정보보안지침

제정 2023.12.05 지침 제459호

지침 제459호 정보보안지침

목 차

지침 제459호 정보보안지침

지침 제459호 정보보안지침

제1장 총칙

제1조(목적) 이 지침은 국가정보원의 「국가 정보보안 기본지침」(이하 「기본지침」이라 한다), 「외교부 정보통신보안지침」(이하 「통신보안지침」이라 한다)에 따라 한국국제교류재단(이하 "재단"이라 한다) 정보보안에 관한 세부사항을 정함을 목적으로 한다.

제2조(적용범위) 재단의 정보보안 업무는 「기본지침」, 「통신보안지침」, 그 밖에 정보보안 관계 법령, 정관 및 규정에서 정한 사항을 제외하고는 이 지침에서 정한 바에 따른다.

제3조(정의) ① 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. "직원등"이라 함은 재단에 재직 중인 임직원을 말한다.
2. "개별사용자"라 함은 이사장으로부터 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 직원등과 이사장과 계약에 의해서 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 사람을 의미한다.
3. "정보통신망"이라 함은 전기통신설비와 컴퓨터의 이용기술을 활용하여 정보를 수집, 가공, 저장, 검색, 송·수신하는 정보통신체제를 말한다.
4. "정보통신실"이라 함은 서버·스위치·라우터·교환기 등 전산 및 통신장비 등이 설치·운용되는 장소 또는 전산실·통신실·데이터센터 등을 말한다.
5. "보안관제"라 함은 사이버공격을 실시간으로 즉시 탐지 및 분석, 대응하는 일련의 활동을 말한다.
6. "취약점"이라 함은 사이버공격에 악용되어 관리자가 설정한 접근 권한 외 정보를 열람·취득하게 하거나 보안기능을 회피 가능하게 하는 정보통신망·정보시스템의 결함을 말한다.
7. "정보시스템"이라 함은 재단의 정보를 수집, 가공, 저장, 검색, 송·수신하는 등의 활용과 관련된 기기와 소프트웨어의 조직화된 체계를 말한다.
8. "정보보호시스템"이라 함은 「지능정보화 기본법」 제2조제15호에 따른 정보보호시스템을 말한다.
9. "비밀"이라 함은 누설될 경우 국가안전보장에 해를 끼칠 우려가 있는 정보를 말한다.
10. "대외비"라 함은 비밀 외에 「공공기관의 정보공개에 관한 법률」 제9조제1항 제3호부터 제8호까지의 비공개 대상 정보 중 직무 수행상 특별히 보호가 필요한 정보를 말한다.
11. "업무자료"라 함은 다음 각 목의 어느 하나에 해당하는 것을 말한다.
    가. 재단의 업무와 관련하여 생산하거나 접수한 문서·도서·대장·카드·도면·시청각물·전자문서 등 모든 형태의 기록정보 자료

    나. 재단의 직원 등이 직무상 작성·취득하였거나 보유·관리하는 자료로서 전자적으로 처리되어 부호·문자·음성·음향·영상 등으로 표현된 것
12. "비공개 업무자료"라 함은 「공공기관의 정보공개에 관한 법률」 제9조 비공개 대상 정보가 포함된 자료를 말한다.
13. "공개 업무자료"라 함은 업무자료 중에서 비밀 및 대외비, 비공개 업무자료를 제외한 모든 자료 또는 정보(「공공데이터의 제공 및 이용 활성화에 관한 법률」 제19조에 따라 공표된 공공데이터를 포함한다)를 말한다.
14. "정보화"라 함은 정보를 생산 유통 또는 활용하여 사회 각 분야의 활동을 가능하게 하거나 그러한 활동의 효율화를 도모하는 것을 말한다.
15. "휴대용 저장매체"라 함은 CD·외장형 하드디스크·USB메모리 등 정보를 저장할 수 있는 것으로 PC·서버 등의 정보시스템과 분리할 수 있는 기억장치를 말한다.
16. "내부망"이라 함은 재단의 정보통신망 중 재단의 업무를 수행하기 위하여 인터넷과 별도로 분리하여 구축한 업무 전용 정보통신망을 말한다.
17. "재단 인터넷망"이라 함은 재단의 정보통신망 중에서 소속 직원 등의 업무 활용 또는 공개서버 운용을 주(主) 목적으로 인터넷과 연동하여 구축한 정보통신망을 말한다.
18. "상용 인터넷망"이라 함은 재단 인터넷망과 별개로 소속 직원 등이나 민원인 등의 보편적인 편의성을 위하여 인터넷에 연동하여 구축한 정보통신망을 말한다.
19. "정보보호팀"이라 함은 전문 또는 전담인력을 갖추고 정보보호시스템 운영 및 보안관제 업무를 수행하는 조직을 말한다.

② 이 지침에서 사용하는 용어는 제1항에서 정하는 것을 제외하고는 「기본지침」 등 관계법령이 정하는 바에 따른다.

제4조(책무) ① 이사장은 국가안보 및 국익과 관련된 정보(업무자료를 포함한다. 이하 같다)와 정보통신망을 보호하기 위하여 보안대책을 수립·시행하여야 하며 정보보안에 대한 책임을 진다.

② 이사장은 직원등에 대한 근무성적 또는 성과 평가를 실시할 경우 정보보안내규 준수여부 등을 반영할 수 있다.

제2장 정보보안 기본활동

제5조(기본원칙) ① 재단 업무 추진 시 발생된 정보자산은 재단의 소유이며, 정보자산의 관리는 각 부서 단위로 한다.
② 재단 정보자산에 대한 접근이 필요한 경우 업무처리를 위한 최소한의 권한만 부여되어야 한다.
③ 인가된 개별사용자는 전자정보를 사용함과 동시에 보호할 책임을 가지며, 비인가자는 자신의 업무와 무관한 어떠한 정보자산에도 접근을 시도해서는 아니 된다.

제6조(정보보안 조직 구성) ① 이사장은 재단 정보통신시스템 보안과 정보의 안전한 관리를 위하여 정보보안 소관부서를 총괄하는 임원을 정보보호책임자로 둔다.
② 정보보호책임자는 정보보안 소관부서의 장을 정보보안관리자로 지정하고 업무를 위임할 수 있다.
③ 정보보안관리자는 소관부서의 직원을 정보보안담당자로 지정하여 정보보안 실무를 수행하도록 하고, 현황을 주기적으로 보고 받는다.

제7조(정보보호책임자 역할) 정보보호책임자는 다음 각 호의 정보보안 기본활동을 수행하여야 한다.

1. 정보보안 정책 및 계획의 수립 · 시행 및 정보보안내규 제 · 개정
2. 정보보안 전담조직 관리, 전문인력 및 관련예산 확보
3. 정보화사업 보안성 검토 및 보안적합성 검증
4. 정보통신실, 정보통신망 현황자료 등에 관한 보안관리
5. 재단 정보통신기반시설 보호
6. 사이버공격 대응훈련 및 정보보안 관련 평가 대응
7. 보안관제, 사고대응 및 정보협력
8. 정보보안 교육 총괄 및 ‘사이버보안진단의 날’ 계획 수립 · 시행
9. 정보보안 감사
10. 그 밖에 정보보안과 관련한 사항

제8조(정보보안위원회) ① 정보보안업무의 효율적인 운영과 보안관련 중요사항을 심의하기 위해 재단에 정보보안위원회(이하 “위원회”라 한다)를 둔다.
② 위원회는 다음 각 호와 같이 위원장 1인과 위원 5인 이상으로 구성하되, 필요에 따라 외부 전문가를 포함하여 8인 이내로 구성 · 운영한다.

1. 위원장: 정보보호책임자
2. 위원: 미래기획실장, 경영협력실장, 글로벌사업1실장, 글로벌사업2실장, 아세안문화원장

③ 위원회는 사무를 처리하기 위하여 간사를 두며, 간사는 사안에 따라 정보보안관리자 또는 「개인정보보호지침」 제5조의2에 따른 개인정보보호관리자가 된다.
④ 위원회의 임무는 다음 각 호로 한다.

1. 정보보안 사고에 대한 처리 심의
2. 정보보안 정책 검토 및 심의
3. 정보보안 책임 및 관리체계 검토
4. 그 밖에 정보보안상 중요하다고 판단하는 사항

⑤ 위원회의 소집을 위해 별지 제1호서식에 의하여 일시 및 장소와 심의 안건을 회의 개최 5일 전까지 위원들에게 통보하여야 한다. 단, 긴급을 요하는 경우에는 예외로 할 수 있다.
⑥ 위원회는 재적위원 3분의 2이상 출석으로 개회하고, 출석위원 과반수의 찬성으로 의결하며, 가부동수일 때에는 위원장이 결정한다.
⑦ 긴급을 요하거나, 토의를 필요로 하지 않는 경미한 안건 등은 별지 제2호서식에 의해 서면으로 심의할 수 있다.
⑧ 위원회에서 심의한 사항은 이사장의 결재를 득한 후 시행한다.

제9조(정보보안 감사) 정보보호책임자는 재단의 정보보안 업무 및 활동을 조사 · 점검하기 위하여 국가정보원장이 배포하는 가이드라인(홈페이지 · 네트워크 · 시스템 · DBMS 취약점 점검매뉴얼, 정보보안점검 체크리스트 등)을 활용하여 연 1회 이상 정보보안 감사를 실시하여야 한다.

제10조(정보보안 교육) ① 정보보호책임자는 정보보안 교육계획을 수립하여 연 1회 이상 전 직원을 대상으로 관련 교육을 실시하여야 한다.
② 정보보호책임자는 직원등을 대상으로 정보보안 관련 전문기관 교육 및 기술 세미나 참석을 장려하는 등 정보보안 의식 제고를 위해 노력하여야 한다.

제11조(사이버보안진단의 날) ① 정보보호책임자는 매월 세 번째 수요일을 ‘사이버보안진단의 날’로 지정 · 시행한다. 다만, 부득이한 사유로 해당 일에 시행하지 못할 경우 같은 달 다른 날에 시행하여야 한다.
② 정보보호책임자는 ‘사이버보안진단의 날’에 소관 정보통신망과 정보시스템의 보안취약 여부 확인 등 보안진단을 실시하여야 한다.
③ 정보보호책임자는 제1항 및 2항에 따른 보안진단 결과를 게시할 수 있고, 개인 및 부서평가에 활용할 수 있다.

제12조(정보보안 업무 위탁) ① 정보보호책임자는 정보통신망과 정보시스템 등에 대한

보안관제와 취약점 분석·평가 업무의 일부를 외부 정보보안 전문기관에 위탁할 수 있다.

② 제1항에 따라 정보보안 업무의 일부를 위탁하는 경우에는 위탁업무 수행에 참여하는 업체에 별지 제3호서식의 대표자 명의의 보안서약서를 징구하고, 업무관련 기록과 자료의 안전한 보존·폐기 절차의 준수를 요구하는 등의 필요한 보안 조치를 하여야 한다.

제3장 정보화사업 보안

제1절 사업 계획

제13조(보안책임) ① 재단에서 정보화전략계획 수립, 소프트웨어 개발, 정보통신망 또는 정보시스템을 구축·운용·유지보수하는 등의 정보화사업을 담당하는 정보화사업담당자는 해당 정보화사업에 대한 보안관리를 수행하여야 한다.

② 정보화사업을 추진하는 부서의 장은 정보화사업에 대한 보안관리 책임을 지고 관리·감독하여야 한다.

③ 정보보호책임자는 각종 정보화사업과 관련한 보안대책의 적절성을 평가하고 정보화사업 수행 전반에 대하여 보안대책의 이행여부를 점검하여야 한다.

제14조(보안대책 수립) ① 정보화사업담당자는 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, 검증필 암호모듈 및 정보보호시스템 도입·운용계획
5. 긴급사태 대비 및 재난복구 계획
6. 용역업체 작업장소에 대한 보안대책
7. 온라인 개발 또는 온라인 유지보수가 필요하다고 판단할 경우 제23조(원격지 개발보안) 또는 제36조(지정 단말기를 통한 온라인 유지보수)에 따른 보안대책
8. 누출금지정보 목록 및 보안관리 방안

② 제1항제8호의 누출금지정보 목록을 작성할 경우 다음 각 호의 사항을 포함하여야 한다.

1. 재단 정보시스템 내·외부 IP주소 현황
2. 정보시스템 구성 현황 및 정보통신망 구성도
3. 개별사용자의 계정·비밀번호 등 정보시스템 접근권한 정보

4. 정보통신망 또는 정보시스템 취약점 분석·평가 결과물
5. 정보화사업 용역 결과물 및 관련 프로그램 소스코드(외부에 유출될 경우 국가안보, 국익 또는 재단에 피해가 우려되는 중요 용역사업에 해당)
6. 암호자재, 암호가 주 기능인 제품 및 정보보호시스템 도입·운용 현황
7. 정보보호시스템 및 네트워크장비 설정 정보
8. 대외비, 비공개 업무자료, 개인정보가 포함된 정보
9. 그 밖에 이사장이 공개가 불가하다고 판단한 자료

제15조(제안요청서 기재사항) 정보화사업담당자는 용역업체에 정보화사업을 발주하기 위하여 제안요청서를 작성할 경우 다음 각 호의 사항을 포함하여야 한다.

