[시행 2026. 4. 3.] [소방청 훈령 제461호] [발령 2026. 4. 3.]

소방청 정보보안업무 규정

제1장 총 칙

제1조(목적) 이 규정은 「국가정보원법」과「보안업무규정」, 「국가 정보보안 기본지침」, 「전자정부법」과 같은 법 시행령, 「국가사이버안전관리규정」에 따라 소방청 정보통신 보안업무수행에 필요한 세부사항을 규정함을 목적으로 한다.

제2조(적용범위) 이 규정은 소방청과 그 소속·산하기관에 적용한다.

제3조(용어의 정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

1. "각급기관"이란 소방청과 그 소속·산하기관을 말한다.
2. "각급부서"란 각급기관의 각 부서를 말한다.
3. "개별사용자"란 각급기관의 장으로부터 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 공무원 등을 말한다.
4. "정보보안담당관"이라 함은 정보보안업무를 총괄하기 위하여 소방청장이 지정한 사람을 말한다.
5. "RFID(Radio Frequency Identification) 시스템"이란 대상이 되는 사물 등에 RFID 태그를 부착하고 전파를 사용, 해당 사물 등의 식별정보 및 주변 환경정보를 인식하여 각 사물 등의 정보를 수집·저장·가공 및 활용하는 시스템을 말한다.
6. "정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통

신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집・가공・저장・검색・송수신하는 정보통신체제를 말한다.

7. "정보통신실"이란 서버・스위치・라우터・교환기 등 전산 및 통신장비 등이 설치・운용되는 장소 또는 전산실・통신실・데이터센터 등을 말한다.

8. "정보시스템"이란 정보의 수집・가공・저장・검색・송신・수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 말한다.

9. "정보화사업"이란 「전자정부법」 제2조의 규정에 따른 정보통신망 또는 정보시스템을 개발・구축・운용・유지보수하거나 정보시스템 감리, 전자정부사업관리의 위탁 등을 하기 위한 사업을 말한다.

10. "정보보안" 또는 "정보보호"란 정보시스템 및 정보통신망을 통해 수집・가공・저장・검색・송수신되는 정보의 유출・위조・변조・훼손 등을 방지하기 위하여 관리적・물리적・기술적 수단을 강구하는 일체의 행위로서「국가사이버안전관리규정」제2조제3호의 사이버안전을 포함한다.

11. "정보보호시스템"이란 정보의 수집, 가공, 저장, 검색, 송신, 수신 중 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적・기술적 수단을 말한다.

12. "기관 인터넷망"이라 함은 각급기관의 장이 소속 공무원등의 업무활용 또는 공개서버 운용을 주(主) 목적으로 인터넷과 연동하여 구

축한 정보통신망을 말한다.

13. "상용 인터넷망"이라 함은 각급기관의 장이 기관 인터넷망과 별개로 소속 공무원등이나 민원인 등의 보편적인 편의성을 위하여 인터넷에 연동하여 구축한 정보통신망을 말한다.

14. "내부망"이라 함은 각급기관의 장이 기관의 업무 수행을 위하여 인터넷과 별도로 분리하여 구축한 업무 전용(專用) 정보통신망을 말한다.

15. "휴대용 저장매체"란 디스켓·CD·외장형 하드디스크·USB 메모리 등 정보를 저장할 수 있는 것으로 PC 등의 정보시스템과 분리할 수 있는 기억장치를 말한다.

16. "업무자료"라 함은 다음 각 목의 어느 하나에 해당하는 것을 말한다.

가.「전자정부법」제2조제6호에 따른 행정정보 및 같은 법 제2조제7호에 따른 전자문서

나.「공공기록물 관리에 관한 법률 시행령」제2조제2호에 따른 전자기록물

다. 기타 다른 법령에 의하여 공무원등이 직무상 작성·취득하였거나 보유·관리하는 자료로서 전자적으로 처리되어 부호·문자·음성·음향·영상 등으로 표현된 것

17. "비밀"이라 함은 업무자료 중에서「보안업무규정」제4조에 따라 분류된 비밀을 말한다.

18. "대외비"라 함은 업무자료 중에서 「보안업무규정 시행규칙」 제16조제3항에 따라 분류된 대외비를 말한다.

19. 비공개 업무자료"라 함은 비밀 및 대외비를 제외한 업무자료 중에서 다음 각 목의 어느 하나에 해당하는 자료 또는 정보를 말한다.

가. 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따른 비공개 대상 정보

나. 국회 소속 공무원(「국회의원의 보좌직원과 수당 등에 관한 법률」 제2조에 따른 보좌직원을 포함한다) 또는 「지방자치법」 제30조에 따른 지방의회 소속 공무원의 직무상 요구에 따라 작성 또는 취득한 자료

다. 가목에 따른 비공개 대상 정보의 주요 내용이 기술된 문장 또는 문구

20. "공개 업무자료"라 함은 업무자료 중에서 비밀 및 대외비와 비공개 업무자료를 제외한 모든 자료 또는 정보를 말한다.

21. "암호자재"란 Ⅱ급비밀 이하의 통신내용 등의 정보를 보호할 목적으로 사용하는 문자・숫자・기호 등으로 구성된 환자표와 난수 또는 암호논리 등을 수록한 문서나 도구를 말한다.

22. "검증필 암호모듈"이라 함은 「전자정부법 시행령」 제69조와 「암호모듈 시험 및 검증지침」(행정안전부 고시)에 따라 국가정보원장이 안전성을 확인하여 제22조에 따른 목록에 등재한 상용 암호모듈을 말한다.

23. "대도청 측정"이란 유·무선 도청탐지장비 등을 이용하여 은닉된 무선도청장치 색출과 각종 도청 위해요소를 제거하는 제반활동을 말한다.

24. "고출력전자기파"(EMP)란 지상 30km 이상에서 핵 폭발에 의해 생성되는 고고도(高高度) 핵 전자파와 의도적으로 정보기기 등을 손상시키거나 오동작을 유발할 수 있는 고출력 비핵 전자파를 말한다.

25. "사이버공격"이란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스방해 등 전자적 수단에 의하여 정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 공격 행위를 말한다.

26. "보안관제"라 함은 사이버공격 정보를 실시간으로 탐지 및 분석, 대응하는 일련의 활동을 말한다.

27. "보안관제센터"라 함은 일정한 수준의 시설 및 장비와 이를 운영하기 위한 전문 또는 전담인력을 갖추고 보안관제업무를 수행하는 조직을 말한다.

제4조(책무) 각급기관의 장은 국가안보 및 국가이익 관련 정보(전자정보를 포함한다. 이하 같다)와 정보통신망을 보호하기 위한 보안대책을 수립·시행하여야 하며 정보보안에 대한 책임을 진다.

제5조(정보보안담당관) ① 소방청장은 정보보안업무를 효율적이고 체계적으로 수행하기 위하여 다음 각 호의 사람을 정보보안담당관으로 지정한다.

1. 소방청 : 정보통신과장

2. 중앙소방학교 : 교육지원과장

3. 중앙119구조본부 : 기획협력과장

4. 국립소방연구원 : 연구기획지원과장

5. 한국소방산업기술원 : IT고객부장

② 소방청 정보보안담당관은 각급기관의 정보보안업무를 총괄하며, 각급기관의 정보보안담당관은 다음 각 호의 업무를 수행한다.

1. 정보보안 정책·계획의 수립·시행 및 정보보안내규 제·개정

2. 정보보안 전담조직 관리, 전문인력 및 관련예산 확보

3. 정보화사업 보안성 검토 및 보안적합성 검증

4. 정보통신실, 정보통신망 현황자료 등에 관한 보안관리

5. 소관 주요정보통신기반시설 보호

6. 사이버공격 대응훈련 및 정보보안 관리실태 평가

7. 보안관제, 사고대응 및 정보협력 업무

8. 정보보안교육 총괄 및 '사이버보안진단의 날' 계획 수립·시행

9. 해당 기관 및 관할 하급기관에 대한 정보보안감사

10. 관할 하급기관의 정보보안업무 감독

11. 부서 분임정보보안담당관 업무 감독

12. 그 밖에 정보보안과 관련한 사항

③ 정보보안담당관은 효율적인 정보보안업무를 수행하기 위하여 전담인력을 확보·운영하여야 하며, 중요 정보보안업무에 대하여는 「소방청 보안업무 시행세칙」(이하 "보안업무 시행세칙"이라 한다) 제4조

에 따라 보안심사위원회의 심의를 거쳐 시행하여야 한다.

④ 각급기관의 장은 정보보안담당관이 직무를 효율적으로 수행할 수 있도록 각급 부서의 공무원 중에서 부서의 정보보안업무를 수행할 수 있는 적정인력을 분임정보보안담당관으로 임명하여야 한다. 별도로 임명하지 아니할 경우 각급 부서의 장을 분임정보보안담당관으로 임명한 것으로 본다.

제6조(연도 추진계획 수립) ① 소방청장은 매년 「연도 정보보안업무 추진계획」(「국가사이버안전관리규정」 제9조에 따른 사이버안전대책을 포함한다)을 수립·시행하여야 한다.

② 소방청장은 제1항에 의한 「연도 정보보안업무 추진계획」수립을 위하여 소속·산하기관의 장에게 연도 정보보안업무 추진계획의 제출을 요청할 수 있다.

제7조(정보보안 내규 제정) ① 소속·산하기관의 장은 해당 기관의 정보보안업무를 규정한 정보보안 내규(또는 지침·시행세칙 등)를 「국가정보보안 기본지침」 및 이 규정에 저촉되지 아니하는 범위 내에서 제정·시행할 수 있다.

② 소속·산하기관의 장은 제1항에 따라 정보보안 내규를 제정할 경우 소방청장과 사전 협의하여야 한다.

제8조(정보보안감사 등) ① 소방청장은 소방청 및 소속·산하기관의 정보보안업무 및 활동을 조사·점검하기 위하여 연 1회 이상 정보보안감사를 실시하여야 하며, 이를 위하여 필요한 경우 감사 또는 감찰업

무를 수행하는 부서에 협조를 요청할 수 있다.

② 소방청장은 정보보안감사 이외에 소방청 및 소속·산하기관에 대한 정보보안 지도방문을 실시할 수 있다.

③ 정보보안감사 또는 지도방문은 제도적인 문제점 발굴에 중점을 두고 실시하여야 하며 도출된 취약요인은 근본적인 대책을 수립하여 시행하여야 한다.

④ 소속·산하기관의 장은 제1항에 의한 감사와 별도로 자체 정보보안감사를 실시할 수 있으며, 소방청장에게 감사의 방향 및 중점사항, 감사관 지원 등 협조를 요청할 수 있다

⑤ 각급기관의 장은 정보보안 위규사항을 적발한 경우 「국가공무원 복무·징계 관련 예규」 (인사혁신처) 중 "비밀 엄수의 의무 위반 처리" 부분 및 국가정보원장이 배포한 「정보보안 사고(위규) 처리기준(안)」에 따른 조치를 하여야 한다. 다만, 정보보안 위규사항의 처리기준이 중징계 및 경징계에 해당하는 경우 산하기관은 자체징계기준에 따라 처리하고, 소방청 및 소속기관은 「소방공무원 징계령」에 따라 처분한다.

⑥ 정보보안감사를 실시할 경우에는 국가정보원에서 제공하는「정보보안감사 체크리스트」등을 적극 활용하여야 한다.

⑦ 소방청장은 정보보안감사 담당자를「국가 정보보안 기본지침」제8조제5항에 따라 우대하여야 한다.

제9조(정보보안 교육) ① 소방청장은 정보보안에 대한 경각심을 제고하

기 위하여 정보보안 교육계획을 수립하여 연 1회 이상 모든 소속 공무원을 대상으로 교육(온라인 교육을 포함한다)을 실시하여야 한다.

② 소방청장은 정보보안 교육의 실효성을 제고시키기 위하여 기관별 자체 실정에 맞는 정보보안 교안 및 교재를 작성·활용하여야 하며 필요시 국가정보원장에게 전문인력 및 자료 지원을 요청할 수 있다.

③ 소방청장은 정보보안담당관, 분임정보보안담당관, 정보보안 실무자가 최신 정보보안 정책 및 기술 등을 습득하기 위한 정보보안 관련 전문기관의 교육 및 학술회의 참가 등을 장려하여야 한다.

제10조(사이버보안진단의 날) ① 소방청장은 매월 셋째 수요일을 '사이버보안진단의 날'로 지정·운용하여야 한다.

② 정보보안담당관은 '사이버보안진단의 날'에 소관 정보통신망을 대상으로 악성코드 감염 여부와 정보통신시스템의 보안 취약 여부 등 종합적인 보안진단을 실시하여야 한다.

제11조(정보통신보안 규정 위반) ① 정보통신망을 통해 비인가자에게 누설하거나 위반할 경우 발생하는 정보통신보안 위규사항은 국가정보원 「보안업무규정 시행규칙」을 따른다.

