소방청 훈령 제156호

소방청 정보보안업무 규정 전부를 다음과 같이 개정한다.

2020년 5월 20일
소방청장

소방청 정보보안업무 규정 전부개정안

1. 개정이유

최신 정보통신기술 적용이 확대되고, 국정원 주관의 보안성 검토 및 보안적합성 검증 업무를 중앙행정기관 등으로 일부 위임하는 등 보안 업무환경 변화와 불필요한 통보(제출)제도 폐지·개선 등 국정원「국가 정보보안 기본지침」개정('19.3.22) 내용을 반영하여「소방청 정보보안업무 규정」을 전부 개정하고자 함

2. 주요내용

가. 정보보안담당관의 권한·책임을 분산

○ 정보보안담당관 업무를 부서별 분임정보보안담당관에 분산(제5조)

○ 보안관리책임이 정보화사업은 정보화사업 부서장(제12조), 정보시스템 운용은 시스템관리자(제46조), 개별 단말기·업무자료는 해당 공무원(제61조 및 제70조)에게 각각 있음을 명시

나. 국가·공공기관 청사 내에 무선랜(WiFi)를 설치·운용시 공무원용과 외부인용으로 구분하도록 하고, 보안대책 차별화(제40조)

다. 국정원의 정보화사업 보안성 검토 및 IT제품 보안적합성 검증 업무를 소방청 및 그 소속기관으로 일부 위임하거나 생략

○ 정보화사업의 규모·중요도를 고려하여 보안성 검토 업무를 중앙행정기관 및 소속기관에 일부 위임하고, 단순 제품 교체 등의 경우 보안성검토 생략(제2장제2절)

○ IT제품에 대한 보안적합성 검증 업무를 본청 각 부서 및 소속·산하기관에 일부 위임하고, 관련기관으로부터 인증·시험을 받은 제품의 경우 보안적합성 검증 생략(제2장제4절)

라. 불필요한 관행 폐지 및 개선

○ 정보보안담당관 임면 시 국정원에 통보제도 폐지(제5조)

○ 연도별 보안업무 심사분석 결과 제출 의무 폐지(제6조)

○ 정보화사업 보안성 검토 의뢰 및 홈페이지 자료 등재 시 보안심사위원회 개최 폐지(제15조 및 제65조)

○ 용역사업 참여 인원에 대해 법적 근거 없이 실시하던 신원조사 폐지(제26조)

마. 정보통신망 현황자료를 비밀·대외비로 일괄 분류·관리하던 방식에서 중요도에 따라 비밀 또는 일반 비공개 자료로 관리하도록 개선(제66조)

바. 정보보안업무 절차를 반영하여 조항의 신설·개정·재배치

현재 (7장 127조)	**개정(안)** (6장 99조)
제1장 총칙 제2장 기본활동 제3장 부서별 보안 관리 제4장 국가용 보안시스템 제5장 안전성 확인 제6장 사이버위협 탐지・대응 제7장 보칙	제1장 총칙 제2장 정보화사업 보안 제3장 정보통신망 및 정보시스템 보안 제4장 융합 보안 제5장 훈련·평가 및 탐지·대응 제6장 보칙

3. 참고사항

가. 관계법령 : 국가정보원법, 보안업무 규정, 국가 정보보안 기본지침

나. 예산조치 : 별도조치 필요 없음

다. 합　　의 : 해당기관 없음

라. 기　　타 :

소방청 훈령　제156호

소방청 정보보안업무 규정 전부개정안

소방청 정보보안업무 규정 전부를 다음과 같이 개정한다.

소방청 정보보안업무 규정

제1장 총 칙

제1조(목적) 이 규정은 「국가정보원법」과「보안업무규정」, 「국가정보보안 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. "사용자"란 각급기관의 장으로부터 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 공무원 등을 말한다.

4. "정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집・가공・저장・검색・송수신하는 정보통신체제를 말한다.
5. "정보화사업"이란 「전자정부법」 제2조의 규정에 따른 정보통신망 또는 정보시스템을 개발・구축・운용・유지보수하거나 정보시스템 감리, 전자정부사업관리의 위탁 등을 하기 위한 사업을 말한다.
6. "인터넷서비스망"(이하 "인터넷망"이라 한다)이란 기관의 네트워크 중에서 인터넷을 사용할 수 있도록 연결된 인터넷 전용망을 말한다.
7. "업무전산망"(이하 "내부망"이라 한다)이란 기관의 네트워크 중에서 업무용으로 사용되는 영역으로, 망 분리기관의 경우 인터넷망과 분리된 내부전산망(이하"내부망"이라 한다)을 말하고 망 미분리기관은 인터넷서비스도 병행 제공되는 내부전산망을 포함한다.
8. "정보시스템"이란 서버・PC 등 단말기, 네트워크 장치, 응용 프로그램 등 정보의 수집・가공・저장・검색・송수신에 필요한 하드웨어 및 소프트웨어 일체를 말한다.
9. "휴대용 저장매체"란 디스켓・CD・외장형 하드디스크・USB 메모리 등 정보를 저장할 수 있는 것으로 PC 등의 정보시스템과 분리할 수 있는 기억장치를 말한다.
10. "정보보안" 또는 "정보보호"란 정보시스템 및 정보통신망을 통해 수집・가공・저장・검색・송수신되는 정보의 유출・위변조・훼손

등을 방지하기 위하여 관리적・물리적・기술적 수단을 강구하는 일체의 행위를 말한다.
11. "전자문서"란 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태로 송・수신 또는 저장되는 정보를 말한다.
12. "전자기록물"이란 정보처리능력을 가진 장치에 의하여 전자적인 형태로 송・수신 또는 저장되는 기록정보자료를 말한다.
13. "전자정보"란 업무와 관련하여 취급하는 전자문서 및 전자기록물을 말한다.
14. "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.
15. "정보통신실"이란 서버・PC 등과 스위치・교환기・라우터 등 네트워크 장치 등이 설치 운용되는 장소를 말하며, 전산실・통신실・전자문서 및 전자기록물(전자정보) 보관실 등을 말한다.
16. "암호자재"란 Ⅱ급비밀 이하의 통신내용 등의 정보를 보호할 목적으로 사용하는 문자・숫자・기호 등으로 구성된 환자표와 난수 또는 암호논리 등을 수록한 문서나 도구를 말한다.
17. "음어자재"란 Ⅲ급비밀 이하의 통신내용 등의 정보를 보호할 목적으로 사용하는 문자・숫자・기호 등으로 구성된 환자표 또는 암호논리 등을 수록한 문서나 도구를 말한다.

18. "약호자재"란 대외비 이하의 통신내용 등의 정보를 보호할 목적으로 특정 용어와 그에 대응·변환되는 문자, 숫자, 기호 등을 수록한 문서나 도구를 말한다.

19. "암호논리"란 정보의 유출, 위·변조, 훼손 등을 방지하기 위하여 기밀성·무결성·인증·부인봉쇄 등의 기능을 제공하는 수학적 논리 또는 알고리즘을 말한다.

20. "암호모듈"이란 정보의 유출, 위·변조, 훼손 등을 방지하기 위해 암호논리를 활용하여 구현한 수단이나 도구를 말한다.

21. "정보보호시스템"이란 정보의 수집·저장·검색·송신·수신시 정보의 유출, 위·변조, 훼손 등을 방지하기 위한 하드웨어 및 소프트웨어를 말한다.

22. "무선도청 탐지"란 유·무선 도청탐지장비 등을 이용하여 은닉된 무선도청장치 색출과 각종 도청 위해요소를 제거하는 제반활동을 말한다.

23. "전자파보안"이란 정보통신기기·시설 등을 대상으로 전자파에 의한 정보유출을 방지하고 파괴·오작동 유발 등의 위협으로부터 정보를 보호하는 행위 일체를 말한다.

24. "고출력전자기파"(EMP)란 전자장비를 물리적으로 파괴시키거나 오작동을 유발시킬 수 있는 정도의 강력한 전자기적 충격파를 말한다.

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

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

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

1. 소방청 : 정보통계담당관
2. 소속·산하기관 : 정보통신업무 관련 부서의 장

② 소방청 정보보안담당관은 각급기관의 정보보안업무를 총괄하며, 다음 각호의 업무를 수행한다.

1. 정보보안 정책· 활동 계획 수립·시행
2. 정보보안 관련 규정·지침 등 제·개정
3. 보안심사위원회(정보보안분야) 운영
4. 정보보안 업무 지도·감독, 정보보안 감사
5. IT관제센터(IT관제실), 정보통신망 및 정보자료 등의 보안관리
6. 정보보안 관리실태 평가
7. 사이버공격 초동조치 및 대응
8. 사이버위협정보 수집·분석 및 보안관제
9. 정보보안 예산 및 전문인력 확보

10. 정보보안 사고조사 결과 처리

11. 정보보안 교육 및 정보협력

12. 도청 위해 요소 측정·제거

13. 주요 정보통신기반시설 보호활동

14. 암호자재 및 암호키의 운용·보안관리

15. 안전성을 검증한 암호모듈·CC인증을 획득한 정보보호시스템의 운용 및 보안관리

16. 정보통신망 보안대책의 수립·시행

17. '사이버보안진단의 날' 계획 수립·시행

18. 소관분야 정보보안 업무조정 및 감독

19. 침해사고 대응·복구

20. 그 밖에 정보보안 관련 사항

③ 정보보안담당관은 효율적인 정보보안업무를 수행하기 위하여 전담인력을 확보·운영하여야 하며, 중요 정보보안업무에 대하여는 「소방청 보안업무 시행세칙」(이하 "보안업무 시행세칙"이라 한다) 제4조에 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 분임정보보안담당관을 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 「국가 정보보안 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 감찰업무를 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 정보보안 감사를 실시할 수 있으며, 소방청장에게 감사의 방향 및 중점사항, 감사관 지원 등 협조를 요청할 수 있다

⑤ 소방청장은 사안이 무거운 정보보안 위규사항을 적발한 경우 「국가공무원 복무・징계 관련 예규」 및 「소방공무원 징계양정 등에 관한 규칙」을 참고하여 「소방청 보안업무시행세칙」 제4조에 따른 보안심사위원회의 심의를 거쳐 관련자에 대한 징계를 요청할 수 있다.

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

⑦ 소방청장은 정보보안감사 담당자를「국가 정보보안 기본지침」 제8조 제5항에 따라 우대하여야 한다.

제9조(정보보안 교육) ① 소방청장은 정보보안에 대한 경각심을 제고하기 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 등을 종합적인 보안진단을 실시하여야 한다.

제11조(통신보안 위규) ① 통신망을 통해 비인가자에게 누설하거나 위반할 경우 발생하는 정보통신보안 위규사항은 별표 1과 같다.

② 각급기관 정보보안담당관은 정보보안 위규사항을 적발하였을 경우 소방청장(정보통계담당관)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. 기존 운용 중인 정보통신망 및 정보시스템에 대한 용역업체 접근통제대책
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. 기존 운용 중인 정보통신망 및 정보시스템에 대한 용역업체 접근통제대책
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 발견 시 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 기관이 장이 공개가 불가하다고 판단한 자료

제2절 보안성 검토

제15조(검토 시기 및 절차) ① 정보화사업 부서의 장은 다음 각 호의 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, 국가정보원장은 정보화사업의 규모·중요도 등을 고려하여 소방청장에게 보안성 검토를 위임할 수 있다.

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 따

라 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. 제1항 단서에 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 무선랜, 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 용역

사업

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 해당 기관의 장이 필요하다고 판단하는 정보통신망 또는 정보시스템 구축

③ 정보통신망 보안성검토는 서면 검토를 원칙으로 하되 필요하다고 판단하는 경우에는 현장 확인을 실시할 수 있다.

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. 제15조제1항 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 사

항을 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

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 정보통신망 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) 정보화사업 부서의 장은 정보 및 정보통신망 등을 보호하기 위하여 정보보호시스템・네트워크장비 등 보안기능이 있는 정보통신제품을 도입・운용할 경우 별표 3에 따른 정보보호시스템 유형별 도입요건을 준수하여야 한다.

제21조(암호가 주기능인 제품 도입요건) 정보화사업 부서의 장은 정보통신망을 이용하여 유통・보관되는 중요자료를 보호하기 위하여 암호가 주기능인 제품을 도입・운용하고자 할 경우 별표 4에 따른 암호가 주기능인 제품 도입요건을 준수하여야 한다.

제22조(상용 암호모듈 도입 시 고려사항) 정보화사업 부서의 장은 국가정보원장이 안전성을 확인한 상용 암호모듈을 도입하여 정보시스템 등에 적용하고자 할 경우 실제 적용 이전에 해당 상용 암호모듈의 정상 작동 여부, 정보시스템 적용 단계에서 구동 과정상 오류 발생 여부 등을 점검하여야 한다.

