대전관광공사 정보통신 보안업무내규

제정 2024. 6. 4. 내규 제 458호

제1장 총칙

제1조(목적) 이 내규는 대전관광공사(이하 “공사”라 한다“의 정보통신 보안업무를 처리하는데 필요한 사항을 규정함을 목적으로 한다.

제2조(정의) 이 내규에서 사용하는 용어의 뜻은 다음과 같다.

1. "정보보안" 또는 "정보보호"란 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 「국가사이버안전관리규정」 제2조제3호의 사이버안전을 포함한다.
2. "정보통신망"이란 「지능정보화 기본법」 제2조제8호에 따른 정보통신망을 말한다.
3. "내부망"이란 기관의 업무 수행을 위하여 인터넷과 별도로 분리하여 구축한 업무 전용(專用) 정보통신망을 말한다.
4. "기관 인터넷망"이란 공사 소속 직원의 업무 활용 또는 공개서버 운용을 주(主) 목적으로 인터넷과 연동하여 구축한 정보통신망을 말한다.
5. "정보시스템"이란 「전자정부법」 제2조제13호에 따른 정보시스템으로 PC·서버 등 단말기, 보조기억매체, 전산·통신장치, 정보통신기기, 응용프로그램 등 정보의 수집·가공·저장·검색·송수신에 필요한 하드웨어 및 소프트웨어 일체를 말한다.
6. "정보시스템 관리자"란, 정보시스템으로 정의되는 하드웨어 및 소프트웨어를 다루는 직원을 말하며, 전산담당자 또는 공사 직원이 될 수 있다.
7. "휴대용 저장매체"란 CD·외장형 하드디스크·USB메모리 등 정보를 저장할 수 있는 것으로 PC·서버 등의 정보시스템과 분리할 수 있는 기억장치를 말한다.

8. "정보통신실"란 서버・스위치・라우터・교환기 등 전산 및 통신장비 등이 설치・운용되는 장소 또는 전산실・통신실・데이터센터 등을 말한다.
9. "정보보호시스템"이란「지능정보화 기본법」제2조제15호에 따른 정보보호시스템을 말한다.
10. "사이버공격"이란 해킹・컴퓨터바이러스・논리폭탄・메일폭탄・서비스방해 등 전자적 수단을 사용하여 정보통신망을 불법침입・교란・마비・파괴하거나 정보를 위조・변조・훼손・절취하는 행위를 말한다.
11. "보안관제"란 사이버공격을 실시간으로 즉시 탐지 및 분석, 대응하는 일련의 활동을 말한다.
12. "취약점"이란 사이버공격에 악용되어 관리자가 설정한 접근 권한外 정보를 열람・취득하게 하거나 보안기능을 회피 가능하게 하는 정보통신망・정보시스템의 결함을 말한다.
13. "클라우드컴퓨팅(Cloud Computing)"이란 직접・공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원을 이용자의 요구나 수요변화에 따른 정보통신망을 통하여 신축적으로 이용할 수 있도록 하는 정보처리체계를 말한다.

제3조(적용범위) 정보보안업무 취급에 있어 국가정보원 “보안업무규정 및 국가 정보 보안 기본지침”이 정하는 것을 제외하고는 이 내규가 정하는 바에 따른다.

제4조(정보보안담당관 임명) 정보보안담당관은 정보보안과 관련된 업무를 수행하는 부서의 장으로 임명·운영한다.

제5조(정보보안담당관 책무) ① 정보보안업무를 효율적이고 체계적으로 수행하기 위하여 정보보안 전문지식을 보유한 적정인력을 확보하여 정보보안 전담조직을 구성・운영하여야 한다.

② 전담조직을 운영하는 경우, 다음 각 호에 해당하는 업무를 전담하여 업무를 수행한다.

1. 정보보안 정책・계획의 수립・시행 및 정보보안 업무 지도・감독

2. 정보보안 전담조직 관리, 전문인력 및 관련예산 확보
3. 정보통신실, 정보통신망 및 정보자료 등의 보안관리 활동
4. 소관 주요정보통신기반시설 보호 활동
5. 보안관제, 사고대응 및 정보협력 업무 총괄
6. 정보보안교육 총괄 및 사이버보안진단의 날 계획 수립·시행
7. 정보보호시스템의 운용 및 보안관리
8. 그 밖에 정보보안 관련 사항
9. '사이버보안진단의 날' 내PC 지키미 이행 및 감독에 관한 사항
10. 악성코드 유무 및 인터넷망 PC에 업무자료 무단 사용의 주기적 점검에 관한 사항
11. PC, 휴대용 저장매체 등 정보자산 및 네트워크 현황 관리

③ 정보보안담당관은 제2항 각 호에 해당하는 업무를 수행함에 있어 필요한 경우 해당 업무의 일부를 전산담당자에게 위임할 수 있다.

제6조(정보보안교육) ① 정보보안담당관은 정보보안 교육계획을 수립하여 연 1회 이상 전 직원을 대상으로 교육(온라인 교육을 포함한다)을 실시하여야 한다.

② 정보보안담당관은 공사 소속 직원의 업무 전문성을 제고하고 소속 직원등의 정보보안 지식을 함양하기 위하여 전문기관의 교육 이수나 학술회의 참가 등을 장려하여야 한다.

제7조(사이버보안진단의 날) ① 정보보안담당관은 매월 세번째 수요일을 사이버보안진단의 날로 지정·시행하여야 한다. 다만, 부득이한 사유로 해당 일에 시행하지 못할 경우 같은 달 다른 날에 시행하여야 한다.

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

③ 전산담당자는 종합적인 보안진단 외에 추가적으로 직원들의 PC 및 기타 전산장치에 대해 보안 설정을 권고하여야 한다.

제2장 정보화사업 보안

제1절 사업 계획

제8조(보안책임) ① 각 부서에서 정보통신망 또는 정보시스템을 개발·구축·운용·유지보수하는 사업(「지능정보화 기본법」 제11조제1항에 따른 지능정보화계획에 따른 사업을 포함한다. 이하 “정보화사업”이라 한다)은 해당 정보화사업에 대한 보안관리를 수행하여야 한다.

