# 정 보 보 안 지 침

제정 2012. 8.22
개정 2013. 7.24 시행 2013. 7.26
개정 2015. 3.30 시행 2015. 3.31
개정 2016. 3.28 시행 2016. 3.31
개정 2017. 7.31 시행 2017. 8. 1
개정 2019. 5.15 시행 2019. 5.16
개정 2020.12.30 시행 2020.12.31
개정 2023. 6.19 시행 2023. 6.21

## 제 1 장 총 칙

제1조(목적) 이 지침은 국가정보원 「국가 정보보안 기본지침」, 방송통신위원회 「정보보호 관리지침」, 보안업무관리규정 등에 따라 한국방송광고진흥공사(이하 “공사”라 한다.)가 수행하여야 할 정보보안 기본활동 규정을 목적으로 한다. <개정 2016.3.31.>

제2조(적용범위) 이 지침은 공사의 전 임직원(계약직 포함), 외부용역업체 직원에게 적용한다.

제3조(정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다. <개정 2015.3.31.><개정 2016.3.31.>

1. “정보통신망”이라 함은 「전기통신기본법」 제2조 제2호의 규정에 따른 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송수신하는 정보 통신체제를 말한다.

2. “정보시스템”이라 함은 서버·PC 등 단말기, 보조기억매체, 전산·통신장치, 정보통신 기기, 응용프로그램 등 정보의 수집·가공·저장·검색·송수신에 필요한 하드웨어 및 소프트웨어를 일체를 말한다.

3. “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.

4. “전자문서”라 함은 컴퓨터 등 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 정보를 말한다.

5. “전자기록물”이라 함은 정보처리능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 기록정보자료를 말한다.

6. “전자정보”라 함은 업무와 관련하여 취급하는 전자문서 및 전자기록물을 말한다.

7. “정보보호시스템”이라 함은 정보의 수집·저장·검색·송신·수신시 정보의 유출, 위·변조, 훼손 등을 방지하기 위한 하드웨어 및 소프트웨어를 말한다.

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

9. “저장매체”라 함은 자기저장장치·광 저장장치·반도체 저장장치 등 자료기록이 가능한 전자장치를 말한다.

10. “취약점 점검”이라 함은 해킹·컴퓨터바이러스, 도청 등 각종 위협요소로부터 정보통신망 및 정보시스템에 대한 정보보안 취약점을 진단하기 위한 제반활동을 말한다.

11. “IP(Internet Protocol)주소”라 함은 정보통신망으로 서버와 클라이언트간 연결을 가능하게 하기 위하여 부여되는 주소체계를 말한다.

12. “사용자 계정(ID)”이라 함은 이용자의 식별과 자료이용을 위하여 이용자가 생성한 영문자와 숫자가 조합된 고유계정을 말한다.

13. “휴대용 저장매체”라 함은 디스켓·CD·외장형 하드디스크·USB 메모리 등 정보를 저장할 수 있는 것으로 PC 등의 정보시스템과 분리할 수 있는 기억장치를 말한다.

14. “정보통신실”이라 함은 서버·PC등과 스위치·교환기·라우터 등 네트워크 장치 등이 설치 운용되는 장소를 말하며, 전산실·통신실·전자문서 및 전자기록물(전자정보) 보관실 등을 말한다.

15. “전산자료”라 함은 전산장비에 의하여 전자기적인 형태로 입력·보관 되어 있는 각종 정보 및 데이터를 말하며, 그 자료가 입력되어있는 자기테이프, 디스크 등 보조기억매체를 포함한다.

16. “소자(消磁)”라 함은 저장매체에 역자기장을 이용해 매체의 자화값을 “0”으로 만들어 저장자료의 복원이 불가능하게 만드는 것을 말한다.

17. “완전삭제”라 함은 저장매체 전체의 자료저장 위치에 새로운

자료(0 또는 1)를 중복하여 저장하는 것을 말한다.

18. “국가용 보안시스템”이라 함은 비밀 등 중요자료 보호를 위하여 국가정보원장이 개발하거나 안전성을 검증한 암호장비·보안자재·암호논리 등을 말한다.

19. “보안관제”라 함은 정보보호시스템에서 탐지된 공격 및 침입정보를 종합·분석하여 침해사고에 대한 예방 및 대응 업무를 수행하는 것을 말한다.

## 제 2 장 정보보안 기본활동

제4조(책무) ①공사 사장은(이하 “사장”이라 한다)은 공사의 정보통신망 및 정보자산 등을 보호하기 위한 보안대책을 마련하여야 하며, 정보보안에 대한 책임을 진다.

②사장은 정보보안 조직을 지휘하고 소속 및 공사에 대한 정보보안 업무를 총괄하기 위하여 ‘정보보안책임자’ 및 ‘정보보안담당관’을 임명하여야 한다. <개정 2016.3.31.>

③사장은 정보보호를 위하여 다음 각 호에 해당하는 업무를 전담할 정보보안 담당관을 임명하여야 한다. 이 경우 「정보통신기반 보호법 시행령」 제9조 제1항에 따라 지정한 정보보안책임자를 정보보안담당관으로 임명할 수 있다. <개정 2019.5.15.><개정 2023.6.19.>

1. 정보보안 정책・계획의 수립・시행 및 정보보안내규 제・개정

2. 정보보안 지사 지도점검 실시

3. 정보통신망 보안대책 수립·시행

4. 정보보호 위규 적발 강화 및 사고조사 처리

5. 보안관제, 사고대응 및 정보협력 업무 총괄

6. 정보보안 관련 규정·지침 등 제·개정

7. 정보보안 교육계획 수립·시행

8. 정보보안업무 심사분석 시행

9. 정보보안 전담조직 관리, 전문인력 및 관련예산 확보

10. 정보화사업 보안성 검토 및 보안적합성 검증 총괄

11. 해당 기관 및 관할 하급기관에 대한 정보보안 지도방문 관리 감독

12. 부서 분임정보보안담당관 업무 감독

13. 사이버공격 대응훈련 및 정보보안 관리실태 평가 총괄

14. 그 밖에 정보보안 관련 사항

제5조(정보보안 조직의 구성 및 역할) ①정보보안조직은 정보보안책임자, 정보보안담당관, 정보보안담당자, 부서별 정보보안담당자로 구성한다. <개정 2015.3.31.> <개정 2016.3.31.>

②정보보안책임자는 소관 본부장으로 하며, 전사적 정보보안에 관한 업무를 총괄·관리한다. <개정 2016.3.31.>

③정보보안담당관은 정보보안업무를 추진하는 부서의 장으로 하며,

정보보안 기획, 관리 및 운영 실무를 총괄하고 정보보안 활동을 감독·관리한다. <개정 2019.5.15.>

④정보보안담당자는 정보보안업무를 추진하는 부서의 부서원으로 하며, 정보보안담당관과 협력하여 정보보안 기획, 관리, 운영 실무를 담당하고 정보보안 지침 및 기준에 따라 관리, 운영, 교육 및 점검 활동을 수행한다. <개정 2015.3.31.> <개정 2019.5.15.>

⑤부서별 정보보안담당자는 각 부서의 부서원으로 하며, 부서별 정보보안업무를 수행한다. <개정 2015.3.31.> <개정 2019.5.15.>

⑥그 외 정보보안 조직의 구성 및 역할에 대한 세부사항은 “정보보안 직무기술서”를 따른다. <개정 2016.3.31.>

제6조(정보보안 업무 추진 계획 수립) ① 사장은 정보보안 업무 추진 계획을 수립 및 시행한다. <개정 2019.5.15.>

② <삭제 2019.5.15.>

[본조제목개정 2019.5.15.]

제7조(정보보안 교육) ①사장은 다음과 같이 정보보안에 대한 교육계획(외부전문기관 위탁교육 포함)을 수립·시행하여야 하며, 공사 실정에 맞는 교육자료를 작성 활용해야 한다. <개정 2019.5.15.>

1. 전 직원대상 교육 : 연 1회 이상
2. 부서별 정보보안 담당자 교육 : 연 1회 이상
3. 외부 용역업체 직원 교육 : 연 1회 이상
4. 정보화 사업 담당자 교육 : 연 1회 이상

②정보보안 교육에 대한 세부사항은 “年度 정보보안 교육계획”에서 규정한 내용을 따른다. <개정 2016.3.31.>

③ <삭제 2015.3.31.>

④ <삭제 2016.3.31.>

제8조(정보통신망 현황·자료 관리) ①사장은 다음 각 호에 해당하는 자료를 「공공기관의 정보공개에 관한 법률」제9조 제1항에 따른 비공개 대상 정보로 지정·관리하여야 한다. <개정 2019.5.15.>

1. 정보시스템 운용현황
2. 정보통신망 구성현황
3. IP 할당현황
4. 주요 정보화사업 추진현황
5. 취약점 분석·평가 결과물(「정보통신기반 보호법」 제9조에 따른 취약점 분석·평가결과를 포함한다)

② <삭제 2019.5.15.>

제9조(정보통신실 보안관리) 사장은 정보통신실을 운용 시 다음 각 호에 정하는 보호대책을 강구하여야 한다.

1. 외부로부터의 위험에 대한 방지 및 방재 대책
2. 단일 출입문을 정하고 이중 잠금장치 설치
3. 자료·장비별 관리책임자 지정 운용
4. 비인가자에 대한 출입 및 정보자산 반출·입 통제
5. 정전에 대비한 비상 전원공급 등 전력관리 대책

6. 카메라 장착 휴대폰 등을 이용한 불법 촬영 방지대책 등

7. 출입자 식별·인증 등을 위한 출입문 보안장치 설치 및 주·야간 감시대책 <개정 2019.5.15.>

8. 휴대용 저장매체를 보관할 수 있는 용기 비치 <개정 2019.5.15.>

9. 정보시스템의 안전지출 및 긴급파기 계획 수립 <개정 2019.5.15.>

10. 비상조명 장치 등 비상탈출 대책 <개정 2019.5.15.>

제10조 <삭제 2016.3.31.>

## 제 3 장 정보시스템 보안관리

제11조(정보시스템 및 정보보호시스템 보안관리) ①사장은 정보시스템 및 정보보호시스템(이하 '시스템'이라 한다)의 효율적인 보안관리를 위하여 시스템별로 관리책임자(이하 '시스템관리자'라 한다)를 지정 운영하여야 한다.

