상지대학교 정보보안 기본지침

2024. 02.

전 산 정 보 팀

목 차

상지대학교 정보보안 기본지침

제정 2024. 02. 27

제1장 총 칙

제1조(목적) 이 지침은 [교육부 정보보안 기본지침]에 따라 상지대학교와 그 소속 기관, 산하기관 및 단체(이하 “본교”라 한다)에서 수행하여야 할 정보보안과 관련한 기본업무를 규정함을 목적으로 한다.

제2조(정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. “정보보안”이라 함은 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」 제4조 제1항 제4호에 따른 사이버 공격 및 위협에 대한 예방 및 대응
   나. 「전자정부법」 제56조에 따른 정보통신망과 행정정보 등의 보안
   다. 「정보통신기반 보호법 시행령」 제5조 제4항 제1호 각 목에 해당하는 주요 정보통신기반시설의 보호
   라. 「공공기록물 관리에 관한 법률 시행령」 제5조에 따른 전자기록물의 보안
   마. 「국가 사이버 안전관리 규정」 제2조 제3호에 따른 사이버안전
2. “각급기관”이라 함은 교육부 및 그 소속기관, 시도교육청 및 그 소속 기관, 교육부 장관의 지도 감독을 받는 공공기관 및 각급학교를 말한다.

2의2. “위탁시스템”이라 함은 각급기관 외의 기관에서 교육부로부터 위탁받아 운영하는 정보시스템을 말한다.

3. “각급학교”라 함은 「유아교육법」, 「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 각급의 학교 중 교육부 장관의 지도 감독을 받는 학교를 말한다.

3의2. “교육 현장”이라 함은 「유아교육법」, 「초·중등교육법」, 「고등교육법」에 따른 각급학교의 교육 활동에 사용되는 정보통신환경을 말한다.

4. “상급 기관”이라 함은 교육부를 말한다.
5. “하급 기관”이라 함은 상급 기관과 상지대학교를 제외한 모든 소속기관·산하기

관·단체 등을 말한다.

6. “정보보안담당관”이라 함은 본교의 정보보안 업무를 총괄하기 위하여 총장으로부터 위임받은 사람을 말한다.
7. “정보통신망”이라 함은 「사이버안보 업무규정」 제2조 제1호에 따른 정보통신망을 말한다.
8. “내부망”이라 함은 본교의 업무수행을 위하여 인터넷과 별도로 분리하여 구축한 업무 전용(專用) 정보통신망을 말한다.
9. “기관 인터넷망”이라 함은 본교 구성원 등의 업무 및 교육 활용 또는 공개 서버 운용을 주(主)목적으로 인터넷과 연동하여 구축한 정보통신망을 말한다.
10. “상용 인터넷망”이라 함은 본교의 기관 인터넷망과 별개로 구성원이나 민원인 등의 보편적인 편의성을 위하여 인터넷에 연동하여 구축한 정보통신망을 말한다.
11. “정보시스템”이라 함은 「전자정부법」 제2조 제13호에 따른 정보시스템을 말한다.
12. “휴대용 저장매체”라 함은 CD・외장형 하드디스크・USB 메모리 등 정보를 저장할 수 있는 것으로 PC・서버 등의 정보시스템과 분리할 수 있는 기억장치를 말한다.
13. “업무자료”라 함은 다음 각 목의 어느 하나에 해당하는 것을 말한다.
    가. 「전자정부법」 제2조 제6호에 따른 행정정보 및 같은 법 제2조 제7호에 따른 전자문서
    나. 「공공기록물 관리에 관한 법률 시행령」 제2조 제2호에 따른 전자기록물
    다. 기타 다른 법령에 의하여 구성원 등이 직무상 작성・취득하였거나 보유・관리하는 자료로서 전자적으로 처리되어 부호・문자・음성・음향・영상 등으로 표현된 것
14. “비밀”이라 함은 업무자료 중에서 국가「보안업무규정」 제4조에 따라 분류된 비밀을 말한다.
15. “대외비”라 함은 업무자료 중에서 국가「보안업무규정 시행규칙」 제16조 제3항에 따라 분류된 대외비를 말한다.
16. “비공개 업무자료”라 함은 비밀 및 대외비를 제외한 업무자료 중에서 다음 각 목의 어느 하나에 해당하는 자료 또는 정보를 말한다.
    가. 「공공기관의 정보공개에 관한 법률」 제9조 제1항에 따른 비공개 대상 정보

나. 국회 소속 공무원(「국회의원수당 등에 관한 법률」 제9조에 따른 보좌직원을 포함한다) 또는 「지방자치법」 제30조에 따른 지방의회 소속 공무원의 직무상 요구에 따라 작성 또는 취득한 자료

다. 가목에 따른 비공개 대상 정보의 주요 내용이 기술된 문장 또는 문구

17. “공개 업무자료”라 함은 업무자료 중에서 비밀 및 대외비와 비공개 업무자료를 제외한 모든 자료 또는 정보(「공공데이터의 제공 및 이용 활성화에 관한 법률」 제19조에 따라 공표된 공공데이터를 포함한다)를 말한다.

18. “정보통신실”이라 함은 서버・스위치・라우터・교환기 등 전산 및 통신장비 등이 설치・운용되는 장소 또는 전산실・통신실・데이터센터 등을 말한다.

19. “정보보호 시스템”이라 함은 「지능 정보화 기본법」 제2조 제15호에 따른 정보보호 시스템을 말한다.

20. “국가용 보안요구사항”이라 함은 「사이버안보 업무규정」 제9조 제2항에 따른 정보보호 시스템 등의 도입・운영에 관한 보안 대책의 일환으로 국가정보원장이 정하는 보안 관련 필수사항을 말한다.

21. “국가용 보호 프로파일(Protect Profile)”라 함은 「지능 정보화 기본법」 제58조 제1항 및 같은 법 시행령 제51조에 따라 과학기술정보통신부 장관이 고시한 「정보보호 시스템 평가・인증 지침」에 따른 보호 프로파일 중에서 국가정보원장이 국가용 보안요구사항을 만족한다고 인정한 것을 말한다.

22. “안전성 검증필 제품”이라 함은 국가정보원장이 국가용 보안요구사항 만족 여부 등 안전성을 확인하여 제21조에 따른 안전성 검증필 제품 목록에 등재한 정보통신제품을 말한다.

23. “보안적합성 검증”이라 함은 제20조 제1항 제3호의 보안 기능이 있는 정보통신제품에 대하여 실제 적용・운용 이전에 시험 등의 방법으로 안전성을 검증하는 활동을 말한다.

24. “개별 사용자”라 함은 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 구성원 등과 본교와의 계약에 의하여 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 사람을 말한다.

25. “전자파 보안”이라 함은 정보통신 시설 및 기기 등을 대상으로 전자파에 의한 정보 유출을 방지하고 파괴・오작동 유발 등의 위협으로부터 정보를 보호하는 일체의 행위를 말한다.

26. “대도청 측정(TSCM)”이라 함은 유・무선 도청탐지 장비 등을 사용하여 은닉

된 도청 장치를 색출하거나 누설 전자파(정보통신기기로부터 자유공간 또는 전도성 경로를 통해 비(非)의도적으로 누출되는 정보를 포함한 전자파) 등 각종 도청 위해(危害) 요소를 제거하는 제반 활동을 말한다.

27. “정보보안 수준 진단”이라 함은「사이버안보 업무규정」제12조 및「전자정부법」제56조 등에 따라 정보보안 정책에 대한 이행 여부를 확인하기 위하여 실시하는 평가를 말한다.

28. “암호자재”라 함은 비밀의 보호 및 정보통신 보안을 위하여 암호 기술이 적용된 장치나 수단으로서 Ⅰ급, Ⅱ급, Ⅲ급 비밀 소통용 암호자재로 구분되는 장치나 수단을 말한다.

29. “암호장비”라 함은 암호자재 중에서 국가정보원장이 승인하여 개발・제작・보급되는 암호자재를 말한다.

30. “암호알고리즘”이라 함은 정보의 유출, 위・변조, 훼손 등을 방지하기 위하여 기밀성・무결성・인증・부인방지 등의 기능을 제공하는 수학적 논리를 말한다.

31. “암호가 주기능인 제품”이라 함은 검증필 암호모듈을 사용해 정보의 암・복호화를 주된 목적・기능으로 하는 제품을 말한다.

32. “상용 암호모듈”이라 함은 암호알고리즘을 소프트웨어, 하드웨어, 펌웨어 또는 이를 조합한 형태로 구현한 것으로서 비밀이 아닌 업무자료를 보호하기 위하여 민간이 상용(商用)으로 판매하는 것을 말한다.

33. “검증필 암호모듈”이라 함은「사이버안보 업무규정」제9조 제2항 및 제3항,「전자정부법 시행령」제69조와「암호모듈 시험 및 검증 지침」(국가정보원 지침)에 따라 국가정보원장이 안전성을 확인하여 제22조에 따른 목록에 등재한 상용 암호모듈을 말한다.

34. “사이버 공격”이라 함은「사이버안보 업무규정」제2조 제2호에 따른 행위를 말한다.

35. “보안관제”라 함은 사이버 공격을 실시간으로 즉시 탐지 및 분석, 대응하는 일련의 활동을 말한다.

36. “보안관제센터”라 함은 일정한 수준의 시설 및 장비와 이를 운영하기 위한 전문 또는 전담 인력을 갖추고 보안관제 업무를 수행하는 조직을 말한다.

37. “교육부 보안관제 체계”라 함은 「교육부 사이버안전센터 운영 규정」 제5조 제1항에 따라 교육부 장관이 각급기관의 보안관제를 시행하거나, 사이버 공격 탐지・대응조치 이행 여부 확인을 위하여 구축・운영하는 실시간 탐지・대응 체계를

말한다.

38. “부문 보안관제센터”라 함은 교육부 장관이 각급기관의 정보통신망을 대상으로 운영하는 보안관제센터를 말한다.

39. “단위 보안관제센터”라 함은 총장이 해당 기관 및 소속기관의 정보통신망을 대상으로 운영하는 보안관제센터를 말한다.

40. “취약점”이라 함은 사이버 공격에 악용되어 관리자가 설정한 접근 권한外 정보를 열람·취득하게 하거나 보안 기능을 회피할 수 있게 하는 정보통신망·정보시스템의 결함을 말한다.

41. “클라우드 컴퓨팅(Cloud Computing)”이란 직접·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원을 이용자의 요구나 수요변화에 따른 정보통신망을 통하여 신축적으로 이용할 수 있도록 하는 정보처리체계를 말한다.

42. “공공클라우드센터”란 정보시스템을 통합 관리하기 위해 각급기관 등의 장이 설치·운영 중인 데이터센터를 말한다.

제3조(적용 범위) 이 지침은 본교의 정보보안 업무에 적용한다.

제4조(책무) ① 총장은 본교와 관련된 정보(업무자료를 포함한다. 이하 같다)와 정보통신망을 보호하기 위하여 보안 대책을 수립·시행하여야 하며 정보보안에 대한 책임을 진다.

② 총장은 소속 구성원 등에 대한 근무 성적 또는 성과 평가를 시행하는 경우 정보보안 내규 준수 여부 등을 반영할 수 있다.

제5조(정보보안담당관 운영) ① 총장은 정보보안 업무를 효율적이고 체계적으로 수행하기 위하여 정보보안 전문지식을 보유한 적정인력을 확보하여 정보보안 전담조직을 구성·운영하여야 한다.

② 총장은 학술정보원장을 정보보안담당관으로 임명하여야 한다. 단 별도로 임명하지 않는 경우 당연직으로 임명한 것으로 하며, 정보보안담당관의 업무는 다음 각호에 해당한다.

1. 정보보안 정책·계획의 수립·시행 및 정보보안 관련 규정·지침 등 제·개정
2. 정보보안 전담 조직 관리, 전문 인력 및 관련 예산 확보
3. 정보화 사업 보안성 검토 및 보안적합성 검증 총괄
4. 정보통신실, 정보통신망 현황자료 등에 관한 보안관리 총괄
5. 소관 주요 정보 통신 기반 시설 보호
6. 사이버 공격 대응훈련 및 정보보안 수준 진단 총괄

7. 보안관제, 사고 대응 및 정보 협력 업무 총괄
8. 정보보안 교육 총괄 및 ‘사이버 보안 진단의 날’ 정보보안 부문 계획수립・시행
9. 자체 정보보안 감사
10. 하급 기관의 정보보안 업무 감독
11. 분임정보보안담당관 업무 감독
12. 그 밖에 정보보안과 관련한 사항

③ 총장은 정보보안담당관이 직무를 원활히 수행할 수 있도록 조직, 인력 및 예산을 지원하여야 한다.

④ 총장은 정보보안담당관이 직무를 효율적으로 수행할 수 있도록 분임정보보안담당관을 임명하여야 하며, 별도로 임명하지 않는 경우 각 소속 부서· 산하기관 및 단체의 장을 분임정보보안담당관으로 임명한 것으로 본다.

⑤ 정보보안담당관은 제2항 각호에 해당하는 업무를 수행함에 있어 필요한 경우 해당 업무의 일부를 분임정보보안담당관에게 위임할 수 있다.

⑥ 분임정보보안담당관은 부서 내 정보보안 업무를 책임지며 다음 각호의 사항을 관리·감독하여야 한다.

1. 부서·단체의 소관 정보보안에 관한 사항
2. 부서·단체의 소관 정보화 사업에 관한 사항
3. ‘사이버 보안 진단의 날’ 이행 및 지도·관리에 관한 사항
4. 부서·단체의 단말기 및 휴대용 저장매체 등 정보자산 사용 관리에 관한 사항
5. 부서·단체의 정보시스템 및 정보자산에 대한 접근통제 및 기록에 관한 사항
6. 부서·단체의 정보보안(업무자료 포함) 자료 유·노출 점검에 관한 사항
7. 그 밖에 부서·단체의 정보보안에 관한 사항

제6조(연도 추진계획 수립) ① 정보보안담당관은 매년「연도 정보보안 업무 추진계획」(「국가 사이버 안전관리 규정」 제9조에 따른 사이버안전 대책을 포함한다. 이하 같다)을 수립・시행하여야 한다.

제7조(정보보안 내규) ① 총장은 본교의 정보보안 업무를 규정한 정보보안 내규(또는 지침・시행세칙 등)를 「교육부 정보보안 기본지침」에 저촉되지 않는 범위에서 수립・시행하여야 한다. 다만, 「교육부 정보보안 기본지침」을 적용하는 경우 별도로 수립하지 않을 수 있다.

제8조(정보보안 감사 등) ① 총장은 정보보안 업무 및 활동을 조사・점검하기 위하여 연 1회 이상 자체 정보보안 감사를 시행하여야 하며, 필요한 경우 정보보안담

당관을 감사 또는 감찰업무를 수행하는 부서에 배속하여 정보보안 감사를 수행하도록 할 수 있다.

② 제1항에 따른 정보보안 감사를 시행하는 경우 교육부 장관 및 국가정보 원장이 배포하는 다음 각호의 가이드라인을 활용할 수 있다.

1. 사이버 보안 강화를 위한 길라잡이(정보통신시스템 보안 진단 및 대응 방법)
2. 홈페이지·네트워크·시스템·DBMS 취약점 점검 매뉴얼
3. 정보보안 점검 체크리스트

③ 총장은 필요한 경우 하급 기관의 정보보안 점검 방문을 시행할 수 있다.

제9조(정보보안 교육) ① 정보보안담당관은 정보보안에 대한 경각심을 제고하기 위하여 정보보안 교육계획을 수립하여 연 1회 이상 모든 구성원을 대상으로 교육(온라인 교육을 포함한다.)을 시행하여야 하며, 필요시 수시교육을 시행할 수 있다.

② 제1항에 따라 모든 구성원은 특별한 사유가 없는 한 연 1회 이상 정보보안 교육을 이수하여야 한다. 단, 정보보안담당자와 정보보안실무자는 연간 15시간 이상 정보보안 교육(개인정보보호법 제28조 제2항의 교육 등 포함)을 이수하여야 한다.

③ 정보보안담당관은 제1항에 따라 정보보안 교육을 시행하는 경우 해당 기관의 실정에 맞는 교육 자료를 작성 활용하여야 하며 필요한 경우 외부 강사 지원, 외부 전문가 조청 등 협조를 요청할 수 있다.

④ 총장은 정보보안담당관, 분임정보보안담당관 및 정보보안 담당 직원, 시스템 관리자의 업무 전문성을 제고하고 정보보안 지식을 함양하기 위하여 전문기관의 교육 이수나 학술회의 참가 등을 장려하여야 한다.

제10조(사이버보안진단의 날) ① 총장은 해당 기관의 실정에 맞게 매월 세 번째 수요일을 '사이버 보안 진단의 날'로 지정·시행하여야 한다. 다만, 부득이한 사유로 해당일에 시행하지 못하는 경우 같은 달 다른 날에 시행하여야 한다.

② 분임정보보안담당관은 정보보안담당관 총괄하에 '사이버 보안 진단의 날'에 소속 부서의 정보통신망과 정보시스템의 보안 취약 여부 확인 등 보안 진단을 시행하여야 한다.