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(제어시스템 도입 시 고려사항) ① 정보화사업 부서의 장은 공항·항만·전력·가스·운송설비 등을 중앙에서 감시·제어하기 위한 정보시스템(이하 "제어시스템"이라 한다)을 도입·운용하고자 할 경우 사업 계획 단계(사업 공고 전)에서 국가정보원장이 배포한 「국가·공공기관 제어시스템 보안가이드라인」에 따른 보안대책을 수립·시행하여야 한다.

② 정보화사업 부서의 장은 제어시스템을 도입·운영할 경우 최신 백신 소프트웨어 설치, 응용프로그램 보안패치 및 침해사고 대응방안 등 보안대책을 수립·시행하고 정기적으로 취약점을 점검하여야 한다. 다만, 제어시스템의 정상 운영에 차질을 초래할 경우 국가정보원장과 협의하여 설치하지 아니할 수 있다.

③ 정보화사업 부서의 장은 교통·에너지·수자원 등 국가안보상 중요한 제어시스템을 운용할 경우 인터넷 및 일반사무용 내부망과 분리·구축하여야 한다.

④ 정보화사업 부서의 장은 제3항에서 불구하고 제어시스템을 기관 인터넷망과 연동할 필요가 있을 경우 연동 구간에 일방향 전송장비 설치 등 안전한 망연동 수단을 설치·운용하여야 한다.

제25조(계약 특수조건) ① 각급기관의 장은 「국가를 당사자로 하는 계약에 관한 법률 시행령」 제76조제1항제3호다목에 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 사항
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 자료인계인수대장을 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 제6의3호까지에 해당하는 사람

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

③ 정보화사업 부서의 장은 제1항에 따라 계약서에 명시된 보안 준수사항의 이행 여부를 정기적으로 점검하고 미비점을 발견한 경우 용역업체가 시정하도록 조치하여야 한다.

④ 각급기관의 정보보안담당관은 용역업체의 보안규정 위반 시 확인서 징구, 보안교육 실시, 보안 위약금 부과, 용역업체 대표자에게 재발방지 대책 마련, 용역업체 직원의 교체를 요구할 수 있다.

⑤ 그 밖에 용역업체 보안과 관련한 사항은 「국가·공공기관 용역업체 보안관리 가이드라인」을 준수하여야 한다.

제27조(소프트웨어 개발보안) 정보화사업 부서의 장은 정보시스템을 개발할 경우 「전자정부법」 제45조 및 「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 보안약점을 진단하여야 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 포함함 관리적·기술적 보안대책을 수립·시행하여야 한다. 이 경우 정보화사업 부서의 장은 보안대책을 수립한 후 각급기관의 정보보안담당관의 승인을 받아야 한다.

② 정보화사업 부서의 장은 용역업체의 원격지 개발과 관련한 보안대책 이행 여부를 정기 또는 수시로 점검(불시 점검 포함)하여야 한다. 이 경우 정보화사업 부서의 장이 점검 후 그 결과를 각급기관의 정보보안담당관에게 통보하여야 한다.

③ 정보화사업 부서의 장은 제2항에 따라 용역업체의 원격지 개발과 관련한 보안대책 이행 여부를 점검한 결과 미흡하다고 판단될 경우 원격지 개발 허가를 취소하여야 한다.

④ 정보화사업 부서의 장은 용역업체가 발주기관 내 장소에서 개발 작업을 수행하더라도 개발용 서버가 민간 클라우드컴퓨팅 서비스를 이용하는 등으로 원격지에 위치할 경우 원격지 개발로 간주하고 제1항에 따른 보안대책을 수립·시행하여야 한다.

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 누출금지정보에 해당하지 아니하면 제공하여야 한다.

② 정보화사업 부서의 장은 제1항에 따라 소프트웨어 산출물을 용역업체에 제공할 경우 업체의 노트북·휴대용 저장매체 등 관련 장비에 저장되어있는 누출금지정보를 완전삭제하여야 하며 업체로부터 누출금지정보가 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 관리·감독에 관한 일반기준」(과학기술정보통신부 고시)을 준수하여야 한다.

제30조(누출금지정보 유출 시 조치) ① 정보화사업 부서의 장은 용역업체가 제안요청서 또는 계약서에 명시된 누출금지정보를 유출한 사실을 알게 된 경우 업체를 대상으로 계약 위반에 따른 조치를 취하여야 한다. 이 경우 용역업체의 누출금지정보 유출 사실을 알게 된 정보화사업 부서의 장 또는 사업과 관계된 공무원 등은 즉시 각급기관의 정보보안담당관을 거쳐 소속 기관의 장에게 보고하여야 한다.

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

제4절 보안적합성 검증

제31조(검증대상 제품) ① 정보화사업 부서의 장은 다음 각 호에 해당하는 제품을 도입하고자 하거나 도입한 경우 실제 적용·운용 이전에 안전성을 확인하기 위하여 보안적합성 검증을 받아야 한다.

1. 상용 정보보호시스템 등 정보보호를 목적으로 도입·운용하는 정보통신제품
2. 각급부서의 장이 자체 개발하거나 업체 등에 의뢰하여 개발한 정보보호시스템

3. 저장매체 소자장비 또는 완전삭제 소프트웨어

4. L3이상 스위치, 라우터 등 네트워크 장비

② 정보화사업 부서의 장은 제1항에도 불구하고 다음 각 호에 해당하는 제품의 경우 보안적합성 검증 절차를 생략할 수 있다. 다만 제1호부터 제4호까지에 해당하는 경우에는 국가정보원장이 해당 인증기관 및 시험기관의 결과를 수용한 제품에 한한다.

1. 「국가정보화 기본법」 제38조제1항 및 동법 시행령 제35조에 따라 과학기술정보통신부장관이 정한 정보보호시스템 공통평가기준을 준수한 인증(이하 "CC인증"이라 한다.) 제도에 따라 국내용 CC인증 또는 국제용 CC인증을 받은 정보통신제품
2. 「소프트웨어산업 진흥법」 제13조에 따른 품질인증(이하 "GS인증"이라 한다.)을 받은 정보통신제품
3. 「정보보호산업의 진흥에 관한 법률」 제17조에 따른 성능평가를 받은 정보통신제품
4. 「국가표준기본법」제23조 및 「공인기관 인정제도 운영요령(국가기술표준원 고시)」제3조에 따른 한국인정기구(KOLAS)(이하"한국인정기구"라 한다.)에 의해 국제표준 (ISO/IES 17025)에 따라 인정받은 시험기관에서 시험한 정보통신제품
5. 국가정보원장이 공지한 검증필 제품목록에 등재된 정보통신제품
6. 국가정보원장이 개발하고 안전성을 확인하여 기술 이전한 정보통신제품

③ 정보화사업 부서의 장은 제2항에도 불구하고 취약점이 발견되거나 보안위협이 제기되는 제품의 경우 보안적합성 검증을 받아야 한다.

제32조(검증 기관) ① 소방청장이 도입하고자 하거나 도입한 제31조제1항에 해당하는 제품은 별도로 위임을 받은 경우를 제외하고 국가정보원장에게 검증을 의뢰하여야 한다.

② 소방청의 소속·산하기관의 장이 도입하고자 하거나 도입한 제31조제1항에 해당하는 제품은 별도로 위임을 받은 경우를 제외하고 소방청장에게 검증을 의뢰하여야 한다

③ 제1항 및 제2항에도 불구하고 국가정보원장 및 소방청장은 필요하다고 판단하는 경우 제31조에 따른 검증신청 기관의 장과 협의하여 해당 기관의 장이 자체적으로 검증을 실시하게 할 수 있다.

제33조(검증 신청) ① 정보화사업 부서의 장은 제31조제1항에 해당하는 제품을 도입할 경우 사전에 소방청 정보보안담당관에게 보안적합성 검증을 신청하여야 한다.

② 제31조에 따라 보안적합성 검증을 받고자 할 경우 제32조에 따른 검증 기관에 다음 각 호에 해당하는 문서·제품 등을 제출하고 검증을 신청하여야 한다.

1. 공통사항

가. 서식 제13호에 따른 보안적합성 검증 신청서

나. 제안요청서 사본(해당하는 경우)

다. 보안기능 운용설명서 등 제품설명서

라. CC인증서 사본(해당하는 경우)

마. 보안기능 점검결과

바. 검증대상 제품(제34조제2항에 따른 시험 단계에서 제출)

2. 네트워크장비

가. 제1호의 공통사항 모두

나. 장비 펌웨어 이미지 및 해시값

다. 서식 제15호에 따른 네트워크 장비 변경 내용 분석서(펌웨어 업데이트 경우에 해당)

3. 자체 개발하거나 업체 등에 의뢰하여 개발한 제품

가. 제1호의 공통사항 모두

나. 기본 및 상세 설계서(검증 기관이 요청할 경우)

다. 개발 완료보고서

③ 제1항에 따라 검증을 신청한 정보화 사업 각급부서의 장은 소방청 정보보안담당관이 필요하다고 판단하여 추가 자료를 요청할 경우 이를 제출하여야 한다.

제34조(안정성 검증) ① 소방청 정보보안담당관은 보안적합성 검증을 효율적으로 수행하기 위하여 제33조에 따라 제출된 문서 내용의 적절성을 검토하여야 한다.

② 소방청청 정보보안담당관은 검증신청 제품에 대하여 보안기능의 정상 작동여부 등 안전성을 시험할 수 있다. 이 경우 소방청 정보보안담당관은 시험에 필요한 추가 자료 및 장비를 요청할 수 있다.

제35조(검증시험 및 결과조치) ① 소방청 정보보안담당관은 제34조에 따른 제품의 안전성 시험을 완료한 경우 적합여부・개선방안 등 검증 결과를 검증신청 기관의 장에게 통보하여야 한다.

② 제1항에 따라 제품의 보안기능 보완 등 개선 조치가 필요하다고 통보받은 각급부서장은 해당조치를 실시하고 그 결과를 소방청청 정보보안담당관에게 통보하여야 한다.

제36조(도입현황 제출) 정보화시스템 운영부서의 장은 매 반기마다 해당 반기 내에 도입한 제31조에 따른 모든 제품에 대하여 서식 제16호에 따른 정보통신제품 도입현황 등을 소방청 정보보안담당관에게 제출하여야 한다.

제37조(무단 변경 및 오용 금지) 정보화사업 부서의 장은 보안적합성 검증이 완료된 시스템의 형상을 무단 변경하거나 도입 목적 이외의 용도로 운용하기 위해서는 국가정보원장에게 보안적합성 검증 여부를 확인하여야 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 한다. 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 포함함 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 정보화담당관과 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 확인하고 갱신하여야 한다.

제39조(정보보호시스템·네트워크장비 보안) ① 각급기관의 장은 침입차단시스템 등 정보보호시스템과 스위치·라우터 등 네트워크장비를 설치·운영하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 물리적으로 안전한 장소에 설치하여 비인가자의 무단접근 통제
2. 기관 외부 정보통신망에서 정보보호시스템·네트워크장비에 대한 원격접속 금지. 다만 기관 내부에서의 원격접속은 보안대책 수립 후 허용
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 장비관리자는 정보보호시스템·네트워크장비의 로그기록을 1년 이상 유지하여야 하고 비인가자의 접속 여부를 정기적으로 점검하여 그 결과를 각급기관 정보보안담당관에게 통보하여야 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 제70조1항에 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 제1항의 보안대책 수립 시 다음 각 호의 사항을 포함하여야 한다.

1. 네트워크 이름(SSID : Service Set Identifier) 브로드캐스팅 중지
2. 추측이 어려운 복잡한 SSID 사용
3. WPA2 이상(256비트 이상)의 암호체계를 사용하여 소통자료 암호화
4. 비인가 단말기의 무선랜 접속 차단 및 무선랜 이용 단말기를 식별하기 위한 IP주소 할당기록 등 유지

5. IEEE 802.1X, AAA(Authentication Authorization Accounting) 등의 기술에 따라 상호 인증을 수행하는 무선랜 인증제품 사용
6. 무선침입방지시스템 설치 등 침입 차단 대책
7. 내부망 정보시스템 또는 인접해 있는 다른 기관의 정보시스템이 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

③ 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 장 등 기술적 보안대책을 수립·시행하여야 한다.

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

제42조(영상회의시스템 보안) ① 각급기관의 장은 영상회의시스템을 구축·운용하고자 할 경우 통신망(국가정보통신망·전용선·인터넷 등) 암호화 등 보안대책을 수립·시행하여야 한다.

② 그 밖의 영상회의시스템 보안과 관련한 사항은 국가정보원장이 배포한「안전한 정보통신 환경 구현을 위한 네트워크 구축 가이드라인」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 다름 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 이

용을 차단하여야 한다.

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) 소방청장은 외국에 사무소를 개설·운용할 경우 소방청 정보보안담당관으로 하여금 해당 사무소의 정보통신망 및 정보시스템에 대한 보안관리 실태를 점검하고 취약요인을 개선하도록 하여야 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 서식 제6호에 따른 정보시스템 관리대장을 수기 또는 전자적으로 작성·관리하여야 한다.

