가자에 의한 접근시도를 확인하고 적절한 조치를 하여야 한다. (11.6.3 접근 및 사용 모니터링 참고)
					보안시스템별 정책(룰셋 등) 신규 등록, 변경, 삭제 등 절차를 수립하고 정책의 타당성 검토를 주기적으로 수행하고 있는가?	ㅇ 보안시스템별로 정책(룰셋 등) 신규 등록, 변경, 삭제 등을 위한 공식적인 절차(신청, 승인, 적용 등)를 수립·이행하여야 한다. 이는 정책(룰셋 등)의 생성 이력을 확인하기 위한 것이다.

No	통제영역	No	통제항목	통제내용	점검항목	설명
						ㅇ 또한 정책의 타당성 및 적정성을 주기적으로 검토하여 다음 사항에 해당하는 경우 정책을 삭제 또는 변경하여야 한다. - 내부 보안정책 위배 (예 : FW 룰셋 내부망 Inbound Any 정책 허용 등) - 미승인 정책 - 장기간 미사용 정책 - 중복 또는 사용기간 만료 정책 - 퇴직자 및 직무변경자 관련 정책 등
		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.	정보시스템의 성능 및 용량을 지속적으로 모니터링 하기 위한 절차를 수립·이행하고 있는가?	ㅇ 대고객 서비스 및 내부 업무 수행의 연속성을 보장할 수 있도록 주요 정보시스템의 성능 및 용량을 지속적으로 모니터링하여야 하며 다음사항을 포함한 절차를 수립하고 이행하여야 한다. - 성능 및 용량관리 대상 식별 기준 : 서비스 및 업무 수행에 영향을 줄 수 있는 주요 정보시스템 및 정보보호시스템을 식별하여 대상에 포함 - 정보시스템별 성능 및 용량 요구사항(임계치) 정의 : 정보시스템 가용성에 영향을 줄 수 있는 CPU, 메모리, 저장장치 등의 임계치를 정함 - 모니터링 방법 : 성능 및 용량 임계치 초과여부를 지속적으로 모니터링하고 대처할 수 있는 방법 수립 (예 : 알람 등) - 모니터링 결과 기록, 분석, 보고 - 성능 및 용량 관리 담당자 및 책임자 지정 등

No	통제영역	No	통제항목	통제내용	점검항목	설명
					정보시스템 성능 및 용량 요구사항(임계치)을 초과하는 경우 조치절차를 수립 · 이행하고 있는가?	ㅇ 정보시스템의 성능 및 용량 현황을 지속적으로 모니터링하여 요구사항(임계치)을 초과하는 경우 조치방안(예 : 정보시스템, 메모리, 저장장치 증설 등)을 수립하고 이행하여야 한다.
		11.2.4	장애관리	정보시스템 장애 발생 시 효과적으로 대응하기 위한 탐지, 기록, 분석, 복구, 보고 등의 절차를 수립하여야 한다.	정보시스템 장애를 즉시 인지하고 대응하기 위한 절차를 수립 · 이행하고 있는가?	ㅇ 정보시스템 장애유형 및 심각도를 정의하고 장애 발생 시 유형 및 심각도에 따라 다음과 같은 항목이 포함된 절차를 수립하고 이행하여야 한다. - 장애유형 및 심각도 정의 - 장애유형 및 심각도별 보고 절차 - 장애유형별 탐지 방법 수립 : NMS(Network Management System) 등 관리시스템 활용 - 장애 대응 및 복구에 관한 책임과 역할 정의 - 장애기록 및 분석 - 대고객 서비스인 경우 고객 안내 절차 - 비상연락체계(유지보수업체, 정보시스템 제조사) 등
					장애 발생 시 절차에 따라 조치하고 장애조치보고서 등을 통해 기록 · 관리하고 있는가?	ㅇ 다음항목이 포함된 '장애조치보고서'를 작성하여 장애발생에 관한 이력을 기록하고 관리하여야 한다. - 장애일시 - 장애심각도 (예 : 상, 중, 하) - 담당자, 책임자명 (유지보수업체 포함) - 장애내용 (장애로 인한 피해 또는 영향 포함) - 장애원인 - 조치내용 - 복구내용 - 재발방지대책 등

No	통제영역	No	통제항목	통제내용	점검항목	설명
					심각도가 높은 장애의 경우 원인분석을 통한 재발방지 대책을 수립 · 이행하고 있는가?	ㅇ 일상 업무가 중단되는 장애, 과다한 비용(피해)을 초래한 장애, 반복적으로 발생하는 장애 등과 같은 심각한 장애의 경우 원인을 규명하고 재발을 방지하기 위한 대책을 수립하고 이행하여야 한다.
		11.2.5	원격운영관리	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.	내부 네트워크를 통해서 원격으로 시스템을 운영하는 경우 특정 단말에 한해서만 접근을 허용하고 있는가?	ㅇ 내부 네트워크를 통해 정보시스템(서버, 네트워크 장비, 정보보호시스템 등)을 운영하거나 웹관리자 페이지에 접속하는 경우 관리자는 지정된 단말을 통해서만 접근 할 수 있도록 통제(IP 또는 MAC 인증 등)하여야 한다. 특히 패드, 스마트폰 등 스마트기기를 통한 정보시스템 원격운영은 원칙적으로 금지하여야 한다. 다만 부득이한 경우 스마트기기에 대한 보안대책을 마련하고 책임자의 승인 후 사용하여야 한다.
					인터넷과 같은 외부 네트워크를 통한 정보시스템 원격운영은 원칙적으로 금지하고 있으며 부득이하게 허용하는 경우 다음과 같은 대책을 마련하고 있는가? -정보보호 최고책임자 승인 -접속 단말 및 사용자 인증 -한시적 접근권한 부여 -VPN 등의 전송구간 암호화 -접속 단말 보안 -원격운영 현황 지속적인 모니터링 등	ㅇ 인터넷과 같은 외부네트워크를 통한 정보시스템 원격운영은 원칙적으로 금지하여야 하며 긴급 장애 대응, 유지보수 등과 같이 부득이한 경우 다음과 같은 보안대책을 마련하여야 하여야 한다. - 원격운영에 대한 정보보호 최고책임자 승인절차 - 접속 단말 및 사용자 인증절차 : ID/PW 이외의 강화된 인증방식(공인인증서, OTP 등) 적용 권고. 법적 요구사항 의무적 반영 필요. - 한시적 접근권한 부여 : VPN 계정, 시스템 접근권한 등 - VPN 등의 전송구간 암호화 - 접속 단말 보안 (예 : 백신 설치, 보안패치 적용 등)

