한국정책방송원 정보보안 규정

[시행 2017. 9. 18.] [한국정책방송원예규 제146호, 2017. 9. 18., 일부개정]

한국정책방송원(방송기술부), 044-204-8331

제1장 총 칙

제1조(목적) 이 규정은 「보안업무규정」(대통령령), 「국가사이버안전관리규정」(대통령훈령), 국가정보원 「국가 정보보안 기본지침」 등에 따라, 한국정책방송원 정보보안을 위하여 수행하여야 할 기본활동 규정을 목적으로 한다.

제2조(정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

1. "사용자"라 함은 한국정책방송원으로부터 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 직원 등을 말한다.
2. "정보통신망"이라 함은 「전기통신기본법」 규정에 따른 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송수신하는 정보통신체제를 말한다.
3. "인터넷서비스망"(이하 "인터넷망"이라 한다)이라 함은 기관의 네트워크 중에서 인터넷을 사용할 수 있도록 연결되어 있는 인터넷 전용망을 말한다.
4. "업무전산망"(이하 "업무망"이라 한다)이라 함은 기관의 네트워크 중에서 내부 업무를 수행할 수 있도록 연결되어 있는 전산망을 말한다.
5. "정보시스템"이라 함은 PC·서버 등 단말기, 보조기억매체, 전산·통신 장치, 정보통신기기, 응용프로그램 등 정보의 수집·가공·저장·검색·송수신에 필요한 하드웨어 및 소프트웨어 일체를 말한다.
6. "휴대용 저장매체"라 함은 디스켓·CD·외장형 하드디스크·USB메모리 등 정보를 저장할 수 있는 것으로 PC 등의 정보시스템과 분리할 수 있는 기억장치를 말한다.
7. "정보보안" 또는 "정보보호"라 함은 정보시스템 및 정보통신망을 통해 수집·가공·저장·검색·송수신 되는 정보의 유출·위변조·훼손 등을 방지하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위로서 사이버안전을 포함한다.
8. "전자문서"라 함은 컴퓨터 등 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 정보를 말한다.
9. "전자기록물"이라 함은 정보처리능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 기록정보자료를 말한다.
10. "전자정보"라 함은 한국정책방송원이 업무와 관련하여 취급하는 전자문서 및 전자기록물을 말한다.
11. "정보통신실"이라 함은 서버·PC 등과 스위치·교환기·라우터 등 네트워크 장치 등이 설치 운용되는 장소를 말하며, 전산실·통신실·전자문서 및 전자기록물(전자정보) 보관실 등을 말한다.
12. "정보보호시스템"이라 함은 정보의 수집·저장·검색·송신·수신시 정보의 유출, 위·변조, 훼손 등을 방지하기 위한 하드웨어 및 소프트웨어를 말한다.

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

제3조(적용범위) ① 이 규정은 한국정책방송원 직원 및 추진하고 있는 업무와 관련된 모든 인력에 대해 적용한다.

②이 규정은 우리 원이 보유하고 있는 모든 정보자산을 그 대상으로 한다. <2017. 9. 18. 신설>

제2장 정보보안 기본활동

제4조(정보보안담당관 운영) ① 원장은 효율적·체계적인 정보보안 업무를 총괄하기 위하여 정보화업무를 담당하는 부서의 장을 정보보안담당관으로 지정한다. <2017. 9. 18. 개정>

②정보보안담당관은 다음 각 호의 업무를 수행한다.

1. 정보보안 정책 및 기본계획 수립·시행
2. 정보보안 관련 규정·지침 등 제·개정
3. 보안심사위원회에 정보보안 분야 안건 심의 주관
4. 정보보안 업무 지도·감독, 정보보안 감사 및 심사분석
5. 정보통신실, 정보통신망 및 정보자료 등의 보안관리
6. 사이버공격 초동조치 및 대응
7. 사이버위협정보 수집 · 분석 및 보안관제
8. 정보보안 예산 및 전문인력 확보
9. 정보보안 사고 조사 결과 처리
10. 정보보안 교육 및 정보협력
11. 정보통신망 보안대책의 수립 · 시행
12. '사이버보안진단의 날' 계획 수립 · 시행
13. 그 밖에 정보보안 관련 사항

제5조(분임보안담당관 지정·운영) ① 보안담당관은 각 부서의 보안 업무를 위하여 분임보안담당관을 지정하여 운영할 수 있으며, 별도 발령 없이 보직과 동시에 각 부서의 장이 분임보안담당관이 된 것으로 본다.

②분임보안담당관은 다음 각 호의 업무를 수행한다.

1. 보안담당관 또는 정보보안담당관으로부터 지시 또는 위임을 받은 사항
2. 소관의 업무에 대한 제반 보안 관리사항

③각 부서에서는 분임보안담당관을 보좌하는 보안업무 담당자를 둘 수 있으며, 별도로 지정하지 않을 경우, 서무업무 담당자를 부서의 보안담당자로 한다. <2017. 9. 18. 신설>

제6조(정보보안 교육) ① 정보보안담당관은 자체 정보보안 교육계획을 수립하여 연 1회 이상 전 직원을 대상으로 관련 교육을 실시하여야 한다.

②정보보안담당관은 연 1회 이상 부서별 정보보안 담당자 및 신입직원을 대상으로 교육대상에 맞는 교안을 작성하여 교육을 실시하여야 한다.

③정보보안담당관은 정보보안담당자의 업무 전문성을 제고하기 위하여 관련 전문기관 교육 및 기술 세미나 참석을 적극 장려하여야 한다. <2017. 9. 18. 개정·신설>

제7조(사이버보안진단의 날) ① 매월 세 번째 수요일을 '사이버보안진단의 날'로 지정·운영하여야 한다.

②정보보안담당관은 '사이버보안진단의 날'에 소관 정보통신망의 악성코드 감염여부, 정보시스템의 보안 취약여부 등 정보보안업무 전반에 대하여 체계적이고 종합적인 보안진단을 실시하여야 한다.

