정보통신보안업무규정

제정 2000. 12. 1. 행정자치부훈령 제 61호
개정 2005. 4. 23. 행정자치부훈령 제135호
개정 2007. 12. 6. 행정자치부훈령 제246호
제정 2008. 3. 11. 행정안전부훈령 제 17호
개정 2008. 6. 18. 행정안전부훈령 제115호
개정 2009. 1. 19. 행정안전부훈령 제139호
개정 2009. 6. 9. 행정안전부훈령 제147호

제 1 장 총 칙

제1조(목적) 이 규정은「보안업무규정」및「보안업무규정시행규칙」(이하 "시행규칙"이라 한다),「보안업무규정시행요강」(2008.7.7, 행정안전부훈령 제120호)제3조제2항 (이하 "시행요강"이라 한다)에서 위임된 사항과 행정안전부의 정보통신보안업무에 필요한 사항을 규정함을 목적으로 한다.

제2조(적용) 이 규정은 행정안전부와 그 소속기관, 특별시·광역시·도·특별자치도 및 시·군·구와 그 소속기관(이하 "행정기관"이라 한다)에 적용한다.

제3조(정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

1. "정보통신망"이라 함은「전기통신기본법」제2조제2호의 규정에 의한 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.
2. "정보통신보안"이라 함은 정보시스템 및 정보통신망을 통해 수집·가공·저장·검색·송신 또는 수신되는 정보의 유출·위조·변조 및 훼손 등을 방지하기 위하여 관리적·물리적 또는 기술적 수단을 강구하는 모든 행위를 말한다.
3. "정보통신시스템"(이하 "정보시스템"이라 한다)이라 함은 정보의 수집, 가공, 저장, 검색, 송신·수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 말한다.
4. "보조기억매체"라 함은 디스켓(FD), 이동형 하드디스크(HDD), USB메모리, Flash 메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 또는 IC칩 등에 정보를 저장할 수 있는 모든 것으로 정보통신망과 분리할 수 있는 기억장치를 말한다.

5. “정보보호시스템”이라 함은 정보의 수집, 저장, 검색, 송신 또는 수신할 경우에 정보의 유출, 위조, 변조 및 훼손 등을 방지하기 위한 하드웨어 및 소프트웨어를 말한다. 이 경우 정보보안시스템(이하 “보안시스템” 이라 한다)의 정의를 포함한다.
6. “전자정보”라 함은 행정기관이 업무와 관련하여 취급하는 것으로 컴퓨터 등 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 문서 및 기록물을 말한다.
7. “정보통신실”이라 함은 서버·PC 등과 스위치·교환기·라우터 등 네트워크 장비 또는 보안장비 등이 설치 운용되는 장소를 말하며, 전산실·통신실·관제실 또는 전자정보의 보관실 등을 말한다.
8. “관제실”이라 함은 정보통신망이나 정보시스템의 운용과 통신하기 위한 수단으로 수집·가공·저장·검색·송신 또는 수신되는 각종 정보를 종합 관리·감시·분석 또는 대응하는 장소를 말한다.
9. “대도청(對盜聽) 측정”이라 함은 도청탐색장비 등을 이용하여 은닉된 도청장치 색출 등 각종 도청위해 요소를 제거하는 제반 보안활동을 말한다.
10. “본인확인”이란 정보통신망을 통하여 정보시스템 또는 행정정보를 이용하는 업무담당자, 민원인 또는 시스템 관리자가 가지고 있거나 알고 있는 정보를 이용하여 본인임을 확인하는 것을 말한다.
11. “접근권한”이란 정보시스템에 접속하여 정보자원을 활용할 수 있는 권한과 행정정보를 생성·변경·열람 또는 삭제 등을 할 수 있는 권한을 말한다.
12. “침해사고”라 함은 해킹, 컴퓨터바이러스, 악성코드, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등에 의하여 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태를 말한다.
13. “국가용 보안시스템”이라 함은 비밀 등 중요자료 보호를 위하여 국가정보원장(이하 “국정원장”이라 한다)이 개발하거나 안전성을 검증한 암호장비·보안자재 또는 암호논리 등을 말한다.
14. “국가용 보안시스템 제작업체”(이하 “제작업체”라 한다)”라 함은 국가용 보안시스템의 제작권을 획득한 업체를 말한다.
15. “암호장비”라 함은 정보통신망으로 처리·저장·송신 또는 수신되는 정보를 보호할 목적으로 암호논리를 내장하여 제작된 장비를 말한다.
16. “보안자재”라 함은 통신내용 등의 정보를 보호할 목적으로 사용하는 암호·음어·약호자재를 말한다.

17. “암호자재”라 함은 Ⅱ급비밀 이하의 통신내용 등의 정보를 보호할 목적으로 사용하는 문자·숫자·기호 등으로 구성된 환자표와 난수 또는 암호논리 등을 수록한 문서나 도구를 말한다.
18. “음어자재”라 함은 Ⅲ급비밀 이하의 통신내용 등의 정보를 보호할 목적으로 사용하는 문자·숫자·기호 등으로 구성된 환자표 또는 암호논리 등을 수록한 문서나 도구를 말한다.
19. “약호자재”라 함은 대외비 이하의 통신내용 등의 정보를 보호할 목적으로 특정 용어와 그에 대응·변환되는 문자, 숫자, 기호 등을 수록한 문서나 도구를 말한다.
20. “암호논리”라 함은 정보의 유출, 위·변조, 훼손 등을 방지하기 위하여 기밀성·무결성·인증·부인봉쇄 등의 기능을 제공하는 수학적 논리 또는 알고리즘을 말한다.
21. “암호모듈”이라 함은 정보의 유출, 위·변조, 훼손 등을 방지하기 위해 암호논리를 활용하여 구현한 수단이나 도구를 말한다.
22. “암호취급자”라 함은 암호취급인가를 받아 암호체계를 연구하거나 국가용 보안시스템을 취급 관리하는 자를 말한다.
23. “음어취급자”라 함은 음어취급인가를 받아 음어자재를 취급 관리하도록 임명된 자를 말한다.

제4조(책무) 행정기관의 장은 전자정보와 정보통신망을 보호하기 위한 보안대책을 마련하여야 하며 정보통신보안에 대한 책임을 진다.

제5조(기본활동) 행정기관의 장은 정보통신 수단에 의한 각종 정보의 누설(漏泄)을 방지하고 보호하여야 하며 다음 각 호의 정보통신보안 기본활동을 수행하여야 한다.

1. 정보통신보안 정책 및 세부추진계획 수립·시행
2. 정보통신보안 관련 규정·지침 등 제·개정
3. “시행요강 제3조“ 규정에 의한 정보통신보안담당관의 지정 및 운영
4. “시행요강 제4조” 규정에 의한 “보안심사위원회” 운영
5. 정보통신보안 업무 지도·감독
6. 정보통신보안 감사 및 심사분석
7. 정보통신 보안관리 실태에 대한 자체 조사·평가
8. 사이버공격 초동조치 및 대응
9. 사이버위협정보 수집·분석 및 보안관제
10. 정보통신보안 사고조사 결과 처리
11. 정보통신보안 예산 및 전문인력 확보

12. 정보통신보안 교육 및 정보협력
13. 도청위해 요소 측정・제거
14. 주요 정보통신기반시설 보호활동
15. 국가용 보안시스템 및 암호키의 운용・보안관리
16. 암호모듈・정보보호시스템의 운용 및 보안관리
17. 정보통신망 보안대책의 수립・시행
18. 기타 정보통신보안 관련 사항

제6조(정보통신보안담당관 운영) ① 행정기관의 장은 정보통신보안 업무를 원활히 수행하기 위하여 정보통신보안담당관을 임명하여 운영하여야 한다.

② 정보통신보안담당관은 정보통신업무를 관장하는 부서에 발령과 동시에 소관 기관의 정보통신보안담당관이 된다.

③ 행정기관의 장은 정보통신보안담당관이 교체되었을 경우에 "시행요강 제3조 제6항"에 따라 이를 행정안전부장관(이하 "행안부장관"이라 한다)에게 통보하여야 한다.

④ 정보통신보안담당관은 "시행요강 제3조제1항"의 규정에 의한 보안담당관의 지휘감독을 받아 제5조의 기본활동 임무를 수행한다.

제7조(세부추진계획 수립 및 심사분석) ① 행정기관의 장은 제5조의 규정에 의한 당해 기관의 정보통신보안 세부추진계획을 수립・시행하고 그 추진결과를 심사분석 및 평가하여야 한다.

② 행정기관의 장은 제1항의 규정의 세부추진계획을 수립할 경우에 별표 3의 "정보통신보안 점검항목"을 참조하여 주기적으로 보안상태를 자체 점검하여야 한다.

③ 행정기관의 장은 세부추진계획 및 심사분석을 별지 제1호 및 제2호서식에 따라 작성하여 다음 각호의 기한 내에 행안부장관에게 제출하여야 한다. 이 경우 제출기한은 매년도 「보안업무 수행지침」에서 정하는 기한을 우선 적용한다.

1. 보안업무 추진계획 : 1. 25限
2. 보안업무 심사분석 : 10. 15限

제8조(정보통신 보안감사) ① 행정기관의 장은 년1회 이상 본청 및 소속기관에 대하여 자체 정보통신에 대한 보안감사를 실시하여야 한다.

② 행안부장관은 "시행규칙 제64조" 및 "시행요강 제3조제4항 및 제47조"의 규정에 의거 특별시, 광역시, 도, 특별자치도(이하 "시・도"라 한다)를 대상으로, 시・도

지사는 소속 시·군 및 자치구를 대상으로 정보통신에 대한 보안감사와 불시 점검을 병행하거나 별도로 실시할 수 있다.

③ 행정기관의 장은 제1항 및 제2항의 정보통신 보안감사 또는 불시점검을 실시할 경우에 제도적인 문제점 발굴에 중점을 두고 수행하여야 하며 도출된 취약요인은 근본적 대책을 수립하여 개선하여야 한다.

④ 행정기관의 장은 정보통신에 대한 보안감사 실시계획과 감사결과를 다음 각 호의 기한 내에 행안부장관에게 제출하여야 한다. 이 경우 제출기한은 매년도 「보안업무 수행지침」에서 규정한 기한을 우선 적용하며, 불시검검 결과는 제7조에 의한 심사분석에 포함하여야 한다.

1. 연도 정보통신 보안감사 실시계획 : 2.28限
2. 정보통신 보안감사 실시결과 : 10.15限

⑤ 행정기관의 장은 보안감사의 효율적 수행을 위하여 행안부장관에게 감사의 방향, 중점사항, 감사관 지원 등의 업무협조를 요청할 수 있다.

제9조(보안지도방문) ① 행정기관의 장은 “시행요강 제3조제4항”에 의거 정보통신의 운영에 관하여 보안에 취약한 분야를 개선하기 위한 보안지도방문(이하 “지도방문”이라 한다)을 실시하여야 한다.

② 지도방문 실시의 주관 및 대상기관은 제8조제2항을 준용하고 지도방문 실시 결과에 대해서는 제7조의 정보통신보안업무 심사분석에 포함시켜야 한다.

③ 행정기관의 장은 본청 및 소속기관 등에 지도방문을 실시할 경우에는 별표 3의 “정보통신보안 점검항목” 및 “국가사이버안전매뉴얼 보안점검항목”을 적극 활용하여야 한다.

④ 행정기관의 장은 정보통신의 운영에 관하여 보안취약성 진단과 보안관리 개선을 수행하기 위해 행안부장관 또는 국정원장에게 지도방문을 요청할 수 있다.

제10조(재난방지) ① 행정기관의 장은 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애발생에 대비하여 정보시스템 이원화, 백업관리, 복구 등 종합적인 재난방지대책을 수립·시행하여야 한다.

② 행정기관의 장은 재난방지 대책을 정기적으로 시험하고 검토해야 하며 업무 연속성에 대한 영향평가를 실시하여야 한다.

③ 행정기관의 장은 정보시스템 장애에 대비한 백업시설을 확보하고 정기적으로 백업을 수행하여야 한다.

④ 행정기관의 장은 제3항에 의거 백업시설을 설치할 경우에는 정보통신실과 물리적으로 일정거리 이상 위치한 안전한 장소에 설치하여야 하며 전력공급원 분리 등 정보시스템의 가용성을 최대화 할 수 있도록 하여야 한다.

제11조(사이버・보안 진단의 날) ① 행정기관의 장은 매월 세 번째 수요일을 "사이버・보안 진단의 날"로 지정하여 운영하여야 한다. 다만, 당해 기관의 실정에 따라 주와 요일을 달리 지정하여 운영할 수 있다.

② 정보통신보안담당관은 "사이버・보안 진단의 날"에 소관 정보통신망의 악성코드 감염 여부, 정보시스템의 보안 취약여부 등 정보통신보안업무 전반에 대하여 체계적이고 종합적인 보안진단을 실시하여 보안취약성을 발굴・개선하여야 한다.

③ 행정기관의 장은 제2항에 따른 보안취약성 발굴・개선 실적을 심사분석에 포함하여야 한다.

제12조(정보통신보안 위규) ① 행정기관의 장은 국가안보 및 국가이익에 중대한 영향을 미칠 수 있다고 판단되는 별표 1의 정보통신보안 위규사항이 발생된 경우에는 가장 신속한 방법으로 행안부장관을 거쳐 국정원장에게 통보하여야 한다.

③ 행정기관의 장은 제1항의 정보통신보안 위규를 적발했을 때는 위규자, 위규내용 및 조치사항을 행안부장관을 거쳐 국정원장에게 통보하여야 한다.

제13조(보안사고 처리 및 조사) ① 행정기관의 장은 별표 2의 정보통신 보안사고가 발생한 때에는 즉시 피해를 최소화하도록 조치를 취하고, 다음 각호의 사항을 행안부장관을 거쳐 국정원장에게 통보하여야 한다.

1. 일시, 장소, 사고원인, 피해현황 등 개요
2. 사고자 및 관계자의 인적사항
3. 피해 내용 및 원인
4. 조치내용 및 향후대책 등

② 행정기관의 장은 행안부장관이 사고발생 기관에 대한 사고조사를 실시할 때에는 적극 협조하여야 한다. 다만, 경미한 사고발생에 대해 행안부장관이 행정기관의 장에게 사고조사를 위임한 경우에 행정기관의 장은 자체 사고조사를 실시하고 제반 보안조치를 취하여야 하며 그 결과를 행안부장관에게 통보하여야 한다.

④ 행정기관의 장은 정보통신 보안사고 관련자를 관련규정의 징계기준에 의거 처벌토록하며 사고조사 및 징계결과를 행안부장관을 거쳐 국정원장에게 통보하여야 한다.

제14조(정보통신보안 교육) ① 행정기관의 장은 다음과 같이 정보통신에 대한 보안교육계획(외부전문기관 위탁교육 포함)을 수립·시행하여야 한다.

1. 본청 및 소속기관 : 년1회이상
2. 공무원교육기관 : 3일이상 교육과정 년1회이상

② 행정기관의 장은 정보통신에 대한 보안교육의 효율성을 제고시키기 위하여 행정기관별 자체 실정에 맞는 보안교육 교안 및 교재를 작성하여 교육을 실시하여야 한다. 이 경우 행안부장관 또는 국정원장에게 전문인력 및 자료의 지원을 요청할 수 있다.

③ 행정기관의 장은 정보통신보안 관련 전문기관 교육 및 기술 세미나 참석을 장려하는 등 정보통신보안 담당자의 업무 전문성을 제고하기 위하여 노력하여야 한다.

제 2 장 정보 및 정보통신망 보안

제1절 보안관리 행정

제15조(정보통신보안 내규 제·개정) 행정기관의 장은 정보통신보안 업무수행을 위하여 이 규정에 저촉되지 아니하는 범위 내에서 당해 기관의 정보통신보안 내규(지침·규정·시행규칙 등)를 정하여 시행할 수 있다.

제16조(정보통신 보안성 검토) ① 행정기관의 장은 다음 각호의 경우에는 자체 보안대책을 강구하고 국정원장에게 보안성 검토를 의뢰하여야 한다. 다만, 국정원장과 사전 협의를 통해 사안이 경미하다고 판단된 경우에는 보안성 검토를 생략하거나 절차 및 제출자료 등을 간소화할 수 있다.

1. 유·무선 네트워크를 신·증설하거나 정보시스템을 구축 또는 교체하는 경우
2. 내부 정보통신망을 외부망과 연결하고자 하는 경우
3. 국정원장이 개발하거나 안전성을 검증한 암호장비·보안자재·암호논리·암호모듈·정보보호시스템을 도입 운용하고자 할 경우. 단, 암호장비·보안자재·암호논리·암호모듈·정보보호시스템 자체에 대한 검증은 제56조, 제63조, 제92조, 제98조에 따른다.
4. 무선랜 등 무선망을 사용하여 업무를 처리하거나 원격근무 지원 등을 위해 정보시스템을 도입하는 경우
5. 외부기관 및 업체에 정보통신망 보안감리 또는 보안컨설팅(보안취약점 분석·평가 포함)을 받거나 정보처리·보안관제 등 업무를 위탁하는 경우
6. 기타 정보통신 운용환경 변화로 인하여 별도의 보안대책 수립이 필요하다고 인정되는 경우

② 행정기관의 장은 당해 년도의 정보통신 보안성 검토 대상사업 현황을 1월 25일 이전에 국정원장에게 제출하여야 한다. 이 경우 제7조의 규정에 의한 세부추진계획을 활용하거나 별도로 제출할 수 있다.

③ 행정기관의 장은 정보통신 보안성 검토를 요청할 경우 자체적으로 보안대책을 수립한 후 행정안전부는 국가정보원의 본부에 지방자치단체는 해당지역을 관할하는 국가정보원의 지부에 요청한다.

④ 행정기관의 장은 보안성 검토를 요청할 경우에 다음 각호의 서류를 제출하여야 한다.

1. 사업 목적 및 추진계획
2. 사업계획서
3. 기술제안요청서(RFP)
4. 정보통신망 구성도
5. 자체 보안대책 강구사항
6. 암호논리 지원을 요청할 경우에 제93조제2항에 근거한 자료
7. 상용 보안시스템의 보안적합성 검증을 병행하고자 할 경우 제101조에 근거한 자료

⑤ 제4항제5호의 자체 보안대책 강구사항에는 다음 각호를 포함하여야 한다.

1. 보안관리 수행체계(조직, 인원) 등 관리적 보안대책
2. 정보시스템 설치장소에 대한 보안관리방안 등 물리적 보안대책
3. 국가용 보안시스템 및 국정원장이 개발하거나 안전성을 검증한 암호모듈·정보보호시스템 도입 운용 계획
4. 국가기관 간 망 연동할 경우 당해 기관 간 보안관리 협의사항
5. 서버, 단말기, 보조기억매체, 네트워크 등 정보통신망의 요소별 기술적 보안대책
6. 재난복구 계획 또는 상시 운용계획

⑥ 제1항의 보안성 검토를 요청할 경우에는 행정안전부 정보통신보안 업무 시책과 상충할 소지가 있는지에 대하여 면밀히 검토하여야 하며 필요 시 이를 행안부장관과 협의하여야 한다. 다만, 행정안전부 본부 및 소속기관은 제3항의 보안성 검토 요청을 위한 자료를 정보통신보안담당관에게 통보하여야 한다.

제2절 전자정보 보안

제17조(전자정보 보안조치) 행정기관의 장은 전자정부서비스에 대한 보안 강화 및 정보통신망을 통하여 보관·유통되는 전자정보의 유출·위조·변조 또는 훼손 등을 방지하기 위하여 다음 각호의 보안조치를 이행하여야 한다.

1. 「전자정부법」 제27조 등 관계 법령에 규정된 전자정보 보안대책의 수립·시행
2. 「행정기관 정보시스템 접근권한 관리규정(국무총리훈령)」(이하 “접근권한 관리규정” 이라 한다)에 따른 전자정보의 접근권한 정책 수립·시행
3. 전자정보의 백업체계 수립·시행 및 타 행정기관 또는 다른 안전한 지역에 별도 보관
4. 전자정보(보조기억매체 포함)의 보유현황 관리
5. 전자정보 및 장비의 반출 또는 반입 통제

6. 불법접근 및 해킹프로그램·웜·바이러스 감염피해 예방
7. 기타 행안부장관·국정원장이 제공하는 보안대책, 지침·매뉴얼 및 권고사항의 이행

제18조(전자정보 보호등급 분류) ① 행정기관의 장은 비밀이 아닌 중요 전자정보의 효율적인 보호를 위하여 다음 각호에 해당하는 경우에는 자체 실정에 맞는 보호등급을 분류하여야 한다.