②시스템관리자는 각종 서버·네트워크 장비·침입차단장치 등 시스템이 비인가자에게 허용되지 않도록 보안기능을 설정하여야 한다.

③시스템관리자는 소관 시스템의 안정적 운영을 위해 다음 각 호에 따라 관리해야 한다.

1. 시스템의 운영체제 등 보안 권고 또는 취약점 관련 패치 실행

2. 신규·설치·운영 중인 시스템의 수시 보안취약점 점검 및 조치

3. 접속 기록 및 접근자료 관리

4. 불필요한 서비스 및 계정(세션 타임아웃 기능 포함) 관리

5. 접근권한 차등부여, 권한 관리

④시스템관리자가 비인가자의 시스템 침입사실을 인지한 경우에는 시스템 보호를 위한 접속차단 등 초동조치를 취하고 지체 없이 정보보안담당관에게 보고하여야 한다.

⑤정보보안담당관은 시스템에 대하여 외부업체의 원격 유지보수 작업을 허용하여서는 아니 된다. 다만, 부득이한 경우에는 필요한 보안대책을 강구한 후 허용할 수 있으며, 이때에도 원격 유지보수 내용을 확인·감독하고 기록하여야 한다.

[본조전부개정 2015.3.31.]

제12조(웹서버 등 공개서버 관리) ①사장은 외부인에게 공개할 목적으로 설치되는 웹서버 등 각종 공개서버는 내부망과 분리된 영역(DMZ)에서 운영하고 보안적합성이 검증된 침입차단·탐지 시스템을 설치하는 등 보안대책을 강구하여야 한다.

②공개서버에 접근할 수 있는 사용자 계정을 제한하여야 하며 불필요한 계정은 삭제하여야 한다.

③공개서버에 비공개 자료 및 개인정보가 유·노출, 위·변조 되지 않도록 보안조치를 하여야 한다.

④공개서버의 서비스에 필요한 프로그램을 개발하고 시험하기 위해 사용된 도구(컴파일러 등)는 개발 완료 후 사용이 제한되도록 보안기능을 설정하거나 삭제하여야 한다.

⑤공개서버의 보안취약점을 수시로 점검하고, 자료의 위·변조, 훼손 여부를 확인하여야 한다.

[본조전부개정 2015.3.31.]

제13조(사용자 계정관리) ①시스템 관리자는 사용자 계정(ID)의 비인가자 도용 및 정보시스템 불법접속에 대비하여 다음 각 호의 사항을 반영하여 관리하여야 한다. <개정 2015.3.31.>

1. 사용자별 또는 그룹별로 접근 권한 부여, 사용자 계정을 공동으로 사용 금지

2. 외부 사용자의 계정부여는 불허하되 부득이한 경우에는 정보보안담당관 책임 하에 유효기간을 설정하는 등 보안조치 후 허용

3. 비밀번호가 없는 사용자 계정은 사용 금지

4. 5회에 걸쳐 사용자 인증에 실패할 경우 정보시스템 접속을 중지시키고, 비인가자 침입여부 확인 점검

5. 퇴직 또는 보직변경 등으로 사용자 계정을 해지해야할 때에는 신속히 삭제

②정보시스템의 계정은 사용목적 및 권한에 따라 관리자 계정과 사용자 계정으로 분류하여 관리하여야 한다. <개정 2015.3.31.>

③시스템관리자는 정보시스템별로 계정발급현황을 현행화하여 관리해야한다. <개정 2015.3.31.>

④정보시스템관리자는 개별사용자의 보직변경, 퇴진, 계약종료 등 변동사항이 발생할 경우 신속히 사용자 계정을 삭제하거나 부여된

접근권한을 회수하여야 한다. <신설 2019.5.15.>

⑤정보시스템관리자는 사용자 계정 부여 및 관리의 적절성을 연 2회 이상 점검하고 그 결과를 정보보안담당관에게 통보하여야 한다. <신설 2019.5.15.>

⑥정보시스템관리자는 계정에 대한 접근권한 부여, 변경, 회수 또는 삭제 등에 대한 내역을 기록하고 3년 이상 보관하여야 한다. <신설 2019.5.15.>

제14조(비밀번호 관리) ①비밀이나 중요자료를 파일로 보관 시 반드시 자료별 비밀번호를 부여하여야 한다.

②비밀번호는 다음 각 호 사항을 반영하여 숫자와 문자, 특수문자 등으로 9자리 이상으로 정하고 분기1회 이상 주기적으로 변경 사용하여야 한다.

1. 사용자 계정(ID)과 동일하지 않은 것
2. 개인 신상 및 부서명칭 등과 관계가 없는 것
3. 사전에 등록된 단어 또는 추측하기 쉬운 단어는 사용하지 말 것
4. 직전에 사용된 비밀번호는 재사용하지 말 것
5. 패스워드의 전달 시 팩스, 전자우편을 사용하지 말 것
6. 패스워드의 입력 횟수는 최대 5회로 제한
7. 동일 비밀번호를 여러 사람이 공유하여 사용하지 말 것
8. 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용금지

③서버에 등록된 비밀번호는 암호화하여 저장하여야 하며, 비밀번호

는 대외비 이상으로 분류 관리하고, 주기적으로 비밀관리 점검을 실시한다.

④사용하는 모든 비밀번호에 대하여 비밀을 유지해야 하며, 타인에게 고의로 비밀번호 정보를 제공하거나 노출시켜서는 아니 된다.

⑤비밀번호가 노출되었거나 노출이 의심되는 경우, 비밀번호를 즉시 변경하여야 한다.

⑥정보보안담당관은 정보시스템에서 개별사용자를 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. <신설 2019.5.15.>

제15조(정보통신망 보안관리) ①사장은 내부 정보통신망을 외부 정보통신망에 연결하고자 하는 경우에 보안관리 책임한계 설정, 전자정보의 제공범위 및 이용자 접근제한 등 정보통신망 보안대책을 수립・시행하여야 한다.

②사장은 정보통신망을 상용망이나 다른 기관과 정보통신망을 연계하기 위한 보안관리 연결지점을 운용할 경우에는 비인가자의 무단 침입(불법접속)이나 악성코드 및 사이버공격을 방지하기 위하여 국가정보원장이 검증한 보안시스템의 설치・운용 등 보안대책을 강구하여야 한다.

③사장은 정보통신망 및 정보시스템에 사용되는 “IP주소”를 체계적

으로 관리하여야 한다. 이 경우에 내부 정보시스템을 보호하기 위하여 사설주소체계(NAT : Network Address Translation)를 사용한다.

④사장은 인터넷을 통한 불법 사이트 접속이나 프로그램 다운로드를 금지하여야 하며, 서버의 자원(폴더,파일 등)에 대한 공유는 업무상 또는 운영상 필요한 경우에만 제한하여 사용토록 하고 통제대책을 강구하여야 한다.

[본조전부개정 2015.3.31.]

제16조(전자우편 등 보안관리) ①사장은 웜·바이러스 등 악성코드로부터 사용자 PC 등 전자우편 시스템 일체를 보호하기 위하여 백신, 바이러스 월, 해킹메일 차단시스템 구축 등 보안대책을 강구하여야 한다.

②사장은 수신된 전자우편의 발신지 IP주소와 국가명이 표시되고 해킹메일 원본을 신고할 수 있는 기능을 갖춘 웹메일시스템을 구축하여야한다.

③사용자는 상용 전자우편을 이용한 업무자료 송·수신을 금지하며 사내 전자우편으로 송·수신한 중요 업무자료는 열람 등 활용 후 메일함에서 삭제하여야 한다.

④사용자는 출처가 불분명하거나 의심되는 제목의 전자우편은 열람을 금지하고 해킹메일로 의심되는 메일 수신시에는 즉시 정보보안담당자에게 신고하여 필요한 조치를 받아야 한다.

[본조전부개정 2015.3.31.]

제17조(CCTV 시스템 보안관리) ①사장은 CCTV 운용에 필요한 카메라, 관리용 PC 등 관련 시스템을 비인가자의 임의조작이 물리적으로 불가능하도록 설치하여야 한다.

②CCTV 상황실은 보호구역으로 지정 관리하고 출입통제장치를 도입하여야 한다.

③시스템 관리자는 CCTV 카메라, 비디오서버, 관제서버 및 관련 전산망을 설치할 경우 업무망 및 인터넷망과 분리 운영하는 것을 원칙으로 한다.

④CCTV 시스템 일체는 사용자 계정·비밀번호 등 시스템 인증대책을 강구하고 허용된 특정 IP에서만 접속을 허용하는 등 비인가자의 침입에 대비한 통제 대책을 강구하여야 한다.

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

[본조전부개정 2015.3.31.]

제18조(스마트폰 등 모바일 업무 보안관리) ①사장은 스마트폰 등을 활용하여 모바일 업무환경을 구축할 경우 보안대책을 수립·시행하여야 한다.

②기타 상세한 사항은 「국가·공공기관 모바일 활용업무에 대한 보안가이드라인」(국가정보원)을 준수하여야 한다.

[본조전부개정 2015.3.31.]