④ 정보시스템 관리책임자는 해당 부서의 서식 제6호에 따른 정보시스템관리대장에 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 개별사용자, 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 반출·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 내부망 및 인터넷망과 분리된 별도의 유지보수 전용

정보통신망 및 전용 단말기를 사용하여야 하며, 외부 정보통신망에서 원격으로 유지 보수하여서는 아니 된다. 다만 불가피한 경우 보안대책 수립 후 각급기관의 정보보안담당관의 승인을 받아 수행하거나 용역업체에게 일정기간 동안 매번 접속 포트(PORT)를 열어주는 방식으로 접속을 허용할 수 있으며 접속 사실이 기록된 로그기록은 1년 이상 보관하여야 한다.

④ 정보시스템 관리자는 정보시스템의 기능 개선·오류 수정 등을 위하여 용역업체를 통한 프로그램 개발이 필요한 경우 용역업체 인원을 해당 기관에 상주시켜 개발 작업을 수행하여야 한다. 프로그램 개발이 완료된 경우에는 정상작동 여부 등 안전성을 확인한 후 적용하여야 한다.

⑤ 각급기관의 장은 소관 정보시스템에 대하여 중요도·가용성 등에 따라 등급을 분류하고 해당 등급에 맞게 정보 보존 및 관리, 장애관리, 보안관리 등을 수행하여야 한다.

⑥ 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(정보시스템 위탁운영 보안) ① 정보시스템 운영부서의 장은 소관 정보시스템에 대하여 외부업체 위탁운영을 최소화하여야 한다. 다만 위탁운영을 할 경우에는 관리적·물리적·기술적 보안대책을 수립·시행하여야 한다.

② 정보시스템의 위탁운영은 다른 기관 또는 외부업체 인원이 소방청(소속기관 포함)에 상주하여 수행하는 것을 원칙으로 한다. 다만, 소방청(소속기관 포함)에 상주가 불가한 경우에는 보안대책 수립 후 그러하지 아니할 수 있다.

③ 그 밖의 정보시스템 위탁운영 보안과 관련한 사항은 제26조(용역업체 보안)을 준용한다.

제49조(서버 보안) ① 소방청 및 소속·산하기관의 정보시스템 운영부서의 장은 서버(정보통신망 포함)의 보안관리를 위하여 서버별로 관리책임자(이하'시스템관리자'라 한다)를 지정 운영하여야 한다.

② 각급기관의 장은 서버를 도입·운용할 경우, 다음과 같이 소방청 정보보안담당관과 협의하여 해킹에 의한 자료 절취, 위·변조 등에 대비한 아래의 보안대책을 수립·시행하여야 한다.

1. 서버 내 저장자료에 대해 업무별 자료별 중요도에 따라 사용자의 접근 권한을 차등 부여
2. 사용자별 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 관리용 서비스와 사용자용 서비스를 분리 운용
4. 서버의 관리용서비스 접속 시 특정 IP와 MAC 주소가 부여된 관리용 단말을 지정 운용
5. 서버 설정 정보 및 서버에 저장된 자료에 대해서는 정기적으로 백업을 실시하여 복구 및 침해행위에 대비
6. 데이터베이스에 대하여 사용자의 직접적인 접속을 차단하고 개인정보 등 중요정보를 암호화하는 등 데이터베이스별 보안조치를 실시

③ 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 유

지・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 통신단말기를 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.

제54조(원격근무 보안) ① 각급기관의 장은 재택・파견・이동근무 등 원격근무를 지원하기 위한 정보시스템을 도입・운영할 경우 기술적・관리적・물리적 보안대책을 수립하여야 한다.

② 각급기관의 장은 원격근무를 지원하기 위하여 원격근무 가능 업무 및 공개・비공개 업무 선정기준을 수립하여야 하고 비밀・대외비를 취급하는 업무는 원격근무 대상에서 제외하여야 한다. 다만 불가피한 경우에는 보안대책 수립 후 소방청 정보보안담당관과 사전 협의하여야 한

다.

③ 각급기관의 장은 모든 원격근무자에게 보안서약서를 징구하고 원격근무자의 보직변경·퇴직 등 상황 발생 시 정보시스템 접근권한 조정 등 관련 절차를 수립하여야 한다.

④ 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.

⑤ 원격근무자는 원격근무용 단말기 고장 등으로 단말기를 정비 또는 반납하고자 할 경우 자료유출 방지 등 보안대책 수립 후 각급기관 정보보안담당관과 협의하여 관련 조치를 하여야 한다.

⑥ 각급기관 정보보안담당관은 비공개 업무와 관련한 원격근무의 경우에는 안전성이 확인된 상용 암호모듈을 사용하여 소통자료를 암호화하고 행정전자서명체계(GPKI)를 이용하여 일회용 비밀번호·생체인증 등 보안기술을 적용하여야 한다.

⑦ 각급기관의 정보보안담당관은 원격근무와 관련한 보안대책 이행 여부를 정기적으로 점검·보완하여야 한다.

제55조(정보시스템 저장자료의 보안조치 책임) 정보시스템 운영부서의 장은 정보시스템을 폐기·양여·교체·반납(이하 "불용처리"라 한다)하거나 외부 수리를 위하여 기관 외부로 반출할 경우 저장매체에 보관된 자료의 삭제 등 보안조치에 대한 책임을 진다.

제56조(국제회의 보안) ① 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 국가정

보원장이 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 처리 할 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 있다.

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 국가정보원장이 안전성을 확인한 상용 암호모듈을 사용하여 위조·변조·훼손 및 유출 등을 방지하기 위한 보안대책을 강구하여야 하며, 보호기간이 만료된 대외비는 「국가정보보안 기본지침」제66조 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. 소속 또는 근무 중인 기관의 장이 자체적으로 구축·운용하는 전자우편시스템(이하 "기관 전자우편"이라 한다), 공무원 등이 공동으로 사용할 목적으로 문화체육관광부장관이 구축·운용하는 전자우편시스템(이하 "공직자통합메일"이라 한다) 및 공무원 등이 다른 공무원 등과 자료를 공유하거나 소통하기 위하여 사용하는 전용(專用) 소프트웨어(이하 "공공 전용(專用) 메신저"라 한다)를 이용한 수·발신
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. 기관 전자우편, 공직자통합메일 또는 공공 전용(專用) 메신저의 발신 기능을 이용하여 비공개 대상 정보의 주요내용이 기술된 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. 기관 전자우편, 공직자통합메일 또는 공공 전용(專用) 메신저의 발신 기능을 이용하여 비공개 대상 정보의 주요내용이 기술된 문장 또는 문구 작성
2. 기관 전자우편, 공직자통합메일 또는 공공 전용(專用) 메신저로 수·발신하는 과정에서의 일시적 저장
3. 국가정보원장이 안전성을 확인한 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 처리하여서는 아니 된다.

⑤ 공무원등은 제2항부터 제4항까지에 따라 작성·저장한 비공개 업무자료는 활용 후 즉시 삭제하여야 한다.

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

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 각종 정보통신기기 및 서비스를 활용하여 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 「국가 정보보안 기본지침」 제71조제1항 각 호에 해당하는 자료는 비밀로 분류·관리하여야 하며 「국가 정보보안 기본지침」 제2항 각 호에 해당하는 자료는 비공개로 지정·관리하여야 한다.

② 각급기관의 장은 제1항에도 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 「국가 정보보안 기본지침」 제72조제1항 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

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(암호자제 및 암호알고리즘 등) ① 각급기관의 장은 비밀 또는 중요자료를 소통·보호하고자 할 경우 국가정보원장이 개발하거나 안

전성을 확인한 암호자재 또는 암호알고리즘(중요자료 소통・보호에 한함)을 사용하여야 한다.

② 제1항에 따른 암호자제 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 서식 제6호의 정보시스템 관리대장에 적어서 관리하여야 한다.

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

1. CMOS・로그온・자료 암호화 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 이

상 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 컴퓨터바이러

스・트로이목마 등 악성코드로부터 보호하기 위하여 백신 소프트웨어 설치, 해켕메일차단시스템 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 각급부서 장은 휴대용 저장매체를 비밀용・일반용으로 구분하여 [서식 제21호] 및 [서식 제22호]와 같이 관리대장에 기록하고, 휴대용 저장매체에 [서식 제25호]의 라벨과 같이 기입・표시하여야 한다. 각급부서장은 휴대용 저장매체 수량 및 보관 상태 등을 정기적으로 [서식

제23호]와 같이 점검하여야 하고, 외부 반출・입 시 [서식 제24호]와 같이 기록・관리하여야 하며, 휴대용 저장매체 무단 반출 및 미등록 저장매체 사용을 사전 통제하여야 한다.

⑤ 각급부서 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 각급부서 장은 휴대용 저장매체의 용도 변경, 폐기・불용 처리하고자 할 경우 저장자료가 복구 불가하도록 완전삭제 소프트웨어 등을 이용하여 삭제하여야 한다. 다만, 완전삭제가 불가할 경우 파쇄하여야 한다.

⑦ 각급부서 장은 제6항에 따른 휴대용 저장매체 불용처리 시 [별표 제5호]에 따른 기준 이상으로 자료를 삭제하여야 하며, 휴대용 저장매체를 불용처리하거나 재사용 시 [서식 제26호]에 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 「국가공무원 복무·징계 관련 예규」(인사혁신처) 제12장 및「소방공무원 징계양정 등에 관한 규칙」을 참고하여 정보보안 위규자를 처리한다.

제5절 주요 정보통신기반시설 보호

제77조(보호대책 수립) ① 소방청 정보보안담당관은「정보통신기반보호법」제5조 및 같은 법 시행령 제8조에 따라 주요정보통신기반시설(이하 "주요기반시설"이라 한다)에 대한 보호대책을 수립·시행하여야 한다.

② 소방청 정보보안담당관은 제1항에 따른 보호대책을 수립하는 경우에 다음 각 호의 사항이 포함되도록 하고, 전년도 추진실적 평가 및 문제점에 대한 개선사항을 다음 연도 보호대책에 반영하여야 한다.

1. 소관 주요기반시설 현황 및 보호 목적
2. 전년도 보호업무 추진실적 및 해당 연도 추진계획
3. 보안취약점 분석·평가 결과 및 도출된 문제점에 대한 개선사항
4. 「정보통신기반 보호법」제2조제2호에 따른 전자적 침해행위 예방을 위한 관리적·물리적·기술적 보안대책
5. 「정보통신 기반 보호법」 제2조제3호에 따른 침해사고가 발생할 경우 대응 및 복구대책

③ 소방청 정보보안담당관은 매년 소관 주요기반시설의 지정 범위 및 기능변경 여부를 평가하여 변경사항을 보호대책에 반영하여야 한다.

제78조(취약점 분석·평가 보안관리) ① 기반시설 관리부서의 장은「정보통신기반보호법」제9조제3항에 각 호의 기관에 주요기반시설의 취약점 분석·평가를 의뢰하고자 할 경우 정보통신망 구성도 등 중요자료의 유출 방지 등을 위한 보안대책을 수립·시행하여야 한다.

② 기반시설 관리부서의 장은 제1항에 따른 취약점 분석·평가를 완료한 경우에는 취약점 분석·평가 결과물에 대하여 적절성을 검증하여야 한다.

③ 기반시설 관리부서의 장은 제2항에 따른 취약점 분석·평가 결과물을 중요성 및 가치의 정도에 따라 비밀 또는 비공개 대상 정보로 지정·관리하고 인터넷이나 학회지 등 외부에 공개하거나 발표하여서는 아니 된다. 다만, 기술 교류나 학문 연구 등을 목적으로 하는 비공개 회의 등의 경우에는 자체 보안성 검토를 거친 후 발표할 수 있다.

④ 기반시설 관리부서의 장은 취약점 분석·평가의 효율적 수행을 위하여 필요한 경우 소방청 정보보안담당관을 경유하여 국가정보원장에게 평가 방향, 평가중점사항, 평가결과 적절성 검증, 평가업체 보안점검 등의 지원을 요청할 수 있다.

제4장 융합보안

제1절 정보통신시설 및 기기 보호

제79조(정보통신시설 보안) ① 각급기관의 장은 다음 각 호의 어느 하나에 해당하는 정보통신시설 및 장소를 「보안업무규정」 제32조에 따른 보호구역으로 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 보호구역으로 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 전력관리 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」 제32조에 따른 보호구역으로 지정·관리하고 출입통제 장치를 운용하여야 한다.

③ 각급기관의 장은 영상정보처리기기를 인터넷과 분리·운용하여야 한

다. 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 「CCTV 시스템 보안관리방안」 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.

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 복합기 설치·운용할 경우「국가 정보보안 기본지침」제91조제3항 각 호에 해당하는 경우 복합기의 저장매체에 저장된 자료를 완전 삭제하여야 한다.

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 재난방지 대책을 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 최대화 할 수 있도록 하여야 한다.

