상지대학교 정보 보안에 관한 규정

제정 2011. 09. 28.
제4차 개정 2022. 04. 20.

제1장 총칙

제1조(목적) 상지대학교의 정보보안 규정은 다음을 목적으로 한다.

① 정보보안업무 처리에 관한 관련 법률 및 각종 지침에 의거 정보자산의 관리체계와 방향 제시

② 중요한 정보자산을 내·외부의 위협으로부터 안전하게 보호하여 업무의 연속성 보장

③ 정보보안 사고를 예방하고 소관업무와 관련된 개인정보보호에 필요한 사항을 규정하여 원활한 전산서비스 제공

제2조(적용범위 및 책임과 의무) ① 이 규정은 다른 법령에 규정된 것을 제외하고 상지대학교와 그 소속기관, 산하기관 및 단체, 기타 업무상 상지대학교 총장의 조정 및 감독을 받는 단체(이하 '상지대학교'이라 한다)에 적용한다. (개정 2017.04.25)

② 상지대학교 및 각 기관의 컴퓨터에 의하여 처리되는 개인정보보호에 대하여 해당 지침 등에 따로 처리규정이 있을 경우에는 해당 규정이나 지침에 의한다. 다만, 타 법령에 의해 적용되는 경우에는 타 법령, 지침에 따른다.

③ 정보보호에 대한 책임과 의무는 본교의 전산자원을 사용하는 모든 구성원에 있으며 본 규정을 준수하지 않아 발생한 사고의 책임은 원칙적으로 사용자 본인에게 있다.

제3조(정의) ① 이 규정에서 사용하는 용어 정의는 다음과 같다.

1. "정보통신망"이라 함은 유·무선을 매개로 하는 다양한 정보통신 수단에 의하여 부호, 문자, 음향, 영상 등의 정보를 수집, 가공, 저장, 검색, 송·수신하는 정보통신 체제를 말한다.
2. "상지대학교 웹 사이트"(이하 '웹 사이트'라고 한다)라 함은 인터넷상에서 상지대학교에서 구축하고 운영하는 모든 웹 사이트를 말한다.
3. "정보시스템"이라 함은 정보의 수집, 가공, 저장, 검색, 송·수신에 활용되는 PC, 노트북, 서버 등의 전자기기와 소프트웨어의 조직화된 체계를 말하며, 저장매체를 내장한 복사기, 팩스 등 사무용 기기를 포함한다.
4. "정보보안 책임관"이라 함은 정보보호업무를 총괄하는 부서의 장을 말한다.
5. "정보시스템 취급자"(이하 '취급자'라 한다)라 함은 해당 정보시스템을 사용하는 자를 말한다.
6. "정보통신실"이라 함은 전산장비(서버 등)와 전송장비(스위치, 교환기, 라우터 등), 보안장비(방화벽 등) 등 정보통신망과 전송장비 및 보안시스템이 종합적으로 설치, 운용되는 장소를 말하며, 전산실, 통신실, 관제실 및 전산자료 보관실 등을 말한다.
7. "전산실"이라 함은 각종 전산장비(서버 등)를 설치, 운용하는 곳으로 정보를 입력, 보관하고 보조기억매체를 종합 관리, 보관하는 장소로써 자료보관실을 포함한다.
8. "관제실"이라 함은 정보통신망이나 정보시스템의 운용과 통신하기 위한 수단으로 수집, 가공, 저장, 검색, 송·수신되는 각종 정보를 종합 관리, 감시, 분석, 대응하는 장소를 말한다.

9. “전산자료”라 함은 전산장비에 의하여 전자기적인 형태로 입력, 보관 되어 있는 각종 자료(data)를 말하며, 그 자료가 입력되어 있는 보조기억매체를 포함한다.
10. “정보보안” 또는 “정보보호”라 함은 정보통신 수단으로 수집, 가공, 저장, 검색, 송・수신 되는 정보의 유출, 위・변조, 훼손 등을 방지하거나 정보통신망을 보호하기 위하여 관리적, 물리적, 기술적 수단을 강구하는 일체의 행위를 말한다.
11. “정보보안시스템”(이하‘ 보안시스템’이라 한다)이라 함은 학교 학사, 행정업무, 웹사이트, 통신망 등에 필요한 중요자료를 보호하기 위하여 사이버안전기술이 적용된 프로그램이나 장치 등을 말한다.
12. “보안적합성 검증필 정보보호시스템”(이하 ‘검증필 정보보호시스템’이라 한다)이라 함은 상용 정보보호시스템 중 국가정보원장이 각급기관에서 사용하는 것이 적합하다고 승인한 것을 말한다.
13. “암호화”라 함은 자료의 누설, 위・변조, 훼손방지를 위하여 기밀성, 무결성, 인증, 부인봉쇄 등의 기능을 제공하는 프로그램 혹은 알고리즘을 말한다.
14. “보조기억매체”라 함은 디스켓, CD, 하드디스크, USB 메모리 등 자료를 저장할 수 있는 것으로 정보통신시스템과 분리할 수 있는 기억장치를 말한다.
15. “보조기억매체 관리책임자”(이하 ‘관리책임자’라 한다)라 함은 각 부, 팀, 실의 보조기억매체 관리상의 책임을 맡은 그 부장, 팀장, 실장을 말한다.
16. “보조기억매체 취급자”(이하 ‘취급자’라 한다)라 함은 해당 보조기억매체를 사용하는 자를 말한다.
17. “보조기억매체 관리시스템”(이하 ‘관리시스템’이라 한다)이라 함은 보조기억매체의 등록, 파기, 재사용, 반출, 반입, 불용처리 현황 등에 관하여 전자적으로 처리하는 시스템을 말한다.
18. “저장매체”라 함은 자기저장장치, 광 저장장치, 반도체 저장장치 등 자료기록이 가능한 전자장치를 말한다.
19. “소자”라 함은 저장매체에 역자기장을 이용해 매체의 자화값을 0으로 만들어 저장자료의 복원을 불가능하게 만드는 것을 말한다.
20. “완전포맷”이라 함은 저장매체 전체의 자료저장 위치에 새로운 자료(0 또는 1)를 중복하여 저장하는 것을 말한다.
21. “저장매체 완전삭제장비”(이하 ‘완전삭제장비’이라 한다)라 함은 저장매체의 자료를 복구 불가능하게 완전 삭제하는, 국가정보원이 인증한 장비를 말한다.
22. “무선통신망”이라 함은 무선접근(무선랜, 휴대폰, 스마트폰, PDA, 테블릿 PC 등)이 가능한 기기와 통신장비 및 통신망을 말한다.
23. “개인정보”라 함은 생존하는 개인에 관한 정보로써 당해 정보에 포함되어 있는 성명, 주민등록번호 및 화상 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 자격, 직업, 재산상황, 채권채무관계 등 포함)를 말한다.
24. “처리”라 함은 컴퓨터, 폐쇄회로 텔레비전(CCTV) 등 정보의 처리 또는 송・수신 기능을 가진 장치(이하 ‘컴퓨터 등’이라 한다)를 사용하여 정보의 입력, 저장, 편집, 검색, 삭제 및 출력 기타 이와 유사한 행위를 하는 것을 말한다. 다만, 문장만을 작성하는 등의 단순 업무처리를 위한 행위를 하는 것은 제외한다.
25. “개인정보파일”이라 함은 컴퓨터 등에 의하여 처리할 수 있도록 체계적으로 구성된 개인 정보의 집합물로써 전자적인 매체에 기록된 것을 말한다.
26. “처리정보”라 함은 개인정보파일에 기록되어 있는 개인정보를 말한다.
27. “보유”라 함은 개인정보파일을 작성 또는 취득하거나 유지, 관리하는 것(개인정보의 처리를 다른 기관, 단체 등에 위탁하는 경우를 포함하되, 다른 기관, 단체 등

으로 부터 위탁받은 경우는 제외)을 말한다.

28. “보유기관”이라 함은 개인정보파일을 보유하는 기관을 말한다.
29. “정보주체”라 함은 처리정보에 의하여 식별되는 자로서 당해 정보의 주체가 되는 자를 말한다.
30. “개인정보처리시스템”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다. (신설 2017.04.25)
31. “개인정보 보호책임자”라 함은 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자로서 개인정보 보호법 시행령 제32조제2항에 해당하는 자를 말한다. (신설 2017.04.25)
32. “개인정보보호 분야별책임자”란 업무를 위하여 개인정보파일을 처리하는 부서의 장으로 개인정보 보호책임자가 지정한 자를 말한다. (신설 2017.04.25)
33. “개인정보 보호담당자”라 함은 개인정보 보호책임자를 보좌하여 개인정보보호 업무에 대한 실무를 담당하는 자를 말한다. (신설 2017.04.25)
34. “개인정보취급자”라 함은 개인정보보호책임자의 지휘.감독을 받아 개인정보를 처리하는 업무를 담당하는 교직원, 파견자 등을 말한다. (신설 2017.04.25)

제2장 위원회

제4조(구성) ① 학교의 장은 체계적이고 효율적인 보안정책 수립, 심의 및 관리를 위하여 정보보안 심사위원회(이하 ‘위원회’라 한다)를 둔다.

② 위원회는 정보보안 책임관을 위원장으로 하며 위원장을 포함하여 7인 내외의 위원으로 구성한다.

③ 위원회는 학술정보원장, 기획처장을 당연직으로 하되, 정보보안 책임관이 필요로 하는 경우 외부 보안전문위원을 포함 할 수 있다. (개정 2019.06.25., 2022.04.20)

④ 위원회는 위원장을 포함한 당연직 위원의 임기는 보직 재임기간으로 하며, 그 외 위원은 2년으로 한다. 다만, 보궐위원의 임기는 전임자의 잔여기간으로 한다.