1. 용역업체 작업장소에 대한 보안요구사항
2. 온라인 개발 또는 온라인 유지보수가 필요하다고 판단할 경우 제23조 또는 제36조에 따른 보안 준수사항
3. 누출금지정보 목록
4. 용역업체가 누출금지정보를 제외한 소프트웨어 산출물을 제3자에게 제공하고자 할 경우 발주자의 승인절차

제16조(보안성 검토) ① 이사장은 별표 1에 해당하는 정보화사업을 수행하고자 할 경우 정보화사업과 관련한 보안대책의 적절성을 평가하기 위하여 사업계획단계(사업 공고 전)에서 보안성 검토 절차를 이행하여야 한다.

② 별표 1에 해당하지 않는 아래 각 호에 대해서는 보안성 검토 절차의 이행을 생략할 수 있다.

1. 정보화사업에 해당하지 아니하는 장비·물품을 도입하는 경우
2. 시설보수 등 추가 보안대책이 요구되지 않을 경우
3. 단말기 수준의 구조변경, 통신회선의 증설 등 보안상 큰 변화가 없을 경우
4. 운영 중인 시스템과 동일한 방법으로 증설할 경우
5. 시스템 구성방법은 변경하지 않고 이동 설치할 경우
6. 보안수준을 낮추지 않는 범위에서 개별사용자 확대 등 일상적인 업무
7. 보안성 검토를 거쳐 완료한 정보화사업에 대하여 정보통신망 구성을 변경하지 않는 범위 내에서 다음 각 목의 사항을 포함한 후속운영·유지보수·컨설팅(단일 회선의 이중화는 본 호를 적용함에 있어 정보통신망 구성의 변경이 아닌 것으로 본다)
   가. 서버·스토리지·네트워크장비 등 장비 노후화로 인한 장비 교체
   나. 전화기·무전기·CCTV 등 통신·영상기기의 노후화로 인한 장비 교체
   다. 기존 운용하던 정보보호시스템을 동일한 보안기능을 보유한 다른 정보보호시스템으로 교체

8. 다년도에 걸쳐 계속되는 사업으로서 사업 착수 당시 보안성 검토를 완료한 후 사업 내용의 변동 없이 계속 추진하는 운영 · 유지사업의 경우(기존 보안성 검토 결과를 준수하여야 한다.)
9. 기타 정보보호책임자가 경미사안으로 인정한 경우

③ 보안성 검토 절차의 이행을 위해 이사장은 다음 각 호의 사항이 포함된 문서를 외교부에 제출하여야 한다.

1. 사업계획서(사업목적 및 추진계획을 포함한다)
2. 제안요청서
3. 정보통신망 구성도(필요시 IP주소체계를 추가한다)
4. 자체 보안대책

④ 정보보안담당자는 외교부, 국정원으로부터 보안성 검토 결과를 통보받은 경우 검토 결과를 반영하여 보안대책을 보완하여야 한다.

제2절 제품 도입

제17조(정보통신제품 도입) ① 정보 및 정보통신망 등을 보호하기 위하여 보안기능이 있는 정보통신제품을 도입할 경우 다음 각 호에 해당하는 제품을 도입하여야 한다.

1. 별표 2의 안전성 검증필 제품 목록에 등재되어 있는 제품
2. 업무자료의 암 · 복호화를 목적으로 한 경우 별표 3의 암호가 주기능인 제품 도입요건을 만족하는 제품
3. 제1호 및 제2호에 해당하지 않는 정보통신제품 중 국가정보원장이 별도로 공지하는 도입요건을 만족하는 제품
4. 취약점으로 인해 국가정보원에서 운용중지를 요청한 취약 정보통신제품을 긴급 대체하기 위한 제품

② 영상정보처리기기(불특정 사람 또는 사물을 촬영한 영상을 유 · 무선 정보통신망으로 전송 · 저장 · 분석하는 CCTV · IP카메라 · 이동형 영상촬영장비 · 중계서버 · 관제서버 · 관리용 PC 등의 기기 · 장비를 말한다. 이하 “영상정보처리기기”라 한다)를 도입하는 경우 한국정보통신기술협회(TTA)의 공공기관용 보안 성능품질 인증 등 일정한 보안 성능이 확인된 제품을 도입하여야 한다.

제18조(보안적합성 검증) ① 이사장은 보안기능이 있는 정보통신제품을 도입하는 경우 실제 적용 · 운용 이전에 안전성 확인을 위해 별표 4, 별지 제4호 및 제5호서식에 따라 외교부에 보안적합성 검증을 신청하여야 한다.

② 외교부가 요청할 경우 재단은 추가 자료를 제출하여야 한다.

③ 외교부로부터 추가 조치를 필요로 하는 검증결과를 통보받을 경우 재단은 해당 조치를 실시한 후 그 결과를 외교부에 제출하여야 한다.

제3절 계약 및 사업수행

제19조(계약 특수조건) ① 정보화사업담당자는 정보통신망 또는 정보시스템 구축 및 유지보수 등의 계약 이행과정에서 정보통신망 또는 정보시스템에 허가 없이 접속하거나 무단으로 정보를 수집할 수 있는 비인가 프로그램을 설치하거나 그러한 행위에 악용될 수 있는 정보통신망 또는 정보시스템의 약점을 고의로 생성 또는 방치하는 행위 등을 금지하는 내용의 계약 특수조건을 계약서에 명시하여야 하며 계약기간(하자 보증기간을 포함한다) 내에 발생한 보안약점 등에 대해서는 계약업체로 하여금 개선 조치하도록 하여야 한다.

② 정보화사업담당자는 필요한 경우 계약업체로부터 제1항과 관련한 행위가 없다는 대표자 명의의 확약서를 요구할 수 있다.

제20조(용역업체 보안) ① 정보화사업담당자는 용역업체에 정보화사업을 발주할 경우 다음 각 호의 보안사항을 준수하도록 계약서에 명시하여야 한다.

1. 제15조(제안요청서 기재사항)제1항 각 호에 따른 제안요청서에 포함된 사항
2. 제23조에 따른 원격지 개발, 제36조에 따른 지정 단말기를 통한 온라인 유지보수를 허용할 경우 보안 준수사항
3. 소프트웨어 개발보안에 필요한 사항
4. 사업 참여인원의 보안관련 준수사항과 위반할 경우 손해배상 책임에 관한 사항
5. 사업 수행과 관련된 보안점검, 교육 및 사업기간 중 참여인원 임의 교체 금지
6. 정보통신망 구성도 · IP주소 현황 등 업체에 제공하는 자료는 자료 인수인계대장을 비치하여 보안조치 후 인수인계하고, 무단 복사 및 외부반출 금지
7. 업체의 노트북 · 휴대용 저장매체 등 관련 장비는 반출입 시마다 악성코드 감염 여부, 누출금지정보 무단 반출여부 등 점검
8. 사업 종료 시 업체의 노트북 · 휴대용 저장매체 등 관련 장비는 저장자료 복구가 불가하도록 완전 삭제
9. 사업 종료 시 누출금지정보 전량 회수
10. 그 밖에 이사장이 보안관리가 필요하다고 판단하는 사항 또는 국가정보원장이 보안조치를 권고하는 사항

② 정보화사업담당자는 용역사업을 수행할 때 용역업체 참여 인원 혹은 업체가 「국가를 당사자로 하는 계약에 관한 법률」 제27조제1항 각 호에 해당되는 사실을 알게 된 경우 교체를 요구하여야 한다.

③ 정보화사업담당자는 제1항에 따른 보안 준수사항의 이행여부를 정기 또는 수시로 점검(불시 점검을 포함한다)하고 미비점을 발견한 경우 용역업체로 하여금 시정 조치하도록 하여야 한다. 이 경우 정보화사업담당자가 점검한 후 그 결과를 정보보호책임자

에게 보고하여야 한다.
④ 정보보호책임자는 제3항에 따른 점검 결과, 용역업체 보안대책 준수가 미흡하고 시정조치가 어렵다고 판단할 경우 제23조에 따른 원격지 개발 또는 제36조에 따른 지정 단말기를 통한 온라인 유지보수 허가를 취소할 수 있다.
⑤ 정보보호책임자는 제23조에 따른 원격지에서의 온라인 개발, 제36조에 따른 지정 단말기를 통한 온라인 유지보수를 허용하고자 할 경우에는 용역업체의 온라인 접속을 통제하기 위한 온라인 용역통제시스템을 구축 · 운영하여야 한다.
⑥ 그 밖에 용역업체 보안과 관련한 사항은 국가정보원장이 배포한 「국가 · 공공기관 용역업체 보안관리 가이드라인」을 준수하여야 한다.

제21조(정보시스템 개발보안) ① 정보시스템 개발 시 「행정기관 및 공공기관 정보시스템 구축 · 운영지침」(행정안전부 고시) 제50조부터 제53조까지에 따라 보안 취약점이 발생하지 아니하도록 개발하여야 하며, 정보보호책임자는 「행정기관 및 공공기관 정보시스템 구축 · 운영지침」 제52조를 참고하여 주기적으로 진단, 교육, 감리 등을 수행하여야 한다.
② 정보시스템 개발 및 변경 시 다음 각 호의 사항을 고려한 보안대책을 수립하여야 한다.

1. 외부인원 대상 신원확인, 보안서약서 징구, 보안교육 및 점검
2. 장비 반입, 반출 및 자료 무단반출
3. 작업 장소에 대한 비인가자 접근 통제
4. 개발시스템과 운영시스템의 분리
5. 정보시스템 최소 접근권한 부여
6. 소스코드 관리 및 형상관리
7. 소스코드 취약점 예방 조치(시큐어코딩)
8. 그밖에 행정안전부 “소프트웨어 개발보안 가이드”에서 명시한 내용

제22조(재단 내 작업장소 보안) ① 정보보호책임자는 재단 내(이사장이 임차한 외부 사무실을 포함한다) 용역업체 작업장소를 설치할 경우 보안 통제가 가능한 공간을 마련하여 운영하여야 한다.
② 재단 내 용역업체 작업장소에 설치 · 운영하는 정보통신망은 재단의 정보통신망과 분리하여 구성해야 한다. 다만, 용역업체가 사업 수행을 위하여 발주기관 정보시스템 이용이 불가피할 경우에는 필요한 정보시스템에 한해 지정된 단말기로부터의 제한적 접근을 허용하는 등 보안대책을 수립 · 시행하여야 한다.
③ 작업장소 내 정보시스템은 용역사업 수행을 위해 필요한 경우 해당 정보화사업담당자의 보안통제 하에 인터넷에 연결할 수 있다. 다만, 제2항 단서에 따른 재단 정보시스템 접근용 단말기의 경우에는 인터넷 연결을 금지한다.

④ 용역업체가 재단 내 작업장소에서 개발 작업을 수행하더라도 개발용 서버가 민간 클라우드 컴퓨팅 서비스를 이용하는 등으로 원격지에 위치할 경우 제23조에 따른 원격지 개발로 간주하고 제23조제1항에 따른 보안대책을 수립 · 시행하여야 한다.

제23조(원격지 개발보안) ① 용역업체가 재단 이외 장소(이하 “원격지”라 한다)에서 개발 작업(유지보수는 제외한다)을 수행하고자 요청할 경우 해당 정보화사업담당자는 제15조(제안요청서 기재사항)제1항제1호에 따른 용역업체 작업장소에 대한 보안요구사항 등을 포함한 관리적 · 기술적 보안대책을 수립 · 시행하여야 한다. 이 경우 정보화사업담당자는 보안대책을 수립한 후 정보보호책임자의 승인을 받아야 한다.
② 원격지의 정보시스템은 개발 작업을 위하여 필요한 경우 해당 정보화사업담당자의 보안통제 하에 인터넷에 연결할 수 있다.
③ 정보보호책임자가 필요하다고 판단하고 용역업체가 다음 각 호에 따른 보안대책에 서면으로 동의하는 경우에 한하여, 정보보호책임자는 용역업체에게 원격지에서 인터넷을 통해 재단 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 용역통제시스템 접속 전용으로 운용하고 다른 목적의 인터넷 접속은 차단
3. 재단 내 온라인 용역 통제시스템을 경유하여 개발에 필요한 정보시스템에 접속하는 등 소통구간 보호 · 통제
4. 접속사실이 기록된 로그 기록을 1년 이상 보관
5. 재단의 정기 또는 수시 보안점검(불시 점검을 포함한다) 수검
6. 기타 국가정보원이 배포한 「국가 · 공공기관 용역업체 보안관리 가이드라인」에 제시된 온라인 개발에 관련된 보안대책의 준수

제24조(소프트웨어 산출물 제공) ① 정보화사업담당자는 용역업체가 「소프트웨어 진흥법」 제59조 및 「(계약예규)용역계약일반조건」(기획재정부 계약예규) 제56조에 따른 지식재산권을 행사하기 위하여 소프트웨어 산출물의 반출을 요청할 경우 제안요청서 또는 계약서에 명시된 누출금지정보에 해당하지 아니하면 제공하여야 한다.
② 정보화사업담당자는 제1항에 따라 소프트웨어 산출물을 용역업체에 제공할 경우 업체의 노트북 · 휴대용 저장매체 등 관련 장비에 저장되어 있는 누출금지정보를 완전삭제 소프트웨어 등을 이용하여 완전삭제하여야 하며 업체로부터 누출금지정보가 완전삭제 되었다는 대표자 명의의 확약서를 받아야 한다.
③ 정보화사업담당자는 용역업체가 소프트웨어 산출물을 제3자에게 제공하고자 할 경우 제공하기 이전에 승인을 받도록 하여야 한다.
④ 그 밖에 소프트웨어 산출물 제공과 관련한 사항은 「소프트웨어사업 계약 및 관리감독에 관한 지침(과학기술정보통신부 고시)」 제32조를 준수하여야 한다.