③ 총장은 매월 사이버 보안 진단의 날에 시행한 정보시스템 점검 결과를 문서 또는 전자적 시스템을 통하여 기록 관리하여야 하며, 시행 결과 발견된 문제 또는 미비점에 대하여 대책을 수립하고 개선하여야 한다.

제2장 정보화 사업 보안

제1절 사업 계획

제11조(보안책임) ① 정보화 사업을 추진하는 부서의 장(이하 “정보화 사업담당관”이라 한다.)은 정보화 사업에 대한 보안관리 책임을 지고 관리·감독하여야 한다.

② 정보통신망 또는 정보시스템을 개발·구축·운용·유지보수하는 사업(「지능 정보화 기본법」 제11조 제1항에 따른 지능 정보화 계획에 따른 사업을 포함한다. 이하 “정보화 사업”이라 한다)을 담당하는 정보화 사업담당관은 해당 정보화 사업에 대한 보안관리를 수행하여야 한다.

③ 정보보안담당관은 각종 정보화 사업과 관련한 보안 대책의 적절성을 평가하고 정보화 사업 수행 전반에 대하여 보안 대책의 이행 여부를 점검하여 필요한 경우 정보화 사업을 추진하는 부서의 장에게 시정을 요구할 수 있다.

제12조(보안 대책 수립) 정보통신망 또는 정보시스템을 구축·운용하기 위한 정보화 사업 계획을 수립하는 경우 다음 각호의 사항을 포함한 보안 대책을 수립·시행하여야 한다.

1. 보안 관리체계(조직, 인원 등) 구축 등 관리적 보안 대책
2. 설치·운용 장소 보안관리 등 물리적 보안 대책
3. 정보통신망 또는 정보시스템의 구성 요소별 기술적 보안 대책
4. 국가정보원장이 개발하거나 안전성을 확인한 암호자재, 검증필 암호모듈 및 정보보호 시스템 도입·운용계획
5. 긴급사태 대비 및 재난복구 계획
6. 용역업체 작업 장소에 대한 보안 대책
7. 온라인 개발 또는 온라인 유지보수가 필요하다고 판단할 경우, 제26조 또는 제45조에 따른 보안 대책
8. 누출금지 정보 보안관리 방안

제13조(제안요청서 기재 사항) ① 용역업체에 정보화 사업을 발주하기 위하여 제안요청서를 작성하는 경우 다음 각호의 사항을 포함하여야 한다.

1. 용역업체 작업 장소에 대한 보안요구사항
2. 온라인 개발 또는 온라인 유지보수가 필요하다고 판단할 경우, 제26조 또는 제45조에 따른 보안 준수사항
3. 누출금지 정보 목록
4. 용역업체가 누출금지 정보를 제외한 소프트웨어 산출물을 제3자에게 제공하고자 하는 경우 발주자의 승인 절차

② 제1항 제3호에 따른 누출금지 정보 목록을 작성하는 경우 다음 각호의 사항을 포함하여야 한다.

1. 해당 기관의 정보시스템 내·외부 IP주소 현황
2. 정보시스템 구성 현황 및 정보통신망 구성도
3. 개별 사용자의 계정·비밀번호 등 정보시스템 접근권한 정보
4. 정보통신망 또는 정보시스템 취약점 분석·평가 결과물
5. 정보화 사업 용역 결과물 및 관련 프로그램 소스 코드(외부에 유출될 때 국가안보 및 국익에 피해가 우려되는 중요 용역사업에 해당)
6. 암호자재, 암호가 주 기능인 제품 및 정보보호 시스템 도입·운용 현황
7. 정보보호 시스템 및 네트워크 장비 설정 정보
8. 「공공기관의 정보공개에 관한 법률」 제9조 제1항에 따라 비공개 대상 정보로 분류된 해당 기관의 내부 문서
9. 「개인정보 보호법」 제2조 제1호에 따른 개인 정보
10. 「보안업무규정」 제4조에 따른 비밀 및 「보안업무규정 시행규칙」 제16조 제3항에 따른 대외비
11. 그 밖에 해당 기관의 장이 공개가 불가하다고 판단한 자료

제2절 보안성 검토

제14조(검토 시기 및 절차) ① 총장은 정보화 사업을 수행하고자 할 때 정보화 사업과 관련한 보안 대책의 적절성을 평가하기 위하여 사업 계획단계(사업 공고 전)에서 자체 보안성 검토 절차(「고등교육법」 제2조 각호의 학교 중 사립학교에 해당)를 수행하여야 한다.

② 분임정보보안담당관은 제15조 제1항부터 제3항의 각호에 따른 정보화 사업을 추진하는 경우 정보보안담당관에게 보안성 검토를 의뢰하거나 자체적으로 실시하여야 한다.

③ 보안성 검토는 서면 검토를 원칙으로 하며 정보보안담당관이 필요하다고 판단하는 경우 현장 확인을 병행하여 시행할 수 있다.

제15조(검토 기관) ① 총장은 다음 각호의 정보화 사업을 추진하는 경우 자체 보안성 검토를 시행하여야 한다. 단 필요시 상급 기관을 경유하여 국가정보원장에게 보안성 검토를 의뢰할 수 있다.

1. 비밀·대외비를 유통·관리하기 위한 정보통신망 또는 정보시스템 구축

2. 국가정보원장이 개발하거나 안전성을 확인한 암호자재를 적용하는 정보통신망 또는 정보시스템 구축
3. 외교·국방 등 국가안보상 중요한 정보통신망 또는 정보시스템 구축
4. 100만명 이상의 개인에 대한「개인정보 보호법」상 민감정보 또는 고유 식별정보를 처리하는 정보시스템 구축
5. 주요 정보통신기반시설로 지정이 필요한 정보통신기반시설 구축
6. 내부망 또는 폐쇄망을 인터넷 또는 다른 정보통신망과 연동하는 사업
7. 내부망과 인터넷망을 분리하는 사업
8. 통합데이터센터·보안관제센터 구축
9. 구성원들이 업무상 목적으로 활용하도록 하기 위한 인터넷망(업무용 무선랜 형태를 포함한다)의 구축
10. 원격근무시스템 구축
11.「전자정부법」제54조의2 및「클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률」제20조에 따라 클라우드 컴퓨팅 서비스제공자의 클라우드 컴퓨팅 서비스(이하 “민간 클라우드 컴퓨팅 서비스”라 한다)를 이용하는 사업
12. 첨단 정보통신기술을 활용하는 정보화 사업으로서 국가정보원장이 해당 기술에 대하여 안정성 확인이 필요하다고 지정하는 사업

② 총장은 다음 각호에 해당하는 정보화 사업에 대하여 자체 보안성 검토를 시행한다.

1. 국가정보원장으로부터 보안성 검토를 위임받은 사업
2. 홈페이지 및 웹메일 등 웹 기반 정보시스템 구축
3. 인터넷전화 시스템구축
4. 다른 기관의 정보통신망 또는 정보시스템과 연동하여 정보의 소통 또는 서비스를 제공하는 정보시스템 구축
5. 내부망에 구축하는 구성원 등의 인사·복지시스템
6. 주요 정보통신기반시설 취약점 분석·평가, 정보보안 컨설팅 등 용역사업
7. 기존 분리된 내부망·기관 인터넷망 간 자료전송시스템 구축 등 후속 사업
8. 대규모 백업·재해복구센터 구축

③ 분임보안담당관은 다음 각호에 해당하는 정보화 사업에 대하여 자체 보안성 검토를 시행한다.

1. 제40조 제1항에 따른 영상회의시스템을 내부망 또는 기관 인터넷망과 분리하여

구축하는 경우

2. 제70조에 따른 영상정보처리기기를 같은 조 제3항에 따라 인터넷과 분리하여 구축하는 경우
3. 백업시스템 구축
4. 대민(對民) 콜 센터시스템 구축
5. 제15조 제1항 각호의 정보화 사업에 해당하지 않으며 예산이 5억원 미만인 정보화 사업
6. 제15조 제1항 각호의 정보화 사업에 해당하지 않으며 개인 정보가 5만건 미만인 정보화 사업
7. 상급 기관으로부터 보안성 검토를 위임받은 사업
8. 기타 총장이 필요하다고 판단하는 정보통신망 또는 정보시스템 구축

제16조(검토 생략) ① 다음 각호에 해당하는 정보화 사업에 대하여 보안성 검토 절차의 이행을 생략할 수 있다. 이 경우 총장은 관련 매뉴얼·가이드라인 등을 준수하는 등 자체 보안 대책을 수립·시행하여야 한다.

1. 제15조 각항 각호의 정보화 사업에 해당하지 않는 단순 장비·물품 도입
2. 제15조에 따른 보안성 검토를 거쳐 완료한 정보화 사업에 대하여 정보통신망 구성을 변경하지 않는 범위 내에서 다음 각 목의 사항을 포함한 후속 운영·유지보수·컨설팅(단일 회선의 이중화는 본 호를 적용함에 있어 정보통신망 구성의 변경이 아닌 것으로 본다)
   가. 서버·스토리지·네트워크 장비 등 장비 노후화로 인한 단순 장비 교체
   나. 전화기·무전기·CCTV 등 통신·영상기기의 노후화로 인한 단순 장비 교체
   다. 기존 운용하던 정보보호 시스템을 동일한 보안 기능을 보유한 다른 정보보호 시스템으로 교체
3. 다년도에 걸쳐 계속되는 사업으로써 사업 착수 당시 보안성 검토를 완료한 후 사업 내용의 변동 없이 계속 추진하는 운영·유지 사업
4. PC·프린터 및 상용 소프트웨어 등 단순 제품 교체
5. 교육 현장에서 구축하는 무선랜, 클라우드 및 이동통신망 사업

② 총장은 제1항 제2호부터 제5호까지에 해당하는 정보화 사업을 수행하는 경우 기존 보안성 검토 결과를 준수하여야 한다.

제17조(제출 문서) 분임정보보안담당관은 제14조 제2항에 따라 보안성 검토를 의뢰

하는 경우 다음 각호의 사항이 포함된 문서를 제출하여야 한다.

1. 사업계획서(정보화 사업개요·사업목적 및 추진계획 포함)
2. 제안요청서
3. 정보통신망 구성도(필요시 IP주소 체계를 추가)
4. 자체 보안 대책(관리적, 물리적, 기술적 보안 대책을 포함)

제18조(검토 결과 조치) ① 분임정보보안담당관은 보안성 검토 결과를 통보받는 경우 검토 결과를 반영하여 보안 대책을 보완하여야 한다.

② 정보보안담당관은 제1항에 따른 보안성 검토 결과 반영 여부를 확인하기 위하여 각 부서 또는 단체에 현장 점검을 시행할 수 있다.

제19조(현황 제출) 총장은 상급 기관의 요청이 있는 경우 본교의 정보화 사업에 대한 보안성 검토 결과 현황을 제출할 수 있다.

제3절 제품 도입

제20조(정보통신제품 도입) ① 총장은 정보 및 정보통신망 등을 보호하기 위하여 보안 기능이 있는 다음 각호에 해당하는 정보통신제품을 도입할 수 있다.

1. 안전성 검증필 제품 목록에 등재된 제품
2. 비밀이 아닌 업무자료의 암·복호화를 목적으로 한 경우 [별표 2]의 암호가 주기능인 제품 도입 요건을 만족하는 제품
3. 제1호 및 제2호에 해당하지 않는 정보통신제품 중에서 국가정보원장이 별도로 공지하는 도입 요건을 만족하는 제품
4. 제품 유형의 특성상 보안 기능의 비중이 미미하여, 총장이 자유롭게 도입·운용이 가능한 '단순 보안 기능 제품 유형'으로 국가정보원장이 공지한 제품
5. 취약 정보통신제품을 긴급 대체하기 위하여 도입하는 제품

② 제1항 제3호에 해당하는 제품은 실제 적용·운용 이전에 보안적합성 검증을 받아야 한다.

제21조(영상정보처리기기 도입) 총장은 제72조 제1항에 따른 영상정보처리기기를 도입하고자 하는 경우 한국정보통신기술협회(TTA)의 공공기관용 보안 성능품질 인증 등 일정한 보안성능이 확인된 제품을 도입하여야 한다.

제4절 계약 및 사업수행

제22조(계약 특수조건) ① 총장은 정보통신망 또는 정보시스템 구축 및 유지보수 등의 계약 이행 과정에서 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 보안 취약점 등에 대해서는 계약업체의 책임으로 개선 조치하도록 하여야 한다.

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

제23조(용역업체 보안) ① 총장은 용역업체에 정보화 사업을 발주하는 경우 다음 각호의 보안 사항을 준수하도록 계약서에 명시하여야 한다.

1. 제13조 제1항 각호에 따른 제안요청서에 포함된 사항
1의2. 원격지개발, 원격지에서의 온라인 개발, 온라인 유지보수를 허용하는 경우 보안 준수사항
2. 소프트웨어 개발 보안에 필요한 사항
3. 사업 참여 인원의 보안 관련 준수사항과 위반하는 경우 손해배상 책임에 관한 사항
4. 사업 수행과 관련한 보안 교육, 보안 점검 및 사업 기간 중 참여 인원 임의 교체 금지
5. 정보통신망 구성도・IP주소 현황 등 업체에 제공하는 자료는 자료 인계인수대장을 비치하여 보안 조치 후 인계・인수하고 무단 복사 및 외부 반출 금지
6. 업체의 노트북・휴대용 저장매체 등 관련 장비는 반출・입시마다 악성코드 감염 여부, 누출금지 정보 무단 반출 여부 등 점검
7. 사업 종료 시 업체의 노트북・휴대용 저장매체 등 관련 장비는 저장자료 복구가 불가하도록 완전 삭제
8. 사업 종료 시 누출금지 정보 전량 회수
9. 그 밖에 정보보안담당관이 보안관리가 필요하다고 판단하는 사항 또는 상급 기관이 보안 조치를 권고하는 사항

② 총장은 비밀, 중요 용역사업 중 용역업체 참여 인원이 다음 각호에 해당하는 사실을 알게 된 경우 교체를 요구하여야 한다.

1. 「국가공무원법」 제33조 제3호부터 제6의 4호까지에 해당하는 사람
2. 「국가를 당사자로 하는 계약에 관한 법률」 제27조 제1항 각호의 행위를 한 사람

③ 총장은 다음 각호에 따른 보안 준수사항의 이행 여부를 정기 또는 수시로 점검(불시 점검을 포함한다)하고 미비점을 발견하는 경우 용역업체에 시정 조치하도록 하여야 한다. 이 경우 정보화 사업담당관이 점검한 후 그 결과를 정보보안담당관에게 통보하여야 한다.

1. 제1항에 따라 계약서에 명시된 보안 준수사항
2. 발주기관 내 작업 장소 보안 준수사항
3. 원격지개발 보안 및 원격지에서의 온라인 개발 시 보안 준수사항
4. 제44조에 따른 정보시스템 유지보수 및 제49조에 따른 온라인 유지보수 시 보안 준수사항

④ 정보보안담당관은 본교의 정보화 사업에 대하여 용역업체 보안관리 실태점검을 시행할 수 있으며, 필요한 경우 상급 기관에 지원을 요청할 수 있다.

⑤ 총장은 제3항 및 제4항에 따른 점검 결과 용역업체 보안 대책 준수가 미흡하고 시정조치가 어렵다고 판단되는 경우 원격지개발, 원격지에서의 온라인 개발 또는 온라인 유지보수 허가를 취소할 수 있다.

⑥ 총장은 원격지에서의 온라인 개발, 온라인 유지보수를 허용하고자 하는 경우 용역업체의 온라인 접속을 통제하기 위한 온라인 용역 통제시스템을 구축・운영하여야 한다.

⑦ 그 밖에 용역업체 보안과 관련한 사항은 국가정보원장이 배포한「국가・공공기관 용역업체 보안관리 가이드라인」을 준수하여야 한다.

제24조(소프트웨어 개발보안) 총장은 정보시스템을 개발하는 경우「전자정부법」에 따라 규정된「행정기관 및 공공기관 정보시스템 구축・운영 지침」(행정안전부 고시)에 따라 보안 취약점이 발생하지 않도록 개발(이하 “소프트웨어 개발 보안”이라 한다) 하고 보안 취약점을 진단하여야 한다.

제25조(발주기관내 작업장소 보안) ① 본교에(필요에 따라 임차한 외부 사무실을 포함한다) 용역업체 작업 장소를 설치하는 경우 보안 통제가 가능한 공간을 마련, 운영하여야 한다.

② 본교의 용역업체 작업 장소에 설치 운영하는 정보통신망은 발주기관의 정보통신망과 분리 구성하여야 한다. 다만, 용역업체가 사업 수행을 위하여 발주기관 정

보시스템 이용이 불가피한 경우에는 필요한 정보시스템에 한하여 지정된 단말기로부터의 제한적 접근을 허용하는 등 보안 대책을 수립·시행하여야 하며, 이 경우 내부망 정보시스템에 대한 접근허용에 대해서는 상급 기관 또는 정보보안담당관과 사전 협의하여야 한다.

③ 작업 장소 내 정보시스템은 용역사업 수행을 위해 필요한 경우 해당 정보화 사업담당관의 보안 통제하에, 인터넷에 연결할 수 있다. 다만, 제2항 단서에 따른 발주기관 정보시스템 접근용 단말기의 경우에는 인터넷 연결을 금지한다.

