



제 428회 국회 (임시회)
제2차 과학기술정보방송통신위원회

정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안

검 토 보 고

〈고위험 정보통신서비스 제공자 정보보호 관리체계 인증기준 강화 등〉
■ 조인철의원 대표발의(의안번호 제2211594호)

2025. 8.

과학기술정보방송통신위원회

수석전문위원 이복우

목 차

I . 제안경 위	1
II . 제안이유 및 주요내용	1
III . 검토의견	2
1. 주요 정보통신서비스 제공자 등의 정보기술 및 정보보호 분야별 전문인력·예 산 확보 노력 의무 규정(안 제45조 제5항 신설)	2
2. 정보보호 관리체계(ISMS) 인증기준 차등화 등(안 제47조 제8항 등)	6

I. 제안경위

가. 발 의 자 : 조인철의원 등 11인

나. 발 의 일 : 2025. 7. 21.

다. 회 부 일 : 2025. 7. 22.

II. 제안이유 및 주요내용

현행법은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 그 적합성을 인증하는 제도를 두고 있음.

최근 SK텔레콤의 침해사고의 경우 SK텔레콤이 정보보호 관리체계 인증을 받았음에도 불구하고 사고 예방이나 사후조치에 미흡한 모습을 보여 현행 정보보호 관리체계 인증제도의 실효성 확보가 시급한 상황임. 또한, 2024년 기준 SK텔레콤의 정보기술 투자금액 대비 정보보호 투자금액 비율은 4.1%로 KT 6.4%, LGU+6.6%에 비해 낮은 수준으로, 정보보호 투자 확대를 유도하기 위한 제도적 개선이 필요한 실정임.

이에 주요 정보통신서비스 제공자 등이 정보기술 및 정보보호 분야별 전문성을 갖춘 인력과 충분한 예산을 확보하도록 노력할 의무를 규정하고, 고위험 정보통신서비스 제공자에 대하여 강화된 인증기준을 적용할 수 있도록 하였음. 또한, 정보보호 관리체계 인증을 받지 아니한 자에게 과징금을 부과할 수 있는 근거를 마련함으로써 정보보호 관리체계 인증제도를 개선하고 안전한 정보통신망 환경 조성에 기여하고자 함(안 제45조제5항, 제47조의7제2항 및 제47조의8 신설 등).

Ⅲ. 검토의견

1. 주요 정보통신서비스 제공자 등의 정보기술 및 정보보호 분야별 전문인력·예산 확보 노력 의무 규정(안 제45조 제5항 신설)

가. 개정안 요지

- 「전기통신사업법」에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자(이하 “주요정보통신서비스 제공자”), 집적정보통신시설 사업자, 그 밖에 대통령령으로 정하는 정보통신서비스 제공자는 정보기술 및 정보보호 분야별 전문인력과 충분한 예산을 확보하도록 노력하여야 함(안 제45조 제5항 신설).

나. 개정안 조문대비표

현행	개정안
제45조(정보통신망의 안정성 확보 등) ① ~ ④ (생략) <u><신설></u>	제45조(정보통신망의 안정성 확보 등) ① ~ ④ (현행과 같음) ⑤ 「전기통신사업법」 제6조 제1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 <u>정보통신망서비스를 제공하는 자(이하 “주요정보통신서비스 제공자”라 한다), 집적정보통신시설 사업자, 그 밖에 대통령령으로 정하는 정보통신서비스 제공자는 정보기술 및 정</u>

현행	개정안
	<u>보보호 분야별 전문성을 갖춘 인력과 충분한 예산을 확보하도록 노력하여야 한다.</u>

다. 검토사항

- 최근 SK텔레콤 해킹 사고와 관련하여, SK텔레콤의 정보보호 투자 비중이 다른 이동통신사에 비해 낮다는 점이 침해사고의 원인 중 하나로 지적되고 있음.
- 정보보호 공시에 따르면 2024년 SK텔레콤의 정보기술부문 투자금액 대비 정보보호 투자금액 비율은 4.2%로, 케이티(6.4%)·LG유플러스(6.6%) 및 전체 정보보호 공시 기업 평균(6.2%)에 비해 낮은 수준으로 나타남¹⁾.
- 「정보보호산업의 진흥에 관한 법률」에서 사업 분야, 매출액 및 서비스 이용자 수 등을 고려하여 일정 기준에 해당하는 자에 대하여 정보보호 투자 및 인력 현황 등 정보보호 현황을 공시하도록 하고 있으나²⁾, 정보보호 투자 금액 또는 비율을 일정 수준 이상으로 의무화하는 규정은 없음.

1) 한국인터넷진흥원 정보보호 공시 종합 포털(<https://isds.kisa.or.kr/>) - 정보보호공시현황
한국인터넷진흥원, 「2024 정보보호 공시 현황 분석」, 2024.12., p.25

2) 제13조(정보보호 공시) ① 정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제2호에 따른 정보통신 서비스를 이용하는 자의 안전한 인터넷이용을 위하여 정보보호 투자 및 인력 현황, 정보보호 관련 인증 등 정보보호 현황을 대통령령으로 정하는 바에 따라 공개할 수 있다. (후단생략)

② 제1항에도 불구하고 정보통신서비스를 이용하는 자의 안전한 인터넷이용을 위하여 정보보호 공시를 도입할 필요성이 있는 자로서 사업 분야, 매출액 및 서비스 이용자 수 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자는 제1항에 따른 정보보호 현황을 공시하여야 한다. (단서생략)

○ 안 제45조 제5항은 주요정보통신서비스 제공자 등이 정보기술 및 정보보호 분야별 전문인력 및 충분한 예산을 확보하도록 노력할 의무를 부과함으로써,

사업자가 정보통신망 침해사고 예방에 필요한 정보보호 역량을 갖추 수 있도록 인력·재원 등 자원의 투자를 유도하려는 것임.

○ 현재는 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」에 따른 정보보호 관리체계(ISMS; Information Security Management System) 인증기준 세부 항목에 인력 및 예산 등 자원 할당에 관한 사항을 규정³⁾하고 있어,

개정안이 시행될 경우 사업자의 정보보호 분야 자원 확보 의무에 관한 근거가 고시에서 법률로 상향된다는 의의가 있음.

- 참고로, 주요정보통신서비스 제공자 등에게 정보기술부문 예산에 대통령령으로 정하는 비율 이상의 정보보호 예산을 반영하도록 하려는 동법 개정안⁴⁾이 현재 우리 위원회에 계류되어 있으므로 병합하여 심사할 필요가 있음.

3)23조(인증심사 기준)① 다음 각 호의 인증의 구분에 따라 별표 7의 인증기준을 적용한다.

2. 정보보호 관리체계 인증 : 별표 7 가목 및 나목

[별표 7] 인증기준(제23조 관련)

항목	상세 내용
1.1.6	자원 할당 최고경영자는 정보보호와 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고, 관리체계의 효과적 구현과 지속적 운영을 위한 예산 및 자원을 할당하여야 한다.