제25조(누출금지정보 유출시 조치) ① 정보화사업담당자는 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 정보화사업담당자 또는 사업과 관계된 직원 등은 즉시 정보보호책임자에게 보고하여야 한다.

② 제1항에 따라 용역업체의 누출금지정보 유출 사실을 알게 되거나 보고를 받은 정보보호책임자는 그 사실을 관계 외교부 장관 및 국가정보원장에게 통보하여야 한다. 또한 정보보호책임자는「국가를 당사자로 하는 계약에 관한 법률 시행령」제76조에 따라 입찰 참가자격 제한 등 관련조치를 취하여야 한다.

제4장 정보통신망 및 정보시스템 보안

제1절 정보통신망 보안

제26조(내부망 · 인터넷망 분리) ① 정보보호책임자는 내부망과 재단 인터넷망 및 상용 인터넷망을 분리 · 운영하여야 한다.

② 정보보호책임자는 내부망과 재단 인터넷망을 분리 · 운영 시 다음 각 호의 사항을 포함한 보안대책을 수립 · 시행하여야 한다.

1. 침입차단 · 탐지시스템 설치 등 비(非)인가자 침입 차단대책
2. 네트워크 접근관리시스템 설치 등 비(非)인가 장비의 내부망 접속 차단대책
3. 내부망 정보시스템의 인터넷 접속 차단대책
4. 내부망과 재단 인터넷망 간 안전한 자료전송 대책
5. 기타 국가정보원장이 배포한「국가 · 공공기관 업무전산망 분리 및 자료전송 보안가이드라인」에서 제시하는 보안대책

③ 정보보호책임자는 정보시스템에 부여되는 IP주소를 체계적으로 관리하여야 하며 비(非)인가자로부터 내부망을 보호하기 위하여 네트워크주소변환기(NAT)를 이용하여 사설 IP주소체계를 구축 · 운영하여야 한다. 또한 IP주소별로 정보시스템 접속을 통제하여 비(非)인가 기기에 의한 내부망 접속을 차단하여야 한다.

④ 정보보호책임자는 분리된 내부망과 재단 인터넷망간 자료전송을 위한 접점이 불가피한 경우 다음 각 호의 사항을 포함한 보안대책을 수립 · 시행하여야 한다.

1. 침입차단 · 탐지시스템 설치 · 운용
2. 내부망과 재단 인터넷망 간 접점 최소화
3. 내부망과 재단 인터넷망 간 일방향 전송장비 등을 이용한 자료전송체계를 구축 · 운영하고 원본파일은 3개월 이상, 전송기록은 6개월 이상 유지
4. 정기적으로 전송실패 기록을 확인하고 악성코드 유입여부 등 점검

5. 내부망 자료를 인터넷망으로 전송할 경우 부서장, 결재권자의 사전 또는 사후 승인절차 마련

⑤ 정보보호책임자는 내부망과 기관 인터넷망의 IP주소 현황을 정기적으로 확인하고 갱신하여야 한다.

제27조(보안 · 네트워크장비 보안) ① 정보보호책임자는 침입차단 · 탐지시스템, 스위치 · 라우터 등 재단 정보통신망 구성 또는 정보보안 정책 전반에 영향을 미치는 보안 · 네트워크장비를 설치 · 운용하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립 · 시행하여야 한다.

1. 물리적으로 안전한 장소에 설치하여 비(非)인가자의 무단접근 통제
2. 콘솔에서 관리함을 원칙으로 하되, 다음 각 목의 경우 재단 내 지정 단말기로부터의 접속 · 관리 허용
   가. 장비 관리자의 접속
   나. 제22조(재단 내 작업장소 보안)제2항 단서에 따른 재단 내 용역업체 작업장소에서의 접속
3. 최초 설치할 경우 디폴트(default) 계정은 삭제하거나 변경한 후에 사용하고 장비 관리를 위한 관리자 계정을 별도로 생성 · 운영
4. 불필요한 서비스 포트 및 사용자 계정 차단 및 삭제
5. 펌웨어 무결성, 컴퓨터 운영체제 · 소프트웨어의 취약점 및 버전 업데이트 여부를 정기적으로 점검하고 최신 버전으로 유지

② 정보보호책임자는 로그기록을 1년 이상 유지하도록 하고 비(非)인가자의 접속여부를 정기적으로 점검하여야 한다.

③ 정보보호책임자는 침입차단 · 탐지시스템의 침입차단 · 탐지규칙의 생성 근거를 유지하고 정기적으로 필요성 여부를 점검 · 갱신하여야 한다.

제28조(무선랜 보안) ① 정보보호책임자는 내부망을 제외한 정보통신망에서 다음 각 호의 경우와 같이 재단 내에 무선랜[WiFi]을 구축 · 운용할 수 있다.

1. 재단 인터넷망에 중계기(AP)를 설치하여 제54조(단말기 보안)제1항에 따라 재단에서 지급한 단말기의 접속만을 허용하는 업무용 무선랜
2. 상용 인터넷망에 중계기(AP)를 설치하여 제59조(비인가 기기 통제)제1항 각 호에 따라 반입한 직원등의 개인 소유 이동통신단말기의 접속만을 허용하는 무선랜
3. 상용 인터넷망에 중계기(AP)를 설치한 외부인 전용 무선랜

② 정보보호책임자는 제1항에 따라 무선랜을 구축 · 운용하고자 할 경우 국가정보원장이 배포한 「국가 · 공공기관의 무선랜 구축 및 RFID 보안가이드라인」을 준수하여 보안대책을 수립 · 시행하여야 한다.

③ 제2항에 따른 보안대책을 수립할 경우 제1항제1호 및 제2호에 따른 무선랜에 대하

여는 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 암호체계를 사용하여 소통자료 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 상호 인증을 수행하는 무선랜 인증제품 사용
6. 무선침입방지시스템 설치 등 침입 차단대책
7. 내부망 정보시스템 또는 인접해 있는 다른 기관의 정보시스템이 해당 무선랜에 접속되지 아니하도록 하는 기술적 보안대책
8. 그 밖에 무선랜 단말기 · 중계기(AP) 등 구성요소별 분실 · 탈취 · 훼손 · 오용 등에 대비한 관리적 · 물리적 보안대책

제29조(영상회의 보안) ① 정보보호책임자는 영상회의시스템을 구축 · 운용하고자 할 경우 통신망(국가정보통신망 · 전용선 · 인터넷 등) 암호화 등 보안대책을 수립 · 시행하여야 한다.

② 기타 영상회의시스템 보안과 관련한 사항은 국가정보원장이 배포한 「안전한 정보통신 환경 구현을 위한 네트워크 구축 가이드라인」을 준수하여야 한다.

③ 정보보호책임자는 다음 각 호의 구분에 따라 상용 소프트웨어에 탑재된 영상회의 서비스를 이용할 수 있다.

1. 비공개 업무자료를 취급하거나 회의 내용이 비공개 업무자료에 준하다고 판단할 경우 : 영상 · 음성 · 업로드 데이터가 국내 서버로만 전송되는 상용 영상회의 소프트웨어(이하 “국내 영상회의 솔루션”이라 한다)를 활용
2. 공개 업무자료를 취급하거나, 회의 내용이 공개 업무자료에 준하다고 판단할 경우 : 국내 영상회의 솔루션 또는 그 밖의 영상회의 소프트웨어를 활용

④ 전항 제1호에도 불구하고, 정보보호책임자는 다음 각 호의 어느 하나에 해당하는 등 정당한 사유가 있는 경우 국가정보원장과 협의하여 국내 영상회의 솔루션이 아닌 소프트웨어를 일시적 또는 정기적으로 활용할 수 있다.

1. 안보 · 국익상 필요한 외국기관[외국군(軍)을 포함한다]과의 영상회의 시에 상대방이 국내 영상회의 솔루션을 활용할 수 없거나, 상대방이 국내 영상회의 솔루션이 아닌 소프트웨어 활용을 제안할 경우
2. 정책자문 등의 목적으로 민간인과 영상회의 시에 상대방이 국내 영상회의 솔루션을 활용할 수 없는 경우

⑤ 기타 영상회의 보안과 관련한 사항은 국가정보원장이 배포한 「원격업무 통합보안 매뉴얼」을 준수하여야 한다.

제30조(인터넷전화 보안) ① 정보보호책임자는 인터넷전화시스템을 구축 · 운용하거나 민간 인터넷전화 사업자망을 이용하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립 · 시행하여야 한다.

1. 한국정보통신기술협회(TTA) verified ver.4 이상 보안규격으로 인증 받은 행정기관용 인터넷전화시스템 설치 · 운용
2. 인터넷전화기에 대한 장치 및 사용자 인증
3. 제어신호 및 통화내용 등 데이터 암호화
4. 인터넷전화망과 다른 정보통신망 분리
5. 인터넷전화 전용 침입차단시스템 등 정보보호시스템 설치 · 운용
6. 백업체계 구축

② 정보보호책임자는 민간 인터넷전화 사업자망을 이용할 경우 해당 사업자로 하여금 서비스 제공 구간에 대한 보안대책을 수립하도록 하여야 한다.

③ 기타 인터넷전화 보안과 관련한 사항은 국가정보원장이 배포한 「국가 · 공공기관 인터넷전화 보안 가이드라인」을 준수하여야 한다.

제31조(인터넷 사용제한) ① 정보보호책임자는 국가비상사태 및 대형 재해 · 재난의 발생, 사이버공격 등으로부터 정보통신망과 정보시스템의 정상적인 운영을 보장하기 위하여 직원등에 대한 인터넷 사용을 일부 제한할 수 있다.

② 정보보호책임자는 재단 인터넷망의 효율적인 운영 관리 및 악성코드 유입 차단을 위하여 게임 · 음란 · 도박 등 업무와 관련이 없는 인터넷 이용을 차단하여야 하며, 악성코드 유입 차단을 위하여 필요할 경우 제46조(비공개 업무자료 처리)제4항에 따른 상용 정보통신서비스의 접속을 제한할 수 있다.

제32조(해외사무소 정보통신 보안) ① 해외사무소장은 인터넷과 연결된 PC를 이용하여 비밀 등 중요자료를 작성 · 보관 · 소통하여서는 아니 된다. 다만, 불가피한 경우 국가정보원장이 안전성을 확인한 방법을 사용하여 한시적으로 작성 · 보관 · 소통할 수 있다.

② 정보보호책임자는 해외사무소에서 운용하는 중요 정보통신기기 및 시설을 보호하기 위하여 전자파보안 대책을 수립 · 시행하여야 한다.

③ 정보보호책임자는 해외사무소의 정보통신망과 정보시스템 운용 전반에 대한 보안관리 실태를 정기적으로 점검 · 보완하여야 한다.

④ 정보보호책임자는 해외사무소에 직원을 파견하고자 할 경우 해당 직원에 대하여 파견 이전에 정보시스템 보안관리 방법 등 정보보안 교육을 실시하여야 하며 파견 후에는 정보보안업무에 대한 인계인수를 철저히 하여야 한다.

⑤ 직원등은 주요인사의 외국방문 행사와 관련한 자료 및 장비 등을 수발하고자 할 경우 외교행낭 등 안전한 수단을 이용하여야 하며 일반 국제전화 · 팩스 · 인터넷 등 보안

성이 없는 정보통신 수단을 이용하여서는 아니 된다.
⑥ 해외사무소장은 정보보호책임자가 배포한 별지 제6호서식의 점검 양식에 따라 연1회 정보보안점검을 실시하여야 하고 그 점검결과를 종합하여 매년 정보보호책임자에게 보고하여야 한다.

제33조(파견자용 정보통신망) ① 정보보호책임자는 다른 기관에 파견된 직원등의 활용을 위하여 파견기관의 장과 협의하여 재단 정보통신망 전용 단말기를 파견기관에 설치·운영할 수 있다.
② 정보보호책임자는 제1항에 따라 단말기를 설치할 경우 단말기와 재단 정보통신망 간 소통내용을 보호하여야 한다.
③ 제1항에 따라 파견기관의 내부망과 연동된 단말기는 이 지침을 적용함에 있어 재단의 내부망 단말기로 본다.
④ 제1항에 따라 파견기관의 인터넷망과 연동된 단말기는 이 지침을 적용함에 있어 재단 인터넷망 단말기로 본다.