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

제2절 전자파 보안

제85조(대도청측정) ① 소방청 정보보안담당관은 다음 각 호의 어느 하나에 해당하는 시설·장소에 대하여 각종 수단에 의한 도청으로부터 정보유출을 방지하기 위한 보안대책(TSCM)을 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「국가 정보보안 기본지침」제93조제1항 각 호에 해당하는 시설·장소에 대하여 자체 또는「통신비밀보호법」제10조의3에 따른 불법감청설비탐지업자 활용 등을 통해 대도청 측정을 실시하

여야 한다.

③ 제2항에도 불구하고「국가 정보보안 기본지침」제93조제2항 각 호에 해당하는 시설·장소에 대하여는 국가정보원장에게 대도청 측정을 요청할 수 있다.

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

⑦ 기타 대도청 측정과 관련한 사항은 국가정보원장이 배포한「도청 탐지·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 개발하거

나 안전을 확인한 암호자재 사용

3. 무선국 현황 관리 및 정기적인 전파 감시·측정

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 1.20까지 제출하고 전파측정 실시 후 20일 이내에 서식 제5호에 따른 결과보고서를 제출하여야 한다.

제87조(고출력 전자파 보안) ① 주요기반시설 부서의 장은 소관 주요기반시설을 고출력 전자파(EMP)로부터 안전하게 보호하기 위한 예방·백업·복구등 물리적·기술적 대책을 포함한 보호대책을 수립·시행할 수 있다.

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

제5장 훈련·평가 및 위협 탐지·대응

제1절 훈련 및 진단

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

실시하여야 한다.

② 국가정보원장은 국가차원의 사이버위기 발생에 대비하여 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망을 대상으로 사이버공격 대응훈련을 실시할 수 있다.

③ 제2항에 따른 대응훈련은 「비상대비자원 관리법」 제14조에 따른 비상대비훈련과 함께 실시할 수 있다.

제89조(정보통신망 보안진단) 소방청 정보보안담당관은 정보통신망을 대상으로 취약점을 진단하는 제반활동(이하 "보안진단"이하 한다.)을 매년 정기적으로 실시하거나 관련 예산확보 등을 위하여 노력하여야 한다.

제2절 정보보안 관리실태 평가

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

② 소방청 정보보안담당관은 자체평가의 적절성을 입증하기 위하여 필요하다고 판단하는 경우 평가지표별 증빙자료를 국가정보원장에게 제출할 수 있다.

제91조(현장실사 및 결과 통보) ① 소방청장은 국가정보원장이 정보보안 관리실태 자체평가 결과를 검증하기 위한 현장실사에 대하여 증빙자료 제출, 담당자 면담 등에 협조하여야 한다.

② 소방청장은 제1항에 의한 현장실사를 거쳐 통보받은 정보보안 관리 실태 평가 결과를 해당 기관의 장에게 통보하고 평가결과를 통보받은 기관의 장은 평가결과에 따른 미비점을 개선·보완하여 정보보안 수준을 제고하여야 한다.

제3절 보안관제

제92조(사이버보안관제센터 설치·운영) ① 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 별표2의 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 이 훈령에 대하여 2020년 5월 20일을 기준으로 매 3년이 되는 시점마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부 칙

이 훈령은 발령한 날부터 시행한다.

별 표

< 별표 1 >

정보통신보안 규정 위반사항

내용	세부내용
1. 적성국과의 통신	가. 적성국 인터넷망과의 메시지 또는 자료 송수신 나. 적성국의 국내외 인터넷 거점(경유지를 포함한다)과의 통신 다. 적성국의 국내외 인터넷 거점(경유지를 포함한다)에서 공직자 상용메일 불법 접속 라. 적성국의 인터넷 사회관계망서비스(SNS) 사용계정과의 메시지 또는 자료 송수신
2. 정보통신망을 통한 군사상 기밀의 누설 또는 유출	가. 군사전략, 작전계획 및 진행사항의 누설 또는 유출 나. 군 편제·임무·시설 및 그 밖의 부대현황의 누설 또는 유출 다. 병력(군·경·예비군) 현황 및 이동 상황의 누설 또는 유출 라. 경찰 및 특수기관의 장비(작전·정보·수사용) 현황과 집행 사항의 누설 또는 유출 마. 특수기관·군사시설의 위치 및 이동상황의 누설 또는 유출 바. 군사장비의 구성·성능 및 발명개량 연구사항의 누설 또는 유출 사. 군사장비(군수품 등) 생산 및 공급사항의 누설 또는 유출 아. 그 밖에 국가방위에 영향을 초래하는 사항의 누설 또는 유출
3. 정보통신망을 통한 외교상 기밀의 누설 또는 절취	가. 국가 외교방침, 기본계획 및 재외공관에 발하는 훈령의 누설 또는 유출 나. 공개할 수 없는 외교조약 또는 협약의 누설 또는 유출 다. 특수임무를 수행하는 해외주재원의 활동(계획·지시·보고) 및 신원정보와 관련된 사항의 누설 또는 유출 라. 그 밖에 국가외교에 영향을 초래하는 사항의 누설 또는 유출

내용	세부내용
4. 정보통신망을 통한 국가정보활동 관련 사항의 누설 또는 절취	가. 대공업무와 관련된 사항의 누설 또는 유출 나. 정보(첩보) 수집활동에 필요한 사항의 누설 또는 유출 다. 간첩 또는 대공용의자 발견과 수사활동의 누설 또는 유출 라. 정보 및 특수 수사기관의 기구 또는 임무기능 관련 사항의 누설 또는 유출 마. 국가원수 및 그 밖의 요인의 비공개행사의 누설 또는 유출 바. 불명선박의 발견 및 처리의 누설 또는 유출 사. 중요물자 수송활동의 누설 또는 유출 아. 테러·마약·밀수 및 국제범죄조직 관련 정보·수사활동의 누설 또는 유출 자. 적 또는 경쟁국에 유리한 과학기술 및 산업 관련 정보의 누설 또는 유출 차. 그 밖에 국가안보 및 공안유지에 불리한 영향을 초래하는 사항의 누설 또는 유출
5. 암호자재 관련 사항	가. 암호자재의 연구개발 및 제작에 필요한 사항 누설 나. 암호전문을 허위로 조립하여 송신 다. 암호를 부정한 목적에 사용 라. 암호문과 암호화되지 아니한 평문의 혼용 및 이중사용 마. 암호문 작성시 동일 난수를 2회 이상 반복사용 바. 사용기간이 경과된 암호자재를 계속 사용 사. 암호문에 암호화되지 아니한 평문을 삽입하여 송신 아. 그 밖에 암호자재 보호체계를 손상시킬 우려가 있는 사항 누설

내용	세부내용
6. 전자정보	가. 주전산기(주요 서버 등)·대용량 전자기록(DB)의 손괴 나. 전자정보의 위조·변조·훼손
7. 정보통신망 및 정보통신시스템 관련 사항	가. 정보통신망에 대한 불법침입, 해킹·악성코드의 유포 나. 중요 정보시스템 및 정보통신실 파괴 다. 중요 정보시스템 기능 장애 및 정지
8. 비인가 통신시설 및 통신제원 사용에 필요한 사항	가. 비인가된 무선시설의 설치·운용 나. 비인가된 무선시설과 교신 다. 비인가된 호출부호 및 주파수 사용 라. 비인가된 전파형식 사용 마. 지정출력의 초과사용
9. 허가목적 외의 방법으로 사용하는 경우	가. 허가목적 업무와 관련이 없는 통신 나. 군 통신망에서 군사업무와 관련이 없는 통신 다. 그 밖에 사회질서를 해치는 통신

< 별표 2 >

정보보안 사고 유형

구 분	세 부 내 용
1. 전자정보 (전자문서 및 전자기록물)	가. 비밀의 유출 나. 주전산기(주요 서버 등)·대용량 전자기록(DB) 손괴 다. 전자정보의 위조·변조·훼손 및 유출 라. PC 등 단말기內 비밀의 평문 보관 및 유통
2. 정보시스템 및 정보통신실	가. 정보통신망에 대한 해킹·악성코드의 유포 나. 비밀이 저장된 PC, 휴대용 저장매체 등 분실 다. 정보시스템 및 정보통신실 파괴 라. 고의적 중요 정보시스템 기능 장애 및 정지 마. 상용메일·메신저 등을 통한 업무자료 무단 소통 바. 업무자료의 무단 반출 사. 첨단 정보통신기기를 통한 업무자료 무단 소통
3. 암호장비	가. 암호장비 분실 및 피탈 나. 암호장비 파손 및 임의파기 다. 암호장비 복제·복사 라. 비인가 암호장비 사용 마. 암호장비 비닉체계 특성 및 제원 노출 바. 암호장비 키 운용체계 노출
4. 암호자재	가. 암호자재의 분실 및 누설 나. 암호자재의 파손 및 임의파기 다. 암호자재의 임의제작 사용 라. 세부 암호체계 노출

< 별표 3 >

정보보호시스템 유형별 도입요건

제품유형	도입 요건	비고
침입차단시스템(FW) 침입방지시스템(침입탐지 포함) 통합보안관리제품 웹 응용프로그램 침입차단제품 서버 접근통제제품 DB 접근통제제품 네트워크 접근통제제품 인터넷전화 보안제품 무선침입방지시스템 무선랜 인증제품 가상화 제품 네트워크 자료유출 방지제품 디지털 복합기 스마트폰 보안관리제품	CC인증	EAL 2 이상 또는 관련 PP 준수
스마트카드		EAL 4 이상
가상사설망제품 소프트웨어기반 보안USB 호스트 자료유출 방지제품	CC인증 및 검증필 암호모듈	EAL 2 이상 또는 관련 PP 준수 검증필 암호모듈 필히 적용
스팸메일차단시스템 패치관리시스템 망간자료전송제품	CC인증 또는 국가용 보안요구사항 준수 GS인증	CC인증시 : EAL 2 이상 또는 관련 PP준수 - GS인증시 : ISO 25023 및 국가용 보안요구사상 준수
DDos 대응제품 안티바이러스제품 소스코드 보안약점 분석도구	CC인증 또는 국가용 보안요구사항 준수 성능평가	- CC인증시 : EAL 2 이상 또는 관련 PP 준수 - 성능평가시 : 국가용 보안요구 사항 준수
행정기관용 인터넷전화	TTA verified ver4 이상	
그 밖의 정보보호제품		CC인증 및 검증필 암호모듈 탑재 권고

* 최신 도입요건은 국가정보원 홈페이지(보안적합성 검증) 참조

< 별표 4 >

암호가 주기능인 제품 도입요건

제품유형	도입 요건	비고
메일 암호화제품	검증필 암호모듈 탑재	
구간 암호화제품		
하드웨어 보안토큰		
디스크·파일 암호화제품		
그 밖의 암호화제품		
SSO 제품	검증필 암호모듈 탑재 및 CC인증	CC인증시 : 관련 PP 준수
DB 암호화제품		
문허 암호화제품(DRM 등)		

* 최신 도입요건은 국가정보원 홈페이지(암호모듈 검증) 참조

< 별표 5 >

정보시스템 저장매체·자료별 삭제방법

저장 자료 / 저장 매체	공개 자료	비공개 자료	대외비 자료	비밀 자료
자기테이프 플로피디스크	분임정보보안담당관 판단	물리적 파괴	물리적 파괴	물리적 파괴
광디스크 (CD·DVD 등)	분임정보보안담당관 판단	물리적 파괴	물리적 파괴	물리적 파괴
반도체메모리 (SSD·USB 등)	포맷 또는 삭제	물리적 파괴	물리적 파괴	물리적 파괴
하드디스크	포맷 또는 삭제	디가우징 또는 완전삭제 S/W	물리적 파괴	물리적 파괴

* 불용처리시 위 분류에 따른 기준 이상으로 삭제

* 물리적 파괴는 소각·파쇄·용해 등을 말함

* 디가우징 또는 완전삭제 S/W는「국가 정보보안 기본지침」제31조(검증대상 제품)에 따라 보안적합성을 검증받았거나 국가정보원이 인정하는 인증을 받은 제품에 한함