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

③ 정보보안담당관은 필요한 경우 각종 정보화사업과 관련한 보안대책의 적절성을 평가하고 정보화사업 수행 전반에 대하여 보안대책의 이행 여부를 점검하여 정보화사업을 추진하는 부서의 장에게 시정을 요구할 수 있다.

제9조(보안대책 수립) 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
5. 긴급사태 대비 및 재난복구 계획
6. 용역업체 작업장소에 대한 보안대책
7. 온라인 개발 또는 온라인 유지보수가 필요하다고 판단할 경우
8. 누출금지정보 보안관리 방안

제10조(제안요청서 기재사항) ① 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 보안 준수사항 또는 보안대책

3. 누출금지정보 목록

② 제1항제3호에 따른 누출금지정보 목록을 작성할 경우 다음 각 호의 사항을 포함하여야 한다.

1. 기관 소유 정보시스템의 내·외부 IP주소 현황
2. 세부 정보시스템 구성현황 및 정보통신망 구성도
3. 사용자계정·비밀번호 등 정보시스템 접근권한 정보
4. 정보시스템(서버, 네트워크, 보안장비) 취약점 분석 및 결과물
5. 정보화사업 결과물 및 프로그램 소스코드
6. 국가용 보안시스템 및 정보보호시스템 도입 현황
7. 침입차단시스템(방화벽), 침입방지시스템(IPS) 등 정보보호제품 및 라우터, 스위치 등 네트워크 장비 설정 정보
8. '공공기관의 정보공개에 관한 법률' 제9조 1항에 따라 비공개 대상 정보로 분류된 기관의 내부문서
9. '개인정보 보호법' 제2조 1호의 개인정보
10. '보안업무규정' 제4조의 비밀, 동 시행규칙 제16조 제3항의 대외비
11. 그 밖에 각급기관의 장이 공개가 불가하다고 판단한 자료

제2절 보안성 검토

제11조(검토 시기 및 절차) ① 정보화사업을 수행하고자 할 경우 정보화사업과 관련한 보안대책의 적절성을 평가하기 위하여 사업 계획 단계(사업 공고 전)에서 보안성 검토 절차를 이행하여야 한다.

② 제1항에 따른 보안성 검토를 위하여 자체적으로 수립한 보안 대책에 대하여 상급기관의 장에게 검토를 의뢰하여야 한다.

③ 보안성 검토는 서면 검토를 원칙으로 하며 상급기관의 장이 필요하다고 판단하는 경우 현장 확인을 병행 실시할 수 있다.

제12조(검토 생략) ① 다음 각 호에 해당하는 정보화사업에 대하여는 보안성 검토 절차의 이행을 생략할 수 있다. 이 경우 관련 매뉴얼·가이드라

인 등을 준수하는 등 자체 보안대책을 수립·시행하여야 한다.

1. 정보화사업에 해당하지 아니하는 단순장비·물품 도입
2. 보안성 검토를 거쳐 완료한 정보화사업에 대하여 정보통신망 구성을 변경하지 아니하는 범위에서 다음 각 목의 사항을 포함 한 후속운영·유지보수·컨설팅(단일 회선의 이중화는 본 호를 적용함에 있어 정보통신망 구성의 변경이 아닌 것으로 본다)
   가. 서버·스토리지·네트워크 장비 등 장비 노후화로 인한 단순 장비 교체
   나. 전화기·무전기·CCTV 등 통신·영상기기의 노후화로 인한 단순 장비 교체
   다. 기존 운용하던 정보보호시스템을 동일한 보안기능을 보유한 다른 정보보호시스템으로 교체
3. 다년도에 걸쳐 계속되는 사업으로써 사업 착수 당시 보안성검토를 완료 한 후 사업 내용의 변동 없이 계속 추진하는 운영·유지사업
4. PC·프린터 및 상용 소프트웨어 등 단순 제품 교체

제13조(검토결과 조치) 사업 추진 담당자는 보안성 검토결과를 통보받은 경우 검토결과를 반영하여 보안대책을 보완하여야 한다.

제3절 제품 도입

제14조(정보통신제품 도입) ① 정보보안담당관은 정보 및 정보통신망 등을 보호하기 위하여 보안기능이 있는 다음 각 호에 해당하는 정보통신제품을 도입할 수 있다.

1. 국가정보원장이 별도로 공지하는 도입요건을 만족하는 제품
2. 제품유형의 특성상 보안기능의 비중이 미미하여, 자유롭게 도입·운용이 가능한 '단순 보안기능 제품유형'으로 국가정보원장이 공지한 제품
3. 국가정보원장의 요청에 따라 취약 정보통신제품을 긴급 대체하기 위하여 도입하는 제품

② 제1항제1호에 해당하는 제품은 필요하다는 판단하에, 실제 적용·운용 이전에 보안적합성 검증을 받아야 한다.

제15조(영상정보처리기기 도입) 영상정보처리기기 담당자는 영상정보처리기기를 도입하고자 할 경우 한국정보통신기술협회(TTA)의 공공기관용 보안 성능품질 인증 등 일정한 보안성능이 확인된 제품을 우선적으로 도입할 수 있다.

제4절 계약 및 사업수행

제16조(용역업체 보안) ① 용역업체에 정보화사업을 발주할 경우 다음 각 호의 보안사항을 준수하도록 계약서에 명시하여야 한다.

1. 제안요청서에 포함된 사항
2. 원격지 개발, 원격지에서의 온라인 개발, 온라인 유지보수를 허용할 경우 보안 준수사항
3. 소프트웨어 개발보안에 필요한 사항
4. 사업 참여인원의 보안관련 준수사항과 위반할 경우 손해배상 책임 명시, 용역 참여인원에 대한 친필 보안서약서 제출 등
5. 사업 수행과 관련한 보안교육, 보안점검 및 사업기간 중 참여인원 임의 교체 금지
6. 정보통신망 구성도·IP주소 현황 등 업체에 제공하는 자료는 자료 인계 인수대장을 비치하여 보안조치 후 인계·인수하고 무단 복사 및 외부반출 금지
7. 업체의 노트북·휴대용 저장매체 등 관련 장비는 반출·입시마다 악성코드 감염여부, 누출금지정보 무단 반출여부 등 점검
8. 사업 종료시 업체의 노트북·휴대용 저장매체 등 관련 장비는 저장자료 복구가 불가하도록 완전 삭제, 사업자 대표자 명의 보안확약서 제출
9. 사업 종료 시 누출금지정보를 포함한 용역 결과물 전량 회수하고 비인가자에게 제공·열람 금지
10. 그 밖에 기관의 장이 보안관리가 필요하다고 판단하는 사항 또는 국

가정보원장이 보안조치를 권고하는 사항

② 용역사업 추진 시 과업지시서・입찰공고・계약서에 누출금지 대상정보를 명시해야 하며, 해당 정보 누출 시 입찰 참가자격 제한을 위한 부정당업자로 등록하여야 한다.

