인터넷침해대응센터 정보보안지침

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

제 1 장 총 칙

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

제2조(적용범위) ① 이 지침은 인터넷침해대응센터의 전 직원 및 외주직원에게 적용한다.
② 인터넷침해대응센터의 정보보안 업무는 진흥원의 「보안업무규칙」, 「정보보안기본지침」에서 정한 사항을 제외하고는 이 지침에서 정한 바에 따른다.

제3조(정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. “인터넷침해대응센터“라 함은 정보통신망 이용촉진 및 정보보호 등에 관한 법률 48조의 2(침해사고의 대응 등)를 원활하게 수행하기 위해 침해사고대응업무를 수행하는 곳으로 인터넷침해대응시스템 전산실 및 종합상황실로 구성되어 있다.
2. “인터넷침해대응시스템”이라 함은 국내 ISP의 정보수집개소에서 받는 정보를 가공, 처리하여 국내 인터넷침해 관련 정보를 수집, 저장, 처리하는 데 필요한 시스템으로 네트워크 장비, 보안장비 및 데이터 처리 시스템 등으로 구성되어 있다.
3. “종합상황실”이라함은 인터넷침해대응시스템에서 처리한 정보를 전자적으로 출력하여 국내 인터넷침해상황을 종합적으로 관제 및 대응하는 시설을 말한다.
4. “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.<신설 2022.12.23.>

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 전자기록물의 보안

마.「국가사이버안전관리규정」제2조제3호에 따른 사이버안전

5. “외주”란 “외주업체” 또는 외주직원“을 말한다.

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

7. "외주직원"이란 인터넷침해대응센터의 정보자산을 이용하여 서비스와 기타 업무를 대행하는 자를 말하며, 아래와 같이 구분한다.

1) 상주

2) 비상주

8. “보호지역”이란 통제구역 및 제한구역을 말한다.

9. “통제구역”이란 인터넷침해대응센터의 정보보안을 위해 매우 중요한 구역으로서 비인가자의 출입이 금지되는 구역을 말한다.<개정 2022.12.23.>

10 “제한구역”이란 인터넷침해대응센터의 사무공간에 대한 외부인의 접근을 방지하기 위해 출입의 안내가 요구되는 지역을 말한다.

11. “정보시스템 자산”이라 함은 인터넷침해대응센터에서 운영하는 정보시스템, 네트워크장비, 보안장비 및 프린터 등을 말한다.

12. “소프트웨어 자산”이라 함은 인터넷침해대응센터에서 자체 개발한 응용프로그램, 소스코드, 운영체제 및 응용프로그램 등의 소프트웨어를 말한다.

13. “정보 자산”이라 함은 인터넷침해대응시스템에서 처리하는 침해사고 정보, 데이터베이스, 감사기록 및 백업기록 등의 정보를 말한다.

14. “문서 자산”이라 함은 업무지침서, 운영지침서, 문서관리대장, 백업관리대장, 보고서, 기록문서 등을 말한다.

15. “설비 자산”이라 함은 항온항습기, 방범장치, 출입통제설비 및 무정전 전원공급장치 등의 설비를 말한다.

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

1. 인터넷침해대응센터 소속직원의 보안업무 수행에 관한 교육 및 감독
2. 인터넷침해대응센터의 각 종 보안 침해사고 예방 및 조치
3. 인터넷침해대응센터 시설 보안 및 안전 관리
4. 인터넷침해대응센터 비밀문서의 관리
5. 업무수행 상 보안을 요하는 사항의 협조

6. 기타 인터넷침해대응센터의 보안업무 관련 사항

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

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

③ 정보시스템관리자는 분임정보보안담당관을 보좌하고, 인터넷침해대응시스템의 전산자원 관리 업무를 수행하는 팀의 팀장이 하며, 다음 각 호의 업무를 수행한다.<개정 2023. 12. 28.>

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 운영ㆍ보안 관리

④ 정보보안담당자는 정보시스템관리자에 의해 임명된 직원으로 분임정보보안담당관을 보좌하여인터넷침해대응센터의 정보보안 실무를 수행하며, 다음 각 호의 업무를 수행한다.<개정 2023. 12. 28.>

1. 정보보안 관련 법규 및 지침의 제·개정 소요 검토
2. 자체 모의 훈련 계획 수립ㆍ시행 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 정보시스템운영담당자는 정보시스템관리자에 의해 임명된 직원으로 서버, 네트워크, 보안장비 등의 각 정보시스템을 운영·관리하며, 다음 각 호의 업무를 수행한다.<개정 2023. 12. 28.>

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 인터넷침해대응센터 직원 개인은 부여된 업무와 관련하여 보안책임을 진다.