1. 최초로 정보통신망을 신설하여 전자정보의 보호등급 구분이 필요한 경우
2. 현재 운용중인 정보통신망을 재구성할 경우. 다만, 국정원장과 사전 협의를 통해 사안이 경미하다고 판단되는 경우 기존 보호등급을 적용한다.
3. 행정기관의 장이 필요하다고 인정하는 경우

② 제1항의 규정에 의한 전자정보의 보호등급 분류는 다음 각호와 같이 구분한다.

1. '가'급 : 유출 또는 손상되는 경우 행정기관의 업무수행에 중대한 장애를 초래하거나 개인 신상에 심각한 영향을 줄 수 있는 전자정보
2. '나'급 : 유출 또는 손상되는 경우 행정기관의 업무수행에 장애를 초래하거나 개인 신상에 영향을 줄 수 있는 전자정보
3. '다'급 : 유출 또는 손상되는 경우 행정기관의 업무수행 및 기관의 이미지에 경미한 영향을 줄 수 있는 전자정보

③ 행정기관의 장은 제2항에 따른 보호등급을 분류하기 위한 자체 기준을 수립하여야 한다. 다만, 소속기관에 대한 분류기준은 행정기관의 장이 수립한다.

④ 행정기관의 장이 보호등급 분류기준을 정하고자 할 경우에는 행안부장관·국정원장이 제정한 지침이나 다른 법령에서 규정하고 있는 분류기준을 참고할 수 있다.

⑤ 행정기관의 장은 제2항의 규정에 의하여 분류된 전자정보를 보호하기 위하여 정보보호시스템 구축 등을 추진할 경우 제99조의 규정에 의한 검증제품 중에서 선택하여 국정원장에게 보안적합성 검증을 신청하여야 한다.

제19조(비밀 전자정보 보안조치) ① 행정기관의 장은 비밀 등 중요 전자정보를 정보통신망을 이용하여 생산·보관·분류·열람·출력·송신·수신 또는 이관하는 등 전자적으로 처리하기 위해서는 국가용 보안시스템을 사용하여 암호화하는 등 국정원장이 안전성을 확인한 보안조치를 수행하여야 한다.

② 비밀을 전자적으로 생산하고자 할 때에는 해당 비밀등급과 "시행요강 제24조의2"에 따른 예고문을 입력하여 열람 또는 출력할 경우 비밀등급이 자동으로 표시되도록 하여야 한다.

③ 비밀을 전자적으로 생산·열람·출력·송신·수신 또는 이관할 경우 작업내용을 전자적으로 기록 유지하여야 하며, 송신·수신할 경우에는 정당성 확인 및 부인방지를 위하여 전자적으로 생성된 영수증을 사용하여야 한다. 다만, 전자적으로 처리된 비밀을 종이문서로 출력한 이후의 취급관리는「보안업무규정」등에 따른다.
④ 비밀 생산을 완료한 경우에는 PC에 입력된 비밀내용을 즉시 삭제하여야 한다. 다만, 업무상 계속 보관할 경우에는 관리책임자의 승인 하에 비밀용 보조기억매체에 저장할 수 있다. 이 경우 보안시스템을 이용하여 암호화하는 등 적절한 보안대책을 강구하여야 한다.
⑤ 행정기관의 장은 비밀을 전자적으로 안전하게 처리하기 위하여 접근제어, 기밀성, 부인방지 및 인증 등 보안기능을 제공하며 이 과정에서 발생하는 모든 정보를 기록 관리하는 기능을 가지는 정보시스템(이하 “비밀관리시스템”이라 한다)을 구축 또는 자체 개발하여 운용하고자 하는 경우에는 미리 국정원장의 승인을 받아야 한다.

제3절 정보통신시설 보안

제20조(중요 정보통신시설 보안관리) ① 행정기관의 장은 “시행요강 제43조”에 의거 다음 각호에 해당하는 경우 중요 정보통신 시설 및 장소를 보호구역으로 설정하여야 한다.

1. 암호실
2. 정보통신실
3. 통합전산센터
4. 국가용 보안시스템 개발·설치 장소
5. 경호통신, 국가비상통신 등 중요통신망의 교환국, 회선집중국 또는 중계국
6. 백업센터 및 중요한 정보통신시설을 집중 제어하는 장소
7. 기타 보안관리가 필요하다고 인정되는 정보시스템 설치 장소

② 행정기관의 장은 제1항에서 지정된 보호구역에 대한 보안 대책을 강구할 경우 다음 각호의 사항을 참고하여야 한다.

1. 방재대책 및 외부로부터의 위해(危害) 방지대책
2. 상시 이용하는 출입문은 한 곳으로 정하고 이중 잠금장치 설치
3. 출입문 보안장치 설치 및 주·야간 감시대책
4. 보조기억매체를 보관할 수 있는 용기 비치
5. 정보시스템 안전지출 및 긴급파기 계획 수립

6. 관리책임자 및 자료·장비별 취급자 지정 운용
7. 정전에 대비한 비상전원 공급, 시스템의 안정적 중단 등 전력관리 대책
8. 비상조명 장치 등 비상탈출 대책
9. 전자파 누설 방지대책
10. 카메라 장착 휴대폰 등을 이용한 불법 촬영 방지대책
11. 비인가자의 출입 및 정보자산의 반출·입 통제 등

③ 행정기관의 장은 제1항에서 지정된 보호구역에 대한 보안취약 요인을 발굴·개선하거나 외부의 위협요소로부터 보호대책을 강구하기 위하여 정기적으로 보안점검을 실시하여야 한다.

제21조(기반시설 보안관리) ① 행정기관의 장은 소관 정보통신시설이 「정보통신기반보호법」제8조의 규정에 의한 국가안보와 국민생활의 안정을 보장하는 주요 정보통신기반시설(이하 "기반시설"이라 한다)의 지정기준에 부합하는지 여부를 검토하여야 한다.

② 기반시설을 관리하는 기관(이하 "관리기관"이라 한다)의 장은 「정보통신기반보호법」및 同法시행령에 따라 기반시설에 대한 보호대책을 수립·시행하여야 하며, 공항·전력·가스·원자력 등 국가안보상 중요한 기반시설의 정보통신망은 인터넷 등 상용망과 분리 운용함을 원칙으로 한다.

③ 관리기관의 장은 외부기관에 의뢰하여 보안취약점 분석·평가를 수행하는 경우 취약점 분석·평가 세부 결과를 그 중요성과 가치의 정도에 따라 대외비 또는 비밀로 지정 관리하여야 한다.

제22조(대도청 방지대책) ① 행정기관의 장은 청사(해외공관 포함)를 신설·이전 또는 증·개축하고자 할 때에는 도청방지 대책을 강구하여야 한다.

② 행정기관의 장은 전자파 방출 또는 도청장치에 의한 정보 유출을 방지하기 위하여 다음 각호를 대상으로 대도청(對盜聽) 측정 계획을 수립·시행할 수 있다.

1.「보안업무규정」에 의한 행정기관의 주요 시설, 지역, 정보통신망
2. 기관장 및 주요간부의 사무실, 주요 회의실
3. 행정기관의 해외공관 및 해외무역관 등

③ 행정기관의 장은 도청징후를 포착하였거나 중요한 협상이나 회의 또는 회담을 개최하는 장소 및 공사가 진행 중인 주요시설 등에 대하여 국정원장에게 대도청 측정을 요청할 수 있다.

④ 카메라 장착 휴대폰 등을 이용하여 불법적으로 내부 중요자료나 제20조제1항의 중요시설에 대한 사진촬영을 금지토록 하는 등 보안대책을 강구하여야 한다.
⑤ 행정기관의 장은 디지털·레이저 등 첨단도청장치에 의한 불법도청을 방어하기 위한 시스템을 도입할 경우 국정원장과 사전 협의하여야 한다.
⑥ 행정기관의 장은 비의도적인 전자파 발생 또는 침입 전자파에 의한 기밀유출 방지를 위하여 관련 장비를 도입하고자 할 경우 국정원장과 사전 협의하여야 한다.
⑦ 행정기관의 장은 전자파 차폐실을 구축할 경우에는 국정원장이 제정한 「전자파 차폐실 구축 및 측정기준」에 따른다.
⑧ 행정기관의 장은 주요 사무실에 차폐유리·도료 등 차폐재료 설치를 권장하고 전자파장애(EMI)·전자파적합성(EMC) 검증을 받은 정보시스템을 사용하여야 한다.
⑨ 행정기관의 장은 대도청 측정결과 도출된 문제점에 대하여 국정원장과 협의하여 필요한 보안방책을 수립·시행하여야 한다. 이 경우 대도청측정 계획 및 결과에 관한 내용을 외부에 공개하여서는 아니 된다.

제4절 정보시스템 보안

제23조(정보시스템 보안관리) ① 행정기관의 장은 정보시스템의 효율적인 보안관리를 위하여 정보시스템별로 관리책임자(이하 '시스템관리자'라 한다)를 지정 운영하여야 한다.
② 시스템관리자는 운영되는 정보시스템이 비인가자에게 불필요한 서비스를 허용하지 않도록 보안기능을 설정하여야 하며, 보안취약점을 제공할 수 있는 다음 각호의 프로그램의 설치를 제한하여야 한다.
1. P2P, 웹하드 등 파일 공유 프로그램
2. 메신저 프로그램 등

③ 시스템관리자는 서버를 도입할 경우 별지 제4호서식의 정보시스템 관리대장에 따라 그 하드웨어 목록을 유지·관리해야 하며, 비인가자가 접근할 수 없도록 물리적인 접근통제 장치가 마련된 공간에 서버를 설치해야 한다.
④ 시스템관리자는 소관 시스템의 안정적 운영을 위해 다음 각호에 따라 관리해야 한다.
1. 신규로 설치되는 시스템은 취약점 점검 및 제거 후 네트워크에 연결
2. 사용 중인 운영체제는 최신의 패치 프로그램 설치, 주기적인 패치 실행
3. 설치·운영 중인 서버의 수시 보안취약점 발굴 및 보안조치

⑤ 시스템관리자는 외부자가 전산실에 출입하여 서버와 관련된 작업을 할 경우 이를 운영하는 담당공무원이 입회·감독하도록 해야 한다.

제24조(웹서버 등 보안관리) ① 행정기관의 장은 외부자에게 공개할 목적으로 설치되는 웹서버 등 각종 공개서버는 내부망(업무망)과 분리하여 운영하고 보안 적합성이 검증된 침입차단·탐지시스템을 설치하는 등 보안대책을 강구하여야 한다.

② 시스템관리자는 공개서버의 서비스에 필요한 프로그램을 개발하고 시험하기 위해 사용된 도구(컴파일러 등)는 개발 완료 후 사용이 제한되도록 보안기능을 설정하거나 삭제하여야 한다.

③ 시스템관리자는 보안사고에 대비하여 서버 설정 정보, 저장 자료 및 프로그램(Source Code)에 대하여 정기적인 백업체계를 구축하여야 한다.

④ 시스템관리자는 홈페이지 게재내용에 비밀 등 비공개 자료가 포함되지 않도록 하여야 하며, 공개서버를 통해 개인정보가 유출 또는 위·변조되지 않도록 보안대책을 강구하여야 한다.

⑤ 시스템관리자는 행안부장관 또는 국정원장이 제공하는 홈페이지 보안관리 개선대책, 매뉴얼 등에 따라 주기적으로 홈페이지의 취약점을 점검·제거하여야 한다.

제25조(접근권한 관리) ① 행정기관의 장은 "접근권한 관리규정"에 따라 소관 정보시스템의 이용자에 대한 본인확인 및 접근권한 관리를 위하여 다음 각호의 조치를 수행하여야 한다.

1. 접근권한관리책임자(이하 "권한관리책임자"라 한다)의 지정·운영.
2. 기관별 특성에 맞는 접근권한 정책의 수립 및 이행
3. 연 1회이상 접근권한 정책의 이행여부 확인
4. 접근권한의 불법적 이용에 대하여 수시 확인·감독 등

② 접근권한은 법령 또는 업무규정 등에 따라 허용된 자에 한하여 업무수행에 필요한 최소한의 범위로 업무담당자에 따라 차등적으로 부여하여야 한다.

③ 비밀 등 중요 정보를 취급하는 정보시스템의 경우 전자인증서와 별도로 바이오정보, 일회용 비밀번호(OTP) 등을 이용한 인증방식을 복수로 채택하는 등 안전성을 강화할 수 있는 방안을 강구하여야 한다.

제26조(접근기록 관리) ① 행정기관의 장은 "접근권한 관리규정"에 따라 정보시스템 및 행정정보의 이용내역을 기록·보관·관리하여야 한다.

1.「공공기관의 정보공개에 관한 법률」제9조에 따른 비공개 대상정보의 경우 이용자의 식별, 접근 등 정보를 기록으로 남길 수 있는 정보시스템 구축·운영
2. 전산자료의 보호등급에 따라 최소한 3년이상 보관
3. 권한관리책임자의 사전 승인 없이 시스템관리자 외에는 접근금지 조치
4. 이용내역 기록이 변경 또는 삭제될 수 없도록 시스템 구축 등 보안조치 강구

② 시스템관리자는 접근기록을 분석한 결과 비인가자의 접속 시도, 정보 위·변조 및 무단삭제 등의 의심스러운 활동이나 위반혐의가 발생한 사실을 발견한 경우 정보통신보안담당관에게 즉시 보고하여야 한다.

③ 정보통신보안담당관은 제2항에 따라 접근기록을 검토·분석한 후 이상 징후를 발견한 경우 제52조 내지 제55조에서 정한 바에 따라 대응·조치해야 한다.

제27조(사용자계정 관리) ① 시스템관리자는 사용자계정(ID)의 비인가자 도용 및 정보시스템 불법접속 등을 방지하기 위해 다음 각호 사항을 반영·관리하여야 한다.

1. 신규 사용자계정 생성 시 신청서 작성, 신원확인 등의 절차를 거쳐 발급
2. 퇴직 또는 보직변경 등으로 사용자계정을 해지해야할 때에는 신속히 삭제
3. 사용자별 또는 그룹별로 접근권한 부여, 사용자계정을 공동으로 사용 금지
4. 외부 사용자의 계정부여는 불허하되, 부득이한 경우에는 행정기관장의 책임하에 유효기간을 설정하는 등 보안조치를 강구한 후 허용
5. 비밀번호 등 사용자 식별·인증 수단이 없는 사용자계정은 사용 금지
6. 장시간 사용하지 않는 휴면계정을 점검하여 필요하지 않은 경우 삭제
7. 계정을 주기적(사용자계정 6개월, 관리자계정 3개월)으로 점검하여 접근권한을 재검토하고 권한 남용을 감시

② 정보시스템의 계정은 사용목적 및 권한에 따라 관리자계정과 사용자계정으로 분류하여 관리하여야 한다.

③ 관리자계정은 관리자로 지정된 자만이 사용할 수 있으며, 그 외의 자에게는 대여할 수 없다. 다만, 업무상 필요에 의해 부득이하게 타인에게 대여한 경우에는 회수 후 즉시 비밀번호 변경 등의 보안조치를 해야 한다.

④ 시스템관리자는 연속으로 3회이상 로그인을 실패하거나 제공된 권한이상으로 접근을 시도하는 등 위반사항이 발견된 경우 정보통신보안담당관에게 해당 사실을 통지하고 비인가자의 침입여부를 확인·점검해야 한다.

⑤ 시스템관리자와 정보통신보안담당관은 제4항의 이상 접근시도에 대하여 점검한 결과, 불법접근 등 위반사항이 발견된 경우 해당 계정의 사용자에게 관련사실을

통지하고 위반경위를 확인하여 계정삭제 등의 필요한 조치를 해야 한다.

⑥ 시스템관리자는 정보시스템별로 계정발급현황을 별지 제27호서식의 사용자계정 관리대장에 현행화하여 관리해야 한다.

⑦ 시스템운영자는 사용자계정을 등록·변경 또는 폐기할 경우 시스템관리자의 승인하에 수행하고 그 결과를 "사용자계정 관리대장"에 등재하여 관리하여야 하며 정보통신보안담당관에게 보고하여야 한다. 이 경우 제6항 및 제7항에 따른 사용자계정의 발급, 변경 및 삭제 등 관련 작업을 계정관리시스템을 도입하여 전자적으로 수행할 수 있다.

제28조(비밀번호 관리) ① 시스템관리자는 정보시스템 비밀번호의 무단사용 방지를 위하여 다음 각호와 같이 비밀번호를 구분하여 사용하여야 한다.

1. 비인가자의 정보시스템 접근방지를 위한 접근용 비밀번호(1차)
2. 사용자가 정보시스템 접속 시 인가된 인원인지 여부를 확인하는 사용자인증(2차)
3. 문서의 열람·수정 및 출력 등 사용권한을 제한할 수 있는 자료별 비밀번호(3차)

② 시스템관리자는 비밀이나 중요자료에는 반드시 자료별로 비밀번호를 부여하여야 한다. 다만, 공개 또는 열람을 위한 자료에 대하여는 그러하지 아니할 수 있다.

③ 시스템관리자는 다음 각호의 사항을 반영하여 정보시스템의 비밀번호를 설정하고 분기 1회이상 주기적으로 변경해야 한다.

1. 영문, 숫자와 문자 및 특수문자 등을 조합하여 8자리이상으로 설정
2. 사용자계정(ID)과 동일하지 않은 것
3. 개인 신상 및 부서명칭 등과 관계가 없는 것
4. 일반 사전에 등록된 단어는 사용을 피할 것
5. 이미 사용된 비밀번호는 재사용하지 말 것
6. 동일 비밀번호를 여러 사람이 공유하여 사용하지 말 것
7. 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지
8. 관리자계정과 사용자계정의 비밀번호를 다르게 부여
9. 초기 할당된 임시 비밀번호는 사용자 로그인 후 즉시 변경

④ 시스템관리자는 정보시스템에 등록되어있는 비밀번호를 암호화하여 보관하여야 한다.

제29조(악성코드 방지) ① 행정기관의 장은 웜·바이러스, 해킹프로그램, 스파이웨어 등 악성코드 감염을 방지하기 위하여 예방대책을 수립·시행하여야 한다.

② 시스템관리자 및 개인용 장비사용자(이하 “시스템운영자”이라 한다)는 악성코드 감염을 방지하기 위하여 다음 각호에 따라 정보시스템을 관리·운영하여야 한다.

1. 출처, 유통경로 및 제작자가 명확하지 않은 응용프로그램은 사용을 자제하고 불가피한 경우 백신 등 검색프로그램으로 진단 후 사용
2. 업무상 불필요한 서비스는 제한
3. 실행파일은 읽기 전용으로 속성을 변경
4. 출처가 불분명한 전자우편은 열람하지 않아야 하며 자동으로 첨부파일이 실행되지 않도록 설정
5. 인터넷 등 상용망으로 입수한 자료는 필히 악성코드 여부 검색 후 사용
6. 악성코드 조기 발견을 위하여 최신 백신프로그램 활용 및 보안 업데이트 실행
7. 정보시스템이 작동할 때마다 컴퓨터 하드디스크의 부트섹터 또는 메모리 등에 악성코드가 감염되었는지 점검

③ 시스템운영자는 악성코드 감염이 발견되었을 경우 다음 각호의 조치를 하여야 한다.

1. 악성코드 감염피해를 최소화하기 위하여 감염된 시스템의 사용 중지 및 내부망과 접속 분리
2. 최신 백신 등 악성코드 제거 프로그램을 이용하여 퇴치
3. 악성코드의 감염확산 방지를 위하여 정보통신보안담당관에게 관련내용 및 보안조치 사항을 즉시 보고
4. 악성코드 감염의 재발을 방지하기 위하여 원인분석 및 예방조치 수행

④ 시스템운영자는 악성코드가 신종이거나 감염피해가 심각하다고 판단할 경우에는 관련사항을 정보통신보안담당관을 거쳐 행안부장관에게 신속히 보고하여야 한다.