No	통제영역	No	통제항목	통제내용	점검항목	설명
						- 원격운영 현황(원격운영 인가자, VPN 계정 발급 현황 등) 지속적인 모니터링 - 원격 접속 기록 로깅 및 주기적 분석 - 원격운영 관련 보안인식교육 등 ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적 · 관리적 보호조치(고시)' 제 4 조(접근통제) - 개인정보보호법 '개인정보의 안전성 확보기준(고시)' 제 6 조(접근통제 시스템 설치 및 운영)
		11.2.6	스마트워크 보안	재택근무, 원격협업 등과 같은 원격 업무 수행 시 이에 대한 관리적 · 기술적 보호대책을 수립하고 이행하여야 한다.	재택근무, 원격협업 등과 같은 원격업무 수행, 클라우드 환경을 이용한 스마트워크 환경에서 주요정보자산을 보호하기 위한 정책 및 절차가 수립 · 이행하고 있는가?	ㅇ "스마트워크"란 정보통신망을 활용하여 언제, 어디서나 편리하게 효율적으로 업무에 종사할 수 있도록 하는 업무형태를 말한다. (스마트워크 활성화를 위한 정보보호 권고 제 2 조) - 스마트워크 업무형태에는 재택근무, 스마워크센터, 원격협업(영상회의 등), 모바일오피스(BYOD 포함) 등이 있다. ※ "모바일오피스"란 스마트폰, 스마트패드, 노트북 등 모바일기기를 이용하여 시간적, 공간적 제약없이 업무를 수행하는 근무환경을 말함 ㅇ 조직이 구축하고 있는 스마트워크 업무형태에 따라 위협요인을 분석하여 중요정보 유출, 해킹 등의 침해사고 예방을 위한 절차 및 보호대책을 다음과 같이 수립 · 이행하여야 한다. - 스마트워크 업무형태 정의 : 재택근무, 스마트워크 센터, 원격협업, 모바일오피스 환경

No	통제영역	No	통제항목	통제내용	점검항목	설명
						- 스마트워크 업무형태에 따른 업무 허가 범위 설정 : 내부 시스템 및 서비스 원격접근 허용 범위 ※ 스마트워크 서비스 영역과 내부네트워크 영역을 분리하고 스마트워크용 단말에서 내부네트워크 영역 직접 연결 차단 필요(중계서버 구축 등) - 스마트워크 업무 승인절차 : 스마트워크를 위한 원격접근 권한 신청, 승인, 회수 등 - 원격접근에 필요한 기술적 보호대책 : 전송구간 암호화 (예 : VPN, SSL 인증서 등), 사용자 인증(예 : ID/PW 이외 OTP, 공인인증서 등 강화된 인증방식 도입 권고) 등 - 접속 단말(PC, 모바일기기 등) 보안 : 백신 설치, 보안패치 적용, 단말 인증, 분실/도난 시 대책(신고절차, 단말잠금, 중요정보 삭제 등), 중요정보 저장 금지(필요 시 암호화 조치) 등 - 스마트워크 업무 환경에서의 이용자 정보보호 지침 마련 등 ※ 참고 ※ - 스마트워크 활성화를 위한 정보보호 권고 해설서 (KISA)
		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.	조직 내 무선네트워크 환경을 구축(AP 설치)할 경우 허가(승인), 보안성 검토 등 절차를 마련하고 구축에 따른 다음 (주요) 보호대책을 적용하고 있는가? - 무선네트워크 장비(AP) 접속 단말 인증(MAC 인증 등) - 무선네트워크 장비(AP) 정보 송수신 시 암호화 기능 설정(WPA2 이상 권고)	ㅇ 조직 내부네트워크에 연결이 가능한 무선네트워크 환경 구축 시에는 내부 승인절차를 마련하여 비인가된 (사설) 무선네트워크 장비(Rogue AP : Access Point)를 운영하지 않도록 하여야 하며 사전 보안성 검토를 수행하여 다음과 같은 보호대책을 적용하여야 한다. - 무선네트워크 장비 접속 단말기 인증 및 보안

No	통제영역	No	통제항목	통제내용	점검항목	설명
					- 무선네트워크 장비(AP) SSID 숨김(브로드캐스팅 중지) 기능 설정	- 무선네트워크 장비 (예 : AP, Access Point) 보안 및 허용 장비 리스트 - 무선 네트워크를 통하여 접근 할 수 있는 정보시스템 범위 정의 - 무선네트워크 사용권한 신청/변경/삭제 절차 - 사용자 식별 및 인증 - 무선네트워크 서비스 거리 제한 (주파수 세기 조정) - 정보송수신 시 무선망 암호화 기준 (예 : WPA2) - 전산실 등 통제구역 내 무선네트워크 사용 제한 - SSID(ServiceSetIDentification)브로드캐스팅 중지 및 추측 어려운 SSID 사용 등 o 내부네트워크에 무선네트워크 환경을 구축하는 것은 업무의 편리성을 증대할 수는 있으나 충분한 보호대책 마련 없이 적용할 경우 내부 정보유출, 해킹 등의 심각한 상황을 초래할 수 있으므로 업무상 반드시 필요한 경우를 제외하고는 매우 신중하게 접근하여야 한다. ※ 참고 ※ - 알기쉬운 무선랜 보안 안내서 및 무선랜 보안안내서 (KISA)
					정상적인 절차에 따라 무선네트워크 사용을 허가한 경우 인가된 임직원만 무선네트워크를 사용할 수 있도록 사용 신청 및 해지 절차를 수립하고 있는가?	o 외부인이 무선네트워크 통해 내부네트워크(업무망)에 접속할 수 없도록 인가받은 임직원만 무선네트워크을 사용할 수 있도록 필요한 절차를 마련하여야 한다.

No	통제영역	No	통제항목	통제내용	점검항목	설명
					외부인에게 제공하는 무선네트워크를 내부네트워크(업무망)와 분리하고 있는가?	o 회의실, 교육장, 기자실, 민원실 등 외부인의 접근이 빈번한 장소인 경우 외부인에게 무선네트워크 사용을 허용할 수 있으나 내부네트워크(업무망)과 분리하여 무선네트워크를 통한 내부네트워크 침투 및 내부 정보유출을 방지하여야 한다.
		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.	웹서버 등 공개 서버를 운영하는 경우 이에 대한 보호대책을 마련하고 있는가?	o 공개서버(웹서버, 메일서버 등)를 운영하는 경우 다음과 같은 보호대책을 마련하여야 한다. - 공개서버 전용서버로 운영 - 웹서버를 통한 개인정보 송 · 수신 시 SSL(Secure Socket Layer)/TLS(Transport Layer Security) 인증서 설치 등 보안서버 구축 - 접근권한 설정 - 백신설치 및 OS 최신 패치 - 불필요한 서비스 제거 및 포트 차단 - 불필요한 소프트웨어 · 스크립트 · 실행파일 등 설치 금지 등 - 불필요한 페이지(테스트 페이지) 및 에러처리 미흡에 따른 시스템 정보 노출 방지 - 주기적인 취약점 점검 등
					공개서버는 내부 네트워크와 분리된 DMZ(Demilitarized Zone)영역에 설치하고 침입차단시스템 등 보안시스템을 통해 보호하고 있는가?	o 공개서버(웹서버, 메일서버 등)는 DMZ 영역에 설치하고 공개서버가 침해당하더라도 공개서버를 통한 내부 네트워크 침입이 불가능하도록 침입차단시스템 등을 통한 접근통제 정책을 적용하여야 한다. - DMZ의 공개서버가 내부 네트워크에 위치한 DB, WAS(Web Application Server) 등의 정보시스템과 접속이 필요한 경우 엄격하게 접근통제 정책을 적용하여야 한다.