⑤ 위원장은 전문가의 의견이 필요한 경우 내·외부 전문가로부터 자문을 구할 수 있다.

⑥ 위원장은 목적달성을 위하여 위원회 산하의 실무협의회를 구성할 수 있으며, 실무협의회 구성 및 운영에 관한 사항은 본 위원회에서 정한다.

⑦ 위원장은 위원회의 사무를 처리하기 위하여 간사를 둘 수 있다.

제5조(기능) 위원회는 제1조의 목적을 달성하기 위하여 각 호의 사항을 심의, 의결한다.

1. 정보보호 정책 및 총괄 계획 심의
2. 정보보안사고 처리에 관한 주요사항 심의
3. 정보보안교육 계획 및 정보보안준수 사항 감사 계획 심의
4. 개인정보보호에 관한 정책 및 제도 개선에 관한 사항 심의
5. 개인정보에 관한 부서 간의 의견조정에 관한 사항 심의
6. 정보보안 및 개인정보에 관한 심의요청 사항 심의
7. 본 위원회 규정의 제·개정 및 운영에 관한 사항 심의
8. 기타 정보보안책임관이 인정하는 정보보안 및 개인정보보호에 필요한 제반사항

제6조(회의 및 운영) ① 위원장은 위원회의를 소집하고 위원회 의장이 된다.

② 위원회는 재적위원 과반수 출석과 출석위원의 과반수 찬성으로 의결한다. 다만 가부 동수의 경우 위원장이 결정한다.

③ 위원회의 회의록은 위원장을 포함한 출석위원 과반수 이상이 서명 날인해야 하며, 위원회 심의·의결된 사항은 총장에게 보고한다.
④ 이 규정에 명시되지 아니한 세부 운영에 관한사항은 위원회의 심의를 거쳐 위원장이 정한다.

제3장 조직

제7조(책임) 상지대학교의 정보보안에 관한 책임은 상지대학교 총장에게 있다.

제8조(조직) ① 학교의 장은 학술정보원장을 정보보안책임관으로 지정한다. (개정 2018.10.17)
② 정보보안책임관은 정보보안담당자(정보보안 실무책임자)와 정보보안실무자(정보보안 실무운영자)를 지정한다.
③ 정보보안에 관한 업무의 전담부서는 학술정보원 전산정보팀으로 한다. (개정 2018.10.17)

제9조(임무) ① 정보보안 책임관의 임무는 다음 각 호와 같다.
1. 정보보호에 관한 지휘 감독
2. 정보보안 심사위원장으로 참여
3. 정보보안 정책 및 규정의 검토
4. 정보보안 대책의 수립
5. 개인정보보호 계획 및 방침 수립
6. 상지대학교 및 각 기관 정보보호에 관한 지휘, 감독, 감사 및 의견 제시
7. 정보자산 신·증설 시 보안대책 수립 및 보안성 검토
8. 정보보안 침해사고 조사, 처리, 대응
9. 사이버 위협정보 수집, 분석, 경보발령 및 보안관제
10. 외부 유관기관과 협력 창구 마련
11. 기타 정보보안을 위해 필요한 사항 등

② 전산정보팀의 업무는 다음 각 호와 같다. (개정 2018.10.17)
1. 보안시스템의 운용과 보안사고 예방
2. 소관분야 정보보안 업무조정 및 지도, 감독
3. 침해사고접수, 조사, 처리, 대응
4. 사이버 위협정보 수집, 분석 및 보안관제
5. 침해사고 예방을 위한 취약점 분석
6. 침해사고 대응 및 복구
7. 정보보안에 관한 홍보 및 교육
8. 각종 정보시스템 운영 및 관리
9. 사이버 공격 관련 경보 발령 시 대응활동
10. 개인정보에 관한 제반 업무
11. 정보보안 위규 적발 및 사고조사 처리
12. 소관분야 정보보안 업무조정 및 감독
13. 기타 정보보안 관련 사항

제4장 정보보안

제1절 정보자산관리

제10조(자산의 분류) ① 정보자산의 분류는 정보, 소프트웨어, 하드웨어, 부대설비로 분류하며 다음 각 호에 따른다.

1. 정보 : 데이터베이스(DB)나 파일 형태로 저장된 전자정보 및 정보자산 운영에 필요한 문서 등
2. 소프트웨어 : 운영체제(OS), 시스템 소프트웨어(웹 서버, 웹 어플리케이션, 데이터베이스관리 시스템 등), 사무자동화소프트웨어, 업무용 응용프로그램, 보안소프트웨어, 통신 소프트웨어, 기타 개발 및 관리용 소프트웨어 등
3. 하드웨어 : 컴퓨터자원, 스토리지, 백업장비, 네트워크 장비, 보안장비 등
4. 부대설비 : 무정전전원공급장비, 발전기, 항온항습기, 출입 통제장치 등

제11조(정보자산의 등급) 정보자산은 침해사고 발생 시 재정적, 운영적, 대외 이미지 손실 등과 기밀성, 무결성, 가용성을 고려하여 다음 각 호에 따라 정한다.

1. 1등급 : 재정적 손실만 있고 그 정도가 미약함
2. 2등급 : 재정적, 이미지 손실 등 면에서 약간의 손실은 있으나, 법에 위배되지 않음
3. 3등급 : 법에 위배되며, 소규모 재정적 손실과 조직운용관리 등에 지장 있음
4. 4등급 : 법에 위배되며, 중규모 재정적 손실과 운용업무에 심각한 영향 있음
5. 5등급 : 법에 위배되며, 대규모 재정적 손실과 경쟁력에 심각한 영향 있고, 조직 자체의 존립에 영향이 있음

제12조(정보자산관리) 정보보안책임관는 정보자산목록을 작성 관리해야 하며 정기적으로 정보자산을 점검하여 최신성을 유지해야 한다.

제13조(정보자산의 도입) ① 정보보안책임관은 보안시스템 및 소프트웨어의 도입 시 안전성과 침해사고 방지를 위하여 규정된 구매절차와 보안성에 대한 검토를 실시하여야 한다. 다만, 공신력 있는 기관의 인증된 제품에 대하여 생략 할 수 있다.

② 상지대학교 및 각 기관에서는 다음 각 호의 경우 사업계획 단계부터 보안성 검토를 실시후 진행하여야 한다.

1. 정보통신망을 신·증설하거나 서버 등 정보통신시스템을 교체하는 경우
2. 내부 정보통신망을 외부 망과 연결하고자 하는 경우
3. 보안시스템 또는 검증필 정보보호시스템을 도입, 운용하고자 할 경우
4. 소프트웨어개발 등 정보화 용역개발 할 경우
5. 외부기관 및 업체의 보안감리 또는 보안컨설팅(보안취약성 분석, 평가 포함)을 받거나 정보처리 업무를 위탁 할 경우
6. 기타 정보보안책임관이 인정하는 사항

③ 정보보안책임관은 정보시스템 도입 시 보안성 검토를 실시하며, 필요 시 위원회 심의를 거친다.

④ 정보보안책임관은 정보자산 중 보안시스템과, 기밀시스템, 개인정보처리시스템 등은 상시 모니터링 가능해야 하며, 비인가자의 불법접근, 인가자의 오·남용을 방지하기 위하여 물리적인 출입통제가 시행되도록 한다.

⑤ 정보보안책임관은 보안시스템의 경우 본래 도입에 맞게 설치 및 사용하여야 하며 허가 없이 변경할 수 없다.

제14조(정보자산 폐기 또는 매각) ① 상지대학교 및 각 기관은 정보자산의 폐기 또는 매각 시 저장매체는 완전포맷 또는 저장매체 완전파기 시스템을 통하여 복구 불가능하도록 해야 한다.

② 상지대학교 및 각 기관은 백업 미디어와 같은 기록매체는 폐기 전 데이터 삭제 및

포맷 후 폐기하며, 필요시 물리적으로 완전파기 하여야 한다.
③ 상지대학교 및 각 기관은 하드웨어의 매각 폐기는 반출 전 모든 구성정보, 로그정보, 비밀번호 등 초기화 또는 삭제 하여야 한다.
④ 상지대학교 및 각 기관은 개인정보가 포함된 문서 또는 정보자산 운영에 필요한 문서는 파쇄 또는 완전 소각해야 하며 폐기 전문 업체를 통하여 매각할 경우 정보유출과 관련한 보안사항을 계약서에 명시하여야 한다.

제2절 보안교육

제15조(보안교육 계획) ① 정보보안책임관은 전 교직원을 대상으로 정보보안 교육을 실시할 수 있도록 학기 초 교육계획을 수립하여야 한다.
② 정보보안책임관은 필요시 외부 전문가에게 위탁하여 보안교육을 실시할 수 있으며, 교육 전 교육계획을 사전 협의하도록 한다.

제16조(보안교육) ① 정보보안책임관은 전 교직원을 대상으로 하는 정보보안 교육은 매년 정기적으로 실시하며 필요 시 비정기적 교육을 실시할 수 있다.
② 정보보안책임관은 교직원의 채용, 전보 시 직무와 관련된 정보보안 교육을 실시한다.
③ 정보보안책임관은 외부자에 대한 정보보안 교육은 정보보안 담당부서와 업무주관부서의 협의에 따라 시행 한다.
④ 정보보안책임관은 다음 각 호에 정보보호 교육내용을 업무 특성에 맞게 교육하여야 한다.
1. 정보보안 정책, 규정
2. 정보보안 관련 법률
3. 개인정보보호에 관한 법률 및 업무처리
4. 업무용 PC 보안
5. 외부자 교육, 보안요구사항 계약 시 준수사항 등
6. 정보보호 윤리
7. 기타 보안관련 사항
⑤ 정보보안책임관은 정보보안 교육 실시 후 교육대상, 교육 참석자, 교육장소, 일시, 내용 등을 포함하여 교육결과 분석결과 보고서를 총장에게 보고하여야 한다.