제2절 정보시스템 보안

제34조(정보시스템 보안책임) ① 정보보호책임자는 정보시스템(PC·서버·네트워크장비·정보통신기기 등을 포함한다)을 도입·운용할 경우 해당 정보시스템에 대한 관리자를 지정·운영하여야 한다.
② 정보시스템 관리자는 별지 제7호서식에 따른 정보시스템 관리대장을 수기 또는 전자적으로 작성·관리하여야 하며 정보시스템의 최종 변경 현황을 유지하여야 한다.
③ 정보보호책임자는 정보시스템 운용과 관련하여 보안취약점을 발견하거나 보안대책 수립이 필요하다고 판단하는 경우 개별사용자, 정보시스템 관리자에게 개선 조치를 요구할 수 있으며 조치가 완료될 때까지 정보시스템의 운용을 일시 제한할 수 있다.

제35조(정보시스템 유지보수) ① 정보보호책임자는 정보시스템의 유지보수와 관련한 절차, 주기, 문서화 등을 사전에 정의하여야 하며 고려사항은 다음 각 호와 같다.

1. 유지보수 인원에 대한 보안서약서 집행, 보안교육 등을 포함한 유지보수 인가 절차를 마련하고 인가된 인원만 유지보수에 참여
2. 결함이 의심되거나 발생한 결함, 예방 및 유지보수에 대한 기록 유지
3. 유지보수를 위하여 정보시스템을 원래 설치장소에서 다른 장소로 이동할 경우 통제수단 마련
4. 유지보수 일시 및 담당자 인적사항, 출입통제 조치사항, 작업수행 내용 등 기록 유지

② 정보보호책임자는 용역업체 등이 유지보수와 관련한 장비·도구 등을 제22조제1항

에 따른 재단 내 용역업체 작업장소로 반출입할 경우 악성코드 감염여부 및 자료 무단 반출여부 확인 등 보안조치를 실시하여야 한다.
③ 정보보호책임자는 직접 또는 용역업체를 활용하여 정보시스템을 유지 보수할 경우 콘솔 또는 지정된 단말기로부터의 접속만을 허용하여야 한다.
④ 정보보호책임자는 재단 정보시스템에 대하여 중요도·가용성 등에 따라 등급을 분류하고 해당 등급에 맞게 정보 보존 및 관리, 장애관리, 보안관리 등을 수행하여야 한다.

제36조(지정 단말기를 통한 온라인 유지보수) ① 제35조(정보시스템 유지보수)제3항에 따른 지정된 단말기를 통해 유지보수를 함에 있어 정보보호책임자가 필요하다고 판단하고 용역업체가 다음 각 호에 따른 보안대책에 서면으로 동의하는 경우에 한하여, 정보보호책임자는 용역업체에게 내부망을 포함하여 소관 정보시스템(보안·네트워크장비는 제외한다)에 대하여 인터넷을 통한 온라인 유지보수를 허용할 수 있다.

1. 지정된 장소에 설치된 지정된 단말기에서만 접속 및 해당 단말기에 대한 접근인원 통제
2. 지정 단말기는 제3호에 따른 온라인 용역통제시스템 접속 전용으로 운용하고 다른 목적의 인터넷 접속은 차단
3. 재단 내 온라인 용역통제시스템을 경유하여 유지보수 대상 정보시스템에 접속하는 등 소통구간 보호·통제
4. 접속사실이 기록된 로그기록을 1년 이상 보관
5. 유지보수 계약 시행일로부터 종료 후 30일이 경과하는 날까지의 기간 중에 정기 또는 수시 보안점검(불시 점검을 포함한다) 수행
6. 기타 국가정보원장이 배포한 「국가·공공기관 용역업체 보안관리 가이드라인」에서 제시된 온라인 유지보수에 관련된 보안대책의 준수

② 제1항제2호 및 제3호에도 불구하고 온라인 용역통제시스템이 구축되지 않았지만 온라인 유지보수를 즉시 실시하지 않고서는 재단 업무수행에 현저한 저해가 있다고 예상되는 경우에는 정보보호책임자의 승인 하에 인터넷망 정보시스템에 한하여 직접 접속하는 온라인 유지보수를 일시적으로 허용할 수 있다.

제37조(서버 보안) ① 정보보호책임자는 서버를 도입·운용하고자 할 경우 사이버공격으로 인한 자료 절취 및 위·변조 등에 대비하여 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 서버 내 저장자료에 대하여 업무별·자료별 중요도에 따라 개별사용자의 접근권한을 차등하여 부여
2. 개별사용자별 자료 접근범위를 서버에 등록하여 인가여부를 식별하도록 하고 인가된 범위 이외의 자료에 대해서는 접근통제

3. 서버 운용에 필요한 서비스 포트 이외 불필요한 서비스 포트는 제거하고, 관리자용 서비스와 개별사용자용 서비스를 분리하여 운용
4. 관리자용 서비스 접속 시 특정 IP주소가 부여된 관리용 단말기 지정 · 운용
5. 서버 설정 정보 및 저장자료를 정기적으로 백업
6. 데이터베이스에 대하여는 개별사용자의 직접 접속 차단, 개인정보 등 중요정보 암호화 등 데이터베이스별 보안조치

② 정보보호책임자는 제1항에 따른 보안대책의 적절성을 수시 확인하여야 하며 연1회 이상 서버 설정 정보와 저장자료의 절취 및 위 · 변조 가능성 등 보안취약점을 점검 · 보완하여야 한다.

제38조(공개서버 보안) ① 정보보호책임자는 외부인에게 공개할 목적으로 웹서버 등 공개서버를 구축 · 운용하고자 할 경우 내부망과 분리된 영역[DMZ]에 설치하여야 한다.

② 정보보호책임자는 비(非)인가자의 공개서버 저장자료 절취 및 위 · 변조, 분산서비스 거부(DDoS) 공격 등에 대비하여 침입차단 · 탐지시스템 및 DDoS 대응장비 설치 등 보안대책을 수립 · 시행하여야 한다.

③ 정보보호책임자는 비(非)인가자의 공개서버 내 비공개 정보에 대한 무단접근을 방지하기 위하여 서버에 접근할 수 있는 개별사용자를 제한하고 불필요한 계정은 삭제하여야 한다.

④ 정보보호책임자는 공개서버 서비스에 필요한 프로그램을 개발 · 시험하기 위하여 사용한 도구(컴파일러 등) 및 서비스와 관계가 없는 산출물은 개발 완료 후 삭제하여야 한다.

⑤ 기타 공개서버 보안과 관련한 사항은 제37조(서버 보안)를 준용한다.

제39조(로그기록 유지) ① 정보보호책임자는 정보시스템의 효율적인 통제 · 관리 및 사고발생 시 추적 등을 위하여 로그기록을 유지 · 관리하여야 한다.

② 제1항에 따른 로그기록에는 다음 각 호의 사항이 포함되어야 한다.

1. 접속자, 정보시스템 · 응용프로그램 등 접속대상
2. 로그온 · 오프, 자료의 열람 · 출력 등 작업 종류 및 시간
3. 접속 성공 · 실패 등 작업 결과
4. 전자우편 등을 사용하여 외부에 발송한 정보

③ 정보시스템 관리자는 로그기록을 생성하는 정보시스템의 경우 시간 동기화 프로토콜(NTP) 적용 등을 통해 정확한 기록을 유지하여야 한다.

④ 정보시스템 관리자는 로그기록을 정기적으로 점검하고 점검 결과 비(非)인가자의 접속 시도, 자료의 위변조 및 삭제 등 의심스러운 정황이나 위반한 사실을 발견한 경우 즉시 정보보호책임자에게 통보하여야 한다.

⑤ 정보시스템 관리자는 로그기록을 1년 이상 보관하여야 하며 로그기록의 위변조 및

외부유출 방지대책을 수립 · 시행하여야 한다.

제40조(업무용 통신단말기 보안) 정보보호책임자는 업무용 통신단말기를 이용하여 업무자료 등 중요정보를 소통 · 관리하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립 · 시행하여야 한다.

1. 통신단말기에 대한 장치 및 사용자 인증
2. 제어신호 및 통화내용 등 데이터 암호화
3. 분실 · 탈취 · 훼손 등에 대비한 관리적 · 물리적 · 기술적 보안대책

제41조(원격근무 보안) ① 정보보호책임자는 직원등이 재택근무, 출장지 현장 근무 또는 파견 근무(제33조에 따라 기관 정보통신망 전용 단말기를 설치 운영하는 경우는 제외한다)시 인터넷을 통해 본인 인증을 거쳐 재단 정보시스템에 접속하여 온라인으로 업무를 수행(이하 “원격근무”라 한다)하게 할 수 있다.

② 제1항에 따른 원격근무를 위해 접속할 수 있는 재단 정보시스템은 다음 각 호와 같다.

1. 재단 인터넷망에 위치한 서버 및 서버에서 구동되는 가상 PC
2. 제26조(내부망 · 인터넷망 분리)제2항 각 호의 보안대책이 적용된 방법을 통해 접속할 수 있는 내부망 서버 및 서버에서 구동되는 가상 PC

③ 제1항에 따른 원격근무로 취급할 수 있는 업무자료의 범위는 공개 및 비공개 업무자료로 한다.

④ 정보보호책임자는 원격근무를 시행하고자 할 경우 다음 각 호의 사항을 포함한 보안대책이 강구된 정보시스템(이하 “원격근무시스템”이라 한다)을 구축 · 운영하여야 한다.

1. 검증필 암호모듈이 탑재된 정보보호시스템을 사용해 원격근무시스템과 원격근무자의 단말기 간 소통구간 암호화
2. 문서 암호화 제품(DRM) 사용 등 문서 보호대책 강구
3. 원격근무자를 식별 · 인증하기 위하여 공인인증서, 생체인증 기술 및 일회용 비밀번호 생성기(OTP) 등 보안성을 강화한 사용자 인증방식 적용
4. 원격근무자로 하여금 원격근무시스템 접속과정에서 제1호부터 제3호까지의 보안대책을 준수토록 조치

⑤ 원격근무자는 정보보호책임자 등이 원격근무용 단말기(개인 소유의 정보통신기기를 포함한다)의 보안을 위하여 취하는 다음 각 호의 조치에 적극 협조하여야 한다.

1. 제4항에 따라 정보보호책임자가 제공하는 보안소프트웨어 설치 · 운영
2. 사이버공격 등으로 인한 자료유출 사고 발생 시 정보보호책임자가 요청하는 점검 및 제76조(정보통신보안 규정 위반 및 자료유출 사고)제2항에 따른 자료제출 요청 협력

3. 재단에서 지급받은 단말기의 경우 제54조에 따른 단말기 보안대책 준수

⑥ 정보보호책임자는 원격근무자에게 제5항에 따른 보안조치 등이 포함된 보안서약서를 징구하고 직위·임무에 부합한 정보시스템 접근권한 부여 및 보직변경·퇴직 등 변동사항이 발생 시 접근권한 조정 등의 절차를 마련·시행하여야 한다.

⑦ 기타 원격근무 보안과 관련한 사항은 국가정보원장이 배포한 「원격업무 통합보안 매뉴얼」을 준수하여야 한다.

제42조(모바일 업무 보안) ① 정보보호책임자는 휴대폰·태블릿 PC 등을 이용한 모바일 업무환경(내부 행정업무, 현장 행정업무 및 대민서비스 업무 등)을 구축·운용하고자 할 경우 보안대책을 수립·시행하여야 한다.

② 기타 모바일 업무 보안과 관련한 사항은 국가정보원장이 배포한「국가·공공기관 모바일 활용 업무에 대한 보안가이드라인」을 준수하여야 한다.

제43조(사물인터넷 보안) ① 정보보호책임자는 사물인터넷을 이용한 시스템을 구축·운용하고자 할 경우 사물인터넷 기기 및 중요 데이터 등을 보호하기 위하여 보안대책을 수립·시행하여야 한다.

② 정보보호책임자는 사물인터넷을 이용한 시스템을 구축·운용하고자 할 경우 내부망과 분리하여야 한다. 다만, 내부망과 연동이 필요한 경우에는 망간 자료전송제품 설치 등 보안대책을 수립하여야 한다.

③ 정보보호책임자는 사물인터넷 서비스를 위한 소프트웨어를 개발할 경우 제21조(정보시스템 개발보안)를 준수하여야 한다.

④ 기타 사물인터넷 보안과 관련한 사항은 국가정보원장이 배포한 「국가·공공기관 사물인터넷(IoT) 보안가이드라인」을 준수하여야 한다.

제44조(저장매체 불용처리) ① 정보보호책임자는 정보시스템 또는 저장매체(하드디스크·반도체 기반 저장장치(SSD) 등)를 외부수리·교체·반납·양여·폐기·불용 처리하고자 할 경우 정보시스템 및 저장매체에 저장된 자료가 외부에 유출되지 않도록 자료 삭제 등 보안조치를 실시하여야 한다.

② 제1항에 따라 자료를 삭제할 경우 재단의 실정에 맞게 저장매체별·자료별 차별화된 삭제 방법을 적용할 수 있다.

