한국인터넷정보센터 정보보안지침

제정 2015. 07. 14.
개정 2017. 04. 13.
개정 2018. 12. 28.
개정 2020. 1. 31.
전부개정 2021. 2. 25.
개정 2022. 1. 27.
전부개정 2022. 12. 23.
개정 2023. 12. 28.

제 1 장 총 칙

제1조(목적) 이 지침은 한국인터넷진흥원(이하 “진흥원”이라 한다) 한국인터넷정보센터의 안정적인 운영과 정보보안과 관련한 제반 사항을 정의하는 것을 목적으로 한다

제2조(적용범위) ① 이 지침은 한국인터넷정보센터의 전 직원 및 외주직원에게 적용한다.

② 한국인터넷정보센터의 정보보안 업무는 진흥원의 「보안업무규칙」,「정보보안기본지침」에서 정한 사항을 제외하고는 이 지침에서 정한 바에 따른다.

제3조(정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. “정보통신망”이란 「전기통신기본법」 제2조 제2호의 규정에 따른 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집・가공・저장・검색・송수신하는 정보 통신체제를 말한다.
2. “정보보안”이라 함은 각급기관의 기능 유지를 주 목적으로 정보통신망 및 정보시스템을 통해 수집, 가공, 저장, 검색, 송・ 수신되는 정보의 유출, 위・변조, 훼손 등을 방지하기 위하여 관리적・물리적・기술적 수단을 강구하는 일체의 행위로서 다음 각 목에 따른 사항을 포함한다.

가.「국가정보원법」제4조제1항제4호에 따른 사이버공격 및 위협에 대한 예방 및 대응
나.「전자정부법」제56조에 따른 정보통신망과 행정정보 등의 보안
다.「정보통신기반 보호법 시행령」제5조제4항제1호 각 목에 해당하는 주요정보통신기반시설의 보호

라.「공공기록물 관리에 관한 법률 시행령」제5조에 따른 전자 기록물의 보안
마.「국가사이버안전관리규정」제2조제3호에 따른 사이버안전

3. “외주”란 “외주업체” 또는 “외주직원“을 말한다.

4. "외주업체"란 국가정보원 “정보보안기본지침”의 외부 용역업체를 뜻하며, 계약을 통해 한국인터넷정보센터의 정보자산을 이용하여 서비스와 기타 업무를 대행하는 업체를 말한다.

5. "외주직원"이란 한국인터넷정보센터의 정보자산을 이용하여 서비스와 기타 업무를 대행하는 자를 말한다. <개정 2023. 12. 28.>

6. “보호지역”이란 통제구역 및 제한구역을 말한다.

7. “통제구역”이란 한국인터넷정보센터의 정보보안을 위해 매우 중요한 구역으로서 비인가자의 출입이 금지되는 구역을 말한다.

8. “제한구역”이란 한국인터넷정보센터의 사무공간에 대한 외부인의 접근을 방지하기 위해 출입의 안내가 요구되는 지역을 말한다. <개정 2023. 12. 28.>

9. “정보시스템”이란 서버, 네트워크, 보안장비, PC 등 정보의 수집・가공・저장・검색・송수신에 필요한 하드웨어 및 소프트웨어 일체를 말한다.

10. “침입차단시스템”이란 불법 침입으로부터 내부 정보자산을 보호하고 유해정보 유입의 차단을 위하여 접근통제를 수행하는 네트워크 구성 요소로서 하드웨어 또는 소프트웨어로 구성된 시스템을 말한다.

11. “침입탐지(방지)시스템”이란 외부 침입에 의해 불법적인 접근이 감지되었을 경우, 침입사실을 탐지(방지)하는 시스템을 말한다.

12. “보안장비”란 정보의 수집, 가공, 저장, 검색, 송수신 중에 나타나는 정보의 훼손, 변조, 유출 등을 방지하기 위한 시스템을 말하는 것으로써, 침입차단시스템, 침입탐지(방지)시스템 등을 포함한다.

13. “응용프로그램”이란 사용자의 실무 업무 처리를 위해 사용하는 프로그램을 말한다.

14. “DB”란 논리적으로 연관된 레코드나 파일의 모임으로 조직 내에서 여러 사람에 의해 공유되어 사용될 목적으로 통합적으로 조직되고 관리되는 운영 자료의 집합을 말한다.

15. “암호화”란 중요한 정보의 보안을 유지하기 위해 그 정보를 특정한 규칙에 따라 변형하여 저장함으로써 해독방법을 모르는 사람은 그 정보의 내용을 알아볼 수 없도록 하는 것을 말한다. 이와 반대로 암호화된 문장으로부터 원래의 정보를 복구하는 것을 복호화라 한다.