4) 의안번호 제2211048호(구자근의원 대표발의)

○ 과학기술정보통신부는 개정안과 같이 정보보호 분야 인력, 예산 확보 노력을 의무화하는 것에는 동의하나,

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 “정보통신망법”)은 정보통신망의 이용, 정보보호 등 정보기술 분야 중 일부에 대해서만 규율하고 있으므로,

정보기술 부문에 대한 인력, 예산 확보 노력 의무는 정보통신망법이 아닌 다른 법에 규율하는 것이 바람직하다는 의견을 제출함

2. 정보보호 관리체계(ISMS) 인증기준 차등화 등(안 제47조 제8항 등)

가. 개정안 요지

- 한국인터넷진흥원, 정보보호 관리체계 인증기관 및 심사기관은 정보보호 관리체계에 대한 사후관리 시 현장심사와 서면심사의 방법을 병행하여 실시하여야 함(안 제47조 제8항).
- 정보보호 관리체계 인증 취소 사유로 ‘정보보호 관련 법령을 위반하고 그 위반사유가 중대한 경우’를 추가함(안 제47조 제10항 제4호 신설).
- 과학기술정보통신부장관은 정보보호 관리체계 인증을 받으려는 자 중 생성·처리하는 정보의 규모, 사회적 파급력으로 인하여 침해사고 발생 시 중대한 위협을 초래할 우려가 있는 자에 대하여 인증기준 및 절차 등을 강화하여 적용할 수 있음(안 제47조의7 제2항 신설).
- 과학기술정보통신부장관은 정보보호 관리체계 인증 의무 대상임에도 인증을 받지 아니한 자에게 대통령령으로 정하는 매출액의 100분의 3을 초과하지 않는 범위(매출액이 없거나 매출액의 산정이 곤란한 경우 10억원을 초과하지 않는 범위)에서 과징금을 부과할 수 있음(안 제47조의8 신설).

나. 개정안 조문대비표

현행	개정안
제47조(정보보호 관리체계의 인증) ① (생략)	제47조(정보보호 관리체계의 인증) ① (현행과 같음)
② 「전기통신사업법」 제2조 제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.	② ----- ----- ----- ----- ----- ----- -----.
1. 「전기통신사업법」 제6조제1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자(이하 “주요정보통신서비스 제공자”라 한다)	1. <u>주요정보통신서비스 제공자</u>
2. 3. (생략)	2. 3. (현행과 같음)
③ ~ ⑦ (생략)	③ ~ ⑦ (현행과 같음)
⑧ 한국인터넷진흥원, 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관은 정보보호 관리체계의 실효성 제고를 위하여 연 1회 이상 사후관리를 실시하고 그 결과를 과학	⑧ ----- ----- ----- ----- ----- -----

현행	개정안
기술정보통신부장관에게 통보하여야 한다. <후단 신설> ⑨ (생략) ⑩ 과학기술정보통신부장관은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 경우에는 인증을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 인증을 취소하여야 한다. 1. ~ 3. (생략) <신설> ⑪·⑫ (생략) 제47조의7(정보보호 관리체계 인증의 특례) ① (생략) <신설>	----- ----- 이 경우 사후관리는 현장심사와 서면심사의 방법을 병행하여 실시한다. ⑨ (현행과 같음) ⑩ ----- ----- ----- ----- ----- 1. ~ 3. (현행과 같음) 4. 정보보호 관련 법령을 위반하고 그 위반사유가 중대한 경우 ⑪·⑫ (현행과 같음) 제47조의7(정보보호 관리체계 인증의 차등적용 등) ① (현행과 같음) ② 과학기술정보통신부장관은 제47조제1항 및 제2항에 따른 인증을 받으려는 자 중 생성·처리하는 정보의 규모와 사회적 파급력으로 인하여 침해사고 발생 시 국민의 생명·신체

현행	개정안
② 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 제1항에 관련된 비용 및 기술 등 필요한 지원을 할 수 있다. ③ 과학기술정보통신부장관은 제1항에 따른 인증기준 및 절차 등 그 밖에 필요한 사항을 정하여 고시할 수 있다. <신설>	또는 재산에 중대한 위험을 초래할 우려가 있는 자로서 대통령령으로 정하는 자에 대하여 제47조에 따른 인증기준 및 절차 등을 강화하여 적용할 수 있다. ③ ----- ----- -----제1항 및 제2항에----- -----. ④ ----- 제1항 및 제2항에----- ----- ----- -. 제47조의8(과징금의 부과) ① 과학기술정보통신부장관은 제47조제2항을 위반하여 정보보호관리체계 인증을 받지 아니한 자에게는 대통령령으로 정하는 매출액의 100분의 3을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다. 다만, 매출액이 없거나 매출액의 산정이

현행	개정안
	<u>곤란한 경우로서 대통령령으로 정하는 경우에는 10억원을 초과하지 아니하는 범위에서 과징금을 부과할 수 있다.</u> <u>② 제1항에 따른 과징금의 구체적인 산정기준과 절차는 대통령령으로 정한다.</u> <u>③ 과학기술정보통신부장관은 제1항에 따른 과징금을 내야 할 자가 납부기한까지 이를 내지 아니하면 납부기한의 다음 날부터 내지 아니한 과징금의 연 100분의 6에 해당하는 가산금을 징수한다. 이 경우 가산금을 징수하는 기간은 60개월을 초과하지 못한다.</u> <u>④ 과학기술정보통신부장관은 제1항에 따른 과징금을 내야 할 자가 납부기한까지 내지 아니한 경우에는 기간을 정하여 독촉하고, 독촉으로 지정한 기간 내에 과징금과 제3항에 따른 가산금을 내지 아니하면 국세강제징수의 예에 따라 징수한다.</u>

현행	개정안
제76조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료	⑤ 과학기술정보통신부장관은 법원의 판결 등의 사유로 제1항에 따라 부과된 과징금을 환급하는 경우에는 과징금을 낸 날부터 환급하는 날까지의 기간에 대하여 금융회사 등의 예금이자율 등을 고려하여 대통령령으로 정하는 이자율을 적용하여 계산한 환급가산금을 지급하여야 한다.
	⑥ 과학기술정보통신부장관은 제5항에도 불구하고 법원의 판결에 따라 과징금 부과처분이 취소되어 그 판결이유에 따라 새로운 과징금을 부과하는 경우에는 당초 납부한 과징금에서 새로 부과하기로 결정한 과징금을 공제한 나머지 금액에 대해서만 환급가산금을 계산하여 지급한다. 제76조(과태료) ① ----- ----- ----- ----- -----

현행	개정안
를 부과한다. 1. ~ 6의4. (생략) 6의5. 제47조제2항을 위반하여 정보보호 관리체계 인증을 받 지 아니한 자 6의6. ~ 12. (생략) ② ~ ④ (생략)	-----. 1. ~ 6의4. (현행과 같음) <삭제> 6의6. ~ 12. (현행과 같음) ② ~ ④ (현행과 같음)

다. 검토사항

- 정보보호 관리체계(ISMS; Information Security Management System) 인증제도는 정보통신서비스 제공자가 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치 등 종합적 관리체계를 수립하면 과학기술정보통신부장관이 그 적합성을 인증하여 주는 제도임.
- ISMS 인증제도는 정부가 ISMS 모델을 개발·제공함으로써 기업이 스스로 ISMS를 구축·운영할 수 있도록 하려는 취지로 2001년 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 “정보통신망법”) 개정을 통해 도입되었음.
- ISMS 인증을 받으려는 자는 관리체계 수립 및 운영에 대한 기준 (16개)과 보호대책 요구사항(64개)을 충족하여야 함⁵⁾.