제19조(악성코드 감염 방지대책) ①사장은 웜·바이러스, 해킹프로그램, 스파이웨어 등 악성코드 감염을 방지하기 위하여 다음 각 호와 같은 대책을 수립·시행하여야 한다. <개정 2016.3.31.>

1. 사용자는 출처, 유통경로 및 제작자가 명확하지 않은 응용프로그램은 사용을 금지하고 불가피한 경우에는 백신 등 관련 프로그램을 사용할 수 없으며 인터넷 등 상용망으로 자료 입수시 신뢰할 수 있는 인터넷사이트를 활용하되 최신 백신으로 진단 후 사용하여야 한다.

2. 사용자는 인터넷 파일공유 프로그램과 업무상 불필요한 프로그램의 사용을 금지하고 시스템관리자는 인터넷 연동구간의 침입차단시스템 등에서 관련 사이트 접속을 차단하도록 보안설정하여야한다.

3. 사용자는 웹브라우저를 통해 서명되지 않은 Active-X 등이 PC내에 불법 다운로드 되고 실행되지 않도록 보안설정 하여야 한다.

4. 사용자는 개인PC에서 작성하는 문서·데이터베이스 작성기 등 응용프로그램을 보안패치하고 백신은 최신상태로 업데이트·상시 감시상태로 설정 및 주기적인 점검을 실시하여야 한다.

②시스템관리자 또는 PC 등의 사용자는 시스템에 악성코드가 설치되거나 감염된 사실을 발견하였을 경우에 다음 각 호의 조치를 하여야 한다. <개정 2016.3.31.>

1. 악성코드 감염 원인 규명 등을 위하여 파일 임의삭제 등 감염시스템 사용을 중지하고 전산망과의 접속을 분리

2. 악성코드의 감염확산 방지를 위하여 정보보안담당관에게 관련 사실을 즉시 통보

3. <삭제 2016.3.31.>

4. <삭제 2016.3.31.>

③사장은 악성코드가 신종이거나 감염피해가 심각하다고 판단될 경우에는 관련사항을 상급기관에게 신속히 보고하고 필요한 조치를 수행하여야 한다. <개정 2016.3.31.>

④사장은 상급기관이 악성코드 감염사실을 확인하여 조치를 권고할 경우, 즉시 이행하여야 한다. <신설 2016.3.31.>

[본조전부개정 2015.3.31.]

제20조(백업관리) ①서버 장애 및 데이터 파손으로 인한 피해를 최소화하고 조속한 복구를 위해 가동 및 복구에 필요한 데이터를 주기적으로 다른 매체에 백업하여 보관한다.

②서버의 특성과 신속한 데이터 복구를 고려한 백업을 수행해야 한다.

③주기적으로 백업 매체의 상태를 점검한다.

④본 절에 명시되지 않은 서버 보안에 대한 세부사항은 “서버보안 가이드라인”을 따른다. <개정 2016.3.31.>

제21조(네트워크 보안정책) ①공사 내 네트워크의 접속관리 정책은 다음 각 호와 같다.

1. 외부로부터 공사 내 네트워크에는 비인가자가 접속할 수 없도록

네트워크 장비를 설정하여 운영한다.

2. 안전이 보장되지 않은 외부 네트워크로부터 시스템 및 네트워크 자원의 관리를 위해 접속하는 것은 원칙적으로 금지한다. 단, 필요한 경우 정보보안담당관의 승인을 득한 후 접속할 수 있다.

3. 허가되지 않은 사용자의 LAN포트 사용을 금지한다.

②공사 내 네트워크 원격 접속 관리정책은 다음 각 호와 같다.

1. 공사 내 네트워크로의 원격 접속이 필요한 사용자는 분임정보보안담당자의 승인을 득하여야 한다.

2. 분임정보보안담당자는 원격 접속의 보안관리를 위해 역 호출(Call back) 기능 등 강화된 사용자 인증 제도를 시행할 수 있다.

③외부 네트워크로의 접속관리 정책은 다음 각 호와 같다.

1. 외부 네트워크로의 연결이 필요한 경우 분임정보보안담당자는 정보보안담당관의 승인을 득한 후 행한다.

2. 인터넷 등 공중망으로의 연결을 위해서는 접점에 침입차단시스템을 설치하여 비인가자의 접근을 차단할 수 있도록 조치를 취해야 하며, 침입탐지 시스템을 이용하여 외부로 부터의 침입여부를 실시간으로 모니터링 할 수 있다.

④공사 내의 네트워크에서 승인되지 않은 프로토콜을 사용하여서는 안된다.

⑤공사의 네트워크를 사용하는 모든 사용자는 내부 서버에 임의로 비공식적인 인터넷 홈페이지의 구축을 하여서는 안된다.

⑥IP 주소의 체계적인 관리 규정은 다음 각 호와 같다.

1. IP 주소의 사용은 다음 사항을 따른다.

가. 공용 IP 주소는 외부 접점 등 특정한 노드에만 사용하며, 공용 IP 주소의 사용은 분임정보보안담당자의 승인을 득한 후 사용한다.

나. 내부 네트워크에서는 사설 IP 주소를 사용하는 것을 원칙으로 하며, 사용 시에는 고정 IP 주소를 부여한다.

다. 사용자는 IP 주소를 2개 이상 사용할 필요가 있을 경우 분임정보보안담당자의 승인을 득한 후 사용한다.

2. 사용자는 인사이동, 퇴사 등으로 인하여 네트워크 자원을 더 이상 사용하지 않는 경우 사용한 IP 주소를 네트워크 관리자에게 반납한다.

제22조(접근기록 관리) ①시스템관리자는 주기적으로 보안도구를 이용하여 정보시스템의 보안취약점을 진단하여야 하며, 정보시스템의 효율적인 통제, 관리, 사고발생시 추적을 위하여 다음 각 호의 사용자 접근기록을 유지 관리하여야 한다.

1. 접속자, 접속 일시, 정보시스템·응용프로그램 등 접속 대상

2. 로그 온·오프, 파일 열람·출력 등 작업 종류, 작업 시간

3. 작업 성공·실패 등 작업결과

4. 전자우편 사용 등 외부발송 정보 등

②시스템 관리자는 정보보안 사고 발생시 확인 등을 위하여 접근기록을 6개월 이상 유지하여야 하고 접근기록 위·변조 및 외부유출 방

지 대책을 강구하여야한다.

[본조전부개정 2015.3.31.]

제23조(사이버보안 진단의 날 운영) ①사장은 매월 셋째주 수요일을 ‘사이버보안 진단의 날’로 지정·운영하여야 한다.

②사장은 ‘사이버보안 진단의 날’에 소관 정보통신망을 대상으로 악성코드 감염여부와 정보시스템의 보안 취약여부 등을 진단하고 문제점을 발굴 개선하여야 한다.

[본조전부개정 2015.3.31.]

제24조(보안성 검토) ①정보화사업담당관은 정보화사업을 수행하고자 할 경우 정보화사업과 관련한 보안대책의 적절성을 평가하기 위하여 사업 계획단계(사업 공고 전)에서 보안성 검토를 받아 사업계약에 반영해야 한다. <개정 2019.5.15.><개정 2020.12.30.>

② <삭제 2019.5.15.>

③정보화사업담당관은 제1항에 따른 보안성 검토를 정보보안담당관에게 의뢰하여야한다. 정보보안담당관은 제24조의2 제1항 및 제24조의2 제2항에 따른 보안성 검토 기관의 장에게 검토를 의뢰하거나 자체적으로 실시하여야 한다. 제24조의2 제1항 각 호에 해당하는 정보화사업에 대하여 국가정보원장에게 보안성 검토를 의뢰하고자 할 경우 관계 상급기관의 장을 거쳐 의뢰하여야 한다. <신설 2019.5.15.> <개정 2020.12.30.>

④보안성 검토는 서면 검토를 원칙으로 하며 보안성 검토 기관의

장이 필요하다고 판단하는 경우 현장 확인을 병행 실시할 수 있다. <신설 2019.5.15.>

⑤정보화사업에 대한 보안성 검토 의뢰 절차는 「정보화사업 보안 가이드라인」에 따른다. <신설 2020.12.30.>

[본조전부개정 2015.3.31.]

제24조의2(검토 기관) ①사장은 다음 각 호에 해당하는 정보화 사업에 대하여 국가정보원장에 의뢰하여 보안성 검토를 실시한다. 다만, 정보화사업의 규모·중요도 등을 고려하여 국가정보원장과 협의 후 방송통신위원회에 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 또는 정보시스템 구축

4. 100만명 이상의 개인에 대한 「개인정보보호법」상 민감정보 또는 고유식별정보를 처리하는 정보시스템 구축

5. 주요정보통신기반시설로 지정이 필요한 정보통신기반시설 구축

6. 제어시스템 도입(SCADA)

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, 국제회의 등 국제행사를 위한 정보통신망 또는 정보시스템 구축

11. 내부망 또는 폐쇄망을 인터넷 또는 다른 정보통신망과 연동하는 사업

12. 내부망과 기관 인터넷망을 분리하는 사업

13. 통합데이터센터·보안관제센터 구축

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

15. 원격근무시스템 구축

16. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제20조에 따라 클라우드컴퓨팅서비스제공자의 클라우드컴퓨팅서비스(이하 “민간 클라우드컴퓨팅서비스”라 한다)를 이용하는 사업

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

18. 외국에 개설하는 사무소 운영을 위한 정보통신망 또는 정보시스템 구축

19. 첨단 정보통신기술을 활용하는 정보화사업으로서 국가정보원장

이 해당 기술에 대하여 안전성 확인이 필요하다고 지정하는 사업

②사장은 다음 각 호에 해당하는 정보화 사업에 대하여 방송통신위원회에 의뢰하여 보안성 검토를 실시한다. 다만, 제10호부터 제14호까지에 해당하는 정보화사업에 대한 보안성검토는 방송통신위원회와 협의 후 자체적으로 실시 할 수 있다.