No	통제영역	No	통제항목	통제내용	점검항목	설명
					공개서버의 취약점 점검을 주기적으로 수행하고 발견된 취약점을 조치하고 있는가?	ㅇ 웹서버의 경우 최소한 OWASP TOP 10 웹취약점은 기본적으로 점검하여 취약점이 발견된 경우 신속하게 조치를 하여야 한다. (인증기준 11.2.10 취약점 점검 참고) ※ 참고 ※ - 전자금융거래법 '전자금융감독규정(고시)' 제 17 조(홈페이지 등 공개용 웹서버 관리대책) - 웹서버구축 보안점검 안내서 (KISA)
					웹사이트에 중요정보를 게시하거나 웹서버에 중요정보를 저장하여야 할 경우 책임자 승인 등 게시절차를 수립·이행하고 중요정보 노출 여부를 주기적으로 확인하고 있는가?	ㅇ 웹서버의 보안설정 미흡, 기술적 취약점, 담당자의 실수 등으로 인해 조직의 중요정보(개인정보, 기밀정보 등)가 외부로 누출되는 경우(무단게시 등)가 빈번하게 발생하고 있다. 이를 예방하기 위하여 웹사이트에 정보를 공개하거나 업무상 웹서버에 중요정보를 저장하여야 할 경우 허가 및 게시절차를 수립하여 이행하여야 한다. 다만 원칙적으로 DMZ 구간내 웹서버에 조직의 중요정보(개인정보, 기밀정보 등)를 저장 관리하지 않는 것이 바람직하다. ㅇ 또한 게시절차 위반 등으로 조직의 중요정보가 웹사이트 및 웹서버를 통해 노출되고 있는지 여부를 주기적으로 확인하여 중요정보 노출을 인지한 경우 이를 즉시 차단하는 등의 조치를 취하여야 한다.

No	통제영역	No	통제항목	통제내용	점검항목	설명
		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.	백업 대상, 주기, 방법, 절차 등이 포함된 백업 및 복구절차를 수립 · 이행하고 있는가?	ㅇ IT 재해, 장애, 침해사고 등으로 인한 정보시스템 손상 시 적시에 복구가 가능하도록 백업 및 복구 절차를 수립하고 이행하여야 한다. - 백업대상 선정기준 수립 - 백업담당자 및 책임자 지정 - 백업대상별 백업 주기 및 보존기한 정의 - 백업방법 및 절차 : 백업시스템 활용, 매뉴얼 방식 등 - 백업매체 관리 (예 : 라벨링, 보관장소, 접근통제 등) - 백업 복구 절차 : 주요 정보시스템의 경우 IT 재해복구 측면(인증기준 13. IT 재해복구 참고)에서 백업정보의 완전성, 정확성 등을 점검하기 위하여 정기적인 복구 테스트 수행 필요 - 백업관리대장 관리 등 ㅇ 백업대상은 중요정보(개인정보, 기밀정보 등), 문서, 각종 로그(정보시스템 보안감사로그, 이벤트 로그, 정보보호시스템 이벤트 로그 등), 환경설정파일 등 대상 정보 및 정보시스템의 중요도를 고려하여 선정하여야 하며 정해진 절차에 따라 백업관리를 수행하여야 한다.
					중요정보가 저장된 백업매체의 경우 재난에 대처할 수 있도록 백업매체를 물리적으로 떨어진 장소에 소산하고 있는가?	ㅇ 중요정보가 저장된 백업매체는 운영중인 정보시스템 혹은 백업시스템이 위치한 장소로부터 물리적으로 거리가 있는 곳에 소산 보관하고 관리대장으로 소산 이력을 관리하여야 한다. - 소산일자 (반출, 반입 등) - 소산 백업매체 및 백업정보 내용

No	통제영역	No	통제항목	통제내용	점검항목	설명
						ㅇ 주기적으로 관리대장에 따라 소산 여부를 실사하여야 한다. ㅇ 소산장소에 대해 다음과 같은 보안대책을 마련하여야 한다. - 화재, 홍수와 같은 자연재해에 대한 대책 (예 : 내화금고, 방염처리 등) - 접근통제 등
		11.2.10	취약점 점검	정보시스템이 알려진 취약점에 노출되어 있는 지 여부를 확인하기 위하여 정기적으로 기술적 취약점 점검을 수행하고 발견된 취약점들은 조치하여야 한다.	정보시스템 취약점 점검 절차를 수립하여 정기적으로 점검을 수행하고 있는가?	ㅇ 정보시스템 취약점 점검 정책과 절차를 다음과 같은 내용을 포함하여 수립하여야 한다. - 취약점 점검 대상 (예 : 서버, 네트워크 장비 등) - 취약점 점검 주기 - 취약점 점검 담당자 및 책임자 지정 - 취약점 점검 절차 및 방법 등 ㅇ 정보시스템 중요도에 따라 주기적으로 다음과 같은 내용을 포함하여 취약점 점검을 실시하여야 한다. - 라우터, 스위치 등 네트워크 장비 구성, 설정 취약점 - 서버 OS, 보안 설정 취약점 - 방화벽 등 정보보호시스템 취약점 - 어플리케이션 취약점 - 웹서비스 취약점 - 스마트기기 및 모바일 서비스(모바일 앱 등) 취약점 ㅇ 취약점 점검 시 회사의 규모 및 보유하고 있는 정보의 중요도에 따라 모의침투테스트를 수행하는 것을 고려하여야 한다. ㅇ 취약점 점검 시 이력관리가 될 수 있도록 '점검일시', '점검대상', '점검방법', '점검내용 및 결과', '발견사항', ' 조

No	통제영역	No	통제항목	통제내용	점검항목	설명
						치사항' 등이 포함된 보고서를 작성하여야 한다.
					발견된 취약점에 대한 조치를 수행하고 그 결과를 책임자에게 보고하고 있는가?	ㅇ 취약점 점검 결과 발견된 취약점별로 대응방안 및 조치결과를 문서화하여야 하며 조치결과서를 작성하여 책임자에게 보고하여야 한다. - 불가피하게 조치를 할 수 없는 취약점의 경우 그 사유를 명확하게 확인하고 책임자에게 보고하여야 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.	전자(상)거래서비스를 제공하는 경우 전자(상)거래의 안전성과 신뢰성 확보를 위한 보호대책을 수립 · 이행하고 있는가?	ㅇ "전자거래"는 재화나 용역을 거래할 때 그 전부 또는 일부가 전자문서에 의하여 처리되는 거래를 말한다. (전자문서 및 전자거래 기본법 제 2 조) ㅇ "전자상거래"는 전자거래의 방법으로 상행위를 하는 것을 말한다. (전자상거래 등에서의 소비자보호에 관한 법률 제 2 조) ㅇ 전자(상)거래사업자는 전자(상)거래의 안정성과 신뢰성을 확보하기 위하여 전자(상)거래이용자의 개인정보, 영업비밀(거래처 식별정보, 재화 또는 용역 가격 등 공개 시 영업에 손실을 초래할 수 있는 거래 관련 정보), 결제정보 수집, 저장관리, 파기 등의 과정에서의 침해사고를 예방하기 위한 위한 보호대책(인증, 암호화, 접근통제 등)을 수립하여 이행하여야 한다. 보호대책 수립 시에는 다음과 같은 법률 등을 고려하여야 한다. ※ 참고 ※ - 전자문서 및 전자거래 기본법 - 전자상거래 등에서의 소비자 보호에 관한 법률