5) ISMS 인증기준의 구체적인 내용은 참고자료 참조

○ 현행 정보통신망법은 ISMS 인증을 받고자 하는 자가 자율적으로 인증을 신청·취득하는 것을 기본으로 하고 있음(현행 제47조 제1항)⁶⁾.

- ISMS 인증을 받은 자에 대해서는 기업의 대외 이미지 제고를 위해 그 인증의 내용을 표시하거나 홍보할 수 있도록 하고⁷⁾, 공공부문 사업 입찰 시 가산점 등 인센티브를 얻을 수 있도록 함으로써 인증 취득의 유인을 제공함⁸⁾.

○ 한편, 서비스 종류 및 규모 등이 일정 기준에 해당하는 사업자의 경우 의무적으로 ISMS 인증을 받도록 하고 있음(현행 제47조 제2항)⁹⁾¹⁰⁾.

6) 제47조(정보보호 관리체계의 인증) ① 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 “정보보호 관리체계”라 한다)를 수립·운영하고 있는 자에 대하여 제4항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.

7) 제47조(정보보호 관리체계의 인증) ⑨ 제1항 및 제2항에 따라 정보보호 관리체계의 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다.

8) 과학기술정보통신부·개인정보보호위원회, 「정보보호 및 개인정보보호 관리체계 인증제도 안내서」, 2024.7., p.12

9) 제47조(정보보호 관리체계의 인증) ② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.

1. 「전기통신사업법」 제6조제1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자(이하 “주요정보통신서비스 제공자”라 한다)

2. 집적정보통신시설 사업자

3. 전년도 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 전년도 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

정보통신망법 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.

② 법 제47조제2항제3호에서 “대통령령으로 정하는 기준에 해당하는 자”란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 전년도 매출액 또는 세입이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자
가. 「의료법」 제3조의4에 따른 상급종합병원

나. 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교
2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자. 다만, 「전자금융거래법」 제2조제3호에 따른 금융회사는 제외한다.

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

10) 2024년 12월 기준 인증 의무대상자는 총 548개 사(社)임

- 인증의무자가 인증을 받지 아니한 경우 3천만원 이하의 과태료를 부과함¹¹⁾.

< ISMS 인증 의무대상자 >

구분	의무대상자 기준
정보통신망서비스 제공자(ISP)	「전기통신사업법」 제6조 제1항에 따른 등록을 한 자(기간통신사업자)로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자
집적정보통신시설 사업자(IDC)	타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 자
매출액 또는 이용자수 요건에 따른 대상자	정보통신서비스 부문 전년도 매출액이 100억원 이상인 자 (「전자금융거래법」 제2조 제3호에 따른 금융회사 제외)
	전년도 일일 평균 정보통신서비스 이용자 수가 100만명 이상인 자 (「전자금융거래법」 제2조 제3호에 따른 금융회사 제외)
	전년도 매출액 또는 세입이 1,500억원 이상이며 다음에 해당하는 자 - 「의료법」 제3조의4에 따른 상급종합병원 - 직전년도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교

- 그런데 최근 SK텔레콤 해킹 사고에서 SK텔레콤이 ISMS 인증을 취득하였음에도 침해사고 대응 절차가 제대로 작동하지 않았다는 지적에 따라¹²⁾, 침해사고 발생 시 국가사회적 영향이 큰 사업자에 대한 관리를 강화하는 등 ISMS 인증제도를 개선할 필요성이 제기되고 있음.
- 이에 개정안은 ISMS 인증에 대한 사후관리 시 현장심사와 서면심사를 병행하도록 하고,

11) 제76조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다.

6의5. 제47조제2항을 위반하여 정보보호 관리체계 인증을 받지 아니한 자

12) 보안뉴스, “[SKT 해킹 사태] SKT, ISMS 인증받아도 해킹..실효성 강화 시급”, 2025.4.29.

정보보호 관련 법령을 위반하고 그 사유가 중대한 경우에 ISMS 인증을 취소할 수 있도록 하며

침해사고 발생 시의 사회적 과급력 등을 고려하여 ISMS 인증기준을 달리 정할 수 있도록 하고,

ISMS 인증 의무대상자가 인증을 받지 아니한 경우 과징금을 부과할 수 있도록 함으로써 ISMS 인증제도를 전반적으로 개선하려는 것임.

□ ISMS 사후관리 절차 규정(안 제47조 제8항)

○ 안 제47조 제8항은 한국인터넷진흥원, 정보보호 관리체계 인증기관 및 심사기관이 ISMS 인증에 대한 사후관리 시에 현장심사와 서면심사를 병행하도록 함으로써 보다 심도 있는 사후관리를 하려는 것임.

- 현행 정보통신망법은 ISMS 인증의 실효성 제고를 위하여 인증사업자에 대하여 연 1회 이상 사후관리를 실시하도록 하고, 그 결과를 과학기술 정보통신부장관에게 통보하도록 하고 있음¹³⁾.

○ 다만, 현행법상 사후관리의 방법·절차에 관한 사항은 대통령령으로 정하도록 하고 있고¹⁴⁾, 이에 따라 동법 시행령에서 사후관리는 서면심사 또는 현장심사의 방법으로 하도록 하고 있음¹⁵⁾.

13) 제47조(정보보호 관리체계의 인증) ⑧ 한국인터넷진흥원, 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관은 정보보호 관리체계의 실효성 제고를 위하여 연 1회 이상 사후관리를 실시하고 그 결과를 과학기술정보통신부장관에게 통보하여야 한다.

14) 제47조(정보보호 관리체계의 인증) ⑪ 제1항 및 제2항에 따른 인증의 방법·절차·범위·수수료, 제8항에 따른 사후관리의 방법·절차, 제10항에 따른 인증취소의 방법·절차, 그 밖에 필요한 사항은 대통령령으로 정한다.

15) 제51조(인증의 사후관리) ① 법 제47조제8항에 따른 사후관리는 서면심사 또는 현장심사의 방법으로 실시한다.