③ 비밀 및 중요 용역사업을 수행할 경우 용역업체 참여인원이 다음 각 호에 해당되는 사실을 알게 된 경우 교체를 요구하여야 한다.

1.「국가공무원법」제33조제3호부터 제6호의4까지에 해당하는 사람

2.「국가를 당사자로 하는 계약에 관한 법률」제27조제1항 각 호의 행위를 한 사람

④ 정보보안담당관은 다음 각 호에 따른 보안 준수사항의 이행여부를 정기 또는 수시로 점검(불시 점검을 포함한다)하고 미비점을 발견한 경우 용역업체로 하여금 시정 조치하도록 하여야 한다. 이 경우 해당 사업 담당자가 점검한 후 그 결과를 정보보안담당관에게 통보하여야 한다.

1. 계약서에 명시된 보안 준수사항

2. 발주기관 내 작업장소 보안 준수사항

3. 원격지 개발보안 및 원격지에서의 온라인 개발 시 보안 준수사항

4. 정보시스템 유지보수 및 온라인 유지보수 시 보안 준수사항

⑤ 정보보안담당관은 제3항 및 제4항에 따른 점검 결과, 용역업체 보안대책 준수가 미흡하고 시정조치가 어렵다고 판단할 경우 원격지 개발, 원격지에서의 온라인 개발 또는 온라인 유지보수 허가를 취소할 수 있다.

제17조(원격지 개발보안) ①「소프트웨어 진흥법」제49조제3항 및 제4항,「소프트웨어사업 계약 및 관리감독에 관한 지침」제14조에 따라 용역업체가 발주기관 이외 장소(이하 "원격지"라 한다)에서 개발 작업(유지보수는 제외한다)을 수행하고자 요청할 경우 해당 사업 담당자는 용역업체 작업장소에 대한 보안요구사항 등을 포함한 관리적・기술적 보안대책을 수립・시행하여야 한다. 이 경우 정보보안담당관의 승인을 받아야 한다.

② 용역 수행 업체는 원격지내 정보시스템에 대하여 개발 작업을 위하여 필요한 경우 해당 사업 담당자의 보안통제 하에 인터넷에 연결할 수

있다.

제18조(소프트웨어 산출물 제공) ① 사업 담당자는 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 사업 담당자는 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.

③ 사업 담당자는 용역업체가 소프트웨어 산출물을 제3자에게 제공하고자 할 경우 제공하기 이전에 정보보안담당관의 승인을 받도록 하여야 한다.

④ 그 밖에 소프트웨어 산출물 제공과 관련한 사항은 「소프트웨어사업 계약 및 관리감독에 관한 지침(과학기술정보통신부 고시)」 제32조를 준수하여야 한다.

제19조(누출금지정보 유출시 조치) ① 해당 사업 담당자는 용역업체가 제안요청서 또는 계약서에 명시된 누출금지정보를 유출한 사실을 알게 된 경우 업체를 대상으로 계약 위반에 따른 조치를 취하여야 한다. 이 경우 용역업체의 누출 금지정보 유출 사실을 알게 된 직원 및 관계자는 즉시 정보보안담당관을 거쳐 사장에게 보고하여야 한다.

② 제1항에 따라 용역업체의 누출금지정보 유출 사실을 알게 되거나 보고를 받은 기관의 장은 그 사실을 직접 또는 상급기관을 통하여 「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.

제5절 보안적합성 검증

제20조(검증대상 제품) 보안기능이 있는 정보통신제품을 도입하는 경우 실제 적용·운용 이전에 안전성을 확인하기 위하여 보안적합성 검증을 받아야 한다.

제21조(검증 기관 및 신청) ① 해당 사업 담당자는 보안적합성 검증을 받고자 할 경우 정보보안담당관의 경유를 통해 상급기관에 신청하여야 한다.

② 해당 사업 담당자는 제1항에 따라 보안적합성 검증을 신청할 경우 상급기관에 별표 1의 보안적합성 검증 신청시 제출물에 해당하는 문서 등을 제출하여야 한다.

③ 제1항에 따라 검증을 신청한 경우 상급기관의 장이 필요하다고 판단하여 추가 자료를 요청할 경우 이를 제출하여야 한다.

제22조(검증결과 조치) 보안적합성 검증을 완료한 경우 적합여부·개선방안 등 제품의 안전성을 종합 검토한 검증 결과에 대한 해당 조치를 실시하고 그 결과를 상급기관의 장에게 통보하여야 한다.

제23조(취약점 조치) ① 보안적합성 검증이 완료된 제품에서 새로운 취약점이 발견된 경우 이를 제거 또는 보완하고 그 결과를 정보보안담당관에게 통보하여야 한다.

② 보안적합성 검증이 완료된 제품에서 새로운 취약점이 발견된 경우 상급기관의 취약점의 제거 또는 보완 조치를 요청받아 이에 대한 취약점의 제거 또는 보완조치를 실시하고 그 결과를 정보보안담당관에게 통보하여야 한다.

제3장 정보통신망 및 정보시스템 보안

제1절 정보통신망 보안

제24조(내부망·인터넷망 분리) ① 전산담당자은 내부망과 기관 인터넷망을 분리·운영할 수 있다.

② 전산담당자는 내부망과 기관 인터넷망을 분리·운영하고자 할 경우 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 기관 인터넷망간 안전한 자료전송 대책

5. 그 밖에 국가정보원장이 배포한 「국가·공공기관 업무전산망 분리 및 자료전송 보안가이드라인」에서 제시하는 보안대책

③ 정보보안담당관은 내부망과 기관 인터넷망의 IP주소 현황을 정기적으로 확인하고 갱신하여야 한다.