No	통제영역	No	통제항목	통제내용	점검항목	설명
						- 정보통신 이용촉진 및 정보보호 등에 관한 법률 - 개인정보보호법 - 전자금융거래법 등
					전자(상)거래 서비스 제공을 위하여 전자적 수단의 거래대금 지급방법을 이용하는 경우 전자(상)거래사업자와 전자결제업자간에 송 · 수신되는 결제관련 정보의 보호를 위한 대책을 수립 · 이행하고 있는가?	ㅇ "전자결제업자"는 전자결제수단의 발행자, 전자결제서비스 제공자, 해당 전자결제수단을 통한 전자결제서비스의 이행을 보조하거나 중개하는 자를 말하며(전자상거래 등에서의 소비자 보호에 관한 법률 시행령 제 8 조) 다음에 해당하는 자를 말한다. - 금융회사, 신용카드업자, 결제수단 발행자(전자적 매체 또는 정보처리시스템에 화폐가치 또는 그에 상응하는 가치를 기록저장하였다가 재화 등의 구매 시 지급하는 자), PG 사 ※ PG(Payment Gateway)사는 인터넷 상에서 금융 기관과 하는 거래를 대행해 주는 서비스. 신용 카드, 계좌 이체, 핸드폰 이용 결제, ARS 결제 등 다양한 소액 결제 서비스를 대신 제공해 주는 회사 ㅇ 전자(상)거래사업자와 전자결제업자간에 송 · 수신되는 결제관련 정보의 유출, 조작, 사기 등의 침해사고로 인한 거래당사자간 피해가 발생하지 않도록 적절한 보호대책을 수립하여 이행하여야 한다.

No	통제영역	No	통제항목	통제내용	점검항목	설명
		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.	업무상 조직 간에 중요정보(개인정보, 기밀정보 등)를 상호교환하는 경우 안전한 전송을 위한 협약체결 등 보호대책을 수립 · 이행하고 있는가?	ㅇ 조직 또는 계열사 간 다음과 같은 업무수행을 위하여 중요정보를 전자적으로 상호 교환하는 경우 안전한 전송을 위한 협약(보안약정서, 계약서, 부속합의서, SLA 등)을 체결하고 이에 따라 이행하여야 한다. - 관련 업무 정의 : DM 발송을 위한 개인정보 DM 업체 전달, 채권추심업체에 추심정보 전달, 개인정보 제 3 자 제공, 신용카드결제 정보 VAN(Value Added Network)社 전달 등 - 정보전송 범위 정의 : 법규 준수 또는 정보유출 위험을 예방하기 위해 업무상 필요한 최소한의 정보만을 송·수신 - 담당자 및 책임자 지정 - 정보 전송 기술 표준 정의 (예 : 정보 전송 시 협의 등) - 정보 전송, 저장, 파기 시 관리적·기술적 · 물리적 보호대책 등 ※ DM(Direct Mail advertising) : 우편물을 통한 홍보활동을 의미하며 편지, 엽서, 안내장, 리플렛, 카다롤그, 청구서 등의 인쇄물을 우편물 등의 형태로 직접 또는 우편 수단을 이용하여 전달하는 커뮤니케이션 수단
11.4	매체 보안	11.4.1	정보시스템 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.	정보시스템 폐기 또는 재사용 발생 시 중요정보를 담고 있는 저장매체 처리(폐기, 재사용) 절차를 수립 · 이행하고 있는가?	ㅇ 사용연한 경과, 고장 등의 사유로 정보시스템을 폐기 또는 재사용(양도, 내부판매, 재활용 등)할 경우 저장매체 처리에 관한 절차를 수립하여 저장매체에 저장된 중요정보 유출을 방지하여야 한다. - 저장매체 확인 및 승인 : 정보시스템 폐기 또는 재사용 시 저장매체 확인하고 폐기 또는 재사용 여부 결정

No	통제영역	No	통제항목	통제내용	점검항목	설명
						- 저장매체 폐기, 재사용에 따른 처리방법 정의 (예 : 폐기 → 물리적 폐기 · 디가우징 등, 재사용 → 완전 포맷) - 저장매체 처리 확인 및 기록
					저장매체 폐기 또는 재사용 시 정보가 복구되지 않는 방법으로 처리하고 있는가?	o 저장매체의 폐기 시 물리적, 전자적으로 완전파괴하고 재사용 시에는 완전포맷 방식으로 정보를 삭제하여야 한다. "완전포맷"은 저장매체 전체의 자료저장 위치에 새로운 자료를 중복하여 저장하는 것을 의미하여 완전포맷 횟수는 조직이 스스로 정하여 적용할 수 있다.
					자체적으로 저장매체를 폐기할 경우 관리대장을 통해 폐기이력을 남기고 폐기확인증적을 함께 보관하고 있는가?	o 조직이 자체적으로 저장매체 폐기할 경우 폐기이력에 대한 감사증적을 확보할 수 있도록 다음 항목이 포함된 관리대장을 작성하고 관련 책임자가 확인하여야 한다. - 폐기일자 - 폐기 담당자, 확인자명 - 폐기방법 - 폐기확인증적(사진 등) 등
					외부업체를 통해 저장매체를 폐기할 경우 폐기 절차를 계약서에 명시하고 완전한 폐기에 대한 확인을 하고 있는가?	o 아웃소싱등 외부업체를 통해 저장매체를 폐기할 경우, 내부 폐기정책과 절차 내용을 계약서에 명시하고 폐기 시 가능하면 외부업체와 함께 현장에서 함께 폐기현장을 실사하고 폐기증적을 사진, 동영상 등으로 받아 확인하여야 한다.
					정보시스템, PC 등 유지보수, 수리 과정에서 저장매체 교체, 복구 등 발생 시 저장매체 내 정보를 보호하기 위한 대책을 마련하고 있는가?	o 정보시스템, PC 등 유지보수, 수리과정에서 저장매체 교체, 복구 등의 상황 발생 시 저장매체 내 중요정보를 보호하기 위하여 유지보수 신청 전 데이터 이관 및 파기, 암호화, 계약 시 비밀유지서약 등과 같은 보호대책을 마련하여야 한다.