⑤ 행안부장관 또는 국정원장이 악성코드 감염사실을 확인하여 조치를 권고할 경우 시스템운영자는 즉시 이를 이행하여야 한다.

제5절 PC·보조기억매체·전자우편 보안

제30조(PC 등 보안관리) ① 행정기관의 장은 PC, 단말기(업무용), 노트북 등(이하 “개인용 장비”라 한다)을 사용할 경우에 취급자 또는 관리책임자(이하 “관리책임자”라 한다)를 지정하여야 한다. 이 경우 사용자를 별지 제4호서식의 정보시스템 관리대장에 등재하여야 하며 제27조 내지 제28조의 규정을 준용하여야 한다.

② 관리책임자는 비인가자가 무단으로 개인용 장비 등을 조작하여 전산자료를 유출하거나 위·변조 및 훼손시키지 못하도록 다음 각 호에 정한 보안대책을 강구하여야 한다.

1. 장비별·자료별 및 사용자별로 비밀번호 사용
2. PC 하드웨어 CMOS, 운영체제 로그인 및 화면보호기에 각각 비밀번호 설정
3. 10분이상 작업을 중단할 경우 비밀번호가 적용된 화면보호기 설정
4. 백신, PC용 침입차단시스템 등 운용 및 주기적(최소 월1회이상) 보안패치 실시
5. P2P, 해킹용 S/W 등 업무와 무관하거나 보안에 취약한 프로그램의 사용금지

③ 관리책임자는 개인용 장비 등을 교체·반납 또는 폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 하드디스크에 수록된 자료가 유출 또는 훼손되지 않도록 보안조치를 강구하여야 한다.

④ 개인용 장비를 반출·입할 경우 별지 제23호서식의 보조기억매체(전산장비 포함) 반출·입 대장에 등재한 후 관리책임자의 승인을 얻어 제29조의 보안조치를 한 후 반입 또는 반출할 수 있다.

⑤ 관리책임자는 출장 또는 휴가 등으로 장시간 이석할 때에 휴대용 단말기를 시건장치가 있는 사물함 등 안전한 장소에 보관하거나 도난방지 케이블을 설치하여 관리하여야 한다.

제31조(보조기억매체 관리) ① 행정기관의 장은 보조기억매체를 안전하게 관리하기 위하여 각 부서의 장 등을 보조기억매체 관리책임자(이하 "관리책임자"라 한다)를 지정하여 운영하여야한다.

② 행정기관의 장은 USB 등 보조기억매체를 안전하게 관리하기 위하여 보안USB·관리시스템 등 보안관리시스템 구축을 위해 노력하여야 한다.

③ 관리책임자는 보조기억매체를 일반용, 비밀용(대외비 포함) 및 공인인증서용으로 구분하여 각각 별지 제20호 서식의 보조기억매체 라벨을 작성하고 별도의 보조기억매체 관리대장(별지 제21-1호서식 내지 제21-3호서식)에 등록한 후에 사용토록 하여야 한다.

④ 관리책임자는 사용자가 보조기억매체를 제3항과 같이 등록된 경우에만 사용하고 업무목적 이외에 사적인 용도로 사용할 수 없도록 하여야 한다. 다만, 공인인증서용에 한하여 등록 후 개인소지 및 사용을 허가할 수 있다.

⑤ 관리책임자는 보조기억매체에 대외비이상 비밀자료를 보관하고자 하는 경우 다음 각호와 같이 관리하여야 한다.

1. "시행규칙"의 비밀관리기록부에 등재·관리하며 이중캐비넷 또는 금고에 보관
2. 비밀 작업 및 보관을 하는 경우 그 작업을 완료하거나 일시 중단할 때에는 PC에서 즉시 분리

3. 비밀등급별로 각각 보조기억매체를 마련하여 하나의 보조기억매체에 등급이 다른 비밀 또는 대외비를 혼합하여 보관 금지

⑥ 관리책임자는 월1회이상 보조기억매체의 수량 및 보관 상태를 점검하고 별지 제22호서식의 보조기억매체 점검대장에 확인·서명하여야 한다.

⑦ 관리책임자는 보조기억매체를 반입 또는 반출할 때에 별지 제23호서식의 보조기억매체 반출·입 대장에 이를 기록·관리하여 무단 반·출입을 통제하여야 한다. 다만, 사적소지가 허용된 공인인증서용은 제외할 수 있다.

⑧ 관리책임자는 보조기억매체를 파기 등 불용처리하거나 비밀용을 일반용 또는 다른 등급의 비밀용으로 전환하여 재사용할 경우 저장되어 있는 정보가 복구되지 못하도록 제32조에 따른 조치를 하여야 한다. 이 경우 별지 제24호서식의 보조기억매체 불용처리 확인서에 정보통신보안담당관의 확인을 받아 이를 보관하여야 한다.

제32조(정보시스템 저장매체 불용처리) ① 행정기관의 장은 PC·복사기·팩스 등의 정보시스템 저장매체를 교체, 반납, 양여, 폐기 또는 보안 통제할 수 없는 공간으로 이동하는 등 불용처리 할 경우 수록된 정보가 복구되어 유출되지 않도록 삭제 조치하여야 한다.

② 제1항의 자료를 삭제할 경우 저장된 자료와 매체의 특성에 따라 다음 각호 중 조직별로 실정에 맞는 방법을 선택하여 조치하여야 한다.

1. 완전파괴(소각·파쇄·용해) : 파쇄조각 크기가 0.25mm 이하가 되도록 조치
2. 전용 소자장비 이용 삭제 : 저장매체의 자기력 보다 큰 자기력을 가진 소자장비로 자기력을 소거
3. 완전포맷 3회 수행 : 저장매체를 '난수', '0', '1'로 각각 중복 저장하여 삭제
4. 완전포맷 1회 수행 : 저장매체를 '난수'로 중복 저장하는 방식으로 삭제

③ 정보시스템의 사용자를 변경할 경우 저장자료를 다음 각호와 같이 삭제하여야 한다.

1. 비밀처리 정보시스템 : 완전포맷 3회이상
2. 일반 정보시스템 : 완전포맷 1회이상

④ 정보통신보안담당관은 정보시스템 저장자료의 삭제를 외부업체에 의뢰할 경우 작업장소에 입회하여 삭제 절차 및 방법의 준수여부 등을 확인·감독하여야 한다.

⑤ 행정기관의 장은 정보시스템 저장매체 불용처리 업무를 효율적으로 수행하기 위하여 저장장치의 자성을 완전히 소멸시키거나 데이터를 완전히 삭제시키는 전용 장비 또는 소프트웨어를 도입하여 사용할 수 있다.

제33조(전자우편 등 보안관리) ① 행정기관의 장은 당해 기관의 상용e-mail의 접속을 차단하고 직원들이 업무용으로 허용된 e-mail만 사용토록 해야 한다. 다만, 인터넷망과 업무망이 분리된 기관의 경우에 인터넷망에서 상용e-mail의 접속을 허용할 수 있다.
② 각 행정기관의 전자우편 사용자는 보안조치 없이 전자우편을 이용하여 중요 자료를 전송하지 못하며, 비공개 자료를 전자우편으로 송신하는 경우 해당 파일을 국정원장이 승인한 국가용 보안시스템으로 암호화하여야 한다.
③ 시스템관리자는 e-mail서버를 설치하는 경우 내부망에 설치하는 내부용 서버와 침입차단시스템 외부에 설치하는 외부용 서버를 서로 분리하여 운용하거나 이에 상응하는 적절한 보안대책을 수립한 후에 시행하여야 한다.

제6절 정보통신망 보안

제34조(정보통신망 현황·자료 관리) ① 행정기관의 장은 다음 각호에 해당하는 정보통신망 관련 현황 및 자료를 관리하고 보안에 유의하여야 한다.

1. 정보시스템 운용현황
2. 정보통신망 구성현황
3. IP 할당현황
4. 주요 정보화사업 추진현황

② 행정기관의 장은 다음 각호의 자료를 대외비로 분류하여 관리하여야 한다. 다만, 국가안보와 직결되는 중요한 정보통신망 관련 세부자료는「보안업무규정」, “시행규칙” 및 “시행요강”에 의한 비밀로 분류하여 관리하여야 한다.

1. 정보통신망 세부 구성현황(IP 세부 할당현황 포함)
2. 국가용 보안시스템 운용 현황
3. 보안취약점 분석·평가 결과물
4. 별지 제4호서식의 정보시스템 관리대장(다만 PC, 노트북 등 개인용 장비는 비밀번호를 기재한 경우에 해당)
5. 기타 보호할 필요가 있는 정보통신망 관련 자료

③ 서버 등 주요 정보시스템의 비밀번호를 종합기록 관리하고자 할 경우 별지 제4호서식의 정보시스템 관리대장에 등재하여 관리하여야 한다. 다만, PC 등 개인용 장비는 비밀번호를 기재하지 아니할 수 있다.
④ 제2항에 명시되지 않은 정보통신망 관련 대외비 및 비밀의 분류는 국정원장이 제정한 「비밀 세부분류지침」(대외비)을 따른다.

제35조(상용망 등 외부망 연동) ① 행정기관의 장은 중앙행정기관이나 소속기관 등과 외부 정보통신망을 연결하고자 하는 경우에 보안관리 책임한계 설정, 전자정보의 제공범위 및 이용자 접근제한 등에 대해 보안심사위원회의 심의를 거친 정보통신망 보안대책을 수립·시행하여야 한다. 이 경우 다음과 같은 보안조치를 하여야 한다.

1. 접속자료의 주기적 분석
2. 보안도구를 이용한 네트워크 취약성 수시 점검
3. 보안적합성이 검증된 침입차단·탐지 시스템 설치 운용 등 보안대책 실시
4. 연결지점을 지정 운영하여 임의 접속 차단

② 행정기관의 장은 정보통신망을 상용망(인터넷 포함)이나 다른 기관과 정보통신망을 연계하기 위한 보안관리 연결지점을 운용할 경우에는 비인가자의 무단침입(불법접속)이나 악성코드 및 사이버공격을 방지하기 위하여 국정원장이 검증한 보안시스템의 설치·운용 등 보안대책을 강구하여야 한다.

③ 행정기관의 장은 정보통신망 및 정보시스템에 사용되는 "IP주소"를 체계적으로 관리하여야 한다. 이 경우에 내부 정보시스템을 보호하기 위하여 사설주소체계(NAT : Network Address Translation)를 사용한다.

④ 행정기관의 장은 행정안전부의 종속망인 자체 정보통신망을 소속·민간기관(상용망 포함)·인터넷 등에 연계하여 내부망과 외부망을 연동하고자 할 경우에는 행안부장관과 사전 협의하여야 한다. 다만, 원격접속을 위하여 연계가 필요할 경우에는 제36조제2항에 따른 보안조치를 하고 행안부장관과 협의하여야 한다.

⑤ 행정기관의 장은 같은 청사를 사용하는 유관기관 등에서 상용망(인터넷 포함)을 이용하기 위해 정보통신망 이용요청이 있을 경우 내부망에 접근할 수 있는 IP부여를 금해야 한다.

⑥ 행정기관의 장은 인터넷을 통한 불법 사이트 접속이나 프로그램 다운로드를 금지하여야 하며, 개인용 장비에서 음란·도박·증권 등 업무와 무관한 인터넷 사이트 접근에 대한 통제대책을 강구하여야 한다.

⑦ 행정기관의 장은 비밀을 취급하는 정보통신망 또는 제21조제1항의 규정에 따른 기반시설의 네트워크는 상용망과 분리·운용하여야 한다.

제36조(원격근무 보안관리) ① 행정기관의 장은 재택·파견·이동근무 등 원격근무를 지원하기 위한 정보시스템을 도입·운영하고자 할 경우에 행안부장관과 사전 협의하여야 한다.

② 원격근무를 지원하고 있는 행정기관의 장은 다음 각호에 따라 관리하여야 한다.

1. 원격근무 사유(재택, 파견, 이동근무, 출장, 전산망 유지보수 등) 확인

2. 원격근무지원시스템의 사용기록을 보관하고 사용자, 사용자계정, 접속 주소와 시간 및 특이사항 등을 주기적으로 점검
3. 원격근무 완료 후 사용자계정 및 비밀번호의 신속한 회수
4. 원격근무 이용자에게 별지 제28호서식의 원격근무 보안서약서 징구
5. 별지 제29호서식의 원격근무 보안관리대장 작성 비치
6. 「별표4」의 원격근무 보안점검표의 점검사항에 따른 점검

③ 행정기관의 장은 제1항 및 제2항에 따라 원격근무를 지원하고 있거나 이를 지원하기 위한 정보시스템을 도입하고자 하는 경우 정부원격접속서비스(GVPN)의 이용 가능 여부를 사전에 확인하여, 활용 가능한 기관의 경우 이를 우선 활용하여야 한다.

제37조(원격정비 보안관리) 행정기관의 장은 정보시스템을 외부에서의 네트워크를 통해 원격으로 접속하여 정비하는 것을 원칙적으로 금지하여야 한다. 다만, 부득이한 경우에는 아래의 각호에 해당하는 보안대책을 강구하고 국정원장과 협의한 후 한시적으로 허용하여야 한다.

1. 원격접속 수행자에게 임시 접근권한 부여
2. 접근권한의 사용시간 명시, 시간경과 후 접근권한 삭제
3. 원격정비 시스템의 IP 사전 파악, 지정된 시스템에서만 수행
4. 원격시스템과의 통신정보를 점검하여 실행코드에 악성코드 유입 방지
5. 원격정비를 수행할 때 대상 정보시스템을 내부망과 분리
6. 원격 정비기록을 유지, 정비결과 시스템관리자에게 보고
7. 원격 정비자가 네트워크를 통해 원격지 컴퓨터 파일을 자신의 컴퓨터 파일처럼 접근하여 작업할 수 있도록 하는 등 해킹에 취약한 방식으로 원격정비 금지

제38조(무선통신 보안관리) ① 행정기관의 무선통신망(이하 “무선망”이라 한다) 운용을 위한 보안관리 방침은 다음과 같다.

1. 보안상 취약한 무선망의 신설 또는 증설 억제
2. 도서·내륙지역 취약무선망의 유선화·다원화 연차적 추진 등 보안대책 수립 추진
3. 국가 및 공공기관의 무선망으로 비밀 등 중요자료를 소통하고자 하는 경우 국가용 보안시스템을 사용
4. 무선망을 신규 도입 및 운용환경 변경하고자 할 때에는 국가용 보안시스템을 개발 적용할 수 있도록 입찰 조건에 명시
5. 관공서 통신시설(MTS 및 SSB 등)에 대한 보안대책 수립 추진

② 무선망을 운용하는 행정기관의 장은 다음 각호에 대하여 보안대책을 강구하여야 한다.

1. 전파월경 방지대책 강구
2. 무선망에 국가용 보안시스템 설치 운용
3. 무선국의 현황 관리와 보안지도 점검
4. 정보통신보안 위규, 보안취약성 근절을 위한 전파감시 및 전파측정
5. 공중통신망 이용 시 국가용 보안시스템 활용

③ 행정기관의 장은 무선랜을 구축·운용할 경우 제1항 및 제2항 이외에 다음과 같은 보안대책을 수립·시행하여 통신 내용을 보호하여야 한다.

1. 국가용 보안시스템 또는 국정원장이 안전성을 확인한 정보보호시스템 설치
2. 무선랜은 유선 네트워크 설치가 어려운 장소에 한하여 한시적으로 사용
3. 무선중계기(AP) 전파범위 조정, 사용자 인증, 패킷 암호화 등 보안대책 적용
4. 인가되지 않은 무선통신 장치 사용 여부 주기적 점검

제39조(국제통신 보안관리) ① 행정기관의 장은 국제전화·인터넷망·팩스 등 국제통신망에 의해 국가기밀 및 중요자료를 소통하고자 하는 경우 국정원장이 안전성을 확인한 다음 각호의 보안대책을 강구하고 사전에 국정원장에게 보안성검토를 요청하여야 한다.

1. 국정원장이 개발하거나 안전성을 검증한 암호장비·보안자재·암호논리·암호모듈·정보보호시스템의 도입 운용
2. 국정원장이 안전성을 확인한 정보통신망 보안대책의 시행

② 행정기관의 장은 국제통신망으로 업무와 관련된 사항을 송·수신하고자 할 경우에는 사전에 자료 및 소통내용에 대한 보안통제를 실시하여야 한다.

제40조(경호통신 운용관리) ① 국가원수 행사 및 경호업무 수행 중에는 경호통신망 이외의 다른 통신수단을 이용하여 송수신할 수 없다. 다만, 부득이한 경우에는 대통령실과 협의한 후 그러하지 아니할 수 있다.

② 경호업무를 수행·지원하는 행정기관의 장은 다음 각호의 사항을 소통할 경우 국가용 보안시스템을 사용하여야 한다. 다만, 행사 중인 국가원수 동정이나 행사 동향 등은 경호통신망 이외 다른 통신망을 이용하여 송·수신할 수 없다.

1. 행사 준비단계에서 준비사항
2. 유관기관 간 행사 관련 협조사항
3. 대통령 이동과 관련한 모든 사항
4. 행사 종료 후 지휘 보고사항

제41조(남북통신 보안관리) ① 행정기관의 장은 본청 및 소속기관이 남북회담 또는 남북경협사업 등을 위하여 북한지역에 정보시스템을 반출하거나 정보통신망을 구축할 경우 국정원장의 사전 보안성 검토를 거친 보안대책을 수립·시행하여야 한다.

② 남북경협사업 등에 참가한 사업자를 관할하는 행정기관의 장은 사업자가 북한 현지에서 운영하는 정보통신망이나 정보시스템이 해킹·도청(盜聽) 등에 악용되지 않도록 주기적인 정보통신 보안교육 등 보안지도 활동을 실시하여야 한다.

③ 제1항에 따라 남·북한 지역간 정보통신망을 연결할 경우에는 통신경로를 임의로 변경하거나 인가받지 않은 다른 정보통신망과 연결하여서는 아니 된다.

제42조(비상통신 보안관리) ① 전시 또는 비상사태 발생에 대비하여 비상통신망을 운용하고 있거나 중요한 정보시스템을 관리 감독하는 행정기관의 장은 평상시 이에 대한 보안대책을 강구하여야 한다.

② 비상통신망 관리기관의 장은 소관 비상통신망을 통하여 국가기밀 등 중요 정보를 보관·유통하는 경우 국가용 보안시스템을 사용하여 암호화하여야 한다.

③ 비상통신망 관리기관의 장은 소관 비상통신망의 위치·구성도·관리인원 등 세부사항이 외부에 공개되지 않도록 하여야 하며, 주기적으로 보안 취약점을 점검하여야 한다. 이를 위해 필요한 경우에는 국정원장에게 그 지원을 요청할 수 있다.

④ 비상통신망의 신·증설 또는 유지보수, 취약점 분석·평가 등을 외부 기관에 의뢰하여 수행하고자 할 경우에는 국정원장의 사전 보안성 검토를 거친 보안대책을 수립·시행하여야 한다.

제43조(외교통신 보안관리) ① 행정기관의 장은 해외공관과 비밀 등 중요자료를 소통하고자 할 때에는 외교정보통신망을 사용하는 등 국정원장이 승인한 보안대책을 시행하여야 한다.

② 행정기관의 장은 해외 순방행사 관련 사항은 외교정보통신망 또는 파우치 등을 이용하여 수발하여야 하며 일반 국제전화·인터넷망·팩스 등 보안성이 없는 정보통신망을 이용하여 수발하여서는 아니 된다.

③ 행정기관의 장은 외교정보통신망에 인터넷 및 현지 고용원 PC와 연결을 차단하여야 하며 국정원장이 승인한 보안대책 없이 인터넷에 연결된 PC를 이용하여 해외전문 등 비밀·중요자료의 작성·보관·소통을 금지하여야 한다.