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

제6조(비밀유지의무) ① 인터넷침해대응센터 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) 정보시스템관리자는 다음 각 호에 해당하는 정보통신망 관련 현황·자료를 대외비에 준하여 관리해야 한다.<개정 2023. 12. 28.>

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(자산 분류) 인터넷침해대응센터의 자산은 자산의 종류에 따라 정보시스템 자산, 소프트웨어 자산, 정보 자산, 문서 자산 및 설비 자산으로 분류한다.

제9조(자산 관리) ① 정보시스템관리자는 자산의 중요도를 평가하여 자산의 등급과 유형에 따른 관리 및 보호를 해야한다.<개정 2023. 12. 28.>

② 정보시스템관리자는 분류된 자산에 대해 “자산 관리대장”을 작성하고 각 자산에 대해 관리번호, 책임자, 담당자, 운영자, 사용자 현황을 관리해야 한다.<개정 2023. 12. 28.>

③ 신규도입 및 폐기 등 자산의 변동사항이 발생할 경우 정보시스템관리자에게 승인을 받아 변경사항을 기록하여 최신화해야 한다.<개정 2023. 12. 28.>

④ 자산의 반ㆍ출입 이력은 “자산 반ㆍ출입 관리대장”을 통해 관리하고 분기 1회 이상 자산의 반ㆍ출입 이력을 확인해야 한다.

제 2 절 물리적 보안 관리

제10조(보호지역의 설정) 진흥원 보안업무규칙 제49조(보호지역의 설정 및 관리)에 따라 인터넷침해대응센터는 제한구역으로 설정하고 전산실, 종합상황실을 통제구역으로 설정한다.

제11조(보호지역의 보호조치) ① 출입통제 및 감시를 위해 출입통제시스템(카드키, 정맥인식),

감시 카메라 등을 설치한다.
② 진흥원 「보안업무규칙」제50조(보호지역의 보호대책)에 의거, 보호지역에 따라 제한구역 또는 통제구역 표시를 해야한다.
③ 통제구역 출입에 대한 접근권한을 주기적으로 점검하고, 정보시스템관리자에게 보고해야 한다.<개정 2023. 12. 28.>
④ 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.
⑤ 통제구역 내부에서 사전 승인을 득하지 않은 사진 및 동영상 촬영을 금지한다.

제12조(보호지역의 출입통제) ① 인터넷침해대응센터는 다음 각 호에 해당하는 경우에만 출입을 허용한다.

1. 인터넷진흥원 내부직원 중 인터넷침해대응센터 관련 업무 수행자
2. 출입인가를 받은 외주직원(청소대행업체, 공사업체 및 납품업체, 유지보수업체 직원 등)
3. 사전 승인을 받은 종합상황실 방문자(유지보수 등)
4. 그 밖에 분임보안담당관이 필요하다고 인정하는 자

② 통제구역 상시출입권한은 다음 각 호에 따르며, 직책 및 직무 변경 시 즉시 출입권한을 제거하고, 정보시스템관리자는 매월 출입자 명부를 검토하여 불필요한 권한이 있는지 확인한다.<개정 2023. 12. 28.>

1. 종합상황실 : 인터넷진흥원 내부 팀장급 이상 보직자, 인터넷침해대응센터 직원, 상주 외주 인력
2. 전산실 : 인터넷침해대응센터내 정보시스템관리자/담당자 및 외부 상주 용역업체 인력 <개정 2023. 12. 28.>

③ 통제구역을 출입하는 외주직원은 다음 각 호와 같이 관리한다.