제3절 외부자 정보보안

제17조(외부자 보안관리 책임) 상지대학교 및 각 기관은 외부자의 관리와 감독의 책임은 주관부서에 있으며, 정보보안책임관은 상지대학교 및 각 기관의 외부자의 정보보안 준수 사항에 대한 이행여부에 대하여 지도, 감독, 감사를 할 수 있다.

제18조(보안서약) ① 상지대학교 및 각 기관은 외부자가 법인일 경우 대표자의 보안서약서 이외업무를 수행할 개인에 대하여 보안서약서를 작성하여야 한다.
② 보안서약서를 작성한 외부자는 내부직원과 동일한 정보보안 책임과 의무를 가진다.

제19조(외부자 접근통제) ① 외부자는 본 대학교 시스템에 접근할 경우, 별도 사용자 계정을 발급 받아야 한다.
② 정보보안책임관이 운영 중인 정보시스템의 접근을 승인한 경우 이용시간과 작업시간을 제한하여 접근 통제할 수 있다.
③ 정보보안책임관은 외부자가 업무에 필요한 정보만 접근할 수 있도록 통제하며 필요 이상의 접근권한을 설정하지 않도록 한다.

④ 정보보안책임관은 외부자에게 원격접근을 허용한 경우 접근통제관리 및 모니터링 하고 그 기록을 일정기간 보관하여야 한다.

⑤ 외부자는 업무완료 시 본 대학교 소유의 모든 정보자산을 반환해야 하며, 개인 PC, 노트북, 저장장치 등에 포함된 모든 정보는 삭제한다. 다만, 정보보안책임관의 승인을 득한 경우에는 예외로 한다.

제20조(외부자의 장비 반·출입) ① 정보보안책임관은 외부자 소유의 정보자산의 반·출입을 제한한다. 단, 정보보안 책임관이 승인을 득한 경우는 예외로 한다.

② 정보보안책임관은 정보자산의 반·출입에 대한 이력을 관리하여야 한다.

제4절 물리적 보안

제21조(보호구역의 지정) 학교의 장은 정보자산을 보호하기 위하여 보호구역을 다음 각 호에 따라 정한다.

1. 제한구역 : 총장실, 통신실, 전기실, 기계실, 문서고, 상황실(CCTV 감시 장소), 개인정보 취급 장소
2. 통제구역 : 전산실(주 전산기 설치구역 및 정보자료 보관 장소)

제22조(보호구역의 관리) ① 보호구역의 관리책임자는 다음과 같다.

1. 제한구역 : 시설을 관리하는 주무처장
2. 통제구역 : 정보보안책임관

② 보호구역 관리책임자는 소속부서의 직원 중 관리 부책임자를 지정할 수 있다.

③ 보호구역의 관리책임자는 제한구역의 출입인가에 대하여 업무상 꼭 필요한 자에게 인가한다.

④ 보호구역의 관리책임자는 통제구역에는 출입이 인가된 자 외에 엄격하게 출입을 통제하여야 하며 출입자 명부를 비치하고 기록을 유지하여야 한다.

⑤ 보호구역의 관리책임자는 통제구역에는 바이오 인식장치와 상시 감시 장치 및 이중 출입통제 안전장치를 설치하여 엄격하게 출입을 통제 하여야 한다.

⑥ 통제구역 출입자는 보호구역의 관리책임자의 허가를 득한 외부인이라 하더라도 통제구역의 출입 시 인가된 직원과 동행해야만 한다.

⑦ 보호구역의 관리책임자는 통제구역 및 제한구역의 출입문에는 “통제구역”, “제한구역”표시를 할 수 있으며 그 규격은 내규로 정한다.

⑧ 보호구역 관리책임자는 수시 자체점검을 실시하여 문제점 및 취약요소를 파악하고 이에 대한 대책을 수립하여 보호구역 관리에 노력을 하여야 한다.

제23조(통제구역 시설 관리) 보호구역의 관리책임자는 통제구역의 시설은 다음 각 호의 안전시설을 갖춰야 한다.

1. 방수, 방화, 방진, 외부침입 방지 시설
2. 지진재해, 침수지대, 위험물 보관 장소 등이 없는 안전한 지역에 구축
3. 출입통제 관리시스템
4. 재난대비 누수감지, 열감지기, 연기감지기 등 방화시설, 하론 가스 등 소화시설, 기타 방재설비
5. 일정 온도습도 유지 장치
6. 정전 등 비상시에 대비하여 사무실과 분리하여 전원배선을 하며, 최소 30분 이상 유지할 수 있도록 무정전 전원공급장치를 설치하며, 장시간 정전을 대비하여 자가발전기를 설치
7. 화재 발생 시 사람이 대피할 수 있도록 경고, 비상벨이 울리고 일정시간 후 자동소화 설비가 작동 되도록 설비

8. 비상사태 발생 시 빠른 복구를 위하여 비상연락망 비치
9. 이중 잠금장치, 상시 출입문 일원화, 출입 시 출입문이 개방되지 않도록 자동 잠금장치 구축

제5절 보안시스템 보안

제24조(보안시스템 운영 및 관리) ① 정보보안책임관은 보안시스템 담당자를 선임하며 보안시스템 접근에 대하여 규정된 콘솔(console) 또는 경로를 통하여 접속하여야 한다.

② 정보보안책임관은 인터넷을 통하여 외부에서 내부 망으로 접속 시 신뢰할 수 있는 호스트 및 통신망을 제한하며, 사용하지 않는 프로토콜은 차단한다.

③ 정보보안책임관은 보안시스템의 접근에 대하여 보안시스템 담당자에 한하여 허용하며, 규정된 규칙으로 지속적 관리한다.

④ 정보보안책임관은 보안시스템의 각종 위협에 대한 신속한 대응과 복구를 위하여 자격을 갖춘 업체와 유지보수 계약한다.

⑤ 정보보안책임관은 보안시스템 자체에 본래 목적 이외 어떠한 프로그램이나 소프트웨어의 설치를 금지한다.

⑥ 정보보안책임관은 보안시스템 규칙에 대한 유효성 검증을 위하여 매년 정기적으로 분석하여 적용한다.

⑦ 정보보안책임관은 보안시스템의 긴급 패치와 신규 적용 룰을 신속하게 적용한다.

제25조(보안시스템 계정관리) ① 정보보안책임관은 보안시스템의 관리자 계정 이외의 모든 계정을 삭제한다.

② 정보보안책임관은 보안시스템 관리자 계정 및 비밀번호는 보안시스템 담당자 외에 유출되어서는 안된다.

③ 정보보안책임관은 보안시스템 관리자 계정의 비밀번호는 최소 분기마다 변경하여야 하며 영문, 숫자, 특수 문자를 혼용하여 최소 8자리 이상 설정한다.

제26조(보안시스템 접근통제 정책) ① 정보보안책임관은 허가된 트래픽만 허용하고, 불법적인 트래픽의 유입은 차단한다.

② 정보보안책임관은 외부의 모든 통신은 침입차단시스템 또는 침입방지시스템, 침입탐지시스템 등을 경유하도록 설정 및 운영되어야 한다.

③ 정보보안책임관은 업무 목적 상 외부에서 본 대학교 내부 망에 위치한 업무용 서버에 접근하고자 할 경우 SSL, VPN등을 통한 암호화 통신 채널을 이용하도록 하여야 한다.

제27조(보안시스템 로그 관리) ① 정보보안책임관은 로그는 최소 3개월 보관하며, 필요 시 별도 백업 미디어에 보관할 수 있다.

② 정보보안책임관은 로그 파일들은 별도 로그서버를 지정하여 통합하여 운영할 수 있으며, 로그에 대한 정기적인 분석 및 백업을 실시한다.

③ 정보보안시스템 담당자는 보안시스템 관제 중 이상 징후를 발견하거나, 로그 분석 결과 특이 사항 발생한 즉시 정보보안책임관에게 보고한다.

제28조(보안시스템의 도입) ① 정보보안책임관은 정보통신망을 보호하기 위하여 정보보호시스템 또는 정보보호기능이 탑재된 정보통신시스템을 사용하고자 할 경우 국가정보원으로부터 “검증필 정보보보호시스템”을 도입하여야 한다.

② 정보보안책임관은 국가정보원 또는 신뢰할 수 있는 기관의 검증되지 아니한 제품을 도입하고자 하는 경우 위원회의 심의를 거쳐야 한다.

③ 정보보안책임관은 보안시스템의 도입 시 유관기관과 연동 가능한 제품을 도입하고

중요 시스템에 대하여 이중화 구성을 통한 안전성이 확보되어야 한다.

제6절 네트워크 통신망 보안

제29조(네트워크통신망 운영 및 관리) ① 네트워크 통신망을 운영하는 부서는 네트워크 통신망 담당자를 선임하여야 하며 네트워크 통신망 담당자는 다음 각 호의 보안대책을 강구하여야 한다.

1. 각종 네트워크 통신망에 대한 접근권한 제한 및 통제 조치
2. 접근에 대한 통제 및 접근 로그 분석 및 유지관리
3. 중요 정보통신망 시설이 있는 장소에 대한 물리적 보호 조치
4. 네트워크 통신망에 대한 취약점 방지 조치
5. 통신망 운영에 관한 기타

② 다음 각 호에 해당하는 정보통신 운영현황을 대외비로 관리 하여야 한다.