16. “침해사고”란 정보보안 관리 대상에 속하는 정보 및 정보시스템이 무단으로 파괴되거나, 유출, 변조되어 업무수행에 지장을 초래하는 사고를 말한다.

17. “장애”란 IT장비의 일시적 정지, 작동 오류, 유지보수 활동 등으로 부분적 또는 일시적으로 IT 기능의 정지 및 기능의 저하 상태를 말한다.

18. “보안점검”이란 한국인터넷정보센터 및 정보시스템이 수립된 규정 및 지침에 준하여 안전하게 운용되고 있는지 확인하기 위하여 각종 사용자 행위에 대한 상세 내용을 조사·분석하

는 것을 의미하며, 내부에서 시행하는 자체 점검과 외부 전문가들에 의한 보안감사를 모두 포함한다.

제4조(역할과 책임) ① 분임보안담당관은 한국인터넷정보센터를 총괄하는 본부장이 수행하며, 다음 각 호의 업무를 수행한다.

1. 한국인터넷정보센터 소속직원의 보안업무 수행에 관한 교육 및 감독
2. 한국인터넷정보센터의 각 종 보안 침해사고 예방 및 조치
3. 한국인터넷정보센터 시설 보안 및 안전 관리
4. 한국인터넷정보센터 비밀문서의 관리
5. 업무수행 상 보안을 요하는 사항의 협조
6. 기타 한국인터넷정보센터의 보안업무 관련 사항

② 분임정보보안담당관은 분임보안담당관을 보좌하고, 한국인터넷정보센터 전산자원 관리 업무를 하는 단(센터)의 단장(센터장)이 수행하며, 다음 각 호의 업무를 수행한다.

1. 한국인터넷정보센터의 정보보안 실무 총괄
2. 한국인터넷정보센터의 정보보안 정책·계획의 수립·시행 및 정보보안지침 제·개정
3. 한국인터넷정보센터의 정보보안 인력 관리, 전문인력 및 관련 예산 등 운영
4. 기타 한국인터넷정보센터의 정보보안 업무 관련 사항

③ 시스템관리자는 분임정보보안담당관을 보좌하고, 한국인터넷정보센터의 전산자원 관리 업무를 수행하는 팀의 팀장이 하며, 다음 각 호의 업무를 수행한다.

1. 센터에서 운영하는 정보 자산의 유지 관리
2. 신규 정보시스템 구매 및 구축
3. 센터의 운영 및 관련 시설 관리
4. 외주 용역 보안관리
5. 계정 관리, 시스템 도입/변경/폐기, 로그관리, 백업/패치관리 등 시스템 운영 · 보안 관리

④ 정보보안담당자는 시스템관리자에 의해 임명된 직원으로 분임정보보안담당관을 보좌하여한국인터넷정보센터의 정보보안 실무를 수행하며, 다음 각 호의 업무를 수행한다.

1. 정보보안 관련 법규 및 지침의 제·개정 소요 검토
2. 자체 모의 훈련 계획 수립 · 시행 및 정보보안 관리실태 평가 대응
3. 주기적인 정보보안 취약점 분석·평가 및 정보보안 점검
4. 정보시스템 신규 도입 시 보안성 검토 추진
5. 침해사고 대응 관리

⑤ 정보시스템담당자는 시스템관리자에 의해 임명된 직원으로 서버, 네트워크, 보안장비 등의 각 정보시스템을 운영·관리하며, 다음 각 호의 업무를 수행한다.

1. 정보시스템 하드웨어, 소프트웨어 목록 유지관리
2. 신규 정보시스템 도입 시 보안 설정
3. 정보시스템 변경사항 기록 관리
4. 정보시스템 계정 및 접근권한 관리
5. 침해사고 및 장애 등 시스템 이상 발생 시 정보보안담당자와 협업하여 대응
6. 그 밖에 정보시스템 운영 및 보안에 관한 사항

⑥ 한국인터넷정보센터 직원 개인은 부여된 업무와 관련하여 보안책임을 진다.

제5조(정보보안 지침 및 정책 타당성 검토) 정보보안담당자는 상위지침 변경사항 반영 등 한국인터넷정보센터 정보보안 지침 및 보안정책의 타당성을 주기적으로 검토해야 하며, 필요 시 개선해야 한다.

제6조(비밀유지의무) ① 한국인터넷정보센터 직원 및 외주직원은 업무 수행과정에서 알게 된 민감한 사항 및 정보를 외부에 유출하거나 공개해서는 안 된다.

제2장 보안 관리

제 1 절 관리적 보안 관리

제7조(정보통신망 자료 보안관리) 시스템관리자는 다음 각 호에 해당하는 정보통신망 관련 현황·자료를 대외비 이상으로 관리해야 한다.