No	통제영역	No	통제항목	통제내용	점검항목	설명
		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.	외장하드, USB, CD 등 휴대용 저장매체 취급(사용), 보관, 폐기, 재사용에 대한 정책 및 절차를 수립 · 이행하고 있는가?	o "휴대용 저장매체"라 함은 디스켓, 외장형 하드디스크, USB 메모리, CD, DVD 등 자료를 저장할 수 있는 일체의 것으로 PC 등의 정보통신시스템과 분리할 수 있는 기억장치를 말한다. o 업무용으로 개인 휴대용 저장매체를 사용하는 것은 원칙적으로 금지하여야 하며 업무 목적상 외장하드, USB 메모리, CD 등 휴대용 저장매체를 사용하여야 하는 경우 허가된 저장매체만 사용할 수 있도록 다음과 같은 정책 및 절차를 수립하고 이행하여야 한다. - 휴대용 저장매체 취급(사용)범위 : 통제구역, 제한구역 등 보호구역별 저장매체 사용 정책 및 절차 수립 - 휴대용 저장매체 사용허가 및 등록절차 - 휴대용 저장매체 반출, 반입 절차 - 휴대용 저장매체 폐기, 재사용에 대한 절차 - 휴대용 저장매체 보호대책 등
					주요 정보시스템이 위치한 통제구역, 중요 제한구역 등에서 휴대용 저장매체 사용을 제한하고 있는가?	o 주요 정보시스템이 위치한 통제구역(전산실 등), 조직 내 중요정보에 접근이 가능한 제한구역(운영실, 관제실 등)에서는 휴대용 저장매체의 사용 및 반입을 엄격하게 제한하여야 한다. 불가피하게 사용할 경우 책임자의 허가절차를 거친 후 적법한 절차에 따른 사용여부 확인을 위하여 지속적인 점검을 수행하여야 한다.

No	통제영역	No	통제항목	통제내용	점검항목	설명
					휴대용 저장매체를 통한 악성코드 감염 및 중요정보 유출 방지를 위한 대책을 마련하고 있는가?	ㅇ 휴대용 저장매체를 통해 바이러스, 악성코드가 유포되지 않도록 휴대용 저장매체가 연결되는 단말기에 다음과 같은 대책을 적용하고 주기적으로 점검하여야 한다. - 휴대용 저장매체 자동실행 기능 해지 - 휴대용 저장매체 이용 시 바이러스 및 악성코드 사전(자동) 검사 - 휴대용 저장매체 내 숨김파일 및 폴더 등이 표시되도록 PC 등 단말기 옵션 변경 등 ㅇ 조직의 중요정보(개인정보, 기밀정보 등)의 경우 휴대용 저장매체 저장을 제한하고 업무상 저장이 필요한 경우에는 암호화 등의 보호대책을 마련하여 매체 분실, 도난 등에 따른 중요정보 유출을 방지하여야 한다.
					휴대용 저장매체 보유현황 및 관리실태를 주기적으로 점검하고 있는가?	ㅇ 업무목적으로 사용이 허용된 휴대용 저장매체의 경우 식별번호, 유형, 사용목적, 관리자, 책임자 등이 명시된 보유목록을 작성하고 주기적인 자산실사를 통해 목록을 현행화하여야 한다.
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.	바이러스, 웜, 트로이목마 등의 악성코드로부터 정보시스템을 보호하기 위하여 보호대책을 수립 · 이행하고 있는가?	ㅇ 바이러스, 웜, 트로이목마 등의 악성코드로부터 내부 정보시스템을 보호하기 위하여 다음 항목을 포함한 지침 및 절차를 수립하여야 한다. - 사용자 PC 사용지침 (불분명한 이메일 및 파일 열람 금지, 허가받지 않은 프로그램 다운로드 및 설치 금지 등) - 백신프로그램 설치 범위 및 절차 - 백신프로그램을 통한 주기적인 악성코드 감염여부 모니터링 정책 - 사용자 교육 및 정보제공

No	통제영역	No	통제항목	통제내용	점검항목	설명
						ㅇ 백신프로그램 설치 범위는 다음사항을 고려하여 정하여야 한다. - 내부 네트워크에서 사용되는 업무용 단말기 (PC, 노트북 등) - 정보자산 중요도 평가 과정에서 등급이 높은 정보자산(인증기준 4.2.1 보안등급과 취급 참고) (예 : DMZ 구간의 공개서버, 공개서버와 연계되어 있는 서버(WAS, DB 등), 중요정보가 저장되어 있는 DB, 기타 중요하다고 판단되는 정보자산 (DNS, DHCP 등)) - 정보통신망 이용촉진 및 정보보호 등에 관한법률 시행령에 따른 개인정보처리시스템, 개인정보처리에 이용되는 정보기기 (PC, 노트북 등 단말기) - 윈도우, 리눅스, 유닉스 등 다양한 운영체제 ㅇ 기존 시스템 환경과 충돌이 발생하여 백신프로그램을 설치할 수 없는 경우에는 책임자의 승인을 받고 보완대책을 마련하여 관리하여야 한다. ※ 참고 ※ - 백신프로그램 이용 안내서 (KISA)
					백신프로그램 등을 통한 최신 악성코드 예방, 탐지 활동을 지속적으로 수행하고 있는가?	ㅇ 악성코드가 정보시스템과 PC 등의 단말기에 유입되어 확산되는 것을 방지하기 위하여 다음 사항을 포함한 예방, 탐지 활동을 수행하여야 한다. - 전자우편 등 첨부파일에 대한 악성코드 감염 여부 검사 - 실시간 악성코드 감시 및 치료 - 주기적인 악성코드 점검 : 자동 바이러스 점검 일정 설정 - 백신엔진 최신버전 유지 : 주기적 업데이트 등

No	통제영역	No	통제항목	통제내용	점검항목	설명
					악성코드 감염 발견 시 악성코드 확산 및 피해 최소화 등의 대응절차를 수립·이행하고 있는가?	o 악성코드 감염 발견 시 추가적인 확산과 피해 최소화를 위하여 다음과 같은 항목이 포함된 대책을 마련하여야 한다. - 악성코드 감염 발견 시 대처 절차 (예 : 네트워크케이블 분리 등) - 비상연락망 (예: 백신업체 담당자, 관련 기관 연락처 등) - 대응보고서양식 (발견일시, 대응절차 및 방법, 대응자, 방지대책 포함) 등
		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.	서버, 네트워크 장비, 보안시스템, PC 등 자산 중요도 또는 특성에 따라 OS, 소프트웨어 패치관리 정책 및 절차를 수립·이행하고 있는가?	o 운영체제(서버, 네트워크, PC 등) 및 (상용) 소프트웨어(오피스 프로그램, 백신, DBMS 등) 의 경우 지속적으로 취약점이 발견되며 이를 해결하기 위한 패치(patch)파일도 지속적으로 공개된다. 따라서 서버, 네트워크 장비, PC 등에 설치되어 있는 운영체제, 소프트웨어 패치적용을 위한 정책 및 절차를 수립하여 이행하여야 한다. - 서버, 네트워크 장비, 보안시스템, PC 등 대상별 패치정책 및 절차 : 패치정보 입수 및 적용방법 등 - 패치 담당자 및 책임자 지정 - 패치 관련 업체(제조사) 연락처 등
					주요 서버, 네트워크 장비 등의 경우 설치된 OS, 소프트웨어 패치적용 현황을 관리하고 있는가?	o 주요 서버, 네트워크 장비, 보안시스템 등에 설치된 운영체제, 소프트웨어 버전 정보, 패치일 등을 확인할 수 있도록 목록 등으로 관리하고 최신 보안패치 여부를 주기적으로 확인하여야 한다.