② 각급기관 정보보안담당관은 정보통신보안 규정 위반 사항을 적발하였을 경우 소방청장(정보통신과장)에게 보고하여야 하며 국가안보 및 국가이익에 중대한 영향을 미칠 수 있다고 판단되는 정보보안 위규사항에 대해서는 가장 신속한 방법으로 국가정보원장에게 통보하여야 한다.

제2장 정보화사업 보안

제1절 사업 계획

제12조(보안책임) ① 정보통신망 또는 정보시스템을 개발·구축·운용·유지보수하는 사업(이하 "정보화사업"이라 한다)을 담당하는 부서의 장은 해당 정보화사업에 대한 보안관리를 수행하여야 한다.

② 정보화사업 부서의 장은 정보화사업에 대한 보안관리책임을 지고 관리·감독하여야 한다.

③ 각급기관의 정보보안담당관은 각종 정보화사업과 관련한 보안대책의 적절성을 평가하고 정보화사업 수행 전반에 대하여 보안대책의 이행 여부를 점검하여 필요한 경우 정보화사업 부서의 장에게 시정을 요구할 수 있다.

제13조(보안대책 수립) 정보화사업 부서의 장은 정보통신망 또는 정보시스템을 구축·운용하기 위한 정보화사업 계획을 수립할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 보안관리체계(조직, 인원 등) 구축 등 관리적 보안대책
2. 설치·운용장소 보안관리 등 물리적 보안대책
3. 정보통신망 또는 정보시스템의 구성요소별 기술적 보안대책
4. 국가정보원장이 개발하거나 안전성을 확인한 암호자재, 상용 암호모듈 및 정보보호시스템 도입·운용계획
5. 긴급사태 대비 및 재난복구 계획

6. 용역업체 작업장소에 대한 보안대책

7. 온라인 개발 또는 온라인 유지보수가 필요하다고 판단할 경우 제28조의2 또는 제52조에 따른 보안대책

8. 누출금지정보 보안관리 방안

제14조(제안요청서 기재사항) ① 정보화사업 부서의 장은 정보화사업을 발주하기 위하여 제안요청서를 작성할 경우 다음 각 호의 사항을 포함하여야 한다.

1. 용역업체 작업장소에 대한 보안요구사항

2. 온라인 개발 또는 온라인 유지보수가 필요하다고 판단할 경우 제28조의2 또는 제52조에 따른 보안 준수사항

3. 누출금지정보 목록

4. 용역업체가 누출정보를 제외한 소프트웨어 산출물을 제3자에게 제공하고자 할 경우 발주자 승인 절차

5. 연 1회 이상 정기적으로 보안 취약점 점검 실시 및 보안취약점 발견시 조치 후 결과 제출

② 제1항제3호에 따른 누출금지정보 목록을 작성할 경우 다음 각 호의 사항을 포함하여야 한다.

1. 해당 기관의 정보시스템 내·외 IP주소 현황

2. 정보시스템 구성 현황 및 정보통신망 구성도

3. 개별사용자의 계정·비밀번호 등 정보시스템 접근권한 정보

4. 정보통신망 또는 정보시스템 취약점 분석·결과물

5. 정보화사업 용역 결과물 및 관련 프로그램 소스코드(외부에 유출될 경우 국가안보 및 국익에 피해가 우려되는 중요 용역사업에 해당)

6. 암호자재 및 정보보호시스템 도입·운영 현황

7. 정보보호시스템 및 네트워크 장비 설정 정보

8. 「공공기관의 정보공개에 관한 법률」 제9조 제1항에 따라 비공개 대상 정보로 분류된 해당 기관의 내부문서

9. 「개인정보보호법」제2조제1호에 따른 개인정보

10. 「보안업무규정」 제4조에 따른 비밀 및 같은 규정 시행규칙 제16조제3항에 따른 대외비

11. 그 밖에 해당 기관의 장이 공개가 불가하다고 판단한 자료

제2절 보안성 검토

제15조(검토 시기 및 절차) ① 정보화사업 부서의 장은 정보화사업을 수행하고자 할 경우 자체 보안대책을 강구하고 안전성을 확인하기 위하여 사업 계획단계(사업 공고 전)에서 소방청 정보보안담당관을 경유하여 국가정보원장에게 보안성 검토를 의뢰하여야 한다. 다만, 국가정보원장이 정보화사업의 규모·중요도 등을 고려하여 소방청장에게 보안성 검토를 위임한 사항은 소방청장이 실시 할 수 있다.

② 정보통신망 보안성검토는 서면 검토를 원칙으로 하되 필요하다고 판단하는 경우에는 현장 확인을 실시할 수 있다.

제15조의2(보안성 검토대상) ① 제15조의 보안성 검토 대상 정보화 사업

은 다음 각 호와 같다.

1. 비밀·대외비를 유통·관리하기 위한 정보통신망 또는 정보시스템 구축
2. 국가정보원장이 개발하거나 안전성을 확인한 암호자재를 적용하는 정보통신망 또는 정보시스템 구축
3. 외교·국방 등 국가안보상 중요한 정보통신망 및 정보시스템의 구축
4. 100만명 이상의 개인에 대한 「개인정보보호법」상 민감정보 또는 고유식별정보를 처리하는 정보시스템 구축
5. 주요정보통신기반시설로 지정이 필요한 정보통신기반시설 구축
6. 제어시스템 도입
7. 재난관리·국민안전·치안유지·비상사태 대비 등 국가위기 관리와 관련한 정보통신망 또는 정보시스템 구축
8. 국가정보통신망 등 여러 기관이 공동으로 활용하기 위한 정보통신망 또는 정보시스템 구축
9. 행정정보, 국가지리, 환경정보 등 국가 차원의 주요 데이터베이스 구축
10. 정상회의, 국가지리, 환경정보 등 국가 차원의 주요 데이터베이스 구축
11. 내부망 또는 폐쇄망을 인터넷 또는 다른 정보통신망과 연동하는 사업

12. 내부망과 기관 인터넷망을 분리하는 사업

13. 통합데이터센터·보안관제센터 구축

14. 소속 공무원등이 업무상 목적으로 이용하도록 하기 위한 무선랜, 이동통신망(HSDPA, WCDMA, LTE, 5G 등) 구축

15. 원격근무시스템 구축

16. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제20조에 따라 클라우드 컴퓨팅 서비스제공자의 클라우드컴퓨팅서비스(이하"민간 클라우드컴퓨팅서비스"라 한다)를 이용하는 사업

17. 남북 회담 및 협력사업 등을 위한 북한지역 내 정보통신망 또는 정보시스템 구축

18. 외국에 개설하는 사무소 운영을 위한 정보통신망 또는 정보시스템 구축

19. 첨단 정보통신기술을 활용하는 정보화사업으로서 국가정보원장이 해당 기술에 대하여 안전성 확인이 필요하다고 지정하는 사업

② 소방청 정보보안담당관은 다음 각 호에 해당하는 정보화사업에 대하여 자체 보안성 검토를 실시한다.

1. 제15조 제1항에 따라 국가정보원장으로부터 보안성 검토를 위임받은 사업

2. 홈페이지 및 웹메일 등 웹기반 정보시스템 구축

3. 인터넷전화시스템 구축

4. 다른 기관의 정보통신망 또는 정보시스템과 분리된 외부인 전용 무

선랜, 인터넷망 및 교육장 정보통신망 등 구축

5. 해당 기관의 정보통신망 또는 정보시스템과 분리된 외부인 전용 무선랜, 인터넷망 및 교육장 정보통신망 등 구축

6. 인터넷과 분리된 소속 공무원등의 인사·복지관리 등의 목적을 위한 정보시스템 구축

7. 주요정보통신기반시설 취약점 분석·평가, 정보보안컨설팅 등 용역사업

8. 기존 분리된 내부망·기관 인터넷망간 자료전송시스템 구축 등 후속사업

9. 대규모 백업·재해복구센터 구축

10. 해당 기관의 정보통신망 또는 정보시스템과 분리된 영상회의시스템 구축

11. 인터넷과 분리된 CCTV 등 영상정보처리기기 구축

12. 백업시스템 구축

13. 대민 콜센터시스템 구축

14. 그 밖의 소방청장이 필요하다고 판단하는 정보통신망 또는 정보시스템 구축

제16조(검토 생략) ① 정보화사업 부서의 장은 다음 각 호에 해당하는 정보화사업에 대하여는 보안성 검토 절차의 이행을 생략할 수 있다. 이 경우 정보화사업 각급부서의 장은 관련 매뉴얼·가이드라인 등을 준수하는 등 자체 보안대책을 수립·시행하여야 한다.

1. 제15조의2제1항 및 제2항 각 호의 정보화사업에 해당하지 아니하는 단순장비·물품 도입

2. 제15조에 따른 보안성 검토를 거쳐 완료한 정보화사업에 대하여 정보통신망 구성을 변경하지 아니하는 범위 내에서 다음 각 목의 사항을 포함한 후속 운영·유지보수·컨설팅(단일회선의 이중화는 제외한다)

가. 서버·스토리지·네트워크장비 등 장비 노후화로 인한 단순 장비 교체

나. 전화기·무전기·CCTV 등 통신·영상기기의 노후화로 인한 단순 장비 교체

다. 기존 운용하던 정보보호시스템을 동일한 보안기능을 보유한 다른 정보보호시스템으로 교체

3. 다년도에 걸쳐 계속하는 사업으로써 사업 착수 당시 보안성검토를 완료한 후 사업 내용의 변동 없이 계속 추진하는 운영·유지사업

4. PC·프린터 및 상용 소프트웨어 등 단순 제품 교체

② 정보화사업 부서의 장은 제1항제2호부터 제4호까지에 해당하는 정보화사업을 수행할 경우 기존 보안성 검토 결과를 준수하여야 한다.

제17조(제출 문서) 정보화사업 부서의 장은 정보화사업의 보안성검토를 요청할 경우에는 다음 각 호의 문서를 제출하여야 한다.

1. 사업계획서(사업목적 및 추진계획 포함)

2. 기술제안요청서(RFP)

3. 정보통신망 구성도(IP주소체계 포함)

4. 자체 보안대책 강구사항

제18조(검토결과 조치) ① 정보화사업 부서의 장은 보안성 검토결과를 통보받은 경우 검토 결과를 반영하여 보안대책을 보완하여야 한다.

② 소방청 정보보안담당관은 보안성검토 결과를 통보한 경우 그 반영 여부를 확인하기 위하여 현장점검을 실시할 수 있다.

제19조(현황 제출) 각급기관의 장은 전년도에 실시한 정보화사업에 대한 보안성검토 현황을 매년 1월 20일까지 소방청 정보보안담당관에게 제출하여야 한다.

제3절 사업 수행

제20조(정보통신제품 도입요건) ① 정보화사업 부서의 장은 정보 및 정보통신망 등을 보호하기 위하여 보안기능이 있는 다음 각 호의 정보통신제품을 도입할 수 있다.

1. 국가정보보안 기본지침 제21조에 따른 안전성 검증필 제품 목록에 등재되어 있는 제품

2. 비밀이 아닌 업무자료의 암·복호화를 목적으로 한 경우 암호가 주 기능인 제품 도입요건을 만족하는 제품

3. 제1호 및 제2호에 해당하지 않는 정보통신제품 중에서 국가정보원장이 별도로 공지하는 도입요건을 만족하는 제품

② 제1항제3호에 해당하는 제품은 실제 적용·운용 이전에 제15조에

따른 보안적합성 검증을 받아야 한다.

제21조 삭제

제22조 삭제

제23조(영상정보처리기기 도입 시 고려사항) 정보화사업 부서의 장은 영상정보처리기기를 도입·운용하고자 할 경우 한국정보통신기술협회(TTA)의 공공기관용 보안성능이 확인된 제품을 우선적으로 도입할 수 있다.

제24조 삭제

제25조(계약 특수조건) ① 각급기관의 장은 「국가를 당사자로 하는 계약에 관한 법률 시행령」 제76조제2항제3호다목에 따른 정보통신망 또는 정보시스템 구축 및 유지보수 등의 계약 이행과정에서 정보통신망 또는 정보시스템에 허가 없이 접속하거나 무단으로 정보를 수집할 수 있는 비인가 프로그램을 설치하거나 그러한 행위에 악용될 수 있는 정보통신망 또는 정보시스템의 약점을 고의로 생성 또는 방치하는 행위 등을 금지하는 내용의 계약 특수조건을 계약서에 명시하여야 하며, 계약기간(하자 보증기간 포함) 내에 발생한 보안약점 등에 대해서는 계약업체가 개선 조치하도록 하여야 한다.

② 각급기관의 장은 필요한 경우 계약업체로부터 제1항과 관련한 행위가 없다는 대표자 명의의 확약서를 요구할 수 있다.