제25조(클라우드컴퓨팅 보안) ① 정보보안담당관은 클라우드컴퓨팅(공공클라우드 센터를 포함)을 자체 구축·운영하고자 할 경우, 국가정보원장이 배포한 「국가 클라우드 컴퓨팅 보안 가이드라인」에 명시된 기관 자체 클라우드컴퓨팅 구축 보안기준에 따라 보안대책을 수립·시행하여야 한다.

② 정보보안담당관은 민간 클라우드컴퓨팅서비스를 이용하고자 할 경우 다음 각 호에 해당하는 사항을 준수하여야 한다.

1. 국내에 위치한 정보시스템(인증서버, 로그 및 백업서버 등)·관리주체에 의해 데이터가 저장·관리되는 서비스의 이용

2. 다음 각목의 요건에 따라 일반 이용자용 서비스와 영역이 분리되어 제공되는 서비스(이하 “공공 전용(專用) 민간클라우드”라 한다)의 이용

가. 영역 분리는 일반 이용자용 서비스와 데이터 및 프로세스 등의 간섭 없이 이용 기관의 보안관제, 사고조사, 예방보안활동 유지를 위한 제반 환경을 만족해야 함

나. 영역 분리는 ‘시스템 중요도’에 따라 물리적 또는 논리적으로 구현

다. ‘시스템 중요도’ 분류는 [별표 3]의 기준 준용

3. 국가정보원장이 배포한 「국가 클라우드 컴퓨팅 보안가이드라인」에서 정하는 바에 따라 국가정보원장이 게시하거나 게시 예정인 민간 클라우드컴퓨팅서비스 이용

4. ‘내부망·인터넷망 분리’ 원칙 등 여타 보안 관련사항은 「국가정보보안기본지침」 및 「국가 클라우드 컴퓨팅 보안가이드라인」 준수

③ 내부망과 연동된 공공 전용(專用) 민간클라우드는 이 규정을 적용함에 있어 내부망으로 본다.

④ 기관 인터넷망과 연동된 공공 전용(專用) 민간클라우드는 이 규정을 적용함에 있어 기관 인터넷망으로 본다.

⑤ 제2항에 따라 민간 클라우드컴퓨팅서비스를 이용하는 해당 사업 담당자는 클라우드컴퓨팅서비스제공자에 의하여 누출금지정보가 유출된 경우 제29조에 따른 조치를 취하여야 한다.

⑥ 제2항에 따라 민간 클라우드컴퓨팅서비스의 제공자는 공공 전용(專用) 민간클라우드 영역에 대해 정부 기관에 준하는 보안관리 책임을 진다.

제26조(보안·네트워크장비 보안) ① 전산담당자는 침입차단·탐지시스템, 스위치·라우터 등 기관 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 청사 내 지정 단말기로부터의 접속·관리 허용

가. 장비 관리자의 접속

나. 발주기관내 용역업체 작업장소에서의 접속

3. 최초 설치할 경우 디폴트(default) 계정은 삭제하거나 변경 사용하고

장비 관리를 위한 관리자 계정을 별도로 생성·운영

4. 불필요한 서비스 포트와 개별사용자 계정은 차단 및 삭제

5. 펌웨어 무결성과 컴퓨터 운영체제·소프트웨어의 취약점 및 버전 업데이트 여부를 정기적으로 점검하고 최신 버전으로 유지

② 전산담당자는 로그기록을 1년 이상 유지하여야 하고 비(非)인가자의 접속 여부를 정기적으로 점검하여 그 결과를 정보보안담당관에게 통보하여야 한다.

③ 보안·네트워크장비 관리자는 침입차단·탐지시스템의 침입차단·탐지규칙(rule)의 생성 근거를 유지하고 정기적으로 필요성 여부를 점검·갱신하여야 한다.

제27조(무선랜 보안) ① 전산담당자는 내부망을 제외한 정보통신망에서 다음 각 호의 경우와 같이 공사 내에 무선랜(WiFi)을 구축·운용할 수 있다.

1. 기관 인터넷망에 중계기(AP)를 설치하여 공사에서 지급한 단말기의 접속만을 허용하는 업무용 무선랜

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

제28조(이동통신망 보안) ① 전산담당자는 이동통신망(HSDPA·WCDMA·LTE·5G 등)을 이용하여 시스템을 구축하거나 중요자료를 소통하고자 할 경우 암호화 및 비인가 단말기의 이동통신망 접속 차단 등 기술적 보안대책을 수립·시행하여야 한다.

② 전산담당자는 제1항에 따라 이동통신망을 이용한 시스템을 구축·운용할 경우 해당 기관의 정보통신망과 혼용되지 않도록 하여야 한다.

제29조(파견자용 정보통신망) ① 전산담당자는 다른 기관에 파견된 소속 직원등의 활용을 위하여 파견기관의 장과 협의하여 원(原) 소속 기관의

정보통신망 전용(專用) 단말기를 파견기관에 설치·운영할 수 있다.

② 전산담당자는 제1항에 따라 단말기를 설치할 경우 단말기와 기관 정보통신망 간 소통내용을 보호하여야 한다.

③ 제1항에 따라 각급기관의 내부망과 연동된 단말기는 이 지침을 적용함에 있어 원(原) 소속 기관의 내부망 단말기로 본다.

④ 제1항에 따라 각급기관의 기관 인터넷망과 연동된 단말기는 이 지침을 적용함에 있어 원(原) 소속 기관의 기관 인터넷망 단말기로 본다.

제2절 정보시스템 보안

제30조(정보시스템 보안책임) ① 정보보안담당관은 정보시스템(PC·서버·네트워크장비·정보통신기기 등을 포함한다)을 도입·운용할 경우 해당 정보시스템에 대하여 관리자 및 관리책임자를 지정·운영하여야 한다.

② 정보시스템 관리자 및 전산담당자는 서버·네트워크장비 등 부서가 공동으로 사용하는 정보시스템의 운용·관리에 대한 보안책임을 진다.

③ 정보시스템 관리자는 별지 제1호서식에 따른 정보시스템 관리대장을 수기 또는 전자적으로 작성·관리하여야 한다.

④ 정보시스템 관리자는 해당 부서의 별지 제1호서식에 따른 정보시스템 관리대장에 정보시스템의 최종 변경 현황을 유지하여야 하며 사본 1부를 정보보안담당관에게 제출하여야 한다.