No	통제영역	No	통제항목	통제내용	점검항목	설명
					주요 서버, 네트워크 장비, 정보보호시스템 등의 경우 공개 인터넷 접속을 통한 패치를 제한하고 있는가?	o 일반적으로 통제구역(전산실 등)에 위치하고 있는 서버, 네트워크 장비, 정보보호시스템에 관련 패치를 적용하여야 할 경우 공개 인터넷 접속을 통한 패치적용은 원칙적으로 금지하여야 한다. 다만 불가피한 경우 사전 위험분석을 통해 보호대책을 마련한 후 책임자 승인 후 적용하여야 한다.
					패치관리시스템(PMS)를 활용하는 경우 접근통제 등 충분한 보호대책을 마련하고 있는가?	o 패치관리시스템(PMS)의 경우 내부망 서버 또는 PC에 악성코드 유포에 활용될 수 있으므로 패치관리시스템(PMS) 서버, 관리 콘솔에 대한 접근통제(관리자 이외의 비인가자 접근 차단, 패스워드 주기적 변경, 임시계정 삭제 등) 등 충분한 보호대책을 마련하여야 한다. - 패치관리시스템은 업데이트를 내려받는 경우 해당 업데이트 파일이 변조되었는지 확인하기 위한 무결성 점검 기능이 있는지 확인하고 도입하는 것이 좋다.
					운영시스템 경우 패치 적용하기 전 시스템 가용성에 미치는 영향을 분석하여 패치를 적용하고 있는가?	o 운영시스템에 패치를 적용하는 경우 시스템 가용성에 영향을 미칠 수 있으므로 패치 적용은 운영시스템의 중요도와 특성을 고려하여 위험도 분석 등 정해진 절차에 따라 충분하게 영향을 분석한 후 책임자 승인 후 적용하여야 한다. 다만 운영환경에 따라 즉시 패치 적용이 어려운 경우 그 사유와 추가 보완대책을 마련하여 책임자에게 보고하고 그 현황을 관리하여야 한다.

No	통제영역	No	통제항목	통제내용	점검항목	설명
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.	각 정보시스템 시각을 표준시각으로 동기화하고 있는가?	ㅇ 로그기록 시간의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위하여 타임서버 등을 이용하여 주기적으로 시각의 설정 및 동기화 여부를 점검하여야 한다. 예를 들어 NTP(Network Time Protocol)등의 방법을 활용하면 시스템간 시간을 동기화할 수 있다.
		11.6.2	로그기록 및 보존	정보시스템, 응용프로그램, 보안시스템, 네트워크 장비 등 기록해야 할 로그유형을 정의하여 일정기간 보존하고 주기적으로 검토하여야 한다. 보존기간 및 검토주기는 법적요구사항을 고려하여야 한다.	주요 정보시스템에 대한 로그관리 절차를 수립하고 이에 따라 로깅하고 있는가? - 로그기록 및 보존이 필요한 주요 정보시스템 지정 - 각 시스템 및 장비별 로그유형 및 보존기간 정의 - 로그기록 보존(백업) 방법	ㅇ 서비스 및 업무 중요도를 고려하여 로그 기록 및 보존이 필요한 주요 정보시스템(서버, 응용프로그램, 정보보호시스템, 네트워크 장비, DB 등)을 지정하고 각 시스템 및 장비별로 기록하여야 할 로그유형 및 보존기간을 정하여야 한다. 특히 로그유형 및 보존기간(최소 6개월 이상 권고)은 법적요건을 고려하여 정하여야 한다. - 로그 기록 및 보존이 필요한 시스템 및 장비는 정보자산의 중요도 평가 과정(인증기준 4.2.1 보안등급과 취급 참고)을 통해 정할 수 있으며 서비스 및 업무 지원을 위한 핵심 정보보호 시스템은 대상에 포함하여야 한다. 특히 법률(정보통신 이용촉진 및 정보보호 등에 관한 법률, 개인정보보호법 등)에서 정하고 있는 개인정보처리시스템은 대상에 포함하여야 한다. ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적·관리적 보호조치(고시)' 제4조(접근권한의 관리) 및 제8조 (접속기록의 보관 및 위·변조 방지) ㅇ 각 정보시스템별 로그유형은 다음과 같이 정할 수 있다. - 보안관련 감사로그 : 사용자 접속기록 (사용자식별정보 : ID, 접속일시, 접속

No	통제영역	No	통제항목	통제내용	점검항목	설명
						지 : 단말기 IP, 수행업무 : 정보생성, 수정, 삭제, 검색 출력 등), 인증 성공/실패 로그, 파일 접근, 계정 및 권한 등록/변경/삭제 등 - 시스템 이벤트 로그 : 운영체제 구성요소에 의해 발생되는 로그(시스템 시작, 종료, 상태, 에러코드 등) - 보안시스템 정책(룰셋 등)등록/변경/삭제 및 이벤트 로그 - 기타 정보보호 관련 로그
					로그기록은 별도 저장장치를 통해 백업하고 로그기록에 대한 접근권한 부여를 최소화 하고 있는가?	ㅇ 로그기록은 스토리지 등 별도 저장장치를 사용하여 백업하고 로그기록에 대한 접근권한부여는 최소화하여 비인가자에 의한 로그기록 위변조 및 삭제 등이 발생하지 않도록 하여야 한다. - 위변조 방지대책은 개인정보, 기밀정보 취급 이력 로그에 한해서 적용할 수 있다. ※ 참고 ※ - 정보통신 이용촉진 및 정보보호 등에 관한 법률 시행령 제15조 (개인정보의 보호조치)
		11.6.3	접근 및 사용 모니터링	중요정보, 정보시스템, 응용프로그램, 네트워크 장비에 대한 사용자 접근이 업무상 허용된 범위에 있는 지 주기적으로 확인하여야 한다.	중요정보 및 주요 정보시스템에 대한 사용자 접속 기록을 주기적으로 검토(모니터링)하고 있는가?	ㅇ 중요정보(개인정보, 기밀정보 등) 및 정보시스템(서버, 응용프로그램, 정보보호시스템, 네트워크 장비 등) 사용자 접속기록을 주기적으로 검토하여 중요정보 및 정보시스템 오남용 등의 이상징후를 확인하여야 한다. 다음 사항이 포함된 검토(모니터링)절차를 수립하고 절차에 따라 이행하여야 한다. - 검토대상 : 사용자 접속기록을 검토할 중요정보 및 주요 정보시스템 선정 - 검토주기 : 월 1회 이상 권고