④ 용역업체가 발주기관 내 작업 장소에서 개발 작업을 수행하더라도 개발용 서버가 민간 클라우드 컴퓨팅 서비스를 이용하는 등으로 원격지에 위치하는 경우 원격지개발로 간주하고 이에 따른 보안 대책을 수립·시행하여야 한다.

제26조(원격지 개발보안) ① 총장은 용역업체가 발주기관 이외의 장소(이하 “원격지”라 한다)에서 개발 작업(유지보수는 제외한다)을 수행하고자 요청하는 경우 제13조 제1항 제1호에 따른 용역업체 작업 장소에 대한 보안요구사항 등을 포함한 관리적·기술적 보안 대책을 수립·시행하여야 한다. 이 경우 정보화 사업담당관은 보안 대책을 수립한 후 정보보안담당관의 승인을 받아야 한다.

② 원격지 내 정보시스템은 개발 작업을 위하여 필요한 경우 해당 정보화 사업담당관의 보안 통제하에, 인터넷에 연결할 수 있다.

제27조(원격지에서의 온라인 개발) 정보보안담당관은 원격지개발이 필요하다고 판단되고 용역업체가 다음 각호에 따른 보안 대책에 서면으로 동의하는 경우, 용역업체가 원격지에서 인터넷을 통해 발주기관 정보시스템에 온라인 접속한 상태의 개발 작업을 허용할 수 있다.

1. 지정된 단말기에서만 접속 및 해당 단말기에 대한 접근 인원 통제
2. 지정 단말기는 온라인 용역 통제시스템 접속 전용(專用)으로 운용하고 다른 목적의 인터넷 접속은 차단
3. 발주기관 내 설치된 온라인 용역 통제시스템을 경유하여 개발에 필요한 정보시스템에 접속하는 등 소통 구간 보호·통제
4. 접속 사실이 기록된 로그기록을 1년 이상 보관
5. 계약 시행일로부터 종료 후 30일까지 본교 또는 상급 기관의 정기 또는 수시 보안 점검(불시 점검을 포함한다) 수검
6. 기타 국가정보원장이 배포한「국가·공공기관 용역업체 보안관리 가이드라인」에서 제시된 온라인 개발에 관련된 보안 대책의 준수

제28조(소프트웨어 산출물 제공) ① 총장은 용역업체가 「소프트웨어 진흥법」 제59조 및 「(계약예규) 용역계약 일반조건」(기획재정부 계약예규) 제56조에 따른 지식재산권을 행사하기 위하여 소프트웨어 산출물의 반출을 요청하는 경우 제안요청서 또는 계약서에 명시된 누출금지 정보에 해당하지 않으면 제공하여야 한다.

② 제1항에 따라 소프트웨어 산출물을 용역업체에 제공하는 경우 업체의 노트북·휴대용 저장매체 등 관련 장비에 저장된 누출금지 정보를 완전히 삭제하여야 하며 업체로부터 누출금지 정보가 완전히 삭제되었다는 대표자 명의의 확약서를 받아야 한다.

③ 용역업체가 소프트웨어 산출물을 제3자에게 제공하고자 하는 경우 제공하기 이전에 승인받도록 하여야 한다.

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

제29조(누출금지 정보 유출 시 조치) ① 총장은 용역업체가 제안요청서 또는 계약서에 명시된 누출금지 정보를 유출한 사실을 알게 된 경우 업체를 대상으로 계약 위반에 따른 조치를 하여야 한다. 이 경우 용역업체의 누출금지 정보 유출 사실을 알게 된 정보화 사업담당관 또는 사업과 관계된 구성원 등은 즉시 정보보안담당관을 거쳐 총장에게 보고하여야 한다.

② 제1항에 따라 용역업체의 누출금지 정보 유출 사실을 알게 되거나 보고를 받은 총장은 그 사실을 상급 기관에 통보하여야 하고 용역업체를 「국가를 당사자로 하는 계약에 관한 법률 시행령」 및 「지방자치단체를 당사자로 하는 계약에 관한 법률 시행령」에 따라 입찰 참가 자격 제한 등 관련 조처를 하여야 한다.

제5절 보안적합성 검증

제30조(대상 제품) 총장은 보안 기능이 있는 정보통신제품을 도입하는 경우 실제 적용·운용 이전에 안전성을 확인하기 위하여 보안적합성 검증을 받아야 한다. 다만, 「고등교육법」 제2조 각호의 학교 중 사립학교는 제외한다.

제31조(검증기관 및 신청) ① 총장은 제30조에 따른 보안적합성 검증을 받고자 하는 경우 국가정보원(이하 “검증기관”이라 한다)에게 검증을 신청하여야 한다.

② 제1항에도 불구하고 총장은 필요하다고 판단하는 경우 검증기관의 장과 협의하여 자체적으로 검증을 시행할 수 있다.

제32조(검증 신청시 제출물) ① 총장은 보안적합성 검증을 신청하는 경우 검증기관

의 장에게 [별표 3] '보안적합성 검증신청 시 제출물'에 해당하는 문서 등을 제출하여야 한다.

제33조(취약점 조치) ① 총장은 보안적합성 검증이 완료된 제품에서 새로운 취약점이 발견되는 경우 이를 제거 또는 보완하고 그 결과를 상급 기관의 장에게 통보하여야 한다.

② 검증기관의 장은 보안적합성 검증이 완료된 제품에서 새로운 취약점이 발견되는 경우 해당 제품을 개발·유통하는 자 또는 도입·운용 중인 기관의 장에게 취약점의 제거 또는 보완 조치를 요청할 수 있다.

③ 제2항에 따라 요청을 받은 기관의 장은 취약점의 제거 또는 보완 조치를 시행하고 그 결과를 검증기관의 장에게 통보하여야 한다.

제34조(형상 변경 및 용도변경 시 조치) 총장은 보안적합성 검증이 완료된 제품의 보안 기능 등 형상 변경이 필요하거나 도입 목적 이외의 용도로 운용이 필요한 경우 검증기관의 장과 협의하여 재검증 등 필요한 조처를 하여야 한다.

제3장 정보통신망 및 정보시스템 보안

제1절 정보통신망 보안

제35조(내부망·인터넷망 분리) ① 총장은 내부망과 기관 인터넷망을 분리·운영하여야 한다.

② 내부망과 기관 인터넷망을 분리·운영하고자 하는 경우 다음 각호의 사항을 포함한 보안 대책을 수립·시행하여야 한다.

1. 침입 차단·탐지시스템 설치 등 비(非)인가자 침입 차단 대책
2. 네트워크 접근관리시스템 설치 등 비(非)인가 장비의 내부망 접속 차단 대책
3. 내부망 정보시스템의 인터넷 접속 차단 대책
4. 내부망과 기관 인터넷망 간 안전한 자료전송 대책
5. 기타 국가정보원장이 배포한 「국가·공공기관 업무 전산망 분리 및 자료전송 보안 가이드라인」에서 제시하는 보안 대책

③ 정보시스템에 부여되는 IP주소를 체계적으로 관리하여야 하며 비(非)인가자로

부터 내부망을 보호하기 위하여 네트워크 주소변환기(NAT)를 이용하여 사설 IP 주소 체계를 구축·운영하여야 한다. 또한 IP주소별로 정보시스템 접속을 통제하여 비(非)인가 기기에 의한 내부망 접속을 차단하여야 한다.

④ 분리된 내부망과 기관 인터넷망 간 자료전송을 위한 접점이 불가피한 경우 다음 각호의 사항을 포함한 보안 대책을 수립·시행하여야 한다.

1. 침입 차단·탐지시스템 설치·운용
2. 내부망과 기관 인터넷망 간 접점 최소화
3. 내부망과 기관 인터넷망 간 일방향 전송 장비 등을 이용한 자료전송 체계를 구축·운영하고 원본 파일은 3개월 이상, 전송기록은 6개월 이상 유지
4. 정기적으로 전송 실패 기록을 확인하고 악성코드 유입 여부 등 점검
5. 내부망 자료를 기관 인터넷망으로 전송하는 경우 분임정보보안담당관 또는 결재권자의 사전 또는 사후 승인 절차 마련

⑤ 제1항에도 불구하고 예산 부족 등 사유로 부득이한 경우 상급 기관과 협의하여 내부망과 기관 인터넷망을 분리하지 아니할 수 있다. 이 경우 다음 각호의 사항을 포함한 보안 대책을 수립·시행하여야 한다.

1. 정보시스템과 개별 사용자 PC 영역 등에 대한 접근통제 대책
2. 인터넷 PC의 악성코드 감염 최소화를 위한 인터넷 사용 통제 대책
3. 인터넷 PC의 악성코드 감염에 따른 내부망으로 피해확산 차단 대책
4. 사이버 공격 탐지·대응 등 안전한 업무환경을 위한 보호 대책

⑥ 내부망과 기관 인터넷망의 IP주소 현황을 정기적으로 확인하고 갱신하여야 하며, 필요한 경우 전자적 시스템을 통하여 관리할 수 있다.

제36조(클라우드 컴퓨팅 보안) ① 총장은 클라우드 컴퓨팅(공공클라우드센터를 포함)을 자체 구축·운영하고자 하는 경우 국가정보원장이 배포한 「국가 클라우드 컴퓨팅 보안 가이드라인」에 명시된 기관 자체 클라우드 컴퓨팅 구축 보안 기준에 따라 보안 대책을 수립·시행하여야 한다.

② 총장은 민간 클라우드 컴퓨팅 서비스를 이용하고자 하는 경우 다음 각호에 해당하는 사항을 준수하여야 한다.

1. 국내 위치한 정보시스템(인증 서버, 로그 및 백업 서버 등)·관리주체에 의해 데이터가 저장·관리되는 서비스의 이용
2. 다음 각 목의 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 간섭없이 국가정보원 및 이용기관의 보안관제, 사고조사, 예방 보안 활동 유지를 위한 제반 환경을 만족해야 함
   나. 영역 분리는 ‘시스템 중요도’에 따라 물리적 또는 논리적으로 구현
   다. ‘시스템 중요도’ 분류는 [별표 9]에 따른 기준 준용
3. 국가정보원장이 배포한 「국가 클라우드 컴퓨팅 보안 가이드라인」에서 정하는 바에 따라 국가정보원장이 게시하거나 게시 예정인 민간 클라우드 컴퓨팅 서비스 이용
4. ‘내부망・인터넷망 분리’ 원칙 등 여타 보안 관련 사항은 「국가 정보보안 기본지침」 및 「국가 클라우드 컴퓨팅 보안 가이드라인」 준수
5. 민간 클라우드 컴퓨팅 서비스사업자와 계약 시 해킹 사고 및 장애 대응, 재발방지 등에 필요한 조치를 위해 국가정보원과 이용 기관의 보안관제 및 사고조사, 사이버 공격 및 위협에 대한 예방 및 대응 활동 등에 적극 협조하도록 하는 내용의 명시

③ 본교의 내부망과 연동된 공공 전용(專用) 민간 클라우드는 이 지침을 적용 함에 있어 본교의 내부망으로 본다.

④ 본교의 기관 인터넷망과 연동된 공공 전용(專用) 민간 클라우드는 이 지침을 적용 함에 있어 본교의 기관 인터넷망으로 본다.

⑤ 제2항에 따라 민간 클라우드 컴퓨팅 서비스를 이용하는 중 클라우드 컴퓨팅 서

비스제공자에 의하여 누출금지 정보가 유출된 경우 제29조에 따른 조치를 하여야 한다.

⑥ 제2항에 따라 본교가 이용하는 민간 클라우드 컴퓨팅 서비스의 제공자는 공공 전용(專用) 민간 클라우드 영역에 대해 정부 기관에 준하는 보안관리 책임을 진다.

⑦ 교육 현장에는 제1항 및 제2항을 적용하지 않으며, 총장의 책임하에 자체 구축하거나 민간 클라우드 컴퓨팅 서비스를 이용할 수 있다.

제37조(보안・네트워크장비 보안) ① 총장은 침입 차단・탐지시스템, 스위치・라우터 등 정보통신망 구성 또는 본교 정보보안 정책 전반에 영향을 미치는 보안시스템, 네트워크 장비를 설치・운용하고자 하는 경우 다음 각호의 사항을 포함한 보안대책을 수립・시행하여야 한다.

1. 물리적으로 안전한 장소에 설치하여 비(非)인가자의 무단 접근통제
2. 콘솔에서 관리함을 원칙으로 하되, 다음 각 목의 경우 본교 내 지정 단말기로부터의 접속 관리 허용

   가. 장비 관리자의 접속

   나. 제25조의2 제2항 단서에 따른 본교의 용역업체 작업 장소에서의 접속
3. 최초 설치하는 경우 디폴트(default) 계정은 삭제하거나 변경 사용하고 장비 관리를 위한 관리자 계정을 별도로 생성・운영
4. 불필요한 서비스 포트와 개별 사용자 계정은 차단 및 삭제
5. 펌웨어 무결성과 컴퓨터 운영체제・소프트웨어의 취약점 및 버전 업데이트 여부를 정기적으로 점검하고 최신 버전으로 유지

② 보안・네트워크 장비 관리자는 로그기록을 1년 이상 유지하여야 하고 비(非)인가자의 접속 여부를 정기적으로 점검하여 그 결과를 정보보안담당관에게 통보하여야 한다.

③ 보안・네트워크 장비 관리자는 침입 차단・탐지시스템의 침입 차단・탐지규칙

(rule)의 생성 근거를 유지하고 정기적으로 필요성 여부를 점검・갱신하여야 한다.

제38조(무선랜 보안) ① 총장은 내부망을 제외한 정보통신망에서 다음 각호의 경우와 같이 무선랜(WiFi)을 구축・운용할 수 있다.

1. 기관 인터넷망에 중계기(AP)를 설치하여 본교에서 지급한 단말기의 접속만을 허용하는 업무용 무선랜
2. 상용 인터넷망에 중계기(AP)를 설치하여 구성원 등의 개인 소유 이동통신단 말기의 접속만을 허용하는 무선랜
3. 상용 인터넷망에 중계기(AP)를 설치한 외부인 전용(專用) 무선랜

② 제1항에 따라 무선랜을 구축・운용하고자 하는 경우 국가정보원장이 배포한 「국가・공공기관의 무선랜 구축 및 RFID 보안 가이드라인」을 준수하여 보안대책을 수립・시행하여야 한다.

③ 제2항에 따른 보안 대책을 수립하는 경우 제1항 제1호 및 제2호에 따른 무선랜에 대하여 다음 각호의 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 할당 기록 등 유지
5. IEEE 802.1X, AAA(Authentication Authorization Accounting) 등의 기술에 따라 상호 인증을 수행하는 무선랜 인증 제품 사용
6. 무선 침입방지시스템 설치 등 침입 차단 대책
7. 기관의 내부망 정보시스템 또는 인접해 있는 다른 기관의 정보시스템이 해당 무선랜에 접속되지 않도록 하는 기술적 보안 대책
8. 그 밖에 무선랜 단말기・중계기(AP) 등 구성 요소별 분실・탈취・훼손・오용

등에 대비한 관리적·물리적 보안 대책

④ 분임정보보안담당관은 제2항 및 제3항에 따른 보안 대책의 적절성을 수시로 점검·보완하여야 한다.

⑤ 교육 현장에는 제1항부터 제3항까지를 적용하지 않으며, 총장의 책임하에 무선랜을 구축·운용할 수 있다.

제39조(이동통신망 보안) ① 총장은 이동통신망(HSDPA·WCDMA·LTE·5G 등)을 이용하여 시스템을 구축하거나 중요자료를 소통하고자 하는 경우 암호화 및 비인가 단말기의 이동통신망 접속 차단 등 기술적 보안 대책을 수립·시행하여야 한다.

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

③ 교육 현장에는 제1항 및 제2항을 적용하지 않으며, 총장의 책임하에 구축·운용할 수 있다.

제40조(영상회의 보안) ① 총장은 영상회의시스템을 구축·운용하고자 하는 경우 통신망(국가정보통신망·전용(專用)선·인터넷 등) 암호화 등 보안 대책을 수립·시행하여야 한다.

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

③ 총장은 다음 각호의 구분에 따라 상용 소프트웨어에 탑재된 영상회의 서비스를 이용할 수 있다.

1. 비공개 업무자료를 취급하거나 회의 내용이 비공개 업무자료에 준하다고 판단되는 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 판단되는 경우 : 국내 영상회의 솔루션 또는 그 밖의 영상회의 소프트웨어를 활용

④ 기타 영상회의 보안과 관련한 사항은 국가정보원장이 배포한「원격업무 통합 보안 매뉴얼」을 준수하여야 한다.

제41조(인터넷전화 보안) ① 총장은 인터넷전화 시스템을 구축·운용하거나 민간 인터넷전화 사업자 망을 이용하고자 하는 경우 다음 각호의 사항을 포함한 보안 대책을 수립·시행하여야 한다.