⑤ 정보보안담당관은 정보시스템 운용과 관련하여 보안취약점을 발견하거나 보안대책 수립이 필요하다고 판단하는 경우 정보시스템 관리자 및 관리자에게 개선 조치를 요구할 수 있으며 조치가 완료될 때까지 정보시스템의 운용을 일시 제한할 수 있다.

제31조(정보시스템 유지보수) ① 정보시스템의 유지보수와 관련한 절차, 주기, 문서화 등과 관련한 사항을 자체 규정(또는 지침 등)에 포함하여야 한다. 정보시스템의 유지보수 절차 및 문서화를 수립할 경우 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 정보시스템 관리자는 용역업체 등이 유지보수와 관련한 장비·도구 등을 발주기관내 용역업체 작업장소로 반출·입할 경우 악성코드 감염 여부 및 자료 무단 반출여부 확인 등 보안조치를 실시하고 그 결과를 정보보안담당관에게 제출하여야 한다.

③ 정보시스템 관리자는 직접 또는 용역업체를 활용하여 정보시스템을 유지 보수할 경우 콘솔 또는 지정된 단말기로부터의 접속만을 허용하여야 한다.

④ 정보시스템 관리자는 정보시스템에 대하여 중요도·가용성 등에 따라 등급을 분류하고 해당 등급에 맞게 정보 보존 및 관리, 장애관리, 보안관리 등을 수행하여야 한다.

제32조(지정 단말기를 통한 온라인 유지보수) ① 지정된 단말기를 통해 유지보수를 함에 있어 해당 사업 담당자가 필요하다고 판단하고 용역업체가 다음 각 호에 따른 보안대책에 서면으로 동의하는 경우에 한하여, 해당 사업 담당자는 용역업체에게 내부망을 포함하여 소관 정보시스템(제37조제1항에 따른 보안·네트워크 장비는 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 용역 통제시스템 접속 전용(專用)으로 운용하고 다른 목적의 인터넷 접속은 차단

3. 발주기관내 온라인 용역 통제시스템을 경유하여 유지보수 대상 정보시스템에 접속하는 등 소통구간 보호·통제

4. 접속사실이 기록된 로그기록을 1년 이상 보관

② 전항 제2호 및 제3호에도 불구하고 온라인 용역 통제시스템이 구축되지 않음에도 불구하고 업무 수행에 현저한 저해가 있다고 예상되는 경우에는 인터넷망 정보시스템에 한하여 직접 접속하는 온라인 유지보수를 일시적으로 허용할 수 있다.

제33조(로그기록 유지) ① 정보시스템의 효율적인 통제·관리 및 사고 발생시 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 사용 등 외부발송 정보 등

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

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

⑤ 정보시스템 관리자는 로그기록을 1년 이상 보관하여야 하며 로그기록의 위조·변조 및 외부유출 방지대책을 수립·시행하여야 한다.

제34조(모바일 업무 보안) ① 휴대폰·태블릿 PC 등을 이용한 모바일 업

무환경(내부 행정업무, 현장 행정업무 및 대민서비스 업무 등)을 구축·운용하고자 할 경우 보안대책을 수립·시행하여야 한다.

② 그 밖에 모바일 업무 보안과 관련한 사항은 국가정보원장이 배포한 「국가·공공기관 모바일 활용업무에 대한 보안가이드라인」을 준수하여야 한다.

제35조(원격근무 보안) ① 직원등이 재택근무, 출장지 현장 근무 또는 파견 근무(기관 정보통신망 전용(專用) 단말기를 설치 운영하는 경우는 제외한다)시 인터넷을 통해 본인 인증을 거쳐 기관 정보시스템에 접속하여 온라인상으로 업무를 수행(이하 “원격근무”라 한다)하게 할 수 있다.

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

1. 기관 인터넷망에 위치한 서버 및 서버에서 구동되는 가상 PC

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

5. 원격근무시스템에 대한 보안취약점 정기 점검

④ 원격근무자는 원격근무용 단말기(개인 소유의 정보통신기기를 포함한다)의 보안을 위하여 취하는 다음 각 호의 조치에 적극 협조하여야 한다.

1. 소속된 기관에서 지급받은 단말기의 경우 단말기 보안대책 준수

제36조(저장매체 불용처리) ① 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. 이 경우 정보시스템 관리자 및 개별사용자는 정보보안담당관과 협의하여야 한다.

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

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

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

제3절 자료 보안

제37조(비밀의 전자적 처리) ① 「보안업무규정」에 따라 비밀의 생산, 분류, 보관, 열람, 출력, 송신·수신, 이관, 파기 등을 전자적으로 처리할 수 있다.

② 제1항에 따라 비밀을 전자적으로 처리할 경우 내부망과 기관 인터넷망이 물리적으로 분리된 기관은 내부망 PC에서 비밀을 전자적으로 처리할 수 있다.

③ 종이문서로 출력된 비밀의 관리에 관하여는 「보안업무내규」를 준수하여야 한다.

제38조(비공개 업무자료 처리) ① 비공개 업무자료를 다음 각 호의 어느 하나에 해당하는 방법으로만 처리하여야 한다.

1. 소속 또는 근무중인 기관의 내부망 PC 및 서버에 작성 및 저장·보관
2. 소속 또는 근무중인 기관의 장이 지급한 휴대용 저장매체에 작성 및 저장·보관
3. 다음 각 목의 어느 하나에 해당하는 수단(이하 “업무자료 공식 소통수단” 이라 한다)을 이용한 수신·발신 또는 등재·열람
   가. 소속 또는 근무중인 기관의 장이 자체적으로 구축·운용하는 전자우편시스템(이하 “기관 전자우편”이라 한다)
4. 그 밖에 다른 법규에 따라 허용되는 처리방법

② 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 경우 소속 또는 근무중인 기관의 장이 지급한 인터넷 PC 또는 출장용 노트북을 이용하여 비공개 업무자료를 처리할 수 있다.