③사용자는 '사이버보안진단의 날'에 해당 보안 프로그램을 반드시 실행하고 미비점을 보완하여야 한다.

④정보보안담당관은 '사이버보안진단의 날'에 월별 중점 점검사항 점검 및 미비점 보완 등 체계적이고 종합적인 보안진단을 실시한다.

⑤제1항 및 제2항에 따른 보안진단 결과를 문화체육관광부 정보화담당관에게 제출하여야 한다. <2017. 9. 18. 개정·신설>

제8조(정보보안 사고 조사) ① 별표 1의 정보보안 사고가 발생한 때에는 즉시 피해확산 방지를 위한 조치를 취하고 다음 각 호의 사항을 문화체육관광부 정보화담당관에게 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

②정보보안담당관은 재발방지를 위한 보안대책의 수립·시행 등 사고조사 결과에 따라 필요한 조치를 하여야 한다. <2017. 9. 18. 개정·신설>

제9조(재난방지) ① 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애 발생에 대비하여 정보시스템 이원화, 백업관리, 복구 등 종합적인 재난방지 대책을 수립·시행하여야 한다.

②정보시스템 장애에 대비한 백업시설을 확보하고 정기적으로 백업을 수행하여야 한다.

③제2항에 따른 백업시설을 설치할 경우에는 정보통신실과 물리적으로 일정거리 이상 떨어진 안전한 장소에 설치하여야 하며 전력공급원 이원화 분리 등 정보시스템의 가용성을 최대화 할 수 있도록 하여야 한다. <2017. 9. 18. 개정>

제10조(보안 위규자 처리) 정보보안담당관은 정보보안 규정 위규자 및 정보보안 사고자가 발생한 때에는 공무원 징계령 시행규칙상 보안위규 징계기준과 문화체육관광부 보안위규 처리기준에 따라 징벌 조치를 보안담당관에게 요구할 수 있다. <2017. 9. 18. 신설>

제11조(보안업무 세부추진계획 수립 및 심사분석) ① 정보보안담당관은 정보보안업무 세부추진계획(「국가사이버안전관리규정」제9조에 따른 사이버안전대책을 포함한다)을 수립·시행하고, 그 추진결과를 심사분석 하여야 한다.

②제1항의 경우 정보보안담당관은 세부추진계획 및 심사분석을 작성하여 운영관리부에 제출한다. <2017. 9. 18. 신설>

제3장 정보보안 관리

제1절 기본사항

제12조(인적보안) ① 정보통신망을 통하여 비밀 등 중요정보를 취급하는 사용자에 대해서는 비밀취급인가, 보안서약서 징구 등의 보안조치를 하여야 한다.

②시스템관리자는 사용자가 보직변경, 퇴직 등 인사이동이 있을 경우 관련 정보 시스템 접근권한을 조정하고, 분임보안담당관은 별지 제10호 서식을 활용하여 보안점검을 하여야 한다. <2017. 9. 18. 개정>

③외부 인력을 활용하여 정보시스템의 개발, 운용, 정비 등을 수행할 경우에는 해당 인력의 고의 또는 실수로 인한 정보유출이나 파괴를 방지하기 위하여 보안조치를 수행하여야 한다. 용역사업에 관련된 세부 사항은 제33조(용역사업 보안관리) 또는 「외부 용역업체 보안관리방안」(「국가 정보보안 기본지침」부록 7)을 따른다.

제13조(정보시스템 보안) ① 정보시스템(PC·서버·네트워크장비, 정보통신기기 등 포함)을 도입·사용할 경우, 사용자와 해당 스템의 관리자 및 관리책임자를 지정 운용하여야 한다.

②사용자는 개인PC 등 소관 정보시스템을 사용하거나 본인 계정으로 정보통신망에 접속하는 것과 관련한 보안책임을 가진다.

③시스템관리자는 서버·네트워크 장비 등 부서 공통으로 사용하는 정보시스템의 운용과 관련한 보안책임을 가진다.

제14조(정보통신시설 보안) ① 중요 정보통신시설 및 장소를 「보안업무규정」 제32조에 따른 보호구역으로 설정 관리하여야 한다. <2017. 9. 18. 개정>

1. 통신실
2. 정보통신실
3. 백업센터 및 중요한 정보통신시설을 집중 제어하는 국소
4. 그 밖에 보안관리가 필요하다고 인정되는 정보시스템 설치 장소

②제1항에서 지정된 보호구역에 대한 보안대책을 강구할 경우 다음 각 호 사항을 참고하여야 한다.

1. 방재대책 및 외부로부터의 위해(危害) 방지대책
2. 상시 이용하는 출입문은 한 곳으로 정하고 이중 잠금장치 설치
3. 출입자 인증·식별 등을 위한 출입문 보안장치 설치 및 주야간 감시대책
4. 정보시스템 안전지출 및 긴급파기 계획 수립
5. 관리책임자 및 자료 · 장비별 취급자 지정 운용
6. 정전에 대비한 비상전원 공급, 시스템의 안정적 중단 등 전력관리 대책

제15조(전자적 수단에 의한 비밀의 관리) ① 전자적 방법을 사용하여 비밀을 관리할 경우 국가정보원장이 안전성을 확인한 암호자재를 사용하여 비밀의 위조·변조·훼손 및 유출 등을 방지하기 위한 보안대책을 마련하여 시행하여야 한다.

②비밀을 전자적 수단으로 생산하는 경우 해당 비밀등급 및 예고문을 입력하여 열람 또는 인쇄 시 비밀등급이 자동적으로 표시되도록 하여야 한다.

③비밀을 전자적 수단으로 생산·보관·열람·인쇄·송수신 또는 이관하는 경우 그 기록이 유지되도록 하여야 하며, 송수신 또는 이관하는 경우에는 전자적으로 생성된 접수증을 사용하여야 한다.