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 연동하여 정보의 소통 또는 서비스를 제공하는 정보시스템 구축

5. 공사의 정보통신망 또는 정보시스템과 분리된 외부인 전용(專用) 무선랜, 인터넷망 및 교육장 정보통신망 등 구축

6. 인터넷과 분리된 소속 공문원등의 인사·복지관리 등 의 목적을 위한 정보시스템 구축

7. 주요정보통신기반시설 취약점 분석·평가, 정보보안컨설팅 등 용역사업

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

9. 대규모 백업·재해복구센터 구축

10. 해당 기관의 정보통신망 또는 정보시스템과 분리된 영상회의시

스템 구축

11. 인터넷과 분리된 CCTV 등 영상정보처리기기 구축

12. 백업시스템 구축

13. 대민(對民) 콜센터시스템 구축

14. 기타 사장이 필요하다고 판단하는 정보통신망 또는 정보시스템 구축

[본조신설 2019.5.15.]

제24조의3(검토 생략) ①정보화사업담당관은 다음 각 호에 해당하는 정보화사업에 대하여는 보안성 검토 절차의 이행을 생략할 수 있다. 이 경우 정보화사업담당관은 관련 매뉴얼·가이드라인 등을 준수하는 등 자체 보안대책을 수립·시행하여야 하며, 이를 정보보안담당관에게 알려야한다. <개정 2020.12.30.>

1. 제24조의2 제1항 및 제2항 각 호의 정보화사업에 해당하지 아니하는 단순 장비·물품 도입

2. 제24조에 따른 보안성 검토를 거쳐 완료한 정보화사업에 대하여 정보통신망 구성을 변경하지 아니하는 범위 내에서 다음 각 목의 사항을 포함한 후속 운영·유지보수·컨설팅(단일 회선의 이중화는 본 호를 적용함에 있어 정보통신망 구성의 변경이 아닌 것으로 본다)

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 계속되는 사업으로 사업 착수 당시 보안성검토를 완료 한 후 사업 내용의 변동 없이 계속 추진하는 운영·유지 사업

4. PC·프린터 및 사용 소프트웨어 등 단순 제품 교체

5. 회계규정 제96조제1항에 해당하는 사업

②사장은 제1항 제2호부터 제4호까지에 해당하는 정보화사업을 수행할 경우 기존 보안성 검토결과를 준수하여야 한다.

③제1항에도 불구하고, 정보보안담당관은 정보시스템의 안전한 운영을 위해 필요시 정보화사업당관에게 보안성 검토 이행을 요구할 수 있으며, 이 경우 정보화사업당관은 제24조의 보안성검토를 생략할 수 없다. <신설 2020.12.30.>

[본조신설 2019.5.15.]

제24조의4(제출 문서) 사장은 제24조 제3항에 따라 보안성 검토를 의뢰할 경우 다음 각 호의 사항이 포함된 문서를 제출하여야 한다.

1. 사업계획서(사업목적 및 추진계획을 포함한다)

2. 제안요청서

3. 정보통신망 구성도(필요시 IP주소체계를 추가한다)

4. 자체보안대책

[본조신설 2019.5.15.]

제24조의5(검토결과 조치) ①사장은 제24조의2에 따라 보안성 검토결

과를 통보받은 경우 검토결과를 반영하여 보안대책을 보완하여야 한다.

②보안성 검토 기관의 장은 제1항에 따른 보안성 검토결과 반영여부를 확인하기 위하여 현장 점검을 실시할 수 있다.

[본조신설 2019.5.15.]

제24조의6(현황 제출) 사장은 공사의 정보화사업에 대한 보안성 검토결과 현황을 매년 1.25까지 국가정보원장에게 제출하여야 한다.

[본조신설 2019.5.15.]

제25조(정보보호시스템의 설치 및 구성) ①국가정보원장이 국가기관용으로 보안적합성을 검증한 정보보호시스템을 설치하여 사용한다.

②침입차단시스템의 운영은 다음 각 호의 절차를 준수한다.

1. 인터넷 등 모든 공동망 및 대외 망과의 접점에는 침입차단시스템을 사용하여 비인가 접속을 차단하여야 한다.

2. 침입차단시스템은 원칙적으로 어플리케이션 레벨의 침입차단시스템을 사용한다. 단, 정보보안담당관의 승인을 득한 경우 라우터의 패킷 필터링 기능 등을 사용하여 침입차단시스템을 대신할 수 있다.

3. 침입차단시스템은 침입차단을 위한 고유 목적 이외의 다른 서비스 제공을 위해 사용되어서는 안된다.

4. 콘솔에 물리적으로 접근할 수 있는 사용자는 침입차단시스템 담당자로 제한한다.

5. 침입차단시스템에 직접 접근할 수 있는 사용자는 최소한의 인원

으로 제한하며, 직접 접근할 수 있는 호스트를 지정 및 최소화한다.

6. 원격 관리는 공사 내부 네트워크에서만 가능하며, 인터넷 등의 외부 네트워크를 통한 원격 관리는 금한다.

7. 침입차단시스템 관리자는 시스템 자체에 대한 침해를 예방하기 위하여 시스템 자체 운영체제의 보안 취약점을 보완 및 관리하여야 한다.

8. 정보보안담당관은 침입탐지시스템 설치 시 네트워크 부하 증가 등을 고려하여 미리 로드밸런싱 하는 방안을 강구하여 일정수준 이상의 네트워크 성능을 유지하도록 하여야 한다.

③침입탐지시스템 운영은 다음 각 호의 절차를 준수한다.

1. 침입탐지시스템에는 침입탐지시스템 이외의 다른 응용프로그램을 설치하여 사용하는 것을 금지한다.

2. 콘솔에 물리적으로 접근할 수 있는 사용자는 침입탐지시스템 관리자로 제한한다.

3. 침입탐지시스템에 직접 접근할 수 있는 사용자 및 호스트는 침입탐지시스템 담당자와 네트워크 관리자로 제한한다.

4. 침입탐지시스템 담당자는 시스템 자체에 대한 침해를 예방하기 위하여 시스템 자체 운영체제의 보안 취약점을 보완 및 관리하여야 한다.

제26조(보안적합성 검증) ①사장은 국가용 보안시스템을 제외한 정보보호시스템, 네트워크 장비 등 보안기능이 있는 정보통신제품을 도

입할 경우 안정성 확인을 위하여 방송통신위원회를 경유하여 국가정보원장에게 보안적합성 검증을 의뢰하여야 한다. 보안적합성 검증 대상 시스템은 다음 각 호와 같다. <개정 2019.5.15.>

1. 상용 정보보호시스템 등 정보보호를 목적으로 도입·운용하는 정보통신제품

2. 자체 개발하거나 외부업체 등에 의뢰하여 개발한 정보보호시스템

3. 저장매체 소자장비 혹은 완전삭제 소프트웨어 제품

4. L3 이상 스위치, 라우터 등 네트워크 장비

②제1항에도 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. <개정 2019.5.15.>

1. 국내용 CC인증 또는 국제용 CC인증을 받은 정보통신 제품

2.「소프트웨어산업 진흥법」제13조에 따른 품질인증을 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)에 의해 국제표준(ISO/IEC 17025)에 따라 인정받은 시험기관에서 시험한 정

보통신제품

5. 국가정보원장이 공지한 검증필 제품목록에 등재된 정보통신제품

6. 국가정보원장이 개발하고 안전성을 확인하여 기술 이전한 정보통신제품

③제2항에도 불구하고 취약점이 발견되거나 보안위협이 제기되는 제품의 경우 보안적합성 검증을 받아야 한다. <개정 2019.5.15.>

[본조전부개정 2015.3.31.]

제26조의2(도입현황 제출) ①사장은 매 반기마다 해당 반기 내에 도입한 제26조에 따른 모든 제품에 대하여 정보통신제품 도입현황 등을 상급 기관의 장에게 제출하여야 한다.

[본조신설 2019.5.15.]

제27조(로그관리) ①정보보안담당자는 서버, 네트워크 장비, 정보보호시스템의 로그지원기능에 대한 내역을 정리하고 해당 시스템관리자와의 협의를 거쳐 접근일시, IP 주소, 대상자원 등 로그에 기록할 항목을 선정한다. <개정 2015.3.31.>

②로그에 기록할 항목을 변경하는 경우에는 정보보안담당관과 협의하여 보안에 미치는 영향을 검토한 후에 변경한다.

③로그는 중요 시스템을 대상으로 기록되도록 설정되어야 한다.

④이상 기록 발견 시 조치 사항은 다음 각 호와 같다.

1. 침해사고 등 이상기록 발생 시 “침해사고대응절차”에 따라 관련 증적을 수집한다.

2. 비인가자에 의한 불법 로그 변경에 대비하여 관련 로그기록은 신속히 오프사이트로 이관하도록 한다.

3. 침해사고 분석이 어려울 경우 정보보안전문업체 등 전문기관에 의뢰하여 정확한 분석이 수행되도록 한다.

4. 특정 호스트로부터의 이상기록이 지속적으로 발생하는 경우 해당 시스템 관리자에게 신속하게 연락을 취하여 조치가 이루어지도록 한다.

⑤로그 정보의 분석 결과는 정보보안담당관에게 보고해야 하며, 이상 발견 시에는 시스템 유지보수 담당 부서장에게 즉시 통보하도록 한다.

⑥로그 정보의 분석 결과는 정보보안담당관에게 보고해야 한다.

## 제 4 장 단말기 보안

제28조(PC 등 단말기 보안관리) ①단말기 사용자는 PC·노트북 등 단말기(이하 “PC 등”이라 한다) 사용과 관련한 일체의 보안관리 책임을 진다.