- 또한, 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」는 사후관리와 관련하여 인증심사에 대한 규정을 준용하도록 하고 있는데¹⁶⁾, 인증심사의 경우 신청인을 방문하여 서면심사와 현장심사를 병행하도록 하고 있음.
- 따라서 현행 법령에 의해서도 사후관리 시 서면심사와 현장심사의 병행이 가능할 것으로 보임.
- 과학기술정보통신부는 현재도 서면심사와 현장심사를 병행하여 실시 중이나, 이를 명문화하는 경우 규범력을 강화할 수 있다는 점에서 개정안에 동의하는 입장임.

□ ISMS 인증 취소 사유 추가(안 제47조 제10항 제4호 신설)

- 현행 정보통신망법은 ISMS 인증의 취소 사유로 ① 거짓이나 그 밖의 부정한 방법으로 인증을 받은 경우, ② 인증기준에 미달하게 된 경우, ③ 사후관리를 거부 또는 방해한 경우로 제시하고 있음.
- 안 제47조 제10항 제4호는 ISMS 인증을 받은 자가 정보보호 관련 법령을 위반하고 그 위반사유가 중대한 경우에도 과학기술정보통신부장관이 인증을 취소할 수 있도록 함으로써 관련 법령의 준수를 유도하려는 것임.

16) 제27조(사후관리) ① 인증을 취득한 자는 인증서 유효기간 중 연 1회 이상 심사수행기관에 사후심사를 신청하여야 한다.

② 사후심사는 제5장(인증심사의 신청 및 수수료 납부) 및 제6장(인증심사의 기준과 방법)을 준용하여 진행한다.

제25조(인증심사 방법 및 보완조치) ① 인증심사는 신청인을 방문하여 서면심사와 현장심사를 병행한다.

- 다만 정보보호 관련 의무를 규정하고 있는 법령은 정보통신망법과 그 하위법령 외에도 「정보통신기반 보호법」, 「정보보호산업의 진흥에 관한 법률」 등 다양하고, 어떠한 위반사유가 ‘중대한’ 것인지에 대한 객관적인 판단기준이 없으므로,
수범자의 예측가능성을 위하여 법률에서 인증취소의 사유를 가능한 한 구체적으로 명시할 필요가 있음.
- 또한, 현행 제47조 제2항에 따른 ISMS 인증 의무대상자의 경우 개정안에 따라 인증이 취소되더라도 인증의무 이행을 위해 다시 동일한 내용의 인증을 신청하게 될 것이고, 이 경우 별다른 사유가 없는 한 과학기술정보통신부장관은 다시 인증을 해 주어야 할 것이므로 인증 취소에 따른 제재의 효과가 크지 않을 수 있음.
- 과학기술정보통신부는 법령위반에 대한 엄정한 제재를 위해 인증취소의 요건을 신설하는 것에 동의하나,
정보보호 관련 법령의 범위가 구체적이지 않으므로 정보통신망법 및 하위법령으로 한정하여 구체화할 필요가 있다는 입장임.

□ ISMS 인증기준 차등화(안 제47조 제4항)

- 안 제47조 제4항은 생성·처리하는 정보의 규모, 침해사고 발생 시 사회적 파급력 등을 고려하여 ISMS 인증기준을 달리함으로써 ISMS의 실효성을 제고하려는 것으로, 다음의 사항을 고려할 필요가 있음.

- 첫째, 앞서 언급한 바와 같이 현행 ISMS 인증제도가 기본적으로 기업들의 자율적인 참여를 유도하여 전반적인 정보보호 수준을 향상하려는 취지로 도입·활용되고 있음을 고려할 때, 인증기준 강화에 따른 인증 취득 유인 저하 가능성과 강화된 인증기준에 의한 기업 신뢰 제고 등 기대이익 사이의 비교형량이 필요해 보임.
- 둘째, 현재 이동통신사업자 등 국가사회적 영향력이 큰 사업자들에게 대해서는 이미 「정보통신기반 보호법」에 보다 심화된 관리체계가 마련되어 있음.
- 「정보통신기반 보호법」에 따른 ‘주요정보통신기반시설’이란 업무의 국가사회적 중요성, 침해사고 발생 시 국가안전보장과 경제사회에 미치는 피해규모 및 범위 등을 고려하여 지정된 전자적 제어·관리 시스템 또는 정보통신망으로, 중앙행정기관의 장이 정보통신기반보호위원회의 심의를 거쳐 지정함¹⁷⁾.
- 주요정보통신기반시설로 지정되는 경우 해당 시설의 관리기관이 침해 행위 예방, 백업, 복구 등 물리적·기술적 대책을 포함한 관리대책을 수립하여 관계 중앙행정기관의 장에게 제출하고, 정기적으로 취약점을

17) 제8조(주요정보통신기반시설의 지정 등) ①중앙행정기관의 장은 소관분야의 정보통신기반시설 중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.

1. 해당 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
2. 제1호에 따른 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
3. 다른 정보통신기반시설과의 상호연계성
4. 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
5. 침해사고의 발생가능성 또는 그 복구의 용이성

⑤중앙행정기관의 장이 제1항 및 제3항에 따라 지정 또는 지정 취소를 하고자 하는 경우에는 위원회의 심의를 받아야 한다. 이 경우 위원회는 제1항 및 제3항에 따라 지정 또는 지정취소의 대상이 되는 관리기관의 장을 위원회에 출석하게 하여 그 의견을 들을 수 있다.

분석·평가하도록 하고 있으며¹⁸⁾,

과학기술정보통신부장관과 국가정보원장 등은 관리기관에 대하여 해당 대책의 이행 여부를 확인하도록 하고 있음¹⁹⁾.

- 또한, 관계중앙행정기관의 장은 주요정보통신기반시설에 대한 보호지침을 제정하고 관리기관의 장에게 이를 지키도록 명령할 수 있으며²⁰⁾, 별도의 보호조치가 필요하다고 인정하는 경우 관리기관의 장에게 필요한 조치를 명령할 수 있음²¹⁾.

- 따라서 현재 국가사회적 중요성이 인정되는 사업자에 대해서는 그 특수성을 고려한 별도의 관리가 이루어지고 있다고 보이며, 필요한 경우 주요정보통신기반시설 지정 확대 또는 관리대책·보호지침의 개선을 통해서도 개정안의 취지를 달성할 수 있을 것으로 보임.

18) 제5조(주요정보통신기반시설보호대책의 수립 등) ①주요정보통신기반시설을 관리하는 기관(이하 “관리기관”이라 한다)의 장은 제9조제1항 또는 제2항에 따른 취약점 분석·평가의 결과에 따라 소관 주요정보통신기반시설 및 관리 정보를 안전하게 보호하기 위한 예방, 백업, 복구 등 물리적·기술적 대책을 포함한 관리대책(이하 “주요정보통신기반시설보호대책”이라 한다)을 수립·시행하여야 한다.