④전자적 수단으로 비밀을 생산한 경우 컴퓨터에 입력된 비밀내용을 삭제하여야 한다. 다만, 업무수행을 위하여 필요한 경우에는 비밀저장용 보조기억매체를 지정·사용하거나 암호자재로 암호화한 후 보관하여야 한다.

⑤제4항의 경우 업무망 전용 PC에서 비밀 등 중요 전자정보를 처리한다.

⑥비밀을 전자적으로 생산하고자 할 때에는 해당 비밀등급과 예고문을 입력하여 종이문서로 출력 시 비밀등급이 표시되도록 하여야 한다. 사용자는 비밀을 전자적으로 생산하고자 할 경우 업무망 전용 PC에서 비밀 등 중요 전자정보를 생성하되 반드시 비밀번호를 설정하여야 한다.

⑦전자적으로 처리된 비밀을 종이문서로 출력한 이후의 취급 관리는 「보안업무규정」(대통령령)에 따른다. <2017. 9. 18. 신설>

제16조(보안성 검토) 정보통신망의 신·증설 등에 대하여 보안 대책을 강구하고 적절성 확인을 위하여 관련 사업 계획단계에서 (사업 공고 전) 문화체육관광부 정보화담당관에게 보안성 검토를 의뢰하여야 한다. <2017. 9. 18. 개정>

제2절 전자정보 보안대책

제17조(PC 등 단말기 보안관리) ① 사용자는 PC·노트북·스마트폰 등 단말기(이하 "PC 등"이라 한다) 사용과 관련한 일체의 보안관리 책임을 가진다.

②정보보안담당관은 비인가자가 PC 등을 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손시키지 못하도록 다음 각 호의 보안대책을 단말기 사용자에게 지원하며, 사용자는 이를 준수하여야 한다.

1. 장비(CMOS 비밀번호) ·자료(문서자료 암호화 비밀번호)·사용자(로그온 비밀번호)별 비밀번호를 주기적으로 변경 사용
2. 10분 이상 PC 등의 작업 중단 시 비밀번호 등이 적용된 화면보호 조치
3. PC용 최신 백신 운용·점검, 침입차단·탐지시스템 등을 운용하고 운영체제(OS) 및 응용프로그램(아래아한글, MS Office, Acrobat 등)의 최신 보안 패치 유지
4. 업무상 불필요한 응용프로그램 설치 금지 및 공유 폴더의 삭제
5. 그 밖에 국가정보원장이 안전성을 확인하여 배포 승인한 프로그램의 운용 및 보안권고문

③사용자는 PC 등을 교체·반납·폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 정보보안담당관과 협의하여 하드디스크에 수록된 자료가 유출, 훼손되지 않도록 보안조치 하여야 한다.

④부서별 보안담당자는 사용자가 PC 등을 기관 외부로 반출하거나 내부로 반입할 경우에 별지 제1호 서식을 작성하여 관리하고 최신 백신 등을 활용하여 해킹프로그램 감염 여부를 점검하여야 한다.

⑤누구든지 개인 소유의 PC 등을 무단 반입하여 사용하여서는 안 된다. 다만, 부득이한 경우에는 정보보안담당관의 승인을 받아 사용할 수 있다. <2017. 9. 18. 개정>

제18조(인터넷PC 보안관리) ① 사용자는 인터넷PC에 대해 비인가자가 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손시키지 못하도록 다음 각 호의 보안대책을 준수하여야 한다.

1. 메신저·P2P·웹하드 등 업무에 무관하거나 Active-X 등 보안에 취약한 프로그램과 비인가 프로그램·장치의 설치 금지
2. 업무망과 인터넷망이 분리된 인터넷PC는 특별한 사유가 없는 한 문서프로그램은 읽기전용으로 운용

3. 음란·도박·증권 등 업무와 무관한 사이트 접근 차단조치

②대외 공개용 전산자료의 유통 등의 업무를 위해 제1항의 예외처리가 필요한 경우 정보보안담당관과 협의하고 별지 제3호, 제4호, 제5호 서식에 의거 신청서를 제출하여 승인을 받아야 한다.

③그 밖에 인터넷 PC의 보안 관리에 관련한 사항에 대해서는 제17조(PC 등 단말기 보안관리)를 따른다. <2017. 9. 18. 개정·신설>

제19조(서버 보안관리) ① 서버 관리자는 서버를 도입·운용할 경우, 정보보안담당관과 협의하여 해킹을 이용한 자료 절취, 위·변조 등에 대비한 보안대책을 수립·시행하여야 한다.

1. 서버 관리자는 서버 내 저장자료에 대해 업무별·자료별 중요도에 따라 사용자의 접근권한을 차등 부여
2. 사용자별 자료의 접근범위를 서버에 등록하여 인가여부를 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 단말 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

②정보보안담당관은 제1항에서 수립한 보안대책의 적절성을 수시 확인하되, 연 1회 이상 보안도구를 이용하여 서버 설정 정보 및 저장자료의 절취, 위·변조 가능성 등 보안취약점을 점검하여야 한다. <2017. 9. 18. 개정>

제20조(웹서버 등 공개서버 보안관리) ① 서버 관리자는 외부인에게 공개할 목적으로 설치되는 웹서버 등 공개서버를 내부망과 분리된 영역(DMZ)에 설치·운용하여야 한다. <2017. 9. 18. 개정>

②비인가자의 서버 저장자료 절취, 위·변조 및 분산서비스거부(DDoS) 공격 등에 대비하기 위하여 국가정보원장이 안전성을 검증한 침입차단·탐지시스템 및 DDoS 공격대응시스템을 설치하는 등 보안대책을 강구하여야 한다.

③서버 관리자는 비인가자의 공개서버내 비공개 정보에 대한 무단 접근을 방지하기 위하여 서버 접근 사용자를 제한하고 불필요한 계정을 삭제하여야 한다.