No	통제영역	No	통제항목	통제내용	점검항목	설명
						- 검토기준 및 방법 : 업무목적 이외의 중요정보 과다처리(조회, 변경, 삭제 등), 업무시간 외 접속, 비정상적인 접속(미승인 계정 접속 등)등의 기준 및 확인 방법 수립 - 검토 담당자 및 책임자 지정 - 이상징후 대응절차 등 ※ 참고 ※ - 정보통신 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적 · 관리적 보호조치(고시)' 제 5 조 (접속기록의 위 · 변조 방지)
					사용자 접속기록 검토결과를 책임자에게 보고하고 이상징후 발견 시 절차에 따라 대응하고 있는가?	ㅇ 사용자 접속기록을 검토기준에 따라 검토 한 후 이상징후 여부 등 그 결과를 관련 책임자에게 보고하여야 한다. 또한 이상징후 발견 시 정보유출, 해킹 등 발생 여부를 확인하기 위한 절차를 수립하고 절차에 따라 대응하여야 한다.
		11.6.4	침해시도 모니터링	외부로부터의 침해시도를 모니터링 하기 위한 체계 및 절차를 수립하여야 한다.	외부로부터의 침해시도가 의심되는 이상징후를 지체 없이 인지할 수 있도록 모니터링 체계 및 절차를 수립하고 있는가?	ㅇ 외부로부터의 침해시도가 의심되는 이상징후를 지체없이 인지할 수 있도록 다음과 같은 항목이 포함된 모니터링 절차를 수립하여 이행하여야 한다. - 모니터링 대상범위 : 침해시도 탐지 및 차단하기 위한 각종 정보보호시스템 이벤트 로그 등 - 모니터링 방법 : 외부 전문업체를 통한 모니터링, 자체 모니터링 체계 구축 등 - 담당자 및 책임자 지정 - 모니터링 결과 보고체계 - 침해시도 발견 시 대응절차 등 ㅇ 조직의 규모 및 정보시스템 중요도가 높은 경우 24 시간 침해시도 실시간 모니터링 수행을 고려하여야 한다.

< 정보보호대책_12. 침해사고 관리 >

No	통제영역	No	통제항목	통제내용	점검항목	설명
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.	침해사고대응절차가 수립되어 있고 대응절차에는 다음과 같은 사항을 포함하고 있는가? - 침해사고의 정의 및 범위(중요도 및 유형 포함) - 침해사고 선포절차 및 방법 - 비상연락체계 - 침해사고 발생시 기록, 보고절차 - 침해사고 신고 및 통지 절차(관계기관, 이용자 등) - 침해사고 보고서 작성 - 침해사고 대응 및 복구 절차 - 침해사고 복구조직의 구성 및 책임, 역할 - 침해사고 복구장비 및 자원조달 - 침해사고 대응 및 복구 훈련, 훈련 시나리오 - 외부 전문가나 전문기관의 활용방안 - 기타 보안사고 예방 및 복구를 위하여 필요한 사항	ㅇ 침해사고의 정의 및 범위, 긴급연락체계 구축, 침해사고 발생 시 보고 및 대응 절차, 사고 복구조직의 구성 등을 포함한 침해사고 대응절차를 수립하여야 한다.
		12.1.2	침해사고 대응체계 구축	침해사고 대응이 신속하게 이루어질 수 있도록 중앙집중적인 대응체계를 구축하고 외부기관 및 전문가들과의 협조체계를 수립하여야 한다.	침해사고를 모니터링 하고 신속하게 대응할 수 있도록 모니터링 및 대응 방법, 절차, 대응조직 및 인력, 보고 및 승인 방법 등을 포함한 중앙집중적인 대응체계를 수립하고 있는가?	ㅇ 침해사고를 효과적으로 모니터링하고 신속하게 대응하기 위해서는 중앙집중적인 대응체계를 수립하여야 한다.
					침해사고가 유형 및 중요도에 따라 분류되어 있고 이에 따른 보고체계를 정의하고 있는가?	ㅇ 침해사고를 유형 및 중요도에 따라 분류하고 분류에 따른 보고체계를 정의하여야 한다.
					외부관제시스템 등 외부 기관을 통해 침해사고 대응체계를 구축 · 운영하는 경우 침해사고 대응절차의 세부사항을 계약서에 반영하고 있는가?	ㅇ 침해사고 대응체계를 외부 기관을 통해 구축한 경우 수립된 침해사고 대응절차 및 체계를 계약서에 반영하여야 한다.
					침해사고의 모니터링, 대응 및 처리와 관련된 외부전문가, 전문업체, 전문기관(KISA) 등과의 협조체계를 수립하고 있는가?	ㅇ 침해사고의 모니터링, 대응 및 처리와 관련되어 외부 전문가, 전문업체, 전문기관(KISA) 등과의 연락 및 협조체계를 수립하여야 한다.

12.2	대응 및 복구	12.2.1	침해사고 훈련	침해사고 대응 절차를 임직원들이 숙지할 수 있도록 시나리오에 따른 모의 훈련을 실시하여야 한다.	침해사고 대응절차에 관한 모의훈련계획을 수립하고 이에 따라 주기적으로 훈련을 실시하고 있는가?	ㅇ 침해사고 대응절차 및 방법에 대한 적정성과 효과성을 평가하기 위하여 주기적으로 침해사고 대응 훈련을 수행하여야 한다.
		12.2.2	침해사고 보고	침해사고 징후 또는 사고 발생을 인지한 때에는 침해사고 유형별 보고절차에 따라 신속히 보고하고 법적 통지 및 신고 의무를 준수하여야 한다.	침해사고의 징후 또는 침해사고 발생을 인지한 경우 정의된 침해사고 보고절차에 따라 신속하게 보고가 이루어지고 있는가?	ㅇ 하드웨어 및 소프트웨어상의 침해사고 징후 또는 침해사고 발생을 인지한 경우 신속하게 보고하여야 한다.
					침해사고보고서에는 사고 날짜, 사고 내용 등 필요 내용을 모두 포함하고 있는가?	ㅇ 침해사고 발생시 침해사고보고서가 작성되어야 하고, 보고서에는 다음과 같은 사항이 포함하여야 한다. - 침해사고 발생일시 - 보고자와 보고일시 - 사고내용 (발견사항, 피해내용 등) - 사고대응 경과 내용 - 사고대응까지의 소요시간 등
					침해사고가 조직에 미치는 영향이 심각할 경우 최고경영층까지 신속하게 보고하고 있는가?	ㅇ 조직의 유·무형 자산에 심각한 영향을 끼칠 수 있는 침해사고가 발견되거나 발생한 경우 최고경영층까지 보고하여야 한다.
					침해사고 발생 시 관련 법률 및 규정에 따라 신고, 통지하는 절차를 따르고 있는가?	ㅇ 침해사고 발생 시 법률이나 규정 등에 따라 관계기관에 신고하여야 하며 개인정보와 관련한 침해사고는 이용자(정보주체)에게 신속하게 통지하여야 한다. ※ 참고 ※ - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 48 조의 3(침해사고의 신고 등) - 개인정보보호법 제 34 조(개인정보 유출 통지 등)