1. 정보시스템 운영 현황
2. 정보통신망 구성도
3. IP 할당 정보
4. 주요 정보화사업 추진현황
5. 기타 정보보안 책임관이 인정하는 문서 혹은 파일

③ 정보보안책임관은 네트워크에 대한 일관성과 기밀성을 위해 통합관리를 원칙으로 하며 주요시스템에 대하여 이중화 구성을 통하여 장애 시 안전하게 구축하여야 한다.

④ 정보보안책임관은 네트워크의 신규 및 변경 시 위원회의에 보안성 검토를 거쳐 승인한다.

⑤ 정보보안책임관은 네트워크시스템을 보호하기 위하여 보안적합성이 검증된 침입탐지시스템, 침입방지시스템, 침입차단시스템 등의 보안시스템을 운영하여야 한다.

⑥ 정보보호담당부서에서는 본교에 유해하거나 불필요하다고 판단되는 웹 사이트 접속을 차단 할 수 있으며 신뢰할 수 없는 정보시스템 및 서버의 접속을 통제할 수 있다.

⑦ 상지대학교 및 각 기관은 네트워크 신·증설 시 정보보안담당부서의 보안성 검토를 받아야 하며 정보시스템의 적정 무결성 수준 및 보안수준에 대하여 기대수준에 미달할 경우 네트워크사용을 제한할 수 있다.

⑧ 상지대학교 및 각 기관은 사용자의 불법 접근, 불법 사이트운영, 불법 IP 도용, 바이러스 유포 등 불법 사용자에 대하여 사용을 제한할 수 있으며, 각종 불법 사용으로 인하여 해를 끼치거나, 명예를 훼손시켰을 경우에 법률에 의한 법적조치, 학칙에 의한 징계조치, 손해 발생 시 손해배상청구 등을 할 수 있다.

제30조(네트워크 시스템 계정관리) ① 정보보안책임관은 네트워크 시스템 관리자계정 이외의 모든 계정은 삭제한다.

② 정보보안책임관은 네트워크 관리자 계정 및 비밀번호는 네트워크 시스템 담당자 외에 유출되어서는 안된다.

③ 정보보안책임관은 네트워크 관리자 계정의 비밀번호는 최소 분기마다 변경하여야 하며 영문, 숫자, 특수 문자를 혼용하여 최소 8자리 이상 설정한다.

제31조(네트워크 접근통제) ① 정보보안책임관은 정보보호 시스템에서 P2P 등 업무에 불필요한 서비스 사용을 금지하고 관련 서비스 포트를 차단하도록 패킷 필터링 정책을 설정하여야 한다.

② 정보보안책임관은 네트워크시스템의 접근은 허가된 관리자에게만 허용하여야 한다.

③ 정보보안 책임관은 다른 기관과 정보통신망을 연결하여 사용하고자 할 경우에는 보안관리 책임한계를 설정하고 보안대책을 수립, 시행하여야 한다.
④ 정보보안책임관은 인터넷 등 상용망 및 타 기관과의 정보통신망에 대한 불법 침입(해킹)을 방지하고 효율적인 보안관리를 위해 연결지점을 지정 운용함으로써 임의 접속을 차단하여야 한다.
⑤ 상지대학교 및 각 기관은 네트워크 사용 시 적법한 사용자임을 인증 받아야 한다.

제32조(무선통신 보안관리) ① 정보보안책임관은 무선통신망(이하'무선망'이라 한다)을 운용할 경우 보안관리 방침은 다음 각 호와 같다.
1. 보안상 취약하거나, 비인가 된 무선망의 신·증설 억제
2. 상지대학교 및 각 기관에서 운용하고 있는 무선망으로 비밀 등 중요 자료를 수집, 전송하지 않는다.
3. 무선망을 신규 도입하거나 운용환경을 변경하고자 할 때에는 무선랜 보안시스템을 적용하여 구축하여야 하며 보안시스템 적용 시 위원회의 심의를 받아야 한다. 단 국가정보원 인증이 있는 경우는 그러하지 않아도 된다.
4. 무선 랜 보안을 위하여 별도 인증시스템을 사용할 수 있으며, 각 사용자에 대하여 접근 제어 및 업무제한 등 필요한 조치를 해야 한다.
5. 기타 정보보안 책임관이 인정하는 사항

제7절 정보시스템 및 전산자료 관리

제33조(주요 정보시스템 및 전산자료 운영 관리) ① 정보보안 책임관은 각종 서버, 데이터베이스(이하 'DB'라 한다)등 보안관리를 위하여 정보시스템 관리자(이하 시스템관리자)를 지정 운영하여야 한다.
② 시스템관리자는 비인가자의 각종 정보시스템 접근을 허용하지 않도록 보안기능을 설정하여야 한다.
③ 시스템관리자는 비인가자의 정보통신시스템 침입 사실을 인지한 경우에는 시스템 보호를 위한 접속차단 등 초동조치를 취하고 지체없이 정보보안 책임관에게 보고하여야 하며, 정보보안책임관은 그 결과를 총장에게 보고하여야 한다. 필요 시 정보보호 유관기관에 협조 요청을 할 수 있다.
④ 시스템관리자는 각종 정보시스템(서버, 네트워크, DB, 보안시스템 등)의 관리자계정에 대한 비밀번호는 유출되지 않도록 철저히 관리하여야 한다.

제34조(접근통제) ① 시스템관리자는 각종 서버의 보유 자료에 대해 업무별, 자료별 중요도에 따라 접근 권한을 차등 부여하여야 한다.
② 프로그램 개발자가 서버, DB등에 접근이 필요한 경우 정보보안 책임관의 승인을 득하여야 하며 개발에 필요한 최소한의 권한을 부여하고 이외의 접근을 통제하여야 한다.
③ 정보보안 책임관은 정보시스템에 대하여 외부업체의 원격 유지보수 작업을 허용하여서는 안된다. 다만, 부득이한 경우에는 필요한 보안대책을 강구한 후 허용할 수 있으며, 이 때에도 원격 유지보수 내용을 확인, 감독하여 기록으로 유지하여야 한다.
④ 시스템관리자는 정보보안책임관의 승인이 있는 일반사용자라 하더라도 서버에 접근 할 경우 인가 여부를 식별토록하며 인가된 범위 이외의 자료접근을 통제하여야 한다.

제35조(기록유지) 시스템관리자는 각종 보안 도구를 이용하여 보안취약점을 진단하여야 하며 접근기록에 대한 데이터는 일정기간 유지 관리하여야 한다.

제36조(전산자료 보안관리) ① 정보보안 책임관은 전산자료에 대한 유출이나 파괴 또는

위・변조 등에 대비하여 다음 각 호에 정하는 보안대책을 강구하여야 한다.
1. 자료 복사 본 확보 및 안전지역 별도 보관
2. 전산자료(보조기억매체) 보유현황 관리
3. 전산자료 및 장비의 반출 또는 반입 통제
4. 불법 접근 및 컴퓨터바이러스(이하'바이러스'라 한다) 피해 예방
5. 전산자료 접근권한 구분, 통제
6. 자료 저장소(DB 등)에 대한 기술적, 관리적, 물리적 보안조치
7. 예비(backup)체계 수립, 시행
8. 재난복구대책 수립 및 상시 운영계획 수립 시행
9. 정보보안책임관이 인정하는 기타 보안대책

② 정보보안책임관은 전산자료를 입력, 저장하기 위한 보조기억매체는 각 매체별로 관리하여야 하며, 비밀 등 중요자료가 입력된 보조기억매체는 별도로 관리하여야 한다.

③ 정보보안책임관은 비밀로 분류하지 않더라도 민감한 보고서나 자료에 대해서는 자료별 접근 비밀번호를 사용하고 보조기억매체를 적극 활용하여야 한다.

④ 정보보안책임관은 민감한 전산자료를 보호하기 위한 보안대책을 강구하여야 하며 세부사항 은 별도로 제정할 수 있다.

제37조(데이터베이스 관리) ① 정보보안책임관은 "데이터베이스관리자(DBA)"를 지정하여 DB접근 제한, DB생성, DB유지관리, DB권한부여 등의 권한과 책임을 갖는다.

② 데이터베이스관리자는 프로그램 개발을 위한 DB를 신규 생성하고자 하는 경우 정보 및 사용목적, 사용 기간, 연락처 등이 포함된 신청서를 제출하고 정보보안책임관의 승인을 득한 후 DBA가 생성한다.

③ 데이터베이스관리자는 비밀번호가 없는 계정은 사용을 금지하며, 사용하지 않는 DB계정은 삭제한다.

④ 정보보안책임관은 DB의 도입 또는 변경시 안전성과 범용성이 검증된 DB를 도입 또는 변경하여야 한다.

제38조(데이터베이스 접근제어) ① 데이터베이스관리자는 개발자, 사용자의 DB 계정 접근권한은 최소한의 접근권한만 부여하는 것을 원칙으로 하며 원칙에 따라 필요이상의 권한이 부여되지 않도록 데이터베이스관리자는 적절한 규칙을 생성하여 객체 권한을 부여한다.

② 정보보안책임관은 필요 시 접근제어 강화를 위하여 별도 보안솔루션(DB 접근제어 등)을 도입, 운영할 수 있다.

제39조(데이터베이스 암호화) ① 정보보안책임관은 기밀성, 개인정보 등 DB내 중요한 필드에 대하여 암호화하는 등 안전조치를 하여야 한다.

② 정보보안책임관은 DB 암호화 시 DB 암호화 알고리즘이나 DB 암호화 솔루션은 국가정보원에서 검증된 DB 암호화 솔루션을 이용하여 안전하게 구축되어야 한다.

제40조(비공개 자료 보호) ① 정보보안책임관은 정보보안과 관련된 행정정보를 비공개로 분류 관리한다.

② 정보보안책임관은 소속직원 중 비밀 및 중요업무 담당자의 인적사항, 세부 담당업무와 전자 우편 주소 등을 인터넷 등에 공개하여서는 안 된다.