1. 한국정보통신기술협회(TTA) verified ver.4 이상 보안 규격으로 인증받은 행정기관용 인터넷전화 시스템 설치·운용
2. 인터넷전화기에 대한 장치 및 사용자 인증
3. 제어신호 및 통화 내용 등 데이터 암호화
4. 인터넷 전화망과 다른 정보통신망과의 분리
5. 인터넷전화 전용(專用) 침입 차단 시스템 등 정보보호 시스템 설치·운용
6. 백업체제 구축

② 민간 인터넷전화 사업자 망을 이용하는 경우 해당 사업자에게 서비스 제공 구간에 대한 보안 대책을 수립하도록 하여야 한다.

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

제42조(인터넷 사용제한) ① 총장은 국가비상사태 및 대형 재해·재난의 발생, 사이버 공격 등으로부터 정보통신망과 정보시스템의 정상적인 운영을 보장하기 위하여 소속 구성원 등에 대한 인터넷 사용을 일부 제한할 수 있다.

② 총장은 본교 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 상용 정보통신 서비스의 접속을 제한할 수 있다.

제2절 정보시스템 보안

제43조(정보시스템 보안책임) ① 총장은 정보시스템(PC・서버・네트워크 장비・정보통신기기・정보 보호시스템・DB 및 소프트웨어・부대설비 등을 포함한다)을 도입・운용하는 경우 해당 정보시스템에 대하여 시스템 관리책임자와 관리자를 지정・운영하여야 한다.

② 정보시스템 관리책임자는 총장이 별도로 지정하지 않는 경우 정보시스템을 실제 운용하는 각 처, 원, 실, 센터, 단, 부의 장이 되며, 정보시스템 관리자는 관리책임자가 지정한다. 단 정보시스템 관리자를 별도 지정하지 않는 경우 각 소속 부서 또는 단체의 업무분장표에 따른다.

③ 정보시스템 관리책임자와 관리자는 소속 부서 또는 단체가 사용하는 정보시스템(DB나 파일 형태의 전자정보를 포함한다) 및 정보시스템 관련 문서정보의 운용・관리에 대한 보안책임을 가진다.

④ 정보시스템 관리책임자는 [별표 7] '자산 분류 기준' 및 '자산 보안등급 기준'을 참조하여 [서식 제1호]의 정보시스템 관리 대장에 자산 현황(자산 보안등급을 포함)을 수기 또는 전자적으로 작성・관리하여야 하며, 정보시스템의 최종 변경 현황을 항시 기록하고 유지하여야 한다.

⑤ 정보보안담당관은 정보시스템 운용과 관련하여 보안 취약점을 발견하거나 보안 대책 수립이 필요하다고 판단되는 경우 개별 사용자, 정보시스템 관리자 또는 관리책임자에게 개선 조치를 요구할 수 있으며 조치가 완료될 때까지 정보시스템의 운용을 일시 제한할 수 있다.

제44조(정보시스템 유지보수) ① 정보시스템의 유지보수를 위하여 절차 및 문서화를 수립하는 경우 다음 각호의 사항을 포함하여야 한다.

1. 유지보수 인원에 대한 보안 서약서 집행, 보안 교육 등을 포함한 유지보수인가 절차를 마련하고 인가된 인원만 유지보수에 참여
2. 결함이 의심되거나 발생한 결함, 예방 및 유지보수에 대한 기록유지
3. 유지보수를 위하여 정보시스템을 원래 설치 장소에서 다른 장소로 이동하는 경우 통제 수단 마련
4. 유지보수 일시 및 담당자 인적 사항, 출입 통제 조치 사항, 작업수행 내용 등 기록유지

② 정보시스템 관리자는 용역업체 등이 유지보수와 관련한 장비・도구 등을 발주기관 내 용역업체 작업 장소로 반출・입하는 경우 악성코드 감염 여부 및 비밀자

료· 누출금지 대상 정보 등 무단 반출 여부 확인 등 보안 조치를 시행하고 그 결과를 정보보안담당관에게 제출하여야 한다.

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

④ 정보보안담당관은 소관 정보시스템에 대하여 서비스 영향, 중요도, 기밀성・무결성・가용성 등에 따라 등급을 분류하고 해당 등급에 맞게 정보 보존 및 관리, 장애관리, 보안관리 등을 수행하여야 한다.

제45조(지정 단말기를 통한 온라인 유지보수) ① 총장은 지정된 단말기를 통해 유지보수를 함에 있어 정보보안담당관이 필요하다고 판단하고 용역업체가 다음 각 호에 따른 보안 대책에 서면으로 동의하는 경우, 용역업체에 내부망을 포함하여 소관 정보시스템에 대하여 인터넷을 통한 온라인 유지보수를 허용할 수 있다.

1. 지정된 장소에 설치된 지정된 단말기에서만 접속 및 해당 단말기에 대한 접근 인원 통제
2. 지정 단말기는 제3호에 따른 온라인 용역 통제시스템 접속 전용(專用)으로 운용하고 다른 목적의 인터넷 접속은 차단
3. 발주기관 내 설치된 온라인 용역 통제시스템을 통하여 유지보수 대상 정보시스템에 접속하는 등 소통 구간 보호・통제
4. 접속 사실이 기록된 로그기록을 1년 이상 보관
5. 유지보수 계약 시행일로부터 종료 후 30일까지의 기간 중 발주기관의 정기 또는 수시 점검(불시 점검을 포함한다) 수검
6. 기타 국가정보원장이 배포한 「국가・공공기관 용역업체 보안관리 가이드라인」에서 제시된 온라인 유지보수에 관련된 보안 대책의 준수

② 총장은 전항 제2호 및 제3호에도 불구하고 온라인 용역 통제시스템이 구축되지 않은 경우, 온라인 유지보수를 즉시 실시하지 않고서는 기관 업무수행에 현저한 저해가 있다고 예상된 때에는 인터넷망 정보시스템에 한하여 직접 접속하는 온라인 유지보수를 일시적으로 허용할 수 있다.

③ 기타 정보시스템 온라인 유지보수 보안과 관련한 사항은 제23조(용역업체 보안)를 준용한다.

제46조(서버 보안) ① 총장은 서버를 도입・운용하고자 하는 경우 사이버 공격으로 인한 자료 절취 및 위・변조 등에 대비하여 다음 각호의 사항을 포함한 보안 대책을 수립・시행하여야 한다.

1. 서버 내 저장자료에 대하여 업무별・자료별 중요도에 따라 개별 사용자의 접근 권한 차등 부여
2. 개별 사용자별 자료 접근 범위를 서버에 등록하여 인가 여부를 식별하도록 하고 인가된 범위 이외 자료 접근 통제
3. 서버 운용에 필요한 서비스 포트 이외 불필요한 서비스 포트 제거 및 관리자용 서비스와 개별 사용자용 서비스 분리・운용
4. 악성코드 등의 감염 방지를 위한 보안프로그램 설치・운영
5. 관리자용 서비스 접속 시 특정 IP주소가 부여된 관리용 단말기 지정・운용
6. 서버 설정 정보 및 저장자료에 대한 정기적 백업 시행
7. 데이터베이스에 대해서는 개별 사용자의 직접 접속 차단, 중요정보 암호화(개인정보, 비밀번호 등), 접근제어 시스템 적용 등 데이터베이스별 보안 조치실시

② 서버 관리자는 제1항에 따른 보안 대책의 적절성을 수시 확인하여야 하며 연1회 이상 서버 설정 정보와 저장자료의 절취 및 위・변조 가능성 등 보안 취약점을 점검・보완하여야 한다.

제47조(제어시스템 보안) ① 총장은 전력・가스・환기・에너지・운송설비 등을 중앙에서 감시・제어하기 위한 정보시스템(이하 “제어시스템”이라 한다)을 구축・운용하고자 하는 경우 최신 백신 소프트웨어 설치, 응용프로그램 보안패치 및 침해사고 대응 방안 등 보안 대책을 수립・시행하고 정기적으로 취약점을 점검・제거하여야 한다. 다만, 제어시스템 관리책임자는 백신 소프트웨어 등 보안 소프트웨어를 설치함으로써 제어시스템의 정상 운영에 차질을 초래하는 경우 정보보안담당관과 협의하여 설치하지 아니할 수 있다.

② 기타 제어시스템 보안과 관련한 사항은 국가정보원장이 배포한 「국가・공공기관 제어시스템 보안 가이드라인」을 준수하여야 한다.

제48조(공개 서버 보안) ① 총장은 외부인에게 공개할 목적으로 웹서버 등 공개 서버를 구축・운용하고자 하는 경우 내부망과 분리된 영역(DMZ)에 설치하여야 한다.

② 정보보안담당관은 비(非)인가자의 공개 서버 저장자료 절취 및 위・변조, 분산서비스거부(DDoS) 공격 등에 대비하여 침입 차단・탐지시스템 및 DDoS 대응 장비 설치 등 보안 대책을 수립・시행하여야 한다.

③ 공개 서버 관리자는 비(非)인가자의 공개 서버 내 비공개 정보에 대한 무단 접근을 방지하기 위하여 서버에 접근할 수 있는 개별 사용자를 제한하고 불필요한 계

정은 삭제하여야 한다.

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

⑤ 기타 공개 서버 보안과 관련한 사항은 제46조(서버 보안)를 준용한다.

제49조(로그기록 유지) ① 총장은 정보시스템의 효율적인 통제·관리 및 사고 발생 시 추적 등을 위하여 로그기록을 유지·관리하여야 한다.

② 제1항에 따른 로그기록에는 다음 각호의 사항이 포함되어야 한다.

1. 접속자, 정보시스템·응용프로그램 등 접속 대상
2. 로그온·오프 자료의 열람·출력 등 작업 종류 및 시간
3. 접속 성공·실패 등 작업 결과
4. 전자우편 사용 등 외부 발송 정보 등

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 위·변조 및 삭제 등 의심스러운 정황이나 위반한 사실을 발견하는 경우 즉시 정보보안담당관에게 통보하여야 한다.

⑤ 정보시스템 관리자는 로그기록을 1년 이상 보관하여야 하며 로그기록의 위·변조 및 외부 유출 방지 대책을 수립·시행하여야 한다.

제50조(모바일 업무 보안) ① 총장은 휴대전화·태블릿 PC 등을 이용한 모바일 업무환경(내부 행정업무, 현장 행정업무 및 대민서비스 업무 등)을 구축·운용하고자 하는 경우 보안 대책을 수립·시행하여야 한다.

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

제51조(사물인터넷 보안) ① 총장은 사물인터넷을 이용한 시스템을 구축·운용하고자 하는 경우 사물인터넷 기기와 중요 데이터 등을 보호하기 위하여 보안 대책을 수립·시행하여야 한다.

② 사물인터넷을 이용한 시스템을 구축·운용하고자 하는 경우 내부망과 분리하여야 한다. 다만, 내부망과 연동이 필요한 경우에는 망간 자료전송 제품 설치 등 보안 대책을 수립하여야 한다.

③ 사물인터넷 서비스를 위한 소프트웨어를 개발하는 경우 제24조(소프트웨어 개

발 보안)를 준수하여야 한다.

④ 기타 사물인터넷 보안과 관련한 사항은 국가정보원장이 배포한 「국가・공공기관 사물인터넷(IoT) 보안 가이드라인」을 준수하여야 한다.

제52조(원격근무 보안) ① 총장은 소속 구성원 등이 재택근무, 출장지 현장 근무, 또는 파견 근무 시 인터넷을 통해 본인 인증을 거쳐 기관 정보시스템에 접속하여 온라인으로 수행하는 업무를 수행(이하 “원격근무”라 한다)하게 할 수 있다.

② 제1항에 따른 원격근무를 위해 접속할 수 있는 본교의 정보시스템은 다음 각호와 같다.

1. 인터넷망(DMZ 망)에 위치한 서버와 서버에서 구동되는 가상 PC
2. 안전한 자료전송 대책(VPN, 암호화 전송 등)을 통해 접속할 수 있는 내부망 서버 및 내부망 서버에서 구동되는 가상 PC

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

④ 원격근무를 시행하고자 하는 경우 다음 각호의 사항을 포함한 보안 대책이 강구된 정보시스템(이하 “원격근무 시스템”이라 한다)을 구축・운영하여야 한다.

1. 검증필 암호모듈이 탑재된 정보보호 시스템을 사용해 원격근무시스템과 원격근무자의 단말기 간 소통 구간 암호화
2. 문서 암호화 제품(DRM) 사용 등 문서 보호 대책 강구
3. 원격근무자를 식별・인증하기 위하여 공인인증서, 생체인증 기술 및 일회용 비밀번호 생성기(OTP) 등 보안성을 강화한 사용자 인증 방식 적용
4. 원격근무자에게 원격근무시스템 접속 과정에서 제1호부터 제3호까지의 보안 대책을 준수토록 조치
5. 원격근무시스템에 대한 보안 취약점 정기 점검

⑤ 원격근무자는 정보보안담당관이 원격근무용 단말기(개인 소유의 정보통신기기를 포함한다)의 보안을 위하여 취하는 다음 각호의 조치에 적극적으로 협조하여야 한다.

1. 제4항에 따라 본교에서 제공하는 보안 소프트웨어 설치・운영
2. 사이버 공격 등으로 인한 자료 유출 사고 발생 시 정보보안담당관이 요청하는 점검 및 이에 따른 자료 제출 요청 협력
3. 본교에서 지급한 단말기의 경우 본 지침의 단말기 보안 대책 준수

⑥ 총장은 원격근무자에게 보안 조치 등이 포함된 보안 서약서를 징구하고 직위・

임무에 부합한 정보시스템 접근권한 부여 및 보직 변경·퇴직 등 변동 사항이 발생 시 접근권한 조정 등의 절차를 마련·시행하여야 한다.

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

제53조(저장매체 불용 처리) ① 총장은 정보시스템 또는 저장매체(광디스크·자기테이프·휴대용 저장매체·하드디스크·반도체 기반 저장장치(SSD 및 EEPROM 등)를 외부 수리·교체·반납·양여·폐기·불용 처리하고자 하는 경우 정보시스템 또는 저장매체에 저장된 자료가 외부에 유출되지 않도록 자료 삭제 등 보안 조치를 시행하고 현황을 기록하여야 한다. 이 경우 정보시스템 관리자 및 개별 사용자는 분임정보보안담당관과 협의하여야 한다.

② 제1항에 따라 자료를 삭제하는 경우 [별표 8] '정보시스템 저장매체 자료별 삭제 방법'을 준수하여야 하며, 본교의 실정 및 중요도에 맞게 저장매체별·자료별 차별화된 삭제 방법을 적용할 수 있다.

③ 비밀·대외비를 저장하거나 암호화키를 저장한 저장매체는 소각·파쇄·용해 등의 방법으로 완전히 파괴하여야 한다.

④ 저장매체에 저장된 자료의 삭제·소각·파쇄·용해 등을 외부 업체에 의뢰할 때는 정보시스템 관리책임자 또는 관리자가 입회하여 완전 삭제 및 완전 파괴 등을 확인하여야 하며, 그 결과를 분임정보보안담당관에게 보고하여야 한다.

⑤ 기타 정보시스템 및 저장매체의 불용 처리와 관련한 사항은 국가정보원장이 배포한 「정보시스템 저장매체 불용 처리 지침」을 준수하여야 한다.

제3절 자료 보안

제54조(비밀의 전자적 처리) ① 총장은 비밀의 생산, 분류, 보관, 열람, 출력, 송·수신, 이관, 파기 등을 전자적으로 처리할 수 있다.

② 총장은 비밀을 전자적으로 처리하는 전(全) 과정에서 기밀성, 무결성, 인증, 부인방지 등 보안성을 확보하여야 하며 이를 위하여 국가정보원장이 개발하거나 안전성을 확인한 암호자재를 사용하여야 한다.

③ 제1항에 따라 비밀을 전자적으로 처리하는 경우 내부망과 기관 인터넷망이 물리적으로 분리된 기관은 내부망 PC에서 비밀을 전자적으로 처리할 수 있으며 그 밖의 기관은 내부망 및 기관 인터넷망과도 분리된 별도의 비밀 작업용 PC에서 처리하여야 한다.

제55조(비밀 관리시스템 운용) ① 총장은 국가정보원장이 비밀을 전자적으로 안전하게 처리하기 위하여 개발·보급하는 비밀 관리시스템을 도입·운용할 수 있다.

② 비밀 관리시스템을 운용하는 경우 비밀의 생산·보관·유통 등 전반에 대하여 비밀 관리시스템을 활용하여 비밀을 안전하게 관리하여야 하며 기타 비밀 관리에 관한 사항은 국가「보안업무규정」을 준수하여야 한다.

제56조(대외비의 전자적 처리) ① 총장은 대외비를 전자적으로 처리하고자 하는 경우 검증필 암호모듈을 사용하여 위조·변조·훼손 및 유출 등을 방지하기 위한 보안대책을 강구 하여야 한다.

② 제1항에 따라 업무와 관계되지 아니한 사람은 대외비를 열람, 복제·복사, 배부할 수 없다.

제57조(행정전자서명 인증서 등 관리) ① 본교 구성원은 비공개 업무자료를 처리하기 위하여「전자정부법」 제29조에 따른 행정전자서명의 인증서(이하 “행정전자서명 인증서”라 한다)를 인터넷 PC 또는 개인이 소유한 PC·휴대용 저장매체·휴대전화 등에 저장·보관할 수 있다.