< 별표 6 >

사업자 정보보안 위규 처리기준

구 분	위 규 사 항	처 리 기 준
심 각	1. 비밀 및 대외비 급 정보 유출 및 유출시도 가. 정보시스템에 대한 구조, 데이터베이스 등의 정보 유출 나. 개인정보·신상정보 목록 유출 다. 비공개 항공사진·공간정보 등 비공개 정보 유출 2. 정보시스템에 대한 불법적 행위 가. 관련 시스템에 대한 해킹 및 해킹시도 나. 시스템 구축 결과물에 대한 외부 유출 다. 시스템 내 인위적인 악성코드 유포	◦사업참여 제한 ◦위규자 및 직속 감독자 등 중징계 ◦재발 방지를 위한 조치계획 제출 ◦위규자 대상 특별 보안교육 실시
중 대	1. 비공개 정보 관리 소홀 가. 비공개 정보를 책상 위 등에 방치 나. 비공개 정보를 휴지통·폐지함 등에 유기 또는 이면지 활용 다. 개인정보·신상정보 목록을 책상 위 등에 방치 라. 기타 비공개 정보에 대한 관리소홀 마. 참여인원에 대한 보안서약서 미징구 및 교육 미실시 2. 사무실(작업장) 보안관리 허술 가. 출입문을 개방한 채 퇴근 등 나. 인가되지 않은 작업자의 내부 시스템 접근 다. 통제구역 내 장비·시설 등 무단 사진촬영 3. 전산정보 보호대책 부실 가. 업무망 인터넷망 혼용사용, USB 등 보조기억매체 기술적 통제 미흡 나. 웹하드·P2P 등 인터넷 자료공유사이트를 활용하여 용역사업 관련 자료 수·발신 다. 개발·유지보수 시 허가받지 않은 원격작업 실시 라. 저장된 비공개 정보 패스워드 미부여 마. 인터넷망 연결 PC 하드디스크에 비공개 정보를 저장 바. 외부용 PC를 업무망에 무단 연결 사용 사. 비공개 자료가 포함된 저장매체(전산장비 포함) 무단 반출 아. 보안관련 프로그램 강제 삭제 자. 제공된 계정관리 미흡 및 오남용(시스템 불법접근 시도 등) 차. 바이러스 백신 정품 S/W 미설치	◦위규자 및 직속 감독자 등 중징계 ◦재발 방지를 위한 조치계획 제출 ◦위규자 대상 특별보안교육 실시

구 분	위 규 사 항	처 리 기 준
보 통	1. 기관 제공 중요정책·민감 자료 관리 소홀 가. 주요 현안·보고자료를 책상위 등에 방치 나. 정책·현안자료를 휴지통·폐지함 등에 유기 또는 이면지 활용 다. 중요정보에 대한 자료 인수·인계 절차 미 이행 2. 사무실 보안관리 부실 가. 캐비닛·서류함·책상 등을 개방한 채 퇴근 나. 출입키를 책상위 등에 방치 3. 보호구역 출입 소홀 가. 통제·제한구역 출입문을 개방한 채 근무 나. 보호구역내 비인가자 출입허용 등 통제 불순응 4. 전산정보 보호대책 부실 가. 휴대용저장매체를 서랍·책상 위 등에 방치한 채 퇴근 나. 비인가 메신저 무단 사용 다. PC를 켜 놓거나 보조기억 매체(CD, USB 등)를 꽂아 놓고 퇴근 라. 부팅·화면보호 패스워드 미부여 또는 "1111" 등 단순숫자 부여 마. PC 비밀번호를 모니터 옆 등 외부에 노출 바. 비인가 저장매체(전산장비 포함) 무단 사용 사. 정보시스템 반입시 바이러스 백신 미검사 또는 반출시 자료 삭제 미확인 아. 바이러스 백신 최신 업데이트 또는 정밀점검 미실시	◦위규자 및 직속 감독자 등 경징계 ◦위규자 및 직속 감독자 사유서 /경위서 징구 ◦위규자 대상 특별 보안교육 실시
경 미	1. 업무 관련서류 관리 소홀 가. 진행중인 업무자료를 책상 등에 방치, 퇴근 나. 복사기·인쇄기 위에 서류 방치 2. 근무자 근무상태 불량 가. 각종 보안장비 운용 미숙 나. 경보·보안장치 작동 불량 3. 전산정보 보호대책 부실 가. PC내 보안성이 검증되지 않은 프로그램 사용 나. 보안관련 소프트웨어의 주기적 점검 위반 다. PC 월1회 보안 점검 미이행	◦위규자 서면·구두 경고 등 문책 ◦위규자 사유서 / 경위서 징구

* 정보화용역사업에서 취급하는 정보의 중요도 등 사업 실정에 따라 처리기준을 달리 정할 수 있음

※ 사업자 보안위규시 각급부서 처리 절차

경위 확인 ▶ 보안위규 처리기준에 따라 조치 ▶ 재발방지 대책 ▶ 보안조치 이행여부 점검

< 별표 7 >

보안 위약금 부과 기준

1. 사업규모 및 위규수준 등을 고려하여 차등 부과

가. 사업 예산이 1억원 이상인 경우 : 계약금액의 비율로 위약금 부과

구분	위규 수준			
	A급	B급	C급	D급
위규	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금/처분	부정당업자 등록	건당 계약금액의 5%	계약금액의 3%	계약금액의 1%

나. 사업 예산이 1억원 미만인 경우 : 정액으로 위약금 부과

- 사업 예산이 3천만원 이상인 경우

구분	위규 수준			
	A급	B급	C급	D급
위규	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금/처분	부정당업자 등록	건당 100만원	50만원	경고조치

- 사업 예산이 3천만원 미만인 경우

구분	위규 수준			
	A급	B급	C급	D급
위규	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금/처분	부정당업자 등록	50만원	경고조치	주의조치

2. 보안 위약금 및 처분은 다른 요인에 의해 상쇄나 삭감 불가

3. 위약금은 사업 종료 시 또는 기성대금 지급 시 지출금액 조정을 통해 정산

< 별표 8 >

용역업체 보안교육 내용

예 시 ※ 각 용역사업 환경에 맞게 교육내용 수정하여 자체 교재제작 및 교육실시

1. 공통사항

- 제안요청서에 명시한 '누출금지 대상정보' 및 '보안위반 처리기준' 을 반드시 숙지

※ 해당 정보 누출시 국가계약법 시행령 제76조에 따라 사업자를 부정당업체로 등록

- 사업자는 발주기관의 보안정책을 위반하였을 경우 위규처리 기준 및 위약금 부과기준에 따라 위규자 및 관리자를 행정조치하고 손해배상 책임

2. 인적 보안관리

- 인사혁신처 정보보호 정책 준수
- 사업 참여시 보안서약서 제출
- 참여인원 중 용역책임자를 보안책임관으로 지정·관리
- 참여인원 교체 시 발주기관의 사전 승인
- 용역사업 시작 전 참여인원에 대한 비밀유지의무 준수 등 교육 실시

3. 사무실 보안관리

- 퇴근 시에는 캐비닛 등을 잠그고 보안 상태 확인
- 사업관련 문서, 외장저장매체는 책상, 프린터 등에 방치 금지
- 퇴근 시에는 PC 및 장비의 전원을 OFF 시킬 것
- 일과시간 이외 근무시 발주기관의 사전 승인
- 업무를 수행할 장소는 외부인의 출입을 통제

4. 전산장비 보안관리

- 정보시스템 관리대장 및 전산장비 반출·입 대장을 지속적으로 관리

- CMOS 및 Windows 패스워드를 설정하고 화면보호기 잠금 기능을 사용하여 비인가자의 접근을 차단
- 백신 및 악성코드 방지 프로그램을 반드시 설치하고, 최신 업데이트 유지
- PC점검툴(내PC지키미 등)을 설치하고, 월1회 이상 점검 실시
- 휴대용 저장매체 사용 금지, 다만 업무에 꼭 필요한 경우 발주기관의 사전 승인
- 보안스티커 훼손 금지, 훼손시 발주기관에 즉시 신고
- 비인가 단말기 반입 금지, 사용 장비 무단반출 금지
- 허가받지 않은 하드웨어 및 소프트웨어의 임의 설치 불가

※ 원격접속SW, 게임, 증권, 웹하드, 메신저, p2p 등

5. 네트워크 보안관리

- 발주기관 내부망에 대한 접속은 반드시 발주기관 사전 승인후 접속
- 인터넷 연결을 원칙적으로 금지

※ 다만, 사업 수행상 필요 한 경우, 사업체의 보안책임관이 접속이 필요한 PC와 웹사이트·서버 등을 선정, 발주기관 보안담당자의 승인을 득한 후 사용

6. 자료 보안관리

- 계약서에 명시된 누출금지대상 자료 확인하고, 자료관리대장을 통해 관리
- 누출금지대상 자료는 지정된 사용자만 접근이 가능하도록 하고 다른 자료와 구분하여 보관, 비밀번호를 설정하거나 암호화 기능 사용
- 상용이메일 · 웹하드 · P2P 사용 금지, 기관메일의 경우 발주기관 보안담당자의 승인을 득한 후 사용, 첨부자료는 암호화
- 사업과정에서 생산된 모든 산출물은 발주기관 내 설치된 파일서버 또는 발주기관 보안담당자가 지정한 PC에서만 저장·관리
- 사업 수행시 생산된 산출물 및 기록은 발주기관이 인가하지 않은 자에게 제공·대여·열람 금지

서 식

[서식 제1호]

대 외 비		
원 본	보호기간 : 20 . . .	보존기간 : 년
사 본	20 . . .	

보안심사위원회 심의요구서

(의안번호 제 호)

제 목	
회 부 근 거	
회 부 기 관	
주 요 내 용	
요 구 자 의 의 견	

붙임서류 :

위와 같이 보안심사위원회 심의를 요구합니다.

20 . .

심의요구자 직위

성명 (서명, 인)

보안심사위원회 위원장 귀하

210㎜×297㎜(백상지 80g/㎡)

[서식 제2호]

대 외 비		
원 본	보호기간 : 20 . . .	보존기간 : 년
사 본	20 . . .	

보안심사위원회 회의록(갑)

○ 일 시 :

○ 장 소 :

○ 참 석 자 :

○ 안 건 :

○ 회부기관 :

발 언 자	내 용

210㎜×297㎜(백상지 80g/㎡)

회 의 록 (을)

발 언 자	내 용

210㎜×297㎜(백상지 80g/㎡)

[서식 제3호]

대 외 비		
원 본	보호기간 : 20 . . .	보존기간 : 년
사 본	20 . . .	

보안심사위원회심의결정서

(의안번호 제 호)

개 최 일 시	
장 소	
안 건	
회 부 기 관	
결 정 주 문	
결 정 이 유	별 첨

위 주문과 같이 심의 결정함.

20 . . .

위 원 장 (서명, 인)

부위원장 (서명, 인)

위 원 (서명, 인)

〃 (서명, 인)

〃 (서명, 인)

〃 (서명, 인)

〃 (서명, 인)

〃 (서명, 인)

간 사 (서명, 인)

210㎜×297㎜(백상지 80g/㎡)

[서식 제4호]

정보보안업무 세부 추진계획

< 작성 요령 >

1. 활동 목표
2. 기본 방침
3. 세부 추진계획

분야별	사업명	세부 추진계획	주관・관련부서	비고

* 보안성검토 대상여부 표기

4. 전년도 보안감사・지도방문 시 도출내용과 조치내용

도 출 내 용	조 치 내 역	담당부서

* 형식위주의 계획수립을 지양하고 소속 및 산하기관의 추진계획을 종합, 자체 실정에 맞게 작성

210㎜×297㎜<일반용지 60g/㎡(재활용품)>

[서식 제5호]

전파측정 활동 결과보고

1. 일반 사항

o 측정기간 및 지역

o 측정장비

o 참여기관 및 인원

2. 측정결과 내용

기간	측정지점	통신구간	주파수 (MHz)	신호세기 (dBM)	취약여부	비고
						디지털/ 아날로그 구분

3. 분석 및 평가

4. 조치 및 대책

210㎜×297㎜<일반용지 60g/㎡(재활용품)>

[서식 제6호]

정보시스템 관리대장

부서명 :

연번	소속	취급자 성명	종류 (서버·PC 등)	제조사	모델명	관리번호 (IP등)	도입일자	비고

○ 「종류」: 업무망PC, 인터넷망PC, 서버, 노트북 등으로 구분

210㎜×297㎜<일반용지 60g/㎡(재활용품)>

[서식 제7호]

암호실 및 암호 취급자 현황

구분 / 부서	암호실				암호취급자				비고
	인가	운용	과부족	변동 내용	인가	운용	과부족	변동 내용	
총계									

210㎜×297㎜<일반용지 60g/㎡(재활용품)>

[서식 제8호]

암호실(통제구역)출입자 기록부

출입일시	소속	직책	직급/성명	용무	서명	인가자인	비고

210㎜×297㎜<일반용지 60g/㎡(재활용품)>

[서식 제9호]

서 약 서(개인용)

본인은 년 월 일부로 소방청 국가용 보안시스템(정보시스템 포함)과 관련한 업무(연구개발, 제작, 입찰, 기타)를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 국가용 보안시스템(정보시스템 포함)과 관련된 소관업무가 국가기밀 사항임을 인정하고 제반 보안관계규정 및 지침을 성실히 준수한다.
2. 나는 이 기밀을 누설함이 이적행위가 됨을 명심하고 재직 중은 물론 퇴직 후에도 알게 된 모든 기밀사항을 타인에게 누설하지 아니한다.
3. 나는 기밀을 누설한 때에는 아래의 관계법규에 따라 엄중한 처벌을 받을 것을 서약한다. 다만, 부패행위 신고 및 공익신고 등의 경우 비밀준수 의무를 위반하지 않은 것으로 본다.