④ 행정기관의 장은 해외공관 등 해외에 직원을 파견하고자 할 경우에 파견 직원에 대하여 정보통신망 및 정보시스템의 운용시 보안관리방안 등 정보통신 보안교육을 실시하여야 하며, 정보통신 보안업무에 대하여 인계인수를 철저히 하여야 한다.

제44조(국제협상 보안관리) ① 행정기관의 장은 국제 협상을 위해 노트북 PC 등 정보시스템을 현지에서 사용하고자 하는 경우 중요 협상정보가 유출되지 않도록 다음 각 호의 보안대책을 수립·시행하여야 한다.

1. 정보시스템 설치장소에 대한 물리적 접근통제 대책
2. 정보시스템 접근통제 및 분실방지 등 보안관리 대책
3. 암호화 등 정보시스템 저장정보 보안대책
4. 전화·팩스 등 통신시설에 대한 도청 방지 대책
5. 기타 협상정보 보호를 위해 필요하다고 인정되는 대책

② 행정기관의 장이 제1항의 보안대책을 수립한 경우 미리 국정원장에게 보안성 검토를 요청하여야 한다.

③ 국제협상 참가자는 대상국이 제공한 정보시스템을 이용하여 중요 협상정보를 작성하거나 저장 또는 송·수신하여서는 아니 된다. 다만 불가피한 경우에는 보안대책을 수립, 국정원장의 보안성 검토를 거쳐 시행하여야 한다.

제45조(제어정보망 보안관리) ① 행정기관의 장은 공항, 항만, 원자력, 전력, 가스, 운송설비 및 대규모 산업 플랜트 등을 중앙에서 감시 및 제어하기 위한 정보통신망(이하 "제어정보망"이라 한다)을 구축할 경우 자체 보안대책을 수립하고 국정원장과 협의를 거쳐 보안성 검토를 요청하여야 한다.

② 행정기관의 장은 제어정보망에 대한 침해사고 대응책을 마련하고 주기적으로 보안 취약점을 점검하여야 한다.

③ 행정기관의 장은 제어정보망의 취약점과 보안대책 등이 포함된 문서를 대외비 이상으로 관리하고 세부적인 취약점 분석·평가 결과를 인터넷이나 학회지 등 외부에 공개 또는 발표하여서는 아니 된다. 다만, 정보통신보안 기술 교류나 학문적 연구 등을 목적으로 하는 비공개 회의 등의 경우에는 자체 보안성검토를 거친 후 발표할 수 있다.

④ 행정기관의 장은 제어정보망을 인터넷 등 다른 정보통신망과 분리 운영하여야 하며 연동이 필요한 경우에는 국정원장과 사전 협의하여 보안대책을 마련하여야 한다.

제7절 용역사업자 등 인원보안

제46조(보호구역 근무자 보안) ① 행정기관의 장은 정보통신실 등 제20조제1항의 보호구역에 신규로 근무하는 직원 또는 직원 외의 상시 근무자에 대해 다음 각 호의 보안조치를 수행해야 한다.

1. 보안의식 교육 및 별지 제7호서식에 의한 보안서약서 징구
2.「보안업무규정」제8조에 의한 비밀취급 대상자인 경우에 비밀취급인가 신청

② 행정기관의 장은 보호구역으로부터 전출 또는 퇴직자에 대해 다음 각호의 보안조치를 수행해야 한다.

1. 전출 또는 퇴직자가 사용하던 PC에 저장되어 있는 비공개 자료 삭제
2. 전출 또는 퇴직자가 사용하던 사용자계정(ID)을 즉시 변경 또는 사용 중지

제47조(업무대행자 보안관리) ① 행정기관의 장은 정보시스템을 관리하기 위하여 일용직, 단순고용직, 청원경찰, 공익근무요원 등을 업무대행자로 지정하여서는 아니 된다. 다만, 부득이한 경우에는 "시행요강 제3조제3항"에 의거 지정된 분임보안담당관의 승인 하에 지정하되, 다음 각 호의 사항을 준수하여야 한다.

1. 정보시스템의 접속시간, 접속 및 이용 권한을 최소화
2. 유효기간이 설정된 임시 접속계정 부여
3. 인가되지 않은 정보시스템에 불법 접속하는지 여부를 주기적으로 확인 점검

② 행정기관의 장이 제1항에 의하여 특정 정보시스템에 대해 업무대행자를 지정한 경우에는 다음 각호의 사항을 확인하는 등 보안조치를 수행하여야 하며, 그 사유가 소멸할 경우에는 즉시 해지하여야 한다.

1. 접속할 사용자, 사용자계정, 비밀번호
2. 접속주소, 접속시간, 접속사유(자료입력, 통계작성 등)
3. 접속 종료 후 사용자계정 및 비밀번호 회수 등 조치사항
4. 별지 제7호서식의 보안서약서 징구 및 별지 제27호 서식의 사용자계정 관리대장 작성 비치
5. "시행요강"에 의한 신원조사 결과 또는 사본 비치

제48조(용역사업 준비단계 보안) ① 행정기관의 장은 정보화·정보보호사업 및 보안감리·보안컨설팅 수행 등을 외부 용역으로 추진할 경우에 제16조에 따른 보안조치를 실시하여야 한다.

② 행정기관의 장은 제1항 관련 용역사업을 계약할 경우 계약서에 용역사업 참가직원의 보안준수 사항과 위반할 경우에 손해배상 책임 등을 명시하여야 한다.

③ 행정기관의 장은 용역업체가 사업의 일부 또는 전부에 대하여 하도급 계약을 체결하는 경우에 용역업체로 하여금 하도급 계약서에 본 사업계약 수준의 비밀유지 조항을 포함하도록 조치해야 한다.

④ 행정기관의 장은 「보안업무규정」 제31조 내지 제34조의 규정에 따라 필요한 경우에 업무위탁 또는 용역인력을 대상으로 신원조사를 실시하여야 한다. 이 경우 신원조사 대상자에 대한 조사결과를 고지하거나 누설행위를 금지하며, 업무상 직접적인 관련이 없이 신원기록을 열람하지 않도록 하는 등 신원조사 정보의 보안이 유지되도록 하여야 한다.

제49조(용역사업 수행단계 보안) ① 행정기관의 장은 용역사업의 참여인력에 대하여 별지 제7호서식에 의한 보안서약서를 작성·제출토록 해야 한다.

② 행정기관의 장은 용역인력에 대해 비밀유지의 준수 의무 및 위반할 경우 처벌내용 등에 대한 보안교육을 실시해야 한다.

③ 행정기관의 장은 비밀관련 용역사업을 수행할 경우에 외부 참여인원에 대한 비밀취급인가 등 보안조치를 취해야 한다.

④ 행정기관의 장은 용역업체에게 자료를 제공하거나 용역수행 중 생산된 산출물에 대하여 다음 각호에 따라 관리하여야 한다.

1. 비공개자료를 용역업체에게 열람하게 하거나 제공할 경우에 별지 제25호 서식의 열람·제공자료 관리대장으로 작성하여 인계자와 인수자가 직접 서명한 후 인수·인계 실시
2. 산출물 등 사업 관련자료는 인터넷 웹하드 등의 자료공유사이트 및 개인 메일함에 저장 금지, 대외비이상의 비밀은 전자우편으로 수·발신 금지
3. 용역업체에 제공한 비공개자료는 매일 퇴근할 때 반납 조치하며, 비밀문서를 제외한 일반 문서는 시건장치가 된 보관함에 보관
4. 산출물 중 비공개 자료는 비인가자 또는 대외에 제공 또는 열람 금지

⑤ 행정기관의 장은 용역사업을 수행하는 사무실과 장비에 대하여 다음 각호에 따라 관리하여야 한다.

1. 시건장치가 구비되고 출입통제가 가능한 사무실 사용
2. 용역업체의 사무실과 인원·장비를 대상으로 정기적으로 보안점검 실시
3. 보호구역에서 용역사업자가 정보시스템이나 보조기억매체 등 정보자산을 반입 또는 반출하는 경우에 악성코드 감염 및 자료 무단반출 여부를 확인
4. 용역수행 PC에 허가받지 않은 USB 등 외부 저장매체 사용을 금지

⑥ 행정기관의 장은 용역업체가 업무를 위해 전산망을 이용하는 것이 필요하다고 판단되는 경우 전산망 접근을 허용하되 다음 각호에 따라 관리를 해야 한다.

1. 사업별 또는 사용자별로 접속계정을 부여

2. 계정별로 정보시스템의 접근권한 부여, 계정에 대한 작업이력 확인
3. 용역인력의 접속계정에 대한 비밀번호를 기록·관리
4. 서버 및 네트워크 장비에 대한 접근기록을 확인·관리
5. 용역사업에 투입된 PC가 인터넷에 연결되는 것을 원칙적으로 금지하여야 한다. 다만, 필요한 경우에는 전용단말기를 지정하거나 필요한 사이트에만 접속가능토록 통제하여야 한다.

⑦ 행정기관의 장은 용역업체 근무인력 중 대표 1인을 용역업체인력의 보안관리자로 지정하여 용역사업자 자체적인 보안관리체계를 마련한다.

제50조(용역사업 종료단계 보안) ① 행정기관의 장은 최종 용역산출물 중 대외보안이 요구되는 자료는 관련 법령 및 제18조에서 정하는 바에 따라 비밀, 대외비 또는 비공개자료로 등록하여 관리해야 한다.

② 행정기관의 장은 용역업체에 제공한 자료·장비·문서 및 중간·최종산출물 등 사업 관련 제반자료를 확인하여 전량 회수해야 하며, 노트북·보조기억매체 등에 의해 전자적으로 기록된 자료도 데이터 완전삭제 도구 등을 활용하여 복구가 불가능하도록 삭제 조치해야 한다.

③ 행정기관의 장은 제2항의 용역사업 관련자료 회수 및 삭제조치 후에 용역업체가 용역산출물의 복사본 등 용역사업 관련 자료를 보유하고 있지 않다는 용역업체 대표명의 별지 제26호서식의 보안확약서를 작성·제출토록 해야 한다.

④ 행정기관이 장은 필요한 경우 용역사업에 투입된 PC 등에 대하여 제2항 및 제3항의 용역사업 관련자료 회수 및 삭제조치에 대한 이행여부를 확인할 수 있다.

제 3 장 사이버공격 대응 및 조치

제51조(보안관제) ① 행정기관의 장은 불법침입, 해킹프로그램·웜·바이러스 유포 등의 사이버공격에 신속히 대응 및 조치하기 위하여 사이버침해를 대응하기 위한 보안관제실(이하 "보안센터"이라 한다)을 구축·운영하여야 한다.

② 제1항에 따라 구축된 보안센터는 다음 각 호의 역할을 수행한다.

1. 사이버위협 관련 정보의 탐지 및 정보공유체계의 구축·운영
2. 사이버공격 관련 경보 발령 시 대응활동
3. 사이버침해 사고 대응·복구
4. 사이버침해 대응 보안시스템 개발·운용
5. 사이버공격 기법 분석 및 공격차단 등 대응방안
6. 긴급사태에 대비한 정기적 훈련과 교육실시
7. 그 밖에 경보의 수준별 세부 대응조치 등 필요한 사항

③ 행정기관의 장은 보안센터의 업무 수행과 관련하여 필요하다고 인정하는 경우에는 행안부장관에게 지원을 요청할 수 있다.

제52조(초동조치) ① 행정기관의 장은 소관 정보시스템 및 정보통신망에 대하여 다음 각호에 해당하는 사이버공격을 인지할 경우 그 피해실태를 파악하고 관련 로그자료를 보존하여야 하며, 필요할 경우 정보시스템을 통신망과 분리하는 등 초동조치를 취하여야 한다.

1. 비인가자의 정보시스템·어플리케이션에 대한 접근 및 접근시도
2. 정보자산의 유출(H/W, S/W, DATA 등)
3. 비인가자에 의한 중요 정보의 위·변조 및 삭제에 관한 사항
4. 악성 프로그램(바이러스, 백도어 등) 유포
5. 정보시스템에 대한 서비스 거부공격(DOS 공격 등) 발생
6. 네트워크 장비, 서버 및 PC 등에 대한 해킹
7. 그 밖에 별표 제2의 정보통신 보안사고유형에 해당하는 사항

② 행정기관의 장은 단순 웜·바이러스 감염 등 경미한 사항의 경우 행정기관이 자체 처리 후에 관련사항을 행안부장관에게 보고하여야 한다.

③ 행정기관의 장은 홈페이지 변조, 정보통신망 기능장애·마비 또는 중요 정보자료 유출 등 중대사고가 발생한 경우에는 초동조치 후 즉시 행안부장관을 거쳐 국정원

장에게 보고하여야 한다. 이 경우 해당 피해시스템은 사고원인을 규명할 때까지 증거보전을 의무화하고 임의 자료삭제 또는 포맷을 하여서는 아니 된다.

제53조(경보발령) ① 행안부장관은 사이버공격에 대한 체계적인 대응 및 대비를 위하여 사이버공격의 파급영향, 피해규모 등을 고려하여 각 행정기관에 관심·주의·경계·심각 등 수준별 경보를 발령할 수 있다.

② 행안부장관은 국정원장과 협조하여 제1항의 경보 발령에 필요한 정보를 행정기관의 장에게 요청할 수 있다. 이 경우 행정기관의 장은 특별한 사유가 없는 한 이에 협조하여야 한다.

제54조(대응활동) ① 행정기관의 장은 소관분야의 사이버공격 대응절차를 수립·시행하고 그 이행실태를 지속적으로 확인·점검하여야 한다.

② 행정기관의 장은 행안부장관이 경보를 발령하였을 경우 소관분야 직원을 대상으로 관련사항을 전파하고 대응조치를 이행하여야 하며, 진행상황을 예의주시하는 등 대응절차에 따라 신속하게 대처하여야 한다. 이 경우 경보 단계별 조치결과를 행안부장관을 거쳐 국정원장에게 통보하여야 한다.

③ 행안부장관은 사이버공격에 대하여 소관분야의 정보시스템 및 정보통신망에 대한 안전성을 확인할 수 있다.

④ 행정기관의 장은 사이버안전을 위한 대응절차 기준을 정하고자 할 경우에는 국정원장이 제정한「국가사이버안전매뉴얼」을 활용할 수 있다.

⑤ 행안부장관은 국정원장과 사전 협의하여 각 행정기관의 사이버위기에 대한 체계적이고 효율적인 대응을 위해 매년 정기 또는 수시로 모의훈련을 실시할 수 있다.

제55조(사고통보 및 복구) ① 행정기관의 장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취하고 지체 없이 그 사실을 행안부장관을 거쳐 국정원장에게 통보하여야 한다.

② 행안부장관은 사이버공격으로 인한 사고의 발생 또는 징후를 발견하거나 통보를 받은 때에는 관계 행정기관의 장에게 사고복구 및 피해의 확산방지에 필요한 조치를 요청할 수 있다. 이 경우 요청받은 관계 행정기관의 장은 특별한 사유가 없는 한 이에 협조하여야 한다.

제 4 장 국가용 보안시스템

제 1 절 공 통

제56조(개발 및 제작) ① 행정기관이 보안시스템을 사용하고자 할 경우에 국정원장이 개발하거나 제작한 보안시스템을 해당기관에 공급한다. 다만, 국정원장이 필요하다고 인정할 때에는 사용기관으로 하여금 개발하게 하거나 제작하게 할 수 있다.

② 제1항에 의거 사용기관이 개발하거나 제작한 보안시스템은 국정원장에게 미리 보안성 및 신뢰성에 대한 검토·승인을 얻어야 한다.

③ 국가용 보안시스템 연구개발 절차 등은「국가 정보보안기술 연구개발 지침」(대외비)이 정하는 바에 따른다.

제57조(사용) ① 행정기관의 장이 국가용 보안시스템을 사용하고자 할 때에는 국정원장이 개발·제작하거나 제56조제2항의 규정에 의하여 검토·승인된 제품을 사용하여야 한다.

② 행정기관의 장은 국가용 보안시스템을 운용하거나 관리를 담당하는 정·부 책임자를 지정하여야 한다.

제58조(암호문 보안관리) ① 행정기관의 장은 암호문을 평문과 분리 보관하여야 한다.

② 행정기관의 장은 동일내용을 암호문과 평문으로 이중 송신하거나 암호문을 전송한 후 이를 다시 평문으로 문의하는 등 암호문과 평문을 혼용하여서는 아니 된다.

제59조(관리실태 점검) 행안부장관은 행정기관의 장과 협조하여 국가용 보안시스템 관리실태 등을 점검할 수 있다. 이 경우 점검결과 드러난 문제점을 행정기관에 통보하고 행정기관의 장은 이에 대한 보안대책을 강구하여야 한다.

제60조(복제·복사 금지) 국가용 보안시스템은 어떠한 경우에도 복제·복사할 수 없으며 다른 기관이나 개인에게 임의 대여할 수 없다.

제61조(사용 제한) ① 행정기관의 장은 국정원장이 승인하지 않은 보안시스템이나 외국에서 생산한 보안시스템을 무단으로 사용하여서는 아니 된다.

② 국가용 보안시스템은 주한 외국인 및 주한 외국기관(대사관, 외국군 등)에 제공하거나 외국으로 무단 반출하여서는 아니 된다.
③ 제1항 및 제2항의 규정에도 불구하고 부득이하다고 판단되는 경우에는 사전에 행안부장관을 거쳐 국정원장의 승인을 얻어 사용하거나 제공 또는 반출할 수 있다.

제62조(국가암호체계 보안관리) ① 암호개발 업무를 수행하는 자는 관련 사항을 비인가자에게 공개하거나 비인가자에게 노출된 장소에서 국가 암호체계 및 운용 등에 대한 토의를 하여서는 아니 된다. 다만, 국정원장의 승인 하에 비인가자로부터 별지 7호서식의 보안서약서 징구 등 보안조치를 한 경우에는 그러하지 아니하다.
② 국가 암호체계와 관련된 사항을 알고 있는 자는 이를 학술·논문지, 간행물, 전시회 및 공개된 정보통신망 등을 통해 공개하여서는 아니 된다. 다만, 국정원장의 승인을 받은 내용은 공개할 수 있다.

제 2 절 암호장비

제63조(사용승인 요청) 행정기관의 장이 암호장비를 사용하고자 할 경우에는 다음 각호에 정하는 사항을 구비하여 국정원장에게 제출하고 승인을 얻어야 한다.

1. 사용목적
2. 사용기관
3. 암호장비의 종류, 소요량 및 산출근거
4. 관련 정보시스템 제원
5. 대상 정보통신망 구성도
6. 보안대책
7. 기타 참고자료

제64조(제작) 행정기관의 장은 암호장비를 제작할 경우에는 다음 각호의 사항에 따라야 한다.

1. 암호장비는 지정된 제작업체에서 제작하여야 한다.
2. 암호장비의 외부에는 일반적인 운용상의 기능, 형식승인 번호, 기관번호 및 일련번호를 제외한 어떠한 표지도 하여서는 아니 된다.
3. 제작된 암호장비의 검사는 국정원장에게 제작을 의뢰한 기관장의 책임 하에 행하여야 한다. 다만, 암호처리부에 대한 검사는 국정원장에게 요청하여 실시하여야 한다.

제65조(설치) 행정기관의 장은 암호장비 설치장소를 선정할 경우 보안사고(분실, 도난, 피탈 등)를 방지하기 위하여 다음 각 호의 제반 보안대책을 강구하여야 하며 부득이한 경우에는 행안부장관과 협의하여 조정할 수 있다. 다만, 암호장비에 대한 별도의 운영체계가 수립된 경우에는 이를 따른다.

1. 보호구역 설정 운영
2. 이중 잠금장치가 된 보관함·보관장소 설치 운용
3. 사진 촬영금지
4. 비인가자 출입통제
5. 화재예방 대책 등

제66조(등록) 암호장비 사용기관의 장은 암호장비를 설치한 후 30일 이내에 행안부장관에게 별지 제8호서식의 암호장비 운용관리현황에 의거 통보하여야 하며, 행정안전부장관은 지체없이 이를 국가정보원장에게 등록하여야 한다.