②관리기관의 장은 제1항에 따라 주요정보통신기반시설보호대책을 수립한 때에는 이를 주요정보통신기반시설을 관할하는 중앙행정기관(이하 “관계중앙행정기관”이라 한다)의 장에게 제출하여야 한다. 다만, 관리기관의 장이 관계중앙행정기관의 장인 경우에는 그러하지 아니하다.

제9조(취약점의 분석·평가) ①관리기관의 장은 대통령령으로 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다.

19) 제5조의2(주요정보통신기반시설보호대책 이행 여부의 확인) ① 과학기술정보통신부장관과 국가정보원장 등 대통령령으로 정하는 국가기관의 장(이하 “국가정보원장등”이라 한다)은 관리기관에 대하여 주요정보통신기반시설보호대책의 이행 여부를 확인할 수 있다.

20) 제10조(보호지침) ①관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설에 대하여 보호지침을 제정하고 해당분야의 관리기관의 장에게 이를 지키도록 명령할 수 있다.

② 제1항에 따른 명령을 받은 관리기관의 장은 이를 이행하여야 한다.

21) 제11조(보호조치 명령) ① 관계중앙행정기관의 장은 다음 각 호의 어느 하나에 해당하는 경우 해당 관리기관의 장에게 주요정보통신기반시설의 보호에 필요한 조치를 하도록 명령할 수 있다.

1. 제5조제2항에 따라 제출받은 주요정보통신기반시설보호대책을 분석하여 별도의 보호조치가 필요하다고 인정하는 경우
2. 제5조의2제3항에 따라 통보된 주요정보통신기반시설보호대책의 이행 여부를 분석하여 별도의 보호조치가 필요하다고 인정하는 경우

- 참고로, 현재 이동통신 3사의 인터넷접속망과 이동전화(무선인터넷망)는 주요정보통신기반시설로 지정되어 있음²²⁾.
- 셋째, 인증기준 차등화 기준인 ‘사회적 파급력’ 등의 의미와 범위가 불명확한 측면이 있음을 고려할 때, 수범자의 예측가능성 측면에서 이와 같은 기준 설정이 적정한지 검토가 필요해 보임.
- 과학기술정보통신부는 정보의 규모 및 사회적 파급력 등을 고려하여 별도의 인증기준을 마련하는 것에 동의하는 입장임.
- 한국인터넷기업협회는 정보의 규모, 사회적 파급력 등의 기준이 모호하여 명확성의 원칙에 위배될 우려가 있다는 의견을 제출함.

□ ISMS 미인증 사업자에 대한 과징금의 부과(안 제47조의8 신설 및 제76조제1항제6호의5 삭제)

- 안 제47조의8은 현행 제47조 제2항에 따른 ISMS 인증의무를 위반한 자에 대하여 현행법상 제재인 과태료에 비해 중한 제재인 과징금을 부과함으로써 의무의 준수를 유도하려는 것이고,
- 안 제76조제1항제6호의5는 동일한 행위에 대하여 과징금과 과태료를 중복적으로 부과하는 경우 수범자에게 과도한 제재가 될 수 있음을 감안하여, 동일 위반사항에 대한 현행 과태료 부과 근거를 삭제하려는 것임.

²²⁾ 방송통신위원회 소관분야 주요정보통신기반시설(방송통신위원회고시)

- 다만 과징금 부과에 대해서는 과징금 제도의 취지 및 타 위반행위와의 형평성 등을 고려하여 도입 필요성을 신중하게 논의할 필요가 있음.
- 과징금은 행정상 의무위반으로 얻은 경제적 이익을 박탈하거나 영업 정지 처분을 갈음하여 행정청이 부과하는 금전상의 제재를 말함.
- 현재 정보통신망법에는 과징금 규정이 없으므로, 개정안에 따르면 ISMS 관련 의무위반이 정보통신망법상 유일한 과징금 부과 대상이 됨.
- 그런데 ISMS 의무자가 ISMS 인증을 받지 않음으로써 박탈이 필요한 만큼의 경제적 이익을 획득한다고 보기 어려운 측면이 있고, ISMS 인증의무 위반으로 획득한 이익이 정보통신망법상 타 위반 행위로 획득한 이익에 비해 그 규모나 환수의 필요성이 더 크다고 볼 수 있는지에 대해서도 논의가 필요할 것으로 보임.
- 과학기술정보통신부는 인증제도의 실효성을 강화하려는 개정취지에는 공감하나, 과징금은 불법적인 경제적 이득을 취하거나 사회적 파급효과가 큰 위반행위 등에 대한 제재수단으로, 인증의무 위반을 이유로 매출액에 비례한 과징금을 부과하는 것은 기업에게 과도한 부담이 될 우려가 있고, 현행 정보통신망법이 과징금을 규정하지 않고 있음을 고려할 때 과징금 도입 필요성에 대해서는 법체계 전반을 고려하여 검토할 필요가 있다는 입장임.
- 한국인터넷기업협회는 과징금 부과는 과도한 규제로서 침해사고 예방이라는 목적을 달성하기에 적합한 수단인지 검토할 필요가 있고, 현행

ISMS 인증제도는 보다 많은 사업자들이 인증을 취득할 수 있도록 인센티브 구조로 설계되어 있음을 감안할 필요가 있다는 의견을 제출함.

문 의 처
02)6788-5230

※참고: ISMS 인증기준(「정보보호 및 개인정보보호 관리체계 인증
등에 관한 고시」 [별표 7])

가. 관리체계 수립 및 운영

분야		항목		상세 내용
1.1.	관리체계 기 반 마련	1.1.1	경영진의 참여	최고경영자는 정보보호 및 개인정보보호 관리체계의 수립 과 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여 운영하여야 한다.
		1.1.2	최고책임자의 지정	최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책 임자와 개인정보보호 업무를 총괄하는 개인정보보호 책임 자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.
		1.1.3	조직 구성	최고경영자는 정보보호와 개인정보보호의 효과적 구현을 위한 실무조직, 조직 전반의 정보보호와 개인정보보호 관 련 주요 사항을 검토 및 의결할 수 있는 위원회, 전사적 보호활동을 위한 부서별 정보보호와 개인정보보호 담당자 로 구성된 협의체를 구성하여 운영하여야 한다.
		1.1.4	범위 설정	조직의 핵심 서비스와 개인정보 처리 현황 등을 고려하여 관리체계 범위를 설정하고, 관련된 서비스를 비롯하여 개 인정보 처리 업무와 조직, 자산, 물리적 위치 등을 문서 화하여야 한다.
		1.1.5	정책 수립	정보보호와 개인정보보호 정책 및 시행문서를 수립·작성 하며, 이때 조직의 정보보호와 개인정보보호 방침 및 방 향을 명확하게 제시하여야 한다. 또한 정책과 시행문서는 경영진 승인을 받고, 임직원 및 관련자에게 이해하기 쉬 운 형태로 전달하여야 한다.
		1.1.6	자원 할당	최고경영자는 정보보호와 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고, 관리체계의 효과적 구현과 지속적 운영을 위한 예산 및 자원을 할당하여야 한다.
1.2.	위험 관리	1.2.1	정보자산 식별	조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요 도를 산정한 후 그 목록을 최신으로 관리하여야 한다.
		1.2.2	현황 및 흐름분석	관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.
		1.2.3	위험 평가	조직의 대내외 환경분석을 통해 유형별 위협정보를 수집 하고 조직에 적합한 위험 평가 방법을 선정하여 관리체계 전 영역에 대하여 연 1회 이상 위험을 평가하며, 수용할 수 있는 위험은 경영진의 승인을 받아 관리하여야 한다.
		1.2.4	보호대책 선정	위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 조직에 적합한 보호대책을 선정하고, 보호대책의 우선순 위와 일정·담당자·예산 등을 포함한 이행계획을 수립하 여 경영진의 승인을 받아야 한다.
1.3.	관리체계 운 영	1.3.1	보호대책 구현	선정한 보호대책은 이행계획에 따라 효과적으로 구현하 고, 경영진은 이행결과의 정확성과 효과성 여부를 확인하 여야 한다.