제41조(중요자료 저장 보조기억매체 관리) ① 정보보안책임관은 비밀 등 중요자료가 평문 또는 암호화되어 있는 보조기억매체를 사용하고자 할 경우 유출, 훼손, 비인가자 접근 및 내용 위・변조 등에 대비한 보안대책을 강구하여 정보보안책임관의 승인을 받아야 한다.

② 정보보안책임관은 비밀자료가 저장된 보조기억매체는 매체별 관리번호를 부여하고 관리기록부에 등재하며 이중캐비닛 또는 금고에 보관하여야 한다. 암호화되어 저장된 보조기억매체는 예외로 한다.

제42조(재난 및 복구대책) ① 정보보안책임관은 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애 발생에 대비하여 주요시스템 이원화, 백업 및 복구 등 종합적인 재난복구 대책을 수립 시행하여야 한다.

② 정보보안책임관은 정보통신망 장애에 대비한 백업시설을 확보하고 정기적으로 백업을 수행하여야 한다.

③ 정보보안책임관은 제1항에 의거 백업시설을 설치할 경우에는 정보통신실과 물리적으로 일정거리 이상 위치한 안전한 장소에 설치하여 재난에 대비하여야 한다.

④ 정보보안책임관은 긴급사태에 대비하여 다음 각 호의 백업 및 복구 절차 등을 수립, 시행하여야 한다.

1. 긴급사태에 대비한 조직, 임무 및 업무처리 절차
2. 백업시설 구성, 백업방법 및 절차
3. 정상상태로의 복구절차
4. 긴급사태에 대비한 정기적 훈련과 교육실시 등
5. 정보보안 책임관이 인정하는 기타 사항

제8절 저장매체 관리

제43조(정보시스템 저장자료 보안조치책임) 각 부서의 관리책임자는 정보시스템을 폐기, 양여, 교체, 반납하거나 외부수리를 위하여 외부로 반출할 경우 저장매체에 저장된 자료의 보안조치를 책임진다.

제44조(정보시스템 저장자료 삭제) 각 부서의 관리책임자 불용처리 등 정보시스템 저장매체에 저장된 자료를 삭제할 경우는 다음과 같다.

1. 정보시스템의 사용연한이 경과하여 폐기 또는 양여할 경우
2. 정보시스템 무상 보증 기간 중 저장매체 또는 저장매체를 포함한 정보시스템을 교체할 경우
3. 정보시스템의 임대기간이 만료되어 반납할 경우
4. 고장 수리를 위해 외부 반출 등 정보시스템 저장매체를 통제할 수 없는 환경으로 이동할 경우
5. 기타 정보시스템 사용자 변경 등으로 저장자료 삭제가 필요하다고 판단되는 경우

제45조(저장자료 삭제책임) ① 개인에게 지급된 정보시스템의 저장자료는 사용자 본인 책임하에 삭제하여야 한다.

② 정보보안책임관은 홈페이지 등 각 부서가 공통적으로 사용하는 정보시스템의 저장자료를 유출되지 않도록 안전하게 삭제하여야 한다.

제46조(저장자료 삭제방법의 지정) ① 정보보안책임관은 정보시스템별 저장자료 삭제방법은 [별표1] 을 준용하여 삭제한다.

② 저장매체 사용자는 인사이동 등의 사유로 정보시스템의 사용자가 변경된 경우, 비밀처리에 사용한 정보시스템은 완전포맷 3회 이상, 그 외의 정보시스템은 완전포맷 1회 이상으로 저장자료를 삭제하여야 한다.

③ 정보보안책임관은 보조기억매체 관리시스템 운영 및 완전삭제장비를 이용하여 삭제한 경우 관리규정의 준수사항을 대체할 수 있다.

④ 저장매체 사용자는 [별표1] 외 다른 방법으로 저장자료를 삭제하고자 할 때에는 사전에 정보보안 책임관과 협의 하여야 한다.

제47조(저장자료 삭제확인) ① 각 부서의 관리책임자는 정보시스템을 불용 처리할 경우 사전에 저장자료 삭제여부를 확인하여야 한다.
② 저장매체 사용자가 정보시스템에 저장된 자료의 삭제를 외부업체에 의뢰할 때에는 정보시스템 취급자가 입회하여 삭제 절차, 방법 등의 준수여부를 감독 및 확인하여야 한다.

제48조(정보시스템 도입 시 보안조치) ① 정보보안책임관은 정보시스템의 도입, 고장수리 등을 위해 공급업체가 저장매체를 교환, 반출 할 경우 저장자료 삭제방법 등 저장매체 보안조치 방안을 계약서상에 포함하도록 하여야 한다.
② 정보보안책임관은 정보시스템을 임차 사용할 때에는 임차기간 만료 후 반납 시, 당해 시스템의 저장자료 삭제방법 등 저장매체 보안조치 방안을 임차계약서상에 포함하여야 한다.

제49조(정보시스템 외부반출시 보안조치) ① 각 부서 관리책임자는 불용처리 등을 위해 정보시스템을 외부로 반출할 경우 복구가능하지 않도록 삭제 후 현황을 기록 유지하여야 한다.
② 각 부서의 관리책임자는 저장매체의 고장수리, 저장자료 복구 등을 외부에 의뢰할 경우 저장 매체에 저장된 자료의 유출 방지를 위해 수리 또는 복구 참여자에 대해 보안서약서 징구, 교육 등 필요한 보안조치를 하여야 한다.
③ 정보시스템 취급자는 정보시스템을 불용 처리할 경우 당해 시스템의 사용 기관, 부서, 사용자 등을 인식할 수 있는 표시를 모두 제거하여야 한다.

제50조(소자장비 등의 적합성 검증) 정보보안책임관은 정보시스템의 저장자료를 삭제하는 장비나 소프트웨어를 도입할 경우 국가정보원의 보안 적합성 검증을 필한 제품을 도입하여야 한다.

제9절 PC 보안관리

제51조(PC 보안관리) ① PC관리책임자는 단말기를 포함한 PC 등을 사용할 경우 비인가자가 PC를 무단으로 조작하여 전산자료를 유출, 위·변조 및 훼손시키지 못하도록 사용자는 다음 각 호에 정한 보안대책을 강구하여야 한다.
1. 장비 별, 자료 별, 사용자 별 비밀번호 사용
2. 10분 이상 PC 작업 중단 시 화면보호 조치
3. 백신 및 PC용 침입차단시스템 등 운용
4. P2P 등 업무와 무관하거나 보안에 취약한 비인가 된 프로그램의 사용 금지
5. 정보보안 책임관이 인정하는 기타 보안대책

② PC관리책임자는 PC를 교체, 반납, 폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 하드디스크 내 수록된 자료가 유출, 훼손되지 않도록 보안조치를 하여야 한다.
③ PC관리책임자 PC에 적용되는 사용자계정 및 비밀번호 관리는 제52조의 규정을 준용한다.
④ 정보보안 책임관은 상지대학교 및 각 기관 업무용 노트북 PC, PDA 등 휴대용 단말기의 운용 현황을 파악하여 관리하고, 반·출입 시 최신 백신을 활용하여 해킹프로그램 및 바이러스 감염 여부를 점검하여야 한다.
⑤ 개인소유의 PC(노트북 PC 등)는 부서 내부로 반입 또는 반출하여 사용하여서는 안 된다. 다만, 부득이한 경우에는 정보보안책임관의 승인을 받아 보안조치 후 반·출입할 수 있다.
⑥ PC관리책임자 PC의 시스템 자원(폴더, 파일 등)에 대한 공유는 모두 제거되어야

한다. 다만, 필요에 의해 공유할 경우에는 패스워드 설정, 보안인증, 암호화 등의 보안대책을 수행하여야 한다.

제52조(비밀번호 관리) PC관리책임자 비밀번호는 다음 각 호 사항을 반영하여 숫자와 문자, 특수문자 등으로 8자리 이상으로 정하고 분기 1회 이상 주기적으로 변경하여야 한다.

1. 사용자 계정(ID)과 동일하게 사용하지 않을 것
2. 개인 신상 및 부서명칭 등과 관계가 없는 것
3. 일반 사전에 등록된 단어는 사용을 피할 것
4. 동일단어 또는 숫자를 반복하여 사용하지 않을 것
5. 이미 사용된 비밀번호는 재사용하지 않을 것

제53조(악성코드 방지대책) ① 정보보안책임관은 바이러스, 해킹프로그램, 스파이웨어 등 악성코드 감염을 방지하기 위하여 다음 각 호에 따라 정보통신시스템을 운영, 관리하여야 한다.

1. 출처, 유통경로 및 제작자가 명확하지 않은 응용프로그램은 사용을 자제하고 불가피할 경우에는 백신 등 관련 검색프로그램으로 진단 후 사용
2. 업무상 불필요한 서비스를 제한
3. 실행파일은 읽기 전용으로 속성 변경
4. 인터넷 등 상용망으로 입수한 자료는 필히 악성코드 검색 후 사용
5. 악성코드 조기 발견을 위하여 최신 백신프로그램 활용 및 보안업데이트 실행
6. 시스템이 작동할 때마다 컴퓨터 하드디스크의 부트섹터 및 메모리 등에 악성코드가 감염되었는지 점검

② 정보보안책임관은 악성코드 감염이 발견되었을 경우, 시스템관리자 또는 PC 사용자는 다음 각 호의 조치를 하여야 한다.

1. 악성코드 감염피해를 최소화하기 위하여 감염된 시스템 사용 중지 및 내부망과 접속 분리
2. 최신 백신 등 악성코드 제거 프로그램을 이용하여 치료
3. 악성코드의 감염확산 방지를 위하여 정보보안책임관에게 관련 내용 및 보안조치사항을 즉시 보고
4. 악성코드 감염의 재발방지를 위하여 원인 분석 및 예방 조치 수행

③ 정보보안 책임관은 바이러스, 악성코드 등의 피해방지를 위하여 노력해야 한다.