③ 비밀·대외비를 저장하거나 암호화 키를 저장한 저장매체는 소각·파쇄·용해 등의 방법으로 완전파괴하여야 한다.

④ 기타 정보시스템 및 저장매체의 불용처리와 관련한 사항은 국가정보원장이 배포한 「정보시스템 저장매체 불용처리지침」을 준수하여야 한다.

제3절 자료 보안

제45조(대외비의 전자적 처리) ① 정보보호책임자는 대외비를 전자적으로 처리하고자 할 경우에는 검증필 암호모듈을 사용하여 위조·변조·훼손 및 유출 등을 방지하기 위한 보안대책을 강구하여야 하며, 보호기간이 만료된 대외비는 제46조에 따른 비공개 업무자료의 처리 기준을 적용하여야 한다.

② 정보보호책임자는 업무와 관계되지 아니한 사람이 대외비를 열람, 복제·복사, 배부할 수 없도록 보안대책을 수립·시행하여야 한다.

제46조(비공개 업무자료 처리) ① 직원등은 비공개 업무자료를 다음 각 호의 어느 하나에 해당하는 방법으로만 처리하여야 한다.

1. 재단 내부망 PC 및 서버에 작성 및 저장·보관
2. 재단이 지급한 휴대용 저장매체에 작성 및 저장·보관
3. 다음 각 목의 어느 하나에 해당하는 수단(이하 “업무자료 공식 소통수단” 이라 한다)을 이용한 수·발신 또는 등재·열람
   가. 재단이 자체적으로 구축·운용하는 전자우편시스템(이하 “재단 전자우편” 이라 한다)
   나. 직원등이 다른 직원등과 자료를 공유하거나 소통하기 위하여 사용하는 전용 소프트웨어(이하 “재단 메신저”라 한다)
   다. 국회사무처가 구축·운용하는 의정자료전자유통시스템 등 기관 간 업무자료의 소통 또는 공동 활용을 위해 구축한 정보시스템
4. 그 밖에 다른 법규에 따라 허용되는 처리방법

② 직원등은 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 경우 재단이 지급한 인터넷 PC 또는 출장용 노트북을 이용하여 비공개 업무자료를 처리할 수 있다.

1. 업무자료 공식 소통수단의 발신 또는 등재 기능을 이용하여 공개 대상 정보의 주요 내용이 기술된 문장 또는 문구 작성
2. 업무자료 공식 소통수단의 수·발신 또는 등재·열람 과정에서의 일시적 저장
3. 제29조(영상회의 보안)제3항 및 제4항에 따라 영상회의 솔루션을 활용하여 비공개 업무자료의 화면 영상을 공유하기 위한 일시적 저장

③ 직원등은 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 경우 개인이 소유한 PC·휴대용 저장매체·휴대폰 등을 이용하여 비공개 업무자료를 처리할 수 있다.

1. 업무자료 공식 소통수단의 수·발신 또는 등재·열람 과정에서의 일시적 저장
2. 제41조(원격근무 보안)제4항에 따른 원격근무시스템에 접속하여 작성
3. 제29조(영상회의 보안)제3항 및 제4항에 따라 영상회의 솔루션을 활용하여 비공개 업무자료의 화면 영상을 공유하기 위한 일시적 저장
4. 국민의 생명·신체, 국가안보 및 공공의 안전 등을 위하여 긴급히 작성, 저장, 수·발신이 필요하다고 이사장이 인정하는 경우

④ 직원등은 제2항부터 제4항까지에 따라 작성 · 저장한 비공개 업무자료는 활용이 종료된 후에는 삭제하여야 한다.
⑤ 직원등은 국회 · 정부와 비공개 업무자료를 소통할 경우에는 우선적으로 제1항제3호 다목의 의정자료전자유통시스템을 활용하여 처리하여야 하며, 시스템 장애 등 부득이한 사유로 활용이 곤란할 경우에 한해 제1항 제3호에 허용된 다른 방법으로 처리할 수 있다.
⑥ 재단 소속 직원등이 자문 등의 목적으로 비공개 업무자료를 업무자료 공식 소통수단을 활용할 수 없는 민간인에게 발신하거나 민간인으로부터 수신 받고자 할 경우에는 재단 전자우편을 활용해 발신하거나 수신하여야 한다.

제47조(비공개 업무자료 유출방지) 정보보호책임자는 제46조(비공개 업무자료 처리)에 따른 비공개 업무자료 처리 절차 준수여부를 관리 · 통제할 수 있는 보안체계를 구축 · 운영하여야 하며, 검증필 암호모듈 등을 사용하여 비공개 업무자료의 위조 · 변조 · 훼손 · 유출 등을 방지하기 위한 보안대책을 강구하여야 한다.

제48조(공개 업무자료 처리) 직원등은 관계 법규에 위배되지 않는 범위 내에서 인터넷 PC나 개인이 소유한 PC · 휴대용 저장매체 · 휴대폰(재단 내에서는 제59조제1항 각 호에 따라 반입한 경우를 말한다), 상용 정보통신서비스(재단 내에서는 제31조제2항에 따른 제한이 없는 경우를 말한다) 등을 이용하여 공개 업무자료를 처리할 수 있다.

제49조(행정전자서명 인증서 등 관리) ① 직원등은 비공개 업무자료를 처리하기 위하여 「전자정부법」 제29조에 따른 행정전자서명의 인증서(이하 “행정전자서명 인증서”라 한다)를 인터넷 PC 또는 개인이 소유한 PC · 휴대용 저장매체 · 휴대폰 등에 저장 · 보관할 수 있다.
② 직원등은 행정전자서명 인증서 및 인증서의 비밀번호, 재단 전자우편의 비밀번호 등을 상용 정보통신서비스를 이용하여 수발신하거나 저장 · 보관하여서는 아니 된다.

제50조(홈페이지 등 게시자료 보안) ① 정보보호책임자는 비공개 업무자료가 홈페이지 또는 외부 웹사이트(이하 “홈페이지 등”이라 한다)에 무단 게시되지 않도록 기술적 · 관리적 대책을 수립하고 적용하여야 한다.
② 정보보호책임자는 홈페이지 등에 업무자료를 게시하고자 할 경우 자료 내용을 사전 검토하여 비공개 업무자료가 게시되지 아니하도록 하여야 한다.
③ 정보보호책임자는 운용하는 홈페이지에서 비공개 업무자료가 무단 게시되었는지 여부를 정기적으로 점검하여야 한다.
④ 정보보호책임자는 홈페이지 등에 비공개 업무자료가 무단 게시된 사실을 알게 된 경우 즉시 삭제 또는 차단 등 보안조치를 취하여야 한다.

제51조(정보통신망 현황자료 관리) ① 정보보호책임자는 다음 각 호에 해당하는 자료를 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따른 비공개 정보로 지정 · 관리하여야 한다.

1. 정보통신망 구성현황(IP주소 할당현황을 포함한다. 이하 본 조에서 같다.)
2. 정보시스템 운용현황
3. 취약점 분석 · 평가 결과물
4. 주요 정보화사업 추진현황

② 정보보호책임자는 제1항에도 불구하고 다른 기관과 협력하여 정보통신망 및 정보시스템 운용 또는 정보보안 업무를 수행할 필요가 있는 경우 제1항 각 호에 해당하는 자료를 다른 기관의 장에게 제공할 수 있다.

제52조(빅데이터 보안) ① 정보보호책임자는 빅데이터와 관련한 시스템을 구축 · 운용하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립 · 시행하여야 한다.

1. 데이터 수집 출처 확인 및 데이터 오남용 방지
2. 데이터 수집을 위한 정보통신망 보안체계 수립
3. 수집된 데이터의 저장 및 보호체계 수립
4. 중요 데이터 암호화
5. 개별사용자별(데이터 제공자 · 수집자 · 분석요청자 및 분석결과 제공자 등) 권한 부여 체계 수립
6. 데이터 파기절차 수립

② 그 밖에 빅데이터 보안과 관련한 사항은 개인정보보호위원회가 고시한 「개인정보의 안전성 확보조치 기준」 및 국가정보원장이 배포한 「국가 · 공공기관 빅데이터 보안 가이드라인」을 준수하여야 한다.

제4절 사용자 보안

제53조(개별사용자 보안) ① 정보보호책임자는 소관 정보통신망 또는 정보시스템의 사용과 관련하여 다음 각 호의 사항을 포함한 개별사용자 보안에 관한 절차 및 방법을 마련하여야 한다.

1. 직위 · 임무별 정보통신망 접근권한 부여 심사
2. 비밀취급 인가 등급에 따른 보안서약서 징구 등 보안조치
3. 보직변경, 퇴직 등 변동사항 발생 시 정보시스템 접근권한 조정

② 개별사용자는 본인이 PC 등 정보시스템을 사용하거나 정보통신망에 접속하는 행위와 관련하여 스스로 보안책임을 진다.

제54조(단말기 보안) ① 개별사용자는 재단에서 지급받은 PC · 노트북 · 휴대폰 · 스마트패드 등 단말기(이하 “단말기”라 한다) 사용과 관련한 일체의 보안관리 책임을 진다.
② 개별사용자는 단말기에 대하여 다음 각 호에 해당하는 보안대책을 준수하여야 한다.

1. CMOS · 로그온 비밀번호의 정기적 변경 사용
2. 단말기 작업을 일정 시간 중단 시 화면보호기 및 해제에 필요한 비밀번호 설정
3. 최신 백신 소프트웨어 설치
4. 운영체제 및 응용프로그램에 대한 최신 보안패치 유지
5. 출처, 유통경로 및 제작자가 불분명한 응용프로그램 사용 금지
6. 인터넷을 통해 자료(파일) 획득 시 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. 재단 인터넷 PC에서는 정보보호책임자가 정한 특별한 사유가 없는 한 문서프로그램을 읽기 전용으로 운용
10. 그 밖에 국가정보원장이 안전성을 확인하여 배포한 프로그램의 운용 및 보안권고문 이행

③ 정보보호책임자는 개별사용자의 제2항 각 호에 해당하는 보안대책의 준수여부를 정기적으로 점검하고 개선 조치하여야 한다.

제55조(계정 관리) ① 정보보호책임자는 개별사용자에게 담당 정보통신망 또는 공용 정보시스템의 접속에 필요한 개별사용자 계정[아이디]를 부여하고자 할 경우 다음 각 호에 해당하는 사항을 준수하여야 한다.

1. 개별사용자별 또는 그룹별 접근권한 부여
2. 외부인에게 계정을 부여하지 아니하되 업무상 불가피한 경우 정보보호책임자의 승인 하에 보안조치 후 필요한 업무에 한하여 일정기간 동안 접속 허용
3. 특별한 사유가 없는 한 용역업체 직원에게 관리자 계정 부여 금지
4. 비밀번호 등 식별 및 인증 수단이 없는 사용자 계정은 사용 금지

② 정보보호책임자는 개별사용자가 시스템 접속[로그온]에 5회 이상 실패할 경우 접속이 중단되도록 시스템을 설정하고 비(非)인가자의 침입여부를 점검하여야 한다.
③ 정보보호책임자는 개별사용자의 보직변경, 퇴직, 계약종료 등 변동사항이 발생할 경우 신속히 사용자 계정을 삭제하거나 부여된 접근권한을 회수하여야 한다.
④ 정보보호책임자는 사용자 계정 부여 및 관리의 적절성을 연2회 이상 점검하여야 한다.

⑤ 정보보호책임자는 제1항 및 제3항에 의한 접근권한 부여, 변경, 회수 또는 삭제 등에 대한 내역을 기록하고 3년 이상 보관하여야 한다.

제56조(비밀번호 관리) ① 개별사용자 및 정보보호책임자는 각종 비밀번호를 다음 각 호에 해당하는 사항을 반영하고 숫자 · 문자 · 특수문자 등을 혼합하여 안전하게 설정하고 정기적으로 변경 · 사용하여야 한다.

1. 사용자 계정[아이디]와 동일하지 않은 것
2. 개인 신상 및 부서 명칭 등과 관계가 없는 것
3. 일반 사전에 등록된 단어의 사용을 피할 것
4. 동일한 단어 또는 숫자를 반복하여 사용하지 말 것
5. 동일한 비밀번호를 여러 사람이 공유하여 사용하지 말 것
6. 응용프로그램 등을 이용한 자동 비밀번호 입력기능을 사용하지 말 것

② 정보보호책임자는 서버 등 정보시스템에 보관되는 비밀번호가 복호화되지 않도록 일방향 암호화하여 저장하여야 한다.
③ 정보보호책임자는 공용 정보시스템에서 개별사용자를 식별 및 인증하기 위하여 비밀번호에 갈음하거나 병행하여 지문인식 등 생체인증 기술이나 일회용 비밀번호 생성기(OTP) 등을 안전성 확인 후 사용할 수 있다. 이 경우 생체인증 정보는 안전하게 보관하여야 한다.