② 행정전자서명 인증서 및 인증서의 비밀번호, 전자우편의 비밀번호 등을 상용 정보통신 서비스를 이용하여 수·발신하거나 저장·보관하여서는 아니 된다.

제58조(홈페이지 등 게시자료 보안) ① 총장은 비공개 업무자료가 홈페이지 또는 외부 웹 사이트(이하 “홈페이지 등”이라 한다.)에 무단 게시되지 않도록 게시자료의 범위, 자료의 게시 방법 등을 규정한 자체 홈페이지 정보공개 보안 지침을 수립·시행하여야 한다.

② 분임정보보안담당관은 해당 부서에서 홈페이지 등에 업무자료를 게시하고자 하는 경우 자료 내용을 사전 검토하여 비공개 업무자료가 게시되지 않도록 하여야 한다.

③ 분임정보보안담당관은 소속 부서에서 운영하는 홈페이지에 비공개 업무자료가 무단 게시되었는지를 정기적으로 점검하여야 한다.

④ 정보보안담당관은 홈페이지 등에 비공개 업무자료가 무단 게시된 사실을 알게 된 경우 즉시 삭제 또는 차단 등 보안 조치를 하여야 한다.

제59조(정보통신망 현황자료 관리) ① 총장은 다음 각호에 해당하는 자료를 「공공기관의 정보공개에 관한 법률」 제9조 제1항에 따른 비공개 대상 정보로 지정·관리하여야 한다.

1. 정보통신망 구성 현황(IP주소 할당 현황을 포함한다. 이하 본 조에서 같다)

2. 정보시스템 운용 현황
3. 취약점 분석·평가 결과물(「정보통신기반 보호법」 제9조에 따른 취약점 분석·평가 결과를 포함한다. 이하 본 조에서 같다)
4. 암호자재 운용 현황
5. 주요 정보화 사업 추진 현황

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

제60조(빅데이터 보안) ① 총장은 빅데이터와 관련한 시스템을 구축·운용하고자 하는 경우 다음 각호의 사항을 포함한 보안 대책을 수립·시행하여야 한다.

1. 데이터의 수집 출처 확인 및 데이터 오·남용 방지
2. 데이터의 수집을 위한 정보통신망 보안 체계 수립
3. 수집된 데이터의 저장 및 보호 체계 수립
4. 중요 데이터 암호화
5. 사용자별(데이터 제공자·수집자·분석요청자 및 분석 결과 제공자 등) 권한 부여 체계 수립
6. 데이터 파기 절차 수립

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

제4절 사용자 보안

제61조(개별 사용자 보안) ① 총장은 소관 정보통신망 또는 정보시스템의 사용과 관련하여 다음 각호의 사항을 포함하여 개별 사용자 보안에 관한 사항을 실시하여야 한다.

1. 직위·임무별 정보통신망 접근권한 부여
2. 비밀 취급 시 비밀취급 인가, 보안 서약서 징구 등 보안 조치
3. 보직 변경, 퇴직 등 변동 사항 발생 시 정보시스템 접근권한 조정

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

제62조(단말기 보안) ① 개별 사용자는 본교에서 지급한 업무용 PC·노트북·휴대

전화・스마트 패드 등 단말기(이하 “단말기”라 한다) 사용과 관련하여 모든 보안 관리 책임을 진다.

② 개별 사용자는 단말기에 대하여 다음 각호에 해당하는 보안 대책을 준수하여야 한다.

1. CMOS・로그온 비밀번호의 정기적 변경 사용
2. 단말기 작업을 일정 시간 이상 중단 시 비밀번호 등을 적용한 화면보호 조치
3. 최신 백신 소프트웨어 및 본교에서 운영하는 보안프로그램 설치
4. 운영체제 및 응용프로그램에 대한 최신 보안패치 유지
5. 출처, 유통경로 및 제작자가 불분명한 응용프로그램의 사용 금지
6. PC 폴더, 파일 등 공유 금지(부득이한 경우 패스워드, 보안인증 설정 후 사용)
7. 인터넷을 통해 자료(파일) 획득 시 신뢰할 수 있는 인터넷사이트를 활용하고 자료(파일) 다운로드 시 최신 백신 소프트웨어로 검사 후 활용
8. 인터넷 파일 공유・메신저・대화방 프로그램 등 업무상 불필요한 프로그램의 설치 금지 및 공유 폴더 삭제
9. 웹브라우저를 통해 서명되지 않은 액티브-X 등이 다운로드・실행되지 않도록 보안 설정
10. 내부망과 기관 인터넷망이 분리 운영 시 인터넷 PC에서는 총장이 정한 특별한 사유가 없는 한 문서프로그램을 읽기 전용(專用)으로 운용
11. 그 밖에 국가정보원장이 안전성을 확인하여 배포한 프로그램의 운용 및 보안 권고문 이행

③ 분임정보보안담당관은 정보보안담당관 총괄하에 개별 사용자의 제2항 각호에 해당하는 보안 대책의 준수 여부를 정기적으로 점검하고 개선 조치하여야 한다.

④ 개별 사용자는 개인 소유의 단말기(PC, 노트북PC, 기타 네트워크 접속 단말기 등)를 무단 반입하여 교내 네트워크에 연결할 수 없다. 다만 부득이한 경우에는 정보보안담당관의 승인 및 제2항 각호에 따른 보안 대책 후 반입하여 네트워크에 연결할 수 있다.

⑤ 개별 사용자는 사용하는 단말기에 악성코드 감염을 발견하는 경우 즉시 네트워크와 접속 분리 조치 후 시스템 관리자와 분임정보보안담당관에 보고하여야 한다. 이때 개별 사용자 또는 시스템 관리자는 다음 각호의 조치를 하여야 한다.

1. 감염된 시스템 사용 중지 조치 및 네트워크 접속 분리 확인
2. 최신 백신 등 악성코드 제거 프로그램을 이용하여 치료

3. 필요시 악성코드 감염 증거 보전 또는 별도 보관
4. 원인 분석 및 예방조치 수행
5. 정보보안담당관에 관련 내용 및 보안 조치 사항 보고(긴급 사항 시 즉시 보고)

⑥ 정보보안담당관은 악성코드에 감염된 단말기의 원인 분석 결과 개별 사용자의 잘못이 명백한 경우 해당 사용자에 대하여 주의·경고 및 사용 제한 조치를 할 수 있으며, 중대한 악성코드 감염 관련 사항으로 상급 기관에서 조치 및 보고를 요구하는 경우 이를 이행하여야 한다.

⑦ 교육 현장에는 제1항부터 제3항까지를 적용하지 않으며, 단말기 보안과 관련한 사항을 총장이 별도로 정할 수 있다.

제63조(계정관리) ① 총장은 개별 사용자에게 소관 정보통신망 또는 정보시스템의 접속에 필요한 사용자 계정(아이디)을 부여하고자 하는 경우 다음 각호에 해당하는 사항을 준수하여야 한다.

1. 개별 사용자별 또는 그룹별 접근권한 부여
2. 외부인에게는 계정을 부여하지 않되 업무상 불가피한 경우 정보보안담당관의 책임하에 보안 조치 후 필요한 업무에만 일정 기간 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 정보시스템 관리자는 개별 사용자가 시스템 접속(로그온)에 5회 이상 실패하는 경우 접속이 중단되도록 시스템을 설정하고 비(非)인가자의 침입 여부를 점검하여야 한다.

③ 정보시스템 관리자는 개별 사용자의 보직 변경, 퇴직, 계약종료 등의 변동이 있는 경우 신속히 사용자 계정을 삭제하거나 부여된 접근권한을 회수하여야 한다.

④ 정보시스템 관리자는 사용자 계정 부여와 관리의 적절성을 연 2회 이상 점검하고 그 결과를 정보보안담당관에게 통보하여야 한다.

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

제64조(비밀번호 관리) ① 개별 사용자 및 시스템 관리자는 각종 비밀번호를 다음 각호에 해당하는 사항을 반영하여, 숫자・영문 대소문자・특수문자 등을 9자리 이상 혼합하여 안전하게 설정하고, 최소 분기마다 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 입력 기능을 사용하지 말 것

② 정보시스템 관리자는 서버 등 정보시스템에 보관되는 비밀번호가 복호화되지 않도록 일 방향 암호화하여 저장하여야 한다.

③ 총장은 정보시스템에서 개별 사용자를 식별 또는 인증하기 위하여 비밀번호에 갈음하거나 병행하여 지문인식 등 생체인증 기술 및 일회용 비밀번호 생성기(OTP) 등을 안전성 확인 후 사용할 수 있다. 이 경우 생체인증 정보는 안전하게 보관하여야 한다.

④ 「개인정보 보호법」에 따른 고유 식별정보 또는 민감정보를 취급하는 업무용 정보시스템은 비밀번호가 아닌 생체인증, 일회용 비밀번호 생성기(OTP), 전자서명 인증서, 2차 인증시스템 등 보안성을 강화한 인증 체계를 적용하여야 한다.

제65조(전자우편 보안) ① 총장은 전자우편을 컴퓨터바이러스·트로이목마 등 악성코드로부터 보호하기 위하여 백신 소프트웨어 설치, 해킹 메일 차단 시스템구축 등 보안 대책을 수립·시행하여야 한다.

② 전자우편을 구축·운용하는 경우 다른 전자우편과 자료를 안전하게 소통하기 위하여 전자우편시스템에 암호화 기술을 적용하여야 한다.

③ 전자우편을 구축·운용하는 경우 수신된 전자우편의 발신지 IP주소 및 국가명이 표시되고 해킹 메일로 의심되는 경우 해킹 매일 원본을 전송하여 신고할 수 있는 기능을 갖추어야 한다.

④ 개별 사용자는 수신된 전자우편에 포함된 첨부파일이 자동 실행되지 않도록 기능을 설정하고 첨부파일을 다운로드 시에는 최신 백신 소프트웨어로 악성코드 은닉 여부를 검사하여야 한다.

⑤ 개별 사용자는 출처가 불분명하거나 의심되는 제목의 전자우편은 열람하지 말고 해킹 메일로 의심되는 경우 즉시 정보보안담당관에게 신고하여야 한다. 정보보안담당관은 해킹 메일로 판단되는 경우 교육부 장관에게 통보하여야 한다.

⑥ 본교 전자우편을 통한 비밀 및 비공개 업무자료의 외부 전송은 금지한다. 단 부득이하게 비공개 업무자료를(비밀자료는 전송금지) 전송하여야 하는 경우 비밀번

호설정·암호화 전송 기술 등을 통하여 안전한 방법으로 전송하여야 한다.

⑦ 총장은 전자우편 발신자 조작 등을 통한 기관 사칭 전자우편의 유포를 차단하기 위하여 보안 대책을 수립·시행하여야 한다.

제66조(휴대용 저장매체 보안) ① 총장은 휴대용 저장매체를 사용하여 업무자료를 보관하고자 하는 경우 자료의 위·변조, 저장매체의 훼손·분실 등에 대비한 보안대책을 수립·시행하여야 한다.

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

③ 정보보안담당관은 개별 사용자가 휴대용 저장매체를 PC·서버 등에 연결하는 경우 자동 실행되지 않고 최신 백신 소프트웨어로 악성코드 감염 여부를 자동 검사하는 등의 보안정책을 수립·시행하도록 관리하여야 한다.

④ 분임정보보안담당관은 소속 부서의 휴대용 저장매체를 비밀 용·일반용으로 구분·관리하고 수량 및 보관 상태를 정기적으로 점검하며 외부 반출·입을 통제하여야 한다.

⑤ 분임정보보안담당관은 비밀이 저장된 휴대용 저장매체를 관리할 때는 매체별로 비밀등급 및 관리 번호를 부여하고 비밀 관리기록부에 등재·관리하여야 한다. 이 경우 매체 전면에 비밀등급 및 관리 번호가 표시되도록 하여야 하며, 이중 잠금장치 또는 금고에 보관하여야 한다.

⑥ 분임정보보안담당관은 비밀 용 휴대용 저장매체를 다른 등급의 비밀 용 또는 일반용으로 변경 사용하고자 하는 경우 저장자료가 복구 불가하도록 완전 삭제 소프트웨어 등을 사용하여 삭제하여야 한다. 다만, 완전 삭제가 불가할 경우 변경 사용하여서는 아니 된다.

⑦ 분임정보보안담당관은 휴대용 저장매체를 폐기·불용 처리하고자 하는 경우 저장자료가 복구 불가하도록 완전 삭제 소프트웨어 등을 사용하여 삭제하여야 한다. 다만, 완전 삭제가 불가할 경우 파쇄하여야 한다.

⑧ 분임정보보안담당관은 정보보안담당관 총괄하에 소속 부서에 대하여 개별 사용자의 휴대용 저장매체 무단 반출, 미(未)등록 휴대용 저장매체 사용 여부 등 보안관리 실태를 정기적으로 점검하여야 한다.

⑨ 그 밖에 휴대용 저장매체 보안과 관련한 사항은 국가정보원장이 배포한 「USB 메모리 등 휴대용 저장매체 보안관리 지침」을 준수하여야 한다.

제67조(위규자 처리) ① 총장은 정보보안 위규자에 대해 [별표 4] '정보보안 위규자

처리 기준'에 따라 필요한 조치를 할 수 있다.

제4장 융합 보안

제68조(정보통신시설 보호 대책) ① 총장은 다음 각호의 어느 하나에 해당하는 정보통신시설 및 장소를 보호지역으로 지정·관리하여야 한다.

1. 암호실·정보통신실
2. 통합데이터센터
3. 암호자재 개발·설치·정비 장소
4. 국가 비상통신 등 중요통신망의 교환국, 회선집중국 또는 중계국
5. 보안관제센터, 백업센터, 중요 정보통신시설을 집중제어하는 국소
6. 그 밖에 보안관리가 필요하다고 인정되는 정보시스템 설치 장소

② 제1항에 따라 보호지역으로 지정된 정보통신시설 및 장소에 대한 보안 대책을 위하여 다음 각호에 해당하는 사항을 운영하여야 한다.

1. 방재 대책 및 외부로부터의 위해(危害) 방지 대책
2. 상시 이용하는 출입문은 한 곳으로 정하고 이중 잠금장치 설치
3. 출입자 식별·인증 등을 위한 출입문 보안장치 설치와 주·야간 감시 대책
4. 휴대용 저장매체를 보관할 수 있는 용기 비치
5. 정보시스템의 안전 지출 및 긴급파기 계획수립
6. 관리책임자와 자료·장비별 관리자 지정·운영
7. 정전에 대비한 비상 전원 공급 및 시스템의 안정적 중단 등 전력 관리 대책
8. 비상조명 장치 등 비상탈출 대책
9. 카메라 장착 휴대전화 등을 이용한 불법 촬영 방지 대책

제69조(정보통신시설 출입관리) ① 총장은 외부인이 정보통신시설을 방문하는 경우 반드시 신원을 확인하고 보안 교육 및 보안 검색 후 출입을 허용하여야 한다.

② 총장은 불가피한 경우를 제외하고는 정보통신시설에 대한 관람 및 견학은 지양하고 외국인의 출입은 금지한다. 다만, 외국인의 출입이 꼭 필요한 경우 정보보안 담당관과 사전 협의하여 출입을 허용할 수 있다.

제70조(영상정보처리기기 보안) ① 총장은 업무상 목적으로 불특정 사람 또는 사물을 촬영한 영상을 유·무선 정보통신망으로 전송·저장·분석하는 CCTV·IP카메라·이동형 영상 촬영 장비·중계 서버·관제 서버·관리용 PC 등의 기기·장비(이하 "영상정보 처리 기기" 이라 한다)를 설치·운용하고자 하는 경우 운영자

의 계정·비밀번호 설정 등 인증 대책을 수립하고 특정 IP주소에서만 접속 허용 등 비(非)인가자 접근통제 대책을 수립·시행하여야 한다.

② 영상정보처리기기를 통합·운용하는 시설(이하 "영상 관제상황실"이라 한다)을 운영하고자 하는 경우 영상 관제상황실을 제한구역 또는 통제구역으로 지정·관리하고 출입 통제장치를 운용하여야 한다.

③ 영상정보처리기기 관리자는 영상정보처리기기를 인터넷과 분리·운용하여야 한다. 다만, 부득이하게 인터넷과 연결·사용하여야 하는 경우 전송 내용을 암호화하여야 한다.

④ 영상정보처리기기 관리자는 제1항부터 제3항까지와 관련한 보안 대책의 적절성을 수시 점검·보완하여야 한다.

⑤ 기타 영상정보처리기기 보안과 관련한 사항은 국가정보원장이 배포한 「국가공공기관 영상정보 처리기기 도입·운영 가이드 라인」 및 「안전한 정보 통신 환경 구현을 위한 네트워크 구축 가이드라인」을 준수하여야 한다.

제71조(RFID 보안) ① 총장은 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 하는 경우 다음 각호의 사항을 포함한 보안 대책을 수립·시행하여야 한다.

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

② RFID 시스템 관리자는 제1항과 관련한 보안 대책의 적절성을 수시 점검·보완하여야 한다.

③ 기타 RFID 보안과 관련한 사항은 국가정보원장이 배포한 「RFID 보안관리 실무 매뉴얼」을 준수하여야 한다.