②정보보안담당관은 비인가자가 PC 등을 무단으로 조작하여 전산자료를 유출하거나, 위・변조 및 훼손시키지 못하도록 다음 각 호에 따른 보호대책을 강구하여야 한다. <개정 2016.3.31.>

1. 장비별・자료별・사용자별 비밀번호 사용

2. PC용 최신 백신 및 침입차단시스템 등  운용

3. P2P 등 업무와 무관하거나 보안에 취약한 프로그램의 사용 금지

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

④PC 등에 적용되는 사용자 계정(ID) 및 비밀번호의 취급관리는 제13조(사용자계정 관리)와 제14조(비밀번호 관리)의 규정을 준용한다.

⑤사용자는 PC 등 보안관리를 위한 다음 각 호의 사항을 준수하여야 한다. <개정 2016.3.31.>

1. PC부팅 시 패스워드 설정

2. 컴퓨터명은 사용자 실명으로 설정하고 작업그룹명은 부서(팀)명으로 설정

3. 최대 10분을 초과하지 않도록 비밀번호 등이 적용된 화면보호기 설정

4. IP주소 임의변경 금지

5. 운영체제(OS) 및 응용프로그램(아래아한글, MS Office, Acrobat 등)의 최신 보안 패치 유지

6. 업무상 불필요한 응용프로그램 설치 금지 및 공유 폴더의 삭제

7. 퇴근 시 전원 차단

⑥방문자 PC 등은 공사 내부 업무망 접속을 원칙적으로 금지한다.

단, 사전에 정보보안담당관의 승인을 받은 사용자의 경우 인터넷 망에 한하여 접속을 허용할 수 있다. <신설 2016.3.31.>

[본조전부개정 2015.3.31.]

제28조의2(비인가 기기 통제) ①공사 임직원등은 개인 소유의 정보통신기기(휴대폰 등 이동통신단말기를 제외한다. 이하 본 조에서 같다)를 소속된 기관으로 무단 반입·사용하여서는 아니 된다. 다만, 부득이한 경우 소속 부서의 분임정보보안담당관을 거쳐 정보보안담당관의 승인을 받은 후 사용할 수 있다.

②공사 임직원등은 개인 소유의 이동통신단말기 또는 이동통신망 접속장치(USB형 등)를 공사 업무망 및 인터넷망에 연결하여서는 아니 되며, 업무망 및 인터넷망 정보시스템을 상용 인터넷망에 연결하는 수단으로 사용하여서는 아니된다. 부서 분임정보보안담당관은 이에 대하여 수시로 점검하여야 한다.

③정보보안담당관은 개인 소유의 정보통신기기가 업무자료를 외부로 유출하는데 악용될 수 있거나 소속된 기관의 정보통신망 운영에 위해(危害)가 된다고 판단될 경우 반출·입 통제 등 보안대책을 수립·시행하여야 한다.

[본조신설 2019.5.15.]

제29조(소프트웨어의 설치 제한) ①업무용 소프트웨어의 사용 시 다음 각 호의 보안사항을 준수한다.

1. 모든 PC에는 정품 소프트웨어만이 설치되고 사용되어야 한다.

2. 업무용 소프트웨어는 항상 최신버전으로 유지해야 한다.

3. 웹 브라우저를 사용할 경우에는 보안문제가 해결된 최신버전을 사용해야 한다.

4. 사용 중인 소프트웨어에 보안상 문제가 발견 혹은 공지되었을 경우에는 즉시 문제가 해결된 최신 프로그램이나 패치를 적용하여야 한다.

5. 타인의 PC에 접근할 수 있거나 자료를 수집할 수 있는 악의적 소프트웨어를 설치하거나 사용해서는 안 된다.

6. 사용할 수 있는 정품 소프트웨어의 기준은 다음과 같다.

가. 원본의 저장 매체를 보유하고 있는 경우(CD,테이프,디스켓 등)

나. 해당 소프트웨어의 구입 영수증을 보유하고 있는 경우

다. 라이선스 구입 계약 사본을 보유한 경우

7. 공개용 소프트웨어의 사용 시에는 공개용 소프트웨어 자체에 상용 공개 또는 무료 배포용이라는 사실이 명기되어 있어야 하며, 공개용 또는 셰어웨어라 할지라도 업무상 사용이 금지되는 문구가 라이선스 상에 표기되어 있을 경우는 사용을 금지한다.

②하드웨어 이용 시 다음 각 호의 보안사항을 준수한다. <신설 2016.3.31.>

1. 기밀정보를 보관 또는 처리하고 있는 PC 등의 모니터는 창문 옆에 설치하지 않도록 한다.

2. PC등의 내·외부에 설치 또는 부착된 하드웨어를 임의로 변경·제

거하거나 외부로 반출해서는 안된다.

3. 잠금 장치가 설치된 PC 등은 사용치 않을 경우 반드시 잠금 기능을 설정해야 한다.

[본조전부개정 2015.3.31.]

제30조(인터넷PC 보안관리) ①정보보안담당관은 인터넷과 연결된 PC(이하 “인터넷PC”라 한다)에 대하여 비인가자가 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손시키지 못하도록 다음 각 호의 보안대책을 사용자에게 지원하며, 사용자는 이를 준수하여야 한다. <개정 2019.5.15.>

1. 메신저·P2P·웹하드 등 업무에 무관하거나 Active-X 등 보안에 취약한 프로그램과 비인가 프로그램·장치의 설치 금지

2. 특별한 사유가 없는 한 문서프로그램은 읽기 전용으로 운용

3. 게임·음란·도박 등 업무와 무관한 인터넷 이용 차단

②사용자는 인터넷PC에서 무단으로 업무자료를 작성·저장 및 소통하는 것이 금지되고 최신 백신을 활용하여 바이러스 감염 여부 등을 주기적으로 점검하여야 한다.

③사장은 인터넷PC에서 업무자료의 저장을 금지하기 위한 기술적·관리적 방안을 강구하여야 한다.

④그 밖에 인터넷PC의 보안관리에 관련한 사항에 대해서는 제28조(PC 등 단말기 보안관리)를 따른다.

[본조전부개정 2015.3.31.] [본조전부개정 2016.3.31.]

제31조(보안프로그램 설치·운영) 사장은 사용자 PC 등의 안정성을 강화하기 위하여 다음 각 호의 필수 보안프로그램 설치 및 운용방안을 강구하여야 한다.

1. 바이러스백신 소프트웨어
2. 패치관리 소프트웨어
3. PC보안 및 접근통제 소프트웨어 등
4. 개인정보 모니터링 소프트웨어 등

[본조전부개정 2015.3.31.]

제32조(업무망 보안관리) ①사장은 업무자료를 소통하기 위한 전산망(이하 “업무망”이라 한다) 구축시 인터넷과 분리하도록 망을 설계하여야 한다. 이 경우 다음 각 호의 보안대책을 강구하여 사업 계획단계(사업 공고 전)에서 국가정보원장에게 보안성 검토를 의뢰하여야 한다.

1. 비인가자의 업무망·인터넷 침입 차단대책(침입차단·탐지시스템 등)
2. 비인가 장비의 업무망 접속 차단대책(네트워크 관리시스템 등)
3. 업무PC의 인터넷 접속 차단대책
4. 업무망과 인터넷간 안전한 자료전송 대책(「국가·공공기관 업무망과 인터넷간 안전한 자료전송 보안가이드라인」(2010.8, 국가정보원) 참조)

②사장은 제1항에도 불구하고, 부득이 한 경우 국가정보원장과 협조하여 적정 보안대책을 강구한 후 망 분리하지 아니할 수 있다.

③업무망 관리자는 정보시스템에 부여되는 'IP주소'를 체계적으로 관리하여야 하고, 비인가자로부터 업무망을 보호하기 위하여 사설주소체계(NAT)를 적용하여야 한다. 또한, IP주소별로 정보시스템 접속을 통제하여 비인가 정보통신기기나 PC 등을 이용한 업무망內 정보시스템 접속을 차단하여야 한다.

④사장은 업무망을 여타 기관의 망 및 인터넷과 연동하고자 할 경우에는 보안관리 책임한계를 설정하고 망 연동에 따른 보안대책을 마련하여 보안심사위원회 심의 후 국가정보원장에게 보안성 검토를 의뢰하여야 한다.

⑤업무망 관리자는 제4항과 관련하여 비인가자의 망 침입을 방지하기 위하여 안전성이 검증된 침입차단·탐지시스템을 운용하는 등 보안대책을 강구하여야 한다.

⑥업무망 관리자는 업무망을 인터넷과 연동시 효율적인 보안관리를 위하여 연결지점을 최소화하여 운용하여야 한다.

⑦업무망과 인터넷망 간의 자료교환은 망간자료전송시스템을 사용하여야 하고 전송로그는 6개월 이상, 원본파일은 3개월 이상 유지하여야 한다.

⑧업무망 관리자는 전송 실패기록을 점검하여 악성코드 유입여부 등을 주기적으로 확인조치하여야 한다.

⑨업무망 PC의 자료를 인터넷 PC로 전송시에는 보안담당자 혹은 결재권자의 사전 또는 사후 승인절차를 마련하여 이를 준수하여야

한다.

[본조전부개정 2015.3.31.] [본조전부개정 2016.3.31.]

제33조(정보시스템 반출·입 관리) 정보시스템 반출·입 관리는 다음 각 호의 보안사항을 준수한다.

1. 공사에서 사용 중인 정보시스템은 정보보안담당관의 승인 없이 외부로 반출할 수 없다.

2. 반·출입에 대한 사항은 관리대장에 기록·관리해야 한다.

3. 반·출입에 대한 관리기록은 정보보안담당관에 의해 점검되어야 한다.