1. 정보시스템 운용현황
2. 정보통신망 세부 구성현황(IP/PORT 세부 할당현황 포함)
3. 주요 정보화사업 관련 산출물
4. 그 밖에 보호할 필요가 있는 정보통신망 관련 자료

제8조 <삭제 2023. 12. 28.>

제9조(자산 관리) ① 시스템관리자는 자산의 중요도를 평가하여 자산의 등급과 유형에 따른 관리 및 보호를 해야한다.

② 시스템관리자는 분류된 자산에 대해 "「정보보안 기본지침」별지 제3호 서식에 따른 정

보시스템 관리대장”을 작성하고 각 자산에 대해 관리번호, 책임자, 담당자, 운영자, 사용자 현황을 관리해야 한다.

③ 정보시스템담당자는 신규도입 및 폐기 등 자산의 반·출입이 발생할 경우 “[별지 제3호 서식] 한국인터넷정보센터 장비 반입·반출증”을 작성하여야 한다.<개정 2023. 12. 28.>

④ 자산의 반ㆍ출입 이력은 “「정보보안 기본지침」별지 제30호 서식 정보시스템 반출·입 대장”을 통해 관리하고 분기 1회 이상 자산의 반ㆍ출입 이력을 확인해야 한다.

제 2 절 물리적 보안 관리

제10조(보호지역의 설정) 진흥원 보안업무규칙 제51조(보호지역 관리책임) 제1항에 따라 한국인터넷정보센터는 제한구역으로 설정하고 전산실, 종합상황실을 통제구역으로 설정한다. <개정 2023. 12. 28.>

제11조(통제구역의 보안관리) ① 출입통제 및 감시를 위해 출입통제시스템(카드키, 정맥인식), 감시 카메라 등을 설치한다.

② 통제구역 출입 시 인가자는 출입통제시스템을 통해서만 출입하며, 비인가자의 경우 「보안업무규칙」별지 제17호 서식 출입통제대장을 작성한다.

③ 한국인터넷진흥원「보안업무규칙」제50조(보호지역의 보호대책)에 따라 통제구역 표시를 해야 한다.

④ 출입자에 대한 방문일자, 방문목적, 출입시각 등의 출입기록은 3개월 이상 보관 한다.

⑤ 통제구역 출입에 대한 접근권한을 주기적으로 점검하며, 시스템관리자에게 보고해야 한다.

⑥ 외주직원에 대한 통제구역의 출입 및 업무 수행은 정규 업무시간으로 제한하며, 정규 업무시간 이외에 접근이 필요한 경우 정보시스템담당자의 승인을 득해야 한다. 단, 상황실 야간 관제요원은 예외로 한다.

⑦ 통제구역으로 반/출입되는 모든 가방, 서류, 기타 휴대용 전산장비 등은 필요 시 검색할 수 있으며, 사진기, 녹음기 또는 비디오 장비 등은 원칙적으로 통제구역 내 반입을 금지한다.

⑧ 통제구역 내부에서 시스템관리자의 사전 승인을 득하지 않은 사진 및 동영상 촬영을 금지한다.

⑨ 면직, 전보된 임직원에 대한 불필요한 접근은 제한되어야 한다.

제12조(제한구역의 보안관리) ① 출입통제를 위해 출입통제시스템(카드키)을 설치한다.

② 비인가자의 제한구역 출입은 해당 업무담당자와 동행 하에 출입한다.

③ 면직, 전보된 임직원에 대한 불필요한 접근은 제한되어야 한다.

제13조(출입통제 절차) 보호지역의 세부 출입통제 절차는 「한국인터넷정보센터 시설 및 전산자원 관리수칙」을 따른다.

제 3 절 기술적 보안 관리

제14조(정보통신망 보안관리) ① 시스템관리자는 업무자료를 소통하기 위한 전산망 또는 기반시설망에 대해 인터넷과 분리되도록 해야하며, 다음 각 호의 보안대책을 강구해야 한다.

1. 비인가자의 업무망·기반시설망 침입 차단대책(침입차단·탐지시스템 등)
2. 비인가 장비의 접속 차단
3. 업무·관리용 PC의 인터넷 접속 차단 대책
4. 업무망·기반시설망에 대한 안전한 자료전송 대책

② 외주직원이 사용하는 망은 내부 업무망 및 인터넷망을 분리하여 운영하여야 한다.

③ 운용중인 정보통신망의 신뢰성을 확보하기 위해 주기적으로 네트워크 취약점 점검, 망간 자료전송시스템 점검, 우회경로 존재여부 점검 등을 수행하여야 한다.

④ 그 밖에 정보통신망 보안관리에 관한 사항은 진흥원「정보보안 기본지침」제3장 제1절 정보통신망 보안관리에 따른다.

제15조(보안성 검토 신청) ① 시스템관리자는 신규 정보시스템 도입 시 분임정보보안담당관을 통해 진흥원 정보보안담당관에게 사전 보안성 검토를 요청해야 한다.