제67조(성능개선 등) 암호장비 사용기관의 장은 암호장비의 성능개선이나 운용 편의성 제고 등이 필요하다고 판단되는 경우에는 그 사유서를 작성하여 행안부장관에게 요청하여야 한다.

제68조(운용관리) ① 암호장비를 설치 운용하고 있는 행정기관의 장은 별지 제9호서식의 국가용 보안시스템 관리기록부를 비치하고 기록·유지하여야 한다.

② 암호장비의 암호체계 및 키 운용체계와 관련된 서류 등 결과물(암호논리, 보안모듈, 키 주입기 등)은 비밀로 분류하여야 한다.

③ 암호장비의 고유명칭, 제원, 대상국소 및 수량 등 운용현황이 기록된 문서는 대외비이상으로 분류하여야 한다.

④ 암호장비 취급책임자는 설치 운용중인 암호장비의 보관상태 및 정상 작동여부 등 이상 유무를 수시로 점검하고, 그 결과를 별지 제10호서식의 국가용 보안시스템 점검기록부에 월 1회 기록 유지하여야 하며 관리책임자는 점검여부를 확인하여야 한다.

⑤ 암호모듈이 내장된 경우 오인파기 등을 방지하기 위하여 외부에 경고문구 등 표지를 부착할 수 있다.

제69조(비밀소통 기준) 암호장비의 비밀 소통기준은 기종 및 운용하고자 하는 정보통신망의 특성을 고려하여 장비 개발 완료시 기종별로 국정원장이 정한다.

제70조(운반 및 전시) ① 암호장비는 취급책임자가 직접 운반하여야 하며 이를 확인하기 위하여 별지 제11호서식의 국가용 보안시스템 증명서를 사용한다.

② 암호장비를 운반하거나 전시하고자 할 경우에는 분실·피탈 등 사고를 방지하기 위한 보안대책을 강구하여야 한다.

③ 암호장비 운반이나 전시(展示)도중 보안조치가 필요할 경우에는 가까운 경찰서나 군부대에 암호장비의 보호를 요청할 수 있다. 이 경우 요청받은 기관은 필요한 조치를 지원하여야 한다.

④ 암호장비의 운반이나 전시 중에 사고가 발생한 경우에는 즉시 행안부장관을 거쳐 국정원장에게 통보하여 필요한 후속조치를 행할 수 있도록 하여야 한다.

제71조(정비) ① 암호장비 사용기관에서의 정비는 암호처리부를 제외한 일반부분으로 제한하며, 암호처리부의 정비는 국정원장의 승인 하에 암호장비 제작업체에서 행하여야 한다. 다만, 암호처리부가 완전 밀폐된 별개의 구성품으로 되어 있을 경우에는 사용기관에서 예비용으로 교체할 수 있다.

② 암호장비 정비장소는 보호구역으로 설정하여야 하며, 정비절차는 암호장비 사용기관의 장이 정한다.

③ 암호장비 사용기관의 정비요원은 암호취급인가를 받아야 한다.

제72조(파기) ① 암호장비 사용기관의 장이 암호장비를 파기하고자 할 때에는 다음 각호의 사항을 행안부장관을 거쳐 국정원장에게 제출하고 승인을 얻어야 하며, 긴급파기계획은 평시에 수립하여야 한다.

1. 파기사유
2. 장비명칭, 수량 및 등록번호
3. 파기일시 및 장소
4. 파기방법
5. 파기자

② 암호장비 사용기관의 장은 긴급사태 발생 등으로 암호장비를 안전하게 보호할 수 없을 때에는 긴급 파기할 수 있으며, 파기 후 제1항 각 호의 사항을 행안부장관을 거쳐 국정원장에게 지체 없이 통보하여야 한다.

제73조(현황통보) 암호장비 사용기관의 장은 별지 제8호서식의 암호장비 운용관리 현황을 작성하여 매년 1월 25일까지 행안부장관에게 제출하여야 한다.

제74조(인계인수) ① 행정기관의 장은 암호장비 운용관리 정·부 책임자가 교체될 경우에 인계인수를 실시하여야 하며 별지 제9호서식의 국가용 보안시스템 관리기록부의 최종 기록 여백에 인계인수 사항을 기록 유지하여야 한다.

② 인계인수를 할 경우에는 다음 각 호의 사항을 확인하여야 한다.

1. 암호장비의 종류와 수량
2. 납봉 또는 봉인표지의 이상유무
3. 암호장비의 정상 작동여부
4. 암호논리·키 수록매체(메모리카드 포함) 및 운용법 등 관련자료 이상 유무

제75조(외국산 암호장비 사용) ① 외국군 또는 외국기관과의 합동통신망에 설치 운용되는 외국산 암호장비는 당해 국가와의 협정에 의거 행정기관 장의 책임 하에 운용관리하여야 한다.

② 제1항에 의한 암호장비를 설치 운용하고자 할 경우에는 사전에 보안대책을 강구하여야 하며 운용추진 경위 및 그 현황을 행안부장관에게 통보하여야 한다.

제 3 절 보안자재(암호·음어·약호자재)

제76조(제작) 행정기관의 장은 암호자재를 제작할 경우 다음 각호의 사항에 따른다.

1. 국정원장은 암호자재를 제작하여 필요한 기관에 배부한다. 다만, 필요한 경우 사용기관에 암호자재의 제작을 위임할 수 있다.
2. 음어 및 약호자재 제작을 위임받은 행정기관의 장은 암호처리부에 대하여 국정원장의 인가를 받아야 한다.

제77조(사용 신청) ① 암호 및 음어자재를 사용하고자 하는 행정기관의 장은 다음 해의 연간 소요량(소속기관용 포함)을 파악하여, 매년 1월 25일까지 별지 제12호서식의 암호·음어·약호자재 신청서에 따라 행안부장관에게 신청하여야 한다. 다만, USB형 음어자재의 경우는 제84조제1항에 의한 정보유통시스템을 통해 신청할 수 있다.

② 직제개편 및 특별한 요인발생 등으로 암호 및 음어자재가 추가 소요되는 행정기관의 장은 다음 각호의 사항을 반영하여 행안부장관에게 신청하여야 한다.

1. 사용대상 및 용도
2. 자재명 및 수량

3. 자재형태 및 사용주기
4. 정보통신망도
5. 암호실 설치여부

제78조(등록 및 관리) ① 행정기관의 장은 자체 제작한 암호·음어 및 약호자재(이하 "보안자재"라 한다.)를 행안부장관에게 등록하여야 한다.

② 보안자재를 보유하고 있는 행정기관의 장은 별지 제9호서식의 국가용 보안시스템 관리기록부를 비치하고 용도별로 구분하여 기록 관리하여야 한다. 다만, 비밀관리기록부에는 등재하지 아니한다.

③ 보안자재는 사용완료(이하 "반납용"이라 한다)·현용·미래용으로 구분하여 보관하되, 현용을 제외하고는 이를 포장한 후 봉인하여 보관함에 보관하여야 한다.

④ 암호자재는 암호실내 금고에 보관하고 음어·약호자재는 평시 사용이 가능하도록 별도 관리하되 일과 후에는 이중 캐비닛 또는 금고에 보관하여야 한다.

⑤ 보안자재 보관함에는 보안자재 이외의 비밀 또는 문건을 혼합 보관하여서는 아니 된다.

⑥ 암호취급자 및 음어취급자는 보안자재의 수시점검을 실시하고 별지 제10호서식의 국가용 보안시스템 점검기록부에 월1회 기록 유지하여야 하며, 정보통신보안담당관은 점검사항을 확인하여야 한다.

제79조(취급 및 운용) ① 행정기관의 장은 보안자재 취급 필요성이 있는 자에 대하여 암호자재 및 음어자재 취급을 인가하여야 한다.

② 암호취급인가를 대한민국 국적소유자로서 Ⅱ급비밀이상 취급인가를 받은 자에 한하여 행정기관의 장에 의해 별도로 임명절차를 거쳐야 하며, 관련업무(등록·배부·반납 등)를 수행하는 자는 국정원장에게 별지 제13호서식의 인감등록서에 의한 인감등록을 하여야 한다.

③ 음어취급인가는 대한민국 국적소유자로서 Ⅲ급비밀이상 취급인가를 받은 자에 한하여 행정기관의 장에 의해 별도로 임명절차를 거쳐야 하며, 관련업무(등록·배부·반납 등)를 수행하는 자는 국정원장에게 별지 제13호서식의 인감등록서에 의한 인감등록을 하거나 또는 제84조제1항의 규정에 따라야 한다.

④ 보안자재의 변경·운용지시는 제작기관의 장이 대외비로 하달한다.

⑤ 비밀을 정보통신 수단으로 수발할 경우나 비밀이 아니더라도 국가이익을 해할 우려가 있는 내용이 있는 경우에는 보안자재 사용을 원칙으로 한다.

⑥ 같은 내용의 전문을 암호문과 평문으로 이중 송신하거나 평문으로 문의하거나 암호문과 평문을 혼용하여서는 아니 된다.
⑦ 비밀이 아닌 일반문서 내용을 암호자재로 소통한 경우에는 전문우측 상단에 암호송신, 암호수신을 표시하여 관리하여야 한다.
⑧ 지편식 암호자재를 사용할 경우 사용현황을 별지 제14호서식의 지편자재 사용기록부에 기록하여 이중 또는 미사용이 발생하지 않도록 하여야 한다.

제80조(암호자재 취급기관) ①암호자재를 취급하는 기관은 등록 암호자재 취급기관(이하 "등록기관"이라 한다)과 위임암호자재 취급기관(이하 "위임기관"이라 한다)으로 구분한다.
② 국정원장이 지정한 등록기관과 행안부장관이 지정한 위임기관은 다음 각호와 같다.
1. 등록기관 : 행정안전부 정보화전략실
2. 위임기관 : 시・도・특별자치도

제81조(취급기관의 임무) 암호자재 취급기관과 위임기관의 임무는 다음 각호와 같다.
1. 등록기관의 임무
가. 암호자재의 운영관리 및 지도감독
나. 암호취급 인가자에 대한 암호교육 훈련
다. 위임기관에 대한 자재 및 암호취급소의 지도조정 및 검열
라. 암호자재 보안에 관한 업무의 발전책 연구
마. 암호자재 수령・배포 반납에 관한 사항
2. 위임기관의 임무
가. 암호자재의 운영관리
나. 암호취급인가자의 숙달훈련
다. 암호실의 관리

제82조(배부・회수 및 반납) ① 행안부장관은 보안자재를 정기적으로 행정기관에 배부하되 제79조제2항 또는 제3항에 의해 취급자로 등록되어 신분확인이 가능한 자에 한하여 직접 배부하거나 회수한다. 다만, 음어자재 및 약호자재의 경우 직접 배부 또는 회수가 불가능할 때에는 비밀취급인가를 받은 사람 중 정책임자의 위임장을 소지한 자에게 수발을 대행토록 할 수 있다.
② 모든 암호자재는 암호취급자에 한하여 직접 배부 또는 회수하여야 한다. 다만, 부득이한 경우는 국정원장이 지정하는 계통에 의하여 배부 또는 회수한다.

③ 행정기관이 소관분야에 대해 보안자재를 배부 또는 회수하는 경우에도 인감등록이 되어 있는 자 또는 행정기관이 규정한 체계에 의해 신분확인이 가능한 자에 한하여 직접 배부 또는 회수하여야 한다.
④ 보안자재를 배부 또는 회수할 경우에는 자재의 명칭과 등록번호 등이 별지 제11호서식의 국가용 보안시스템 증명서의 기재내용과 일치하는지 확인하여야 하며 제70조제2항 내지 제4항을 준용하여 보안조치를 하여야 한다.
⑤ 사용기간이 만료된 보안자재는 배부기관의 장에게 반납하여야 한다.

제83조(소통기준) ① 암호자재는 Ⅱ급비밀 이하의 내용을 소통하는데 사용할 수 있다.
② 음어자재는 Ⅲ급비밀 이하의 내용을 소통하는데 사용할 수 있다.
③ 약호자재는 대외비 이하의 내용을 소통하는데 사용할 수 있다.
④ 보안자재는 비밀이 아니더라도 국가이익을 해할 우려가 있는 내용을 정보통신수단으로 송수신할 경우에 사용할 수 있다.

제84조(USB형 음어자재) ① 음어취급자가 USB형 음어자재를 사용할 경우에는 음어취급자 등록 및 수신기관 검색 등을 할 수 있는 정보유통시스템을 통해 등록하고 인가코드와 인증서를 발급받아야 한다.
② 음어취급자를 교체할 경우에는 USB형 음어자재에 등록된 음어취급자가 정보유통시스템을 통해 신규 음어취급자를 등록하여야 한다.
③ 음어취급자 등록과정에서 발행하는 참조번호와 인가코드(인감도장 대신 사용하는 20자리 숫자)를 행안부장관에게 통보하여야 한다.
④ 음어취급인가를 받지 않은 자가 USB형 음어자재를 사용하여 중요자료를 암·복호화 하고자 하는 경우에는 음어취급자를 통해 일반사용자로 등록하여야 한다. 이 경우 USB형 음어자재 1매당 5명까지 등록할 수 있다.
⑤ 제89조의 규정에 의한 인계인수를 수행할 때 USB형 음어자재의 경우에 아래사항을 추가적으로 인계하여야 한다.
1. USB형 음어자재(설치CD, 매뉴얼, 지문마우스, 연결케이블, 자재상자 등 포함)
2. 제1항 및 제2항에 따른 신규 음어취급자 등록사항
⑥ 음어취급자는 USB형 음어자재를 분실한 경우 다음 각 호의 사항을 지체없이 행안부장관에게 통보하여야 하며, 해당기관의 장은 분실된 자재의 인증서 폐기목록과 신규 인증서를 정보유통시스템을 통하여 신속하게 배포하여야 한다.

1. USB형 음어자재 명칭 및 일련번호
2. 분실 일시 및 장소

⑦ 음어취급자는 USB형 음어자재가 다음 각호에 해당하는 경우, 행안부장관으로부터 자재를 재발급 받아야 한다.

1. 비밀번호를 분실한 경우
2. 사용자 지문등록을 완료했으나 지문 인증에 오류가 발생한 경우
3. 자재에 심각한 오류가 발생한 경우 등

제85조(암호실 설치 및 폐쇄) ①행정기관의 장은 암호자재를 활용하여 암호작업을 할 경우에는 다음 각호의 구비요건을 갖춘 암호실을 설치 운용하여야 한다.

1. 통신실과 인접하고 비인가자 출입통제가 용이한 곳에 설치
2. 출입문 이중 잠금장치(자동잠금)와 창문에 철제 보호망 및 외부 투시 차단 장치 설치
3. 출입문외 천장 등을 통한 외부통로 차단
4. 암호자재의 보관용기는 화재, 도난 및 파괴로부터 보호되고 비인가자의 접근을 방지할 수 있는 이중 잠금장치가 되는 용기 구비
5. CCTV, 지문인식기 등 과학보안장비 운용 등 경계대책, 안전지출 및 파기계획 수립

② 암호실의 폐쇄는 행정기관의 장의 책임 하에 시행하고 암호실을 폐쇄할 경우에는 암호자재를 지체 없이 배부기관의 장에게 반납하여야 한다.

③ 암호실을 설치하거나 폐쇄한 경우에는 행안부장관에게 그 내용을 통보하여야 한다.

제86조(암호실 출입통제) ① 암호실에는 행정기관의 장, 암호취급자 및 국정원장이 인가한 자 이외에는 출입할 수 없다.

② 암호실은 별지 제5호서식의 암호실 및 암호취급자 현황 및 별지 제6호서식의 암호실 출입자 기록부에 의거 암호실 출입을 통제하고 그 내용을 기록 유지하여야 한다.

제87조(암호실의 표지와 경비) ① 암호실에는 “출입제한” 표지 이외의 암호취급을 나타내는 어떠한 표지도 하여서는 아니 된다.

② 암호실은 무장경비원에 의하여 경비되어야 한다. 다만, 군(軍) 이외의 기관으로서 무장 경비원을 둘 수 없는 경우에는 이에 상당하는 특별 경비조치를 취하여야 한다.

제88조(암호실 점검) ① 국정원장이 임명한 암호실 검열관은 모든 암호취급기관에 대한 검열을 할 수 있다.

② 암호실 검열관은 암호취급인가를 받은 자에 한하여 임명될 수 있다. 단, 점검관으로 임명된 자는 그 임무를 제3자에게 위임하거나 대행하게 할 수 없다.

제89조(인계인수) ① 보안자재를 취급하는 정·부·실무 책임자가 교체되는 경우에는 이전책임자가 신임책임자에게 보안자재 및 관련서류 등을 직접 인계하고 운용관리 방법 등을 교육하여야 한다.

② 보안자재를 취급하는 정·부·실무 책임자가 파견 등의 사유로 1개월이상 그 직무를 수행할 수 없는 경우에도 제1항을 준수하여야 한다.

③ 보안자재를 인계인수할 때에는 별지 제9호서식의 국가용 보안시스템 관리기록부의 최종기록 여백에 인계인수사항(명칭·수량·등록번호 등)을 기록 확인하여야 한다.

제90조(파기) ① 보안자재의 파기는 일반파기와 긴급파기로 구분한다.

② 일반파기는 반납용 보안자재를 파기하는 것으로서 회수한 자재는 제작기관의 장이 지정하는 자가 파기한다.

③ 긴급파기는 긴급사태 발생으로 보안자재의 보안관리가 곤란한 경우에 파기하는 것으로 당해 사용기관의 장의 책임 하에 다음 각호의 순서에 따라 파기한다.

1. 긴급한 사태가 발생하였을 때에는 상황 악화정도에 따라 반납용·미래용·현용 순으로 파기한다.
2. 현용 보안자재를 계속 보유할 수 없을 때에는 공통용·단독용 순으로 파기한다.
3. 암호문과 평문, 관련서류는 보안자재의 파기에 앞서 파기하거나 이와 병행하여 파기한다.

④ 제2항 또는 제3항에 따라 보안자재를 파기한 경우에는 다음 각 호의 사항을 지체 없이 행안부장관을 거쳐 국정원장에게 통보하여야 한다.

1. 파기일시 및 장소
2. 보안자재 수량 및 등록번호
3. 파기이유 및 방법
4. 파기자 및 참여자의 직책, 성명
5. 긴급 파기계획은 평시 수립해야 한다.

제91조(현황통보) 행정기관의 장은 보안자재의 운용결과 및 보유실태 등을 별지 제5호(암호실 및 암호취급자 현황)·제14호(지편자재 사용기록부)·제15호(암호 개발요원 현황)·제16호(보안자재 보유현황)서식에 의거 종합 작성하여 다음 해 1월 25일까지 행안부장관에게 대외비로 통보하여야 한다.

제 4 절 암호논리

제92조(개발) ① 행정기관의 장은 암호논리를 개발할 경우 다음 각호의 기준에 따라 개발한다.

1. 행정기관이 사용하는 암호논리는 국정원장이 개발하여 보급한다. 다만, 필요한 경우 자체적으로 암호논리를 개발하여 사용할 수 있으며, 이 경우 행안부장관을 거쳐 국정원장의 안전성 평가·승인을 얻어야 한다.
2. 암호논리를 개발하는 행정기관의 장은 제17조 및 제20조 및 제56조에 따라 개발실 보안대책을 강구 시행하여야 한다.

② 암호논리를 개발하는 행정기관의 장이 국정원장에게 안전성 평가·승인을 요청하고자 할 경우에는 다음 각 호의 사항을 첨부하여 행안부장관에게 신청하여야 한다.

1. 개발 배경 및 적용대상 시스템
2. 암호체계
3. 암호논리 소스코드 및 관련 설명서
4. 안전성 평가 등 관련자료

제93조(요청) ① 행정기관의 장은 정보통신망을 통해 보관·유통되는 전자정보 등을 보호하기 위해 행안부장관에게 국가기관용 암호논리 지원을 요청할 수 있다.

② 암호논리를 요청할 경우에는 다음 각호의 자료를 첨부하여야 한다.

1. 사용 목적
2. 정보시스템 구성도, 기능 및 제원
3. 암호키 운용관리 방식
4. 보안서비스 요구사항

제94조(설치 및 운용) ① 행정기관의 장은 암호논리를 설치하거나 운용할 경우 보안관리를 위한 암호취급자를 지정하여야 한다.