1. 상주 직원은 최초 출입 시 보안준수 서약서(별지 제1호 서식)를 정보시스템관리자에게 제출한다.<개정 2023. 12. 28.>
2. 비상주 직원은 출입할 때마다 보안준수 서약서(별지 제1호 서식)를 작성하여 정보시스템관리자에게 제출하고, 통제구역 출입자 명부(별지 제2호 서식)에 출입기록을 작성해야 한다. <개정 2023. 12. 28.>

④ 종합상황실을 방문하고자 하는 자는 종합상황실 방문 신청서(별지 제3호 서식)를 작성하며, 종합상황실 관리팀장의 사전 승인을 얻은 후 직원의 안내를 받아 출입해야 한다.
⑤ 인터넷침해대응센터의 작업을 수행하기 위해 방문하는 경우에는 작업계획 및 완료보고서(별지 제4호 서식)를 작성한다.

제 3 절 기술적 보안 관리

제13조(정보통신망 보안관리) ① 정보시스템관리자는 업무자료를 소통하기 위한 전산망 또는 기반시설망에 대해 인터넷과 분리되도록 해야하며, 다음 각 호의 보안대책을 강구해야 한다.<개정 2023. 12. 28.>

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」제1절 정보통신망 보안관리에 따른다.

제14조(보안성 검토 신청) ① 정보시스템관리자는 신규 정보시스템 도입 시 분임정보보안담당관을 통해 진흥원 정보보안담당관에게 사전 보안성 검토를 요청해야 한다.<개정 2023. 12. 28.>
② 정보시스템관리자는 사전 보안성 검토 결과 도출된 취약점에 대해 보호대책을 적용한 후 운용해야 한다.<개정 2023. 12. 28.>
③ 정보시스템관리자는 네트워크 장비 및 정보보호시스템 등의 신규 정보시스템 도입 시 보안 적합성 검증을 득한 제품을 우선 도입한다.<개정 2023. 12. 28.>
④ 그 밖에 보안성 검토에 관한 사항은 진흥원「정보보안 기본지침」제2절 보안성 검토에 따른다.

제15조(보안장비 운영) ① 침해사고대응시스템 및 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 보안장비 운영 및 보안관리에 관한 사항은「보안장비관리지침서」를 따른다.

제16조(네트워크장비 운영) ① 인터넷침해대응센터의 네트워크장비는 물리적, 논리적 접근통제가 구현된 안전한 곳에 설치 운영한다.
② 네트워크장비 운영 및 보안관리에 관한 사항은 「네트워크장비관리지침서」를 따른다.

제17조(서버 운영) ① 인터넷침해대응센터의 서버는 물리적, 논리적 접근통제가 구현된 안전한 곳에 설치·운영한다.
② 서버를 관리하는 PC는 외부 인터넷망 접속을 차단하고, 불필요한 프로그램 및 서비스를 삭제한 후 사용한다.

③ 윈도 계열의 서버 및 PC는 안티 바이러스 프로그램을 설치·운영한다.
④ 그 밖에 서버 및 PC 보안에 관한 사항은 「서버보안관리지침서」를 따른다.

제18조(무선랜 보안관리) 인터넷침해대응센터내의 모든 무선랜 사용은 원칙적으로 불허하며, 부득이하게 필요한 경우 분임보안담당관의 승인하에 진흥원「정보보안 기본지침」제43조(무선랜 보안)범위 내애서 운용한다.

제 4 절 사용자 보안 관리

제19조(개별사용자 보안) 인터넷침해대응센터의 모든 인원은 PC 등 정보시스템을 사용하거나 정보통신망에 접속하는 행위와 관련하여 스스로 보안책임을 진다.

제20조(단말기 보안) ① 인터넷침해대응센터의 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 및 침입차단·탐지시스템 등 운용 및 수시 점검
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

제21조(계정 관리) ① 정보시스템운영담당자는 정보시스템 접속에 필요한 사용자계정(ID) 부여 시 비인가자 도용 및 정보시스템 불법 접속에 대비하여 다음 각 호의 사항을 반영하여야 한다.<개정 2023. 12. 28.>

1. 사용자별 또는 그룹별로 접근권한 부여
2. 외부인에게 계정부여는 불허하되, 업무상 불가피한 경우 정보시스템관리자의 승인을 받아 필요업무에 한해 특정기간 동안만 접속가능하도록 보안조치한다.<개정 2023. 12. 28.>
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 정보시스템관리자의 승인 하에 사용 가능 <개정 2023. 12. 28.>

5. 동일 계정으로 다중 접속을 차단한다.