제72조(디지털 복합기 보안) ① 총장은 디지털 복합기(디지털복사기도 포함한다. 이하 "복합기"라 한 설치·운용하고자 하는 경우 복합기 내 저장매체가 있거나 장착이 가능한 경우 자료 유출을 방지하기 위하여 자료 완전 삭제 또는 디스크 암호화 기능이 탑재된 복합기를 도입하여야 한다.

② 복합기 관리자는 제1항에 따라 복합기를 설치·운용하는 경우 다음 각호의 사항을 포함한 보안 대책을 수립·시행하여야 한다.

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

③ 복합기 관리자는 다음 각호의 어느 하나에 해당하면 복합기의 저장매체에 저장된 자료를 완전히 삭제하여야 한다.

1. 복합기 사용 연한이 지나 폐기·양여할 경우
2. 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 복합기 관리자는 소모품 교체 등 복합기 유지보수를 하는 경우 저장매체의 무단 교체 등을 예방하여야 한다.

⑤ 복합기 관리자는 복합기를 통해 내부망과 기관 인터넷망 간 접점이 발생하지 않도록 보안 대책을 수립·시행하여야 한다.

⑥ 정보보안담당관은 소속된 기관의 저장매체가 장착된 복합기 운용과 관련한 보안 대책의 적절성을 수시 점검·보완하여야 한다.

⑦ 기타 복합기 보안과 관련한 사항은 국가정보원장이 배포한 「정보시스템 저장매체 불용 처리 지침」을 준수하여야 한다.

제73조(재난 방지 대책) ① 총장은 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애 발생에 대비하여 정보시스템의 이중화, 백업 관리 및 복구 등 종합적인 재난 방지 대책을 수립·시행하여야 한다.

② 총장은 재난 방지 대책을 정기적으로 시험·검토하고 재난으로 인해 업무에 지장이 초래될 가능성에 대한 점검을 시행하여야 한다.

③ 총장은 정보통신망의 장애 발생에 대비하여 정보시스템 백업 시설을 확보하고 정기적으로 백업을 시행하여야 한다.

④ 총장은 제3항에 따른 백업 시설을 구축·운영하고자 하는 경우 정보통신실·통합데이터센터와 물리적으로 일정 거리 이상 떨어진 안전한 장소에 설치하여야 하며 전력 공급원 이중화 등 정보시스템의 가용성을 최대화할 수 있도록 하여야 한다.

⑤ 총장은 백업 및 복구 등 종합적인 재난 방지 대책을 매년 정보보안업무추진계

획에 반영하여 수립할 수 있다.

제5장 훈련 및 평가

제74조(사이버 공격 대응훈련) ① 총장은 사이버안보 업무규정 제11조에 따른 대응훈련 및 시정조치가 원활히 이루어질 수 있도록 지도·감독하여야 한다.

제75조(정보통신망 보안 진단) ① 총장은「사이버안보 업무규정」제12조 제1항에 따른 진단·점검 또는 그 밖의 법규에 따라 정보통신망 보안 진단·점검을 실시하는 경우, 교육부장관 및 국가정보원장이 배포하는 다음 각호의 가이드라인 등을 참고하여야 하며, 이에 필요한 관련 예산 확보 등을 위하여 노력하여야 한다.

1. 사이버 보안 강화를 위한 길라잡이(정보통신시스템 보안 진단 및 대응 방법)
2. 홈페이지·네트워크·시스템·DBMS 취약점 점검 매뉴얼
3. 정보보안 점검 체크리스트

제76조(정보보안 수준 진단) ① 총장은 매년 교육부 장관이 배포한 진단 지표에 따라 자체 정보보안 수준 진단을 시행하여야 한다.

② 정보보안 수준 진단 시 자체 진단의 적절성을 입증하는 데 필요하다고 판단하는 경우 진단 지표별 증빙 자료를 교육부 장관에게 제출할 수 있다.

③ 총장은 정보보안 수준 진단 결과에 따른 미비점을 개선·보완하여 정보보안 수준을 제고하여야 한다.

제6장 사이버 위협 탐지 및 대응

제1절 보안관제

제77조(보안관제센터 설치·운영) ① 총장은 소관 정보통신망에 대한 사이버 공격정보를 수집·분석·대응할 수 있는 단위 보안관제센터를 설치·운영하여야 한다. 다만, 단위 보안관제센터를 설치·운영하기 어려운 경우 교육부 보안관제센터에 관련 업무를 위탁할 수 있다.

② 단위 보안관제센터를 설치·운영하는 경우 해당 보안관제센터를 교육부 보안관제센터와 연계 운영하여야 한다.

제78조(보안관제 인원) ① 총장은 보안관제 업무를 24시간 중단 없이 수행하여야 하며 이를 담당할 전문 또는 전담 인력을 배치하고 교대근무 체계를 운영하여야

한다. 다만, 단위 보안관제센터의 경우 보안관제 대상 기관의 범위 및 중요성, 보안관제센터의 규모 등을 고려하여 그러하지 아니할 수 있다.

② 「국가 사이버 안전관리 규정」 제10조의2 제4항에 따라 보안관제전문업체의 인원을 활용하고자 하는 총장은 다음 각호에 해당하는 사항을 준수하여야 한다.

1. 업체를 선정하는 경우 과학기술정보통신부 장관이 고시하는 「보안관제 전문기업 지정 등에 관한 공고」에 따른 업무수행 능력 평가 기준 등 준수
2. 보안관제 업무의 책임 있는 수행 및 보안관리 등을 위하여 적정한 수의 정규직원 배치
3. 업체 인원에 대하여 제26조(용역업체 보안) 및 제30조(누출금지 정보 유출 시 조치) 준용
4. 업체 인원을 대상으로 매월 1회 이상 탐지규칙 정보 관리 등에 관한 보안 교육 및 점검실시

제79조(초동 조치) ① 총장은 사이버 공격으로 인한 피해 최소화 및 확산 방지를 위하여 다음 각호의 사항을 포함한 조치를 하여야 한다.

1. 사이버 공격 경유지(사이버 공격에 악용되거나 악용될 우려가 있는 웹 사이트 주소, IP주소, 전자우편 주소를 말한다) 및 공격 IP주소 차단
2. 피해 시스템을 정보통신망으로부터 분리하거나 악성프로그램의 동작을 정지시키는 조치
3. 사고조사를 위한 피해 시스템 및 로그기록의 보전

② 총장은 사이버 공격으로 인한 피해를 최소화하는 데 필요한 경우 피해 시스템과 사용자에 관한 정보를 상급 기관에 제공할 수 있다.

제80조(조치 결과 통보) 총장은 상급 기관으로부터 사이버 공격에 관한 정보를 제공받은 후 5일 이내에 대응조치 결과를 해당 상급 기관에 통보하여야 한다.

제2절 사고 대응

제81조(사이버 공격으로 인한 사고) ① 총장은 사이버 공격으로 인한 사고의 원인 분석 및 재발 방지를 위하여 상급 기관이 다음 각호에 해당하는 자료를 요청하는 경우 관계 법규에 저촉되지 않는 범위 내에서 해당 자료를 제출하여야 한다. 사이버 공격으로 인하여 「보안업무규정」 제38조 및 제45조, 「보안업무규정 시행규칙」 제65조 2에 따라 조사를 하는 경우도 같다.

1. 공격 주체와 피해자를 식별하기 위한 IP주소 및 MAC 주소, 전자우편 주소, 정

보 통신서비스 이용자 계정정보, 피해자의 성명 및 연락처

2. 사이버 공격에 사용된 악성프로그램 및 공격 과정에서 생성·변경 또는 복제된 디지털정보

3. 공격 주체가 절취한 디지털정보

4. 공격 주체의 행위가 기록된 내용 또는 로그기록

② 본교에서 사고 발생 시 사고 관련 모든 구성원은 사고 원인을 규명할 때까지 피해 시스템에 대한 증거를 보전하고 임의로 관련 자료를 위조하거나 삭제·포맷하여서는 안 된다. 또한 정보보안담당관은 사고 원인 규명 후에라도 피해 시스템에 대한 증거를 별도 보관할 수 있다.

③ 본교에서 이용하는 공공 전용(專用) 민간 클라우드에서 사고가 발생하는 경우 정보보안담당관과 합동으로 조사반을 구성하여(이 경우 상급 기관 또는 조사기관의 장에 협조를 요청할 수 있다.) 클라우드 컴퓨팅 서비스제공자에 대하여 계약의 범위 내에서 자료의 보전 및 제출 요구, 현장 조사 등 필요한 조처를 하여야 한다.

④ 분임정보보안담당관은 소관 부서 또는 단체에 정보보안 사고가 발생하는 경우 즉시 피해를 최소화하도록 조치 및 보안 관련 부서에 지원을 요청하고, 그 결과를 정보보안담당관에 보고하여 총장에게 최종 보고할 수 있도록 한다. 이때 보고하여야 할 내용은 다음 각호와 같다.

1. 사고 일시 및 장소

2. 사고 원인, 피해 현황, 피해 디지털정보 등 개요

3. 사고자, 관계자의 인적 사항, 피해 계정정보, IP, 단말기 정보, 전자우편 주소 등

4. 사고 조치, 재발 방지 내용

제82조(정보통신 보안 규정 위반 및 자료 유출 사고) ① 총장은 국가정보원장으로부터 「보안업무규정 시행규칙」[별표 2]에 따른 정보통신 보안 규정 위반 사항에 대한 사실을 통보받은 때에는 동규정 시행규칙 제66조 제3항에 따라 즉시 필요한 조처를 하고 위규자 및 위규 내용과 조치 결과를 교육부 장관을 통하여 국가정보원장에게 통보하여야 한다.

② 총장은 비밀·대외비 등 국가 기밀에 속하는 업무자료가 유출되거나 비공개 업무자료가 유출된 사고 중 국가정보원법 제4조 제1항 제1호와 관련된 사안일 경우 즉시 교육부 장관을 통하여 국가정보원장에게 통보하여 합동 조사를 시행하여야 한다.

③ 본교 구성원 등의 과실로 인하여 제2항에 따른 유출 사고가 발생하는 경우 상급 기관 또는 조사기관의 장은 총장을 통해 해당 구성원 등에게 저장자료·이용 내용 등의 자료 제출을 요청할 수 있다.

④ 본교 구성원 등은 제3항에 따른 요청이 위법하다고 판단되는 경우 그 사유를 소명하고 자료 제출을 거부할 수 있다.

제83조(재발 방지 조치) ① 상급 기관 또는 조사기관의 장은 사고조사에 따른 조사 결과 및 재발 방지를 위한 보안 조치 사항을 총장에게 통보할 수 있다.

② 제1항에 따라 조사 결과를 통보받은 총장은 관계 법규에 따른 관련자 징계, 개선 대책 수립·시행 등 필요한 조치를 하여야 한다.

제7장 보 칙

제84조(다른 법령과의 관계) 이 지침에 명시되지 않은 사항은 국가 「국가 보안업무규정」, 「국가 사이버 안전관리 규정」, 「교육부 정보보안 기본지침」, 「상지대학교 정보보안에 관한 규정」 및 그 밖의 관계 법규에 따른다.

부 칙

제1조(시행일) 이 지침은 공포한 날부터 시행한다.

별 표

[별표 1] ‘안전성 검증필 제품 목록’ 등재 기본요건

[별표 2] ‘암호가 주기능인 제품’ 도입 요건

[별표 3] 보안적합성 검증신청 시 제출물

[별표 4] 상지대학교 정보보안 위규자 처리 기준

[별표 5] 사업수행자 보안 위규 처리 기준

[별표 6] 누출금지 대상 정보의 범위

[별표 7] 자산 분류 기준

[별표 8] 정보시스템 저장매체 자료별 삭제 방법

[별표 9] 클라우드 서비스 이용 ‘시스템 중요도’ 등급 분류 기준

서 식

[서식 제1호] 정보시스템 관리 대장

[서식 제2호] 보안적합성 검증 신청서

[서식 제3호] 보안 관제센터 운영 현황

[서식 제4호] 보안 서약서 및 확약서

[서식 제5호] 정보화 사업 보안 점검 체크리스트

별 표

【 별표 1 】

‘안전성 검증필 제품 목록’ 기본요건

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</th><th>성능평가</th><th>보안기능
확인서</th><th>보안적합성
검증</th></tr>
<tr><td>스마트카드</td><td rowspan="23">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="22">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>○</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(Layer3)</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>

【 별표 2 】

‘암호가 주기능인 제품’ 도입 요건

제품 유형	도입 요건	비 고
메일 암호화 제품	검증필 암호모듈 탑재	
구간 암호화 제품		
하드웨어 보안 토큰		
디스크·파일 암호화 제품		
기타 암호화 제품		
SSO 제품	검증필 암호모듈 탑재 및 CC인증(국가용 보호프로파일 준수)	
DB 암호화 제품		
문서 암호화 제품(DRM 등)		

※ 최신 도입 요건은 국가정보원 홈페이지(암호모듈 검증) 참조

【 별표 3 】

보안적합성 검증 신청 시 제출물

1. 최초 검증 신청 시 제출물

제출물	정보 보호시스템		작성 주체
	상용 제품	자체(용역) 개발	
[서식 제2호]에 따른 보안적합성 검증 신청서	○	○	신청기관
정보통신제품 도입확인서(현황)	○	○	
기술 제안요청서 사본	○	○	
보안 기능 점검표	○	○	
운용 점검 사항	○	○	
CC 인증서 사본	○ (인증서 보유시)		업체
보안 기능 운용 설명서	○	○	
기본 및 상세 설계서		○	
개발 완료 보고서		○	

2. 재검증 신청 시 제출물

제출물	정보 보호시스템		작성 주체
	상용 제품	자체(용역) 개발	
[서식 제2호]에 따른 보안적합성 검증 신청서	○	○	신청기관
정보통신제품 도입확인서(현황)	○	○	
보안 기능 점검표	○	○	
운용 점검 사항	○	○	
변경 내용 분석서	○	○	업체

【 별표 4 】

상지대학교 정보보안 위규자 처리 기준

위규의 정도 및 과실 여부 / 위규의 유형	법률을 위반하고, 위규의 정도가 심하고 고의가 있는 경우	법률을 위반하고 위규의 정도가 심하고 중과실이거나, 위규의 정도가 약하고 고의가 있는 경우	규정 및 지침을 위반하고, 위규의 정도가 심하고 경과실이거나, 위규의 정도가 약하고 중과실인 경우	규정 및 지침을 위반하고, 위규의 정도가 약하고 경과실인 경우	위규의 정도가 약하고 경과실인 경우
1. 전자정보(전자문서 및 전자기록물) 관리 위반					
가. 주전산기(주요 서버 등)· 대용량 전자기록(DB) 손괴	중징계	중징계~경징계	경징계~경고	경고~주의	주의~시정
나. 전자정보의 위조·변조·훼손 및 유출	중징계	중징계~경징계	경징계~경고	경고~주의	주의~시정
2. 정보시스템 관리 위반					
가. 정보통신망에 대한 해킹· 악성코드의 유포	중징계	중징계~경징계	경징계~경고	경고~주의	주의~시정
나. 정보시스템 및 정보통신실 파괴	중징계	중징계~경징계	경징계~경고	경고~주의	주의~시정
다. 고의적인 중요 정보시스템 기능 장애 및 정지	중징계	중징계~경징계	경징계~경고	경고~주의	주의~시정
3. 중요 자료관리 위반					
가. 비밀이 저장된 PC, 휴대용 저장매체 등 분실	중징계	중징계~경징계	경징계~경고	경고~주의	주의~시정
나. 상용메일 등을 통한 비밀 등 중요자료 무단 소통	중징계	중징계~경징계	경징계~경고	경고~주의	주의~시정
다. 정보통신기기를 통한 비밀 등 중요자료 무단 소통	중징계	중징계~경징계	경징계~경고	경고~주의	주의~시정
4. 기타					
가. 관련 법률에 의거 대상이 되는 모든 정보보안 사고	중징계	경징계	경고	주의	시정
나. 상지대학교 정보보안 기본지침 위반	중징계	경징계	경고	주의	시정

【 별표 5 】

사업수행자 보안 위규 처리 기준

구 분	위 규 사 항	처 리 기 준
심 각	1. 비밀 및 대외비급 정보 유출 및 유출 시도 가. 정보시스템에 대한 구조, 데이터베이스 등의 정보 유출 나. 개인 정보·신상정보 목록 유출 다. 비공개 항공사진·공간정보 등 비공개 정보 유출 2. 정보시스템에 대한 불법적 행위 가. 관련 시스템에 대한 해킹 및 해킹 시도 나. 시스템구축 결과물에 대한 외부 유출 다. 시스템 내 인위적인 악성코드 유포	○ 사업 참여 제한 ○ 위규자 및 직속 감독자 등 중징계 ○ 재발 방지를 위한 조치계획 제출 ○ 위규자 대상 특별 보안교육 실시
중 대	1. 비공개 정보 관리 소홀 가. 비공개 정보를 책상 위 등에 방치 나. 비공개 정보를 휴지통 · 폐지함 등에 유기 또는 이면지 활용 다. 개인 정보·신상정보 목록을 책상 위 등에 방치 라. 기타 비공개 정보에 대한 관리 소홀 2. 사무실 · 보호구역 보안관리 허술 가. 통제구역 출입문을 개방한 채 퇴근 등 나. 인가되지 않은 작업자의 내부 시스템 접근 다. 통제구역 내 장비·시설 등 무단 사진 촬영 3. 전산 정보보호 대책 부실 가. 업무망 인터넷망 혼용사용, 보안 USB 사용 규정 위반 나. 웹하드·P2P 등 인터넷 자료공유사이트를 활용하여 용역사업 관련 자료 수발신 다. 개발·유지보수 시 원격작업 사용 라. 저장된 비공개 정보 패스워드 미 부여 마. 인터넷망 연결 PC 하드디스크에 비공개 정보를 저장 바. 외부용 PC를 업무망에 무단 연결사용 사. 보안 관련 프로그램 강제 삭제 아. 사용자 계정관리 미흡 및 오남용(시스템 불법 접근 시도 등)	○ 위규자 및 직속감독자 등 중징계 ○ 재발 방지를 위한 조치계획 제출 ○ 위규자 대상 특별 보안교육 실시