② 암호취급자는 정보시스템 등에 암호논리를 적용하는 전 과정을 감독하고 용역업체 등에 대해서는 보안서약서 징구 등 보안대책을 강구하여야 한다.

③ 암호취급자는 암호논리가 정보시스템에서 정상 동작하는지 여부를 확인하기 위해 관계기관과 합동으로 운영적합성 시험을 실시하여야 한다.

제95조(보안관리) 승인된 암호논리의 세부구조를 알 수 있는 설계도, 소스코드 등은 비밀로 분류하고 암호논리를 개발하고자 하는 자는 제79조의 규정에 의거 암호취급인가를 받아야 한다.

제96조(반납 및 파기) 실용성이 상실되거나 유효기간이 만료된 암호논리는 행안부장관에게 반납하여야 하며, 행안부장관의 책임 하에 파기(소자)하고 국정원장에게 그 결과를 통보하여야 한다.

제97조(현황통보) 행정기관의 장은 별지 제17호서식에 의거 암호논리 운용현황을 작성하여 매년 1월 25일까지 행안부장관에게 통보하여야 한다.

제 5 절 정보보호시스템의 도입·운용

제98조(도입) 행정기관의 장은 소관 정보를 보호하기 위하여 정보보호제품을 도입하고자 할 경우 아래와 같은 정보보호제품을 도입하여야 한다.

1. 정보보호시스템 평가·인증 지침 및 공통평가기준에 의해 인증받은 제품이나 국정원장이 그와 동등한 효력이 있다고 인정한 제품
2. 행정기관의 장이 자체 개발하거나 외부업체 등에 의뢰하여 개발한 제품

제99조(제품선정) ① 정보보호제품을 도입할 경우에는 사전에 별지 제18호서식의 정보보호제품 자체 점검결과를 참조하여 보안기능 구현여부 및 업체 기술지원 가능여부 등을 점검하여야 한다.

② 정보보호제품의 안정적인 운용을 위해 도입시점부터 최소 1년이상 유지보수가 가능한 업체의 제품을 선정하여야 한다.

제100조(보안적합성 검증) 행정기관의 장은 제98조에 규정된 정보보호 제품을 운용하고자 하는 경우에 국정원장에게 안전성 확보를 위한 보안적합성 검증을 신청하여야 한다.

제101조(제출문서) 보안적합성 검증 신청에 필요한 제출문서는 다음과 같으며, 제출문서는 한글로 작성하여야 한다.

1. 국제공통평가기준(CC) 인증제품
   가. 별지 제18호서식의 정보보호제품 자체 점검결과 1부
   나. 별지 제19호서식의 보안적합성 검증 신청서 1부
   다. 기술제안요청서 사본 1부
2. 자체 개발하거나 외부업체 등에 의뢰하여 개발한 제품
   가. 별지 제18호서식의 정보보호제품 자체 점검결과 1부
   나. 별지 제19호서식의 보안적합성 검증 신청서 1부
   다. 기술제안요청서 사본 1부
   라. 상세설계서 1부
   마. 개발완료 보고서 1부
   바. 제품사용설명서 1부

제102조(제품의 취약점 보완) ① 행정기관의 장은 보안적합성 검증결과를 반영하여 도출된 취약점을 제거한 후 제품을 운용하여야 한다.

② 행정기관의 장은 도입제품의 보안기능 및 보증등급 등이 전자정보 보안대책으로 적절치 않다고 검증된 경우 유사기능의 타 제품으로 대체하거나 지적된 사항을 보완하는 등의 조치를 하여야 한다.

제103조(제품의 활용범위) 보안적합성 검증이 완료된 제품은 비밀 및 대외비를 제외한 모든 전자정보를 보호하는데 사용할 수 있다.

제104조(목적이외 사용제한) 행정기관의 장은 보안적합성 검증이 완료된 정보보호시스템에 대해 보안기능을 임의로 변경하거나 도입 목적이외의 용도로 운용하여서는 아니 된다.

제 5 장 보 칙

제105조(준용) 이 지침에 명시되지 않은 사항은 다음 각호의 관련규정·지침에 따른다.

1. 「보안업무규정」
2. 「보안업무규정시행규칙」
3. 「보안업무규정시행요강」
4. 「국가사이버안전관리규정」
5. 「행정기관 정보시스템 접근권한 관리 규정」
6. 「국가정보보안기본지침」
7. 「행정전자서명 인증업무지침」
8. 「국가 정보보안기술 연구개발지침」
9. 「연도 보안업무 수행지침」
10. 「USB메모리 등 보조기억매체 보안관리지침」
11. 「국가 사이버안전관리 매뉴얼」
12. 「전자정부 보안관리 실무매뉴얼」
13. 「RFID 보안관리지침」
14. 「USB형 음어자재 운용관리지침」
15. 「전자정부 암호이용기반시스템 운용 및 관리지침」
16. 「정보보호시스템 평가·인증 지침」
17. 기타 정보통신보안 관계 법령 및 지침·가이드·매뉴얼

부 칙 <제147호, 2009. 6. 9>

제1조(시행일) 이 규정은 2009년 6월 9일부터 시행한다.

제2조(존속기한 설정) 이 규정의 존속기간은 시행일로부터 3년 이내(2012년 4월 30일)로 한다. 다만, 존속기한 만료일 이전에 필요성을 재검토하여 기한을 연장할 수 있다.

별 표

<별표 1>

정보통신보안 위규사항

조	내 용	항	세 부 내 용
1	불온통신에 관한 사항	(1)	북한 통신소와의 불법교신
		(2)	국내침투 간첩과의 교신
		(3)	적성국(또는 반국가단체) 통신소와의 불법교신
		(4)	기타 반국가적인 불법통신
2	군사상 기밀의 누설	(1)	군사전략, 작전계획 및 진행사항
		(2)	군 편제·임무·시설 및 기타 부대현황
		(3)	병력(군·경·예비군) 현황 및 이동 상황
		(4)	경찰 및 특수기관의 장비(작전·정보·수사용) 현황과 집행사항
		(5)	특수기관·군사시설의 위치 및 이동상황
		(6)	군사장비의 구성·성능 및 발명개량 연구사항
		(7)	군사장비(군수품 등) 생산 및 공급사항
		(8)	기타 국가방위에 영향을 초래하는 사항
3	외교상 기밀의 누설	(1)	국가 외교방침, 기본계획 및 재외공관에 발하는 훈련
		(2)	공개할 수 없는 외교조약 또는 협약
		(3)	특수임무를 수행하는 해외주재원의 활동(계획·지시·보고) 및 신원정보에 관한 사항
		(4)	기타 국가외교에 영향을 초래하는 사항
4	국가정보활동에 관한 사항 누설	(1)	대공업무와 관련된 사항
		(2)	정보(첩보) 수집활동에 관한 사항
		(3)	간첩 또는 대공용의자 발견과 수사 활동
		(4)	정보 및 특수수사기관의 기구 또는 임무기능에 관한 사항

조	내 용	항	세 부 내 용
4	국가정보활동에 관한 사항 누설	(5)	국가원수 및 기타 용인의 비공개행사
		(6)	불명선박의 발견 및 처리
		(7)	중요물자 수송활동
		(8)	테러·마약·밀수 및 국제범죄 조직에 관한 정보·수사 활동
		(9)	적 또는 경쟁국에 유리한 과학기술 및 산업에 관한 정보
		(10)	기타 국가안보 및 공안유지에 불리한 영향을 초래하는 사항
5	보안시스템에 관한 사항 누설	(1)	국가용 보안시스템의 연구개발 및 제작에 관한 사항
		(2)	암호전문을 허위로 조립하여 송신
		(3)	암호를 부정한 목적에 사용하였을 때
		(4)	암호문과 평문의 혼용 및 이중사용
		(5)	암호문 작성 시 동일 난수를 2회이상 반복사용
		(6)	사용기간이 경과된 암호자재를 계속 사용
		(7)	암호문에 평문을 삽입하여 송신
		(8)	기타 국가용 보안시스템 보호체계를 손상시킬 우려가 있는 사항
6	허가목적외의 방법으로 사용하는 경우	(1)	허가목적 업무와 관련이 없는 통신
		(2)	군 통신망에서 군사업무와 관련이 없는 통신
		(3)	기타 사회질서를 해하는 통신

<별표 2>

정보통신 보안사고 유형

조	내 용	항	세 부 내 용
1	정보시스템 및 정보통신실	(1)	정보통신망에 대한 해킹·악성코드의 유포
		(2)	비밀이 저장된 PC, 보조기억매체 등 분실
		(3)	정보시스템 및 정보통신실 파괴
		(4)	중요 정보시스템 기능 장애 및 정지
2	암호장비	(1)	암호장비 분실 및 빼앗김
		(2)	암호장비 파손 및 임의파기
		(3)	암호장비 복제·복사
		(4)	비인가 암호장비 사용
		(5)	암호장비 비닉체계 특성 및 제원 노출
		(6)	암호장비 키 운용체계 노출
3	보안자재	(1)	암호·음어·약호자재의 분실 및 누설
		(2)	암호·음어·약호자재의 파손 및 임의파기
		(3)	암호·음어·약호자재의 임의제작 사용
		(4)	세부 암호체계 노출
4	전자정보	(1)	주전산기(주요서버 등)·대용량 전자기록(DB) 손괴
		(2)	전자문서·전자기록물의 위조·변조·훼손 및 유출
		(3)	비밀의 평문 보관 및 유통

<별표3>

정보통신보안 점검항목

3.1 정보통신망 운영준비

구분		점검항목	비고
체계정비	정책수립	정보통신보안과 관련된 자체 내규가 마련되어 있는가?	
		정보통신보안 내규에 팀(과)간 보안업무 수행에 관련된 업무절차, 체계 및 역할이 마련되어 있는가?	
		정보통신보안 내규는 기관의 장이 승인하였는가?	
		정보통신보안 내규의 제·개정 시 국정원장과 협의 하였는가?	
		정보통신보안 내규의 배포 절차 및 방법이 수립되어 있으며 소속 직원에게 배포되었는가?	
		정보통신보안 내규는 연1회 이상 정기적으로 재검토하여 갱신되고 있는가?	
		사이버·보안 진단의 날을 지정하여 운영하고 있는가?	
	조직구성 및 역할분담	정보통신보안담당관 등 정보통신보안 책임자가 지정되어 있는가?	
		정보통신보안책임자는 역할 할당 원칙을 준수하여 업무를 분장하고 있는가?	
		보안심사위원회는 구성되어 있으며 임무를 충실히 수행하고 있는가?	
		정보통신보안 조직체계에 따른 위규 조치 절차가 정의 되어 있는가?	
	교육체계 정비	정기 정보통신보안 교육계획을 수립·시행하고 있는가?	
		신입 직원에 대한 수시 정보통신보안 교육을 실시하고 있는가?	
		정보통신보안 교육 자료가 마련되어 있는가?	
		정보통신보안 책임자의 역량강화를 위한 전문교육을 실시하고 있는가?	
		신규 보안취약점 조치 안내, 보안 홍보메일 발송, 비디오 상영 등 직원 대상 정보통신보안 관련 홍보활동을 수행하고 있는가?	
		직원의 정보통신보안 교육 수강을 점검하고 제재할 수 있는 절차가 마련되어 있는가?	
		직원들은 정보통신보안 규정을 숙지하고 있는가?	
	사고대응 절차정비	정보통신망 장애에 대비한 보고 및 대응절차를 마련하고 직원들에게 주지시켰는가?	
		정보통신망 장애에 대비한 비상연락망이 구축되어 있는가?	
		정보통신망 장애 발생시 보고 및 응급조치 절차가 마련되어 있는가?	
		정보통신망 장애가 발생했을 경우 조사 실시 및 재발방지책을 강구하였는가?	

구분		점검항목	비고
	자체 점검 및 감사	보안대책에 대한 자체 점검 계획을 수립하고 정기적으로 실시하고 있는가?	
		자체 점검 결과에 따라 조직의 정보통신보안 규정 등 보안대책을 개선하였는가?	
		연1회 이상 자체 정보통신보안 감사를 실시하고 있는가?	
		감사결과에 따라 개선대책을 수립·시행하였는가?	
인적보안	사용자 심사 및 보안조치	직위별, 임무별에 따라 정보통신망 접근 인가를 심사하고 있는가?	
		비밀 등 중요정보를 취급하는 직원들에 대해서는 비밀취급인가, 보안서약서 징구 등 보안대책을 수행하는가?	
		정보통신보안담당관은 주기적으로 보조기억매체 보관 등에 대한 보안점검을 수행하는가?	
	인사이동·퇴직시 보안조치	보직변경, 퇴직 등 인사 이동시 정보시스템 접근권한을 신속하게 조정하는가?	
		보직변경, 퇴직 등 인사이동시 정보자산 및 업무자료 불법 반출 방지를 위한 방법을 강구하였는가?	
	외부인력 보안조치	신원확인 및 보안서약서 징구를 수행하고 있는가?	
		내부 정보시스템 접근권한을 제한하고 있는가?	
		외부인력의 보안 위해물품 소지여부를 점검하고 있는가?	
		외부인력 전산실 등 출입시 담당자 입회 등 보안통제를 실시하고 있는가?	
시설보안	보호대책	내부자와 외부인력에 대한 출입시 및 정보자산의 반출입시 통제대책을 실시하고 있는가?	
		출입자에 대한 출입 내역을 기록, 유지하고 있는가?	
		통신회선 도청 및 손상방지 대책을 적용하고 있는가?	
		국가안보 및 국가안위와 관련된 중요 시설에 대해서는 전자파 누설로 인한 정보유출 및 도청 방지대책을 적용하고 있는가?	
		시설내 정보시스템의 화면 출력에 대한 보호조치를 실시하고 있는가?	
		무정전전원공급장치 설치 등 비상시 전력장애에 대한 대책을 강구하고 있는가?	
		화재를 탐지하고 억제할 수 있는 대책을 강구하고 있는가?	
		항온, 항습을 유지하여 시스템 장애를 예방하고 있는가?	
		수해시 시설 및 정보시스템 보호대책을 강구하고 있는가?	
		물품 반출, 반입에 대한 통제절차를 마련하여 적용하고 있는가?	
		시설 및 정보시스템 구성에 대한 설계 도면 등을 최신으로 유지 관리하고 있는가?	
인적보안	보호구역 지정	보호구역 설정 대상을 보호구역으로 설정하여 보호하고 있는가?	
		보호구역에 대해서는 강화된 보안통제를 실시하고 있는가?	
		보호구역의 보호수준을 제한지역, 제한구역, 통제구역으로 분류하여 보안대책을 수행하고 있는가?	
		보호구역에 대한 접근권한을 업무목적에 따라 차등 적용하고 있는가?	
		보호구역에 대한 접근권한을 정기적으로 검토 및 갱신하고 있는가?	

3.2 정보시스템 도입

구분		점검항목	비고
정보시스템 도입	자체 개발시 보안대책	자체 개발시 계획단계부터 정보통신보안 부서와 보안대책에 대해 협의하는가?	
		자체 개발시 국가정보원에 보안성 검토를 의뢰하는가?	
		독립 개발시설을 확보하고 비인가자 접근통제를 실시하는가?	
		개발시스템과 운영시스템을 물리적으로 분리하고 있는가?	
		보안계획 수립, 검토, 이행 및 점검 등 자체 보안대책을 강구하고 있는가?	
		개발 전 과정 및 배포와 관련한 현황을 문서화하여 관리하는가?	
		개발 프로그램의 변경이력을 관리하는가?	
		프로그램 소스에 대한 보안대책을 강구하는가?	
	외부 용역 개발시 보안대책	외주 개발에 대한 보안관리 규정이 있는가?	
		외주에 의한 개발, 운영, 유지보수 계약시 참여인원에 대한 신원확인 및 보안서약서를 받는가?	
		보안준수 사항 및 배상책임을 계약서에 명시하는가?	
		업무 수행기간 중 업체의 외주 참여인원 임의교체 금지를 규정하고 있는가?	
		제공자료에 대한 보안대책을 강구하고 있는가?	
		용역사업 종료 시 산출물 등의 회수 및 삭제조치를 하고 있는가?	
		장비 반입·반출 및 자료 무단반출 여부를 확인하는가?	
	자체 시험·평가	정보시스템 개발 및 도입시 기관에서 필요한 정보통신보안 요구사항을 충족하는지 확인하는가?	
		소프트웨어 개발 및 도입시 악의적 코드와 백도어 등의 은닉여부 탐지를 위해 점검도구의 활용, 소스코드 분석 등의 방법을 사용하여 시험·평가를 수행하는가?	
		업무용 소프트웨어 기능시험시 장애 및 사고발생에 대비한 보안대책을 강구하는가?	
	정보보호 시스템 도입	정보보호시스템 또는 정보보호 기능이 탑재된 정보시스템을 사용하고자 할 경우 보안적합성 검증을 받았는가?	
	암호모듈 도입	암호모듈을 사용할 경우 국정원장이 안전성을 확인한 모듈을 도입하고 있는가?	
정보시스템환경설정	서비스 관리 및 기능별 분리·운영	정보시스템이 비인가자에게 불필요한 서비스를 허용하지 않도록 보안기능을 설정하고 있는가?	
		정보시스템을 기능별로 분리·운영하여 업무에 필요한 최소한의 기능함 제공하도록 하고 있는가?	
	프로그램 설치 제한	P2P·웹하드 등 파일공유 프로그램, 메신저 프로그램 등 정보를 유출시키거나 취약점을 제공할 수 있는 프로그램의 설치를 제한하고 있는가?	

3.3 정보통신망 보안관리

구분		점검항목	비고
사용자 계정 관리	사용자 계정 부여 및 적용	사용자 계정 부여 원칙을 준수하고 있는가?	
		사용자 및 관리자 계정은 주기적으로 점검하여 접근권한을 재검토하는가?	
		사용자가 3회에 걸쳐 로그인을 실패할 경우 정보시스템을 중단시키고 비인가자 침입여부를 확인하는가?	
		정보시스템에 대한 동시 접속수를 제한하고 일정기간 동안 작업을 수행하지 않을 경우 접속을 종료하는가?	
		시스템운영자는 사용자 계정의 등록, 변경, 폐기시 시스템관리책임자의 승인 하에 수행하고 그 결과를 정보통신보안담당관에게 보고하는가?	
	운영체제별 계정관리	정보시스템 운영체제별 계정등록, 보호, 생성, 정지, 폐기 절차를 마련하고 있는가?	
사용자 인증	비밀번호를 이용한 인증	모든 정보시스템 연결시 사용자 인증 절차를 의무적으로 수행하고 있는가?	
		비밀번호는 장비접근용, 사용자인증용, 자료보호용으로 분리 적용하고 있는가?	
		비밀번호 관리정책을 수립하여 적용하고 있는가?	
		관리자 및 사용자의 비밀번호 관리책임을 규정하여 적용하고 있는가?	
	인증서를 이용한 인증	비밀번호의 대안으로 행정전자서명 인증서 또는 공인전자서명 인증서를 활용하고 있는가?	
	복수 사용자 인증	비밀 등 중요 정보를 취급하는 시스템에 대해서는 비밀번호, 인증서와 별도로 바이오 정보 등을 이용한 인증 방식을 복수로 채택하고 있는가?	
		바이오 정보 등을 이용한 인증시스템을 구축할 경우 보안적합성 검증을 완료한 제품을 사용하는가?	
	접근권한 관리	정보시스템 이용자에 대한 접근권한 정책을 수립하여 적용하고 있는가?	
		정보시스템의 접근권한은 법령 또는 업무규정 등에 따라 허용된 자에 한하여 최소한의 범위로 부여하고 있는가?	
접근 기록 관리	접근기록 관리	접근기록은 로그인 성공여부와 무관하게 기록·유지하고 있는가?	
		시스템관리자는 접근기록을 매일 점검하고 분석내용을 월1회 정보통신보안담당관에게 보고하고 있는가?	
		침임 또는 침입시도의 흔적 등 문제점이 있을 경우에는 즉시 정보통신보안담당관에게 보고하고 있는가?	
		시스템관리자는 접근기록이 불법수정이 되지 않도록 보호하거나, 불법수정을 확인할 수 있는 방법을 마련하여 실시하고 있는가?	
		접근기록은 정보통신보안사고 발생 시 확인 등을 위하여 3년이상 보관(백업자료 포함)하고 있는가?	
		3회 이상 접속시도의 오류가 발생하는 경우 경보를 발생하고 시스템관리자에 통보될 수 있는 기능을 설치하고 있는가?	