② 시스템관리자는 사전 보안성 검토 결과 도출된 취약점에 대해 보호대책을 적용한 후 운용해야 한다.

③ 시스템관리자는 네트워크 장비 및 정보보호시스템 등의 신규 정보시스템 도입 시 보안적합성 검증을 득한 제품을 우선 도입한다.

④ 그 밖에 보안성 검토에 관한 사항은 진흥원「정보보안 기본지침」제2장 제2절 보안성 검토에 따른다.

제16조(정보시스템 취약점 점검) ① 정보시스템담당자는 정보보안담당자와 협의하여 매년 1회 이상 시스템의 취약점 점검을 수행해야 한다.

② 정보시스템담당자는 취약점 점검 결과에 따라 보안대책을 수립하고, 정보보안담당자의 검토 및 시스템관리자의 승인을 거쳐 시스템에 대책을 적용해야 한다.

제17조(접근통제 기본원칙) ① 시스템관리자는 정보시스템에 대한 안전한 로그온 절차 식별 및 인증관리 등과 같은 시스템 운영체제 접근통제 방법을 수립해 한다.

② 주기적으로 접근통제에 대한 검토를 실시하고 접근통제 정책이 적합한지를 확인해야 한다.

제18조(원격접속 보안관리) 한국인터넷정보센터 내의 모든 정보시스템의 원격접속은 원칙적으로 불허한다. 단, 한국인터넷정보센터 모니터링 등을 위해 필요한 경우 시스템관리자의 승인 하에 인가된 PC에서만 접근 가능하도록 조치해야 한다.

제19조(정보보호시스템 보안) ① 한국인터넷정보센터 네트워크를 외부의 고의적인 해킹 및 사이버테러 공격을 사전에 탐지 및 대응하기 위해, 방화벽, 침입방지시스템(IPS), 웹 방화벽, DDoS 대응장비 등의 보안장비를 설치하여 운영하며, 네트워크 활동을 모니터링 한다.

② 보안 장비는 연 1회 이상 취약점 점검을 실시하여 발견된 취약점을 조치해야 한다.

③ 보안 장비는 개발 또는 판매사가 제공하는 보안업데이트를 적용하여야 한다.

④ 그 밖에 상세한 보안장비 운영 및 보안관한 사항은「한국인터넷정보센터 전산자원 관리 운영 수칙」을 따른다.

제20조(네트워크장비 보안) ① 한국인터넷정보센터의 네트워크장비는 물리적, 논리적 접근통제가 구현된 안전한 곳에 설치 운영한다.

② 네트워크 장비는 연 1회 이상 취약점 점검을 실시하여 발견된 취약점을 조치해야 한다.

③ 네트워크 장비는 개발 또는 판매사가 제공하는 보안업데이트를 실시한다.

④ 그 밖에 상세한 네트워크 장비 보안에 관한 사항은 「한국인터넷정보센터 전산자원 관리 운영 수칙」을 따른다.

제21조(서버 보안) ① 한국인터넷정보센터의 서버는 물리적, 논리적 접근통제가 구현된 안전한 곳에 설치・운영한다. <개정 2023. 12. 28.>

② 삭제 <2023. 12. 28.>

③ 삭제 <2023. 12. 28.>

④ 서버 장비는 연 1회 이상 취약점 점검을 실시하여 발견된 취약점을 조치해야 한다.

⑤ 서버 장비는 개발 또는 판매사가 제공하는 보안업데이트를 적용하여야 한다.

⑥ 그 밖에 상세한 서버 및 PC 보안에 관한 사항은 「한국인터넷정보센터 전산자원 관리 운영 수칙」을 따른다.

제22조(데이터베이스 보안) ① 데이터베이스의 추가, 변경, 삭제 권한은 소수의 인가자로만 제한되도록 운영되어야 한다.

② 시스템관리자는 정보의 중요도에 따라 사용자 접근권한을 부여하고, 모니터링 하여야 한다.

③ 시스템관리자는 사용자별 접속기록을 관리하여야 하며 진흥원「정보보안 기본지침」제55조(로그기록 유지)에 따라 보안대책을 강구하여야 한다.

④ 정보보안담당자는 주기적으로 보안점검을 수행하여야 한다.

제23조(무선랜 보안관리) ① 한국인터넷정보센터 내의 모든 무선랜 사용은 원칙적으로 불허한다.

② 그 밖에 무선랜 보안관리에 관한 사항은 한국인터넷진흥원「정보보안 기본지침」제43조(무선랜 보안)에 따른다.

제23조의2(로그기록 유지) ① 시스템관리자는 한국인터넷정보센터 정보시스템의 통제·관리 및 사고 발생 시 추적 등을 위하여 다음 각 호의 사항이 포함된 로그기록을 1년 이상 보관하여야 한다.