구 분	위 규 사 항	처 리 기 준
보 통	1. 기관 제공 중요정책 · 민감 자료 관리 소홀 가. 주요 현안 · 보고자료를 책상 위 등에 방치 나. 정책 · 현안 자료를 휴지통 · 폐지함 등에 유기 또는 이면지 활용 2. 사무실 보안관리 부실 가. 캐비닛 · 서류함 · 책상 등을 개방한 채 퇴근 나. 출입 키를 책상 위 등에 방치 3. 보호구역 관리 소홀 가. 통제 · 제한구역 출입문을 개방한 채 근무 나. 보호구역 내 비인가자 출입 허용 등 통제 미 실시 4. 전산 정보보호 대책 부실 가. 휴대용 저장매체를 서랍 · 책상 위 등에 방치한 채 퇴근 나. 네이트온 등 비인가 메신저 무단 사용 다. PC를 켠 상태나 휴대용 저장매체(CD, USB 등)를 꽂아 놓고 퇴근 라. 부팅 · 화면보호 패스워드 미 부여 또는 “1111“ 등 단순 숫자 부여 마. PC 비밀번호를 모니터 옆 등 외부에 노출 바. 비인가 휴대용 저장매체 무단 사용	○ 위규자 및 직속 감독자 등 경징계 ○ 위규자 및 직속 감독자 사유서 / 경위서 징구 ○ 위규자 대상 특별 보안교육 실시
경 미	1. 업무 관련 서류 관리 소홀 가. 진행 중인 업무자료를 책상 등에 방치, 퇴근 나. 복사기 · 인쇄기 위에 서류 방치 2. 근무자 근무 상태 불량 가. 각종 보안장비 운용 미숙 나. 경보 · 보안장치 작동 불량 3. 전산 정보보호 대책 부실 가. PC 내 보안성이 검증되지 않은 프로그램 사용 나. 보안 관련 소프트웨어의 주기적 점검 위반	○ 위규자 서면 · 구두 경고 등 문책 ○ 위규자 사유서 / 경위서 징구

보안 위약금 부과 기준

1. 위규 수준별로 A ~ D 등급으로 차등 부과

구분	위규 수준			
	A급	B급	C급	D급
위규	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금 비중	부정당 업자 등록	500만원 이하	300만원 이하	100만원 이하

* 위약금은 매 점검 또는 보안 사고 적발, 보안 사고 발생 별로 부과

2. 보안 위약금은 다른 요인에 의해 상쇄, 삭감이 되지 않도록 부과

* 보안 사고는 1회의 사고만으로도 그 파급력이 큰 것을 감안하여 타 항목과 별도 부과

3. 사업 종료 시 지출 금액 조정을 통해 위약금 정산

【 별표 6 】

누출금지 대상 정보의 범위

① 기관 소유 정보시스템의 내·외부 IP주소 현황

② 세부 정보시스템 구성 현황 및 정보통신망 구성도

③ 사용자 계정 및 패스워드 등 정보시스템 접근권한 정보

④ 정보통신망 취약점 분석·평가 결과물

⑤ 용역사업 결과물 및 프로그램 소스 코드

⑥ 국가용 보안시스템 및 정보 보호시스템 도입 현황

⑦ 침입 차단·방지시스템(IPS) 등 정보보호 제품 및 라우터·스위치 등 네트워크 장비 설정 정보

⑧ '공공기관의 정보공개에 관한 법률' 제9조 1항에 따라 비공개 대상 정보로 분류된 기관의 내부 문서

⑨ '개인정보 보호법' 제2조 1호의 개인 정보

⑩ '보안업무규정' 제4조의 비밀, 同 시행규칙 제7조 3항의 대외비

⑪ 그 밖의 발주자가 공개가 불가하다고 판단한 자료

※ 사업 중 위 누출금지 대상 정보와 관련된 참여 인원의 교체 시에는 반드시 사업담당자(발주기관)의 사전 허가를 득한 후 시행해야 함. ※

【 별표 7 】

자산 분류 기준

구분		내용	소분류
정보 시스템	서버	대학 업무 및 교육을 운영하기 위한 서버 컴퓨터 장치	블레이드(물리)서버, 가상화(논리)서버, 스토리지 서버 등
	네트워크 장비	교내 네트워크와 관련된 장비로 라우터, L2/L3/L4스위치, 무선AP, IP관리, 트래픽 관리 등을 포함	라우터, L2/L3/ㅣ4스위치, 무선AP, IPM, NMS, QoS 등
	소프트웨어	자체 개발된 대학 업무용 소프트웨어, 서버에 설치된 라이선스 프로그램, 상용 소프트웨어(OS, 오피스, 개발툴, 운영툴 등), 유틸리티 프로그램, 교육용 프로그램, 기타 각종 소프트웨어	학사행정시스템, 전자결재시스템, 웹 관련 소프트웨어, 웹메일, SMS, SSO, 2차인증, 업무 및 개발 관련 소프트웨어 등
	PC(단말기)	업무 및 교육용으로 사용하는 전산 단말기로 사무용 PC, 노트북, 태블릿 등	PC, 노트북, 태블릿 등
	정보통신기기	업무 및 교육용 통신장비, 교내외 통신용 장비 등	교환기, 인터넷전화, 이동통신 장비 등
	저장매체	정보시스템 운영에 사용되는 저장매체	보안 USB, 외장하드 등
정보보호 시스템	서버 보안	서버접근 통제, 서버 보안, 암호화	시큐어OS, 접근제어시스템, DB 암호화 등
	네트워크 보안	네트워크 접근통제, 침입탐지·차단, 외부 취약점공격차단, 무선사용자인증	방화벽, IPS, DDoS, 웹방화벽, TMS, 무선인증, 관제시스템, 스팸 차단, 유해사이트 차단 등
	PC 보안	정보 유출 방지, PC 사용자보안, 바이러스/웜/악성코드 차단	백신, DLP, DRM, 내PC지키미 등
정보	문서 정보	정보보호 관련 정의 문서, 정보보호 관련 보고서, 정보보호 운영 증빙자료, 정보시스템 현황	정보보호규정/지침, 정보보호 관련 매뉴얼, 취약점 보고서, 시스템 현황 및 구성도, 계약서, 각종 대장 등
	전자적 정보	DB 및 전자정보 등 대학 업무 운영에 필요한 정보	학사/학적정보, 인사정보, 회계정보, 도서/대출 정보, 개인정보 등
부대설비		전산 장비실, 정보통신실, 관제실 사무실 등 물리적 공간의 각종 부대시설 정보	출입관리, CCTV, 항온항습기, 가습기, UPS, 발전기, 소화기 등

자산 보안 등급 기준

※ 정보자산 보안 요구사항

유형	내용	점수	평가 기준
기밀성	정보자산의 접근은 인가된 인원만 가능함을 보장해야 하는 기준	상(3)	특정 부서 또는 담당자만 접근이 가능한 자산이며, 유출 시 막대한 금전적 손실이 발생하는 경우
		중(2)	내부에만 공개되는 자산이며, 외부로 유출 시 상당한 금전적 손실이 발생하는 경우
		하(1)	외부로 접근이 가능한 정보를 담고있는 자산이며, 공개돼도 관계없거나 손실이 미비한 경우
무결성	정보자산 내 정보의 정확성, 안정성을 보장해야 하는 기준	상(3)	자산이 변조되는 경우, 업무수행에 막대한 장애를 유발하거나 중대한 금전적 손실을 입히는 경우
		중(2)	자산이 변조되는 경우, 업무수행에 부분적 장애를 유발하거나 상당한 금전적 손실을 입히는 경우
		하(1)	자산이 변조돼도 업무수행에 미치는 영향이 미비한 경우
가용성	인가된 인원이 필요시 정보자산에 접근하는 것을 보장해야 하는 기준	상(3)	자산이 사용 불가능할 때, 장기적인 업무 중단이 발생하여 막대한 금전적 손실을 입히는 경우
		중(2)	자산이 사용 불가능할 때, 단기적인 업무 중단이 발생하여 상당한 금전적 손실을 입히는 경우
		하(1)	자산이 사용 불가능할 때, 업무 중단에 직접적인 영향을 미치지 않는 경우

※ 자산 보안등급 평가 기준= “정보자산 보안 요구사항”의 기밀성+무결성+가용성

※ 평가한 등급을 [서식 제1호] “정보시스템 관리대장”의 ‹자산 보안등급›에 표기

자산 보안 등급	“정보자산 보안 요구사항” 평가 점수 합계
1등급(매우 높음)	9
2등급(높음)	8-7
3등급(중간)	6
4등급(낮음)	4-5
5등급(매우 낮음)	3

【 별표 8 】

정보시스템 저장매체 자료별 삭제 방법

㉮ : 완전 파괴(소각 / 파쇄 / 천공 / 용해)

* 비밀이 저장된 플로피 디스켓, 광디스크 파쇄 시에는 파쇄 조각의 크기가 0.25mm 이하가 되도록 조치

㉯ : 전용 소자 장비 이용 저장자료 삭제

* 소자 장비는 반드시 저장매체의 자기력보다 큰 자기력 보유

㉰ : 완전 삭제 장비 및 완전 삭제 소프트웨어 이용 저장자료 삭제

* 저장매체 전체를 “난수, 0, 1”로 각각 중복저장 하는 방식으로 삭제

㉱ : 완전 포맷 1회 수행

* 저장매체 전체를 난수로 중복저장 하는 방식으로 삭제

<table>
<tr><th>저장자료
저장매체</th><th>공개자료</th><th>민감 자료
(개인정보 등)</th><th>비밀자료
(대외비 포함)</th></tr>
<tr><td>플로피디스크</td><td>㉮</td><td>㉮</td><td>㉮</td></tr>
<tr><td>광디스크
(CD / DVD 등)</td><td>㉮</td><td>㉮</td><td>㉮</td></tr>
<tr><td>자기 테이프</td><td>㉮/㉯ 택일</td><td>㉮/㉯ 택일</td><td>㉮</td></tr>
<tr><td rowspan="2">반도체 메모리
(EEPROM 등)</td><td>㉮/㉰ 택일</td><td>㉮/㉰ 택일</td><td>㉮/㉰ 택일</td></tr>
<tr><td colspan="3">완전 포맷(완전 삭제)이 되지 않는 저장매체는 ㉮ 방법 사용</td></tr>
<tr><td>하드디스크</td><td>㉱</td><td>㉮/㉯/㉰ 택일</td><td>㉮/㉯/㉰ 택일</td></tr>
<tr><td>휴대용 저장매체
(USB 등)</td><td>㉱</td><td>㉮/㉯/㉰ 택일</td><td>㉮/㉯/㉰ 택일</td></tr>
</table>

【 별표 9 】

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 내부 업무의 경우 '시스템 중요도'를 고려하여 등급 조정 가능

※ 위 분류 기준에 따른 분류 절차 및 체크리스트 등 세부 사항은 '국가 클라우드 서비스 보안가이드라인'을 참고한다.

※ 이용 기관은 민간 클라우드 서비스 도입 시 시스템 등급을 자체 분류하고, 국정원은 '보안성 검토' 시 분류의 적정성을 재검토한다.

서 식

【 서식 제1호 】

정보시스템 관리대장

연번	소속	취급자 성명	종류 (서버·PC 등)	제조사	모델명	관리번호	도입일자	관리자 확인(인)	자산 보안 등급

【 서식 제2호 】

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	
	휴대폰 번호		이메일	

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

【 서식 제3호 】

보안관제센터 운영현황

보안관제센터 개요				
개소		* 개소일자	위치	
규모		* 상황실 면적 등	예산	* 구축예산 및 운영예산
조직 현황				
개요		* 조직구성, 인원 및 임무, 근무형태 등		
1	부서		센터장	
	직급		성명	
	이메일		연락처	전화: HP:
2	부서		직급/직책	
	담당분야		성명	
	이메일		연락처	전화: HP:
3	:	* 센터장과 탐지・분석・대응 등 분야별 대표자만 기입		
외부인력 현황				
업체명			대표이사	
인원수			근무형태	
계약기간			수행업무	
지침・매뉴얼 현황				
지침			기준	
매뉴얼			기타	
보안관제시스템 현황				
시스템명		* 주요 기능	시스템명	
시스템명			시스템명	
시스템명			시스템명	

<table>
<tr><th colspan="4">보안장비 현황</th></tr>
<tr><td>F/W</td><td>* 제품명 및 사용대수</td><td>IDS/IPS</td><td></td></tr>
<tr><td>ESM</td><td></td><td>WEB F/W</td><td></td></tr>
<tr><td>라우터</td><td></td><td>그 밖의 장비</td><td>예) NMS 1대
* 네트워크 구성도 사본 제출</td></tr>
<tr><th colspan="4">보안관제 연동기관 현황</th></tr>
<tr><td colspan="4">* 대상기관 수, 기관명, 대상목표(인터넷 또는 내부망, 홈페이지 등)</td></tr>
<tr><th colspan="6">연동기관 IP할당 현황</th></tr>
<tr><td rowspan="3">1</td><td>연동기관</td><td></td><td rowspan="3">IP
관리자</td><td>성 명</td><td></td></tr>
<tr><td>공인IP</td><td></td><td>연락처</td><td>전화: HP:</td></tr>
<tr><td>사설IP</td><td></td><td>이메일</td><td></td></tr>
<tr><td>2</td><td></td><td colspan="4"></td></tr>
<tr><td>3</td><td></td><td colspan="4"></td></tr>
<tr><td>4</td><td></td><td colspan="4"></td></tr>
<tr><td>5</td><td></td><td colspan="4"></td></tr>
<tr><td>6</td><td></td><td colspan="4"></td></tr>
<tr><th colspan="6">국가사이버안전센터 탐지규칙 재배포 현황</th></tr>
<tr><th>기관명</th><th>배포방법</th><th>기관명</th><th>배포방법</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

【 서식 제4호 】

보 안 서 약 서

본인은 ____년 ____월 ____일 부로 _____관련 용역사업(업무)을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 _____ 관련 업무 중 알게 될 일체의 내용이 직무상 기밀 사항임을 인정한다.

2. 본인은 이 기밀을 누설함이 대학의 안전보장 및 이익에 위해가 될 수 있음을 인식하여 업무 수행 중 취득한 제반 기밀 사항을 일체 누설하거나 공개하지 아니한다.

3. 본인이 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다.

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

년 월 일

서 약 자	업 체 명 :		(직인)
	직 위 :	대표이사	
	성 명 :		(서명)
서약집행자 (담당자)	소 속 :		
	직 위 :		
	성 명 :		(서명)

보 안 서 약 서

본인은 ____년____월____일 부로 _____관련 용역사업(업무)을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 전산망도·IP현황, 개인정보 등 상지대학교에서 제공하는 비공개자료 및 사업 수행 중 취득한 자료는 외부로 절대 유출하지 아니한다.
2. 용역사업 관련 자료 및 사업수행 과정에서 생산된 모든 산출물은 동 사업의 감독관이 지정한 PC에 저장·관리한다.
3. 용역사업 관련 자료는 인터넷 웹하드 등 인터넷 자료공유사이트 및 개인 메일함에 저장을 금지하고, 전자우편을 이용해 자료전송이 필요한 경우에는 상지대학교에서 제공하는 전자우편을 이용하여야 한다.
4. 용역사업 수행으로 생산되는 산출물 및 기록은 감독관이 인가하지 않은 비인가자에게 제공·대여·열람을 금지한다.
5. 교내에서 용역사업을 수행하는 경우 휴대용 매체(노트북, USB 등)를 반입 시에는 악성코드 감염 여부를 확인하고, 반출 시에는 반드시 감독관에게 자료의 무단 반출이 없음을 확인받아야 한다.
6. 상지대학교의 내부망에 접속하여 용역사업 수행 시, P2P 및 자료공유사이트 등 악성코드 감염 가능성 있는 유해사이트는 접속하지 않는다.
7. 위 사항을 위반하였을 경우 관계 법률에 의해 처벌을 받게 된다는 사실을 충분히 인식하고, 민·형사상 처벌을 받을 것을 서약한다.