		1.3.2	보호대책 공유	보호대책의 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여 지속적으로 운영 되도록 하여야 한다.
		1.3.3	운영현황 관리	조직이 수립한 관리체계에 따라 상시적 또는 주기적으로 수행하여야 하는 운영활동 및 수행 내역은 식별 및 추적이 가능하도록 기록하여 관리하고, 경영진은 주기적으로 운영활동의 효과성을 확인하여 관리하여야 한다.
1.4.	관리체계 점검 및 개선	1.4.1	법적 요구사항 준수 검토	조직이 준수하여야 할 정보보호 및 개인정보보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토하여야 한다.
		1.4.2	관리체계 점검	관리체계가 내부 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는지 독립성과 전문성이 확보된 인력을 구성하여 연 1회 이상 점검하고, 발견된 문제점을 경영진에게 보고하여야 한다.
		1.4.3	관리체계 개선	법적 요구사항 준수검토 및 관리체계 점검을 통해 식별된 관리체계상의 문제점에 대한 원인을 분석하고 재발방지 대책을 수립·이행하여야 하며, 경영진은 개선 결과의 정확성과 효과성 여부를 확인하여야 한다.

나. 보호대책 요구사항

분야		항목		상세 내용
2.1.	정책, 조직, 자산 관리	2.1.1	정책의 유지관리	정보보호 및 개인정보보호 관련 정책과 시행문서는 법령 및 규제, 상위 조직 및 관련 기관 정책과의 연계성, 조직의 대내외 환경변화 등에 따라 주기적으로 검토하여 필요한 경우 제·개정하고 그 내역을 이력관리하여야 한다.
		2.1.2	조직의 유지관리	조직의 각 구성원에게 정보보호와 개인정보보호 관련 역할 및 책임을 할당하고, 그 활동을 평가할 수 있는 체계와 조직 및 조직의 구성원 간 상호 의사소통할 수 있는 체계를 수립하여 운영하여야 한다.
		2.1.3	정보자산 관리	정보자산의 용도와 중요도에 따른 취급 절차 및 보호대책을 수립·이행하고, 자산별 책임소재를 명확히 정의하여 관리하여야 한다.
2.2.	인적 보안	2.2.1	주요 직무자 지정 및 관리	개인정보 및 중요정보의 취급이나 주요 시스템 접근 등 주요 직무의 기준과 관리방안을 수립하고, 주요 직무자를 최소한으로 지정하여 그 목록을 최신으로 관리하여야 한다.
		2.2.2	직무 분리	권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여 직무 분리 기준을 수립하고 적용하여야 한다. 다만 불가피하게 직무 분리가 어려운 경우 별도의 보완대책을 마련하여 이행하여야 한다.
		2.2.3	보안 서약	정보자산을 취급하거나 접근권한이 부여된 임직원·임시직원·외부자 등이 내부 정책 및 관련 법규, 비밀유지 의무 등 준수사항을 명확히 인지할 수 있도록 업무 특성에 따른 정보보호 서약을 받아야 한다.
		2.2.4	인식제고 및 교육훈련	임직원 및 관련 외부자가 조직의 관리체계와 정책을 이해하고 직무별 전문성을 확보할 수 있도록 연간 인식제고 활동 및 교육훈련 계획을 수립·운영하고, 그 결과에 따른 효과성을 평가하여 다음 계획에 반영하여야 한다.
		2.2.5	퇴직 및 직무변경 관리	퇴직 및 직무변경 시 인사·정보보호·개인정보보호·IT 등 관련 부서별 이행하여야 할 자산반납, 계정 및 접근권한 회수·조정, 결과확인 등의 절차를 수립·관리하여야 한다.
		2.2.6	보안 위반 시 조치	임직원 및 관련 외부자가 법령, 규제 및 내부정책을 위반한 경우 이에 따른 조치 절차를 수립·이행하여야 한다.
2.3.	외부자 보안	2.3.1	외부자 현황 관리	업무의 일부(개인정보취급, 정보보호, 정보시스템 운영 또는 개발 등)를 외부에 위탁하거나 외부의 시설 또는 서비스(집적정보통신시설, 클라우드 서비스, 애플리케이션 서비스 등)를 이용하는 경우 그 현황을 식별하고 법적 요구사항 및 외부 조직·서비스로부터 발생하는 위험을 파악하여 적절한 보호대책을 마련하여야 한다.
		2.3.2	외부자 계약 시 보안	외부 서비스를 이용하거나 외부자에게 업무를 위탁하는 경우 이에 따른 정보보호 및 개인정보보호 요구사항을 식별하고, 관련 내용을 계약서 또는 협정서 등에 명시하여야 한다.
		2.3.3	외부자 보안 이행 관리	계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보보호 요구사항에 따라 외부자의 보호대책 이행 여부를 주기적인 점검 또는 감사 등 관리·감독하여야 한다.