④공개서버의 서비스에 필요한 프로그램을 개발하고 시험하기 위하여 사용된 도구(컴파일러 등)는 개발 완료 후 삭제를 원칙으로 한다.

⑤공개서버의 보안관리에 관련한 그 밖의 사항에 대해서는 제14조(서버 보안관리)에 따른다.

제21조(홈페이지 게시자료 보안관리) ① 정보보안담당관은 문화정보화업무 운영 및 이용에 관한 지침(제6장 홈페이지 운영)에 의거 개인정보를 포함한 중요 업무자료가 홈페이지에 무단 게시되지 않도록 관리한다.

②사용자는 개인정보, 비공개 공문서 및 민감 내용 등이 포함된 자료를 홈페이지에 공개하여서는 아니 된다.

③홈페이지에 정보를 게시하고자 하는 부서의 장은 정보보안담당관과 협의하여 비밀 등 비공개 자료가 게시되지 않도록 하여야 한다. 다만, 기존에 게시한 자료 내용 중 단순하게 수치를 변경하거나 경미한 사항은 그러하지 아니할 수 있다.

④사용자는 인터넷 블로그·카페·게시판·개인 홈페이지 또는 소셜네트워크 서비스 등 일반에 공개된 전산망에 업무관련 자료를 무단 게재하여서는 아니 된다.

⑤정보보안담당관은 홈페이지 등에 비공개 내용이 게시되었는지 여부를 주기적으로 확인하고 개인정보를 포함한 비공개 자료가 홈페이지에 공개되지 않도록 보안교육을 주기적으로 실시하여야 한다.

⑥홈페이지에 중요정보가 공개된 것을 인지할 경우 이를 즉시 차단하는 등의 보안조치를 강구 시행하여야 한다. <2017. 9. 18. 개정>

제22조(사용자계정 관리) ① 시스템관리자는 사용자에게 정보시스템 접속에 필요한 사용자계정(ID) 부여 시 비인가자 도용 및 정보통신시스템 불법 접속에 대비하여 다음 각 호의 사항을 반영하여야 한다.

1. 직무변경, 퇴직 등 인사이동이 있을 경우 접근권한 조정
2. 사용자별·그룹별로 접근권한 부여 및 사용자계정 공용 금지
3. 외부인에게 계정 부여는 불허하되 업무상 불가피시 원장 책임 하에 필요업무에 한해 특정기간 동안 접속토록 하는 등 보안조치 강구 후 허용
4. 장기간 사용하지 않는 휴면계정을 점검하여 불필요 시 삭제
5. 사용자계정을 주기적(관리자 계정 3개월, 사용자계정 6개월)으로 점검하여 접근권한 재검토 <2017. 9. 18. 개정·신설>

②시스템관리자는 사용자가 5회 이상에 걸쳐 로그인 실패 시 정보시스템 접속을 중단시키도록 시스템을 설정하고 비인가자의 침입 여부를 확인 점검하여야 한다.

③시스템관리자는 직원의 퇴직 또는 보직변경 발생 시 사용하지 않는 사용자계정을 신속히 삭제하고, 특별한 사안이 없는 한 유지보수 등을 위한 외부업체 직원에게 관리자계정 제공을 금지하여야 한다.

제23조(비밀번호 관리) ① 사용자는 비밀번호 설정 사용 시 정보시스템의 무단사용 방지를 위하여 다음 각 호와 같이 구분하여야 한다. <2017. 9. 18. 개정>

1. 비인가자의 정보통신시스템 접근방지를 위한 장비 접근용 비밀번호(1차)
2. 정보시스템 사용자가 서버 등 정보통신망에 접속 인가된 인원인지 여부를 확인하는 사용자인증 비밀번호(2차)
3. 문서에 대한 열람·수정 및 출력 등 사용권한을 제한할 수 있는 자료별 비밀번호(3차)

②비밀이나 중요자료에는 자료별 비밀번호를 반드시 부여하되, 공개 또는 열람 자료에 대해서는 부여하지 아니할 수 있다.

③비밀번호는 다음 각 호의 사항을 반영하여 숫자와 영문자, 특수문자 등을 혼합하여 9자리 이상으로 정하고, 분기별로 1회 이상 주기적으로 변경 사용하여야 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. 동일단어 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

④ 서버에 등록된 비밀번호는 암호화하여 저장하여야 한다.

제24조(업무망 보안관리) ① 사용자는 업무망과 인터넷망 간의 자료교환은 보안USB 또는 망간자료전송시스템을 통해 사용하여야 한다.

②사용자는 업무망 PC의 자료를 인터넷PC로 전송할 경우 결재권자의 사전 또는 사후 승인절차를 준수하여야 한다. <2017. 9. 18. 신설>

제25조(네트워크장비 보안관리) ① 시스템관리자는 라우터, 스위치 등 네트워크 장비 운용과 관련하여 다음 각 호의 보안조치를 강구해야 한다. <2017. 9. 18. 개정>

1. 네트워크 장비에 대한 원격접속은 원칙적으로 금지하되, 불가피할 경우 장비 관리용 목적으로 내부 특정 IP · MAC 주소에서의 접속은 허용
2. 물리적으로 안전한 장소에 설치하여 비인가자의 무단접근 통제
3. 최초 설치 시 보안취약점을 점검하여 제거하고 주기적으로 보안패치를 실시
4. 불필요한 서비스 포트 제거

②시스템관리자는 네트워크 장비의 접속기록을 6개월 이상 유지하여야 하고 비인가자의 침투 여부를 주기적으로 점검하여 정보보안담당관에게 관련결과를 제출하여야 한다.