제26조(용역업체 보안) ① 정보화사업 부서의 장은 용역업체에 정보화사업을 발주할 경우 다음 각 호의 보안사항을 준수하도록 계약서 또는

과업지시서에 명시하여야 한다.

1. 제14조제1항 각 호에 따른 제안요청에서 포함된 사항과 제28조에 따른 원격지 개발, 제28조의2에 따른 원격지에서의 온라인 개발, 제52조에 따른 온라인 유지보수를 허용할 경우 보안 준수사항
2. 소프트웨어 개발보안에 필요한 사항
3. 사업 참여인원의 보안관련 준수사항과 위반할 경우 손해배상 책임에 관한 사항
4. 사업 수행과 관련한 보안교육, 보안점검 및 사업기간 중 참여인원 임의 교체 금지
5. 정보통신망 구성도·IP주소 현황 등 업체에 제공하는 자료는 자료 인계인수대장을 비치하여 보안조치 후 인계·인수하고 무단 복사 및 외부반출 금지
6. 정보시스템의 IP가 포함된 최신 구성도 갱신·유지
7. 업체의 노트북·휴대용 저장매체 등 관련 장비는 반·출입 시 악성코드 감염 여부, 누출 금지정보 무단 반출 여부 등 점검
8. 사업 종료 시 업체의 노트북·휴대용 저장매체 등 관련 장비는 저장자료 복구가 불가하도록 완전 삭제
9. 사업 종료 시 누출금지정보 전량 회수
10. 연 1회 이상 정기적으로 보안취약점 점검실시 및 보안취약점 발견 시 조치 후 결과 통보
11. 소방청 정보보안담당관의 정보시스템 보안취약점 점검 시 협조 및

보안취약점 발견 시 보안대책 사항

12. 소방청 보안 관련 규정 준수 의무

13. 그 밖에 소방청 정보보안담당관이 보안 관리가 필요하다고 판단하는 사항 또는 국가정보원장이 보안조치를 권고하는 사항

② 정보화사업 부서의 장은 비밀 및 중요 용역사업을 수행할 경우 용역업체 참여 인원이 다음 각 호에 해당되는 사실을 알게 된 경우 교체를 요구하여야 한다.

1. 「국가공무원법」 제33조제3호부터 제6의4호까지에 해당하는 사람

2. 「국가를 당사자로 하는 계약에 관한 법률」 제27조제1항 각 호의 행위를 한 사람

③ 정보화사업 부서의 장은 다음 각 호에 따른 보안 준수사항의 이행 여부를 정기 또는 수시로 점검(불시 점검을 포함한다)하고 미비점을 발견한 경우 용역업체가 시정하도록 조치하여야 한다. 이 경우 정보화사업담당자가 점검한 후 그 결과를 정보보안담당관에게 통보하여야 한다.

1. 제1항에 따라 계약서에 명시된 보안 준수사항

2. 제27조의2에 따른 발주기관내 작업장소 보안 준수사항

3. 제28조에 따른 원격지 개발 보안 및 제28조의2에 따른 원격지에서의 온라인 개발시 보안 준수사항

4. 제51조에 따른 정보시스템 유지보수 및 제52조에 따른 온라인 유지보수시 보안 준수사항

④ 소방청장은 각급기관에 대하여 용역업체 보안관리 실태 점검을 실시할 수 있으며, 필요한 경우 국가정보원장에게 지원을 요청할 수 있다.

⑤ 각급기관의 장은 제3항 및 제4항에 따른 점검 결과 용역업체 보안대책 준수가 미흡하고 시정조치가 어렵다고 판단할 경우 제28조에 따른 원격지 개발, 제28조의2에 따른 원격지에서의 온라인 개발 또는 제52조에 따른 온라인 유지보수 허가를 취소할 수 있다.

⑥ 각급기관의 장은 제28조의2에 따른 원격지에서의 온라인 개발, 제52조에 따른 온라인 유지보수를 허용하고자 할 경우에는 용역업체의 온라인 접속을 통제하기 위한 온라인 용역 통제시스템을 구축·운영하여야 한다.

⑦ 각급기관의 정보보안담당관은 용역업체의 보안규정 위반 시 확인서 징구, 보안교육 실시, 보안 위약금 부과, 용역업체 대표자에게 재발방지 대책 마련, 용역업체 직원의 교체를 요구할 수 있다.

⑧ 그 밖에 용역업체 보안과 관련한 사항은 「국가·공공기관 용역업체 보안관리 가이드라인」을 준수하여야 한다.

제27조(소프트웨어 개발보안) 정보화사업 부서의 장은 정보시스템을 개발할 경우 「전자정부법」 제45조제3항에 따라 규정된 「행정기관 및 공공기관 정보시스템 구축·운영 지침」(행정안전부 고시) 제50조부터 제53조까지에 따라 보안약점이 발생하지 아니하도록 개발(이하 "소프트웨어 개발보안"이라 한다)하고 정보시스템 감리 등을 통해 보

안약점을 진단하여야 한다.

제27조의2(발주기관내 작업장소 보안) ① 각급기관의 장은 발주기관내(기관장이 임차한 외부 사무실을 포함한다) 용역업체 작업장소를 설치할 경우 보안 통제가 가능한 공간을 마련, 운영하여야 한다.

② 발주기관내 용역업체 작업장소에 설치 운영하는 정보통신망은 발주기관의 정보통신망과 분리 구성하여야 한다. 다만, 용역업체가 사업수행을 위하여 발주기관 정보시스템 이용이 불가피할 경우에는 필요한 정보시스템에 한해 지정된 단말기로부터의 제한적 접근을 허용하는 등 보안대책을 수립·시행하여야 하며, 이 경우 내부망 정보시스템에 대한 접근 허용에 관하여는 소방청 정보보안담당관을 거쳐 국가정보원장과 사전 협의하여야 한다.

③ 작업장소내 정보시스템은 용역사업 수행을 위해 필요한 경우 해당 정보화사업담당자의 보안통제하에 인터넷에 연결할 수 있다. 다만, 제2항 단서에 따른 발주기관 정보시스템 접근용 단말기의 경우에는 인터넷 연결을 금지한다.

④ 각급기관의 장은 용역업체가 발주기관 내 작업장소에서 개발 작업을 수행하더라도 개발용 서버가 민간 클라우드컴퓨팅서비스를 이용하는 등으로 원격지에 위치할 경우 원격지 개발로 간주하고 제1항에 따른 보안대책을 수립·시행하여야 한다.

제28조(원격지 개발보안) ① 정보화사업 부서의 장은 용역업체가 발주기관 이외 장소(이하 "원격지"라 한다)에서 개발 작업(유지보수 제외)을

수행하고자 요청할 경우 제14조제1항제1호에 따른 용역업체 작업장소에 대한 보안 요구사항 등을 포함한 관리적·기술적 보안대책을 수립·시행하여야 한다. 이 경우 정보화사업 부서의 장은 보안대책을 수립한 후 각급기관의 정보보안담당관의 승인을 받아야 한다.

② 원격지내 정보시스템은 개발 작업을 위하여 필요한 경우 해당 정보화사업 부서의 장의 보안통제하에 인터넷에 연결할 수 있다.

제28조의2(원격지에서의 온라인 개발) 제28조에 따른 원격지 개발에서 각급기관의 장이 필요하다고 판단하고 용역업체가 다음 각 호에 따른 보안대책에 서면으로 동의하는 경우에 한하여, 각급기관의 장은 용역업체에게 원격지에서 인터넷을 통해 발주기관 정보시스템에 온라인 접속한 상태의 개발 작업을 허용할 수 있다.

1. 지정된 단말기에서만 접속 및 해당 단말기에 대한 접근인원 통제
2. 지정 단말기는 제3호에 따른 온라인 용역 통제시스템 접속 전용(專用)으로 운용하고 다른 목적의 인터넷 접속은 차단
3. 발주기관내 설치된 온라인 용역 통제시스템을 경유하여 개발에 필요한 정보시스템에 접속하는 등 소통구간 보호·통제
4. 접속사실이 기록된 로그기록을 1년 이상 보관
5. 계약 시행일로부터 종료 후 30일이 경과하는 날까지의 기간 중에 발주기관, 발주기관의 상급기관 및 국가정보원장의 정기 또는 수시 보안점검(불시 점검을 포함한다) 수검
6. 기타 국가정보원장이 배포한 「국가·공공기관 용역업체 보안관리

가이드라인」에서 제시된 온라인 개발에 관련된 보안대책의 준수

제29조(소프트웨어 산출물 제공) ① 정보화사업 부서의 장은 용역업체가 「용역계약일반조건」(기획재정부 계약예규) 제56조에 따른 지식재산권을 행사하기 위하여 소프트웨어 산출물의 반출을 요청할 경우 제안요청서 또는 계약서에 명시된 누출금지 정보에 해당하지 아니하면 제공하여야 한다.

② 정보화사업 부서의 장은 제1항에 따라 소프트웨어 산출물을 용역업체에 제공할 경우 업체의 노트북·휴대용 저장매체 등 관련 장비에 저장 되어있는 누출금지 정보를 완전삭제하여야 하며 업체로부터 누출금지 정보가 완전삭제되었다는 대표자 명의의 확약서를 받아야 한다.

③ 정보화사업 부서의 장은 용역업체가 소프트웨어 산출물을 제3자에게 제공하고자 할 경우 제공하기 이전에 승인을 받도록 하여야 한다.

④ 그 밖에 소프트웨어 산출물 제공과 관련한 사항은 「소프트웨어사업 계약 및 관리감독에 관한 지침」(과학기술정보통신부 고시)을 준수하여야 한다.

제30조(누출금지 정보 유출 시 조치) ① 정보화사업 부서의 장은 용역업체가 제안요청서 또는 계약서에 명시된 누출금지 정보를 유출한 사실을 알게 된 경우 업체를 대상으로 계약 위반에 따른 조치를 취하여야 한다. 이 경우 용역업체의 누출금지 정보 유출 사실을 알게 된 정보화사업 부서의 장 또는 사업과 관계된 공무원 등은 즉시 각급기관의 정

보보안담당관을 거쳐 소속 기관의 장에게 보고하여야 한다.

② 제1항에 따라 용역업체의 누출금지 정보 유출 사실을 알게 되거나 보고를 받은 각급기관의 장은 그 사실을 소방청 정보보안담당관에게 통보하여야 하고 직접 또는 소방청 정보보안담당관을 통하여 「국가를 당사자로 하는 계약에 관한 법률 시행령」 제76조 및「지방자치단체를 당사자로 하는 계약에 관한 법률 시행령」 제92조에 따라 입찰참가자격 제한 등 조치를 하여야 한다.

제4절 보안적합성 검증

제31조(검증대상 제품) 정보화사업 부서의 장은 제20조제1항제3호에 따른 보안기능이 있는 정보통신제품을 도입한 경우 실제 적용·운용 이전에 안전성을 확인하기 위하여 보안적합성 검증을 받아야 한다.

제32조(검증 기관 및 신청) ① 각급기관의 장은 제31조에 따른 보안적합성 검증을 받고자 할 경우 다음 각 호의 기관(이하 "검증기관"이라 한다)의 장에게 검증을 신청하여야 한다.

1. 소방청 : 국가정보원

2. 소속기관 및 산하기관 : 소방청

② 제1항제2호에도 불구하고 소속기관 및 산하기관의 장은 필요하다고 판단하는 경우 소방청장과 협의하여 자체적으로 검증을 실시할 수 있다.

제33조(검증 신청시 제출물) ① 정보화사업 부서의 장은 제32조제1항에

따라 보안적합성 검증을 신청할 경우 검증기관의 장에게 보안적합성 검증 신청시 제출물에 해당하는 문서 등을 제출하여야 한다.

② 제1항에 따라 검증을 신청한 기관의 장은 검증기관의 장이 필요하다고 판단하여 추가 자료를 요청할 경우 이를 제출하여야 한다.

제34조(안정성 검증) ① 소방청 정보보안담당관은 제33조에 따라 제출된 문서 내용의 적절성을 검토한 후 검증대상 제품에 대하여 보안기능의 정상 동작여부 등 안전성을 시험한다. 이 경우 검증기관의 장은 시험에 필요한 사항을 추가로 요청할 수 있다.

② 소방청장은 제1항에 따른 안전성 시험 등 관련 업무를 시험기관에게 의뢰할 수 있다.

③ 소방청장은 검증대상 제품의 제출 지연 등의 사유로 시험을 진행할 수 없을 경우 검증 절차를 중단할 수 있다.

제35조(검증시험 및 결과조치) ① 소방청 정보보안담당관은 제34조에 따른 시험 결과를 토대로 제품의 안전성을 종합 검토한 검증결과를 검증신청 기관의 장에게 통보하여야 한다.

② 제1항에 따라 검증결과를 통보받은 각급부서장은 해당조치를 실시하고 그 결과를 소방청 정보보안담당관에게 통보하여야 한다.