구분		점검항목	비고
네트워크 보안 관리	내부 네트워크 보호	정보통신망 관련자료를 최신으로 유지하고 비밀로 분류하여 보호하고 있는가?	
		사설주소체계 등을 활용하여 내부 네트워크 정보를 보호하고 있는가?	
		스위치, 라우터 등과 같은 네트워크 장비는 ACL 기능 적용, 물리적 안전대책 마련, 보안패치 실시, 불필요한 서비스 및 포트 제거 등의 보안조치를 실시하는가?	
	외부 네트워크 접속 보안대책	내부망과 외부망을 분리하고 있는가?	
		중요 정보시스템에 대해서는 내부망과 외부망을 물리적으로 분리하고 있는가?	
		원격연결서비스(rlogin, rsh 등) 사용을 제한하고 있는가?	
		정보시스템 접속 로그를 자동으로 기록하고 주기적으로 점검하고 있는가?	
		네트워크 취약성 점검 도구를 활용하여 주기적으로 취약성을 분석하여 잠재적인 보안위협을 제거하고 있는가?	
		보안적합성이 검증된 침입탐지·차단시스템 등을 설치 운영하여 네트워크를 보호하고 있는가?	
		외부 네트워크와 접속시 보안대책은 보안심사위원회의 심의를 거쳐 결정하고 있는가?	
		원격근무시 인증서 사용, 보안적합성 검증필 제품 이용 등 보안대책을 수립, 시행하는가?	
		원격근무 수행 직원에 대해 보안서약서를 징구하고 보안교육을 실시하는가?	
		원격근무 관련 사용자의 시스템 접근기록을 확인하고 있는가?	
	가용성 보장	통신회선 용량은 기관의 업무처리속도 저하나 장애 발생을 방지하기에 충분한가?	
		정보통신망 장애 여부를 파악하기 위하여 네트워크관리시스템(NMS)을 설치 운영하고 있는가?	
		정보시스템(H/W)의 저장용량, 처리속도 등이 정상 업무수행에 지장이 없도록 시스템을 구성하고 있는가?	
	무선랜 보안	무선랜 사용에 대한 규정이 있는가?	
		무선랜 구축시 통신내용을 보호하기 위해 국가용 보안시스템 설치 등의 보안대책을 적용하고 있는가?	
		회의실 등 유선 설치가 어려운 장소에 한하여 무선랜을 한시적으로만 사용하는지 점검하는가?	
		직원들은 무선랜 등 무선통신망의 보안취약성에 대해 인지하고 있는가?	

구분		점검항목	비고
		무선랜은 무선중계기(AP; Access Point) 전파범위 조정, 사용자 인증, 패킷 암호화 등 보안대책을 적용하고 있는가?	
		관리자는 인가되지 않은 무선중계기(AP)가 사용되는지 여부를 주기적으로 점검하여 제거하는가?	
RFID 보안 관리	RFID 보안대책	RFID시스템 운영관련 보안관리 책임자를 지정하고 있는가?	
		RFID시스템 구축·운영 관련 국가정보원 등 관계기관의 보안성 검토를 받았는가?	
		RFID 태그 발급·변경·폐기관련 규정이 있는가?	
		RFID 태그 발급기, 리더기 접근통제에 대한 규정이 있는가?	
서버 보안 관리	서버 및 DB 보안관리	관리자서비스와 사용자서비스를 분리 운영하고 있는가?	
		불필요한 서비스 포트는 제거하였는가?	
		업무와 시스템의 중요도, 목적에 따라 서버를 분류하고 사용자 접근을 차등 적용하고 있는가?	
		데이터베이스에 대한 사용자의 직접적인 접속을 제한하고 DBMS 종류에 따른 보안대책을 실시하고 있는가?	
		연1회 보안도구를 활용하여 서버의 보안취약성을 점검하고 있는가?	
	공개서버 보안관리	내부 네트워크와 분리된 영역(DMZ)에 설치하고 침입탐지·차단시스템을 설치하여 보호하는가?	
		서버 접속 사용자 계정을 제한하고 불필요한 계정을 삭제하고 있는가?	
		불필요한 서비스 및 시험·개발도구의 사용을 제한하고 있는가?	
		정기적인 백업을 실시하여 사고에 대비하고 있는가?	
	홈페이지 보안관리	홈페이지 운영서버는 업무용 서버와 분리하고 있는가?	
		홈페이지 장애 또는 자료 위·변조, 훼손 등 이상 유무를 실시간으로 확인하는가?	
		홈페이지에는 보안취약점을 방지하기 위한 입력 데이터 검증기능이 있는가?	
		홈페이지 게시판을 통한 해킹을 방지하기 위해 특정 확장자(jsp, a에, php 등)를 가진 파일 업로드를 제한하는가?	
	전자우편 보안관리	출처가 불분명한 전자우편 수신시 열람을 금지하고 정보통신보안담당자에게 신고하도록 교육하는가?	
		전자우편시스템에 악성메일을 차단하기 위한 보안대책을 수립하는가?	
		전자우편을 이용한 정보유출 등을 방지하기 위하여 첨부파일 용량을 제한하고 있는가?	
		정보통신망에 기술적인 조치로 상용 전자우편을 사용을 제한하고 있는가?	

구분		점검항목	비고
PC 등 단말 보안 관리	PC 등 단말 보안관리	개인 사용자의 PC보안에 관한 내용이 규정되어 있는가?	
		PC내 중요자료 유출 가능성이 있는 P2P, 웹하드 등 비인가 프로그램을 설치하지 않도록 조치하고 있는가?	
		사용자는 10분 이상 자리를 이석할 경우 비인가자의 PC접근을 차단하기 위하여 패스워드를 적용한 화면보호기를 설정하고 있는가?	
		사용자는 비인가자의 PC접근을 차단하기 위하여 부팅 패스워드와 로그인 패스워드를 설정하고 있는가?	
		사용자는 윈도우의 자동업데이트를 설정하고 있는가?	
	휴대단말 보안관리	휴대단말의 반출입시 필요한 보안절차를 규정하고 있는가?	
		휴대단말의 반출입 사항을 기록하는가?	
		휴대단말의 분실로 인한 자료유출 방지대책을 강구하고 있는가?	
		반출된 휴대단말 반입시 바이러스 백신프로그램으로 악성코드 감염여부를 점검하는가?	
		정보시스템과 연결하여 사용할 경우, 자료 유출 가능성이 있는 PDA, PMP 등 휴대용 정보통신기기의 소지 및 사용에 대한 보안대책을 강구하고 있는가?	
		카메라 내장 휴대폰, 디지털 카메라 등의 소지 및 촬영을 제한하는가?	
		블루투스, 지그비, 무선 USB 등 새로운 통신수단의 사적 사용을 제한하는가?	
보조 기억 매체 보안 관리	분류 및 보안관리	보조기억매체(USB, 이동형 하드디스크, 디스켓 등) 구입, 관리, 저장, 파기 관련 전담자 지정, 관련 대장 유지 등에 대한 규정이 있는가?	
		보조기억매체는 등록 후 사용하고 관리번호를 부여하는가?	
		보조기억매체는 비밀용, 일반업무용, 공인인증서 보관용으로 구분하여 사용하는가?	
		정보통신보안담당관은 소속 직원에 대해 보조기억매체 사용에 대한 정보통신 보안관련 주의사항을 공지하거나 교육을 실시하는가?	
		정보통신보안담당관은 기관 내 보조기억매체 등록 현황을 파악하고 있는가?	
		부서 정보통신보안담당자는 보조기억매체 사용에 대해 월1회 이상 관리실태를 점검하고 관리책임자(팀·과장)의 확인 서명을 받는가?	
		비인가 보조기억매체 통제를 위한 기술적 보안대책을 마련하고 있는가?	
		비밀(대외비 포함)을 저장하는 보조기억매체는 이중캐비넷 등 안전한 장소에 보관하고 있는가?	

구분		점검항목	비고
	불용, 분실 등 보안대책	업무상 목적으로 사용한 보조기억매체는 불용 처리시 물리적으로 파기하고 있는가?	
		일반용을 타부서 이전 또는 용도를 전환하여 사용하고자 할 경우에는 수록된 자료를 완전히 삭제·포맷 후 사용하고 있는가?	
		비밀용을 일반용 또는 다른 등급의 비밀용으로 전환하여 사용할 경우 또는 일반용을 외부기관에 이전하여 사용하는 경우에는 완전포맷으로 파일을 복원할 수 없도록 하고 있는가?	
		보조기억매체의 분실 또는 소각 등의 사유가 발생하면 즉시 관리책임자에게 그 사실을 보고하여야 하며 관리책임자는 정보통신보안담당관에게 통지하고 있는가?	
		정보통신보안담당관은 일반용의 분실 또는 소각 사실을 통지받거나 인지한 경우에는 자체 조사를 실시하고 재발방지 대책을 강구하고 있는가?	
		정보통신보안담당관은 비밀용의 분실 또는 소각 사실을 통지받거나 인지한 경우에는 국정원장에게 통보하고 있는가?	
		보조기억매체를 불용처리하거나 재사용하는 경우에는 보조기억매체 불용처리 확인서에 정보통신보안담당관의 확인을 받은 후 확인서를 보관하고 있는가?	
악성코드 방지 대책	예방 대책	출처, 유통경로 및 제작자가 명확하지 않은 응용 프로그램은 사용을 자제하고 불가피한 경우에는 백신 등 관련 검색프로그램으로 진단 후 사용하는가?	
		업무상 불필요한 서비스 사용을 제한하고 있는가?	
		업무상 불필요한 서비스 사용을 제한하고 있는가?	
		가급적 드라이브 전체를 공유해서 사용하지 않도록 하고 있는가?	
		출처가 불분명한 전자우편은 열어보지 않고 있으며 자동으로 첨부파일이 실행되지 않도록 설정하였는가?	
		인터넷 등 상용망으로 입수한 자료는 필히 악성코드 검색 후 사용하고 있는가?	
		웹 브라우저는 서명되지 않은(unsigned) ActiveX와 기타 이동 코드 전달 수단이 로컬 시스템에서 알지 못하는 사이에 다운로드되고 실행되지 않도록 구성된 보안 설정을 갖고 있는가?	
		악성코드 조기 발견을 위하여 최신 백신 프로그램 활용 및 보안 업데이트를 실행하고 있는가?	

구분		점검항목	비고
악성 코드 방지 대책	예방 대책	정보시스템이 작동 할 때마다 컴퓨터 하드디스크의 부트섹터 및 메모리 등에 악성코드가 감염되었는지를 점검하고 있는가?	
		비상시 데이터 손실을 최소화하기 위해 데이터를 정기적으로 백업해놓고 복구 디스켓을 준비하고 있는가?	
		정보통신보안담당관은 악성코드 공격에 의한 피해를 복구하기 위한 적절한 백업, 복구계획을 수립하였는가?	
		시스템관리자는 네트워크상의 서버·단말 등에 대하여 주기적으로 점검을 실시하고 불법 소프트웨어 및 악성 코드에 대한 탐지를 수행하고 있는가?	
		정보통신보안담당관은 악성 소프트웨어에 대한 새로운 정보 및 보호대책에 대해 사용자에게 주기적 혹은 수시로 공지를 수행하고 있는가?	
	감염시 조치사항	감염된 정보시스템은 사용을 중지하고 내부망과 접속을 분리하고 데이터를 백업하였는가?	
		최신 백신 등 악성코드 제거 프로그램을 이용하여 악성코드 퇴치를 실시하였는가?	
		감염이 심각할 경우 포맷 프로그램을 사용하여 하드디스크 저수준 포맷을 실시하였는가?	
		악성코드의 감염 확산 방지를 위하여 정보통신보안담당관에게 관련 내용 및 보안조치 사항을 즉시 보고하였는가?	
		시스템관리자는 악성코드 감염의 재발을 방지하기 위하여 원인 분석 및 예방조치를 수행하였는가?	
재난 복구 대책	계획 수립·시행	인위적 또는 자연적인 원인으로 인한 정보통신망의 장애 발생에 대비하여 시스템 이원화, 백업관리, 복구 등 종합적인 재난복구 대책을 수립 시행하고 있는가?	
		시스템관리자별로 역할을 부여하여 재난에 대비하고 있는가?	
	백업 및 복구	시스템 백업 정책 하에서 중요 파일과 프로그램에 대해 주기적으로 백업을 수행하고 있는가?	
		시스템관리자는 백업 목록을 관리하고 목록에는 백업일자, 백업대상, 작업자, 보관 장소 등을 기술하고 있는가?	
		백업이 들어있는 매체는 적절한 보호구역에 보관하고 있는가?	
		백업이 보관된 장소는 재난에 대비한 조치를 수행하고 있는가?	
		필요시 복수의 백업을 만들어 분산 보관하고 있는가?	
		백업된 매체는 주기적으로 복구가 가능한지 테스트하고 있는가?	

3.4 정보통신망 유지보수

구분		점검항목	비고
정보시스템유지보수	절차 마련 및 기록관리	정보시스템 유지보수 업무절차와 주기, 문서화에 대한 규정이 있는가?	
		자체 유지보수 절차에 따라 정기적으로 정비를 실시하고 관련 기록을 보관하고 있는가?	
	반입·반출시 보안관리	정비도구를 반출 또는 반입할 때마다 악성코드 감염여부, 자료 무단 반출을 확인하는가?	
		정보시스템을 외부로 반출할 경우 정보통신보안담당관 등의 통제를 받고 정보통신보안담당관 등은 현황을 기록 유지하는가?	
	원격정비시 보안관리	외부업체의 원격 정비를 원칙적으로 금지하고 있는가?	
		원격정비 허용시 기관의 장이 승인하고 자체 보안대책에 대해 국정원장과 사전에 협의하고 있는가?	
		원격접속 사용자 식별 및 인증대책을 수립하고 있는가?	
		원격 시스템과의 소통 정보를 점검하는가?	
		원격 정비 대상시스템을 내부망과 분리하는가?	
		원격 정비의 내용을 기록·유지하는가?	
정보시스템저장매체불용처리	삭제기준 및 책임	저장자료 삭제 기준 및 책임을 준수하고 있는가?	
	삭제방법 및 확인	저장자료의 삭제는 요령에서 지정한 방법에 따라 조직별 실정에 적합한 방법을 선택하고 있는가?	
		정보통신보안담당관은 정보시스템을 불용처리할 경우 저장자료의 삭제 여부를 확인하는가?	
	외부반출시 보안조치	불용처리, 정비 또는 임차기간 만료로 인해 저장매체 또는 정보시스템을 외부로 반출할 경우 저장매체 보안조치 방안을 계약서에 명시하고 보안서약서 집행, 교육 등의 보안조치를 실시하는가?	

<별표 4>

원격근무 보안점검표

* 공개 : 공개 원격근무, 비공개 : 비공개 원격근무

구 분	점 검 사 항	적용대상				확인
		공개	비 공 개			
			재택	파견	이동	
관리대책	1. 원격근무 업무 선정 기준이 존재하는가?	○	○	○	○	
	2. 원격근무 관련 보안관리지침이 존재하는가?	○	○	○	○	
보안계획 및 활동	1. 원격근무 보안사고 대응계획이 존재하는가?	○	○	○	○	
	2. 비상 연락체계가 존재하는가?	○	○	○	○	
	3. 원격근무 세부계획에 대하여 국가정보원의 보안성 검토를 받았는가?	○	○	○	○	
정보자산	1. 원격근무용 정보자산의 목록이 주기적으로 관리되고 있는가?	○	○	○	○	
	2. 원격근무 관련 문서의 반출·입 대장이 존재하는가?	○	○	○	○	
	3. 원격근무 관련 중요문서의 반출·입 대장이 정기적으로 점검되는가?	○	○	○	○	
	4. 업무변경 및 인사이동시 전산자료 인계인수 절차가 있는가?		○	○	○	
	5. 원격근무자는 소속기관이 제공 또는 인가한 원격근무용 전용장비(H/W, S/W)를 사용하는가?		○	○	○	
	6. 원격근무 전산장비 고장시 정보통신보안담당관에게 통보가 되고 자료유출 방지 대책이 있는가?		○	○	○	
	7. 원격근무 권한 해제시 정보통신보안담당관은 전산장비를 회수 또는 인가취소 하는가?		○	○	○	
원 격 근 무 자 보안관리	1. 원격근무자의 정보통신보안 관련 직무·책임이 명확히 정의되어 있는가?	○	○	○	○	
	2. 원격근무자의 담당직무에 따라 접근권한이 구분 부여되어 있는가?	○	○	○	○	
	3. 원격근무자에게 보안서약서를 징구하는가?	○	○	○	○	
	4. 원격근무자에게 주기적 보안교육이 시행되는가?	○	○	○	○	
	5. 원격근무자 인사변동에 따른 이용권한 회수 절차가 있는가?	○	○	○	○	

구 분	점 검 사 항	적용대상				
		공개	비 공 개			확인
			재택	파견	이동	
원 격 근 무 자 보안관리	6. 원격근무자가 장기간 작업을 하지 않을 경우 이용권한 회수 절차가 있는가?	○	○	○	○	
	7. 원격근무자가 인증정보 분실시 신속한 재인증 절차가 있는가?	○	○	○	○	
	8. 원격근무자의 보안규정 위반시 징계절차가 있는가?	○	○	○	○	
	9. 정보통신보안 관련자료를 원격근무자에게 신속히 배포할 수 있는 수단이 있는가?	○	○	○	○	
물 리 적 보 안	1. 원격근무용 전산장비는 도난·분실·훼손 방지 대책이 있는가?		○	○	○	
	2. 근무시간 중 출입문 시건장치 등 비인가자의 접근방지 대책이 있는가?		○			
불법접근 차단대책	1. 이용권한에 따라 서버 및 네트워크 접근을 통제하고 내부망 접근을 제한하기 위한 침입차단시스템 등 정보보호시스템이 설치·운영되고 있는가?	○	○	○	○	
	2. 정상·오(誤)사용에 대한 모니터링 및 로그자료의 저장·감사가 이루어지는가?	○	○	○	○	
	3. 원격근무자는 행정전자서명(GPKI)인증서를 사용하는가?		○	○	○	
	4. 일회용 패스워드, 생체인증, 기타수단을 이용하여 다단계 인증을 수행하는가?		○	○	○	
	5. 원격근무 전산장비에 전자문서 저장시 국정원장이 승인한 전자문서 보안체계가 적용되는가?		○	○	○	
	6. 원격근무자가 무선랜 이용시 적절한 보안대책이 있는가?(재택·이동근무 중 상용 무선랜 사용 등 부득이한 경우 국가정보원장과 협의한 보안대책을 적용하고 있는가?)		○	○	○	
	7. 승인되지 않은 프로그램 설치 금지 및 주기적 확인·삭제 절차가 있는가?		○	○	○	
	8. 원격근무 서버가 불필요한 서비스 포트를 개방하지 못하도록 보안설정 하였는가?		○	○	○	

구 분	점 검 사 항	적용대상				
		공개	비 공 개			확인
			재택	파견	이동	
운영관리	1. 원격근무 전산장비에 부팅 패스워드, 화면보호기, 사용자인증 비밀번호가 작동중인가?	○	○	○	○	
	2. 원격근무 전산장비에 바이러스 백신, 침입차단시스템이 운영되고 최신 업데이트를 유지하는가?	○	○	○	○	
	3. 원격근무 전산장비의 운영체제 패치 및 보안 관련 최신 업데이트를 유지하는가?	○	○	○	○	
	4. 원격근무 중 이석시 사전 화면보호기능 구동 등 보안조치가 실시되고 있는가?		○	○	○	
	5. 원격근무용 소프트웨어 설치시 시험평가 절차가 있는가?		○	○	○	
	6. KeyLogging, ScreenCapture 등 자료유출 방지대책이 있는가?		○	○	○	

별지 서식

<별지 제1호서식>

정보통신보안업무 세부 추진계획

1. 활동 목표

2. 기본방침

3. 세부 추진계획

분야별	사업명	세부 추진계획	주관・관련부서	비고

※ 보안성검토 대상여부 표기

4. 전년도 보안감사・지도방문 시 도출내용과 조치내역

도 출 내 용	조 치 내 역	담 당 부 서

※ 형식위주의 계획수립을 지양하고 소속기관의 추진계획을 종합, 자체 실정에 맞게 작성

<별지 제2호서식>

정보통신보안업무 심사분석

1. 총　　평

2. 주요 성과 및 추진사항

3. 세부 사업별 실적 분석

추 진 계 획	추 진 실 적	문 제 점	개 선 대 책

※ 추진실적은 목표량과 대비하여 성과 달성도를 계량화

4. 부진(미진)사업

부 진 사 업	원인 및 이유	익년도 추진계획

5. 애로 및 건의사항

6. 첨부(정보통신망 및 정보보호시스템 운용현황 등)

<별지 제3호서식>

전파측정 활동 결과보고

1. 일반 사항

○ 측정기간 및 지역

○ 측정장비

○ 참여기간 및 인원

2. 측정결과 내용

기 간	측정지점	통신구간	주파수 (MHz)	신호세기 (dBM)	취약여부	비고
						※ 디지털/아날로그 구분

3. 분석 및 평가

4. 조치 및 대책

<별지 제4호서식>

정보시스템 관리대장

연번	소속	취급자 (성명)	관리번호	종류 (서버·PC 등)	비 밀 번 호 (필요시 장비용·사용자 인증용·자료용으로 구분)	인증번호	인증 부여 일자	인증 해제 일자

※ PC 등의 비밀번호를 기재하지 아니할 수 있다.