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

② 시스템관리자는 접속기록을 정기적으로 점검하여 비인가자의 접속 시도 등 의심스러운 정황을 발견한 경우 즉시 분임정보보안담당과에게 보고하여야 한다.

③ 그 밖에 로그기록 유지·관리에 관한 사항은 진흥원「정보보안 기본지침」제55조(로그기록 유지)에 따른다.

[본조 신설 2023. 12. 28.]

제 4 절 사용자 보안 관리

제24조(개별사용자 보안) 한국인터넷정보센터의 모든 인원은 PC 등 정보시스템을 사용하거나 정보통신망에 접속하는 행위와 관련하여 스스로 보안책임을 진다.

제25조(단말기 보안) ① 한국인터넷정보센터의 모든 인원은 지급받은 PC·노트북·휴대폰·스마트패드 등의(이하 "단말기"라 한다) 사용과 관련한 일체의 보안관리 책임을 진다.

② 개별사용자는 단말기에 대하여 다음 각 호에 해당하는 보안대책을 준수하여야 한다.

1. CMOS·로그온·자료 암호화 비밀번호의 정기적 변경 사용
2. 단말기 작업을 10분 이상 중단 시 비밀번호 등을 적용한 화면보호 조치
3. 최신 백신 소프트웨어 설치 및 수시 점검 <개정 2023. 12. 28.>
4. 운영체제 및 응용프로그램에 대한 최신 보안패치 유지
5. 출처, 유통경로 및 제작자가 불분명한 응용프로그램의 사용 금지
6. 인터넷을 통해 자료(파일) 획득시 신뢰할 수 있는 인터넷사이트를 활용하고 자료(파일) 다운로드 시 최신 백신 소프트웨어로 검사 후 활용
7. 인터넷 파일공유·메신저·대화방 프로그램 등 업무상 불필요한 프로그램의 설치 금지 및 공유 폴더 삭제
8. 웹브라우저를 통해 서명되지 않은 액티브-X 등이 다운로드·실행되지 않도록 보안 설정
9. 인터넷 PC에서는 특별한 사유가 없는 한 문서 프로그램을 읽기 전용(專用)으로 운용
10. 그 밖에 국가정보원장이 안전성을 확인하여 배포한 프로그램의 운용 및 보안권고문 이행

제26조(계정 관리) ① 정보시스템담당자는 정보시스템 접속에 필요한 사용자계정(ID) 부여 시 비인가자 도용 및 정보시스템 불법 접속에 대비하여 다음 각 호의 사항을 반영하여야 한다.

1. 사용자별 또는 그룹별로 접근권한 부여
2. 외부인에게 계정부여는 불허하되, 업무상 불가피한 경우 시스템관리자의 승인을 받아 필요업무에 한해 특정기간 동안만 접속가능하도록 보안조치한다.
3. 비밀번호 등 사용자 식별 및 인증 수단이 없는 사용자계정 사용 금지
4. 사용자 계정은 개인별 부여 및 관리를 원칙으로 하며, 공용 계정은 사용하지 않는 것을 원칙으로 한다. 단, 업무 특성상 필요한 경우에는 시스템관리자의 승인 하에 사용 가능
5. 동일 계정으로 다중 접속을 차단한다.

② 정보시스템담당자는 사용자의 면직 또는 전보 시 계정을 즉시 삭제하여야 한다.

③ 정보시스템에 접근할 계정이 필요한 경우 다음의 절차를 따라 계정을 생성한다.

1. 사용자는 ID, 사용기간, 접근권한을 명시하여 정보시스템담당자에게 계정 발급을 요청한다.
2. 정보시스템담당자는 검토 후 관리자 권한이 필요하거나 외주직원이 사용하는 경우 시스템관리자에게 승인을 득한 후 계정을 생성한다.
3. 정보시스템담당자는 생성한 계정과 초기패스워드를 사용자에게 통보한다.
4. 사용자는 제27조(비밀번호 관리)에 따라 초기 패스워드를 변경하여야 한다.

④ 사용자 계정의 중지 및 삭제는 다음의 절차를 따른다.

1. 서버 설치 시, 기본적으로 포함되어 있는 초기 계정 중 업무적으로 불필요한 계정은 삭제 또는 비활성화하여야 한다.

2. 장기간 미사용 계정은 확인 후 즉시 삭제한다. 단, 정보시스템 운영상 필요하나 자주 사용하지 않는 계정은 예외로 할 수 있다.

⑤ 정보시스템담당자는 사용자 계정의 부여 및 관리가 적절한지 주기적으로 점검(관리자 계정 3개월, 사용자 계정 6개월)하여 결과를 시스템관리자에게 보고해야 한다.