제26조(전자우편 보안대책) ① 시스템관리자는 웜·바이러스 등 악성코드로부터 사용자 PC 등 전자우편 시스템 일체를 보호하기 위하여 국가정보원장이 안전성을 확인한 백신, 바이러스 월, 해킹메일 차단시스템을 구축하는 등 보안대책을 강구하여야 한다.

②사용자는 네이버, 다음, 구글 등 상용 전자우편을 이용하여 업무자료를 송·수신할 수 없으며 기관 전자우편(내부메일, 공직메일)으로 송·수신한 업무자료는 활용 후 메일함에서 삭제하여야 한다.

③사용자는 메일에 포함된 첨부파일이 자동 실행되지 않도록 설정하고 첨부파일 다운로드 시 반드시 최신 백신으로 악성코드 은닉여부를 검사하여야 한다.

④사용자는 출처가 불분명하거나 의심되는 제목의 전자우편은 열람을 금지하고 해킹메일로 의심되는 메일 수신시에는 즉시 정보보안담당관 또는 문화체육관광부 사이버안전센터 전자우편(mcstcert@mcst-csc.go.kr)으로 신고하여야 한다.

⑤사용자는 전자우편을 사용하는 PC에 대하여 제17조(PC 등 단말기 보안관리) 및 제23조(비밀번호 관리)에 명시된 보안조치 사항을 따른다. <2017. 9. 18. 개정>

제27조(휴대용 저장매체 보안대책) ① 사용자는 휴대용 저장매체를 사용하여 업무자료를 보관할 필요가 있을 때에는 위변조, 훼손, 분실 등에 대비한 보안대책을 강구하여 USB 관리시스템을 통해 승인을 받아야 한다.

②사용자는 휴대용 저장매체를 비밀용, 일반용으로 구분하여야 한다.

③부서별 보안담당자는 주기적으로 휴대용 저장매체의 수량 및 보관 상태를 점검하며 반출·입을 통제하여야 한다.

④사용자는 휴대용 저장매체에 비밀자료를 저장할 경우, 매체별로 비밀등급 및 관리번호를 부여하고 비밀관리기록부에 등재 관리하여야 한다. 또한 매체 전면에 비밀등급 및 관리번호가 표시되도록 하여야 한다.

⑤사용자는 휴대용 저장매체를 파기 등 불용처리 하거나 비밀용을 일반용 또는 다른 등급의 비밀용으로 전환하여 사용할 경우, 정보보안담당관에게 의뢰하여 완전삭제프로그램을 통해 저장된 정보의 복구가 불가능하도록 조치를 받아야 한다.

⑥사용자는 승인된 보안USB 외에 외장형 저장장치 사용이 필요한 경우 정보보안담당관과 협의하고 별지 제6호 서식에 의거 신청서를 제출하고 USB 관리시스템을 통해 승인을 받아야 한다.

⑦그 밖에 휴대용 저장매체의 보안관리에 관련된 사항은 「USB메모리 등 휴대용 저장매체 보안관리지침」(「국가 정보보안 기본지침부록 5)을 따른다. <2017. 9. 18. 개정·신설>

제28조(악성코드 감염 방지대책) ① 웜·바이러스, 해킹프로그램, 스파이웨어 등 악성코드 감염을 방지하기 위하여 다음 각 호와 같은 대책을 수립·시행하여야 한다.

1. 사용자는 개인PC에서 작성하는 문서·데이터베이스 작성기 등 응용프로그램을 보안패치하고 백신은 최신상태로 업데이트·상시 감시상태로 설정 및 주기적인 점검을 실시
2. 사용자는 출처, 유통경로 및 제작자가 명확하지 않은 응용프로그램 사용을 금지하고 인터넷 등 상용망으로 자료 입수 시 신뢰할 수 있는 인터넷사이트를 활용하되 최신 백신으로 진단 후 사용
3. 사용자는 P2P, 상용 웹하드·메신저 등 업무상 불필요한 프로그램 사용을 금지하고 정보보안담당관은 유해사이트차단시스템을 통해 관련 사이트 접속을 차단하도록 보안 설정
4. 사용자는 웹브라우저를 통해 서명되지 않은(Unsigned) Active-X 등이 PC내에 불법 다운로드 되고 실행되지 않도록 보안 설정
5. 제1호부터 제4호까지의 보안대책과 관련하여 시스템관리자는 정보보안담당관과 협조하여 사용자가 적용할 수 있는 보안기술을 지원

②시스템관리자 또는 PC 등의 사용자는 시스템에 악성코드가 설치되거나 감염된 사실을 발견하였을 경우에 다음 각 호의 조치를 하여야 한다.

1. 악성코드 감염원인 규명 등을 위하여 파일 임의삭제 등 감염 시스템 사용을 중지하고 전산망과의 접속을 분리
2. 악성코드의 감염확산 방지를 위하여 정보보안담당관에게 관련 사실을 즉시 통보 <2017. 9. 18. 개정>

제29조(접근기록 관리) ① 시스템관리자는 정보시스템의 효율적인 통제·관리, 사고 발생 시 추적 등을 위하여 사용자의 정보시스템 접근기록을 유지 관리하여야 한다. <2017. 9. 18. 개정>

② 제1항의 접근기록에는 다음 각 호의 내용이 포함되어야 한다.

1. 접속자, 정보시스템·응용프로그램 등 접속 대상
2. 로그 온·오프, 파일 열람·출력 등 작업 종류, 작업 시간
3. 접속 성공·실패 등 작업 결과
4. 전자우편 사용 등 외부발송 정보 등

③ 시스템관리자는 접근기록을 분석한 결과, 비인가자의 접속 시도, 정보 위변조 및 무단 삭제 등의 의심스러운 활동이나 위반 혐의가 발생한 사실을 발견한 경우 정보보안담당관에게 즉시 보고하여야 한다.

④ 접근기록은 정보보안 사고 발생 시 확인 등을 위하여 최소 6개월 이상 보관하여야 하며 접근기록 위·변조 및 외부유출 방지 대책을 강구하여야 한다.