※ 인증번호 : 기관 정보통신보안담당관이 신규 정보자산 도입시 보안대책의 강구여부, 기존시스템 구성요소와의 호환성 등을 확인 후 부여하는 번호(예:07108110002010547l)

※ 관리번호 : 각 부서별로 정보자산을 관리하기 위하여 부여하는 번호(예:12-28-3)

<별지 제5호서식>

암호실 및 암호취급자 현황

구분 / 부서	암 호 실				암 호 취 급 자				비 고
	인가	운용	과부족	변동 내용	인가	운용	과부족	변동 내용	
총 계									

<별지 제6호서식>

암호실 출입자 기록부

소속	직급	성명	직책	용무	출입 일시	서명	인가자인	비고

<별지 제7호서식>

보 안 서 약 서

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

1. 나는 국가용 보안시스템(정보시스템 포함)과 관련된 소관업무가 국가기밀 사항임을 인정하고 제반 보안관계규정 및 지침을 성실히 준수한다.
2. 나는 이 기밀을 누설함이 국가이익을 침해할 수도 있음을 인식하고 재직중은 물론 퇴직 후에도 알게 된 모든 기밀사항을 일체 타인에게 누설하지 아니한다.
3. 나는 기밀을 누설한 때에는 아래의 관계법규에 따라 엄중한 처벌을 받을 것을 서약한다.
   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 주민등록번호

직위 성 명 인

서 약 소속 직급

집행자 직위 성 명 인

<별지 제8호서식>

암호장비 운용관리현황

기관명 :　　년　월　일 현재

순위	시스템명	등록번호	설치장소	상대국소	회선및방식	설치일자	비고

<별지 제9호서식>

국가용 보안시스템 관리기록부

<암호장비용>

장비명	배 부					회 수				변 동 사 항				비고
	일시	수량	등록번호	대상기관	증빙번호	일시	수량	등록번호	증빙번호	일시	근거	수량	확인	

<암호·음어·약호자재용>

자재명칭	제 작				배 부				회 수			변 동 사 항				비고
	일시	수량	등록번호	발행처	일시	수량	등록번호	대상기관	일시	수량	등록번호	일시	근거	수량	확인	

364×257㎜

<별지 제10호서식>

국가용 보안시스템 점검기록부

<암호장비용>

점검일시	장비명칭	점 검 사 항				점 검 관	
		납 봉	암호화	회 선	동 작	성 명	서 명

※ 점검요령

○ 납봉 상태 : 암호장비 외장 불법개봉 여부 점검

○ 암호화상태 : 암호화 또는 비화상태 점검

○ 회선 상태 : 암호장비와 정보통신장비간 접속코드 등 연결상태 점검

○ 동작 상태 : 암호장비의 성능저하 고장여부 등 정상동작 여부 점검

<암호 및 음어·약호자재용>

점검일시	자재명칭	부 수	보관상태	점 검 관		비 고
				성 명	서 명	

※ 국가용 보안시스템 점검기록부는 필요에 따라 암호장비, 암호·음어·약호자재 등 용도별로 분류 또는 통합권으로 사용

<별지 제11호서식>

국가용 보안시스템 증명서

<암호장비용>

○ 증명서 번호		구분 : (배부, 반납, 파기, 정비)		
발신 :		수신 :		
아래 암호장비 및 부품(대)을 (배부, 반납, 폐기, 정비의뢰)하였음		아래 암호장비 및 부품(대)을 (수령, 회수, 폐기, 정비)하였음		
일자 : 년 월 일		일자 : 년 월 일		
소속 :		소속 :		
성명 : (인)		성명 : (인)		
구 분	암 호 장 비 명 칭	수 량	등 록 번 호	비 고

<암호・음어・약호자재용>

○ 증명서 번호		구분 : (배부, 반납, 파기, 정비)		
발 신 :		수신 :		
아래 기록된 (암호, 음어, 약호)자재 (부)를 (배부, 반납, 파기)하였음		아래 기록된 (암호, 음어, 약호)자재 (부)를 (수령, 회수, 파기)하였음		
일자 : 년 월 일		일자 : 년 월 일		
소속 :		소속 :		
성명 : (인)		성명 : (인)		
구분	자 재 명 칭	수량	등록번호	비고

<별지 제12호서식>

암호·음어·약호자재 신청서

자 재 명	수령 지역	실수령 기 관	부 수	산출내역	보 유	과부족	비 고

※ 작성 요령

○ 수령지역 : 세종로청사, 과천청사, 대전청사, 지자체별

○ 산출내역 : 세부 운용부서 및 부수

○ 보　　유 : 현용 자재기준 산출

○ 과 부 족 : 소요자재 부수-현재 보유자재 부수

○ 비　　고 : 조직 신편·증편·통합 등 참고사항 기재

<별지 제13호서식>

암호취급자 및 음어취급자 인감등록서

1. 기관명 :

2. 변동 및 등록일자 : 년 월 일

가. 정 책임자

인 적 사 항		인 감	서 명
직급 및 성명			
직 책			
주민등록번호			
비밀취급등록			

나. 부 책임자

인 적 사 항		인 감	서 명
직급 및 성명			
직 책			
주민등록번호			
비밀취급등록			

다. 실무자

인 적 사 항		인 감	서 명
직급 및 성명			
직 책			
주민등록번호			
비밀취급등록			

<별지 제14호서식>

지편자재 사용기록부

자재 번호	관리 번호	년월일	전 문 액 표			난 수 사 용				소자 년월일	소자자	비고
			번호	송수 구분	조수	부터		까지				
						쪽	행	쪽	행			

297×210㎜(A4)

<작성 요령>

○ 전문 액표

- 번　　호 : 암호전문 일련번호
- 송수구분 : 수발신으로 구분
- 조　　수 : 암호전문 조수

<별지 제15호서식>

암호 개발요원 현황

구 분	인 가	운 용	과부족	변동내용	비 고
총 계					

<별지 제16호서식>

보안자재(암호・음어・약호자재) 보유현황

구 분	자 재 명 칭	수 량	등록번호	비 고

<별지 제17호서식>

암호논리 운용현황

기 관 명	운용부서	운용 시스템	수 량	설 치 일	비 고

<별지 제18호서식>

정보보호제품 자체 점검결과

항 목 명	점 검 항 목	결 과
인 증	CC인증의 경우(EAL 2이상 인증서 획득 여부)	
	CC미인증의 경우, 검증필 제품목록 등재 여부('09.5.31限)	
	국정원장이 검증한 암호모듈 탑재 여부	
일치성	CC인증보고서와 도입제품 보안기능 일치성 여부	
	기술제안서(RFP)에서 요구하는 보안기능 구현여부	
운용환경	운용환경 설치에 따른 제품기능 등 형상변경 가능여부	
	도입기관의 시스템 관리자 지정여부	
	감사기능 지원여부	
	도입기관 주요업무 및 최대 사용자 등에 대한 가용성 보장 여부	
유지보수	보안적합성 검증결과 반영 가능여부	
	업체 기술지원 전담조직 운영 여부	
	작동중단 등 긴급상황에 대비한 지원절차 구비여부	
	업체 유지보수 매뉴얼 제공여부	
	한글 관리자 설치·운영 매뉴얼 제공여부	
	업체의 제품운용교육 제공여부	
	신규취약성에 대한 통보 및 처리절차 구비여부	

※ 점검결과는 O, ×로 표기

<별지 제19호서식>

보안적합성 검증 신청서

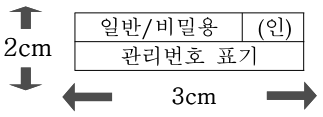
<table>
<tr><td rowspan="8">신청기관</td><td>기 관 명</td><td colspan="3"></td><td>운용부서</td><td></td></tr>
<tr><td>도입목적</td><td colspan="5"></td></tr>
<tr><td rowspan="2">운용환경</td><td>사용자 수</td><td colspan="2"></td><td>망 구성</td><td colspan="2">□ 유선 □ 무선</td></tr>
<tr><td>속도(대역폭)</td><td colspan="5"></td></tr>
<tr><td>운용형태</td><td colspan="5">□ 단독 설치·운용 □ 타 보안제품과 연동 □ 대 국민 배포용</td></tr>
<tr><td>연 동
시 스 템</td><td colspan="5">□ ERP □ KMS □ CRM □ 전자결재 □ 기타 그룹웨어</td></tr>
<tr><td>사 업 명</td><td colspan="5"></td></tr>
<tr><td rowspan="10">신청제품</td><td>업 체 명</td><td colspan="2"></td><td>대 표 자</td><td colspan="2"></td></tr>
<tr><td>주 소</td><td colspan="2"></td><td>전화번호</td><td colspan="2"></td></tr>
<tr><td rowspan="3">제 품 명</td><td colspan="2"></td><td>CC
인증번호</td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td>암호
검증번호</td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td>용역개발
여부</td><td colspan="2">□ 예 □ 아니오</td></tr>
<tr><td>평가기관</td><td></td><td>인증기관</td><td></td><td>등급</td><td></td></tr>
<tr><td rowspan="3">담 당 자</td><td>전화번호</td><td colspan="4"></td></tr>
<tr><td>휴대폰번호</td><td colspan="4"></td></tr>
<tr><td>E-mail</td><td colspan="4"></td></tr>
<tr><td>암호모듈</td><td colspan="6">□ 없음 □ 있음 (□ 검증 □ 미 검증)</td></tr>
</table>

※ 복수의 시스템을 신청하는 경우, 별도 출력하여 대상 시스템 란에만 기재

<별지 제20호서식>

보조기억매체 라벨

<디스켓, 이동형 HDD 서식>



<USB·CD 등 서식>

- 同 서식을 만들어 보조기억매체 중앙의 적절한 위치에 부착
- 첫 번째 줄에는 일반/비밀용은 정보통신 보안담당관의 직인을 날인하고 공인인증서용은 관리책임자의 직인을 날인
- 두 번째 줄에는 보조기억매체 관리번호 표기
- 세 번째 줄의 '정'란에 관리책임자, '부'란에 취급자 표기(USB메모리 및 CD의 경우 생략 가능)
- 보조기억매체의 크기를 고려하여 서식, 글자 크기 조정 가능

[보조기억매체 라벨 사용 像]

일반용			(인)
총무과-일반-01			
정	이순신	부	홍길동

비밀용			(인)
총무과-대외비-01			
정	이순신	부	홍길동

공인인증서용			(인)
총무과-인증-01			
정	이순신	부	홍길동

일반용	(인)
총무과-일반-01	

Ⅱ급비밀용	(인)
총무과-Ⅱ급-01	

공인인증서용	(인)
총무과-인증-01	

<별지 제21-1호서식>

보조기억매체 관리대장(일반용)

<관리책임자 : __급 ○○○>

연번	관리번호 (S/N)	매체 형태	등록 일자	취급자 (성명)	불용처리 일자	불용처리방법 (재사용 용도)	비고 (사유)

<별지 제21-2호서식>

보조기억매체 관리대장(비밀용)

<관리책임자 : __급 ○○○>

연번	관리번호 (S/N)	등급	매체 형태	등록 일자	취급자 (성명)	불용처리 일자	불용처리방법 (재사용 용도)	비고 (사유)

<별지 제21-3호서식>

보조기억매체 관리대장(공인인증서용)

<관리책임자 : __급 ○○○>

연번	관리번호 (S/N)	매체 형태	등록 일자	취급자 (성명)	용도	해지일자	해지사유

<별지 제22호서식>

보조기억매체 점검대장

<관리책임자 : __급 ○○○>

점검 일시	현 보유수량					이상 유무	점검관		비 고 (서명)
	Ⅱ급	Ⅲ급	대외비	일반	인증		성명	서명	

<별지 제23호서식>

보조기억매체(전산장비 포함) 반출·입 대장

<관리책임자 : __급 ○○○>

장비명	관리번호 (S/N)	사용자 (직급)	용도	반출·입 일시 (반/출)	확인

<별지 제24호서식>

보조기억매체 불용처리 확인서

아래와 같이 보조기억매체(　종　점) 불용처리 및 보조기억매체(　종　점) 재사용에 대한 확인을 요청함

연번	관리번호 (S/N)	매체형태	사　유	불용처리 방법	재사용

확인일자 :　　년　　월　　일

요청자 : 소속・직책　　○급 성명 :　　(인)

확인자 : 정보통신보안담당관　○급 성명 :　　(인)

<별지 제25호서식>

열람·제공자료 관리대장

용역업체 관리책임자	각 기관 관리책임자

년 (일련번호:) 사업명: 사업주관기업:

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

297×210㎜(A4)

<별지 제26호서식>

보 안 확 약 서

본인은 귀 기관과 계약한 _____ 사업의 수행을 완료함에 있어, 다음 각호의 보안사항에 대한 준수 책임이 있음을 서약하며 이에 확약서를 제출합니다.

1. 본 업체(단체)는 업체(단체) 및 사업 참여자가 사업수행 중 지득한 모든 자료를 반납 및 파기하였으며, 지득한 정보에 대한 유출을 절대 금지하겠습니다.
2. 본 업체(단체)는 하도급업체에 대해 상기 항과 동일한 보안사항 준수 책임을 확인하고 보안확약서 징구하였으며, 하도급업체가 위의 보안사항을 위반할 경우에 주사업자로서 이에 동일한 법적 책임을 지겠습니다.
3. 본 업체(단체)는 상기 보안사항을 위반할 경우에 귀 기관의 사업에 참여 제한 또는 기타 관련 법규에 따른 책임과 손해배상을 감수하겠습니다.

년 월 일

서약업체(단체) 대표

소 속 :

직 급 :

성 명 : (서명)

○○○○○○○장 귀하

<별지 제27호서식>

사용자계정 관리대장

연번	소속	성명	업무명	계 정	접근권한	처리내용 (등록, 수정, 삭제)	처리일자	확인

<별지 제28호서식>

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.

년 월 일

서약자	소속	직급	주민등록번호	
		직위	성명	인
서 약	소속	직급	주민등록번호	
집행자		직위	성명	인

<별지 제29호서식>

원격근무 보안관리대장

소속명	부서	직급/직위	성명	인증ID	신청일	폐기일	폐기사유

<부록>

전자정보 보호등급 세부분류기준

1. 목적 및 적용대상

1-1. 목　　적

이 기준은 본 지침 제18조(전자정보 보호등급 분류)에 따라 행정기관별 전자정보의 가치 및 중요도에 따른 보호수준을 분류하여 전산자원을 체계적·효율적으로 관리함에 있어 참고할 수 있도록 세부사항을 권고함에 있음

1-2. 적용 대상

이 기준은 비밀로 분류된 전자정보를 제외한 일반자료를 대상으로 함

2. 용어 정의

가. “기밀성”이라 함은 정당한 사용자가 허용된 정보만을 알 수 있도록 하는 정보보호의 특성을 말함

나. “무결성”이라 함은 비인가자가 정보내용을 불법적으로 위·변조 또는 훼손할 수 없도록 하는 정보보호의 특성을 말함

다. “가용성”이라 함은 정당한 사용자가 정보를 접근하고자 할 경우 지체 없이 접근하여 사용할 수 있도록 하는 정보보호의 특성을 말함

3. 분류기준

3-1. 분　　류

전자정보 보호가치 및 업무특성 등 행정기관의 전산환경에 적합한 전자정보의 보호등급을 분류함

3-2. 전자정보 특성

동 기준은 전자정보의 기밀성·무결성·가용성 등 정보보호 특성을 고려하여 설정함. 다만, 행정기관의 전산환경에 따라 동 기준에서 제시한 3가지 특성 이외의 다른 정보보호 특성을 고려할 수 있음

3-3. 보호등급 단계

전자정보의 보호수준은 기밀성·무결성·가용성 등 정보보호 특성이 손상될 경우에 예상 피해정도에 따라 '가'급, '나'급, '다'급의 3단계로 구분할 수 있음

① 보호수준이 '가'급인 경우는 3가지 정보보호 특성 중 한 가지 특성이 손상되더라도 예상되는 피해정도가 클 경우를 말함

② 보호수준이 '나'급인 경우는 3가지 정보보호 특성 중 한 가지 특성이 손상되더라도 예상되는 피해정도가 중간일 경우를 말함

③ 보호수준이 '다'급인 경우는 3가지 정보보호 특성 중 한 가지 특성이 손상되더라도 예상되는 피해정도가 낮은 경우를 말함

3-4. 예상 피해정도의 구분

전자정보의 기밀성·무결성·가용성 등이 손상될 경우 피해정도는 다음과 같이 결정함

가. 피해정도가 큰 전자정보는 다음과 같은 경우임

① 개인 신상 및 재산권에 심각한 손상을 줄 수 있는 피해

② 기관의 신뢰성에 심각한 손상을 줄 수 있는 피해

③ 기관의 중요업무 수행에 장애를 줄 수 있는 피해

④ 복구에 많은 예산과 상당한 기간이 요구되는 피해

⑤ 다른 기관의 업무수행에 영향을 주는 피해

나. 피해정도가 중간인 전자정보는 다음과 같은 경우임

① 개인 신상 및 재산권에 경미한 손상을 줄 수 있는 피해

② 기관의 기본적 임무수행에 지장을 초래하는 피해

③ 기관의 신뢰성을 손상하는 피해

④ 내부 관리상 문제를 주는 피해

⑤ 다른 기관의 업무수행에 경미한 영향을 주는 피해

다. 피해정도가 낮은 전자정보는 다음과 같은 경우임

① 중요 업무가 아닌 부수적 업무수행에 경미한 지장을 주는 피해

② 기관의 신뢰성에 경미한 손상을 주는 피해

③ 내부 관리상 문제가 발생하나 빠른 기간 내에 복구가 가능한 피해

라. 추가 고려사항

전자정보의 기밀성·무결성·가용성 등 정보보호 특성 이외의 해당 자료로 수행되는 업무의 중요성, 전자정보 보유건수 및 대체성 등을 고려할 수 있음

① 해당 전자정보로 수행되는 업무가 행정기관에서 차지하는비중이 클수록 전자정보는 높은 보호수준을 요구함

② 입력된 전자정보의 건수가 많을수록 전자정보의 보호수준은 높게 요구될 수 있음

③ 해당 전자정보의 손상에 대비한 백업 등 대체수단이 없을 경우 전자정보의 보호수준은 높게 요구될 수 있음