제57조(전자우편 보안) ① 정보보호책임자는 재단 전자우편을 컴퓨터바이러스 · 트로이목마 등 악성코드로부터 보호하기 위하여 백신 소프트웨어 설치, 해킹메일 차단시스템 구축 등 보안대책을 수립 · 시행하여야 한다.
② 정보보호책임자는 다른 전자우편과 자료를 안전하게 소통하기 위하여 재단 전자우편시스템에 암호화 기술을 적용하여야 한다.
③ 정보보호책임자는 재단 전자우편시스템에서 수신된 전자우편의 발신지 IP주소를 확인할 수 있고 해킹메일로 의심될 경우 신고할 수 있는 기능을 갖추어야 한다.
④ 개별사용자는 수신된 전자우편에 포함된 첨부파일이 자동 실행되지 아니하도록 기능을 설정하고 첨부파일을 다운로드할 경우 최신 백신 소프트웨어로 악성코드 은닉여부를 검사하여야 한다.
⑤ 개별사용자는 출처가 불분명하거나 의심되는 제목의 전자우편은 열람하지 말고 해킹메일로 의심될 경우 제3항의 해킹메일 신고기능을 통해 정보보호팀에 즉시 신고하여야 한다.
⑥ 정보보호책임자는 전자우편 발신자 조작 등을 통한 기관 사칭 전자우편의 유포를 차단하기 위하여 보안대책을 수립 · 시행하여야 한다.

제58조(휴대용 저장매체 보안) ① 정보보호책임자는 휴대용 저장매체를 사용하여 업무

자료를 보관하고자 할 경우 자료의 위변조, 저장매체의 훼손·분실 등에 대비한 보안대책을 수립·시행하여야 한다.
② 정보보호책임자는 휴대용 저장매체 관리시스템을 운용하고자 할 경우 국가정보원장이 안전성을 확인한 제품을 도입하여야 한다.
③ 정보보호책임자는 개별사용자가 휴대용 저장매체를 PC·서버 등에 연결할 경우 자동 실행되지 아니하고 최신 백신 소프트웨어로 악성코드 감염여부를 자동 검사하는 등의 보안 정책을 수립·시행하도록 관리하여야 한다.
④ 정보보호책임자는 휴대용 저장매체를 비밀용·일반용으로 구분·관리하고 수량 및 보관 상태를 정기적으로 점검하며 외부 반출입을 통제하도록 한다.
⑤ 정보보호책임자는 비밀이 저장된 휴대용 저장매체를 매체별로 비밀등급 및 관리번호를 부여하고 비밀관리기록부에 등재·관리하여야 한다. 이 경우 매체 전면에 비밀등급 및 관리번호가 표시되도록 하여야 한다.
⑥ 정보보호책임자는 비밀용 휴대용 저장매체를 다른 등급의 비밀용 또는 일반용으로 변경 사용하고자 할 경우 저장자료가 복구 불가하도록 완전삭제 소프트웨어 등을 이용하여 삭제하여야 한다. 완전삭제가 불가할 경우 변경 사용하여서는 아니 된다.
⑦ 정보보호책임자는 휴대용 저장매체를 폐기·불용 처리하고자 할 경우 저장자료가 복구 불가하도록 완전삭제 소프트웨어 등을 이용하여 삭제하여야 한다. 다만, 완전삭제가 불가할 경우 파쇄하여야 한다.
⑧ 정보보호책임자는 개별사용자의 휴대용 저장매체 무단 반출, 미(未)등록 휴대용 저장매체 사용여부 등 보안관리 실태를 정기적으로 점검하여야 한다.
⑨ 그 밖에 휴대용 저장매체 보안과 관련한 사항은 국가정보원장이 배포한 「USB메모리 등 휴대용 저장매체 보안관리지침」을 준수하여야 한다.

제59조(비인가 기기 통제) ① 직원등은 다음 각 호의 경우를 제외하고는 개인 소유의 정보통신기기를 소속된 기관으로 무단 반입·사용하여서는 아니 된다.

1. 보편적 통신 목적의 개인 소유 이동통신단말기(LTE·5G 등 이동통신망 접속기능이 있는 휴대폰·태블릿·스마트워치) : 반입하여 개인 용도로만 사용. 이 경우 반입 장비를 도크스테이션(dock station)·마우스·모니터·키보드 등 PC와 유사하게 활용토록 하는 장치와 연결하여 사용하는 행위를 금한다.
2. 제1호를 제외한 정보통신기기 : 제1호에 따른 반입·사용만으로는 보편적 통신 곤란 등 특별한 사정이 있는 경우에 한하여 소속 부서장을 거쳐 정보보호책임자의 승인을 받아 반입 후 개인 용도로만 사용

② 직원등은 제1항 각 호에 따라 반입한 개인 소유의 정보통신기기를 내부망 및 재단 인터넷망에 연결하여서는 아니 되며, 내부망 및 재단 인터넷망 정보시스템을 다른 정보통신망에 연결하는 수단으로 사용하여서는 아니 된다.
③ 정보보호책임자는 개인 소유의 정보통신기기가 업무자료를 외부로 유출하는데 악용

될 수 있거나 소속된 기관의 정보통신망 운영에 위해(危害)가 된다고 판단될 경우 반출입 통제, 보안소프트웨어 설치 후 반입 등 보안대책을 수립·시행하여야 한다.

제60조(위규자 처리) 이 지침을 위반한 직원등에 대해 정보보호책임자는 인사부서 및 감사부서에 관련 사실을 통보하여야 하며, 인사부서의 장은 필요한 절차를 거쳐 인사위원회에 해당 직원에 대한 징계를 요구할 수 있다.

제5장 정보통신시설 및 기기 보호

제61조(정보통신시설 보호대책) ① 정보보호책임자는 다음 각 호의 어느 하나에 해당하는 정보통신시설 및 장소를 「보안업무규정」 제34조에 따른 보호지역으로 지정·관리하여야 한다.

1. KF데이터센터
2. KF사이버안전센터(보안관제센터), 재해복구센터 및 중요 정보통신시설을 집중 제어하는 국소
3. 제주본부, 서울사무소, 부산아세안문화원, 해외사무소 각 층별 정보통신실
4. 그 밖에 보안관리가 필요하다고 인정되는 정보시스템 설치장소

② 정보보호책임자는 제1항에 따라 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

③ 정보보호책임자는 외부인이 정보통신시설을 방문할 경우 반드시 신원을 확인하고 보안교육 후 출입을 허용하여야 한다.
④ 정보보호책임자는 외부인이 정보통신시설을 방문할 경우 별지 제8호서식의 출입관리대장에 기록하도록 하고 관리·운영하여야 한다.

제62조(재난 방지대책) ① 정보보호책임자는 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애 발생에 대비하여 정보시스템의 이중화, 백업관리 및 복구 등 종합적인 재난 방지대책을 수립·시행하여야 한다.

② 정보보호책임자는 재난 방지대책을 정기적으로 시험 · 검토하고 재난으로 인해 업무에 지장이 초래될 가능성에 대한 영향평가를 실시하여야 한다.
③ 정보보호책임자는 정보통신망의 장애 발생에 대비하여 정보시스템 백업시설을 확보하고 정기적으로 백업을 실시하여야 한다.
④ 정보보호책임자는 제3항에 따른 백업시설을 구축 · 운영하고자 할 경우 KF데이터센터와 물리적으로 일정거리 이상 떨어진 안전한 장소에 설치하여야 하며 전력공급원 이중화 등 정보시스템의 가용성을 최대화할 수 있도록 하여야 한다.

제63조(영상정보처리기기 보안) ① 정보보호책임자는 영상정보처리기기를 구축 · 운영하고자 할 경우 운영자의 계정 · 비밀번호 설정 등 인증대책을 수립하고 특정 IP주소에서만 접속을 허용하는 등 비(非)인가자 접근 통제대책을 수립 · 시행하여야 한다.
② 정보보호책임자는 제34조(정보시스템 보안책임)에 따라 영상정보처리기기 관리자를 지정하여 영상정보처리기기를 인터넷과 분리 · 운용하도록 하여야 한다. 다만, 부득이하게 인터넷과 연결 · 사용하여야 할 경우 전송내용을 암호화하여야 한다.
③ 정보보호책임자는 제1항부터 제2항까지와 관련한 보안대책의 적절성을 수시 점검 · 보완하여야 한다.
④ 기타 영상정보처리기기 보안과 관련한 사항은 국가정보원장이 배포한 「국가 공공기관 영상정보 처리기기 도입 · 운영 가이드라인」 및 「안전한 정보통신 환경 구현을 위한 네트워크 구축 가이드라인」을 준수하여야 한다.

제64조(디지털복합기 보안) ① 디지털복합기(이하 "복합기"라 한다)를 설치 · 운용하고자 할 경우 복합기 내 저장매체가 있거나 장착이 가능한 경우 자료유출을 방지하기 위하여 자료 완전삭제 또는 디스크 암호화 기능이 탑재된 복합기를 도입하여야 한다.
② 정보보호책임자는 제1항에 따라 복합기를 설치 · 운용할 경우 다음 각 호의 사항을 포함한 보안대책을 수립 · 시행하여야 한다.

1. 암호화 저장 기능이 있는 경우 해당 기능 사용
2. 정기적으로 저장된 작업 내용(출력 · 스캔 등) 완전 삭제
3. 공유 저장소 사용 제한 및 접근 제어
4. 고정 IP주소 설정 및 불필요한 서비스 제거

③ 정보보호책임자는 다음 각 호의 어느 하나에 해당하는 경우 복합기의 저장매체에 저장된 자료를 완전 삭제하여야 한다.

1. 복합기 사용연한이 경과하여 폐기 · 양여할 경우
2. 복합기 무상 보증기간 중 저장매체 또는 복합기 전체를 교체할 경우
3. 고장 수리를 위한 외부 반출 등의 사유로 해당 기관이 복합기의 저장매체를 통제 관리할 수 없는 장소로 이동할 경우
4. 그 밖에 저장자료의 삭제가 필요하다고 판단되는 경우

④ 소모품 교체 등 복합기 유지보수를 할 경우 복합기 관리자의 입회 · 감독 하에 실시하고 저장매체의 무단 교체 등을 예방하여야 한다.
⑤ 정보보호책임자는 복합기를 통해 내부망과 재단 인터넷망 간 접점이 발생하지 않도록 보안대책을 수립 · 시행하여야 한다.
⑥ 정보보호책임자는 저장매체가 장착되어 있는 복합기 운용과 관련한 보안대책의 적절성을 수시 점검 · 보완하여야 한다.
⑦ 기타 복합기 보안과 관련한 사항은 국가정보원장이 배포한 「정보시스템 저장매체 불용처리지침」을 준수하여야 한다.

제65조(RFID 보안) ① RFID 시스템(대상이 되는 사물 등에 RFID 태그를 부착하고 전파를 사용하여 해당 사물 등의 식별정보 및 주변 환경정보를 인식하여 각 사물 등의 정보를 수집 · 저장 · 가공 및 활용하는 시스템을 말한다)을 구축하여 중요정보를 소통하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립 · 시행하여야 한다.

1. RFID 시스템(태그 및 리더기를 포함한다) 분실 · 탈취 대비 및 백업 대책
2. 태그정보 최소화 대책
3. 장치 및 운용자 인증, 중요정보 암호화 대책

② 정보보호책임자는 제1항과 관련한 보안대책의 적절성을 수시 점검 · 보완하도록 한다.

제6장 훈련 및 진단

제66조(사이버공격 대응훈련) ① 정보보호책임자는 「사이버안보 업무규정」 제11조에 따른 대응훈련 및 시정조치가 원활히 이루어질 수 있도록 지도 · 감독하여야 한다.
② 정보보호책임자는 매년 재단에 대한 사이버공격 · 위협에 대응하기 위한 훈련을 실시해야 한다.

제67조(정보통신망 보안진단) ① 정보보호책임자는 「사이버안보 업무규정」 제12조제1항에 따른 진단 · 점검 또는 그 밖의 법규에 따른 정보통신망 보안진단 · 점검을 실시할 경우, 국가정보원장이 배포하는 다음 각 호의 가이드라인 등을 참고하여야 하며, 이에 필요한 관련예산 확보 등을 위하여 노력하여야 한다.

1. 사이버보안 강화를 위한 길라잡이(정보통신시스템 보안진단 및 대응방법)
2. 홈페이지 · 네트워크 · 시스템 · DBMS 취약점 점검매뉴얼
3. 정보보안 점검 체크리스트

② 정보보호책임자는 재단 정보통신망 안전성을 확인하기 위하여 다음 각 호의 어느 하나에 해당하는 경우 보안진단을 실시할 수 있다.

1. 정보화사업 보안성 검토 결과의 이행여부 확인 또는 보안컨설팅을 수행하는 경우

2. 정보통신망을 이용하여 전자문서를 보관 · 유통할 때 위조 · 변조 · 훼손 · 유출을 방지하기 위하여 보안조치 이행여부를 확인하고자 하는 경우
3. 정보보호책임자가 정보통신망에 대한 보안취약점 점검 또는 종합진단이 필요하다고 판단하여 요청하는 경우

③ 정보보호책임자는 제2항에 따라 보안진단을 실시한 결과 개선이 필요하다고 판단하는 경우 관련 부서의 장에게 개선 조치를 요청할 수 있다. 이 경우 해당 부서의 장은 정당한 사유가 없으면 다음 각 호의 사항을 포함한 조치를 취하여야 하며 정보보호책임자는 그 이행여부를 확인할 수 있다.