		2.3.4	외부자 계약 변경 및 만료 시 보안	외부자 계약만료, 업무종료, 담당자 변경 시에는 제공한 정보자산 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 업무 수행 중 취득정보의 비밀유지 약속서 징구 등의 보호대책을 이행하여야 한다.
2.4.	물리 보안	2.4.1	보호구역 지정	물리적·환경적 위협으로부터 개인정보 및 중요정보, 문서, 저장매체, 주요 설비 및 시스템 등을 보호하기 위하여 통제구역·제한구역·접근구역 등 물리적 보호구역을 지정하고 각 구역별 보호대책을 수립·이행하여야 한다.
		2.4.2	출입통제	보호구역은 인가된 사람만이 출입하도록 통제하고 책임추적성을 확보할 수 있도록 출입 및 접근 이력을 주기적으로 검토하여야 한다.
		2.4.3	정보시스템 보호	정보시스템은 환경적 위협과 유해요소, 비인가 접근 가능성을 감소시킬 수 있도록 중요도와 특성을 고려하여 배치하고, 통신 및 전력 케이블이 손상을 입지 않도록 보호하여야 한다.
		2.4.4	보호설비 운영	보호구역에 위치한 정보시스템의 중요도 및 특성에 따라 온도·습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 보호설비를 갖추고 운영절차를 수립·운영하여야 한다.
		2.4.5	보호구역 내 작업	보호구역 내에서의 비인가행위 및 권한 오·남용 등을 방지하기 위한 작업 절차를 수립·이행하고, 작업 기록을 주기적으로 검토하여야 한다.
		2.4.6	반출입 기기 통제	보호구역 내 정보시스템, 모바일 기기, 저장매체 등에 대한 반출입 통제절차를 수립·이행하고 주기적으로 검토하여야 한다.
		2.4.7	업무환경 보안	공용으로 사용하는 사무용 기기(문서고, 공용 PC, 복합기, 파일서버 등) 및 개인 업무환경(업무용 PC, 책상 등)을 통해 개인정보 및 중요정보가 비인가자에게 노출 또는 유출되지 않도록 클린데스크, 정기점검 등 업무환경 보호대책을 수립·이행하여야 한다.
2.5.	인증 및 권한관리	2.5.1	사용자 계정 관리	정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 사용자 등록·해지 및 접근권한 부여·변경·말소 절차를 수립·이행하고, 사용자 등록 및 권한부여 시 사용자에게 보안책임이 있음을 규정화하고 인식시켜야 한다.
		2.5.2	사용자 식별	사용자 계정은 사용자별로 유일하게 구분할 수 있도록 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 하며, 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하여 책임자의 승인 및 책임추적성 확보 등 보완대책을 수립·이행하여야 한다.
		2.5.3	사용자 인증	정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용하여야 한다. 또한 로그인 횟수 제한, 불법 로그인 시도 경고 등 비인가자 접근 통제방안을 수립·이행하여야 한다.
		2.5.4	비밀번호 관리	법적 요구사항, 외부 위협요인 등을 고려하여 정보시스템 사용자 및 고객, 회원 등 정보주체(이용자)가 사용하는 비밀번호 관리절차를 수립·이행하여야 한다.
		2.5.5	특수 계정 및 권한 관리	정보시스템 관리, 개인정보 및 중요정보 관리 등 특수 목적을 위하여 사용하는 계정 및 권한은 최소한으로 부여하고 별도로 식별하여 통제하여야 한다.

		2.5.6	접근권한 검토	정보시스템과 개인정보 및 중요정보에 접근하는 사용자 계정의 등록·이용·삭제 및 접근권한의 부여·변경·삭제 이력을 남기고 주기적으로 검토하여 적정성 여부를 점검하여야 한다.
2.6.	접근통제	2.6.1	네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위하여 IP관리, 단말인증 등 관리절차를 수립·이행하고, 업무목적 및 중요도에 따라 네트워크 분리(DMZ, 서버팜, DB존, 개발존 등)와 접근통제를 적용하여야 한다.
		2.6.2	정보시스템 접근	서버, 네트워크시스템 등 정보시스템에 접근을 허용하는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 통제하여야 한다.
		2.6.3	응용프로그램 접근	사용자별 업무 및 접근 정보의 중요도 등에 따라 응용프로그램 접근권한을 제한하고, 불필요한 정보 또는 중요정보 노출을 최소화할 수 있도록 기준을 수립하여 적용하여야 한다.
		2.6.4	데이터베이스 접근	테이블 목록 등 데이터베이스 내에서 저장·관리되고 있는 정보를 식별하고, 정보의 중요도와 응용프로그램 및 사용자 유형 등에 따른 접근통제 정책을 수립·이행하여야 한다.
		2.6.5	무선 네트워크 접근	무선 네트워크를 사용하는 경우 사용자 인증, 송수신 데이터 암호화, AP 통제 등 무선 네트워크 보호대책을 적용하여야 한다. 또한 AD Hoc 접속, 비인가 AP 사용 등 비인가 무선 네트워크 접속으로부터 보호대책을 수립·이행하여야 한다.
		2.6.6	원격접근 통제	보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지하고, 재택근무·장애대응·원격협업 등 불가피한 사유로 원격접근을 허용하는 경우 책임자 승인, 접근 단말 지정, 접근 허용범위 및 기간 설정, 강화된 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등 보호대책을 수립·이행하여야 한다.
		2.6.7	인터넷 접속 통제	인터넷을 통한 정보 유출, 악성코드 감염, 내부망 침투 등을 예방하기 위하여 주요 정보시스템, 주요 직무 수행 및 개인정보 취급 단말기 등에 대한 인터넷 접속 또는 서비스(P2P, 웹하드, 메신저 등)를 제한하는 등 인터넷 접속 통제 정책을 수립·이행하여야 한다.
2.7.	암호화 적용	2.7.1	암호정책 적용	개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고 개인정보 및 주요정보의 저장·전송·전달 시 암호화를 적용하여야 한다.
		2.7.2	암호키 관리	암호키의 안전한 생성·이용·보관·배포·파기를 위한 관리 절차를 수립·이행하고, 필요 시 복구방안을 마련하여야 한다.
2.8.	정보시스템 도입 및 개발 보안	2.8.1	보안 요구사항 정의	정보시스템의 도입·개발·변경 시 정보보호 및 개인정보 보호 관련 법적 요구사항, 최신 보안취약점, 안전한 코딩 방법 등 보안 요구사항을 정의하고 적용하여야 한다.
		2.8.2	보안 요구사항 검토 및 시험	사전 정의된 보안 요구사항에 따라 정보시스템이 도입 또는 구현되었는지를 검토하기 위하여 법적 요구사항 준수, 최신 보안취약점 점검, 안전한 코딩 구현, 개인정보 영향 평가 등의 검토 기준과 절차를 수립·이행하고, 발견된 문제점에 대한 개선조치를 수행하여야 한다.