제36조(도입현황 제출) 정보화시스템 운영부서의 장은 제31조에 따른 정보통신제품을 도입 시 정보통신제품 도입 확인서를 작성하여 즉시 소방청장에게 제출하여야 하며, 소방청장은 각급기관에서 도입한 정보통신제품 현황을 분기말에 국가정보원장에게 제출하여야 한다.

제37조(형상변경 및 용도변경 시 조치) 정보화사업 부서의 장은 보안적합성 검증이 완료된 시스템의 형상 변경이 필요하거나 도입 목적 이외의 용도로 운용이 필요한 경우 소방청 정보통신과장에게 재검증 신청 등의 조치를 취하여야 한다.

제3장 정보통신망 및 정보시스템 보안

제1절 정보통신망 보안

제38조(내부망·인터넷망 분리 운영) ① 각급기관의 장은 내부망과 인터넷망을 분리·운영하여야 한다.

② 제1항의 내부망과 인터넷망을 분리·운영할 경우 다음 각 호의 사항을 포함하여 보안대책을 수립·시행하여야 한다.

1. 침입차단·탐지시스템 설치 등 비인가자 침입 차단대책
2. 네트워크 접근관리시스템 설치 등 비인가 장비의 내부망 접속 차단대책
3. 내부망 정보시스템의 인터넷 접속 차단대책
4. 내부망과 기관 인터넷망간 안전한 자료전송 대책
5. 그 밖의 국가정보원장이 배포한 「국가·공공기관 업무전산망 분리 및 자료 전송보안가이드라인」에서 제시하는 보안대책

③ 각급기관의 장은 정보시스템에 부여되는 IP주소를 체계적으로 관리하여야 하며 비인가자로부터 내부망을 보호하기 위하여 네트워크주소변환기(NAT)를 이용하여 사설 IP주소체계를 구축·운영하여야 한

다. 또한 IP주소별로 정보시스템 접속을 통제하여 비인가 기기에 의한 내부망 접속을 차단하여야 한다.

④ 각급기관의 장은 분리된 내부망과 기관 인터넷망간 자료전송을 위한 접점이 불가피한 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 침입차단·탐지시스템 설치·운용
2. 내부망과 기관 인터넷망간 접점 최소화
3. 내부망과 기관 인터넷망간 일방향 전송장비 등을 이용한 자료전송 체계를 구축·운영하고 원본파일은 3개월 이상, 전송기록은 6개월 이상 유지
4. 정기적으로 전송실패 기록을 확인하고 악성코드 유입 여부 등 점검
5. 내·외부망 자료를 전송할 경우 자료전송시스템 이용

⑤ 각급기관의 장은 제1항에도 불구하고 예산 부족 등 사유로 부득이한 경우 소방청 정보통신과와 협의하여 내부망과 인터넷망을 분리하지 아니할 수 있다. 이 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 정보시스템 및 개별사용자 PC 영역 등에 대한 접근 통제대책
2. 인터넷 PC의 악성코드 감염 최소화를 위한 인터넷 사용 통제대책
3. 인터넷 PC의 악성코드 감염에 따른 내부망으로 피해확산 차단대책
4. 사이버공격 탐지·대응 등 안전한 업무환경을 위한 보호대책

⑥ 각급기관의 장은 내부망 및 인터넷망 IP주소 현황을 정기적으로 확

인하고 갱신하여야 한다.

제39조(보안·네트워크장비 보안) ① 각급기관의 장은 침입차단·탐지시스템, 스위치·라우터 등 기관 정보통신망 구성 또는 기관 정보보안 정책 전반에 영향을 미치는 보안·네트워크 장비를 설치·운영하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 물리적으로 안전한 장소에 설치하여 비인가자의 무단접근 통제
2. 콘솔에서 관리함을 원칙으로 하되, 다음 각 목의 경우 청사 내 지정 단말기로부터의 접속 관리 허용
   가. 장비 관리자의 접속
   나. 제27조의2에 따른 발주기관내 용역업체 작업장소에서의 접속
3. 최초 설치할 경우 디폴트 계정은 삭제하거나 변경 사용하고 장비 관리를 위한 관리자 계정을 별도로 생성·운영
4. 불필요한 서비스 포트와 개별사용자 계정은 차단 및 삭제
5. 펌웨어 무결성과 컴퓨터 운영체제·소프트웨어의 취약점 및 버전 업데이트 여부를 정기적으로 점검하고 최신 버전으로 제시

② 정보시스템 운영부서의 장은 정보보호시스템·네트워크장비의 로그기록을 1년 이상 유지하여야 하고 비인가자의 접속 여부를 정기적으로 점검하여 그 결과를 각급기관 정보보안담당관에게 통보하여야 한다.

③ 각급기관의 정보보안담당관은 제2항에서 통보받은 점검결과를 소

방청장에게 제출하여야 한다.

제40조(무선랜 보안) ① 각급기관의 장은 내부망을 제외한 정보통신망에서 다음 각 호의 경우와 같이 청사 내에 무선랜(WiFi)을 구축·운용할 수 있다.

1. 소방청 인터넷 중계기(AP)를 설치하여 제70조제1항에 따라 소방청에서 지급한 단말기의 접속만을 허용하는 업무용 무선랜
2. 상용 인터넷망에 중계기(AP)를 설치하여 제75조에 따라 반입한 공무원 등의 개인 소유 이동통신단말기의 접속만을 허용하는 무선랜
3. 상용 인터넷망에 중계기(AP)를 설치한 외부인 전용 무선랜

② 각급기관의 장은 제1항에 따라 무선랜을 구축·운용하고자 할 경우 국가정보원장이 배포한 「국가·공공기관의 무선랜 구축 및 RFID 보안가이드라인」을 준수하여 보안대책을 수립·시행하여야 한다.

③ 제2항에 따른 보안대책을 수립할 경우 제1항제1호 및 제2호에 따른 무선랜에 대하여는 다음 각 호의 사항을 포함하여야 한다.

1. 네트워크 이름(SSID) 브로드캐스팅(broadcasting) 금지
2. 추측이 어렵고 복잡한 네트워크 이름(SSID) 사용
3. WPA2 이상(256비트 이상)의 암호체계를 사용하여 소통자료 암호화
4. 비(非)인가 단말기의 무선랜 접속 차단 및 무선랜 이용 단말기를 식별하기 위한 IP주소 할당기록 등 유지
5. IEEE 802.1X, AAA(Authentication Authorization Accounting) 등

의 기술에 따라 상호 인증을 수행하는 무선랜 인증제품 사용

6. 무선침입방지시스템 설치 등 침입 차단대책

7. 기관의 내부망 정보시스템 또는 인접해 있는 다른 기관의 정보 시스템이 해당 무선랜에 접속되지 아니하도록 하는 기술적 보안대책

8. 그 밖에 무선랜 단말기·중계기(AP) 등 구성요소별 분실·탈취·훼손·오용 등에 대비한 관리적·물리적 보안대책

④ 각급기관의 정보보안담당관은 제1항 및 제2항과 관련한 보안대책의 적절성을 수시로 점검·보완하여야 한다.

제41조(이동통신망 보안) ① 정보화사업 부서의 장은 이동통신망(HSDPA·WCDMA·LTE·5G)을 이용하여 시스템을 구축하거나 중요자료를 소통하고자 할 경우 암호화 및 비인가 단말기의 이동통신망 접속 차단 장치 등 기술적 보안대책을 수립·시행하여야 한다.

② 제1항에 따라 이동통신망을 이용한 시스템을 구축·운용할 경우 해당 기관의 정보통신망과 혼용되지 않도록 하여야 한다.

제42조(영상회의 보안) ① 각급기관의 장은 영상회의를 실시하는 경우 행정안전부에서 제공하는 온나라 PC영상회의 시스템을 사용하여야 한다.

② 제1항에도 불구하고 영상회의시스템을 구축·운용하고자 할 경우 통신망(국가정보통신망·전용선·인터넷 등) 암호화 등 보안대책을 수립·시행하여야 한다.

③ 기타 영상회의 보안과 관련한 사항은 국가정보원장이 배포한「원

격업무 통합보안매뉴얼」을 준수하여야 한다.

제43조(인터넷전화 보안) ① 각급기관의 장은 인터넷전화시스템을 구축·운용하거나 민간 인터넷전화 사업자망을 이용하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 한국정보통신기술협회(TTA) verified ver4. 이상 보안규격으로 인증받은 행정기관용 인터넷전화시스템 설치·운용
2. 인터넷전화기에 대한 장치 및 사용자 인증
3. 제어신호 및 통화내용 등 데이터 암호화
4. 인터넷전화망과 다른 정보통신망과의 분리
5. 인터넷전화 전용 침입차단시스템 등 정보보호시스템 설치·운용
6. 백업체제 구축

② 민간 인터넷전화 사업망을 이용할 경우 해당 사업자로 하여금 서비스 제공 구간에 대한 보안대책을 수립하도록 하여야 한다.

③ 외교·국방 등 국가안보 관련 각급기관의 장은 인터넷전화시스템을 구축·운용하고자 할 경우 국가정보원장이 별도로 정한 암호기술 규격을 준수하여야 한다.

제44조(인터넷 사용 제한) ① 각급기관의 장은 국가비상사태 및 대형 재해·재난의 발생, 사이버공격 등으로부터 정보통신망과 정보시스템의 정상적인 운영을 보장하기 위하여 소속 공무원 등에 대한 인터넷 사용을 일부 또는 전부를 제한할 수 있다.

② 각급기관의 장은 기관 인터넷망의 효율적인 운영 관리 및 악성코드

유입차단을 위하여 게임・음란・도박 등 업무와 관련이 없는 인터넷 이용을 차단하여야 하며, 악성코드 유입 차단을 위하여 필요할 경우 제61조제4항에 따른 상용 정보통신서비스의 접속을 제한할 수 있다.

③ 제2항에도 불구하고 업무에 필요한 경우 각급부서의 장은 정보보안담당관에게 필요한 웹사이트의 접속허용을 요청할 수 있으며, 정보보안담당관은 접속허용 여부를 검토하여 접속을 허용할 수 있다.

제45조(재외사무소 정보보안점검) 각급기관의 장은 외국에 사무소를 개설・운용할 경우 소방청 정보보안담당관에게 해당 사무소의 정보통신망 및 정보시스템에 대한 보안관리 실태 점검을 요청하고 발견된 취약요인을 개선하여야 한다.

제2절 정보시스템 보안

제46조(정보시스템 보안책임) ① 정보시스템(PC・서버・네트워크장비・정보통신기기 등을 포함한다)을 도입・운용할 운영부서의 장은 해당 정보시스템에 대하여 관리자 및 관리책임자를 지정・운영하여야 한다.

② 정보시스템 운영부서의 장은 서버・네트워크장비 등 부서가 공동으로 사용하는 정보시스템의 운용・관리에 대한 보안책임을 진다.

③ 정보시스템 관리책임자는 정보시스템을 실제 운용하는 부서의 장이 되며 관리책임자는 정보시스템 관리대장을 수기 또는 전자적으로 작성・관리하여야 한다.

④ 정보시스템 관리책임자는 해당 부서의 정보시스템 관리대장에 정보시스템의 최종 변경 현황을 유지하여야 하며 사본 1부를 각 기관의 정보보안담당관에게 제출하여야 한다.

⑤ 각급기관의 정보보안담당관은 정보시스템 운용과 관련하여 보안취약점을 발견하거나 보안대책 수립이 필요하다고 판단하는 경우 개별 사용자, 정보시스템 운영부서의 장에게 개선 조치를 요구할 수 있으며 조치가 완료될 때까지 정보시스템의 운용을 일시 제한할 수 있다.

제47조(정보시스템 유지보수) ① 각급기관의 장은 정보시스템의 유지보수와 관련한 절차, 주기, 문서화 등과 관련한 사항을 자체 규칙에 포함하여야 한다. 정보시스템의 유지보수 절차 및 문서화를 수립할 경우 고려사항은 다음 각 호와 같다.

1. 유지보수 인원에 대한 보안서약서 집행, 보안교육 등을 포함한 유지보수 인가 절차를 마련하고 인가된 인원만 유지보수에 참여
2. 결함이 의심되거나 발생한 결함, 예방 및 유지보수에 대한 기록 유지
3. 유지보수를 위하여 정보시스템을 원래 설치장소에서 다른 장소로 이동할 경우 통제수단 마련
4. 유지보수 일시 및 담당자 인적사항, 출입통제 조치사항, 작업수행 내용 등 기록유지

② 정보시스템 관리자는 용역업체 등이 유지보수와 관련한 장비·도구 등을 제27조의2제1항에 따른 발주기관내 용역업체 작업장소에 반

출·반입할 경우 악성코드 감염 여부 및 자료 무단 반출 여부 확인 등 보안조치를 실시하고 그 결과를 각급기관의 정보보안담당관에게 제출하여야 한다.