4. 반·출입 시에는 하드웨어 사양 뿐 아니라 설치된 소프트웨어의 사양, 하드디스크 저장 공간 정보를 확인하여야 한다.

[본조전부개정 2015.3.31.]

제34조 <삭제 2016.3.31.>

제35조(휴대용 저장매체 관리) ①"휴대용 저장매체 관리책임자"(이하 '관리책임자'라 한다)라 함은 정보보안담당관을 말한다.

②관리책임자는 휴대용 저장매체의 등록, 파기, 재사용, 반출・입, 불용처리 현황 등의 업무를 수행하는 휴대용 저장매체 실무책임자를 해당 부서별 정보보안담당자로 지정하여 운영 한다.

③그 밖에 명시되지 않은 사항은 국가정보원「USB메모리 등 휴대용 저장매체 보안관리지침」에 따른다.

[본조전부개정 2015.3.31.]

## 제 5 장 정보화 용역사업 관리

제36조(정보화 용역사업) 정보화 용역사업(이하 ‘용역사업’이라 한다)은 정보화·정보보호사업, 보안컨설팅, 위탁운영, 유지보수 등의 사업을 외부용역으로 추진하는 경우를 말한다.

[본조전부개정 2015.3.31.]

제36조의2(보안 책임) ①공사에서 정보통신망 또는 정보시스템을 개발·구축·운용·유지보수하는 사업을 담당하는 정보화 사업담당관은 해당 정보화사업에 대한 보안관리를 수행하여야 한다.

②정보화사업을 추진하는 부서의 장은(이하 “정보화사업담당관”이라 한다.) 정보화사업에 대한 보안관리 책임을 지고 관리·감독하여야 한다. <개정 2020.12.30.>

③정보보안담당관 및 보안담당관은 각종 정보화사업과 관련한 보안대책의 적절성을 평가하고 정보화사업 수행 전반에 대하여 보안대책의 이행여부를 점검하여 필요한 경우 정보화사업을 추진하는 부서의 장에게 시정을 요구할 수 있다.

[본조신설 2019.5.15.]

제36조의3(보안대책 수립) ①사장은 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 운용중인 정보통신망 및 정보시스템에 대한 용역업체 접근 통제대책

8. 누출금지정보 보안관리 방안

[본조신설 2019.5.15.]

제36조의4(제안요청서 기재사항) ①사장은 용역업체에 정보화사업을 발주하기 위하여 제안요청서를 작성할 경우 다음 각 호의 사항을 포함하여야 한다.

1. 용역업체 작업장소에 대한 보안요구사항

2. 기존 운용중인 정보통신망 및 정보시스템에 대한 용역업체 접근 통제 대책

3. 누출금지정보 목록

4. 용역업체가 누출금지정보를 제외한 소프트웨어 산출물을 제3자에게 제공하고자 할 경우 발주자의 승인절차

[본조신설 2019.5.15.]

제37조(용역사업 계획단계) ①용역사업 담당자는「국가를 당사자로 하는 계약에 관한 법률」시행령 제76조 제1항 제18호에 따라 용역사업 추진 시 과업지시서·입찰공고·계약서에 다음 각 호의 누출금지 대상정보를 명시해야 하며 해당정보 누출 시 입찰 참가자격 제한을 위한 부정당업자로 등록하여야 한다. <개정 2019.5.15.>

1. 정보시스템의 내·외부 IP주소 현황
2. 세부 정보시스템 구성 현황 및 정보통신망 구성도
3. 사용자 계정·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. 정보보호시스템 도입 현황
7. 침입차단시스템·방지시스템(IPS) 등 정보보호제품 및 라우터·스위치 등 네트워크 장비 설정 정보
8.「공공기관의 정보공개에 관한 법률」제9조 제1항에 따라 비공개 대상 정보로 분류된 기관의 내부문서
9.「개인정보보호법」제2조 제1호의 개인정보
10.「보안업무관리규정」제7조의 비밀(대외비)
11. 암호자재 및 정보보호시스템 도입·운용 현황
12. 기타 공개가 불가하다고 판단한 자료

②용역사업 담당자는 사업수행을 위한 제안요청서 및 계약서에 참

가직원의 보안준수 사항과 보안 위규자 처리기준 및 위약금 부과기준을 명시할 수 있다.

③용역사업 담당자는 제안평가요소에 자료・장비・네트워크 보안대책 등 보안관리 계획의 평가항목 및 배점기준을 마련하여야 한다.

④용역사업 담당자는 사업계획 단계에서 관련 보안대책을 수립·반영하고 제24조에 따른 보안성 검토를 받아야 한다. <개정 2020.12.30.>

[본조전부개정 2015.3.31.]

제38조(용역사업 입찰・계약단계) ①용역사업 담당자는 입찰 공고 시 누출금지 대상정보, 부정당업자 제재조치, 기밀유지 의무 및 위반 시 불이익 등 보안준수사항을 공지하여야 한다.

②용역사업 담당자는 제안업체가 제시한 보안관리 계획의 타당성을 검토하여 사업자 선정 시 반영하여야 한다.

③용역사업 담당자는 사업에 투입되는 자료・장비 등에 대해 대외보안이 필요한 경우 보안의 범위・책임을 명확히 하기 위하여 사업수행계약서와 별도로 비밀유지계약서를 작성하여야한다. 비밀유지계약서에는 비밀정보의 범위, 보안준수 사항, 위반 시 손해배상 책임, 지적재산권 문제, 자료의 반환 등이 포함되도록 명시하여야한다.

④용역사업 담당자는 외부용역을 추진할 경우 사업 책임자로 하여금 다음 각 호의 사항을 포함한 보안대책을 수립・시행하여야 한다.

1. 용역사업 계약서에 참가직원의 보안준수사항과 위반 시 손해배

상 책임 등 명시

2. 용역사업 수행 관련 보안교육·점검 및 용역기간 중 참여인력 임의교체 금지

3. 정보통신망 구성도, IP현황 등 용역업체에 제공할 자료는 자료인계인수대장을 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·반입 시 마다 악성코드 감염여부, 자료 무단반출 여부를 확인

7. 기타, 사장이 보안관리가 필요하다고 판단하는 사항이나 국가정보원장이 보안조치를 권고하는 사항

⑤용역사업 담당자는 용역업체가 사업의 일부 또는 전부에 대하여 하도급 계약을 체결하는 경우에 용역업체로 하여금 하도급 계약서에 본 사업계약 수준의 비밀유지 조항을 포함하도록 조치하여야 한다.

[본조전부개정 2015.3.31.]

제39조(용역사업 수행단계) ①용역사업 담당자는 참여인원에 대하여

다음 각 호에 따라 보안 관리를 하여야 한다.

1. 용역사업의 참여인력에 대하여 보안서약서 징구

2. 용역업체 참여인원에 대해 법적 또는 발주기관 규정에 따른 비밀유지 의무준수 및 위반 시 처벌 내용 등에 대한 보안교육

3. 발주기관은 사업수행 중 업체 인력에 대한 보안점검 실시, '누출금지 대상정보' 외부 누출여부 확인

4. 비밀관련 용역사업을 수행할 경우, 참여인원에 대한 비밀취급인가 등 보안조치를 수행하고 국가정보원에게 보안측정을 요청

②용역사업 담당자는 용역업체에게 자료를 제공하거나 용역사업수행 중에 생산된 산출물에 대하여 다음 각 호에 따라 보안 관리를 하여야 한다. <개정 2019.5.15.>

1. 계약서 등에 명시한 누출금지 대상정보를 업체에 제공할 경우 인수인계대장을 작성, 인계자·인수자가 직접 서명한 후 제공하고 사업완료 시 관련자료 회수

2. 용역사업 관련자료 및 사업과정에서 생산된 산출물은 발주기관의 파일 서버에 저장하거나 사업의 보안담당이 지정한 PC에 저장·관리

3. 용역사업 관련 자료는 인터넷 웹하드·P2P 등 인터넷 공유사이트 및 개인메일함에 저장을 금지하고 용역발주기관과 용역업체간 전자우편을 이용해 자료전송이 필요한 경우에는 자체 전자우편을 이용, 첨부자료 암호화 수발신

4. 발주기관의 사무실에서 용역사업을 수행할 경우, 제공한 비공개 자료는 매일 퇴근 시 반납하고 일반문서는 시건장치가 된 보관함에 보관

5. 용역사업 수행으로 생산된 산출물 및 기록은 정보보안담당관이 인가하지 않은 비인가자에게 제공・대여・열람 금지

③용역사업 담당자는 용역사업을 수행하는 사무실과 장비에 대하여 다음 각 호에 따라 보안관리를 하여야 한다.

1. 시건장치가 구비되고 비인가자 출입통제가 가능한 사무실 사용

2. 용역업체의 사무실과 인원・장비를 대상으로 정기적으로 보안점검 실시

3. 발주기관 내부에서 용역사업을 수행하는 경우 용역 참여직원이 노트북 등 관련 장비를 외부에 반출・입시마다 악성코드 감염여부 및 자료 무단반출 여부 확인

4. 인가받지 않은 USB 등 휴대용 저장매체 사용을 금지하며 산출물 저장을 위하여 휴대용 저장매체가 필요한 경우 발주기관의 승인하에 사용

④용역사업 담당자는 용역업체가 이용하는 전산망에 대하여 다음 각 호에 따라 보안관리를 하여야 한다.