④ 정보보안 책임관은 악성코드 감염사실을 확인하거나, 유관기관에서 조치를 권고할 경우 즉시 이행하여야 한다.

제54조(전자우편 등의 보안관리) ① PC책임자는 전자우편 사용자는 보안조치 없이 전자우편을 이용한 비밀 및 중요 자료 전송을 금지하고 출처가 불분명한 전자우편의 경우 열람하지 말고 삭제한다.

② PC관리책임자는 불분명한 첨부파일은 다운로드 또는 실행을 금지한다.

③ 정보보안 책임관은 광고, 음란, 도박 등 업무와 무관한 전자우편에 대한 수・발신을 필터링 정책을 수립하거나 스팸필터링 시스템에 의해 제한할 수 있다.

④ 정보보안 책임관은 악성코드 유포에 악용되지 않도록 전자우편 주소의 인터넷 공개 또는 대외배포를 제한한다.

⑤ PC관리책임자는 의심스러운 전자우편을 수신한 경우, 첨부파일을 열람하지 말고 발송자에 게 발송여부 확인 및 정보보안 책임관에게 신고한다.

제55조('사이버・보안진단의 날' 운영) ① 정보보안 책임관은 매월 정기적으로 '사이버・보안진단의날'로 지정, 운영하여야 한다.

② 정보보안 책임관은 '사이버・보안진단의 날'에 소관 정보통신망을 대상으로 악성코드 감염 여부와 정보통신시스템의 보안 취약여부 등을 진단, 문제점을 파악하여 개선하여야 한다.

제10절 사이버 침해사고 관리

제56조(사이버침해사고 처리 및 조사) ① 정보보안 책임관은 정보보안사고가 발생한 때에는 즉시 피해를 최소화하도록 조치하고 그 결과를 보고하여야 한다.

1. 일시 및 장소
2. 사고원인, 피해현황 등 개요
3. 사고자 및 관계자의 인적사항
4. 조치내용 등

② 정보보안 책임관은 사고조사를 실시하고 동일유형의 사고가 발생하지 않도록 제반 보안조치를 강구해야 한다.

③ 정보보안 책임관은 사고 조사 후 관련자에 대하여 관련 규정, 내부지침에 의하여 양형기준을 정할 수 있다.

④ 정보보안책임관은 보안사고분석을 위한 분석로그, 분석기록, 분석결과 등은 별도 보관하여야 한다.

⑤ 정보보안 책임관은 부정 접근, 의심사례 보안사고 과정 등은 지속적인 모니터링을 해야 하며 사고 예방을 위하여 상시 관제 체제를 구축한다.

제11절 정보보안감사

제57조(정보보안감사) ① 정보보안 책임관은 제9조의 규정에 따라 상지대학교 및 각 기관에 대해 매년 정기적 또는 비정기적으로 자체 정보보안감사 계획을 수립하여 정보보안감사를 실시하여야 한다.

② 정보보안 책임관은 보안감사 또는 불시점검은 업무 수행 시 발생할 문제점 파악에 중점을 두고 실시하여야 하며 도출된 취약요인은 근본적인 대책을 수립하여 시행하여야 한다.

③ 정보보안 책임관은 총장에게 정보보안감사 실시계획과 감사결과를 제출하여야 한다.

④ 정보보안 책임관은 정보보안감사의 효율적 수행을 위하여 각 처, 부, 팀, 실의 업무협조를 요청할 수 있다.

제58조(정보보안감사위원 구성) ① 정보보안 책임관은 정보보안감사를 실시하기 위하여 전산분야 전문가로 5인 이내 감사위원으로 구성하며 감사위원장은 정보보안 책임관으로 한다.

② 정보보안 책임관은 객관성과 전문성이 필요하다고 인정되는 경우 감사위원 중 외부 전문가를 포함하거나 위탁할 수 있다.

제59조(정보보안감사 결과 기록) ① 정보보안 책임관은 감사결과를 문서화하여 보관하여야 한다.

② 정보보안 책임관은 정보보안감사 결과는 총장 또는 외부 감독기관의 요청이 있는 경우 제출할 수 있다.

③ 정보보안 책임관은 정보보안감사를 외부 전문가를 활용하거나, 위탁한 경우 외부 전문가 감사보고서로 대체할 수 있다.

제5장 개인정보 보호관리

제1절 개인정보 보호 조직

제60조(개인정보 보호책임자의 지정 및 임무) ① 상지대학교 총장은 개인정보의 보호 및 관리를 위하여 부총장(유고 또는 공석 시 행정지원처장)을 개인정보 보호책임자로 지정한다. (개정 2019.06.25)

② 개인정보 보호책임자는 개인정보를 보유, 처리하는 부서의 부서장을 개인정보보호 분야별책임자(이하 '분야별책임자'이라 한다)로 지정, 운영한다.

③ 총괄책임관의 임무는 다음 각 호와 같다.

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독
7. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무

④ 분야별 책임관의 임무는 다음과 같다.

1. 해당 시스템을 이용(단말기제공 등)하는 제반 부서의 개인정보취급자에 대한 개인정보 보호업무의 지도 및 감독
2. 개인정보 취급자 지정 및 권한설정 등 제반 보호 장치에 관한 사항의 확인 및 감독
3. 개인정보 접근 로그 파일 등 접속기록의 주기적인 분석 및 오·남용 사고의 예방
4. 기타 소관분야별 개인정보 보호를 위해 필요한 사항 등

⑤ 그밖에 개인정보보호에 관한 사항은 개인정보보호 내부관리계획으로 정한다. (신설 2017.04.25)

(전문개정 2017.04.25)

제61조(총괄 전담조직) ① 개인정보 보호업무를 위한 총괄 전담부서로 행정지원처 행정지원팀에서 전담하며 업무는 다음 각 호에 따른다. (개정 2017.04.25., 2019.06.25., 2022.04.20)

1. 개인정보 보호정책 수립
2. 개인정보 처리실태 감독 및 관리
3. 개인정보의 수집 및 보유, 이용 및 제공, 파기, 위탁 등 내·외부의 침해로부터 보호되도록 안전하게 관리하기 위한 관리적, 기술적, 물리적 보호조치
4. 개인정보침해사고 및 대응
5. 기타 총괄책임관이 인정하는 사항

② 개인정보 보호책임자는 개인정보보호업무에 대하여 업무를 수행하기 위하여 개인정보보호 전담부서의 개인정보보호담당자를 지정할 수 있다. (개정 2017.04.25)

③ 개인정보 보호책임자는 필요한 경우 보안심사위원회와 별도로 개인정보심사위원회를 운영할 수 있으며 위원회규정은 별도로 정한다. (개정 2017.04.25)

제2절 개인정보의 수집

제62조(개인정보의 수집) ① 개인정보의 수집 및 보유를 위해서 반드시 법령에 근거하거나 정보주체의 동의에 의하되, 목적달성에 필요한 최소한의 범위내로 하여야 한다.

② 분야별책임자는 개인정보의 수집 및 보유를 위하여 다음 각 호의 사항을 준수하여야 한다. (개정 2017.04.25)

1. 당해 보유파일의 기록항목, 개인정보의 범위, 보유(폐기)기간을 소관업무 수행에 필요한 범위내로 한정
2. 당해 개인정보를 수집, 처리함으로써 개인이 입는 사생활 침해와 그로 인해 얻는 공익상의 목적달성 사이에 비례관계를 유지
3. 정보주체의 동의에 의해 수집할 경우 사전에 수집목적, 보유기간, 이용범위, 목적달성 후 처리방법 및 이의제기 절차 등에 대한 충분한 사전설명 후 수집하며, 이 경우 보유 기간을 초과하여 보유하고자 할 때에는 정보주체의 동의 필요
4. 수집한 개인정보는 수집목적을 달성한 즉시 폐기하되, 그 본래 형태 및 수록된 데이터를 식별할 수 없도록 파쇄기 또는 소각의 방법 등을 통해 폐기하여야 하며, 폐기 시 1개월 이내 폐기사실을 홈페이지에 공지한다. 단, 법령에 보유기간 등이 명시되어 있는 경우에는 예외로 한다.
5. 개인정보파일을 추가 및 정정하여 보유할 경우 반드시 행정지원처 행정지원팀과 협의하고, 관련 법령에 의거 행정안전부장관과 사전 협의 후 수집 및 보유 하여야 한다. (개정 2017.04.25., 2019.06.25, 2022.04.20)

제63조(폐쇄회로 텔레비전(CCTV)설치 등) ① 보유부서의 장은 범죄예방, 안전 확보를 위하여 필요한 경우 관련규정에 따라 전문가 및 내부구성원의 의견을 수렴한 후 폐쇄회로 텔레비전(이하 'CCTV'라 한다)을 설치할 수 있다.

② 설치된 CCTV는 설치목적 범위를 넘어 카메라를 임의 조작하거나 본래 목적 외 다른 곳을 비추어서는 아니 되며 녹음기능은 사용할 수 없다.

③ 보유부서의 장은 CCTV를 설치하는 경우 정보주체가 이를 쉽게 인식할 수 있도록 다음 각 호의 사항을 기재한 안내판을 설치하는 등 필요한 조치를 취하여야 한다.

1. 설치목적 및 장소
2. 촬영범위 및 시간
3. 관리책임자 및 연락처

④ 보유부서의 장은 CCTV의 화상정보가 보관된 장소를 통제구역으로 설정하고 화상정보가 유출 되지 않도록 철저히 관리적, 기술적 조치를 하여야 한다.