제27조(비밀번호 관리) ① 사용자는 정보시스템의 무단사용방지를 위하여 단말기 및 업무용 응용프로그램에 안전한 비밀번호를 설정하여야 한다. <개정 2023. 12. 28.>

1. <삭제 2023. 12. 28.>

2. <삭제 2023. 12. 28.>

② 비밀이나 대외비에는 자료별 비밀번호를 반드시 부여하되, 내부 공개 또는 외부공개 자료에는 부여하지 아니할 수 있다.

③ 그 밖에 비밀번호 관리에 관한 사항은 진흥원「정보보안기본지침」제76조(비밀번호 관리)에 따른다.

제28조(전자우편 보안) ① 분임보안담당관은 전자우편을 컴퓨터바이러스·트로이목마 등 악성코드로부터 보호하기 위해 백신 소프트웨어 설치, 해킹메일 차단시스템 구축 등 보안대책을 수립·시행해야 한다.

② 개별사용자는 수신된 전자우편에 포함된 첨부파일이 자동 실행되지 않도록 설정하고 첨부파일을 다운로드할 경우 최신 백신 소프트웨어로 악성코드 감염 여부를 검사해야 한다.

③ 개별사용자는 출처가 불분명하거나 의심되는 제목의 전자우편은 열람하지 말고 해킹메일로 의심될 경우 즉시 분임정보보안담당관과 진흥원 정보보안 담당부서에 신고해야 한다. <개정 2023. 12. 28.>

제29조(휴대용 저장매체 보안) ① 한국인터넷정보센터는 원칙상 휴대용 저장매체를 사용할 수 없다.

② 그 밖에 휴대용 저장매체 보안관리에 관한 사항은 한국인터넷진흥원「정보보안 기본지침」제78조(휴대용 저장매체 보안)에 따른다.

제30조(비인가 기기 통제) ① 개인 소유의 정보통신기기(휴대폰 등 이동통신단말기를 제외한다. 한국인터넷정보센터 내에 무단 반입·사용해서는 안된다. 다만, 부득이한 경우 분임정보보안담당관의 승인을 받은 후 사용할 수 있다.

② 개인 소유의 정보통신기기를 한국인터넷정보센터에서 운용하는 정보통신망에 연결해서는

안되며, 정보보안담당관은 이에 대해 수시로 점검하여야 한다.

③ 분임정보보안담당관은 개인 소유의 정보통신기기가 업무자료를 외부로 유출하는데 악용될 수 있거나 한국인터넷정보센터 정보통신망 운영에 위해가 된다고 판단될 경우 반출·입 통제 등 보안대책을 수립·시행해야 한다.

제31조(악성코드 감염 방지대책) ① 시스템관리자는 사용자에 대하여 웜·바이러스, 악성프로그램, 스파이웨어 등 악성코드 감염을 방지하기 위한 대책을 강구해야 한다.

② 그 밖에 악성코드 감염 방지대책에 관한 사항은 한국인터넷진흥원 「정보보안 기본지침」제80조(악성코드 감염 방지대책)에 따른다.

제 5 절 융합 보안

제32조(정보통신시설 보호대책) 보호지역으로 지정된 정보통신시설 및 장소에 대한 보안대책을 수립하고자 할 경우 다음 각 호에 해당하는 사항을 포함하여야 한다.

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

제33조(영상정보처리기기 보안관리) ① 영상정보처리기기 운용에 필요한 카메라, 관리용 PC 등 관련 시스템은 물리적으로 안전한 장소에 설치해야 한다.

② 정보보안담당자는 영상정보처리기기 설치 시 업무망 및 인터넷망과 분리 운영하는 것을 원칙으로 한다. 다만, 부득이하게 인터넷망을 이용할 경우에는 전송내용을 암호화하여야 한다.

③ 영상정보처리기기 관리시스템은 사용자계정·비밀번호 등 시스템 인증대책을 강구하고 허용된 특정 IP에서만 접속 허용하는 등 비인가자의 침입 통제대책을 강구하여야 한다.

④ 정보보안담당자는 제1항부터 제4항까지와 관련하여 보안대책의 적절성을 수시로 점검하고 개선해야 한다.

제3장 주요정보통신기반시설 관리

제34조(기반시설 관리) 한국인터넷정보센터 내 정보통신기반보호법에 따라 주요정보통신기반시설로 지정된 장비는 진흥원「정보보안기본지침」제82조(주요정보통신기반시설 지정· 보호)에 따른다.

제35조(취약점 분석 · 평가) 기반시설로 지정된 시스템은 정보통신기반 보호법 제9조에 따라 매년 1회 취약점 분석 · 평가를 실시하고, 주요정보통신기반시설 보호대책을 작성하여 관계부처에 제출한다.