③ 정보시스템 관리자는 직접 또는 용역업체를 활용하여 정보시스템을 유지보수 할 경우 콘솔 또는 지정된 단말기로부터의 접속만을 허용하여야 한다.

④ 각급기관의 장은 소관 정보시스템에 대하여 중요도·가용성 등에 따라 등급을 분류하고 해당 등급에 맞게 정보 보존 및 관리, 장애관리, 보안관리 등을 수행하여야 한다.

⑤ 소방청 정보보안담당관은 보안관리를 위한 정보화사업 부서의 장에게 정보시스템 구성도, 정보시스템 사양 등 보안관리에 필요한 자료를 요청할 수 있다. 이 경우 정보화사업 부서의 장은 불가피한 사정이 없는 한 제출하여야 한다.

제48조(지정 단말기를 통한 온라인 유지보수) ① 제47조제3항에 따른 지정된 단말기를 통해 유지보수를 함에 있어 각급기관의 장이 필요하다고 판단하고 용역업체가 다음 각 호에 따른 보안대책에 서면으로 동의하는 경우에 한하여, 각급기관의 장은 용역업체에게 소관 정보시스템(제39조제1항에 따른 보안·네트워크장비를 제외한다)에 대하여 인터넷을 통한 온라인 유지보수를 허용할 수 있다.

1. 지정된 장소에 설치된 지정된 단말기에서만 접속 및 해당 단말기에 대한 접근인원 통제

2. 지정 단말기는 제3호에 따른 온라인 용역 통제시스템 접속 전용(專用)으로 운용하고 다른 목적의 인터넷 접속은 차단

3. 발주기관내 설치된 온라인 용역 통제시스템을 경유하여 유지보수 대상 정보시스템에 접속하는 등 소통구간 보호·통제

4. 접속사실이 기록된 로그기록을 1년 이상 보관

5. 유지보수 계약 시행일로부터 종료 후 30일이 경과하는 날까지의 기간 중에 발주기관, 발주기관의 상급기관 및 국가정보원장의 정기 또는 수시 점검(불시 점검을 포함한다) 수검

6. 기타 국가정보원장이 배포한「국가·공공기관 용역업체 보안관리 가이드라인」에서 제시된 온라인 유지보수에 관련된 보안대책의 준수

② 그 밖의 정보시스템 온라인 유지보수 보안과 관련한 사항은 제26조(용역업체 보안)를 준용한다.

제49조(서버 보안) ① 각급기관의 장은 서버를 도입·운용할 경우, 다음과 같이 소방청 정보보안담당관과 협의하여 사이버공격으로 인한 자료 절취, 위·변조 등에 대비한 아래의 보안대책을 수립·시행하여야 한다.

1. 서버 내 저장자료에 대해 업무별 자료별 중요도에 따라 개별사용자의 접근 권한을 차등 부여

2. 개별사용자별 자료의 접근범위를 서버에 등록하여 인가 여부를 식별토록 하고 인가된 범위 이외의 자료접근을 통제

3. 서버의 운용에 필요한 서비스 포트 외에 불필요한 서비스 포트 제거 및 관리자용 서비스와 개별사용자용 서비스를 분리 운용

4. 관리자용 서비스 접속 시 특정 IP가 부여된 관리용 단말을 지정 운용

5. 서버 설정 정보 및 저장 자료에 대한 정기적 백업을 실시

6. 데이터베이스에 대하여 개별사용자의 직접적인 접속을 차단하고 개인정보 등 중요정보를 암호화하는 등 데이터베이스별 보안조치를 실시

② 정보시스템 운영부서의 장은 제2항에 따른 보안대책의 적절성을 수시 확인하되, 연 1회 이상 서버 설정 정보와 저장자료의 절취 및 위·변조 가능성 등 보안취약점을 점검·보완하여야 한다.

제50조(공개서버 보안) ① 정보화사업 부서의 장은 외부인에게 공개할 목적으로 설치되는 웹서버 등 공개서버를 내부망과 분리된 영역(DMZ)에 설치·운용하여야 한다.

② 정보화사업 부서의 장은 비인가자에 의한 서버 저장자료의 절취, 위·변조 및 분산서비스거부(DDoS) 공격 등에 대비하기 위한 보안대책을 강구하여야 한다.

③ 정보화사업 부서의 장은 비인가자의 공개서버에 대한 무단 접근을 방지하기 위하여 서버 접근 사용자를 제한하고 불필요한 계정을 삭제하여야 한다.

④ 공개서버의 서비스에 필요한 프로그램을 개발하고 시험하기 위해

사용된 도구(컴파일러 등)는 개발 완료 후 삭제를 원칙으로 한다.

⑤ 공개서버의 보안관리에 관련한 그 밖에 사항에 대해서는 제49조에 따른다.

제51조(로그기록 유지) ① 정보시스템 운영부서의 장은 정보시스템의 효율적인 통제・관리 및 사고 발생 시 추적 등을 위하여 로그기록을 유지・관리하여야 한다.

② 제1항에 따른 로그기록은 다음 각 호의 사항이 포함되어야 한다.

1. 접속자, 정보시스템・응용프로그램 등 접속대상
2. 로그온・오프, 자료의 열람・출력 등 작업 종류 및 시간
3. 접속 성공・실패 등 작업 결과
4. 전자우편 사용 등 외부발송 정보 등

③ 정보시스템 관리자는 로그기록을 생성하는 정보시스템의 경우 시간 동기화 프로토콜(NTP) 적용 등을 통해 정확한 기록을 유지하여야 한다.

④ 정보시스템 관리자는 로그기록을 정기적으로 점검하고 점검 결과 비인가자의 접속 시도, 위・변조 및 삭제 등 의심스러운 정황이나 위반한 사실을 발견한 경우 즉시 소방청 정보보안담당관에게 통보하여야 한다.

⑤ 정보시스템 관리자는 로그기록을 1년 이상 보관하여야 하며 로그기록의 위・변조 및 외부유출 방지대책을 수립・시행하여야 한다.

제52조(업무용 통신단말기 보안) ① 각급기관의 장은 업무용 통신단말기

를 이용하여 업무자료 등 중요정보를 소통・관리하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립・시행하여야 한다.

1. 통신단말기에 대한 장치 및 개별사용자 인증

2. 제어신호 및 통화내용 등 데이터 암호화

3. 분실・탈취・훼손 등에 대비한 관리적・물리적・기술적 보안대책

② 각급기관의 장은 제1항제1호에 따른 통신단말기 개별사용자를 대상으로 인증 및 암호화에 필요한 디지털정보를 발급할 수 없을 경우 국가정보원 「정보통신기기 암호기술 적용지침」을 준수하여야 한다.

③ 각급기관의 장은 주요 보직자가 안전한 통화를 위하여 사용하는 공용휴대폰(이하 "보안폰"이라 한다)이 분실・훼손되지 않도록 현황을 관리하여야 한다. 이 경우 데이터 암호화 등을 위하여 필요한 소프트웨어의 설치・유지보수 등을 지원할 수 있다.

제53조(모바일 업무보안) ① 각급기관의 장은 휴대폰・태블릿PC 등을 이용한 모바일 업무환경(내부 행정업무, 현장 행정업무 및 대민서비스 업무 등)을 구축・운용하고자 할 경우 보안대책을 수립・시행하여야 한다.

② 그 밖의 모바일 업무 보안과 관련한 사항은 국가정보원장이 배포한 「국가・공공기관 모바일 활용업무에 대한 보안가이드라인」을 준수하여야 한다.

제53조의2(사물인터넷 보안) ① 각급기관의 장은 사물인터넷을 이용한 시스템을 구축・운용하고자 할 경우 사물인터넷 기기 및 중요 데이터

등을 보호하기 위하여 보안대책을 수립·시행하여야 한다.

② 각급기관의 장은 사물인터넷을 이용한 시스템을 구축·운용하고자 할 경우 내부망과 분리하여야 한다. 다만, 내부망과 연동이 필요한 경우에는 망간 자료전송제품 설치 등 보안대책을 수립하여야 한다.

③ 각급기관의 장은 사물인터넷 서비스를 위한 소프트웨어를 개발할 경우 제27조(소프트웨어 개발보안)를 준수하여야 한다.

④ 기타 사물인터넷 보안과 관련한 사항은 국가정보원장이 배포한 「국가·공공기관 사물인터넷(IoT) 보안가이드라인」을 준수하여야 한다.

제54조(원격근무 보안) ① 각급기관의 장은 소속 공무원등이 재택근무, 출장지 현장 근무, 또는 파견 근무(제48조제1항에 따라 기관 정보통신망 전용(專用) 단말기를 설치 운영하는 경우는 제외한다)시 인터넷을 통해 본인 인증을 거쳐 기관 정보시스템에 접속하여 온라인상으로 수행하는 업무를 수행(이하 "원격근무"라 한다)하게 할 수 있다.

② 제1항에 따른 원격근무를 위해서는 국가정보자원관리원에서 운영하는 정부원격근무서비스(GVPN)을 활용 하여야 한다.

③ 제1항에 따른 원격근무로 취급할 수 있는 업무자료의 범위는 공개 및 비공개 업무자료로 제한하며 비밀·대외비를 취급하는 업무를 원격근무로 처리하여서는 아니된다.

④ 각급기관의 장은 원격근무자에게 보안서약서를 징구하고 원격근무자의 보직변경·퇴직 등 상황 발생 시 정부원격근무서비스(GVPN) 접

근권한을 등록・변경・삭제 등 현행화하여야 한다.

⑤ 원격근무자는 원격근무 시 사이버공격으로 인한 업무자료 유출을 방지하기 위하여 원격근무용 단말기에 보안소프트웨어 등을 설치・운영하고 단말기 수시 점검 및 업무자료 저장금지 등 보안조치를 하여야 한다.

⑥ 각급기관의 정보보안담당관은 원격근무와 관련한 보안대책 이행 여부를 정기적으로 점검・보완하여야 한다.

제55조 삭제

제56조(국제회의 보안) 각급기관의 장은 국제협상 등 중요 국제회의를 위하여 PC・노트북 등 정보시스템을 국외 현지에서 설치・운용하고자 할 경우 관련 정보・자료가 유출되지 아니하도록 다음 각 호의 사항을 포함한 보안대책을 수립・시행하여야 한다.

1. 설치장소에 대한 물리적 접근통제
2. 정보시스템 접근통제 및 분실 방지 등 보안관리
3. 정보시스템 저장자료 암호화 등 자료 접근통제
4. 전화기・팩스 등 통신장비에 대한 도청방지

제57조(저장매체 불용처리) ① 각급기관의 장은 정보시스템 또는 저장매체(하드디스크・반도체 기반 저장장치(SSD) 등)를 외부 수리・교체・반납・양여・폐기・불용 처리하고자 할 경우 정보시스템 및 저장매체에 저장된 자료가 외부에 유출되지 않도록 자료 삭제 등 보안조치를 하여야 한다.

② 제1항에 따라 자료를 삭제할 경우 다음 각 호에 따라야 한다.

1. 공개 자료가 저장된 저장장치 : 포맷 또는 삭제

2. 비공개 자료가 저장된 저장장치 : 물리적 파괴, 디가우징 또는 완전삭제SW에 의한 삭제(하드디스크에 한함)

3. 대외비, 비밀 또는 암호화 키가 저장된 저장장치 : 물리적 파괴

③ 제2항의 물리적 파괴의 방법은 소각·파쇄·용해 등의 방법으로 완전히 파괴하여야 한다.

④ 기타 정보시스템 및 저장매체의 불용처리와 관련한 사항은 국가정보원장이 배포한「정보시스템 저장매체 불용처리지침」을 준수하여야 한다.

제3절 자료 보안

제58조(비밀의 전자적 처리) ① 각급기관의 장은 「보안업무규정」에 따라 비밀의 생산, 분류, 보관, 열람, 출력, 송·수신, 이관, 파기 등을 전자적으로 처리할 수 있다.

② 각급기관의 장은 비밀을 전자적으로 처리하는 전 과정에서 기밀성, 무결성, 인증, 부인방지 등 보안성을 확보하여야 하며 이를 위하여 국가정보원장이 개발하거나 확인한 암호자재를 사용하여야 한다.

③ 제1항에 따라 비밀을 전자적으로 처리할 경우 내부망과 인터넷망이 물리적으로 분리된 기관은 내부망PC에서 비밀을 전자적으로 처리할 수 있으며, 그 밖의 기관은 내부망 및 기관 인터넷망과도 분리된 별

도의 비밀 작업용 PC에서 처리하여야 한다.

④ 종이문서로 출력된 비밀의 관리에 대하여는 「보안업무규정」을 준수하여야 한다.

제59조(비밀관리시스템 운용) ① 각급기관의 장은 비밀을 전자적으로 안전하게 처리하기 위하여 개발·보급된 비밀관리시스템을 도입·운용할 수 있다.