1. 업무자료 공식 소통수단의 발신 또는 등재 기능을 이용하여 문장 또는 문구 작성
2. 업무자료 공식 소통수단의 수·발신 또는 등재·열람 과정에서의 일시적 저장
3. 기관 인터넷망 PC에 작성·저장
4. 영상회의 솔루션을 활용하여 비공개 업무자료의 화면 영상을 공유하기 위한 일시적 저장

③ 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 발신 기능 또는 등재 기능을 이용하여 문장 또는 문구 작성
2. 업무자료 공식 소통수단의 수·발신 또는 등재·열람 과정에서의 일시적 저장
3. 원격근무시스템에 접속하여 작성
4. 「감염병의 예방 및 관리에 관한 법률」 제34조제1항에 따른 감염병 위기관리 조치 등 대규모 질병·재난 발생 등 특별한 사정으로 재택근무를 명받았으나 소속 또는 근무중인 기관에 원격근무시스템이 구축되지 아니한 경우
5. 영상회의 솔루션을 활용하여 비공개 업무자료의 화면 영상을 공유하기 위한 일시적 저장

④ 제3항제5호에 해당하는 경우를 제외하고는 「정보통신망 이용촉진 및

정보보호 등에 관한 법률」 제2조제1항제2호에 따른 정보통신서비스(전자우편・메신저 등을 포함한다) 또는 국외에서 제공하는 이와 유사한 서비스(이하 “상용 정보통신서비스”라 한다)를 이용하여 비공개 업무자료를 작성, 저장, 수・발신하여서는 아니 된다.

⑤ 제2항부터 제4항까지에 따라 작성・저장한 비공개 업무자료는 활용이 종료된 후에는 삭제하여야 한다.

제39조(공개 업무자료 처리) 직원은 관계 법규에 위배되지 않는 범위 내에서 인터넷 PC나 개인이 소유한 PC・휴대용 저장매체・휴대폰, 상용 정보통신서비스 등을 이용하여 공개 업무자료를 처리할 수 있다.

제40조(홈페이지 등 게시자료 보안) ① 홈페이지 담당자는 해당 부서에서 홈페이지 등에 업무자료를 게시하고자 할 경우 자료 내용을 해당 부서의 장과 사전 검토하여 비공개 업무자료가 게시되지 아니하도록 하여야 한다.

② 홈페이지 담당자는 소속 부서에서 운용하는 홈페이지에서 비공개 업무자료가 무단 게시되었는지 여부를 정기적으로 점검하여야 한다.

③ 홈페이지 등에 비공개 업무자료가 무단 게시된 사실을 알게 된 경우 즉시 삭제 또는 차단 등 보안조치를 취하여야 한다.

제4절 사용자 보안

제41조(개별사용자 보안) ① 전산담당자는 소관 정보통신망 또는 정보시스템의 사용과 관련하여 다음 각 호의 사항을 포함한 개별사용자 보안에 관한 절차 및 방법을 마련하여야 한다.

1. 임무별 정보통신망 접근권한 부여 심사
2. 비밀 취급시 비밀취급 인가, 보안서약서 징구 등 보안조치
3. 암호자재 취급시 암호취급자 지정・관리

4. 보직변경, 퇴직 등 변동사항 발생시 정보시스템 접근권한 조정

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

제42조(단말기 보안) ① 개별사용자는 공사에서 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 중단시 비밀번호 등을 적용한 화면보호 조치
3. 최신 백신 소프트웨어 설치
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) 다운로드시 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. 내부망과 기관 인터넷망이 분리된 기관의 인터넷 PC에서는 각급기관의 장이 정한 특별한 사유가 없는 한 문서프로그램을 읽기 전용(專用)으로 운용
10. 그 밖에 국가정보원장이 안전성을 확인하여 배포한 프로그램의 운용 및 보안권고문 이행

③ 전산담당자는 정보보안담당관 총괄 하에 개별사용자의 제2항 각 호

에 해당하는 보안대책의 준수여부를 정기적으로 점검하고 개선 조치하여야 한다.

제43조(계정 관리) ① 전산담당자는 개별사용자에게 소관 정보통신망 또는 공용(公用) 정보시스템의 접속에 필요한 사용자 계정(아이디)을 부여하고자 할 경우 다음 각 호에 해당하는 사항을 준수하여야 한다.

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

② 전산담당자는 개별사용자가 시스템 접속(로그온)에 5회 이상 실패할 경우 접속이 중단되도록 시스템을 설정하고 비(非)인가자의 침입여부를 점검하여야 한다.

③ 전산담당자는 개별사용자의 보직변경, 퇴직, 계약종료 등 변동사항이 발생할 경우 신속히 사용자 계정을 삭제하거나 부여된 접근권한을 회수하여야 한다.

제44조(비밀번호 관리) ① 개별사용자는 각종 비밀번호를 다음 각 호에 해당하는 사항을 반영하고 숫자·문자·특수문자 등을 혼합하여 안전하게 설정하고 정기적으로 변경·사용하여야 한다.

1. 사용자 계정(아이디)과 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. 사용된 비밀번호는 재사용하지 말 것

6. 동일한 비밀번호를 여러 사람이 공유하여 사용하지 말 것

7. 응용프로그램 등을 이용한 자동 비밀번호 입력기능을 사용하지 말 것

② 전산담당자는 서버 등 정보시스템에 보관되는 비밀번호가 복호화 되지 아니하도록 일방향 암호화하여 저장하여야 한다.

제45조(휴대용 저장매체 보안) ① 휴대용 저장매체를 사용하여 업무자료를 보관하고자 할 경우 자료의 위·변조, 저장매체의 훼손·분실 등에 대비한 보안대책을 수립·시행하여야 한다.

② 휴대용 저장매체 관리시스템을 운용하고자 할 경우 국가정보원장이 안전성을 확인한 제품을 도입하여야 한다.

③ 정보보안담당관은 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 전산담당자는 휴대용 저장매체를 비밀용·일반용으로 구분·관리하고 수량 및 보관 상태를 정기적으로 점검하며 외부 반출·입을 통제하여야 한다.

⑤ 휴대용 저장매체를 폐기·불용 처리하고자 할 경우 저장자료가 복구 불가하도록 완전삭제 소프트웨어 등을 이용하여 삭제하여야 한다. 다만, 완전삭제가 불가할 경우 파쇄하여야 한다.

⑥ 전산담당자는 정보보안담당관 총괄 하에 개별사용자의 휴대용 저장매체 무단 반출, 미(未)등록 휴대용 저장매체 사용여부 등 보안관리 실태를 정기적으로 점검하여야 한다.