⑤ CCTV의 설치 및 운영에 관한 세부사항은 CCTV 설치 및 운영에 관한 규정에 의한다.

제64조(웹 사이트에 게재 및 수집 가능한 개인정보) ① 웹 사이트를 운영하는 분야별책임자는 개인정보의 보호방침을 웹 사이트에 게재할 때 분야별책임자의 성명, 전화번호, 이메일 주소 등 국민들의 공공기관 업무 접촉편의를 제공하기 위한 정보를 게재하여야 하며, 이메일 주소를 직접 나타나게 하지 않고 연결시스템을 갖출 수 있다. (개정 2017.04.25)

② 웹 사이트를 운영하는 분야별책임자는 홈페이지의 개선, 보완 및 침입탐지 등의 목적을 위해 필요할 경우 홈페이지 이용자에 대한 최소한의 정보를 수집할 수 있다. 수집된 개인정보는 개인을 식별할 수 없는 통계형태 등으로 처리되어야 하며, 관계법령의 이행목적이나 수집 시 동의한 목적이외 사용할 수 없다. (개정 2017.04.25)

제3절 개인정보의 이용·제공

제65조(개인정보의 열람청구) ① 분야별책임자는 정보주체 또는 법령에 따른 그 대리인이 해당 개인정보 열람을 청구하는 때에는 사본제공을 요청하는 경우와 제3자와 관련 사항(진정, 신고등)이 있는 정보를 제외하고는 즉시 열람할 수 있도록 조치하여야 한다.(단, 법령상 제한이 있는 경우 제외) (개정 2017.04.25)

② 분야별책임자는 사본을 제공하는 경우에 정보주체(본인)에게 불이익이 돌아올 수

있다는 내용을 주지한 후 제공하여야 한다. (개정 2017.04.25)
③ 개인정보 열람 장소는 개인정보를 실제 보유하고 있는 부서의 개인정보파일 사용 부서 또는 별도 지정하여 홈페이지에 공지한다.

제66조(개인정보 침해신고의 신속한 처리) ① 개인정보 보호책임자는 개인정보에 대한 침해신고가 접수되었을 경우 "개인정보침해신고처리대장"에 침해신고를 접수 후 신속하게 처리하여야 한다. (개정 2017.04.25)
② 개인정보 침해신고의 처리절차는 관계법령 및 별도 정한 지침을 준용한다.

제67조(처리정보의 이용 및 제공의 제한) ① 분야별책임자는 다른 법률에 따라 보유기관 내부 또는 보유기관 외에 이용하게 하거나 제공하는 경우를 제외하고 당해 개인정보파일의 보유목적외의 목적으로 처리정보를 이용하거나 제공하여서는 안 된다. (개정 2017.04.25)
② 분야별책임자는 보유목적에 따라 처리정보를 이용하게 하거나 제공하는 경우에도 업무수행에 필요한 최소한의 범위로 이용 또는 제공을 제한하여야 한다. (개정 2017.04.25)
③ 분야별책임자는 제1항의 규정에 불구하고 다음 각 호의 어느 하나에 해당하는 경우에는 당해 개인정보파일의 보유목적 외의 목적으로 처리정보를 이용하게 하거나 제공할 수 있다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에도 정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있다고 인정되는 때에는 그러하지 아니한다. (개정 2017.04.25)
1. 정보주체의 동의가 있거나 정보주체에게 제공하는 경우
2. 처리정보를 보유목적 외의 목적으로 이용하게 하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우
3. 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정개인을 식별할 수 없는 형태로 제공하는 경우
4. 민원만족도 조사용역을 위하여 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 동의를 할 수 없는 경우로서 정보주체 외의 자에게 이용하게 하거나 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우

④ 분야별책임자는 개인정보의 타 기관에 대한 제공은 반드시 문서로 처리하며, 다음 각 호의 사항을 확인 후 이루어져야 한다. (개정 2017.04.25)
1. 법령상 요청 근거 또는 이용목적
2. 요청목적에 따른 제공항목의 적정성
3. 타 기관 전송 시 암호화 등 적절한 보안대책 등

⑤ 분야별책임자는 개인정보를 제공받은 자가 보유기관의 동의없이 당해 처리정보를 제3자에게 이용하게 하거나 제공하지 못하도록 조치하여야 한다. (개정 2017.04.25)

제4절 개인정보의 관리

제68조(개인정보의 관리) ① 분야별책임자는 기관 내 부서간의 개인정보이용 또는 조회할 경우, 법령에 근거하거나 소관업무를 수행하기 위해 필요한 최소한의 범위로 제한하여야 한다. (개정 2017.04.25)
② 분야별책임자는 정보주체의 동의 없이 개인정보를 수집하거나 보유목적 외 또는 보유목적에 맞더라도 권한을 넘어서는 부당한 목적으로 내부직원 등이 이용 또는 조회하지 못하도록 엄격하게 관리하여야 한다. (개정 2017.04.25)
③ 분야별책임자는 보조기억매체 등에 의하여 개인정보를 제공할 경우에 비밀번호 삽

입 등 안전 대책을 수립 하여야 한다. (개정 2017.04.25)
④ 분야별책임자는 처리정보를 법률에 의해 제공할 때에도 다음의 조치사항을 명확히 하도록 하여야 한다. (개정 2017.04.25)
1. 제공범위, 데이터의 가공여부, 제공하는 파일의 형태 및 특성에 따른 보안방법 등 보호 조치
2. 제공된 처리정보(출력자료를 포함)의 폐기방법 및 확인에 관한 사항 등
⑤ 개인정보의 파기 사유가 발생 할 경우 지체 없이 파기하고, 그 결과를 파기대장에 기록 및 파기사실을 정보주체에게 안내 하여야 한다.

제69조(직원의 개인정보와 관련한 업무처리) ① 직원의 개인정보를 보유 중에 있는 분야별책임자는 상지대학교 및 각 기관의 직원에 대한 개인정보를 정보주체에게 제공하는 경우에는 제3자에게 노출되지 않도록 하여야 한다. (개정 2017.04.25)
② 당해 분야별책임자는 각 기관의 직원에 대한 개인정보가 포함된 사항을 시연회 등에 이용 할 경우 목적 달성 후 폐기하여야 하며, 계속 이용할 경우에는 식별할 수 없도록 조치하여야 한다. (개정 2017.04.25)
③ 개인정보취급자가 업무상 수행하여야 할 개인정보의 수정, 입력, 삭제, 정정 등에 대하여는 입·출력자료관리대장에 기록 유지한다.
④ 분야별책임자는 개인정보취급자에 대하여 업무 담당자별 업무상 꼭 필요한 최소한의 권한을 차별화하여 지정 하여야 한다. (개정 2017.04.25)

제70조(개인정보 사무의 인계인수) 분야별책임자는 개인정보를 취급하는 자에 대한 업무 인수인계시 다음 각 호를 준수토록 하여야 한다. (개정 2017.04.25)
1. 개인정보 보호에 관한 지침 등
2. 개인정보처리시스템의 사용자권한 설정 및 보호에 관한 사항
3. 통상적으로 제공하는 개인정보에 관한 사항
4. 기타 개인정보보호업무 수행에 필요한 사항

제71조(개인정보의 보호방침 웹 사이트 게재) ① 상지대학교 및 각 기관의 장은 홈페이지를 보유또는 개설하는 경우, “개인정보의 보호방침”을 웹 사이트에 게재하여야 한다.
② 웹 사이트에 게재할 내용은 다음 각 호와 같다.
1. 인터넷 이용자의 개인정보 보호 등을 포함하는 기관의 개인정보보호 방침
2. 개인정보파일의 열람 및 정정청구 안내
3. 권익침해 구제절차에 대한 안내
4. 개인정보보호책임자 부서명과 성명, 전화번호 및 이메일 등 연락방법 (개정 2017.04.25)
5. 보유하고 있는 개인정보파일(사전 통보대상에 한함)별로 보유근거 및 목적, 관리자, 보호책임관, 파기시기 안내
③ 개인정보의 보호방침의 게재위치는 홈페이지 초기화면 하단 등에 “개인정보보호방침” 웹 페이지를 하이퍼 링크(Hyperlink)할 수 있도록 하는 아이콘, 배너 등을 설치하여 이용자가 쉽게 찾아 볼 수 있도록 조치하여야 한다.

제72조(개인정보의 위탁처리) ① 분야별책임자는 개인정보의 처리를 다른 기관 또는 관련 전문기관에 위탁하는 경우에는 필요한 제한이나 절차를 정하고, 처리를 위탁 받은 기관으로 하여금 개인정보를 처리함에 있어 이를 준수하도록 하여야 하며 계약서에 다음 각 호의 사항을 명시 하여야 한다. (개정 2017.04.25)
1. 재 위탁금지에 관한 사항
2. 개인정보파일의 복사에 관한 사항

3. 개인정보의 관리상황에 대한 검사에 관한 사항
4. 위탁처리기관에서 준수하여야 할 의무를 위반한 경우의 손해배상 등에 관한 사항
5. 개인정보처리 시 기술적, 관리적 보호 지침 적용에 관한사항
6. 기타 개인정보 보호책임자가 인정하는 사항 (개정 2017.04.25)

② 분야별책임자는 위탁처리기관에 대하여 개인정보의 처리현황, 개인정보파일 및 입·출력 자료의 관리 등에 대한 기록과 실태를 점검하여야 한다. (개정 2017.04.25)

③ 분야별책임자는 개인정보처리의 위탁 전 반드시 개인정보 전담부서의 협조와 개인정보 보호책임자의 승인을 받아야 하며, 개인정보 보호책임자는 위탁 시 보안에 취약하거나, 위탁기관의 자격이 부실하다고 판단하는 경우 위탁을 중지 또는 취소할 수 있다. (개정 2017.04.25)

④ 분야별책임자는 개인정보처리를 위탁한 경우 위탁사실을 정보주체가 인지할 수 있도록 학교 웹 사이트(홈페이지)에 공고하여야 한다. (개정 2017.04.25)

제73조(개인정보 기록물 등의 폐기) ① 분야별책임자는 전자매체에 수록된 개인정보를 폐기하는 경우에는 다음 각 호에 따라야 한다. (개정 2017.04.25)

1. 파일 복구기술이 발달되고 있는 점을 감안, 개인정보파일 삭제 및 파기 시 철저한 덧씌우기 등 재생이 불가토록 조치
2. 컴퓨터 등의 불용처분 및 매각 시 저장된 내용의 완전삭제

② 분야별책임자는 출력물로 나타난 개인정보를 폐기하는 경우에는 다음 각 호에 따라야 한다. (개정 2017.04.25)

1. 폐·휴지 수집업자에 출력물의 원래 형태로 매각 등 금지(원래 형태로 매각할 경우에는 제지 공장의 용해작업을 현장 확인)하여야 한다.
2. 출력물을 매각 시에는 직접 파쇄 조치 후 매각한다.