② 비밀관리시스템을 구축한 기관의 장은 비밀의 생산·보관·유통 등 전반에 대하여 비밀관리시스템을 활용하여 비밀을 안전하게 관리하여야 한다.

③ 각급기관의 장은 비밀관리시스템을 자체적으로 개발·운용하고자 할 경우 다음과 같이 비밀의 전자적 처리 규격을 준수하여 개발하여야 한다.

1. 비밀의 생산, 분류, 보관, 열람, 출력, 송·수신, 이관, 파기 등 전과정에서 요구되는 보안기능
2. 비밀의 관리를 위한 기능
3. 비밀을 표시하기 위한 양식 및 외형 정의
4. 비밀을 전자적으로 처리하면서 발생하는 각종 로그 기록·관리 기능
5. 비밀을 관리하기 위한 각종 대장 및 카드 정의
6. 개별사용자 및 시스템 관리 기능
7. 그 밖에 비밀을 전자적으로 처리하는데 필요한 보안·관리 기능

제60조(대외비의 전자적 처리) ① 각급기관의 장은 대외비를 전자적으로 처리하고자 할 경우 보호기간이 만료되지 않은 대외비는 검증필 암호모듈을 사용하여 위조·변조·훼손 및 유출 등을 방지하기 위한 보안대책을 강구하여야 하며, 보호기간이 만료된 대외비는 「국가정보보안 기본지침」 제61조에 따른 비공개 업무자료의 처리 기준을 준용하여야 한다.

② 각급기관의 장은 업무와 관계되지 아니한 사람이 대외비를 열람, 복제·복사, 배부할 수 없도록 보안대책을 수립·시행하여야 한다.

제61조(비공개 업무자료 처리) ① 공무원등은 비공개 업무자료를 다음 각 호의 어느 하나에 해당하는 방법으로 처리하여야 한다.

1. 소속 또는 근무 중인 기관의 내부망 PC, 서버 및 G드라이브에 작성 및 저장·보관
2. 소속 또는 근무 중인 기관의 장이 지급한 휴대용 저장매체에 작성 및 저장·보관
3. 다음 각 목의 어느 하나에 해당하는 수단(이하 "업무자료 공식 소통수단" 이라 한다)을 이용한 수·발신 또는 등재·열람

가. 소속 또는 근무중인 기관의 장이 자체적으로 구축·운용하는 전자우편시스템(이하 "기관 전자우편"이라 한다)

나. 공무원등이 공동으로 사용할 목적으로 문화체육관광부장관이 구축·운용하는 전자우편시스템(이하 "공직자통합메일"이라 한다)

다. 공무원등이 다른 공무원등과 자료를 공유하거나 소통하기 위하여 사용하는 전용(專用) 소프트웨어(이하 "공공 전용(專用) 메신저"라 한다)

라. 국회사무처가 구축·운용하는 의정자료전자유통시스템 등 기관간 업무자료의 소통 또는 공동활용을 위해 구축한 정보시스템

4. 그 밖에 다른 법규에 따라 허용되는 처리방법

② 공무원등은 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 경우 소속 또는 근무 중인 기관의 장이 지급한 인터넷 PC 또는 출장용 노트북을 이용하여 비공개 업무자료를 처리할 수 있다.

1. 업무자료 공식 소통수단의 발신 또는 등재 기능을 이용하여 제3조제19호다목의 문장 또는 문구 작성

2. 기관 전자우편, 공직자통합메일 또는 공공 전용(專用) 메신저로 수·발신하는 과정에서의 일시적 저장

③ 공무원등은 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 경우 개인이 소유한 PC·휴대용 저장매체·휴대폰 등을 이용하여 비공개 업무자료를 처리할 수 있다.

1. 업무자료 공식 소통수단의 발신 기능 또는 등재 기능을 이용하여 제3조제19호다목의 문장 또는 문구 작성

2. 업무자료 공식 소통수단으로 수·발신 또는 등재·열람하는 과정에서의 일시적 저장

3. 제54조에 따른 원격근무시스템에 접속하여 작성

4. 국민의 생명・신체, 국가안보 및 공공의 안전 등을 위하여 긴급히 작성, 저장, 수・발신이 필요하다고 소속 또는 근무 중인 기관의 장이 인정하는 경우

④ 공무원등은 제3항제4호에 해당하는 경우를 제외하고는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제2호에 따른 정보통신서비스(전자우편・메신저 등을 포함한다) 또는 국외에서 제공하는 이와 유사한 서비스(이하 "상용 정보통신서비스"라 한다)를 이용하여 비공개 업무자료를 작성, 저장, 수・발신하여서는 아니된다.

⑤ 공무원등은 제2항부터 제4항까지에 따라 작성・저장한 비공개 업무자료는 활용이 종료된 후에는 삭제하여야 한다.

⑥ 공무원등은 개별사용자 본인의 관리 소홀에 따른 비공개 업무자료 누출 시 일체의 보안관리 책임을 진다.

제61조의2(특정 상황별 비공개 업무자료 처리) ① 각급기관의 소속 공무원등은 「국회법」 제128조제2항, 「국정감사 및 조사에 관한 법률」 제10조제2항, 「국회증언감정법」 제2조 및 제4조에 따라 국회・정부 간 비공개 업무자료를 소통할 경우에는 우선적으로 제60조제1항제3호라목의 의정자료전자유통시스템을 활용하여 처리하여야 하며, 시스템 장애 등 부득이한 사유로 활용이 곤란할 경우에 한해 제60조에 허용된 다른 방법으로 처리할 수 있다.

② 감독・감사・조사 등의 관계 법령에 따라 비공개 업무자료를 제출받을 권한이 있는 공무원등은 업무자료를 제출할 상대방 공무원등에

게 제60조에 위반되는 방법으로 자료 제출을 요구하여서는 아니 된다.

③ 공무원등이 자문 등의 목적으로 비공개 업무자료를 업무자료 공식 소통수단을 활용할 수 없는 민간인에게 발신하거나 민간인으로부터 수신 받고자 할 경우에는 공무원등의 소속 기관 전자우편 또는 공직자 통합메일을 활용해 발신하거나 수신 받아야 한다.

제62조(비공개 업무자료 유출방지) ① 각급기관의 장은 제61조에 따른 비공개 업무자료 처리 절차 준수 여부를 관리·통제할 수 있는 보안체계를 구축·운영하여야 한다.

② 각급기관의 장은 행정안전부장관이「국가 정보보안 기본지침」 제68조제2항에 따라 개발·보급하는 소프트웨어를 적극 이용하여야 한다.

제63조(행정전자서명 인증서 등 관리) ① 공무원등은 비공개 업무자료를 처리하기 위하여「전자정부법」 제29조에 따른 행정전자서명의 인증서(이하"행정전자서명 인증서"라 한다)를 인터넷PC 또는 개인이 소유한 PC·휴대용 저장매체·휴대폰 등에 저장·보관할 수 있다.

② 공무원등은 행정전자서명 인증서 및 인증서의 비밀번호, 기관 전자우편 또는 공직자통합메일의 비밀번호 등을 상용 정보통신서비스를 이용하여 수·발신하거나 저장·보관하여서는 아니 된다.

제64조(공개 업무자료 처리) 공무원등은 관계 법규에 위배되지 않는 범위 내에서 인터넷 PC나 개인이 소유한 PC·휴대용 저장매체·휴대폰, 상용 정보통신서비스 등을 이용하여 공개 업무자료를 처리할 수

있다.

제65조(홈페이지 등 게시자료 보안) ① 각급기관의 장은 비공개 업무자료가 홈페이지 또는 외부 웹사이트(이하 "홈페이지 등"이라 한다)에 무단 게시되지 않도록 게시자료의 범위, 자료의 게시방법 등을 규정한 자체 홈페이지 정보공개 보안지침을 수립·시행하여야 한다.

② 각급기관의 정보보안담당관은 해당 부서에서 홈페이지 등에 업무자료를 게시하고자 할 경우 자료 내용을 사전 검토하여 비공개 업무자료가 게시되지 아니하도록 하여야 한다.

③ 각급기관의 장은 소속 부서에서 운용하는 홈페이지에서 비공개 업무자료가 무단 게시되었는지를 주기적으로 점검하여야 한다.

④ 각급기관의 장은 홈페이지 등에 비공개 업무자료가 무단 게시된 사실을 알게 된 경우 즉시 삭제 또는 차단 등 보안조치를 하여야 한다.

제66조(정보통신망 현황자료 관리) ① 각급기관의 장은 다음 각 호에 해당하는 자료를「공공기관의 정보공개에 관한 법률」 제9조제1항에 따른 비공개 대상 정보로 지정·관리하여야 한다.

1. 정보통신망 구성현황(IP주소 할당현황을 포함한다. 이하 본 조에서 같다)
2. 정보시스템 운용현황
3. 취약점 분석·평가 결과물(「정보통신기반 보호법」 제9조에 따른 취약점 분석·평가결과를 포함한다. 이하 본 조에서 같다)
4. 주요 정보화사업 추진현황

② 제1항에도 불구하고 각급기관의 장은 다음 각 호에 해당하는 자료는「보안업무규정 시행규칙」 제17조에 의거 국가정보원장이 배포한「비밀세부분류지침」에 따라 비밀로 분류·관리하여야 한다.

1. 암호자재 운용현황
2. 「보안업무규정」 제32조에 따른 국가보안시설 및 국가보호장비의 운영·관리에 필요한 정보통신망 구성현황 및 그에 대한 취약점 분석·평가 결과물
3. 그 밖에 제1항의 자료 중에서 국가정보원장이 비밀로 분류할 것을 요청한 자료

③ 각급기관의 장은 제1항 및 제2항에도 불구하고 다른 기관과 협력하여 정보통신망 및 정보시스템 운용 또는 정보보안업무를 수행할 필요가 있는 경우「국가 정보보안 기본지침」 제1항 및 제2항 각 호에 해당하는 자료를 다른 기관의 장에게 제공할 수 있다.

제67조(빅데이터 보안) ① 각급기관의 장은 빅데이터와 관련한 시스템을 구축·운용하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 데이터의 수집 출처 확인 및 데이터 오·남용 방지
2. 데이터 수집을 위한 정보통신망 보안체계 수립
3. 수집된 데이터의 저장 및 보호체계 수립
4. 중요 데이터 암호화
5. 사용자별(데이터 제공자·수집자·분석요청자 및 분석결과 제공자

등) 권한부여 체계 수립

6. 데이터 파기절차 수립

② 그 밖에 빅데이터 보안과 관련한 사항은 행정안전부장관이 고시한 「개인정보의 안전성 확보조치 기준」 및 국가정보원장이 배포한 「국가·공공기관 빅데이터 보안 가이드라인」을 준수하여야 한다.

제68조(암호자재 및 암호알고리즘 등) ① 각급기관의 장은 비밀 또는 중요자료를 소통·보호하고자 할 경우 국가정보원장이 개발하거나 안전성을 확인한 암호자재 또는 암호알고리즘(중요자료 소통·보호에 한함)을 사용하여야 한다.

② 제1항에 따른 암호자재 또는 암호화알고리즘의 개발·적용·운용·보관·반납·파기 등 관리절차 등은 「국가정보보안 기본지침」 제102조부터 제130조를 따른다.

제4절 사용자 보안

제69조(개별사용자 보안) ① 각급기관의 장은 소관 정보통신망 또는 정보시스템의 사용과 관련하여 다음 각 호의 사항을 포함한 개별사용자 보안에 관한 절차 및 방법을 마련하여야 한다.

1. 직위·임무별 정보통신망 접근권한 부여 심사

2. 비밀 등 중요자료 취급 시 비밀취급 인가, 보안서약서 징구 등 보안조치

3. 보직변경, 퇴직 등 변동사항 발생 시 정보시스템 접근권한 조정

② 제1항에 따라 접근권한을 부여하는 경우 필요 최소한으로 부여하여야 하며, 공무원등의 보직변경・유지보수인력 교체 등으로 접근권한 조정 사유가 발생한 경우 즉시 조정하여야 한다.

③ 개별사용자는 본인이 PC 등 정보시스템을 사용하거나 정보통신망에 접속하는 행위와 관련하여 스스로 보안책임을 진다.

제70조(단말기 보안) ① 개별사용자는 소속 기관에서 지급받은 PC・노트북・휴대폰・스마트패드 등 단말기(이하"단말기"라 한다) 사용과 관련한 모든 보안관리의 책임을 진다.

② 각급 부서의 장은 단말기를 포함한 PC 등을 사용할 경우에는 사용자 및 관리책임자를 지정하여야 한다. 이 경우에 관리책임자는 취급자를 정보시스템 관리대장에 적어서 관리하여야 한다.

③ 개별사용자는 단말기에 대하여 다음 각 호에 해당하는 보안대책을 준수하여야 한다.