제46조(비인가 기기 통제) ① 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.

2. 제1호를 제외한 정보통신기기: 제1호에 따른 반입·사용만으로는 보편적 통신 곤란 등 특별한 사정이 있는 경우에 한하여 정보보안담당관의 승인을 받아 반입 후 개인 용도로만 사용

② 제1항 각 호에 따라 반입한 개인 소유의 정보통신기기를 소속된 기관의 내부망 및 기관 인터넷망(무선랜 형태를 포함한다)에 연결하여서는 아니 되며, 내부망 및 기관 인터넷망 정보시스템을 다른 정보통신망에 연결하는 수단으로 사용하여서는 아니 된다. 전산담당자는 이에 대하여 수시로 점검하여야 한다.

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

제4장 융합 보안

제1절 정보통신시설 및 기기 보호

제47조(정보통신시설 보호대책) ① 공사는 관리구역 중 전산실을 정보통신시설로 지정·관리하여야 한다.

② 제1항에 따라 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

제48조(정보통신시설 출입관리) ① 외부인이 정보통신시설을 방문할 경우 반드시 신원을 확인하고 입회를 통해 출입을 허용하여야 한다.

제49조(영상정보처리기기 보안) ① 업무상 목적으로 불특정 사람 또는 사물을 촬영한 영상을 유·무선 정보통신망으로 전송·저장·분석하는 CCTV·IP카메라·이동형 영상촬영장비·중계서버·관제서버·관리용 PC 등의 기기·장비(이하 “영상정보처리기기”이라 한다)를 설치·운용하고자 할 경우 운영자의 계정·비밀번호 설정 등 인증대책을 수립하고 특정 IP주소에서만 접속 허용 등 비(非)인가자 접근 통제대책을 수립·시행하여야 한다.

② 영상정보처리기기를 통합·운용하는 시설(이하 “영상관제상황실”이라 한다)을 운영하고자 할 경우 영상관제상황실을 제한구역 또는 통제구역으로 지정·관리하고 출입통제 장치를 운용하여야 한다.

③ 영상정보처리기기 관리자는 제1항부터 제3항까지와 관련한 보안대책의 적절성을 수시 점검·보완하여야 한다.

④ 그 밖에 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.

제50조(재난 방지대책) ① 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애 발생에 대비하여 정보시스템의 이중화, 백업관리 및 복구 등 종합적인 재난 방지대책을 수립·시행하여야 한다.

② 정보통신망의 장애 발생에 대비하여 정보시스템 백업시설을 확보하

고 정기적으로 백업을 실시하여야 한다.

③ 제3항에 따른 백업시설을 구축·운영하고자 할 경우 정보통신실·통합데이터센터와 물리적으로 일정거리 이상 떨어진 안전한 장소에 설치하여야 하며 전력공급원 이중화 등 정보시스템의 가용성을 최대화 할 수 있도록 하여야 한다.

제5장 사이버위협 탐지 및 대응

제1절 보안관제

제51조(초동 조치) ① 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. 피해시스템을 정보통신망으로부터 분리하거나 악성프로그램의 동작을 정지시키는 조치
3. 사고 조사를 위한 피해 시스템 및 로그 기록의 보전

제2절 사고 대응

제52조(사이버공격으로 인한 사고) ① 피해 발생시 사고 원인을 규명할 때까지 피해 시스템에 대한 증거를 보전하고, 임의로 관련 자료를 삭제하거나 포맷하여서는 아니 된다.

제53조(정보통신보안 규정 위반 및 자료유출 사고) ① 상급기관으로부터 별표 2에 따른 정보통신보안 규정 위반사항에 대한 사실을 통보받은 경우 즉시 필요한 조치를 취하고 위규자, 위규 내용 및 조치 결과를 상급기관의 장에게 통보하여야 한다.

② 정보보안담당관은 정보보안과 관련하여 다음 각 호에 해당한다고 판단되는 부서에 개선을 권고할 수 있다.

1. 사무실·보호구역 보안관리 허술
   가. 인가되지 않은 작업자의 내부 시스템 접근
   나. 통제구역 내 장비·시설 등 무단 사진촬영
2. 전산정보 보호대책 부실
   가. 업무망·인터넷망 혼용사용 및 업무시간 중 음란, 저속, 도박, 비방 등의 목적으로 인터넷을 사용한 경우
   나. 보안 USB 사용규정 위반
   다. 웹하드·P2P 등 인터넷 자료 공유 사이트를 활용하여 용역사업 관련 자료 수·발신
   라. 개발·유지보수 시 원격작업 사용
   마. 저장된 비공개 정보 비밀번호 미부여
   바. 사용자 계정관리 미흡 및 오남용(시스템 불법접근 시도 등)
   사. 외부용 PC를 업무망에 무단 연결 사용
   아. 보안관련 프로그램 강제 삭제
   자. 불법소프트웨어를 임의로 설치하여 사용
   차. 비인가 보조매체, 메신저, 상용메일 무단 사용
3. 그 밖의 위반 사항
   가. 보안관련 소프트웨어의 주기적 점검 위반
   나. 정보보안 교육 미이수
   다. 실태점검 등 보안점검을 통해 발견된 취약점 미 조치
   라. 보안 관련 지적 사항에 대하여 적절한 시정 조치를 취하지 않은 경우
   마. 정보보안 사고 인지 후 미보고
   바. 정보화사업 시 보안점검표에 따른 보안대책 미 수립

제6장 정보 협력

제54조(정보협조 요청) ① 상급기관의 사이버공격에 관한 정보 요청을 받

은 경우 관계 법규에 저촉되지 않는 범위 내에서 해당 자료를 제출하거나 필요한 지원을 할 수 있다. 다만,「형사소송법」,「군사법원법」또는「통신비밀보호법」에 따른 절차는 해당 법률이 정하는 바에 따른다.