제4장 침해사고 대응

제36조(침해사고 대응) ① 시스템관리자는 네트워크를 통한 침해시도 및 기타 시스템의 안전성에 관하여 의심이 가는 활동을 발견한 즉시 분임정보보안담당관 또는 분임보안담당관에게 보고해야 한다.

② 한국인터넷정보센터의 중요 시스템이 해킹되었을 때는 즉시 시스템을 네트워크에서 분리조치하고 디지털 증거를 확보한다.

③ 중요 시스템 등의 해킹사고 발생 시 인터넷침해대응센터 등 유관부서 및 기관에 해킹사고, 악성코드 등에 대한 분석 및 협조를 요청한다.

④ 그 밖에 상세한 침해사고 대응절차에 관한 사항은「한국인터넷정보센터 사이버공격 대응수칙」을 따른다.

제5장 재난 대응

제37조(재난대응) ① 한국인터넷정보센터는 각종 재난 및 비상 상황으로부터 인명을 보호하고, 인터넷 주소자원 서비스의 안정적 제공을 위하여 다음 각 호를 고려하여 상황별 대책을 수립한다.

1. 비상 조직 구성 및 역할
2. 상황 보고, 공지 절차 등 비상 대응 절차
3. 회복 방법

4. 대피 방법 및 절차 등 인명 보호 방법

② 수립한 대책은 연 1회 이상 검토한다.

③ 그 밖에 재난대응 대책 및 절차에 관한 사항은 「한국인터넷정보센터 업무연속성 관리 및 비상시 대응수칙」을 따른다.

제38조(정보시스템 백업 체계) ① 정보시스템의 비상 상황 대응을 위하여 백업체계를 운영한다.

② 백업체계 대상 정보시스템은 중요 정보시스템을 우선 선정하며, 평가는 한국인터넷정보센터「한국인터넷정보센터 전산자원 관리 운영 수칙」을 따른다.

제39조(훈련 및 교육) 재난 및 비상 상황에 대비한 훈련 또는 교육을 연 1회 이상 실시한다.

제40조(비상연락체계 현행화) ① 각종 재난 및 비상 상황으로부터 신속한 대응을 위하여 다음 각 호를 고려한 비상연락체계를 구축하고, 이를 최신의 상태로 유지한다.

1. 주무부처 및 유관기관
2. 진흥원 내 관련 부서
3. 의료기관, 소방기관
4. 유지관리 협력업체 등

제6장 기타

제41조 <삭제 2023. 12. 28.>

부 칙<2015. 7. 14>

이 지침은 경영기획본부장의 승인 받은 날부터 시행한다.

부 칙<2017. 4. 13>

이 지침은 경영기획본부장의 승인 받은 날부터 시행한다.

부 칙<2018. 12. 28>

이 지침은 경영기획본부장의 승인 받은 날부터 시행한다.

부 칙<2020. 1. 31>

이 지침은 경영기획본부장의 승인 받은 날부터 시행한다.

부 칙<2021. 2. 25>

이 지침은 경영기획본부장의 승인 받은 날부터 시행한다.

부 칙<2022. 1. 27>

이 지침은 경영기획본부장의 승인 받은 날부터 시행한다.