1. CMOS・로그온 비밀번호의 정기적 변경 사용
2. PC등 단말기를 10분 이상 작업 중단 시 비밀번호가 적용된 화면보호 조치
3. 최신 백신 소프트웨어 설치
4. 운영체제 및 응용프로그램에 대한 최신 보안패치 유지
5. 출처, 유통경로 및 제작자가 불분명한 응용프로그램의 사용 금지
6. 인터넷을 통해 자료(파일) 획득시 신뢰할 수 있는 인터넷사이트를 활용하고 자료(파일) 다운로드 시 최신 백신 소프트웨어로 검사 후

활용

7. 인터넷 파일공유・메신저・대화방 프로그램 등 업무상 불필요한 프로그램 설치 금지 및 공유 폴더 삭제

8. 웹브라우저를 통해 서명되지 않은 액티브-X 등이 다운로드・실행되지 않도록 보안설정

9. 내부망과 기관 인터넷망이 분리된 기관의 인터넷 PC에서는 특별한 사유가 없는 한 문서프로그램을 읽기 전용으로 운용

10. 그 밖에 국가정보원장이 안전성을 확인하여 배포한 프로그램의 운용 및 보안권고문 이행

④ 각급기관의 정보보안담당관은 개별사용자의 보안대책 준수 여부를 주기적으로 점검하고 개선 조치하여야 한다.

제71조(계정 관리) ① 정보시스템 운영부서의 장은 개별사용자에게 정보시스템 접속에 필요한 사용자 계정(ID)을 부여하고자 할 경우 다음 각 호에 해당하는 사항을 준수하여야 한다.

1. 개별사용자별 또는 그룹별로 접근권한 부여

2. 외부인에게 계정을 부여하지 아니하되 업무상 불가피한 경우 해당 부서장 책임하에 보안조치 후 필요한 업무에 한하여 일정기간 동안 접속 허용

3. 비밀번호 등 사용자 식별 및 인증 수단이 없는 사용자 계정은 사용 금지

4. 특별한 사유가 없는 한 용역업체 인원에게 관리자 계정 부여 금지

② 정보시스템 운용부서의 장은 개별사용자가 시스템 접속에 5회 이상 실패할 경우 접속이 중단되도록 시스템을 설정하고 비인가자의 침입 여부를 점검하여야 한다.

③ 정보시스템 운용부서의 장은 직원의 퇴직 또는 보직변경 발생시 사용하지 않는 사용자계정을 신속히 삭제하거나 부여된 접근권한을 회수하여야 한다.

④ 정보시스템관리자는 사용자 계정 부여 및 관리의 적절성을 연 2회 이상 점검하고 그 결과를 정보안담당관에게 통보하여야 한다.

⑤ 정보시스템 관리자는 접근권한 부여, 변경, 회수 또는 삭제 등에 대한 내용을 기록하고 3년 이상 보관하여야 한다.

제72조(비밀번호 관리) ① 개별사용자 및 정보시스템 관리자는 각종 비밀번호를 숫자와 문자, 특수문자 등을 혼합하여 안전하게 설정하고 정기적으로 변경·사용하여야 한다.

② 비밀번호를 설정할 경우 다음 각 호의 사항을 준수하여야 한다.

1. 사용자계정(ID)과 동일하지 않은 것
2. 개인 신상 및 부서명칭 등과 관계가 없는 것
3. 일반 사전에 등록된 단어는 사용을 피할 것
4. 동일 단어 또는 숫자를 반복하여 사용하지 말 것
5. 사용된 비밀번호는 재사용하지 말 것
6. 동일 비밀번호를 여러 사람이 공유하여 사용하지 말 것
7. 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지

③ 정보시스템 관리자는 서버 등 정보시스템에 보관되는 비밀번호가 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

④ 정보시스템 운영부서의 장은 사용자를 식별 또는 인증하기 위하여 비밀번호에 갈음하거나 병행하여 지문인식 등 생체인증 기술 및 일회용 비밀번호 생성기(OTP) 등을 안전성 확인 후 사용할 수 있다. 이 경우 생체인증 정보는 안전하게 보관하여야 한다.

제73조(전자우편 보안) ① 각급 기관의 장은 전자우편을 컴퓨터바이러스·트로이목마 등 악성코드로부터 보호하기 위하여 백신 소프트웨어 설치, 해킹메일차단시스템 구축 등 보안대책을 수립·시행하여야 한다.

② 개별사용자는 전자우편에 포함된 붙임파일이 자동 실행되지 않도록 설정하고 첨부파일을 다운로드 할 경우 최신 백신으로 악성코드 은닉 여부를 검사하여야 한다.

③ 개별사용자는 출처가 불분명하거나 의심되는 제목의 전자우편은 열람하지 말고 해킹메일로 의심되는 메일 수신 때에는 즉시 소방청 정보보안담당관에게 신고하여야 한다.

제74조(휴대용 저장매체 보안) ① 각급기관의 장은 휴대용 저장매체를 사용하여 업무자료를 보관하고자 할 경우 자료의 위·변조, 저장매체의 훼손·분실 등에 대비한 보안대책을 수립·시행하여야 한다.

② 각급기관의 장은 휴대용 저장매체 관리시스템을 운용하고자 할 경우 국가정보원장이 안전성을 확인한 제품을 도입하여야 한다.

③ 정보보안담당관은 사용자가 휴대용 저장매체를 PC·서버 등에 연결할 경우 자동 실행되지 아니하고 최신 백신 소프트웨어로 악성코드 감염여부를 자동 검사하는 등의 보안 정책을 수립·시행하도록 관리하여야 한다.

④ 각급부서의 장은 휴대용 저장매체를 비밀용·일반용으로 구분하여 휴대용 저장매체 관리대장에 기록하고, 휴대용 저장매체에 관련 정보를 기입·표시하여야 한다. 각급부서장은 휴대용 저장매체 수량 및 보관 상태 등을 정기적으로 휴대용 저장매체 점검대장을 통해 점검하여야 하고, 외부 반출·입 시 휴대용 저장매체 반출·입 대장에 기록·관리하여야 하며, 휴대용 저장매체 무단 반출 및 미등록 저장매체 사용을 사전 통제하여야 한다.

⑤ 각급부서의 장은 비밀이 저장된 휴대용 저장매체는 매체별로 비밀등급 및 관리번호를 부여하고 비밀관리기록부에 등재·관리하여야 한다. 이 경우 매체 전면에 비밀등급 및 관리번호가 표시되도록 하여야 한다. 휴대용 저장매체가 암호자재에 해당될 경우에는 제68조의 암호자재 등의 운용·관리체계에 따라 관리하여야 한다.

⑥ 각급부서의 장은 휴대용 저장매체의 용도변경, 폐기·불용 처리를 하고자 할 경우 저장자료가 복구 불가하도록 완전삭제 소프트웨어 등을 이용하여 삭제하여야 한다. 다만, 완전삭제가 불가할 경우 파쇄하여야 한다.

⑦ 각급부서의 장은 제6항에 따른 휴대용 저장매체 불용 처리 시 정보

시스템 저장매체·자료별 삭제방법에 따른 기준 이상으로 자료를 삭제하여야 하며, 휴대용 저장매체를 불용 처리하거나 재사용 시 휴대용 저장매체 불용처리 확인서에 따라 해당 불용처리 사항을 확인하여야 한다.

⑧ 그 밖에 휴대용 저장매체 보안과 관련한 사항은 국가정보원장이 배포한「USB메모리 등 휴대용 저장매체 보안관리지침」을 준수하여야 한다.

제75조(비인가 기기 통제) 공무원등은 개인 소유 정보통신기기(휴대폰 등 이동통신단말기를 제외한다)를 소속된 기관으로 무단으로 반입·사용하여서는 아니 된다. 다만 부득이한 경우 각급기관의 정보보안담당관의 승인 후 사용할 수 있다.

제76조(위규자 처리) 각급기관의 장은 국가정보원장이 배포한 「정보보안 사고(위규) 처리기준(안)」에 따라 정보보안 위규자를 처리하고, 「국가공무원 복무·징계 관련 예규」(인사혁신처) 제12장 및「소방공무원 징계양정 등에 관한 규칙」을 참고하여 정보보안 위규자를 처리한다.

제77조 삭제

제78조 삭제

제4장 융합보안

제1절 정보통신시설 및 기기 보호

제79조(정보통신시설 보안) ① 각급기관의 장은 다음 각 호의 어느 하나에 해당하는 정보통신시설 및 장소를 「보안업무규정」 제34조에 따른 보호지역으로 지정·관리하여야 한다.

1. 암호실·정보통신실
2. 암호자재 개발·설치 및 정비장소
3. 국가비상통신 등 중요통신망의 교환국, 회선집중국 또는 중계국
4. 사이버보안관제센터, 백업센터 및 중요 정보통신시설을 집중 제어하는 국소
5. IT관제실
6. 그 밖에 보안관리가 필요하다고 인정되는 정보시스템 설치 장소

② 각급기관의 장은 제1항에 따라 보호지역으로 지정된 정보통신시설 및 장소에 대한 보안대책을 수립하고자 할 경우 다음 각 호에 해당하는 사항을 포함하여야 한다.

1. 방재대책 및 외부로부터의 위해(危害) 방지대책
2. 상시 이용하는 출입문은 한 곳으로 정하고 이중 잠금장치 설치
3. 출입자 식별·인증 등을 위한 출입문 보안장치 설치 및 주·야간 감시대책
4. 휴대용 저장매체를 보관할 수 있는 용기 비치
5. 정보시스템의 안전지출 및 긴급파기 계획 수립
6. 관리책임자 및 자료·장비별 취급자 지정·운영
7. 정전에 대비한 비상전원 공급 및 시스템의 안정적 중단 등 전력관

리 대책

8. 비상조명 장치 등 비상탈출 대책

9. 카메라 장착 휴대폰 등을 이용한 불법 촬영 방지대책

제80조(정보통신시설 출입관리) ① 각급기관의 장은 외부인이 정보통신시설을 방문할 경우 반드시 신원을 확인하고 보안교육 및 보안검색 후 출입을 허용하여야 한다.

② 각급부서의 장은 불가피한 경우를 제외하고는 정보통신시설에 대한 관람 및 견학은 지양하고 외국인의 출입은 금지한다. 다만 외국인의 출입이 꼭 필요한 경우 소방청 정보보안담당관과 협의하여야 한다.

제81조(영상정보처리기기 보안) ① 각급기관의 장은 업무상 목적으로 불특정 사람 또는 사물을 촬영한 영상을 유·무선 정보통신망으로 전송·저장·분석하는 CCTV·IP카메라·이동형 영상촬영장비·중계서버·관제서버·관리용 PC 등의 기기·장비(이하"영상정보처리기기"이라 한다)를 설치·운용하고자 할 경우 운영자의 계정·비밀번호 설정 등 인증대책을 수립하고 특정 IP주소에서만 접속 허용 등 비인가자 접근 통제대책을 수립·시행하여야 한다.

② 각급기관의 장은 영상정보처리기기를 통합·운영하는 시설(이하 "영상관제상황실"이라 한다)을 운영하고자 할 경우 영상관제상황실을 「보안업무규정」 제34조제2항에 따른 제한구역 또는 통제구역으로 지정·관리하고 출입통제 장치를 운용하여야 한다.

③ 각급기관의 장은 영상정보처리기기를 인터넷과 분리·운용하여야

한다. 다만 부득이하게 인터넷과 연결·사용하여야 할 경우 전송내용을 암호화하여야 한다.

④ 각급기관의 장은 제1항부터 제3항까지와 관련한 보안대책의 적절성을 수시 점검·보완하여야 한다.

⑤ 기타 영상정보처리기기 보안과 관련한 사항은 국가정보원장이 배포한 「국가 공공기관 영상정보 처리기기 도입·운영 가이드라인」 및 「안전한 정보통신 환경 구현을 위한 네트워크 구축 가이드라인」을 준수하여야 한다.

제82조(RFID 보안) ① RFID 운영부서의 장은 RFID시스템을 구축하여 중요정보를 소통하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. RFID시스템(태그 및 리더기 포함) 분실·탈취 대비 및 백업 대책
2. 태그정보 최소화 대책
3. 장치 및 운용자 인증, 중요정보 암호화 대책

② RFID 시스템 관리자는 제1항과 관련한 보안대책의 적절성을 수시 점검·보완하여야 한다.

③ 기타 RFID 보안과 관련한 사항은 국가정보원장이 배포한「RFID 보안관리 실무매뉴얼」을 준수하여야 한다.

제83조(디지털복합기 보안) ① 각급기관의 장은 디지털복합기(디지털복사기 등도 포함한다. 이하 "복합기"라 한다)를 설치·운용하고자 할 경우 자료유출을 방지하기 위하여 자료 완전삭제 또는 디스크 암호화

기능이 탑재된 복합기를 도입하여야 한다.