   가. 국가보안법 제4조 제1항 제2호·제5호(국가기밀 누설 등)
   나. 형법 제99조(일반이적) 및 제127조(공무상 비밀의 누설)
   다. 군형법 제80조(군사기밀 누설)
   라. 군사기밀보호법 제12조(누설) 및 제13조(업무상 누설)

년 월 일

서약자 소속 직급
직위 성 명 서명 또는 인

서 약 소속 직급
집행자 직위 성 명 서명 또는 인

210mg×297mm<백상지80g/m2>

[서식 제10호]

암호자재 운용관리 현황

기관명 :　　년　　월　　일 현재

자재명	기관번호	일련번호	제작년월	설치장소	상대국소	설치일자	비고

210㎜×297㎜<일반용지 60g/㎡(재활용품)>

[서식 제11호]

암호자재 관리기록부

자재 명칭	등록 번호	제 작		수령(배부)				회수			반납				비고
		일자	수량	일자	수량	증빙 번호	대상 기관	일자	수량	증빙 번호	일자	수량	증빙 번호	확인	

210㎜×297㎜<일반용지 60g/㎡(재활용품)>

[서식 제12호]

암호자재취급자 인감등록서

1. 기관 및 부서명 :

2. 변동 및 등록일자 : 년 월 일

가. 정 책임자

인 적 사 항		인 감	서 명
직 급 및 성 명			
직 책			
생 년 월 일			
비밀취급등급			

나. 부 책임자

인 적 사 항		인 감	서 명
직 급 및 성 명			
직 책			
생 년 월 일			
비밀취급등급			

다. 실무자

인 적 사 항		인 감	서 명
직 급 및 성 명			
직 책			
생 년 월 일			
비밀취급등급			

210mg×297mm<백상지80g/m²>

[서식 제13호]

보안적합성 검증 신청서

<table>
<tr><td rowspan="8">신청기관</td><td>기관명</td><td colspan="3"></td><td>부서</td><td></td></tr>
<tr><td></td><td colspan="3"></td><td>담당자</td><td></td></tr>
<tr><td></td><td colspan="3"></td><td>담당자
전화번호</td><td></td></tr>
<tr><td>도입목적</td><td colspan="5"></td></tr>
<tr><td>사업명</td><td colspan="5"></td></tr>
<tr><td>보안성
검토</td><td colspan="3"></td><td>계약날짜</td><td></td></tr>
<tr><td></td><td colspan="3"></td><td>도입날짜</td><td></td></tr>
<tr><td>유지보수</td><td colspan="5">보안적합성 검증결과 반영여부(□ 반영·개선 □ 반영불가)</td></tr>
<tr><td>공인인증
대상확인</td><td colspan="5">□CC인증 □GS인증 대체가능 □성능평가 대체가능
□검증필 암호모듈 □해당사항 없음</td></tr>
<tr><td rowspan="11">신청제품</td><td>업체명</td><td colspan="3"></td><td>대표자</td><td></td></tr>
<tr><td>주소</td><td colspan="3"></td><td>전화번호</td><td></td></tr>
<tr><td rowspan="3">제품명</td><td rowspan="2">* 신청제품이 2種 이상인 경우 신청서 추가 작성</td><td>제품 유형</td><td colspan="3">방화벽, L3 스위치 등</td></tr>
<tr><td>펌웨어
(SW 버전)</td><td colspan="3"></td></tr>
<tr><td>도입 수량</td><td></td><td>해시값</td><td colspan="3">* 네트워크 장비의 경우 기재</td></tr>
<tr><td rowspan="3">공인인증
현황</td><td>CC인증번호</td><td></td><td>인증등급
또는
준용 PP</td><td colspan="2">EAL 등급 또는 준용 PP</td></tr>
<tr><td>GS인증번호</td><td></td><td>준용 규격</td><td colspan="2"></td></tr>
<tr><td>성능평가
번호</td><td></td><td>준용 규격</td><td colspan="2"></td></tr>
<tr><td rowspan="3">업체
실무
담당자</td><td>전화번호</td><td colspan="4"></td></tr>
<tr><td>휴대폰번호</td><td colspan="4"></td></tr>
<tr><td>이메일</td><td colspan="4"></td></tr>
<tr><td>암호모듈</td><td colspan="2">□없음 □있음 (□검증 □미검증)</td><td>암호검증
번호</td><td colspan="2">* 검증 암호모듈의 경우</td></tr>
</table>

210㎜×297㎜<일반용지 60g/㎡(재활용품)>

[서식 제14호]

사이버보안관제센터 운영현황

보안관제센터 개요			
개소	* 개소일자	위치	
규모	* 상황실 면적 등	예산	* 구축예산 및 운영예산

조직 현황				
개요		* 조직구성, 인원 및 임무, 근무형태 등		
1	부서		센터장	
	직급		성명	
	이메일		연락처	전화: HP:
2	부서		직급/직책	
	담당분야		성명	
	이메일		연락처	전화: HP:
3	:	* 센터장과 탐지・분석・대응 등 분야별 대표자만 기입		

외부인력 현황			
업체명		대표이사	
인원수		근무형태	
계약기간		수행업무	

지침・매뉴얼 현황			
지침		기준	
매뉴얼		기타	

보안관제시스템 현황			
시스템명	* 주요 기능	시스템명	
시스템명		시스템명	
시스템명		시스템명	

보안장비 현황			
F/W	* 제품명 및 사용대수	IDS/IPS	
ESM		WEB F/W	
라우터		그 밖의 장비	예) NMS 1대 * 네트워크 구성도 사본 제출

보안관제 연동기관 현황
* 대상기관 수, 기관명, 대상목표(인터넷 또는 내부망, 홈페이지 등)

연동기관 IP할당 현황					
1	연동기관		IP 관리자	성 명	
	공인IP			연락처	전화: HP:
	사설IP			이메일	
2					
3					
4					
5					
6					

국가사이버안전센터 탐지규칙 재배포 현황			
기관명	배포방법	기관명	배포방법

210㎜×297㎜<일반용지 60g/㎡(재활용품)>

[서식 제15호]

네트워크장비 변경내용 분석서

1. 제품 개요

가. 작성자 정보

도입기관	
개발업체	
작성일	
작성자	

나. 검증제품

제품명	
버전	
펌웨어 파일명 (해시값)	OOO.img (97BA3B7A1B325E4E8A517CDDB01AFFD32F93D27E2F2EAC750FEB)
검증일	

다. 이전 변경승인 내용

제품명	버전	변경승인 일자	변경승인 내용

2. 변경 내용

가. 변경 전·후 시스템 구성

제품명	소프트웨어		하드웨어	
	변경전	변경후	변경전	변경후

나. 변경된 보안기능 및 변경 내용

변경된 기능	변경 내용
로그인	관리자 로그인시 비밀통신을 수행하도록 제품 변경 *** 필요시 화면 캡쳐**

다. 변경이 제품 설계에 미치는 영향

항목	영향 분석
펌웨어 변경 유무	로그인 기능 변경을 위해 관리자 인증과 관련된 일부코드가 변경됨에 따라 펌웨어가 변경됨 변경전: test1.1.img / 97BA3B7A1B325E4E8A517CDDB01AFFD3 변경후: test1.2.img / DCE24E537D2EB6E28E5BADBD1CEC0898 *** 필요시 화면 캡쳐**
사용자 인터페이스(UI) 변경 유무	로그인 기능 변경을 위해 내부 코드가 변경되었으며 제품의 사용자 인터페이스(UI) 변경은 없음 *** 필요시 화면 캡쳐**

라. 변경부분에 대한 자체 시험결과

변경된 기능	시험 내용	시험 결과
로그인	관리자 로그인시 비밀통신 수행여부 확인	정상동작 확인 *** 필요시 화면 캡쳐**

[서식 제16호]

정보통신제품 도입현황

기관명		관계 중앙행정기관	
담당자		담당자 전화번호	
사업명			
보안성	보안성 검토받은 문서 제목 및 번호 표시 *(예) ○○○보안성 검토결과(문서번호, '19.00.00)*		

기관명	관계 중앙 행정 기관명	제품명	제조사	제품 유형	보안기능 시험결과서			cc인증, GS인증, 성능평가			암호모듈검증 (KCMVP)		펌웨어 또는 OS 버전	해시값	비고
					발급 번호	시험 기관	발급 일	인증 번호	등급 또는 준수PP	평가 기관	암호 모듈명	당호 검증 번호			

210㎜×297㎜<일반용지 60g/㎡(재활용품)>

[서식 제17호]

정보화사업 보안성검토 의뢰서

1. 사업개요

사 업 명			
총 사업기간		사업금액	
발주예정시기		사업추진기간	

2. 사업목적

▸

▸

▸

▸

3. 추진일정 요약

▸

▸

▸

▸

첨부서류	1. 사업계획서(안) 및 제안요청서(안) 1부. 2. 정보통신망 구성도 1부. 3. 자체 보안성검토 체크리스트 1부. 4. 자체 보안대책(안) 1부.

유 의 사 항

※ 사전협의 시 보안성검토를 병행할 수 있으며, 이 경우, 보안성검토 의뢰서, 보안성검토 체크리스트, 자체보안대책(안)을 포함하여 사전협의 요구

210㎜×297㎜[백상지 80g/㎡]

[서식 제18호]

보안성검토 체크리스트

(앞 쪽)

사 업 명 :　　작성자 :　　(서명)

구분		항목	Y	N	NA
인증 및 권한	1.1	사용자 인증 처리가 필요한가?			
		- 사용자 인증방식은 OTP(One-Time Password) 혹은 이중인증(Two-Factor Authentication) 등의 보안성이 확보된 방식을 권고 - I-PIN, G-PIN 등 사용자 정보 확인 및 GPKI 시스템(CA, LDAP 등) 사용 여부			
	1.2	사용자 가입절차가 필요한가?			
		- 대민 시스템의 경우, 주민등록번호 대체 수단 (G-PIN) 사용 필요 - 주민등록번호 수집 시 관련 법령에 근거 확인 - 개인정보보호 정책 등 보안관련 정책 수립 및 관련정책 게시			
	1.3	사용자별로 권한을 정의하는가?			
		- 제공하는 정보의 중요도에 따라 권한 정의 필요 - 업무담당자의 ID의 경우, 신청, 부여 및 회수를 위한 절차를 마련하여 시행, 권한 부여 · 변경 · 회수 · 삭제 등의 이력 3년 이상 보관 - 모든 계정의 비밀번호는 숫자 · 문자 · 특수문자 등을 혼합하여 안전하게 설정하고, 3개월 단위로 변경 강제화			
	1.4	별도의 관리자 화면을 구현하는가?			
		- 관리자 화면 접속에 대한 통제기능(중복인증, 접속 IP 통제 등) 필요 - 관리자에게 제공하는 기능 및 정보 범위 등 사전 협의 필요			
	1.5	기관 외부에서 접근 가능한가?			
		- 외부 접속에 대한 네트워크, 데이터 측면 안전대책 수립 필수			
중요 정보 취급	2.1	개인정보를 취급(수집, 저장, 제공 등) 하는가?			
		- 주요 개인정보 : 주민등록번호 및 계좌정보, 신용카드 정보 등의 금융정보 - 일반 개인정보 : 주소, 전화번호, 이메일 등 - 주요 개인정보는 국가정보원 인증 암호방식을 이용하여 암호화 저장 필수			
	2.2	비공개 중요정보에 대한 전송구간 암호화 하는가?			
		- 정보통신망으로 전송되는 비공개 중요정보 소통시 암호화 필수			
	2.3	처에서 보유 중인 개인정보가 필요한가?			
		- 사용 범위, 제공 주기, 보안대책 등 협의 필요			
	2.4	중요 정보에 대한 출력 · 다운로드 기능을 제공하는가?			
		- 중요 정보(개인정보, 미공개 출원 정보 등) 출력 · 다운로드 시, DRM 등의 조치 필수			
시스템 연동	3.1	인사혁신처 내부(행정망) 시스템과 연동하는가?			
		- 대상 시스템, 연동 정보, 연동 방식 등 협의 필요			
	3.2	인사혁신처 외부(인터넷) 시스템과 연동하는가?			
		- 대상 시스템, 연동 정보, 연동 방식 등 협의 필요			

210㎜×297㎜[백상지 80g/㎡]

(뒤 쪽)