		12.2.3	침해사고 처리 및 복구	침해사고 대응절차에 따라 처리와 복구를 신속하게 수행하여야 한다.	침해사고가 발생한 경우 절차에 따라 처리 및 복구를 수행하고 그 기록을 남기고 있는가? - 처리 및 복구 일시 - 담당자 - 처리 및 복구 방법 - 처리 및 복구 수행 경과 내용 (예 : 시작부터 종료까지 시간순으로 작성)	ㅇ 침해사고 처리와 복구는 수립된 절차에 따라 수행하여야 하며 침해사고 이력관리를 위하여 사고발생부터 처리 및 복구 종료까지의 진행경과를 보고서로 작성하여야 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.	침해사고가 종결된 후 사고의 원인을 분석하고 그 결과를 보고하고 있는가?	ㅇ 침해사고가 처리되고 종결된 후 이에 대한 분석이 수행되어야 하며 그 결과가 보고되어야 한다.
					침해사고 정보와 발견된 취약점을 관련조직 및 인력과 공유하고 있는가?	ㅇ 침해사고 정보와 발견된 취약점을 관련 조직 및 인력과 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.	침해사고 분석을 통해 얻어진 정보를 활용하여 유사 사고가 재발하지 않도록 대책을 수립하고 필요한 경우 침해사고 대응절차 등을 변경하고 있는가?	ㅇ 침해사고 분석을 통해 얻어진 정보를 활용하여 유사사고가 반복되지 않도록 하는 재발방지 대책을 수립하여야 한다. ㅇ 분석된 결과에 따라 필요한 경우 침해사고 대응절차, 정보보호정책 및 절차 등의 사고대응체계에 대한 변경을 수행하여야 한다.

No	통제영역	No	통제항목	통제내용	점검항목	설명
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.	다음과 같은 내용을 포함하는 IT 재해복구 체계를 구축하고 있는가? - 재해 시 복구조직 및 역할 정의 - 비상연락체계 - 복구순서 정의 - 복구전략 및 대책 - 복구 절차 및 방법 등	ㅇ IT 재해 발생 시 신속한 복구가 가능하도록 다음과 같은 내용을 포함하여 IT 재해 복구 체계를 구축하여야 한다. - 재해 시 복구조직 및 역할 정의 : IT 재해 발생 시 복구를 위한 관련부서 및 담당자 역할과 책임 부여 - 비상연락체계 : 조직 내 관련 부서 담당자, 유지보수 업체 등 복구 조직상 연락체계 구축 - 복구전략 및 대책 수립방법론 : 업무영향분석, 복구목표시간 및 복구시점 정의, 핵심 IT 서비스 및 시스템 식별 등 - 복구순서정의 : 복구목표시간별로 정보시스템의 복구순서 정의 - 복구절차 : 재해발생, 복구완료, 사후관리 단계 포함
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.	조직의 핵심 서비스(업무) 연속성을 위협할 수 있는 IT 재해 위험요인을 식별하고 위험요인에 따른 피해규모 및 업무에 미치는 영향을 고려하여 핵심 IT 서비스(업무) 및 시스템을 식별하고 있는가?	ㅇ IT 재해복구는 각종 재해 및 위험요인으로 인한 IT 서비스 중단 시 정상 기능으로 복구하는 모든 절차와 행위를 말한다. IT 서비스 중단을 초래할 수 있는 IT 재해 위험요인은 다음과 같다. - 자연재해 : 화재, 홍수, 지진, 태풍 등 - 외부요인 : 해킹, 통신장애, 전력 수급 중단 등 - 내부요인 : 시스템 결함, 기계적 오류, 사용자 실수, 의도적·악의적 운영, 핵심 운영자 근무 이탈(사망, 병가, 휴가, 이직 등), 환경설정 오류 등 ㅇ IT 재해 발생으로 조직의 핵심 서비스(업무) 중단 시 피해규모 및 영향을 분석하여 핵심 IT 서비스 및 시스템을 식별하여야 한다. 피해규모 및 업무영향분석 시 다음 사항을 고려할 수 있다. - 매출감소, 계약위약금 지급 등 재무적 측면 - 손해배상 소송 등 법적 측면 - 대외 이미지 하락 등

					핵심 IT 서비스 및 시스템의 복구목표시간, 복구시점을 정의하고 있는가?	ㅇ IT 서비스 및 시스템 중단시점부터 복구되어 정상가동 될 때까지의 복구목표시간(RTO : Recovery Time Objective)과 데이터가 복구되어야 하는 복구시점(RPO : Recovery Point Objective)을 정의하여야 한다.
					정의한 복구목표시간 및 복구시점을 달성할 수 있는 적절한 복구전략 및 대책을 수립하고 있는가?	ㅇ IT 재해발생 시 사전 정의한 서비스 및 시스템 복구목표시간 및 복구시점을 달성할 수 있도록 비용효과적인 복구전략 및 대책을 수립하여야 하며 실제로 IT 재해발생 시에는 사전 마련한 복구전략 및 대책에 따라 신속하게 복구를 하여야 한다.
		13.2.2	시험 및 유지관리	IT 서비스 복구전략 및 대책에 따라 효과적인 복구가 가능한지 시험을 실시하고 시험계획에는 시나리오, 일정, 방법, 절차 등을 포함하여야 한다. 또한 시험결과, IT 환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완하여야 한다.	수립된 IT 재해 복구 대책의 실효성을 판단하기 위하여 다음과 같은 내용이 포함된 시험계획을 수립 · 수행하고 있는가? - 일정 (일시 및 장소) - 참여인원 - 범위 - 방법 (예 : 시나리오 기반) - 절차 등	ㅇ IT 서비스 및 시스템 복구전략 및 대책이 복구 목표를 달성하기에 효과적인 지 여부를 확인하기 위하여 시험 시나리오, 일정, 방법, 절차 등을 포함하는 시험계획을 수립하여야 한다. 또한 시험계획에 따라 정기적인 시험을 실시하여 복구전략 및 대책이 효과를 발휘하는지, 비상시 복구조직 구성원이 복구절차에 따라 신속하게 대응하는지 등을 점검하여야 한다.
					시험결과, IT 환경변화, 법률 등에 따른 변화를 반영할 수 있도록 복구전략 및 대책을 정기적으로 검토·보완하고 있는가?	ㅇ 시험 결과, IT 환경 변화, 법률 등에 따른 변화 등 조직 내외의 변화를 반영하지 못한 복구전략 및 대책은 실효성이 떨어질 수 있으므로, 공식적인 변화관리 절차를 마련하고, 이에 따라 현실을 반영, 보완하도록 하여야 한다.