제55조(기관간 정보공유 협력) 사이버공격의 예방 및 신속한 대응을 위하여 다음 각 호에 해당하는 정보(이하 "사이버위협정보"라 한다)를 기관간 상호 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

별 표

[별표 1]

보안적합성 검증 신청시 제출물(제31조제2항 관련)

1. 최초검증 신청시 제출물

제출물	정보보호시스템		작성 주체
	상용 제품	자체(용역) 개발	
[서식 제1호]에 따른 보안적합성 검증 신청서	○	○	신청기관
[서식 제3호]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	
[서식 제1호]에 따른 보안적합성 검증 신청서	○	○	신청기관
[서식 제3호]에 따른 정보통신제품 도입확인서(현황)	○	○	
보안기능 점검표	○	○	
운용점검사항	○	○	
변경내용 분석서	○	○	업체

[별표 2]

정보통신보안 규정 위반 사항

내 용	세부 내용
1. 적성국과의 통신	가. 적성국 인터넷망과의 메시지 또는 자료 송수신 나. 적성국의 국내외 인터넷 거점(경유지를 포함한다)과의 통신 다. 적성국의 국내외 인터넷 거점(경유지를 포함한다)에서 공직자 상용 메일 불법 접속 라. 적성국의 인터넷 사회관계망서비스(SNS) 사용계정과의 메시지 또는 자료 송수신
2. 정보통신망을 통한 군사상 기밀의 누설 또는 유출	가. 군사전략, 작전계획 및 진행사항의 누설 또는 유출 나. 군 편제·임무·시설 및 그 밖의 부대현황의 누설 또는 유출 다. 병력(군·경·예비군) 현황 및 이동 상황의 누설 또는 유출 라. 경찰 및 특수기관의 장비(작전·정보·수사용) 현황과 집행사항의 누설 또는 유출 마. 특수기관·군사시설의 위치 및 이동상황의 누설 또는 유출 바. 군사장비의 구성·성능 및 발명개량 연구사항의 누설 또는 유출 사. 군사장비(군수품 등) 생산 및 공급사항의 누설 또는 유출 아. 그 밖에 국가방위에 영향을 초래하는 사항의 누설 또는 유출
3. 정보통신망을 통한 외교상 기밀의 누설 또는 절취	가. 국가 외교방침, 기본계획 및 재외공관에 발하는 훈령의 누설 또는 유출 나. 공개할 수 없는 외교조약 또는 협약의 누설 또는 유출 다. 특수임무를 수행하는 해외주재원의 활동(계획·지시·보고) 및 신원정보와 관련된 사항의 누설 또는 유출 라. 그 밖에 국가외교에 영향을 초래하는 사항의 누설 또는 유출
4. 정보통신망을 통한 국가정보활동 관련 사항의 누설 또는 절취	가. 대공업무와 관련된 사항의 누설 또는 유출 나. 정보(첩보) 수집활동에 필요한 사항의 누설 또는 유출 다. 간첩 또는 대공용의자 발견과 수사활동의 누설 또는 유출 라. 정보 및 특수 수사기관의 기구 또는 임무기능 관련 사항의 누설 또는 유출 마. 국가원수 및 그 밖의 요인의 비공개행사의 누설 또는 유출 바. 불명선박의 발견 및 처리의 누설 또는 유출 사. 중요물자 수송활동의 누설 또는 유출 아. 테러·마약·밀수 및 국제범죄조직 관련 정보·수사활동의 누설 또는 유출 자. 적 또는 경쟁국에 유리한 과학기술 및 산업 관련 정보의 누설 또는 유출 차. 그 밖에 국가안보 및 공안유지에 불리한 영향을 초래하는 사항의 누설 또는 유출
5. 암호자재 관련 사항	가. 암호자재의 연구개발 및 제작에 필요한 사항 누설

	나. 암호전문을 허위로 조립하여 송신 다. 암호를 부정한 목적에 사용 라. 암호문과 암호화되지 아니한 평문의 혼용 및 이중사용 마. 암호문 작성시 동일 난수를 2회 이상 반복사용 바. 사용기간이 경과된 암호자재를 계속 사용 사. 암호문에 암호화되지 아니한 평문을 삽입하여 송신 아. 그 밖에 암호자재 보호체계를 손상시킬 우려가 있는 사항 누설
6. 전자정보	가. 주전산기(주요 서버 등)·대용량 전자기록(DB)의 손괴 나. 전자정보의 위조·변조·훼손
7. 정보통신망 및 정보통신 시스템 관련 사항	가. 정보통신망에 대한 불법침입, 해킹·악성코드의 유포 나. 중요 정보시스템 및 정보통신실 파괴 다. 중요 정보시스템 기능 장애 및 정지
8. 비인가 통신시설 및 통신 제원 사용에 필요한 사항	가. 비인가된 무선시설의 설치·운용 나. 비인가된 무선시설과 교신 다. 비인가된 호출부호 및 주파수 사용 라. 비인가된 전파형식 사용 마. 지정출력의 초과사용
9. 허가목적 외의 방법으로 사용하는 경우	가. 허가목적 업무와 관련이 없는 통신 나. 군 통신망에서 군사업무와 관련이 없는 통신 다. 그 밖에 사회질서를 해치는 통신

[별표 3]

클라우드 서비스 이용 '시스템 중요도' 등급 분류기준

등급	분류기준		영역분리
상	파급영향	- 해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 치명적 악영향을 미칠 수 있음	물리적
	분류기준	- 국가 중대 이익(안보, 국가안전, 국방, 통일, 외교 등), 수사·재판 등 민감정보를 포함하거나 행정 내부업무 등을 운영하는 시스템	
중	파급영향	- 해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 심각한 영향을 미칠 수 있음	물리적
	분류기준	- 비공개 업무자료를 포함 또는 운영하는 시스템	
하	파급영향	- 해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 제한적인 영향을 미칠 수 있음	물리적 또는 논리적
	분류기준	- 개인정보를 포함하지 않고 공개된 공공데이터를 포함 또는 운영하는 시스템	

[표] 시스템 중요도 등급 분류기준 및 영역분리

※ 행정 내부업무의 경우 '시스템 중요도'를 고려하여 등급 조정 가능

※ 위 분류기준에 따른 분류 절차 및 체크리스트 등 세부사항은 '국가 클라우드서비스 보안가이드라인'을 참고한다.

※ 이용기관은 민간 클라우드서비스 도입시 시스템 등급을 자체 분류하고, 국정원은 '보안성 검토'시 분류의 적정성을 재검토한다.

서 식

[별지 제1호서식]

정보시스템 관리대장

연번	소속	취급자 성명	종류 (서버·PC 등)	제조사	모델명	관리번호	도입일자	비고