구분		항목	Y	N	NA
시스템 보안	4.1	설치 시스템 중 보안 시스템(H/W, S/W)이 있는가?			
		- 국가정보원 인증(CC인증 또는 국가용 암호제품 인증) 제품만 설치 가능			
	4.2	SW개발보안 방안 및 절차는 있는가?			
		- 응용SW 개발인 경우 분석 · 설계, 구현, 테스트 등 단계별 개발보안 적용			
	4.3	자체 보안취약점 점검 계획이 있는가?			
		- 웹 기반 시스템 개발인 경우, 외부 모의 해킹 수준의 점검 및 보완 필수			
	4.4	주요 사용자 사용 이력에 대한 관리 기능이 있는가?			
		- 관리자 접근 이력 및 주요 정보 변경 이력 등 저장 필요			
	4.5	참여 인원 중 외부 상주 인원이 있는가?			
		- 해당 인원의 업무수행 방식 협의 및 처 보안담당자 승인 필요			
	4.6	별도 개발 및 테스트 서버가 있는가?			
		- 서버의 위치 확인(처내 개발서버군 또는 개발자 PC 네트워크 등) 필요			
	4.7	신규 도입 정보시스템의 운용전 취약점 제거 방안 및 절차는 있는가?			
		- 네트워크 및 정보보호 장비, 서버 등 운용전 취약점 제거 수행 및 조치 필수 - OS, Web, WAS, DBMS 등의 불필요 서비스, 기본계정 제거, 초기 패스워드 변경 조치			
	4.8	업무시스템 접속시 보안조치 사항은 있는지?			
		- 시스템 접속시 일정 횟수(5회이하 권장) 이상 로그인 실패시 접속을 제한하고 동일계정으로 동시에 시스템 로그인하지 못하도록 차단 - 업무시스템 로그인시 마다 접속 IP, 시간 등을 포함한 최종 접속 기록 표시			
PC 보안	5.1	개발 PC(행정망)에서 외부(인터넷)와 데이터 송수신이 필요한가?			
		- 연결 대상 및 송수신 정보 등 협의 필수			
	5.2	파일서버를 운용하는가?			
		- Windows Server 사용 시, 별도 협의 필수 - 파일서버에 대한 보안대책(접근통제, 데이터 유출 방지 등) 수립 필수 - 업무망에서 용역망 파일서버로 접근하지 못하도록 하여 망혼용 금지			
용역업체보안	6.1	용역사업 수행단계별 외부 용역업체에 대한 보안관리방안은 있는지?			
		- 입찰 · 계약 단계 보안사항, 사업 수행전 보안교육, 수행단계 인원 · 자료 보안, 사무실 · 장비 보안, 내 · 외부망 접근시 보안관리, 사업완료시 보안대책 등을 적용 및 보안점검			

210㎜×297㎜[백상지 80g/㎡]

[서식 제19호]

자체 보안대책(안)

(앞 쪽)

1. 사업개요

사 업 명	
사업기간	
사업내용	

2. 추진일정 및 체계

▸ 추진일정

구 분	M-2	M-1	M	M+1	M+2

▸ 추진체계

▸ 추진조직별 역할

(뒤 쪽)

3. 요소별 보안대책

▸ 관리적(보안관리 수행 조직, 인원 등) 보안대책

구 분	내 용	비 고

▸ 설치장소에 대한 보안관리 방안 등 물리적 보안대책

구 분	내 용	비 고

▸ 안전성을 검증한 암호모듈·정보보호시스템 도입 운용 계획

구 분	내 용	비 고

▸ 서버, 단말기, 휴대용 저장매체 보안대책

구 분	내 용	비 고

▸ 네트워크 보안대책

구 분	내 용	비 고

▸ 백업 및 복구계획

구 분	내 용	비 고

▸ 기타 보안대책

구 분	내 용	비 고

210㎜×297㎜[백상지 80g/㎡]

[서식 제20호]

보안성 검토 결과 통보서

1. 보안성 검토 대상 정보화사업

순번	부 서 명	사 업 명	비고

2. 제한사항

▸

▸

3. 검토결과

▸

▸

▸

▸

▸

▸

▸

▸

▸

▸

210㎜×297㎜[백상지 80g/㎡]

[서식 제21호]

휴대용 저장매체 관리대장(일반용)

[관리자 : 4급 이순○]

연번	관리번호 (S/N)	매체 형태	등록일자	취급자	불용처리 일자	불용처리방법 (재사용 용도)	비고
1	총무과-일반-01 (E-D900-04-3705B)	USB	10.10.20	5급 홍길○	11.10.20	물리적 파기	고장
2	총무과-일반-02 (NP00T512787J)	외장형 HDD	10.10.25	6급 김정○	11.10.27	포맷후 재사용 (시설과-일반-01)	
3	총무과-일반-03 (E-D900-04-3705B)	USB	10.11.1	5급 이수○	11.10.7	물리적 파기	고장

참 고 사 항

※ 전자적 관리 대장을 사용하는 경우 대장 유지 불필요

210㎜×297㎜[백상지 80g/㎡]

[서식 제22호]

휴대용 저장매체 관리대장(비밀용)

< 관리자 : 4급 김유○ >

연번	관리번호 (S/N)	매체 형태	등록일자	취급자	불용처리 일자	불용처리방법 (재사용 용도)	비고
1	총무과-일반-01 (E-D900-04-3705B)	USB	10.10.20	5급 홍길○	11.10.20	물리적 파기	고장
2	총무과-일반-02 (NP00T512787J)	외장형 HDD	10.10.25	6급 김정○	11.10.27	포맷후 재사용 (시설과-일반-01)	
3	총무과-일반-03 (E-D900-04-3705B)	USB	10.11.1	5급 이수○	11.10.7	물리적 파기	고장

참 고 사 항

※ 전자적 관리 대장을 사용하는 경우 대장 유지 불필요

210㎜×297㎜[백상지 80g/㎡]

[서식 제23호]

휴대용 저장매체 점검대장

< 관리자 : 4급 김유○ >

점검일시	현 보유수량				이상 유무	점검관		비고 (서명)
	Ⅱ급	Ⅲ급	대외비	일반		성명	서명	
2019.1.3	1	1	3	15	이상무	5급 홍길○	홍길○	김유○
2019.2.1	1	1	2	16	이상무	5급 홍길○	홍길○	김유○
2019.3.1	1	1	2	16	이상무	5급 홍길○	홍길○	김유○
2019.4.1	1	1	2	17	이상무	5급 홍길○	홍길○	김유○

참 고 사 항

※ 전자적 관리 대장을 사용하는 경우 대장 유지 불필요

210㎜×297㎜[백상지 80g/㎡]

[서식 제24호]

휴대용 저장매체(전산장비 포함) 반출·입 대장

< 관리자 : 4급 김유○ >

장비명	관리번호 (시리얼번호)	사용자	용도	출입 일시 (입·출 구분)	반출·입시 조치사항	확인
PC	KKR-P-99999999-00000001	5급 홍길○	00용역사업 추진	2011.10.1. 11:00(입)	반입시 악성코드 점검	김유○
USB	총무-일반-01 (610-RUCW-61659)	5급 홍길○	국회 제출	2011.10.1. 11:00(출)	반출시 완전삭제	김유○
CD	총무-일반-03 (4589-KK-4585)	5급 유관○	법무부 회의참석	2011.10.7. 09:40 (출)	물리적 파기	김유○
CD	총무-일반-03 (1258-JK-8935)	5급 유관○	법무부 회의참석 회수	2011.10.7. 17:50(입)		김유○
USB	총무-일반-01 (610-RUCW-61659)	5급 홍길○	국회제출 회수	2011.10.8. 18:10 (입)		김유○
노트북PC	s111-001-113 (5004829800055)	5급 홍길○	세미나 발표	2011.12.3. 13:00 (출)		김유○
USB	총무-일반-005 (610-RUFU-61747)	5급 강감○	재택근무	2011.12.3. 10:00(출)		김유○

참 고 사 항

※ 전자적 관리 대장을 사용하는 경우 대장 유지 불필요

210㎜×297㎜[백상지 80g/㎡]

[서식 제25호]

휴대용 저장매체 라벨

구분	서식	예시
외장형 HDD	↑ 2.5cm ↓ 일반/비밀용 (인) 관리번호 표기 정 부 ← 5cm →	일반용 (인) 총무과-일반-01 정 이순○ 부 홍길○ 비밀용 (인) 총무과-비밀-01 정 이순○ 부 홍길○
USB·CD 등	↑ 1cm ↓ 일반/비밀용 (인) 관리번호 표기 ← 3cm →	일반용 (인) 총무과-일반-01 Ⅱ급비밀용 (인) 총무과-Ⅱ급-01

\

참 고 사 항

가. 同 서식을 만들어 휴대용 저장매체 중앙의 적절한 위치에 부착

나. 첫 번째 줄에는 일반/비밀용(인)란에 분임정보보안담당관 또는 관리자의 직인을 날인

다. 두 번째 줄에는 휴대용 저장매체 관리번호 표기

라. 세 번째 줄의 '정' 란에 관리자, '부' 란에 취급자 표기(USB메모리 및 CD의 경우 생략 가능)

마. 휴대용 저장매체의 크기를 고려하여 서식·글자 크기 조정 가능

210㎜×297㎜[백상지 80g/㎡]

[서식 제26호]

휴대용 저장매체 불용처리 확인서

아래와 같이 휴대용 저장매체(　　종　　점) 불용처리 및 휴대용 저장매체 (　　종　　점) 재사용에 대해 확인을 요청함

연번	관리번호 (S/N)	매체형태	사유	불용처리	재사용
1	총무과-일반-01 (E-D900-04-3705B)	USB	고장	물리적 파기	
2	총무과-Ⅲ급-01 (5101-53RA-12567)	CD	고장	물리적 파기	
3	총무과-Ⅱ급-01 (610-RURQ-61750)	USB	용도전환	자성소거	총무과-일반-09
4					
5					
6					
7					
8					
9					
10					

년　　월　　일

요 청 자　　소속·직급　　성명 :　　(서명 또는 인)

확 인 자　　각급부서 정보보안담당관　　성명 :　　(서명 또는 인)

210㎜×297㎜[백상지 80g/㎡]

[서식 제27호]

휴대용 저장매체 분실(소각) 확인서

분실 매체	부서명	
	취급자	
	관리번호 (일련번호)	
저장 자료 내용		
분실 사유 ※ 6하 원칙에 따라 기술		
재발방지 대책		
재신청여부 (보안USB일 경우)	□ 신청함　　□ 신청 안함	

취급자 소속　　직급

직위　　성　　명　서명 또는 인

확인자 소속　　직급

직위　　성　　명　서명 또는 인

※ 확인자 : 부서장

210mg×297mm<백상지80g/m2>

[서식 제28호]

원격근무 보안서약서

본인은 년 월 일부로 원격근무를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 나는 부여받은 인증 관련 정보 및 매체를 타인에게 유출하지 아니한다.
2. 나는 원격근무 중 작성·저장·열람·출력한 문서는 업무 목적에만 활용하고 타인에게 유출하지 아니한다.
3. 나는 원격근무용 소프트웨어 및 전산장비를 업무목적에만 활용하며 바이러스 백신 프로그램 및 기타 보안 프로그램을 설치하여 최신 상태로 유지한다.
4. 나는 여타 보안사항들을 성실히 준수하며 위반시 관련규정에 따라 처벌도 감수한다. 다만, 부패행위 신고 및 공익신고 등의 경우 비밀준수 의무를 위반하지 않은 것으로 본다.

년 월 일

서약자 소속 직급
직위 성 명 서명 또는 인

서 약 소속 직급
집행자 직위 성 명 서명 또는 인

210mg×297mm<백상지80g/m²>

[서식 제29호]

열람·제공자료 관리대장

용역업체 관리책임자	각 기관 관리책임자

년 (일련번호:) 사업명: 사업주관기업:

연번	자료명	인계 및 인수				자료반납	
		인계자	인수자	월일	장소	확인자	월일

210㎜×297㎜<일반용지 60g/㎡(재활용품)>

[서식 제30호]

지편자재 사용기록부

자재 번호	관리 번호	년월일	전문액표			난수사용				소자년 월일	소자자	비고
			번호	송수 구분	조수	부터		까지				
						쪽	행	쪽	행			

297 * 210mm(A4)

< 작성요령 >

○ 전문액표

- 번　　호 : 암호전문 일련번호

- 송수구분 : 수발신으로 구분

- 조　　수 : 암호전문 조수

297㎜×210㎜<일반용지 60g/㎡(재활용품)>

[서식 제31호]

암호자재 관리기록부

자재 명칭	등록 번호	제 작		수령(배부)				회수			반납				비고
		일자	수량	일자	수량	증빙 번호	대상 기관	일자	수량	증빙 번호	일자	수량	증빙 번호	확인	

210㎜×297㎜<일반용지 60g/㎡(재활용품)>

[서식 제32호]

암호자재 점검기록부

점검 일시	점 검 사 항				점 검 관		비 고
	자재 명칭	수량	보관 상태 (암호자재)	정상 동작 (암호장비)	성 명	서 명	

210㎜×297㎜<일반용지 60g/㎡(재활용품)>

[서식 제33호]

암호자재 증명서

○ 증명서 번호	구분 : 배부, 반납, 파기, 분실, 그 밖
발신 :	수신 :
아래 기록된 암호자재(개)를 ( )하였음	아래 기록된 암호자재(개)를 ( )하였음
일자 : 년 월 일	일자 : 년 월 일
소속 :	소속 :
성명 : (인)	성명 : (인)