1. 기존에 알려지지 않은 새로운 취약점일 경우, 취약점 제거를 위한 관리적 · 물리적 · 기술적 조치
2. 해당 보안취약점이 직원등의 고의 또는 중과실로 인하여 발생한 경우, 해당 직원등에 대한 징계검토 및 개선 조치의 지시
3. 제2호의 경우 유사 보안위규행위 방지를 위해 직원등에 대한 교육 실시

제68조(취약 정보통신제품의 긴급 대체) 정보보호책임자는 제17조(정보통신제품 도입)에 따른 보안기능이 있는 정보통신제품 중에서 취약점으로 인해 정보보안을 침해할 수 있는 상당하고 명백한 보안위협이 식별되고 시급한 조치가 필요하다고 판단한 경우 해당 정보통신제품의 운용을 중단하고 가능한 예산 범위에서 동일 성능의 정보통신제품으로 대체하여야 한다.

제7장 사이버위협 탐지 및 대응

제1절 보안관제

제69조(보안관제센터 설치 · 운영) 이사장은 보안관제센터를 설치 · 운영하고자 할 경우 국가보안관제체계(「사이버안보 업무규정」 제14조제1항에 따른 정부보안관제체계를 포함하여 국가정보원장이 각급기관의 장과 합동으로 보안관제를 실시하거나, 사이버공격 탐지 · 대응 조치 이행여부 확인을 위하여 구축 · 운영하는 실시간 탐지 · 대응체계)와 연계 운영하여야 하며, 이 경우 연계 방법은 국가보안관제체계를 운영하는 국가정보원장과 사전 협의하여야 한다.

제70조(보안관제 인원) ① 정보보호책임자는 전문 또는 전담인원을 배치하여 보안관제센터를 운영하여야 한다.

② 정보보호책임자는 보안관제전문업체의 인력을 배치하고자 하는 경우에는 다음 각 호에 해당하는 사항을 준수하여야 한다.

1. 업체를 선정할 경우 과학기술정보통신부장관이 고시하는 「보안관제 전문기업 지정 등에 관한 공고」에 따른 업무수행능력 평가기준 등 준수
2. 보안관제 업무의 책임 있는 수행 및 보안관리 등을 위하여 정규직원 상시 배치
3. 업체 인력에 대하여 제20조(용역업체 보안) 및 제25조(누출금지정보 유출시 조치) 준용
4. 업체 인력을 대상으로 매월 1회 이상 탐지규칙정보 관리 등에 관한 보안교육 및 점검 실시

제71조(공격정보 탐지 · 처리) ① 정보보호책임자는 재단을 대상으로 하는 사이버공격에 관한 정보를 탐지 · 처리하여야 한다.

② 정보보호책임자는 제1항의 업무를 수행하기 위하여 사이버공격에 관한 정보를 실시간 탐지하는 장비[암호화된 사이버공격 패킷을 가시화(可視化)하는 장비를 포함한다]를 정보통신망에 설치 · 운용하거나 탐지규칙정보를 제공하여 관련 정보를 실시간 처리할 수 있다.

③ 정보보호책임자는 보안관제 과정에서 자동적으로 처리되는 다음 각 호의 정보를 수집 · 이용할 수 있다.

1. 사이버공격으로 인하여 발생한 패킷
2. 공격 주체 및 피해자를 식별하기 위한 IP주소 및 MAC주소, 전자우편 주소, 정보통신서비스 이용자 계정 정보, 피해자의 성명 및 연락처
3. 그 밖에 사이버공격의 방법 및 피해 확인 · 식별에 필요한 정보

제72조(초동 조치) 정보보호책임자는 사이버공격으로 인한 피해 최소화 및 확산 방지를 위하여 다음 각 호의 사항을 포함한 조치를 취하여야 한다.

1. 사이버공격 경유지(사이버공격에 악용되거나 악용될 우려가 있는 웹사이트 주소, IP주소, 전자우편 주소를 말한다) 및 공격 IP주소 차단
2. 피해 시스템을 정보통신망으로부터 분리하거나 악성프로그램의 동작을 정지시키는 조치
3. 사고 조사를 위한 피해 시스템 및 로그 기록의 보전

제73조(조치결과 통보) ① 정보보호책임자는 국가보안관리체계를 통해 사이버공격에 관한 정보를 제공받은 경우 제공받은 날로부터 5일 이내에 대응조치 결과를 외교부장관과 국가정보원장에게 통보하여야 한다.

② 정보보호책임자는 국가정보원장이 별도로 요청한 안보위해(危害) 공격을 최초 탐지하거나 초동 조치한 경우 관련내용을 즉시 외교부장관과 국가정보원장에게 통보하여야 한다.

제74조(보안관제 직원 교육) ① 정보보호책임자는 보안관제 업무 담당직원에 대한 교육

계획을 수립 · 시행하여야 한다.
② 정보보호책임자는 보안관제 업무 담당직원이 격년 20시간 이상 보안관제 관련 교육을 이수하도록 하여야 한다.

제2절 사고 대응

제75조(사이버공격으로 인한 사고) ① 정보보호책임자는 사이버공격으로 인한 사고(「보안업무규정」 제38조 각 항을 포함한다.) 발생 시 원인 분석 및 재발 방지를 위하여 다음 각 호에 해당하는 자료에 대해 조사해야 한다.

1. 공격 주체 및 피해자를 식별하기 위한 IP주소 및 MAC주소, 전자우편 주소, 정보통신서비스 이용자 계정 정보, 피해자의 성명 및 연락처
2. 사이버공격에 사용된 악성프로그램 및 공격 과정에서 생성 · 변경 또는 복제된 디지털정보
3. 공격 주체가 절취한 디지털정보
4. 공격 주체의 행위가 기록된 내역 또는 로그기록

② 직원등은 관계 법규에 접촉되지 않는 범위 내에서 제1항 각호의 자료를 제출하여야 하며 정보보호책임자는 제출받은 자료를 사고원인 분석, 공격자 의도 파악, 피해영향 평가 등 사이버공격에 대한 예방 및 대응과 관련한 목적으로만 사용하여야 한다.
③ 직원등은 사고 원인을 규명할 때까지 피해 시스템에 대한 증거를 보전하고 임의로 관련 자료를 삭제하거나 포맷하여서는 아니 된다.

제76조(정보통신보안 규정 위반 및 자료유출 사고) ① 정보보호책임자는 국가정보원장으로부터 「보안업무규정 시행규칙」 [별표 2]에 따른 정보통신보안 규정 위반사항에 대한 사실을 통보받은 경우 동 규정 시행규칙 제66조제3항에 따라 즉시 필요한 조치를 취하고 위규자, 위규 내용 및 조치 결과를 국가정보원장에게 통보하여야 한다.
② 직원등의 과실로 인하여 개인 소유의 정보통신기기 및 이동통신단말기, 상용 정보통신서비스에서 제1항에 따른 유출사고가 발생한 경우 정보보호책임자는 해당 직원등에게 저장자료 · 이용내역 등의 자료 제출을 요청할 수 있다.
③ 직원등은 제2항에 따른 요청이 위법하다고 판단하는 경우 그 사유를 소명하고 자료 제출을 거부할 수 있다.
④ 정보보호책임자는 제1항에 따른 조사를 통해 유출이 확인된 자료에 대하여 관계 기관의 장과 합동으로 국가안보 및 국익, 정부정책, 재단에 미치는 영향을 평가하여 필요한 조치를 취하여야 한다.

제8장 정보 협력

제77조(기관간 정보공유 협력) 정보보호책임자는 사이버공격의 예방 및 신속한 대응을 위하여 다음 각 호에 해당하는 정보(이하 “사이버위협정보”라 한다)를 다른 기관과 공유하도록 노력하여야 한다.

1. 사이버공격의 방법 및 대응조치에 관한 정보
2. 사이버공격에 사용된 악성프로그램 및 이와 관련된 정보
3. 정보통신망, 정보통신기기, 정보보호시스템 및 소프트웨어의 보안취약점에 관한 정보
4. 그 밖에 사이버공격 예방 및 대응에 필요한 정보

제78조(정보공유시스템 운영) ① 정보보호책임자는 국가정보원장이 사이버안보 정보의 배포와 각급기관 · 단체 간 사이버위협정보의 체계적 · 효율적 공유를 위하여 구축한 국가사이버위협 정보공유시스템(「사이버안보 업무규정」 제6조에 따른 정보공유시스템을 포함한다. 이하 “정보공유시스템”이라 한다)의 접근권한을 부여 받아 정보공유시스템을 운영할 수 있다.
② 정보보호책임자는 정보공유시스템에 사이버위협 관련 정보 등을 등록하거나 등록된 정보를 업무에 활용할 수 있으며 다음 각 호에 해당하는 사항을 준수하여야 한다.

1. 정보공유시스템 전용 단말기 운용
2. 정보공유시스템 접근 · 활용 및 단말기 운용 등을 위한 관리자 지정 · 운영
3. 정보시스템 개별사용자 등록 · 삭제 등 접근권한 관리
4. 정보공유시스템 전용 단말기 내 정보공유시스템 이용과 무관한 소프트웨어 설치 및 비인가 휴대용 저장매체 연결 사용 금지
5. 이용기관간 정보공유 활성화를 위하여 월 1회 이상 정보공유시스템 접속 · 활용
6. 기타 국가정보원장이 제시하는 보안대책

제79조(정보공유시스템의 정보 관리) 정보보호책임자는 정보공유시스템에 등록된 정보를 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따른 비공개 대상 정보 및 「국가정보자료관리규정」 제2조제1호에 따른 국가정보자료로서 취급 · 관리함을 원칙으로 한다.

부칙

제1조(시행일) 이 지침은 2024년 1월 1일로부터 시행한다.
제2조(경과조치) 이 지침 시행 이전에 행하여진 정보보안 업무는 이 지침에 따라 처리된 것으로 본다.
제3조(다른 내규와의 관계) 이 지침 시행 당시 다른 내규에서 종전의 「정보보호 조직 운영지침」, 「정보보호정책지침」, 「보안 점검지침」, 「정보시스템 도입 및 개발 보안지침」, 「외주업체 관리지침」, 「인력보안 및 정보보호 교육 지침」, 「정보시스템

운영보안 관리지침」, 「영상회의 보안지침」, 「계정권한 보안 관리지침」, 「생활 보안지침」, 「USB메모리 등 보조기억매체 보안관리지침」, 「물리적 보안지침」, 「보안사고 관리 및 대응지침」을 인용한 경우, 이 내규 가운데 그에 해당하는 규정이 있을 때에는 종전의 규정을 갈음하여 이 내규의 해당 규정을 인용한 것으로 본다.

별 표

【 별표 1 】

정보화사업 보안성 검토 처리기준

외교부 및 국가정보원 보안성 검토 대상 정보화사업

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 고유 식별정보를 처리하는 정보시스템 구축
5. 주요정보통신기반시설로 지정이 필요한 정보통신기반시설 구축
6. 제24조제1항에 따른 제어시스템 도입
7. 재난관리·국민안전·치안유지·비상사태 대비 등 국가위기 관리와 관련 한 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) 등 구축
15. 원격근무시스템 구축
16. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제20조에 따라 클라우드 컴퓨팅서비스제공자의 클라우드컴퓨팅서비스(이하 "민간 클라우드 컴퓨팅서비스"라 한다)를 이용하는 사업
17. 남북 회담 및 협력사업 등을 위한 북한지역 내 정보통신망 또는 정보시스템 구축
18. 외국에 개설하는 사무소 운영을 위한 정보통신망 또는 정보시스템 구축
19. 첨단 정보통신기술을 활용하는 정보화사업으로서 국가정보원장이 해당 기술에 대하여 안전성 확인이 필요하다고 지정하는 사업

외교부 보안성 검토 대상 정보화사업

1. 홈페이지 및 웹메일 등 웹기반 정보시스템 구축
2. 인터넷전화시스템 구축
3. 다른 기관의 정보통신망 또는 정보시스템과 연동하여 정보의 소통 또는 서비스를 제공하는 정보시스템 구축
4. 해당 기관의 정보통신망 또는 정보시스템과 분리된 외부인 전용무선랜, 인터넷망 및 교육장 정보통신망 등 구축
5. 인터넷과 분리된 소속 공무원등의 인사·복지관리 등의 목적을 위한 정보시스템 구축
6. 주요정보통신기반시설 취약점 분석·평가, 정보보안컨설팅 등 용역사업
7. 기존 분리된 내부망·기관 인터넷망간 자료전송시스템 구축 등 후속사업
8. 대규모 백업·재해복구센터 구축
9. 해당 기관의 정보통신망 또는 정보시스템과 분리된 영상회의시스템 구축
10. 인터넷과 분리된 CCTV 등 영상정보처리기기 구축
11. 백업시스템 구축
12. 대민(對民) 콜센터시스템 구축
13. 기타 해당 기관의 장이 필요하다고 판단하는 정보통신망 또는 정보시스템 구축