제30조(정보시스템 개발보안) ① 시스템 개발사업 담당자는 정보시스템을 자체적으로 개발하고자 하는 경우에는 다음 각 호의 사항을 고려하여 보안대책을 수립하고 정보보안담당관의 승인을 받아야 한다. <2017. 9. 18. 개정>

1. 독립된 개발시설을 확보하고 비인가자의 접근 통제
2. 개발시스템과 운영시스템의 물리적 분리
3. 소스코드 관리 및 소프트웨어 보안관리

②시스템 개발사업 담당자는 외부용역 업체와 계약하여 정보시스템을 개발하고자 하는 경우에는 다음 각 호의 사항을 고려하여 보안대책을 수립하고 정보보안담당관의 승인을 득하여야 한다.

1. 외부인력 대상 신원확인, 보안서약서 징구, 보안교육 및 점검

2. 외부인력의 보안준수 사항 확인 및 위반시 배상책임의 계약서 명시
3. 외부인력의 정보시스템 접근권한 및 제공자료 보안대책
4. 외부인력에 의한 장비 반입 · 반출 및 자료 무단반출 여부 확인
5. 제1항 제1호부터 제3호까지의 사항

③정보보안담당관은 제1항 및 제2항과 관련하여 보안대책의 적절성을 수시로 점검하고 정보시스템 개발을 완료한 경우에는 정보보안 요구사항을 충족하는지 시험 및 평가를 수행하여야 한다.

제31조(정보시스템 유지보수) ① 정보시스템 유지보수와 관련한 절차, 주기, 문서화 등에 관련된 사항을 자체 규정에 포함하여야 한다. 유지보수 절차 및 문서화 수립 시 고려사항은 아래의 각 호와 같다. <2017. 9. 18. 개정>

1. 유지보수 인력에 대해 보안서약서 집행, 보안교육 등을 포함한 유지보수 인가 절차를 마련하고 인가된 유지보수 인력만 유지보수에 참여한다.
2. 결함이 의심되거나 발생한 결함, 예방 및 유지보수에 대한 기록을 보관한다.
3. 유지보수를 위하여 원래 설치장소 외 다른 장소로 정보시스템을 이동할 경우, 통제수단을 강구한다.
4. 정보시스템의 유지보수 시에는 일시, 담당자 인적사항, 출입 통제조치, 정비내용 등을 기록·유지하여야 한다.

②시스템관리자는 자체 유지보수 절차에 따라 정기적으로 정보시스템 정비를 실시하고 관련 기록을 보관하여야 한다.

③시스템관리자는 정보시스템의 변경이 발생할 경우, 정보보안담당관과 협조하여 정보시스템의 설계·코딩·테스트·구현과정에서의 보안대책을 강구하며 정보보안담당관은 관련 적절성을 주기적으로 확인하여야 한다.

④정보보안담당관은 시스템관리자 등이 유지보수와 관련된 장비·도구 등을 반출입할 경우, 악성코드 감염여부, 자료 무단반출 여부를 확인하는 등 보안조치 하여야 한다.

⑤시스템관리자는 외부에서 원격으로 정보시스템을 유지보수하는 것을 원칙적으로 금지하여야 하며 부득이한 경우에는 정보보안담당관과 협의하여 자체 보안대책을 강구한 후 한시적으로 허용할 수 있다.

제32조(전자정보 저장매체 불용처리) ① 사용자 및 시스템관리자는 하드디스크 등 전자정보 저장매체를 불용처리(교체·반납·양여·폐기 등) 하고자 할 경우에는 정보보안담당관의 승인 하에 저장매체에 수록된 자료가 유출되지 않도록 보안조치 하여야 한다.

②자료의 삭제는 해당 정보가 복구될 수 없도록 데이터 완전삭제프로그램 또는 장치를 통해 저장매체별, 자료별 차별화된 삭제방법을 적용하여야 한다.

③사용자가 변경된 정보시스템 또는 비밀처리용 정보시스템은 완전포맷 3회 이상, 그 외의 정보시스템은 완전 포멧 1회 이상으로 저장자료를 삭제하여야 한다.

④전자정보 저장매체의 불용처리에 관련된 구체적인 사항은 「정보시스템 저장매체 불용처리지침」(「국가 정보보안 기본지침」부록 6)을 따른다. <2017. 9. 18. 개정>

제3절 주요상황별 보안대책

제33조(무선랜 및 무선인터넷 보안관리) ① 무선랜(와이파이 등) 및 무선인터넷(WiBro, HSDPA 등)을 사용하여 업무자료를 소통하고자 할 경우, 반드시 문화체육관광부 정보화담당관을 통해 국가정보원장에게 보안성 검토를 의뢰하여야 한다.

②정보보안담당관은 청사 전역에 무선인터넷 사용을 제한하고 민원실 등 특별히 무선인터넷 사용이 필요한 구역에 한해 기술적 보안대책을 갖춘 후 기관장 책임하에 운용한다.

③정보보안담당관은 업무용PC에서 무선인터넷 접속장치(USB형 등)가 작동되지 않도록 관련 프로그램 설치 금지 등 기술적 보안대책을 강구하여야 한다.

④정보보안담당관은 개인 휴대폰을 제외한 무선인터넷 단말기의 사무실 무단 반입·사용을 금지하고 수시로 점검하고 보완하여야 한다. <2017. 9. 18. 개정>

제34조(인터넷전화 보안관리) ① 인터넷전화 시스템을 구축하거나 민간 인터넷전화 사업자망(070)을 사용하고자 할 경우에는 사업 계획단계에서 자체 보안대책을 수립 시행하여야 한다.

②시스템관리자는 제1항의 보안대책 수립 시, 다음 각 호의 사항을 포함하여야 한다.