년 월 일

서 약 자 업 체 명 :

직 위 :

성 명 : (서명)

서약집행자 소 속 :

(담당자) 직 위 :

성 명 : (서명)

보 안 확 약 서

본인은 년 월 일부터 년 월 일 까지 _____관련 용역사업(업무)을 완료 함에 있어 관련한 제반 자료, 장비, 서류, 중간·최종 산출물 등 위탁·용역과 관련된 모든 자료 등에 대하여 다음 사항을 준수할 것을 엄숙히 확약합니다.

1. 사업 완료 후 작업PC 및 휴대형 저장매체 등에 저장된 모든 자료는 국가정보원 '보안 관리 표준'에 따라 완전히 삭제 또는 파기 후 반출한다.
2. 수요기관에서 제공받은 장비 및 서류와 중간·최종 산출물 등 용역과 관련된 제반 자료(문서, 전자파일 등)는 전량 반납하고, 사업산출물 복사본 등을 별도 보관하지 않는다.
3. 최종 산출물 중 대외보안이 요구되는 자료는 대외비로 작성·관리하고 불필요한 자료는 삭제 또는 파기한다.
4. 본 사업을 통하여 취득한 모든 정보(개인정보 포함)는 수요기관의 동의 없이 외부에 누설하지 않으며, 정보 누설로 인한 문제 발생 시에는 관련 계약·법령에 따른 처벌을 감수하여 일체의 손해를 배상한다.
5. 본인은 사업에 참여한 협력사 및 하도급업체에 대해 상기 항목 준수 여부를 점검하고, 상기 항목 위반으로 인해 발생한 보안사고에 대하여 모든 책임을 부담한다.

20 년 월 일

서 약 자	업 체 명 :		(직인)
	직 위 :	대표이사	
	성 명 :		(서명)
서약집행자 (담당자)	소 속 :		
	직 위 :		
	성 명 :		(서명)

【 서식 제5호 】

정보화사업 보안 점검 체크리스트

□ 용역업체 보안

구분	점 검 내 용	반영 여부 (반영, 미반영, 향후 반영, 미적용 대상)
1	○ 참가 직원에 대한 보안교육 및 보안서약서 징구	
2	○ 정보화사업 제안요청서(시방서)에 보안요구사항 명시 (용역업체 작업 장소에 대한 보안요구사항 및 누출금지 대상정보 등)	
3	○ 계약서에 참가 직원의 보안준수사항과 위반 시 손해배상 책임 등 보안관련 특약조항 명시	
4	○ 용역사업 수행 관련 보안교육·점검 및 용역기간 중 참여인력 임의 교체 금지	
5	○ 정보통신망도·IP 현황 등 용역업체에 제공할 자료는 자료 인계인수대장을 비치, 보안조치 후 인계·인수하고 무단 복사 및 외부반출 금지	
6	○ 사업 종료시 외부업체의 노트북·휴대용 저장매체 등을 통해 비공개 자료가 유출되는 것을 방지하기 위하여 복구가 불가능하도록 완전 삭제	
7	○ 용역업체로부터 용역 결과물을 전량 회수하고 비인가자에게 제공·열람 금지	
8	○ 용역업체의 노트북 등 관련 장비를 반출·반입시마다 악성코드 감염여부, 자료 무단반출 여부 확인	
9	○ 비밀 및 중요외주 용역사업을 수행할 경우에는 외부인력에 대한 신원조사·비밀취급인가, 보안교육 및 외부유출 방지 등 보안조치 강구	
추가 보안 사항		

※ 용역업체 보안성 검토 사항은 모든 정보시스템 구축 및 용역사업에 적용

□ 소프트웨어 개발보안

구분	점 검 내 용	반영 여부 (반영, 미반영, 향후 반영, 미적용 대상)
1	○ 독립된 개발시설 확보 및 비인가자의 접근통제 여부	
2	○ 개발시스템과 운영시스템의 물리적 분리	
3	○ 소스 코드 관리 및 소프트웨어 보안관리 대책	
4	○ 서버 관리자는 개발 완료 후 시험하기 위해 사용된 도구(컴파일러 등) 삭제	
5	○ 외부인력 대상 신원확인, 보안서약서 징구, 보안 교육 및 점검	
6	○ 외부인력의 보안 준수 확인 및 위반 시 배상책임의 계약서 명시	
7	○ 외부인력의 정보시스템 접근권한 및 제공자료 보안 대책	
8	○ 외부인력에 의한 장비 반입·반출 및 자료 무단 반출에 대한 보안 대책	
9	○ 용역업체 보안성 검토 사항 반영 여부	
추가 보안 사항		

□ 홈페이지 구축 보안

구분	점 검 내 용	반영 여부 (반영, 미반영, 향후 반영, 미적용 대상)
1	○ 웹서버 및 웹 어플리케이션 외부 오픈 전 불필요한 서비스 제거 및 보안 설정 사전 확인	
2	○ '웹서버 보안취약점 대응 가이드'를 참고, 취약점 제거	
3	○ 웹사이트 내 모든 유형의 웹페이지 컨텐츠에 대해 개인정보 노출 점검 및 차단 기능 적용	
4	○ 사용자 접근권한은 업무에 따라 차등 설정·관리	
5	○ DBMS에 개인정보 암호화(주민등록번호, 핸드폰번호 등) 적용	
6	○ 개인정보 및 인증정보(로그인 등) 입력 시 이용자 단말기에 개인정보 유출 방지 대책(보안서버, 키로깅, 2차인증, 화면 캡쳐 방지 등) 마련	
7	○ 비인가자의 서버 저장자료 절치, 위·변조 및 분산서비스거부(DDoS) 공격 등에 대비하기 위하여 국가정보원장이 안전성을 검증한 침입차단·탐지시스템 및 DDoS 대응 시스템 설치 등 보안 대책 강구	
8	○ 관리자 기능은 내부망의 지정된 시스템에서만 접근	
9	○ 외부에 공개될 목적으로 설치된 웹서버가 DMZ에 설치되어 있는 지 확인	
10	○ 민원서류발급시스템(이수증 등)의 경우 출력문서 위·변조 방지 등 보안 대책 강구	
11	○ 생성되는 모든 로그(접속 기록, 에러 기록 등) 1년 이상 저장	
12	○ 소프트웨어 개발 보안 반영 여부	
13	○ 용역업체 보안성 검토 사항 반영 여부	
추가 보안 사항		

□ 네트워크 보안

구분	점 검 내 용	반영 여부 (반영, 미반영, 향후 반영, 미적용 대상)
1	○ 원격 접속은 원칙적으로 금지, 장비 관리용 목적으로 내부망의 인가된 사용자 및 단말기를 통해 관리·운영	
2	○ 물리적으로 안전한 장소에 설치, 비인가자 무단 접근 통제	
3	○ 신규 전산장비 도입 시 기본(default)계정을 삭제 또는 변경, 시스템 운영을 위한 관리자 계정 별도 생성	
4	○ 불필요한 서비스 포트 및 개별 사용자 계정 차단·삭제	
5	○ 펌웨어 무결성 및 소프트웨어·서버 운영체제 취약점과 최신 업데이트 여부 주기적으로 확인, 최신 버전 유지	
6	○ 네트워크 장비의 접속 기록을 1년 이상 유지, 비인가자의 접근통제 여부를 주기적으로 점검	
7	○ 'IP주소' 체계적 관리, 사설 주소체계(NAT) 적용	
8	○ 네크워크 장비(L3 이상 스위치, 라우터 등) 및 보안기능이 있는 L2 스위치는 국가정보원의 보안적합성 검증실시 ※ 국가사이버안전센터 검증필 제품의 경우 보안적합성 검증 예외 가능	
9	○ 용역업체 보안성 검토 사항 반영 여부	
추가 보안 사항		

□ 서버 보안

구분	점 검 내 용	반영 여부 (반영, 미반영, 향후 반영, 미적용 대상)
1	○ 서버 내 저장자료에 대해 업무별·자료별 중요도에 따라 개별사용자의 접근권한 차등 부여	
2	○ 개별사용자별 자료 접근범위를 서버에 등록하여 인가 여부를 식별하도록 하고 인가된 범위 이외 자료 접근 통제	
3	○ 서버의 운영에 필요한 서비스 포트 외에 불필요한 서비스 포트 제거, 관리용 서비스와 사용자용 서비스를 분리·운영	
4	○ 서버의 관리용 서비스 접속 시 특정 IP와 MAC 주소가 부여된 관리용 단말 지정 운영	
5	○ 서버 설정 정보 및 저장자료에 대한 정기적 백업 실시	
6	○ 연 1회 이상 서버 설정 정보와 저장자료의 절취 및 위변조 가능성 등 보안 취약점 점검 및 보완 필요	
7	○ 서버에서 생성되는 모든 로그기록에 대해 1년 이상 저장	
8	○ 시간 동기화 프로토콜(NTP) 적용 등을 통해 정확한 로그 기록 유지	
9	○ 로그기록의 위변조 및 외부유출 방지대책 수립 및 적용	
10	○ 용역업체 보안성 검토 사항 반영 여부	
추가 보안 사항		

□ 무선랜 도입 보안

구분	점 검 내 용	반영 여부 (반영, 미반영, 향후 반영, 미적용 대상)
1	○ 네트워크 이름(SSID, Service Set Identifier) 브로드캐스팅 중지	
2	○ 추측이 어려운 복잡한 SSID 사용	
3	○ WPA2 이상(256비트 이상)의 암호체계를 사용하여 소통자료 암호화(국가정보원장이 승인한 암호논리 사용)	
4	○ 비인가 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	○ 무선 침입방지시스템 설치 등 침입 차단 대책	
7	○ 기관의 내부망 정보시스템 또는 인접해 있는 다른 기관의 정보시스템이 해당 무선랜에 접속되지 않도록 하는 기술적 보안 대책	
8	○ 무선단말기·중계기(AP) 등 무선랜 구성요소별 분실·탈취·훼손·오용 등에 대비한 관리적·물리적 보안 대책	
9	○ 각각의 용도에 따라 업무용 무선랜과 개인 소유 무선기기 접속을 위한 무선랜, 민원실 등 상용 인터넷망에 연결된 외부인 전용 무선랜을 각각 분리하여 사용자를 분리하여 운영	
10	○ 그 밖에 총장이 정하는 무선랜 보안 대책 강구 여부	
11	○ 용역업체 보안성 검토 사항 반영 여부	
추가 보안 사항	무선랜 보안 대책의 경우 교육현장은 제외	

□ 클라우드 컴퓨팅 보안

구분	점 검 내 용	반영 여부 (반영, 미반영, 향후 반영, 미적용 대상)
1	○ 민간 클라우드 컴퓨팅 서비스를 이용하고자 할 경우 다음 사항을 준수 - 국내에 위치한 정보시스템에 데이터가 저장되는 서비스로서 일반 이용자용 서비스 영역과 물리적으로 분리 - 과학기술정보통신부장관이 고시한 「클라우드 컴퓨팅 서비스 정보보호에 관한 기준」에 부합하는 서비스 선정 - 「국가·공공기관 클라우드 컴퓨팅 보안 가이드라인」 및 「행정·공공기관 민간 클라우드 이용 가이드라인」 준수 ※ 교육 현장은 제외	
2	○ 데이터베이스, 업무포털, 그룹웨어 등 내부 업무용 시스템과 홈페이지 등 외부 공개용 시스템은 반드시 물리적으로 분리된 서버 사용	
3	○ 네트워크 스위치, 스토리지 등 중요 장비를 이중화하고 클라우드 서비스의 가용성 보장을 위해 백업체계 구축	
4	○ 클라우드 서비스 제공 관리자가 서비스를 이용하는 기관 및 개인에 할당된 자원(메모리, 디스크 등)에 임의적으로 접근하지 못하도록 접근제어 등 기술적 통제 수단 마련	
5	○ 클라우드 구성 요소(단말 PC, 네트워크 장비, 서버장비, 가상머신 등)간 송수신되는 데이터 암호화	
6	○ 스토리지에 저장된 파일(업무자료·가상이미지 등)이 해킹 및 비인가자에 의해 절취되더라도 열람·실행이 불가능하도록 스토리지 데이터 암호화	
7	○ 신규 도입되는 서버·PC의 가상화 솔루션 및 정보보호제품은 국가정보원장이 정한 국내용 CC인증을 받은 정보보호시스템 도입 적용 ※ 서버 및 PC 가상화 제품 도입 시 국가사이버안전센터 선검증 제품 사용 필수, 선검증 제품이 없을 경우 국제CC인증을 수료한 제품 사용 가능	
8	○ 용역업체 보안성 검토 사항 반영 여부	
추가 보안 사항		

□ 인터넷전화 보안

구분	점 검 내 용	반영 여부 (반영, 미반영, 향후 반영, 미적용 대상)
1	○ 한국정보통신기술협회(TTA) verified ver.4 이상 보안규격으로 인증받은 행정기관용 인터넷전화시스템 설치·운용	
2	○ 인가된 인터넷전화 장비(전화기, 교환기 서버)간 제어신호 및 음성데이터 송수신 이전, 단말기 식별 및 유효성 확인을 위해 상호간 장치(Device) 인증 필요 ※ 공개키 기반 장치인증체계(PKI)에서 발급된 장치인증서 사용 필요	
3	○ 인가된 사용자에게 인터넷전화 사용을 허가하기 위한 주체 확인 및 식별을 통한 접근 제어 수행 ※ 국제 표준인 HTTP Digest 프로토콜을 적용하여 인증 받은 사용자만이 인터넷전화 사용 조치	
4	○ 통화내용 암호화를 위해서는 국제 표준에서 제시하고 있는 SRTP(Secure Real-time Transport Protocol) 프로토콜 반드시 적용	
5	○ 인터넷전화 서비스사업자 이행 보안 대책 적용 여부	
6	○ 인터넷전화망과 다른 정보통신망과 분리	
7	○ 인터넷전화 및 교환장비 대상 해킹·DDoS공격 등을 탐지·차단하기 위해서 인터넷전화 전용 침입차단·탐지시스템 사용	
8	○ 인터넷 전화 관련 서버 및 네트워크 장비, 서버·네트워크 부분 보안성 검토 사항 반영 여부	
9	○ 용역업체 보안성 검토 사항 반영 여부	
추가 보안 사항		

□ CCTV 보안

구분	점 검 내 용	반영 여부 (반영, 미반영, 향후 반영, 미적용 대상)
1	○ 카메라, 비디오서버, 관제서버, 소통망은 내부업무망 및 인터넷과 분리, 별도 단독망 구성 여부	
2	○ 부득이한 사유로 인터넷을 활용할 경우 중간 스니핑을 통한 영상자료 유출을 방지하기 위하여 원격지카메라(비디오서버)↔관제서버 종단간 VPN 설치 등을 통한 자료 암호화 소통 여부	
3	○ 원격지 감시 등의 사유로 단독망 구축 불가 시 전용회선 사용 여부	
4	○ 비인가자의 카메라(비디오서버) 접근을 방지하기 위하여 Telnet 등 원격 접근서비스 차단 설정, 접근 가능 IP제한(관제용서버 IP로 한정), 디폴트 패스워드 변경, 카메라 IP 외부 공개 금지 등 보안조치	
5	○ 내부망 내 시스템과 자료교환 필요 시, CCTV시스템망·업무망 앞의 침입차단시스템을 각각 활용, 특정 IP·포트만 접속토록 설정 여부	
6	○ 외부에 CCTV 설치 시 카메라, 중계 서버는 비인가자의 임의 조작이 물리적으로 불가능하도록 위치하거나 시건 장치 설치	
7	○ 영상기록의 임의열람 및 사적활용 방지대책을 마련하고, 저장매체는 비인가자의 접근이 불가능하도록 시건 장치가 설치된 통제구역에 보관	
8	○ CCTV 관련 서버 및 네트워크 장비, 서버·네트워크 부분 보안성 검토 사항 반영 여부	
9	○ 용역업체 보안성 검토 사항 반영 여부	
추가 보안 사항		

□ 보안장비 보안

구분	점 검 내 용	반영 여부 (반영, 미반영, 향후 반영, 미적용 대상)
1	○ 정보통신실 등 주요 정보통신시설을 보호구역으로 관리	
2	○ 보안장비 인증 등급(국가정보원 CC인증)이 EAL2 이상 여부	
3	○ 관리자로 지정된 IP주소만 접속 허용	
4	○ 신규 장비 및 소프트웨어 도입·설치 시 기존 시스템의 변화로 인한 장애 등의 문제 발생 소지에 대한 안전대책 수립 후 진행	
5	○ 원격 접속은 원칙적으로 금지, 장비 관리용 목적으로 내부망의 인가된 사용자 및 단말기를 통해 관리 운영	
6	○ 신규 장비 도입시 기본(default) 계정을 삭제 또는 변경하고 시스템 운영을 위한 관리자 계정 별도 생성	
7	○ 펌웨어 무결성 및 소프트웨어·서버 운영체제 취약점과 업데이트 여부를 주기적으로 확인하여 최신 버전 유지	
8	○ 시스템 관리자는 보안장비의 접속 기록을 1년 이상 유지, 비인가자의 접근 여부를 주기적으로 점검	
9	○ 장비 설정 주기적 백업 실시	
10	○ 용역업체 보안성 검토 사항 반영 여부	
추가 보안 사항		