1. 용역업체 사용전산망은 방화벽 등을 활용하여 공사 업무망과 분리구성하고 업무상 필요한 서버에만 제한적 접근

2. 사업참여 인원에 대한 사용자 계정은 하나의 그룹으로 등록하고

계정별로 정보시스템 접근권한을 차등 부여하되 내부문서 접근 금지하고 불필요 시 곧바로 권한을 해지하거나 계정을 폐기

3. 참여인원에게 부여한 패스워드는 시스템관리자가 별도로 기록·관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력 확인

4. 시스템관리자는 내부서버 및 네트워크 장비에 대한 접근 기록을 매일 확인하여 이상유무 보고

5. 용역업체에서 사용하는 PC는 인터넷 연결을 PC는 인터넷 연결을 금지하되, 사업수행 상 연결이 필요한 경우에는 발주기관의 보안통제 하에 제한적 허용

6. 발주기관 및 용역업체 전산망에서 P2P, 웹하드 등 인터넷 자료공유사이트로의 접속을 방화벽 등을 이용해 원천차단

⑤그 밖에 용역업체 보안과 관련한 사항은 국가정보원장이 배포한 「국가·공공기관 용역업체 보안관리 가이드라인」을 준수하여야 한다. <개정 2019.5.15.>

[본조전부개정 2015.3.31.]

제40조(용역사업 종료단계) ①용역사업 담당자는 최종 용역산출물 중 대외보안이 요구되는 자료는 대외비 이상으로 작성·관리하고 불필요한 자료는 반드시 삭제 및 폐기하여야한다.

②용역사업 담당자는 용역업체에 제공한 자료·장비·문서 및 중간·최종산출물 등 사업 관련 제반자료를 확인하여 전량 회수해야

하며, 업체에 복사본 등 별도 보관을 금지시켜야 한다.

③용역사업 담당자는 사업완료 후 업체 소유 PC·서버의 하드디스크·휴대용저장매체 등 전자기록 저장매체는 국가정보원장이 안전성을 검증한 삭제 S/W로 완전 삭제 후 반출하여야 한다.

④용역사업 담당자는 제2항의 용역사업 관련자료 회수 및 삭제조치 후에 용역업체가 용역산출물의 복사본 등 용역사업 관련 자료를 보유하고 있지 않다는 용역업체 대표명의 보안확약서를 징구하여야 한다.

[본조전부개정 2015.3.31.]

제41조(외부용역 보안관리) ①중요 정보시스템에 외주업체 직원의 접근이 필요한 경우 정보보안에 영향을 미치는 위험을 사전에 파악하여 다음 각 호의 보안통제사항을 준수한다. <개정 2015.3.31.> <개정 2019.5.15.>

1. 용역업체 인력에 대한 보안책임은 주관부서의 장에게 있다.

2. 정보보안담당자는 용역업체 인력이 공사의 정보자산에 접근할 수 있는 범위를 명확히 지정하고 이의 준수여부를 점검해야 한다. 추가적인 접근이 필요할 경우 별도로 정보보안담당관의 승인을 득해야 한다.

3. 용역업체로부터의 인터넷을 통한 원격 접속은 원칙적으로 금지하며, 반드시 기관에 내방하여 정보보안담당자 통제하에 작업을 진행해야 한다.

4. 용역업체의 원격 접속 요청이 있을 경우 해당 담당자는 네트워크 담당자 및 정보보안담당자와 협의 후에 원격 접속을 허용해야 한다. 이 경우 발신지 IP 주소와 접속시간을 아웃소싱업체에게 요구하여야 한다.

5. 정보보안담당자가 용역업체의 발신지 IP 주소가 해당 업체의 IP 주소와 일치하는지 확인한 후 네트워크 담당자가 접속을 허용 하여야 한다.

②소프트웨어의 개발을 외주할 경우 다음 각 호의 사항들을 고려해야 한다.

1. 라이선스 협정, 소스코드 등에 대한 소유권, 지적재산권 등

2. 수행된 작업의 정확성과 품질에 대한 인증

3. 소스 코드 품질에 대한 계약상의 요구사항

③본 장에 명시되지 않은 외주관리에 대한 세부사항은 “「국가·공공기관 용역업체 보안관리 가이드라인」(2014.3, 국가정보원)”을 따른다. <개정 2016.3.31.>

제41조의2(원격지 개발보안) ①사장은 용역업체가 발주기관 이외 장소(이하 “원격지”라 한다)에서 개발 작업(유지보수는 제외한다)을 수행하고자 요청할 경우 제36조의3 제1항 제6호에 따른 용역업체 작업장소에 대한 보안요구사항 등을 포함한 관리적·기술적 보안대책을 수립·시행하여야 한다. 이 경우 정보화사업담당관은 보안대책을 수립한 후 정보보안담당관의 승인을 받아야 한다. <개정 2023.6.19.>

②사장은 용역업체의 원격지 개발과 관련한 보안대책 이행여부를 정기 또는 수시로 점검(불시 점검을 포함한다)하여야 한다. 이 경우 정보화사업담당관이 점검한 후 그 결과를 정보보안담당관에게 통보하여야 한다.

③사장은 제2항에 따라 용역업체의 원격지 개발과 관련한 보안대책 이행여부를 점검한 결과 미흡하다고 판단될 경우 원격지 개발 허가를 취소하여야 한다.

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

[본조신설 2019.5.15.]

제41조의3(원격지에서의 온라인 개발) 제41조의2에 따른 원격지 개발에서 정보화사업담당관이 필요하다고 판단하고 용역업체가 다음 각 호에 따른 보안대책에 서면으로 동의하는 경우에 한하여, 정보보안담당관은 용역업체에게 원격지에서 인터넷을 통해 발주기관 정보시스템에 온라인 접속한 상태의 개발 작업을 허용할 수 있다.

1. 지정된 단말기에서만 접속 및 해당 단말기에 대한 접근인원 통제

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

3. 공사 내 설치된 온라인 용역 통제시스템을 경유하여 개발에 필요한 정보시스템에 접속하는 등 소통구간 보호·통제

4. 접속사실이 기록된 로그기록을 1년 이상 보관

5. 계약 시행일로부터 종료 후 30일이 경과하는 날까지의 기간 중에 공사, 방송통신위원회 위원장 및 국가정보원장의 정기 또는 수시 보안점검(불시 점검을 포함한다) 수검

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

[본조신설 2023.6.19.]

[종전의 제41조의3은 제41조의4로 이동 <2023.6.19.>]

제41조의4(소프트웨어 산출물 제공) ①사장은 용역업체가 「용역계약 일반조건」(기획재정부 계약예규) 제56조에 따른 지식재산권을 행사하기 위하여 소프트웨어 산출물의 반출을 요청할 경우 제안요청서 또는 계약서에 명시된 누출금지정보에 해당하지 아니하면 제공하여야 한다.

②각급기관의 장은 제1항에 따라 소프트웨어 산출물을 용역업체에 제공할 경우 업체의 노트북·휴대용 저장매체 등 관련 장비에 저장되어 있는 누출금지정보를 완전 삭제하여야 하며 업체로부터 누출금지정보가 완전 삭제되었다는 대표자 명의의 확약서를 받아야 한다.

③사장은 용역업체가 소프트웨어 산출물을 제3자에게 제공하고자

할 경우 제공하기 이전에 승인을 받도록 하여야 한다.

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

[본조신설 2019.5.15.]

[제41조의3에서 이동 <2023.6.19.>]

제41조의5(누출금지정보 유출시 조치) ①정보보안담당관은 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 정보화사업담당관은 즉시 정보보안담당관을 거쳐 정보보안책임자에게 보고하여야 한다.

②제1항에 따라 용역업체의 누출금지정보 유출 사실을 알게되거나 보고를 받은 정보보안담당관은 그 사실을 방송통신위원회 위원장 및 국가정보원장에게 통보하여야 하고 「국가를 당사자로 하는 계약에 관한 법률 시행령」제76조 및 「지방자치단체를 당사자로 하는 계약에 관한 법률 시행령」제92조에 따라 입찰 참가자격 제한 등 관련조치를 취하여야 한다.

[본조신설 2023.6.19.]

## 제 6 장 시스템 개발 보안

제42조(정보시스템 개발 보안) ①시스템 개발사업 담당자는 정보시스템을 자체적으로 개발하고자 하는 경우에 다음 각 호의 사항을 고려하여 보안대책을 수립하고 정보보안담당관의 승인을 받아야 한다.

1. 독립된 개발시설 확보 및 비인가자의 접근통제
2. 개발시스템과 운영시스템의 물리적 분리
3. 소스코드 관리 및 소프트웨어 보안관리

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

1. 외부 인력 대상 신원확인, 보안서약서 징구, 보안교육 및 점검
2. 외부 인력의 보안준수 사항 확인 및 위반시 배상책임의 계약서 명시
3. 외부 인력의 정보시스템 접근권한 및 제공자료 보안대책
4. 외부 인력에 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.

[본조전부개정 2015.3.31.]

제43조(정보시스템 유지보수) ①사장은 정보시스템 유지보수와 관련한

절차, 주기, 문서화 등에 관련된 사항을 계약 시 포함하여야 한다. 유지보수 절차 및 문서화 수립 시 고려사항은 다음 각 호와 같다.

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.

③시스템 관리자는 정보시스템의 변경이 발생할 경우, 정보보안담당관과 협조하여 정보시스템의 설계·코딩·테스트·구현 과정에서의 보안대책을 강구하며 정보보안담당관은 관련 적절성을 주기적으로 확인하여야 한다.

④정보보안담당관은 시스템 관리자 등이 유지보수와 관련된 장비·도구 등을 반출·입 할 경우, 악성코드 감염여부, 자료 무단반출 여부를 확인하는 등의 보안조치를 하여야 한다.

⑤시스템관리자는 외부에서 원격으로 정보시스템을 유지보수하는

것을 원칙적으로 금지하여야 하며 부득이한 경우에는 정보보안담당관과 협의하여 자체 보안대책을 강구한 후 한시적으로 허용할 수 있다.

[본조전부개정 2015.3.31.]