구 분 (자재, 장비)	자 재 명 칭	수 량	등 록 번 호	비 고

<

210㎜×297㎜<일반용지 60g/㎡(재활용품)>

[서식 제34호]

암호자재 보유현황

구 분	자재 명칭	수 량	등록 번호	비 고

210㎜×297㎜<일반용지 60g/㎡(재활용품)>

부 록

정보보안감사(정보지도점검) 체크리스트

1. 정보보안 기본활동

연번	세부 점검사항	비고
1	기관 자체 실정에 맞는 정보보안업무 내규를 수립하고 있는가?	
2	매년 정보보안업무 활동계획을 수립・시행하는가?	
3	정보보안업무 전담 조직 및 직원(정보보안담당관)이 지정되어 있는가?	
4	소속 직원 근무성적 평가시 정보보안내규 준수여부를 반영하고 있는가?	
5	소속・산하기관 대상 정보보안 감사 또는 점검을 실시하는가?	
6	소속・산하기관 대상 정보보안 교육을 실시하고 있는가?	
7	사이버보안진단의 날을 내실 있게 수행하는가?	
8	정보보안 침해사고・규정위반 및 정보통신망 장애발생을 대비한 보고체계・조치절차가 마련되어 있는가?	
9	보직변경 등 인사이동시 정보시스템 접근권한을 신속하게 조정하는가?	
10	서버・PC 등 정보시스템 현황을 제대로 파악하는가?	
11	정보통신장비(노트북 등) 반출입 통제 및 현황 관리를 철저히 하는가?	
12	업무자료를 상용 정보통신서비스로 전송하고 있지 않는가?	
13	정보통신망 구축 및 유지보수를 수행하는 외부인력(보안관제인력 포함)에 대해 보안서약서 청구, 보안교육 등 충분한 보안조치를 하고 있는가?	
14	용역업체 직원의 내부 정보시스템 접근을 통제하고 있는가?	
15	홈페이지 등 외부 게시자료에 대한 정보공개 지침을 수립・반영하는가?	
16	중요 정보화사업에 대하여 보안성 검토절차를 이행하는가?	
17	정보보호시스템(상용 암호모듈 포함) 도입시 보안적합성 검증절차를 준수하는가?	
18	비밀을 전자적으로 처리할 경우 암호자재로 암호화하는 등 규정을 준수하는가?	

2. PC 및 서버 보안관리

연번	세부 점검사항	비고
1	PC・서버에 설치된 운영체제 및 응용프로그램을 최신 보안업데이트 하였는가?	
2	PC・서버의 불필요한 서비스를 검토하여 중단하고 정기적으로 인터넷에서 접속 가능여부를 확인하는가?	
3	백신이 자동 업데이트되고 실시간 감시기능이 설정되어 있는가?	
4	인터넷 PC에 업무관련 자료(비밀 포함)가 방치되어 있는가?	
5	P2P, 웹하드, 상용메신저 등 업무와 무관한 비인가 프로그램이 설치되어 있는가?	
6	비인가자 접근방지를 위해 CMOS・로그인 등 PC 비밀번호를 설정하였는가?	
7	서버내 저장자료는 중요도에 따라 접근권한이 설정되어 있는가?	
8	정보통신망 구성측면에서 PC 및 서버 등의 위치가 적정한가?	
9	비인가 휴대용 저장매체(USB, 외장형 하드디스크, 메모리카드 등) 사용기록이 존재하는가?	
10	전자우편은 발신지 IP의 국가명이 표시되고 해킹메일은 신고가 쉬운가?	
11	비밀은 비밀용 USB를 별도 지정하여 사용하고 일반자료와 혼합 저장하지 않는가?	
12	정보보호시스템・서버・네트워크장비 등 로그기록을 1년 이상 유지・관리하는가?	
13	비인가 USB・정보통신기기 연결시 차단토록 보안 설정되어 있는가?	
14	PC・노트북 등 저장매체가 있는 기기 고장시 저장된 자료의 완전 삭제를 확인하고 외부에 수리를 의뢰하는가?	
15	「정보시스템 저장매체 불용처리지침」에 따라, 저장매체를 불용하였는가?	
16	모바일 업무는 행정업무와 현장업무를 구분하고 별도의 단말기를 운영하는가?	
17	불필요한 원격접속 S/W는 비활성화 또는 제거하였는가?	
18	상주 용역업체 네트워크와 직원용 네트워크를 분리하였는가?	
19	네트워크 접근제어를 위한 보안정책을 적절하게 설정하였는가?	
20	네트워크 접근제어 정책에 대한 생성일・목적・요청자 등 이력을 관리하는가?	
21	주요 정보보호시스템의 보안정책 설정파일을 주기적으로 백업하고 있는가?	

3. 네트워크 보안관리

연번	세부 점검사항	비고
1	정보시스템 세부 구성도(IP 포함)를 최신으로 유지하는가?	
2	업무자료를 소통하기 위한 내부망은 인터넷과 분리 운영하는가?	
3	인터넷·업무망간 자료공유 방안이 적절한가?	
4	업무자료를 소통하기 위한 내부망 구축시 사설주소체계(NAT)를 적용하는가?	
5	국가정보원장이 안정성을 검증한 정보보호시스템을 운용하고 있는가?	
6	인가받지 않은 단말기가 네트워크에 연결하지 못하도록 조치하고 있는가?	
7	네트워크를 통한 파일공유를 제한하고 필요시 보안대책을 세우고 있는가?	
8	장비 신규도입 등 전산망 구성 변동시 관련사항을 기록하는가?	
9	비인가 무선인터넷·무선랜 등 허가받지 않은 인터넷 접속경로가 존재하는가?	
10	첨단 정보통신기기(IoT 등)에 의한 내부 업무자료 유출 가능성이 존재하는가?	
11	시스템 최초 설치시 등록된 초기 계정·패스워드를 변경하였는가?	
12	네트워크 장비·정보보호시스템·서버는 비인가자가 접속하지 못하도록 IP 통제 등 보안설정하고 불필요한 서비스포트를 제거하는가?	
13	네트워크 장비·정보보호시스템·서버 등의 관리자 네트워크를 인터넷·업무망과 별도로 분리하여 운용하고 있는가?	
14	무선네트워크 구축시 사전에 보안성 검토를 수행하고 보안대책을 준수하는가?	
15	정보시스템에 대한 보안취약점을 주기적으로 점검하는가?	
16	소프트웨어개발보안(시큐어코딩)을 적용하여 개발하였는가?	
17	원격지 개발시 개발장소를 점검하고 있는가?	
18	원격 유지보수를 금지하고 비인가 원격접속을 차단하는가?	
19	직원의 재택·파견·이동근무 등 원격근무시 보안관리 대책이 적절한가?	
20	음란·도박 등 유해사이트를 차단하고 사이트목록을 주기적으로 갱신하는가?	
21	해외에 위치한 사무소와 인원에 대해 보안대책을 지원하고 주기적으로 점검하는가?	
22	인터넷전화 제품은 TTA Verified Ver 4. 이상을 사용하는가?	
23	인터넷전화는 인터넷망에 설치된 경우 물리적으로 분리하고, 업무망에 설치된 경우 물리적 또는 논리적(VLAN)으로 분리하였는가?	
24	서버가 위치한 네트워크는 방화벽 등으로 사용자 네트워크와 분리하고 있는가?	

4. 정보통신시설 보안관리

연번	세부 점검사항	비고
1	인위적·자연적 원인에 의한 정보통신망 장애 대비 백업 등 재난방지 대책을 강구하였는가?	
2	통합전산센터, 정보통신실 등 중요 정보통신시설을 보호구역으로 관리하는가?	
3	사무실 책상서랍 등에 비밀문건이나 비인가 정보통신기기가 방치 여부를 주기적으로 확인하는가?	
4	외부인의 정보통신실 출입을 통제하고 기록을 유지하는가?	
5	무정전 전원공급장치 등 비상시 전력장애 대책을 강구하였는가?	
6	침입경보장치, CCTV 등 보안장비와 방화장비(하론소화기 등) 정상동작 여부를 정기적으로 점검하고 있는가?	
7	정보통신시설에 비상시 긴급 파기를 위한 장비(해머 등)를 비치하고 있는가?	
8	정보통신시설에 대한 접근권한을 업무목적에 따라 차등 적용하고 있는가?	
9	정보통신장비 수리·점검시 정보보안담당관 또는 분임정보보안담당관 참석하에 진행하는가?	
10	민간 클라우드 컴퓨팅서비스 사용시 보안인증을 받은 서비스를 이용하는가?	
11	계약서에 정보통신망 구성도, IP주소현황 등 누출금지정보를 명시하고 있는가?	
12	시각동기화를 통하여 정보시스템 시각을 정확히 유지하고 있는가?	
13	CCTV 등 단독망 형태의 시스템을 인터넷망과 혼용하지 않고 분리·운영하는가?	

5. 암호자재 및 암호알고리즘 관리

연번	세부 점검사항	비고
1	비밀을 소통・보호하기 위하여 국가정보원장이 개발하거나 안전성을 확인한 암호자재를 사용하는가?	
2	국가정보원장이 승인하지 아니한 암호자재 또는 외국에서 생산된 암호기능 탑재 시스템을 무단으로 사용하는가?	
3	암호자재를 취급하는 인원을 암호자재 취급자로 지정・관리하는가?	
4	암호자재 취급인가자 중 암호자재 배부 또는 반납하는 직원에 대해 인감등록을 실시하는가?	
5	각 암호자재에 대한 운용관리 정・부책임자 및 실무 담당자를 지정하였는가?	
6	암호자재 설치, 운영, 보관에 대한 보안대책이 수립되었으며 이행되고 있는가?	
7	암호자재를 복제・복사하거나 또는 국가정보원장이 승인 없이 암호자재를 해외 제공・반출한 사례는 없는가?	
8	암호자재 관련 문서를 비밀로 생산하여 관리하고 있는가?	
9	사용중인 암호자재의 사용목적 및 보호대상 변경 시, 국가정보원장에게 승인을 받았는가?	
10	노후 등으로 사용하지 않거나 또는 도입 후 6개월 이내에 설치하지 않는(미래용・예비용 암호자재 제외) 등 보관만 하고 있는 암호자재가 있는가?	
11	'암호자재 관리기록부', '암호자재 점검기록부', '지편자재 사용기록부' 등을 누락하지 않고 작성・유지하고 있는가?	
12	암호자재 책임자는 주1회 이상 암호자재를 점검하여 그 결과를 '암호자재 점검기록부'에 기록・유지하고, 보안담당관은 점검사항을 월 1회 확인하고 있는가?	
13	암호자재 배부・반납 등의 업무는 암호자재 취급자가 직접 수행하고, '암호자재 증명서'를 작성・보관하고 있는가?	
14	암호자재의 정・부 책임자 및 실무 담당자 교체시 인계인수를 실시하고 '암호자재 관리기록부'에 인계인수 사항을 기록하는가?	

6. 보안관제 등 해킹 대응활동

연번	세부 점검사항	비고
1	사이버공격에 대응하기 위해 자체 관제센터를 운영(직접 혹은 보안관제 전문업체 용역)하거나 다른 국가・공공기관에 위탁 하였는가?	
2	보안관제센터 운영을 총괄 관리하는 전담 공무원이 있는가?	
3	사이버공격 탐지・대응 및 자체 DDoS공격 대응매뉴얼 등이 구비되어 있는가?	
4	해킹사고 조사결과, 보안 위규자에 대한 처벌이 자체 규정・지침 등에 명시되어 있고 실제로 이루어지고 있는가?	
5	국가사이버안전센터・부문보안관제센터 등 유관기관과 보안관제시스템을 연계 운영하는가?	
6	자체 사이버위기 대응 모의훈련을 주기적으로 실시하는가?	
7	홈페이지 해킹, DDoS공격, 해킹메일 수신 등 침해사고 발생시 국가정보원・부문보안관제센터 등 유관기관에 즉시 신고하는가?	
8	시스템 장애시 유지보수 업체 및 긴급연락체계가 최신화 되어 있는가?	
9	보안관제시스템에 대한 물리적・관리적・기술적인 보안대책을 준수하고 있는가?	
10	침해사고 발생시 사고조사내용을 작성하고 해당내용을 기관장에 보고하는가?	
11	전직원을 대상으로 해킹메일 대응방안 및 침해사고 대응절차 등 관련 교육을 수행하는가?	
12	보안취약점 발표시 산하기관 또는 담당직원과 즉시 공유하는가?	
13	국가사이버안전센터 등과 사이버위협정보, 탐지기술 등 정보를 공유하고 있는가?	
14	사이버공격 발생시 소속・산하기관에 전파할 수 있는 체계가 구비되었는가?	
15	국가사이버안전센터에서 제공한 탐지규칙정보에 대한 보안관리 및 전담관리자를 지정・운영하고 있는가?	
16	침해사고 발생시 해당 시스템을 무단 포맷할 경우 보안위규(사고조사 방해) 행위임을 시스템 관리자・사용자가 인지하고 있는가?	