부 칙<2022. 12. 23>

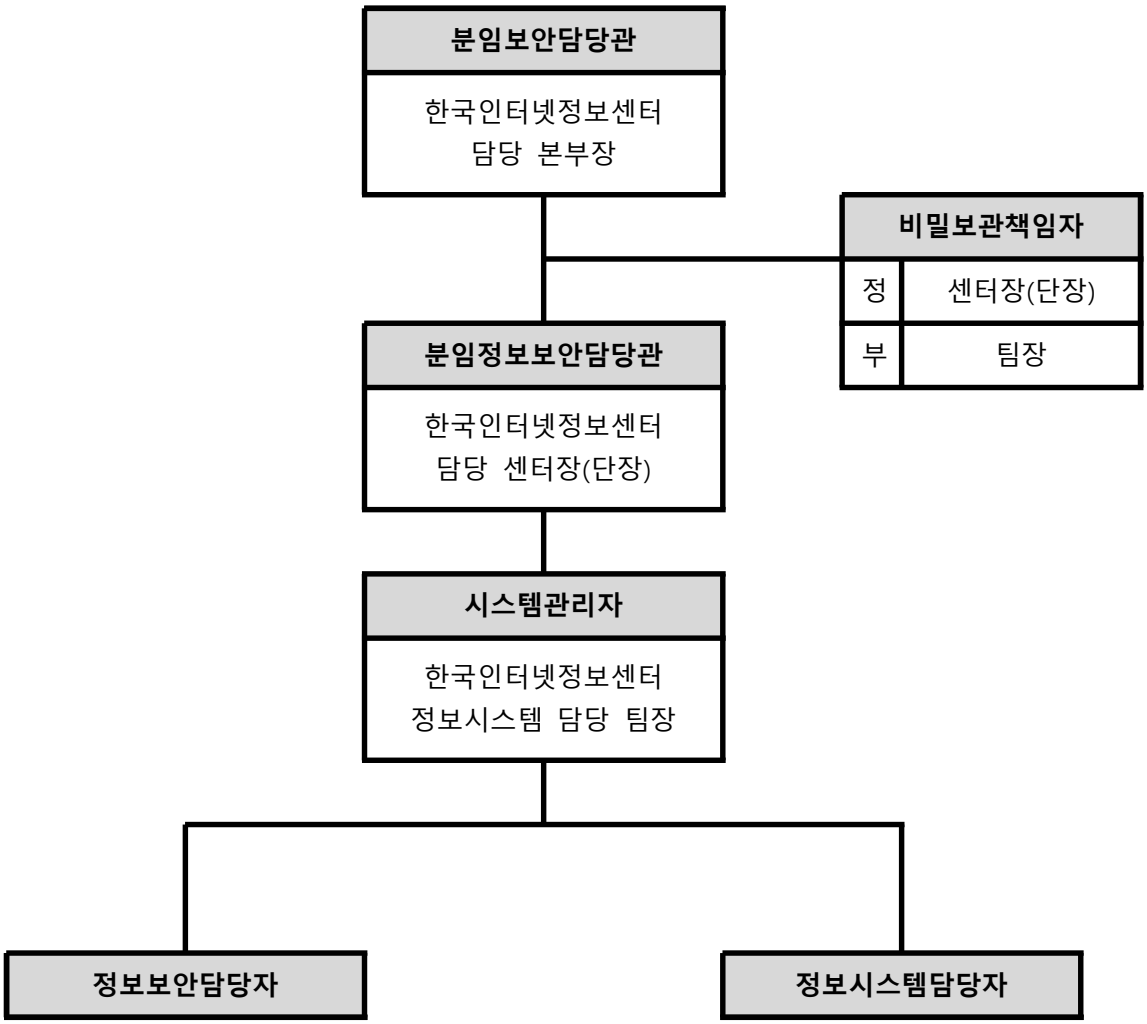
이 지침은 경영기획본부장의 승인 받은 날부터 시행한다.

부 칙<2023. 12. 28>

이 지침은 경영기획본부장의 승인 받은 날부터 시행한다.

[별표 1호] <개정 2022. 12. 23.>

한국인터넷정보센터 보안업무내부감독체제



[별지 제1호 서식]<개정 2022. 12 23.>

한국인터넷정보센터 출입자 보안서약서

본인은 한국인터넷진흥원(이하 “진흥원”) 한국인터넷정보센터(“이하 센터”) 출입 시 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 센터 출입 중 취득한 제반사항을 업무 수행 중은 물론 복귀 후에도 일체 누설하지 않을 것을 서약합니다.

2. 본인은 센터 출입 중 취득한 제반사항을 누설하였을 때는 동기여하를 막론하고 그 결과에 대한 제반 법규에 의거하여 엄중한 처벌을 받을 것을 서약합니다.

3. 본인은 업무상 고의 또는 중대 과실로 인해 진흥원 및 센터에 재산상 손해를 끼쳤을 경우에 그에 대한 형사 및 민사상 책임을 집니다.

< 개인정보 수집·이용 >

o 수집하는 개인정보 항목 : 소속, 전화번호, 성명

o 개인정보 수집·이용 목적 : 한국인터넷정보센터 출입자 신원 확인, 업무상 취득한 사실에 대한 비밀유지 서약, 보안사고·테러 등 발생 시 경위 파악

o 보유 및 이용기간 : **3년**

o 개인정보 수집 및 이용 동의를 거부할 권리가 있습니다.
다만, 동의를 거부할 경우 진흥원「보안업무규칙」,「한국인터넷정보센터 정보보안지침」에 따라 센터 출입이 불가합니다.

▷ 개인정보 수집·이용에 동의 여부 : 동의 □ 미동의 □

년 월 일

서약자 소 속 :

전화번호 :

성 명 : (서명)

[별지 제2호 서식] <삭제 2022.12.23.>

[별지 제3호 서식]<개정 2022.12.23.>

한국인터넷정보센터 장비 반입·반출증

구분	반입·반출	소속 서비스	
일시	20 년 월 일 시 분	(반입시) 반출예정일	년 월 일
목적			

제조사 및 모델명	장비 일련번호	호스트명	KISA자산번호	상면 위치	사이즈(U)	전원		비고
						A	B	

□ **유의사항**

o 반입시 백신 점검, 반출시 데이터 삭제를 확인하였음.

o 저장장치(HDD, SDD 등) 반출 금지

반입·반출	구분	반입·반출자	KISA담당자
	성명		
	소속		

확인	운영실	센터 담당자