## 제 7 장 사이버 공격 대응

제44조(침해사고대응팀 구성) ①사장은 해킹·바이러스 등 사이버공격의 신속한 대응 및 복구를 위한 침해사고대응팀(이하 “침해사고대응팀”)을 구성·운영하여야 한다.

②정보보안담당관은 침해사고대응팀을 총괄 운영한다.

③침해사고대응팀은 각 호의 사항을 수행하여야 한다.

1. 침해사고 접수 및 보고
2. 침해사고 예방 및 복구업무
3. 침해사고에 관한 정보관리

[본조전부개정 2015.3.31.]

제45조(사이버공격 초동조치) ①정보보안담당관은 정보통신망에 대하여 해킹, 웜·바이러스 유포 등 사이버공격 인지 시 피해실태를 파악하고 관련 로그자료 보존 및 필요시 전산망 분리 등 초동조치를 하여야 한다.

②정보보안담당관은 전산망 마비 또는 자료 유출 등 사이버 공격과

관련한 정보를 확인한 경우 초동조치 후 사장에게 보고하고, 전화·팩스·이메일 등 통신수단을 활용하여 지체없이 그 사실을 방송통신위원회 위원장 및 국가정보원장에게 보고하여 필요한 지원을 받아야 한다.

③제2항과 관련하여 피해시스템은 사고원인 규명 시까지 증거보전하고 임의 자료삭제 또는 포맷을 하여서는 아니 된다.

[본조신설 2015.3.31.]

제46조(사이버공격 대응활동) ①정보보안담당관은 소관분야의 사이버공격 대응절차를 수립·시행하고 이행실태를 지속적으로 확인 점검하여야 한다.

②정보보안책임자는 국가정보원장이 경보 발령시 소관분야 직원을 대상으로 관련사항을 전파하고 대응조치를 이행하며 진행상황을 예의주시하는 등 대응절차에 따라 신속하게 대처하여야 한다. <개정 2016.3.31.>

③정보보안책임자는 제2항에 따른 경보 단계별 조치사항을 방송통신위원회 위원장을 경유하여 국가정보원장에게 통보하여야 한다. <개정 2016.3.31.>

④그 밖에 명시되지 않은 사항은 자체 「사이버 위기 대응 매뉴얼」과 「국가 사이버 위기 대응 매뉴얼」에 따른다.

[본조신설 2015.3.31.]

제47조(정보보안 규정 준수) ①공사 직원은 정보보안 관련 지침을 준

수할 의무가 있으며, 정보보안 활동에 모범이 되는 직원이나 팀에 대하여 포상을 실시할 수 있다. 또한, 정보보안담당관은 정보보안 관련 규정을 위반한 직원에 대하여는 보안업무관리규정 제4조 및 인적보안 가이드라인에 따라 다음과 같이 처리해야 한다. <개정 2020.12.30.>

1. 심각한 정보보안 위반사항 보안심사위원회 회부
2. 위험한 정보보안 위반사항에 대한 감사부서 점검 협조
3. 경미한 정보보안 위반사항 처리

②공사 직원은 정보통신망에 의하여 처리·보관 또는 전송되는 비밀정보 및 타인의 개인정보를 훼손하거나 공개를 원하지 않는 타인의 개인정보를 침해·도용 또는 누설하여서는 아니 된다.

③서비스의 제공을 위하여 이용자의 개인정보를 취급하거나 취급하였던 자는 직무상 알게 된 개인정보를 훼손·침해 또는 누설하여서는 아니 된다.

④공사 직원은 공사의 정보통신망 또는 정보시스템에 대하여 다음 각 호에 해당하는 행위를 해서는 아니 된다.

1. 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망 또는 정보시스템에 침입하는 행위
2. 정당한 사유 없이 정보시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조 또는 그 운용을 방해할 수 있는 프로그램(이하 “악성프로그램”이라 한다)을 전달 또는 유포하는 행위

3. 정보통신망 또는 정보시스템의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애를 발생하게 하는 행위

⑤공사 직원은 다음 각 호에 해당하는 기술 및 내부 중요자료를 침해하는 행위를 해서는 안 된다.

1. 부정한 방법으로 타인의 기술 및 중요자료를 취득하는 행위

2. 부정한 방법으로 취득한 기술 및 내부 중요정보를 사용하거나 공개하는 행위 또는 타인에게 제공 하는 행위

3. 기술 또는 중요자료를 비밀로 유지해야 할 의무가 있는 자가 그 내용을 공개하는 행위 또는 타인에게 제공 하는 행위

4. 제1호 내지 제3호의 침해행위가 개입된 사실을 알았거나 중대한 과실로 알지 못하고 그 내용을 취득하거나 취득한 내용을 사용 또는 공개하는 행위

[본조신설 2015.3.31.] [본조전부개정 2016.3.31.]

제47조의2(무선랜 보안) ① 사장은 업무망(내부망)을 제외한 정보통신망에서 다음 각 호의 경우와 같이 건물 내에 무선랜(WiFi)을 구축·운용할 수 있다.

1. 기관 인터넷망에 중계기(AP)를 설치하여 제28조에 따라 공사 사장이 지급한 단말기의 접속만을 허용하는 인터넷망용 무선랜

2. 상용 인터넷망에 중계기(AP)를 설치하여 제28조의2에 따라 반입한 임직원등의 개인 소유 이동통신단말기의 접속만을 허용하는

무선랜

3. 상용 인터넷망에 중계기(AP)를 설치한 외부인 전용(專用) 무선랜

②사장은 제1항에 따라 무선랜을 구축·운용하고자 할 경우 국가정보원장이 배포한 「국가·공공기관의 무선랜 구축 가이드라인」을 준수하여 보안대책을 수립·시행하여야 한다.

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

1. 네트워크 이름(SSID) 브로드캐스팅(broadcasting) 금지

2. 추측이 어렵고 복잡한 네트워크 이름(SSID) 사용

3. WPA2 이상(256비트 이상)의 암호체계 사용하여 소통 자료 암호화

4. 비(非)인가 단말기의 무선랜 접속 차단 및 무선랜 이용 단말기를 식별하기 위한 IP주소 할당기록 등 유지

5. IEEE 802.1X, AAA(Authentication Authorization Accounting) 등의 기술에 따라 상호인증을 수행하는 무선랜 인증제품 사용

6. 무선침입방지시스템 설치 등 침입 차단 대책

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

④부서 분임정보보안담당관은 제2항 및 제3항에 따른 보안대책의

적절성을 수시로 점검·보완하여야 한다.

[본조신설 2019.5.15.]

제47조의3(클라우드컴퓨팅 보안) ①「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제12조에 따라 클라우드컴퓨팅(「행정기관 및 공공기관 정보자원 통합기준(행정안전부 고시)」제2조제5호에 따른 공공클라우드센터를 포함한다)을 자체 구축·운영하고자 할 경우 국가정보원장이 배포한 「국가·공공기관 클라우드 컴퓨팅 보안 가이드라인」에 명시된 기관 자체 클라우드컴퓨팅 구축 보안기준에 따라 보안대책을 수립·시행하여야 한다.

②민간 클라우드컴퓨팅서비스(「행정기관 및 공공기관 정보자원 통합기준(행정안전부 고시)」제2조제4호에 따른 민간클라우드센터를 포함한다)를 이용하고자 할 경우 다음 각 호에 해당하는 사항을 준수하여야 한다.

1. 국내에 위치한 정보시스템에 데이터가 저장되는 서비스로서 일반 이용자용 서비스 영역과 물리적으로 분리되어 제공되는 서비스 영역(이하 “공공 전용(專用) 클라우드”라 한다)에 한하여 활용

2. 과학기술정보통신부장관이 고시한 「클라우드컴퓨팅서비스 정보보호에 관한 기준」에 부합하는 서비스 선정

3. 국가정보원장이 배포한 「국가·공공기관 클라우드컴퓨팅 보안 가이드라인」에서 제시하는 민간 클라우드컴퓨팅서비스 이용 보안기준 및 행정안전부장관이 배포한 「행정·공공기관 민간 클라우드

이용 가이드라인」에 따른 절차 이행

③내부망과 연동된 공공 전용(專用) 클라우드는 이 지침을 적용함에 있어 내부망으로 본다.

④기관 인터넷망과 연동된 공공 전용(專用) 클라우드는 이 지침을 적용함에 있어 기관 인터넷망으로 본다.

⑤제2항에 따라 민간 클라우드컴퓨팅서비스를 이용할 경우 정보보안담당관은 클라우드컴퓨팅서비스제공자에 의하여 누출금지정보가 유출된 경우 제41조의5에 따른 조치를 취하여야 한다.

[본조신설 2023.6.19.]

제48조(준용사항) 공사의 정보보안업무 수행에 필요한 사항 중 이 지침에서 정하지 아니한 사항은 국가정보원 「국가 정보보안 기본지침」 및 방송통신위원회 「정보보호 관리지침」을 준용한다.

[본조신설 2016.3.31.]

## 부 칙

이 지침은 2012년 8월 22일부터 시행한다.

## 부 칙<2013.7.24.>

이 지침은 2013년 7월 26일부터 시행한다.

## 부 칙<2015.3.30.>

이 지침은 2015년 3월 31일부터 시행한다.

## 부 칙 <2016.3.28.>

이 지침은 2016년 3월 31일부터 시행한다.

## 부 칙 <2017.7.31.>

이 지침은 2017년 8월 1일부터 시행한다.

## 부 칙 <2019.5.15.>

이 지침은 2019년 5월 16일부터 시행한다.

## 부 칙 <2020.12.30.>

이 지침은 2020년 12월 31일부터 시행한다.

## 부 칙 <2023.6.19.>

이 지침은 2023년 6월 21일부터 시행한다.