② 정보시스템운영담당자는 사용자의 면직 또는 전보 시 계정을 즉시 삭제하여야 한다.<개정 2023. 12. 28.>

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

1. 사용자는 ID, 사용기간, 접근권한을 명시하여 정보시스템운영담당자에게 계정 발급을 요청한다.<개정 2023. 12. 28.>

2. 정보시스템운영담당자는 검토 후 관리자 권한이 필요하거나 외주직원이 사용하는 경우 정보시스템관리자에게 승인을 득한 후 계정을 생성한다.<개정 2023. 12. 28.>

3. 정보시스템운영담당자는 생성한 계정과 초기패스워드를 사용자에게 통보한다.<개정 2023. 12. 28.>

4. 사용자는 제22조(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 정보시스템운영담당자는 사용자 계정의 부여 및 관리가 적절한지 분기 1회 점검하여 결과를 정보시스템관리자에게 보고해야 한다.<개정 2023. 12. 28.>

제22조(비밀번호 관리) ① 비밀번호는 해당 업무의 담당자만이 알고 있어야 하며, 분기별 1회 변경하여 사용한다.

② 비밀번호는 해당 업무의 담당자가 기록하여 보안금고에 안전하게 관리하여야 한다.

③ 비밀번호는 다음 각 호에 해당하는 사항을 충족하여야 한다.

1. 숫자와 영문자, 특수문자 등을 혼합하여 9자리 이상을 부여할 것

2. 사용자계정과 동일하지 않을 것

3. 일반사전에 등록된 단어의 사용을 피할 것

4. 조직 관련명칭, 연속된 숫자 또는 문자 등의 사용을 피할 것

5. 수첩, 노트에 기록하는 등 문서화 금지

6. USB, 공유 디렉토리 등의 저장매체에 보관 금지

7. 통신매체 또는 온라인매체를 통한 공개 금지

④ 그 밖에 비밀번호 관리에 관한 사항은 진흥원「정보보안기본지침」제76조(비밀번호 관리)에 따른다.

제23조(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 분임정보보안담당관에게 신고해야 한다. 분임정보보안담당관은 해킹메일로 판단될 경우 분임보안담당관과 진흥원 정보보안팀에 보고하여 지시에 따라 조치한다.<개정 2023. 12. 28.>

제24조(휴대용 저장매체 보안) ① 인터넷침해대응센터는 원칙상 휴대용 저장매체를 사용할 수 없다.
② 그 밖에 휴대용 저장매체 보안관리에 관한 사항은 한국인터넷진흥원「정보보안 기본지침」 제78조(휴대용 저장매체 보안)에 따른다.

제25조(비인가 기기 통제) ① 개인 소유의 정보통신기기(휴대폰 등 이동통신단말기를 제외한다. 를 인터넷침해대응센터 내에 무단 반입·사용해서는 안된다. 다만, 부득이한 경우 분임정보보안담당관의 승인을 받은 후 사용할 수 있다.
② 개인 소유의 정보통신기기를 인터넷침해대응센터에서 운용하는 정보통신망에 연결해서는 안되며, 정보보안담당관은 이에 대해 수시로 점검하여야 한다.
③ 분임정보보안담당관은 개인 소유의 정보통신기기가 업무자료를 외부로 유출하는데 악용될 수 있거나 인터넷침해대응센터 정보통신망 운영에 위해가 된다고 판단될 경우 반출·입 통제 등 보안대책을 수립·시행해야 한다.

제26조(악성코드 감염 방지대책) ① 분임정보보안담당관은 웜·바이러스, 해킹프로그램, 스파이웨어, 랜섬웨어 등 악성코드 감염을 방지하기 위해 다음 각 호의 대책을 수립·시행해야 한다.