【 별표 2 】

안전성 검증필 제품 목록

X : 해당사항 없음

<table>
<tr><th rowspan="2">제품 유형</th><th colspan="4">아래 해당되는 항목 중에서 어느 하나 필요</th><th rowspan="2">검증필
암호모듈</th></tr>
<tr><th>CC인증 [1]</th><th>성능평가 [2]</th><th>보안기능
확인서 [3]</th><th>보안적합성
검증</th></tr>
<tr><td>스마트카드</td><td rowspan="15">국가용
보안요구사항

또는

국가용
보호프로파일
(PP)
준수</td><td>X</td><td>X</td><td>○</td><td>X</td></tr>
<tr><td>침입차단시스템</td><td>X</td><td rowspan="16">국가용·일반
보안요구사항
준수</td><td>X</td><td>X</td></tr>
<tr><td>침입방지시스템</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>통합보안관리제품</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>웹 방화벽</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>운영체제(서버) 접근통제제품</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>DB접근통제제품</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>네트워크접근통제제품</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>인터넷전화 보안제품</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>무선침입방지시스템</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>무선랜 인증제품</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>가상사설망제품</td><td>X</td><td>X</td><td>탑재 필요</td></tr>
<tr><td>디지털복합기</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>스마트폰 보안관리제품</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>스팸메일차단시스템</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>패치관리시스템</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>망간자료전송제품</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>DDoS 대응장비</td><td rowspan="3">국가용
보안요구사항
준수</td><td>X</td><td>X</td></tr>
<tr><td>안티바이러스제품</td><td>X</td><td>X</td></tr>
<tr><td>소스코드 보안약점 분석도구</td><td>X</td><td>X</td></tr>
<tr><td>네트워크 자료유출방지제품</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>호스트 자료유출방지제품</td><td>X</td><td>X</td><td>X</td><td>탑재 필요</td></tr>
<tr><td>S/W기반 보안USB제품</td><td>X</td><td>X</td><td>X</td><td>탑재 필요</td></tr>
<tr><td>가상화관리제품</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>네트워크 장비 [4]</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>저장자료 완전삭제제품</td><td>X</td><td>X</td><td>X</td><td>○</td><td>X</td></tr>
</table>

1)「지능정보화 기본법」 제58조제1항 및 같은 법 시행령 제51조에 따라 과학기술정보통신부장관이 고시한「정보보호시스템 평가·인증 지침」에 따른 인증(국내용 CC 또는 국제용 CC). 다만, 인증범위(TOE)에 각급기관이 사용할 보안기능이 포함되어 있어야 함

2) 「정보보호산업의 진흥에 관한 법률」 제17조에 따른 성능평가

3) 보안기능 시험기관이 발급하는 확인 증서

4) 네트워크 장비는 L3 이상 스위치 및 라우터 등을 의미

【 별표 3 】

‘암호가 주기능인 제품’ 도입요건

제품 유형	도입 요건	비 고
메일 암호화제품	검증필 암호모듈 탑재	-
구간 암호화제품		
하드웨어 보안토큰		
디스크·파일 암호화제품		
기타 암호화제품		
SSO제품	검증필 암호모듈 탑재 및 CC인증(국가용 보호프로파일 준수)	-
DB 암호화제품		
문서 암호화제품(DRM 등)		

※ 최신 도입요건은 국가정보원 홈페이지(암호모듈 검증) 참조

【 별표 4 】

보안적합성 검증 신청시 제출물

1. 최초검증 신청시 제출물

제출물	정보보호시스템		작성 주체
	상용 제품	자체(용역) 개발	
[별지 제4호서식]에 따른 보안적합성 검증 신청서	○	○	신청기관
[별지 제5호서식]에 따른 정보통신제품 도입확인서(현황)	○	○	
기술제안요청서 사본	○	○	
보안기능 점검표	○	○	
운용점검사항	○	○	
CC인증서 사본	○ (인증서 보유시)		업체
보안기능 운용 설명서	○	○	
기본 및 상세 설계서		○	
개발완료 보고서		○	

2. 재검증 신청시 제출물

제출물	정보보호시스템		작성 주체
	상용 제품	자체(용역) 개발	
[별지 제4호서식]에 따른 보안적합성 검증 신청서	○	○	신청기관
[별지 제5호서식]에 따른 정보통신제품 도입확인서(현황)	○	○	
보안기능 점검표	○	○	
운용점검사항	○	○	
변경내용 분석서	○	○	업체

별 지

【 별지 제1호 서식 】

정보보안위원회 개최 통지서

년 월 일

수 신 정보보안위원
제 목 OOOO년 제 OO차 정보보안위원회 개최

다음과 같이 한국국제교류재단 정보보안위원회를 개최하오니 참석하여 주시기 바랍니다.

- 다 음 -

1. 회의일시 : 년 월 일 00:00
2. 회의장소 :
3. 회의안건 :

한국국제교류재단 정보보안위원회 의장

【 별지 제2호 서식 】

제○○차 정보보안위원회 서면의결서

정보보안지침 제8조(정보보안위원회)에 의거, 아래 안건을 서면으로 동의를 얻어 의결하고자 하오니 찬성여부를 표기하여 주시기 바랍니다.

심의(보고)안건		의결사항		의 견
안건번호	제 목	찬성 (○)	반대 (×)	
제○○호				
제○○호				

위와 같이 심의 의결함.

년 월 일

직위 :

성명 : (서명)

【 별지 제3호 서식 】

보 안 서 약 서 (업체대표용)

서약업체 대표

업 체 명:

직 위:

성 명: (서 명)

본인은 한국국제교류재단(이하 "재단"이라 한다)의 "○○○" 업무를 수행함에 있어 업무상 취득한 정보의 중요성을 깊이 인식하고, 이에 관련된 소관 업무가 재단에 관함 기밀임을 인정한다.

1. 본인은 재단의 업무를 수행함에 있어 아래의 내용을 준수한다.
   ① 재단 내의 전반적 정보습득이나 운영상의 기밀을 절대 누설하지 않으며,
   ② 업무수행을 통해 축적된 정보를 임의 도용하거나 방출하지 않으며,
   ③ 재단의 운영상 불이익을 줄 수 있는 모든 내용을 외부에 유출하지 않으며,
   ④ 허락된 업무 이외의 업무는 일체 행하지 않으며,
   ⑤ 현행 정보보호 관련 제반 법령 및 규정을 준수한다.

2. 위의 사항들에 대하여 직무상 취득한 제반 비밀사항을 일체 누설하거나 공개하지 않을 것을 서약하며 업무 종료 후에는 관련 자료 일체를 반납한다.

3. 업무수행을 통해 생성된 모든 생성물의 소유권은 재단에 있음을 인정하며, 정보의 무단유출 방지를 위하여 재단이 시행하는 통제 및 정기/비정기적인 점검에 동의한다.

4. 본인은 하도급업체를 통한 사업 수행 시 하도급업체로 인해 발생하는 위반사항에 대하여 모든 책임을 부담한다.

5. 본인은 재단의 업무를 수행함에 있어 사용한 전산장비 및 소프트웨어, 데이터 등 유·무형의 자산을 훼손 또는 멸실시킴으로써 재단에 손해가 발생할 경우 이에 대한 손해배상책임을 진다.

6. 본인은 상기 서약사항을 위반할 경우 관련 법령에 의거 엄중한 처벌을 받을 것이며, 그에 따른 일체의 민·형사상의 책임을 질 것을 서약한다.

년 월 일

한국국제교류재단 귀하

【 별지 제4호 서식 】

보안적합성 검증 신청서

신청 기관	기관명		담당자	
	부서명		전화번호	
	사업명		이메일 ※ 상용메일 불가	
	도입 목적			
	보안성 검토명		계약 날짜	
			도입 날짜	
	검증결과 반영	취약점 등의 개선요청 이행 (□ 반영・개선 □ 반영불가)		
신청 제품	제품명	※ 신청 제품이 2種 이상인 경우, 별도 신청	S/W(펌웨어) 버전	
	제품 유형		도입 수량	대
	사전 인증 대상 여부	□ CC인증 대상 □ 검증필 암호모듈 탑재 □ 해당 없음 ※ CC인증・검증필 암호모듈 탑재 필수 제품은 국정원 홈페이지 참조		
	해시값 (SHA-512)	※ 해시값은 국정원 홈페이지에 게시된 S/W 사용		
	CC 인증기관		CC 인증등급	
	CC 인증번호		CC 만료일	
	암호모듈명		암호검증 번호	CM-
업체	업체명		대표자	
	주소			
	담당자명		전화번호	
	휴대폰번호		이메일	

※ △서식이 변경될 수 있으므로 국가정보원 홈페이지(든든한 안보→사이버안보→보안적합성 검증 →검증공지사항)에 게시된 양식을 참고 △'검증결과 반영'을 포함하여 기재 양식中 해당사항은 빠짐없이 기재

【 별지 제5호 서식 】

정보통신제품 도입 확인서(현황)

기관명		관계 중앙행정기관	
담당자		담당자 전화번호	
사업명			
보안성	보안성 검토받은 문서 제목 및 번호 표시 예) 000 보안성 검토결과(000-000, 2019.1.1)		

기관명	관계 중앙행정기관	제품명	제조사	제품 유형	보안기능 확인서			CC인증, GS인증, 성능평가			암호모듈검증 (KCMVP)		펌웨어 또는 OS버전	해시값 (SHA-512)	비고
					발급 번호	시험 기관	발급일	인증 번호	등급 또는 준수PP	인증 기관	암호 모듈명	암호 검증 번호			
				L3 스위치	ND-0001-0001-2019		2019-01-01		NDcPP			CM-00-000.0	이름 또는 버전		수량 등

※ △서식이 변경될 수 있으므로 국가정보원 홈페이지(든든한 안보→사이버안보→보안적합성 검증→검증 공지사항)에 게시된 양식을 참고하되, 반드시 엑셀(xlsx)양식을 준수 △해시값은 국가정보원 홈페이지에 등재된 S/W 활용

【 별지 제6호 서식 】

정보보안점검 체크리스트 V3.0

1. 정보보안 기본활동

연번	세부 점검사항	비고
1	정보보안 침해사고·규정위반 및 정보통신망 장애발생을 대비한 보고체계·조치절차가 마련되어 있는가?	
2	정보통신장비(노트북 등) 반출입 통제 및 현황 관리를 철저히 하는가?	
3	현지 행정원의 내부 정보시스템 접근을 통제하고 있는가?	

2. PC 및 서버 보안관리

연번	세부 점검사항	비고
1	PC·서버에 설치된 운영체제 및 응용프로그램을 최신 보안업데이트 하였는가?	
2	PC·서버의 불필요한 서비스를 검토하여 중단하고 정기적으로 인터넷에서 접속 가능여부를 확인하는가?	
3	백신이 자동 업데이트되고 실시간 감시기능이 설정되어 있는가?	
4	인터넷 PC에 업무관련 자료(비밀 포함)가 방치되어 있는가?	
5	P2P, 웹하드, 상용메신저 등 업무와 무관한 비인가 프로그램이 설치되어 있는가?	
6	비인가자 접근방지를 위해 CMOS·로그인 등 PC 비밀번호를 설정하였는가?	
7	정보통신망 구성측면에서 PC 및 서버 등의 위치가 적정한가?	
8	비밀은 비밀용 USB를 별도 지정하여 사용하고 일반자료와 혼합 저장하지 않는가?	
9	비인가 USB·정보통신기기 연결시 차단토록 보안 설정되어 있는가?	
10	불필요한 원격접속 S/W는 비활성화 또는 제거하였는가?	

3. 네트워크 보안관리

연번	세부 점검사항	비고
1	업무자료를 소통하기 위한 내부망은 인터넷과 분리 운영하는가?	
2	인터넷·업무망간 자료공유 방안이 적절한가?	
3	인가받지 않은 단말기가 네트워크에 연결하지 못하도록 조치하고 있는가?	
4	비인가 무선인터넷·무선랜 등 허가받지 않은 인터넷 접속경로가 존재하는가?	
5	해외에 위치한 사무소와 인원에 대해 보안대책을 지원하고 주기적으로 점검하는가?	

【 별지 제7호 서식 】

정보시스템 관리대장

연번	관리번호	구분	장비명 (용도)	모델명	제조사	운영체제	IP주소	호스트명	장비 관리자	위치	도입 년월
1	H2000	서버	그룹웨어	Sun Fire V890	Oracle	Solaris9	10.72.10.66	group	홍길동	양재 랙-R11	2012.08
2	H2001	스토리지	메일서버 스토리지	STK SE6140	IBM	N/A	192.168.105.17	N/A	김철수	양재 랙-R16	2012.10
3	H2003	PC	인터넷용	DM-V600	삼성전자	윈도우7	192.168.0.5	N/A	홍길동	제주본부 2층	2011.09

【 별지 제8호 서식 】

정보통신시설 출입관리대장

월 / 일	소 속	성 명	출입시간	퇴실시간	출입사유	확인(서명)
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		
			:	:		