		2.8.3	시험과 운영 환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소시키기 위하여 원칙적으로 분리하여야 한다.
		2.8.4	시험 데이터 보안	시스템 시험 과정에서 운영데이터의 유출을 예방하기 위하여 시험 데이터의 생성과 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립·이행하여야 한다.
		2.8.5	소스 프로그램 관리	소스 프로그램은 인가된 사용자만이 접근할 수 있도록 관리하고, 운영환경에 보관하지 않는 것을 원칙으로 하여야 한다.
		2.8.6	운영환경 이관	신규 도입·개발 또는 변경된 시스템을 운영환경으로 이관할 때는 통제된 절차를 따라야 하고, 실행코드는 시험 및 사용자 인수 절차에 따라 실행되어야 한다.
2.9.	시스템 및 서비스 운영관리	2.9.1	변경관리	정보시스템 관련 자산의 모든 변경내역을 관리할 수 있도록 절차를 수립·이행하고, 변경 전 시스템의 성능 및 보안에 미치는 영향을 분석하여야 한다.
		2.9.2	성능 및 장애 관리	정보시스템의 가용성 보장을 위하여 성능 및 용량 요구사항을 정의하고 현황을 지속적으로 모니터링하여야 하며, 장애 발생 시 효과적으로 대응하기 위한 탐지·기록·분석·복구·보고 등의 절차를 수립·관리하여야 한다.
		2.9.3	백업 및 복구관리	정보시스템의 가용성과 데이터 무결성을 유지하기 위하여 백업 대상, 주기, 방법, 보관장소, 보관기간, 소산 등의 절차를 수립·이행하여야 한다. 아울러 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다.
		2.9.4	로그 및 접속기록 관리	서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 사용자 접속기록, 시스템로그, 권한부여 내역 등의 로그유형, 보존기간, 보존방법 등을 정하고 위·변조, 도난, 분실 되지 않도록 안전하게 보존·관리하여야 한다.
		2.9.5	로그 및 접속기록 점검	정보시스템의 정상적인 사용을 보장하고 사용자 오·남용(비인가접속, 과다조회 등)을 방지하기 위하여 접근 및 사용에 대한 로그 검토기준을 수립하여 주기적으로 점검하며, 문제 발생 시 사후조치를 적시에 수행하여야 한다.
		2.9.6	시간 동기화	로그 및 접속기록의 정확성을 보장하고 신뢰성 있는 로그 분석을 위하여 관련 정보시스템의 시각을 표준시각으로 동기화하고 주기적으로 관리하여야 한다.
		2.9.7	정보자산의 재사용 및 폐기	정보자산의 재사용과 폐기 과정에서 개인정보 및 중요정보가 복구·재생되지 않도록 안전한 재사용 및 폐기 절차를 수립·이행하여야 한다.
2.10	시스템 및 서비스 보안관리	2.10.1	보안시스템 운영	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립·이행하고 보안시스템별 정책적용 현황을 관리하여야 한다.
		2.10.2	클라우드 보안	클라우드 서비스 이용 시 서비스 유형(SaaS, PaaS, IaaS 등)에 따른 비인가 접근, 설정 오류 등에 따라 중요정보와 개인정보가 유·노출되지 않도록 관리자 접근 및 보안 설정 등에 대한 보호대책을 수립·이행하여야 한다.

		2.10.3	공개서버 보안	외부 네트워크에 공개되는 서버의 경우 내부 네트워크와 분리하고 취약점 점검, 접근통제, 인증, 정보 수집·저장·공개 절차 등 강화된 보호대책을 수립·이행하여야 한다.
		2.10.4	전자거래 및 핀테크 보안	전자거래 및 핀테크 서비스 제공 시 정보유출이나 데이터 조작·사기 등의 침해사고 예방을 위해 인증·암호화 등의 보호대책을 수립하고, 결제시스템 등 외부 시스템과 연계할 경우 안전성을 점검하여야 한다.
		2.10.5	정보전송 보안	타 조직에 개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립하고 조직 간 합의를 통해 관리 책임, 전송방법, 개인정보 및 중요정보 보호를 위한 기술적 보호조치 등을 협약하고 이행하여야 한다.
		2.10.6	업무용 단말기기 보안	PC, 모바일 기기 등 단말기기를 업무 목적으로 네트워크에 연결할 경우 기기 인증 및 승인, 접근 범위, 기기 보안설정 등의 접근통제 대책을 수립하고 주기적으로 점검하여야 한다.
		2.10.7	보조저장매체 관리	보조저장매체를 통하여 개인정보 또는 중요정보의 유출이 발생하거나 악성코드가 감염되지 않도록 관리 절차를 수립·이행하고, 개인정보 또는 중요정보가 포함된 보조저장매체는 안전한 장소에 보관하여야 한다.
		2.10.8	패치관리	소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인한 침해사고를 예방하기 위하여 최신 패치를 적용하여야 한다. 다만 서비스 영향을 검토하여 최신 패치 적용이 어려울 경우 별도의 보완대책을 마련하여 이행하여야 한다.
		2.10.9	악성코드 통제	바이러스·웬·트로이목마·랜섬웨어 등의 악성코드로부터 개인정보 및 중요정보, 정보시스템 및 업무용 단말기 등을 보호하기 위하여 악성코드 예방·탐지·대응 등의 보호대책을 수립·이행하여야 한다.
		2.11.1	사고 예방 및 대응체계 구축	침해사고 및 개인정보 유출 등을 예방하고 사고 발생 시 신속하고 효과적으로 대응할 수 있도록 내·외부 침해시도의 탐지·대응·분석 및 공유를 위한 체계와 절차를 수립하고, 관련 외부기관 및 전문가들과 협조체계를 구축하여야 한다.
		2.11.2	취약점 점검 및 조치	정보시스템의 취약점이 노출되어 있는지를 확인하기 위하여 정기적으로 취약점 점검을 수행하고 발견된 취약점에 대해서는 신속하게 조치하여야 한다. 또한 최신 보안취약점의 발생 여부를 지속적으로 파악하고 정보시스템에 미치는 영향을 분석하여 조치하여야 한다.
2.11.	사고 예방 및 대응	2.11.3	이상행위 분석 및 모니터링	내·외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등을 신속하게 탐지·대응할 수 있도록 네트워크 및 데이터 흐름 등을 수집하여 분석하며, 모니터링 및 점검 결과에 따른 사후조치는 적시에 이루어져야 한다.
		2.11.4	사고 대응 훈련 및 개선	침해사고 및 개인정보 유출사고 대응 절차를 임직원과 이해관계자가 숙지하도록 시나리오에 따른 모의훈련을 연 1회 이상 실시하고 훈련결과를 반영하여 대응체계를 개선하여야 한다.
		2.11.5	사고 대응 및 복구	침해사고 및 개인정보 유출 징후나 발생을 인지한 때에는 법적 통지 및 신고 의무를 준수하여야 하며, 절차에 따라 신속하게 대응 및 복구하고 사고분석 후 재발방지 대책을 수립하여 대응체계에 반영하여야 한다.

2.12.	재해복구	2.12.1	재해·재난 대비 안전조치	자연재해, 통신·전력 장애, 해킹 등 조직의 핵심 서비스 및 시스템의 운영 연속성을 위협할 수 있는 재해 유형을 식별하고 유형별 예상 피해규모 및 영향을 분석하여야 한다. 또한 복구 목표시간, 복구 목표시점을 정의하고 복구 전략 및 대책, 비상시 복구 조직, 비상연락체계, 복구 절차 등 재해 복구체계를 구축하여야 한다.
		2.12.2	재해 복구 시험 및 개선	재해 복구 전략 및 대책의 적정성을 정기적으로 시험하여 시험결과, 정보시스템 환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완하여야 한다.