1. 사용자는 개인PC의 운영체제, 응용프로그램 및 백신 프로그램의 보안패치 등 최신상태로 유지한다.
2. 백신은 실시간 감시 기능을 활성화하고, 주기적으로 검사를 실시해야 한다.
3. 사용자는 출처, 유통경로 및 제작자가 명확하지 않은 응용프로그램 사용을 금지한다.
4. 사용자는 인터넷 파일공유 프로그램과 메신저·대화방 프로그램 등 업무상 불필요한 프로그램 사용을 금지하고 정보시스템관리자는 침입차단시스템 등에서 업무와 관련 없는 사이트 접속을 차단하도록 보안정책을 설정해야 한다.<개정 2023. 12. 28.>
5. 사용자는 웹브라우저를 통해 서명되지 않은(Unsigned) Active-X 등이 PC내에 불법 다운로드되고 실행되지 않도록 보안설정을 해야 한다.
6. 제1호부터 제5호까지의 보안대책과 관련하여 분임정보보안담당관은 사용자가 적용할 수

있는 보안기술을 지원해야 한다.

② 악성코드가 설치되거나 감염된 사실을 발견하였을 경우 다음 각 호의 조치를 한다.

1. 악성코드 감염원인 규명 등을 위하여 파일은 임의삭제 등 감염 시스템 사용을 중지하고 전산망과의 접속을 분리한다.
2. 악성코드의 감염확산 방지를 위해 진흥원 정보보안팀에 관련 내용 및 보안조치 사항을 즉시 신고한다.

제 5 절 융합 보안

제27조(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

제28조(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

제29조(기반시설 관리) 인터넷침해대응시스템 중 정보통신기반보호법에 따라 주요정보통신기반시설로 지정된 장비는 진흥원「정보보안기본지침」제82조(주요정보통신기반시설 지정·

보호)에 따른다.

제30조(취약점 분석ㆍ평가) 기반시설로 지정된 시스템은 정보통신기반 보호법 제9조에 따라 매년 1회 취약점 분석ㆍ평가를 실시하고, 주요정보통신기반시설 보호대책을 작성하여 관계부처에 제출한다.

제4장 침해사고 대응

제31조(침해사고 대응) ① 정보시스템관리자는 네트워크를 통한 침해시도 및 기타 시스템의 안전성에 관하여 의심이 가는 활동을 발견한 즉시 분임정보보안담당관 또는 분임보안담당관에게 보고해야 한다.<개정 2023. 12. 28.>
② 인터넷침해대응시스템에 대한 침해사고 발생 시 즉시 시스템을 네트워크에서 분리조치하고 디지털 증거를 확보한다.
③ 그 밖에 침해사고 대응에 관한 사항은 「인터넷침해대응센터 침해사고대응 업무지침서」 및 「침해사고대응지침서」를 따른다.<개정 2022.12.23.>

제5장 침해사고 분석

제32조(침해사고 분석) ① 분석가는 해킹사고, 악성코드, 취약점 분석을 위한 전용 분석 PC(“이하 분석 PC”)에서만 분석업무를 수행한다.
② 분석 PC는 분석을 위한 별도의 가상환경을 구축하여야 한다.
③ 분석 PC는 외부 인터넷 망을 이용하고, VPN 등을 통해 내부망 또는 업무PC에 연결하지 않는다.
④ 분석 PC에서는 업무용 이메일 열람, 결재 등 행정업무를 수행하지 않는다.
⑤ 분석이 완료된 후에는 사용했던 분석용 가상환경을 초기화하고, 분석 PC에서 분석 결과물들을 삭제하여야 한다.
⑥ 그 밖에 침해사고 분석에 관한 사항은 「인터넷침해대응센터 침해사고대응 업무지침서」 및 「침해사고분석업무지침」을 따른다.<개정 2022.12.23.>

제33조(분석보안 관리 감독) ① 분임보안담당관은 해킹사고, 악성코드, 취약점 분석 업무를 총괄하는 부서의 팀장을 분석보안 관리 팀장으로 지정한다.
② 분석보안 관리 팀장은 인터넷침해대응센터「정보보안지침」제30조를 준수할 수 있도록 관리 감독을 수행한다. <개정 2018. 12. 28>

제6장 재난 대응

제34조(재난대응) ① 인터넷침해대응센터는 화재, 지진 등 각종 재난 및 재해로부터 인명 피해를 최소화하고 침해사고대응 업무의 연속성을 보장하기 위하여 다음 각 호가 포함된 재난 대비 대책을 수립하여 시행한다.