1. 인터넷전화기에 대한 장치 인증 및 사용자 인증
2. 제어신호 및 통화내용의 암호화
3. 인터넷전화망(음성 네트워크)과 일반 전산망(데이터 네트워크)의 분리
4. 인터넷전화 전용 방화벽 등 정보보호시스템
5. 백업체제 구축

③시스템관리자는 인터넷전화 시스템 구축을 위하여 민간 사업자망을 이용할 경우, 해당 사업자로 하여금 서비스 제공 구간에 대한 보안대책을 강구하도록 하여야 한다.

④인터넷전화 구축 시 보안 관리에 관련된 구체적인 사항은 「인터넷전화 구축 시 보안준수사항」(「국가 정보보안 기본지침」 부록 8)을 따른다. <2017. 9. 18. 개정>

제35조(CCTV 시스템 보안관리) ① CCTV 운용에 필요한 카메라, 중계·관제서버, 관리용PC 등 관련 시스템을 비인가자의 임의 조작이 물리적으로 불가능하도록 설치하여야 한다.

②CCTV 상황실은 보호구역으로 지정 관리하고 출입통제장치를 도입하여야 한다.

③시스템관리자는 CCTV 카메라, 비디오서버, 관제서버 및 관련 전산망 설치 시 업무망 및 인터넷망과 분리 운영하는 것을 원칙으로 한다. 다만, 부득이하게 인터넷망을 이용할 경우에는 전송내용을 암호화하여야 한다.

④CCTV 시스템 일체는 사용자계정·비밀번호 등 시스템 인증대책을 강구하고 허용된 특정 IP에서만 접속 허용하는 등 비인가자의 침입 통제대책을 강구하여야 한다.

⑤정보보안담당관은 제1항부터 제4항까지와 관련하여 보안대책의 적절성을 수시로 점검하고 보완하여야 한다.

⑥CCTV 시스템의 보안 관리에 관련된 구체적인 사항은 「CCTV 시스템 보안관리 방안」(「국가 정보보안 기본지침」부록 9)을 따른다. <2017. 9. 18. 개정>

제36조(디지털복사기 보안관리) ① 디지털복사기(이하 "복사기"라 한다)를 임대, 구매 등 도입하고자 할 경우 복사기 저장매체에 보관된 자료유출 방지를 위하여 자료의 완전삭제 기능이 탑재된 제품을 도입하여야 한다. <2017. 9. 18. 개정>

②시스템관리자는 다음 각 호의 경우에 복사기 저장매체의 저장자료를 완전삭제 하여야 한다.

1. 복사기의 사용연한이 경과하여 폐기·양여할 경우
2. 복사기의 무상 보증기간 중 저장매체 또는 복사기 전체를 교체할 경우

3. 고장수리를 위한 외부반출 등 해당 기관이 복사기의 저장매체를 보안 통제할 수 없는 환경으로 이동할 경우

4. 그 밖에 해당 기관에서 저장자료 삭제가 필요하다고 판단하는 경우

③시스템관리자는 복사기의 소모품 등을 교체하기 위한 유지보수 시 정보보안담당자 입회·감독 하에 작업을 실시하여 저장매체 무단 교체 등을 예방하여야 한다.

④정보보안담당관은 저장매체 내장 복사기 현황을 파악하고 복사기의 유지보수 및 불용처리 시 저장매체에 대한 보안조치를 수행하여야 한다.

⑤복사기의 저장자료 삭제방법 등에 관련한 구체적인 사항은 「정보시스템 저장매체 불용처리지침」(「국가 정보보안 기본지침」부록 6)을 따른다.

제37조(첨단 정보통신기기 보안관리) ① 스마트폰, 스마트패드, 태블릿PC 등 첨단 정보통신기기를 사용하여 업무자료 등 중요정보를 소통하고자 할 경우, 반드시 국가정보원장에게 보안성 검토를 의뢰하여야 한다.

②정보보안담당관은 개인이 소지한 첨단 정보통신기기가 업무와 무관하더라도 업무자료 유출에 직·간접 악용될 소지가 있다고 판단될 경우, 반출·반입 통제 등 관련 대책을 강구할 수 있다. <2017. 9. 18. 개정>

제38조(정보통신망 자료 보안관리) ① 다음 각 호에 해당하는 정보통신망 관련 현황·자료 관리에 유의하여야 한다. <2017. 9. 18. 개정>

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

②다음 각 호의 자료를 대외비로 분류하여 관리하여야 한다. 다만, 국가안보와 직결되는 중요한 정보통신망 관련 세부자료는 해당 등급의 비밀로 분류 관리하여야 한다.

1. 정보통신망 세부 구성현황(IP 세부 할당현황 포함)
2. 국가용 보안시스템 운용 현황
3. 보안취약점 분석 · 평가 결과물
4. 그 밖에 보호할 필요가 있는 정보통신망 관련 자료

③제2항에 명시되지 않은 정보통신망 관련 대외비 및 비밀의 분류는 국가정보원장이 제정한 「비밀 세부분류지침」(대외비)을 따른다.

제39조(정보화용역사업 보안관리) ① 정보화·정보보호사업 및 보안컨설팅 수행 등을 외부용역으로 추진할 경우 사업 담당자는 다음 각 호의 사항을 포함한 보안대책을 수립하고 문화체육관광부 정보화담당관에게 보안성 검토를 의뢰하여야 한다. <2017. 9. 18. 개정>

1. 용역사업 계약 시 계약서에 참가직원의 보안준수 사항과 위반 시 손해배상 책임 등 명시
2. 용역사업 수행 관련 보안교육·점검 및 용역기간 중 참여인력 임의교체 금지
3. 정보통신망도·IP현황 등 용역업체에 제공할 자료는 자료 인계인수대장을 비치, 보안조치 후 인계·인수하고 무단 복사 및 외부반출 금지