② 제1항에 따라 도입된 복합기는 운용 전에 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 암호화 저장 기능이 있는 경우 해당 기능 사용 여부

2. 정기적으로 저장된 작업 내용(출력·스캔 등) 완전 삭제 여부

3. 공유 저장소 사용 제한 및 접근 제어

4. 고정 IP주소 설정 및 불필요한 서비스 제거 등

③ 각급기관의 장은 복합기를 설치·운용할 경우 다음 각 호의 어느 하나에 해당하는 경우 복합기의 저장매체에 저장된 자료를 완전 삭제하여야 한다.

1. 복합기 사용연한이 경과하여 폐기·양여할 경우

2. 복합기 무상 보증기간 중 저장매체 또는 복합기 전체를 교체할 경우

3. 고장 수리를 위한 외부 반출 등의 사유로 해당 기관이 복합기의 저장매체를 통제 관리할 수 없는 장소로 이동할 경우

4. 그 밖에 저장자료의 삭제가 필요하다고 판단되는 경우

④ 각급기관의 장은 소모품 교체 등 복합기 유지보수를 할 경우 입회·감독하고 저장매체의 무단 교체 등을 예방하여야 한다.

⑤ 복합기 설치·운용하는 각급기관의 장은 복합기를 통해 내부망과 기관 인터넷망간 접점이 발생하지 않도록 보안대책을 수립·시행하여야 한다.

⑥ 소방청 정보보안담당관은 소속된 기관의 저장매체가 장착되어 있는 복합기 운용과 관련한 보안대책의 적절성을 수시 점검·보완하여야 한다.

⑦ 기타 복합기 보안과 관련한 사항은 국가정보원장이 배포한「정보시스템 저장매체 불용처리지침」을 준수하여야 한다.

제84조(재난 방지대책) ① 정보시스템 관리부서의 장은 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애 발생에 대비하여 정보시스템 이원화, 백업관리, 복구, 비상전원설비 설치 등 종합적인 재난방지대책을 수립·시행하여야 한다.

② 정보시스템 관리부서의 장은 정보시스템 장애에 대비한 백업시설을 확보하고 정기적으로 백업을 수행하여야 한다.

③ 정보시스템 관리부서의 장은 제2항에 따라 백업시설을 설치할 경우에는 정보통신실과 물리적으로 일정 거리 이상 위치한 안전한 장소에 설치하여야 하며 전력공급원 분리 등 정보시스템의 가용성을 최대화할 수 있도록 하여야 한다.

④ 정보시스템 관리부서의 장은 재난방지대책을 정기적으로 시험하고 검토해야 하며 업무 연속성에 대한 영향평가를 실시하여야 한다.

⑤ 제1항 내지 제4항에도 불구하고 국가정보자원관리원에 입주한 정보시스템은 국가정보자원관리원의 재난 방지대책을 따른다.

제2절 전자파 보안

제85조(대도청측정) ① 소방청 정보보안담당관은 다음 각 호의 어느 하나에 해당하는 시설·장소에 대하여 각종 수단에 의한 도청으로부터 정보유출을 방지하기 위한 보안대책을 수립·시행하여야 한다.

1. 청사를 신축·이전 및 증·개축, 대규모 수선 등을 하는 경우
2. 기관장실 및 회의실 등 중요업무 장소
3. 중요한 회담·협상·행사를 개최할 경우(필요시)
4. 기타 대도청 측정이 필요하다고 판단되는 시설·장소·장비

② 각급기관의 장은 제1항에 따른 시설·장소에 대하여 자체 또는 「통신비밀보호법」 제10조의4에 따른 불법감청설비탐지업자 활용 등을 통해 대도청 측정을 실시하여야 한다.

③ 제2항에도 불구하고 다음 각 호에 해당하는 시설·장소에 대하여는 국가정보원장에게 대도청 측정을 요청할 수 있다.

1. 국가기관의 장 또는 상급기관의 장이 관리하는 시설·장소
2. 하급기관의 장이 관리하는 시설·장소 중에서 관계 상급기관의 장이 국가안보 및 국익 보호를 위하여 필요하다고 판단하는 시설·장소

④ 제2항에 따라 대도청 측정을 실시한 기관의 장은 측정결과 취약요인이 발견된 경우 그 결과를 소방청 정보보안담당관을 거쳐 국가정보원장에게 통보하고 기술 지원 및 추가 측정을 요청할 수 있다.

⑤ 제2항에 따라 대도청 측정을 실시한 결과 취약요인이 발견된 경우 해당 기관의 장은 개선대책을 수립·시행하여야 한다.

⑥ 각급기관의 장은 대도청 측정 실시 결과를 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따른 비공개 대상 정보로 지정·관리하여야 한다.

⑦ 기타 대도청 측정과 관련한 사항은 국가정보원장이 배포한「도청탐지·방어활동 가이드라인」을 준수하여야 한다.

제86조(무선통신망 보안) ① 무선통신망(제40조 무선랜(WiFi) 보안 제외)을 구축·운영하거나 이동통신망을 이용하여 관련 시스템을 구축·운용하는 기관의 장은 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 접경 지역의 경우 무선통신망의 유선화 추진 또는 전파 차단시설 정책 시행
2. 비밀 등 중요자료를 소통하고자 할 경우 국가정보원장이 개발하거나 안전을 확인한 암호자재 사용
3. 무선국 현황 관리 및 전파월경 등 통신보안 준수
4. 접경지역에 설치된 전파 차단시설 점검

② 제1항에 따른 무선통신망을 운영하는 각급기관 장은 연간 전파측정 계획을 수립하여 연 1회 이상 전파측정을 실시하여야 한다.

③ 무선통신망을 운영하는 각급 부서의 장은 소방청 정보보안담당관에게 제2항에 따른 연간 전파측정 계획서를 매년 1월 20일까지 제출하고 전파측정 실시 후 20일 이내에 전파측정 활동 결과보고서를 제출하여야 한다.

제87조(고출력 전자파 보안) ① 각급기관장은 소관 주요시설을 고출력 전자파(EMP)로부터 안전하게 보호하기 위한 예방・백업・복구등 물리적・기술적 대책을 포함한 보호대책을 수립・시행할 수 있다.

② 각급기관 장은 제1항에 따른 보호대책을 수립하기 위하여 취약점 분석・평가를 실시할 수 있으며 이를 위하여 담당자 지정 또는 전담반을 구성할 수 있다.

제5장 사이버위협 탐지・대응

제1절 훈련 및 진단

제88조(사이버공격 대응훈련) ① 소방청 정보보안담당관은 소방청 정보통신망을 대상으로 매년 정기 또는 수시로 사이버공격 대응훈련을 실시하여야 한다.

② 각급기관장은 국가정보원장이 중앙행정기관, 지방자치단체 및 공공기관을 대상으로 실시하는 사이버공격 대응훈련에 정보보안담당관을 참여시켜야 한다.

③ 제2항에 따른 대응훈련은 「비상대비에 관한 법률」 제14조에 따른 비상대비훈련과 함께 실시할 수 있다.

제89조(정보통신망 보안진단) 소방청 정보보안담당관은 국가정보원장이 배포하는 다음 각 호의 가이드라인 등을 참고하여 정보통신망을 대상으로 취약점을 진단하는 제반활동(이하 "보안진단"이하 한다)을 매년 정기적으로 실시하거나 관련 예산확보 등을 위하여 노력하여야 한다.

1. 정보보안점검 체크리스트

2. 공공분야 정보시스템 취약점

3. 정보통신시스템 보안진단 및 대응방법

제2절 정보보안 관리실태 평가

제90조(자체평가) ① 소방청장은 국가정보원장이 매년 실시하는 정보보안 관리실태평가에 대비하여 국가정보원의 평가지표에 따라 자체 평가를 실시하여야 한다.

② 소방청 정보보안담당관은 자체평가의 적절성을 입증하기 위하여 필요하다고 판단하는 경우 평가지표별 증빙자료를 소속기관, 산하기관 및 정보화사업 부서장에게 요구할 수 있다. 해당 기관은 증빙자료를 즉시 제출하여야 한다.

제91조(결과 통보 및 보완조치) 소방청장은 국가정보원의 현장실사를 거쳐 통보받은 정보보안 관리실태 평가 결과를 해당 기관의 장에게 통보하고 평가결과를 통보받은 기관의 장은 평가결과에 따른 미비점을 개선·보완하여 정보보안 수준을 제고하여야 한다.

제3절 사이버보안관제센터 운영

제92조(사이버보안관제센터 설치·운영) 소방청장은 소관 정보통신망에 대한 사이버공격 정보를 수집·분석·대응할 수 있는 사이버보안관제센터를 설치·운영하여야 한다. 다만, 불가피한 사유가 있을 경우에는

다른 중앙행정기관의 장, 지방자치단체의 장 및 관계 공공기관의 장이 설치·운영하는 사이버보안관제센터에 그 업무를 위탁할 수 있다.

제93조(보안관제 인원) ① 소방청 정보보안담당관은 보안관제업무를 24시간 중단없이 수행하여야 하며 이를 담당할 전문 또는 전담인력을 배치하고 교대근무체계를 운영하여야 한다.

② 「국가사이버안전관리규정」 제10조의2제4항에 따라 보안관제전문업체의 인원을 활용하고자 하는 경우 다음 각 호에 해당하는 사항을 준수하여야 한다.

1. 업체를 선정할 경우 과학기술정보통신부장관이 고시하는 「보안관제 전문기업 지정 등에 관한 공고」에 따른 업무수행능력 평가기준 등 준수
2. 보안관제업무의 책임 있는 수행 및 보안관리 등을 위하여 적정한 수의 공무원 또는 정규직원 상시 배치
3. 업체 인원에 대하여 제26조(용역업체 보안), 제30조(누출금지정보 유출시 조치) 준용
4. 업체 인원을 대상으로 매월 1회 이상 탐지규칙정보 관리 등에 관한 보안 교육 및 점검 실시

제94조(공격정보 탐지·수집) ① 소방청장은 보안관제 대상 기관에 대한 사이버공격에 관한 정보를 탐지·수집하여야 한다.

② 사이버보안관제센터를 운영하는 부서의 장은 제1항의 업무 수행을 위하여 사이버공격에 관한 정보를 실시간 수집하는 장비를 보안관제

대상기관의 정보통신망에 설치·운용하거나 탐지규칙정보를 제공하여 관련 정보를 실시간 수집할 수 있다.

제95조(사이버보안관제센터 수행업무) 사이버보안관제센터 업무수행과 관련한 세부사항은 「국가전산망 보안관제지침」을 따른다.

제4절 사고대응

제96조(사고상황전파) ① 각급부서의 장은 사이버공격과 관련한 정보를 확인한 경우에는 전화·팩스·이메일 등 통신수단을 활용하여 지체없이 그 사실을 소방청 정보보안담당관에게 통보하여야 한다.

② 제1항에 따라 통보해야 할 사항은 다음 각 호와 같다.

1. 대규모 사이버공격 발생 시
2. 사이버공격으로 인하여 피해가 발생하거나 피해 발생이 예상되는 경우
3. 사이버공격이 확산될 우려가 있는 경우
4. 그 밖에 사이버공격 계획 등 사이버안전에 위협을 초래할 수 있는 정보를 입수한 경우

제97조(정보보안 사고조사) ① 각급부서의 장은 정보보안 사고가 발생한 때에는 즉시 피해확산 방지를 위한 조치를 취하고 다음 각 호의 사항을 소방청 정보보안담당관에게 통보하여야 한다. 이 경우, 사고원인 규명 시까지 피해 시스템에 대한 증거를 보전하고 임의로 관련 자료를 삭제하거나 포맷하여서는 아니 된다.

1. 일시 및 장소

2. 사고 원인, 피해 현황 등 개요

3. 사고자 및 관계자의 인적 사항

4. 조치 내용 등

② 소방청 정보보안담당관은 사고조사 후 그 결과를 해당 기관의 장에게 통보하고 동일유형의 사고가 발생하지 않도록 제반 보안조치를 해당 기관에 권고할 수 있다.

③ 소방청 정보보안담당관은 제2항에도 불구하고, 필요하다고 인정할 경우 해당 기관의 장에게 사고 조사에 관련된 권한의 일부를 위임할 수 있다. 다만, 권한을 위임받은 기관의 장은 소방청 정보보안담당관에게 조사결과를 통보해야 한다.

④ 각급기관의 장은 규정에 따른 관련자 징계, 재발방지대책의 수립·시행 등 사고 조사 결과에 따라 필요한 조치를 하여야 한다.

제6장 보칙

제98조(준용) 이 규정에 명시되지 않은 사항은「국가 정보보안 기본지침」을 준용한다.

제99조(재검토기한) 소방청은「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 2026년 1월 1일 기준으로 매 3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부 칙

이 훈령은 발령한 날부터 시행한다.