제74조(개인정보관리 실태조사) ① 개인정보 보호책임자는 개인정보 보유부서의 개인정보관리 실태를 정기적 또는 비정기적으로 실태조사를 할 수 있다. (개정 2017.04.25)

② 개인정보 보호책임자는 실태조사 후 개선사항에 대한 결과조치를 실시할 수 있다. (개정 2017.04.25)

제75조(개인정보의 안전성확보) ① 개인정보 보호책임자는 다음 각 호에 의거 개인정보의 관리적, 기술적 보호 조치를 취해야 한다. (개정 2017.04.25)

1. 개인정보 처리단계별 기술적 보호조치 가이드라인
2. 개인정보 기술적, 관리적 보호조치 지침
3. 공공기관의 개인정보파일 관리지침
4. 공공기관 개인정보보호 기본지침
5. 공공기관 개인정보 업무관리 매뉴얼
6. 개인정보업무처리를 위한 세부시행지침
7. 기타 개인정보 보호책임자가 인정하는 사항, 관련 법령 및 지침 (개정 2017.04.25)

② 개인정보 보호책임자는 개인정보보호를 위하여 개인정보보호시스템을 도입할 수 있으며, 도입 시 국가정보원에서 인증, 교육 사이버 안전센터의 연동 가능한 시스템 및 소프트웨어를 도입하여야 한다. (개정 2017.04.25)

③ 개인정보 보호책임자는 국가정보원의 인증을 받지 아니한 시스템 및 소프트웨어를 도입하고 자 할 경우 위원회 심의 후 도입한다. (개정 2017.04.25)

④ 개인정보 보호책임자는 개인정보보호시스템을 유지보수 하고자 하는 경우 정보보호를 위하여 일정한 자격을 갖춘 업체에 유지보수 계약에 의해 관리하여야 한다. (개정 2017.04.25)

⑤ 상지대학교 및 각 기관의 개인정보의 해외 이전(정보 전송 포함)은 원칙적으로 불허한다. 다만, 개인정보 보호책임자의 승인이 있는 경우는 예외로 한다. (개정 2017.04.25)

⑥ 5항의 개인정보 보호책임자가 승인한 경우라도 해외 이전(정보 전송 포함) 시 개인정보 노출 방지를 위한 기술적, 관리적 안전조치를 해야 하며 정보주체에게 개인정보의 해외 이전(정보 전송 포함) 사실을 통보하여야 한다. (개정 2017.04.25)

제76조(인쇄, 출력물통제) ① 개인정보 취급자가 개인정보를 종이 인쇄물로 출력 시 허용된 범위 내에서 출력, 복사가 가능 하며, 관리적, 기술적 보호조치(워터마킹기술)를 해야 한다.

② 개인정보가 포함된 출력, 복사물에는 해당 기관 명칭, 로그, 일련번호, 출력기기 고유 번호, 출력자 성명, 출력시간, 해당 개인정보 파일명 등을 표시하고 출력물관리대장에 기록하여야 한다. (개정 2017.04.25)

③ 디지털 인쇄물의 경우 암호화되고 인가된 사용자만이 복호화 할 수 있도록 불법복제 방지와 세부권한(조회, 편집, 저장, 출력 등)을 부여하여야 하며, 인쇄에 대하여서는 별도 권한(출력권한, 출력가능횟수, 저장기간 등)을 통제하여야 한다. (개정 2017.04.25)

④ 주요문서는 다운로드 및 사용현황, 보안 위배 시도 등 배포된 문서가 폐기되기까지 모든 내역을 수집하고 추적할 수 있어야 한다.

제77조(교육) ① 개인정보 보호책임자는 개인정보보호를 위하여 개인정보 취급자등 구성원에 대한 자체 교육계획을 수립 시행하여야 한다. (개정 2017.04.25)

② 개인정보 보호책임자는 개인정보보안 교육의 효율성을 제고시키기 위하여 자체 실정에 맞는 정보보안 교안을 작성 활용할 수 있으며, 필요시 전문기관에 전문 인력을 활용 또는 전문기관에 위탁할 수 있다. (개정 2017.04.25)

제78조(시행세칙) 개인정보 보호책임자는 개인정보보호 업무를 수행하기 위하여 관련 법령 및 이 규정에 저촉되지 아니하는 범위에서 세부규칙, 지침 등을 정할 수 있다. (개정 2017.04.25)

제6장 정보보안 규정의 유지관리

제79조(규정의 검토) 정보보안책임관은 정보보안 규정의 타당성에 대하여 매년 1회 정기적으로 검토해야 한다.

제80조(규정의 제·개정) 정보보안책임관 관련 법령, 지침 등이 개정된 경우 관련 전문가 및 실무자에 의해 검토된 결과를 정보보안책임관의 승인을 거쳐 위원회의 심의 후 제·개정 하여야한다.

제81조(규정의 예고) 정보보안책임관은 제·개정된 사항을 모든 사용자에게 일정기간 공지하고 유예기간을 고려하여 시행 하여야 한다.

제82조(지침 및 운영에 관한 내규 제정) 이 규정에서 정하지 않은 사항은 관련 법령을 준용하여 내부 지침, 운영 내규 등을 위원회에 심의를 받아 총장의 승인을 득하여 별도로 정할 수 있다.

부칙 (기획예산부-1113, 2011.9.28)

① (시행일) 이 규정은 2011년 09월 28일부터 시행한다. 단 규정의 효력은 시행일 이후 전 구성원에게 2개월간 공지 후 시행한다.
② (예외적용) 이 규정이 명시한 내용일지라도 정보보안 책임관의 승인을 받아 예외로 취급할 수 있다.
1. 기술 환경의 변화로 적용이 불가능한 경우
2. 기술적, 관리적 필요에 따라 규정의 적용을 보류할 긴급한 사유가 있는 경우
3. 재해 등 불가항력적인 상황일 경우
4. 기관의 특성에 따라 적용이 불가능한 경우 정보보안 운영내규를 별도 제정 운영할 수 있다.
③ (경과조치) 정보보안책임관은 특별한 사유에 의하여 이 규정을 충족하지 못한 경우 개선방안이 강구될 때까지 일정기간 유예할 수 있다.

부칙 (기획예산부-177, 2017.4.27)
이 규정은 2017년 04월 25일부터 시행한다.

부칙 (기획예산팀-529, 2018.10.17)
이 규정은 2018년 10월 17일부터 시행한다.

부칙 (기획예산팀-330, 2019.06.25)
이 규정은 2019년 06월 25일부터 시행한다.

부칙 (기획예산팀-257, 2022.04.20.)
이 규정은 2022년 4월 20일부터 시행한다.

[별표 1]

정보시스템 저장매체 자료별 삭제방법

<table>
<tr><th>저장자료
저장매체</th><th>공개자료</th><th>민감자료
(개인정보등)</th><th>비밀자료
(대외비포함)</th></tr>
<tr><td>플로피디스크</td><td>㉮</td><td>㉮</td><td>㉮</td></tr>
<tr><td>광디스크
(CD/DVD등)</td><td>㉮</td><td>㉮</td><td>㉮</td></tr>
<tr><td>자기테이프</td><td>㉮/㉯중 택일</td><td>㉮/㉯중 택일</td><td>㉮</td></tr>
<tr><td rowspan="2">반도체메모리
(EEPROM등)</td><td>㉮/㉰중 택일</td><td>㉮/㉰중 택일</td><td>㉮/㉰중 택일</td></tr>
<tr><td colspan="3">완전포맷이 되지 않는 저장매체는 ㉮ 방법 사용</td></tr>
<tr><td>하드디스크</td><td>㉱</td><td>㉮/㉯/㉰중 택일</td><td>㉮/㉯/㉰중 택일</td></tr>
<tr><td>USB 등 이동식저장매체</td><td>㉱</td><td>㉮/㉯/㉰중 택일</td><td>㉮/㉯/㉰중 택일</td></tr>
</table>

㉮ : 완전파괴(소각/파쇄/용해)

* 비밀이 저장된 플로피디스켓, 광디스크 파쇄시에는 파쇄조각의 크기가 0.25mm 이하가 되도록 조치

㉯ : 전용 소각장비 이용 저장자료 삭제

* 소자장비는 반드시 저장매체의 자기력보다 큰 자기력 보유

㉰ : 완전삭제장비 이용 저장자료 삭제

* 저장매체 전체를 “난수, 0, 1”로 각각 중복 저장하는 방식으로 삭제

㉱ : 완전포맷 1회 수행

* 저장매체 전체를 난수로 중복 저장하는 방식으로 삭제