1. 재난대응팀 구성
2. 재난 시 인명 대피 및 구조책
3. 재난대응 훈련 계획
4. 사업연속성 확보 계획 등

② 그 밖에 재난대응에 관한 사항은 「인터넷침해대응센터 침해사고대응 업무지침서」 및 「재난대응지침서」를 따른다.<개정 2022.12.23.>

제35조(백업센터 운영) 인터넷침해대응센터는 침해사고대응 업무의 지속성, 안전성 및 신뢰성을 보장하기 위해 백업센터를 운영한다.

제36조(백업) ① 인터넷침해대응시스템의 중요 자료를 주기적으로 백업해야 한다.

② 인터넷침해대응센터는 안전한 백업을 위하여 백업절차서를 작성하고 준수하여야 한다.

③ 백업절차서는 백업의 대상 및 절차를 포함하여야 한다.

④ 백업한 자료는 월 1회 인터넷침해대응센터 및 백업센터에 보관한다.

제37조(비상연락체계 현행화) ① 각종 재난 및 비상 상황으로부터 신속한 대응을 위하여 다음 각 호를 고려한 비상연락체계를 구축하고, 이를 최신의 상태로 유지한다. <개정 2018. 12. 28>

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

제7장 기타

제38조(감사 기록) 인터넷침해대응센터는 아래의 기록에 대해서 감사기록을 저장하며, 1년 이상 보관한다.

1. 네트워크 장비 통신 로그

2. 보안장비 통신 로그
3. 시스템 로그인 계정 접속 로그

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. 12. 23.>

이 지침은 경영기획본부장의 승인 받은 날부터 시행한다.

부 칙<2023. 12. 28.>

이 지침은 경영기획본부장의 승인 받은 날부터 시행한다.

[별지 제1호 서식]

보안준수 서약서

본인은 인터넷침해대응센터를 용무로 출입하게 되어 인터넷침해대응센터 내의 각 시설물 및 업무상 지득한 사실에 대하여 비밀을 준수할 것이며, 규정 위반 시에는 민·형사상 및 보안상의 책임과 관계법규에 의한 조치에 따를 것을 서약합니다.

년 월 일

소 속 :

직 위 :

성 명 : (서명)

한국인터넷진흥원장 귀하

[별지 제2호 서식]

통제구역 출입자 명부

담 당	팀 장

연월일	출입자			출입 및 퇴실 시간	용무	입회자		신원확인	비고
	소속	직급	성명			성명	서명		
. .				~					
. .				~					
. .				~					
. .				~					
. .				~					
. .				~					
. .				~					
. .				~					
. .				~					
. .				~ ~					

[별지 제3호 서식]

종합상황실 방문 신청서

(KrCERT/CC Information Security Clearance Form)

담 당	팀 장

방문희망일시 (Date and Time of Visit)			방문기관명 (Organization)		
인솔자 성명 (Name of Representative)		인솔자 기관명 (Representative Organization)		연락처 (전화/이메일) (TEL/E-mail)	
방문 목적 (Purpose of Visit)					
요청 사항 (Additional Request)					

방문자 정보(Visitor's information)

성명 (Name)	국적 (Nationality)	소속기관/직책 (Organization/Position)	이메일 (E-mail)	전화번호 (Phone number)

위와 같이 귀 진흥원을 용무로 출입하게 되어 진흥원내의 각 시설물 및 업무상 지득한 사실에 대하여 비밀을 준수할 것이며 규정 위반 시에는 민·형사상 및 보안상의 책임과 관계법규에 의한 조치에 따를 것을 서약합니다.

Date : 년 월 일

작성자 성명**(Name)** : _____(서명)

[별지 제4호 서식]

작업계획 및 완료보고서

작성일	년 월 일 요일	**작성자**			
작업분류	서버 / DB / 네트워크 / 시스템 App / 응용 App / 기반시설 / 기타		**작업 코드**		
작업구분	정기점검 / 수시점검 / 장애처리 / 시스템 변경 / 네트워크 변경 / 기반시설 변경 / 기타				
작업제목					
작업일시		**예상 소요시간**			
KISA 담당자					
업체 담당자					
관련대상 및 영향범위	□ o ※				
작업진행 및 확인 작업	□ o 1. 1)				
검토의견사항					
관련문서					
결재자	(인)				