4. 사업 종료 시 외부업체의 노트북·휴대용 저장매체 등을 통해 비공개 자료가 유출되는 것을 방지하기 위하여 복구가 불가능하도록 완전삭제
5. 용역업체로부터 용역 결과물을 전량 회수하고 비인가자에게 제공·열람 금지
6. 용역업체의 노트북 등 관련 장비를 반출·반입시마다 악성코드 감염여부, 자료 무단반출 여부를 확인

②사업 담당자는 용역사업 추진 시 과업지시서·입찰공고·계약서에 다음 각 호의 누출금지 대상정보를 명시해야하며 해당 정보 누출 시 「국가를 당사자로 하는 계약에 관한법률(이하 "국가계약법"이라 한다) 시행령」제76조 제1항 제18호에 따라 사업 책임자를 부정당업자로 등록하여 입찰 참가자격을 제한하여야 한다. <2017. 9. 18. 개정>

1. 기관 소유 정보시스템의 내·외부 IP주소 현황
2. 세부 정보시스템 구성 현황 및 정보통신망 구성도
3. 사용자계정·비밀번호 등 정보시스템 접근권한 정보
4. 정보통신망 취약점 분석·평가 결과물
5. 정보화 용역사업 결과물 및 관련 프로그램 소스코드(유출시 안보·국익에 피해가 우려되는 중요 용역사업에 해당)
6. 국가용 보안시스템 및 정보보호시스템 도입 현황
7. 침입차단시스템·방지시스템(IPS) 등 정보보호제품 및 라우터·스위치 등 네트워크 장비 설정 정보
8. 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따라 비공개 대상 정보로 분류된 기관의 내부문서
9. 「개인정보보호법」 제2조제1호의 개인정보
10. 「보안업무규정」 제4조의 비밀 및 동 시행규칙 제16조제3항의 대외비
11. 그 밖에 원장이 공개가 불가하다고 판단한 자료

③비밀관련 용역사업을 수행할 경우, 외부인원에 대한 신원조사·비밀취급인가, 보안교육 등 보안조치를 수행하여야 한다.

④정보보안담당관은 제1항부터 제3항까지에서 규정한 보안대책의 시행과 관련한 이행실태를 주기적으로 점검하고 미비점 발견 시 사업 책임자로 하여금 보완토록 조치하여야 한다.

⑤그 밖에 사항에 대하여는 「외부 용역업체 보안관리 방안」(「국가 정보보안 기본지침」부록 7)을 참조한다.

제40조(정보시스템 위탁운영 보안관리) ① 소관 정보시스템에 대한 외부업체의 위탁 운영을 최소화하되, 위탁 운영 필요시 관련 관리적 「보안업무규정」 물리적 「보안업무규정」 기술적 보안대책을 수립하여 시행하여야 한다.

②정보시스템의 위탁 운영은 여타 기관 또는 업체 직원이 해당 기관에 상주하여 수행하는 것을 원칙으로 한다. 다만, 해당 기관에 위탁업무 수행 직원의 상주가 불가한 타당한 사유가 있을 경우, 관련 보안대책을 수립 시행하는 조건으로 그러하지 아니할 수 있다.

③정보시스템의 위탁운영과 관련하여 동 조문에 명시되지 않은 사항에 대해서는 제37조(정보화용역사업 보안관리)를 준용한다. <2017. 9. 18. 개정>

제4절 보안성 검토

제41조(보안성 검토 신청) ① 다음 각 호의 정보화사업을 추진할 경우에 대하여 자체 보안대책을 강구하고 안전성을 확인하기 위하여 사업 계획단계(사업 공고 전)에서 문화체육관광부 정보화담당관을 통해 국가정보원장에게 보안성 검토를 의뢰하여야 한다. <2017. 9. 18. 개정>

1. 정보통신망을 신·증설하거나 서버 등 정보통신시스템을 교체하는 경우
2. 내부 정보통신망을 외부망과 연결하고자 하는 경우
3. 정보보안 관련법규를 제정 또는 개정하고자 할 경우
4. 국가용 보안시스템 또는 검증 필 정보보호시스템을 도입 운용하고자 할 경우
5. 외부기관 및 업체의 보안감리 또는 보안컨설팅(보안취약성 분석·평가 포함)을 받거나 정보처리·보안관제 등의 업무를 위탁할 경우
6. 무선랜 등 무선망을 사용하여 업무를 처리하거나 원격근무 지원들을 위해 시스템을 도입하는 경우
7. 그 밖에 정보통신 운용환경 변화로 인하여 보안성 검토가 필요하다고 인정되는 경우

②보안성 검토 대상 정보화사업에 관련된 구체적인 사항은 「정보화사업 보안성 검토 처리기준」(「국가 정보보안 기본지침」부록2)을 참조한다.

제42조(제출 문서) ① 정보화사업 보안성 검토를 요청할 경우에는 다음 각 호의 문서를 제출하여야 한다. <2017. 9. 18. 개정>

1. 사업계획서(사업목적 및 추진계획 포함)
2. 기술제안요청서(RFP)
3. 정보통신망 구성도(필요시, IP주소체계 추가)
4. 자체 보안대책 강구사항

②제1항 제4호의 자체 보안대책 강구사항에는 다음 각 호를 포함하여야 한다.

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

제43조(결과 조치) 국가정보원장의 보안성 검토 결과를 준수하여 보안대책을 보완하여야 한다. 이 경우, 국가정보원장이 보안성 검토 결과 신속한 시정이 필요하다고 판단하는 경우에는 필요한 조치를 요청할 수 있으며 원장은 특별한 사유가 없는 한 이에 따라야 한다. <2017. 9. 18. 개정>

제44조(정보보호시스템의 도입 등) 정보 및 정보통신망 등을 보호하기 위해 정보보호시스템을 도입할 수 있다. 다만, 별표 2에 규정된 유형의 시스템에 대해서는 해당 도입요건을 만족하는 경우로 한정한다. <2017. 9. 18. 개정>