# 상지대학교 정보보안에 관한 규정

제정 2011. 9. 28.
제5차 전부개정 2024. 2. 27.

## 제1장 총칙

**제1조(목적)** 상지대학교의 정보보안 규정은 다음 각 호의 사항을 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 소관 업무와 관련된 정보보호에 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 '본교'라 한다)에 적용한다.

② 본교의 컴퓨터에 의하여 처리되는 개인정보보호에 대하여 관련 지침 등에 규정되어 있을 경우에는 해당 규정이나 지침에 따른다. 다만, 타 법령에 의해 적용되는 경우에는 타 법령, 지침에 따른다.

③ 정보보호에 대한 책임과 의무는 본교의 전산 자원을 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. "본교 웹 사이트"(이하 '웹 사이트'라고 한다)라 함은 본교에서 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. "정보보안담당관"이라 함은 정보보호업무를 총괄하는 부서의 장을 말한다.
5. "정보시스템 사용자"(이하 '사용자'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 장소로서 자료 보관실을 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, 보관되어 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, 웹 사이

트, 통신망 등에 필요한 중요자료를 보호하기 위하여 사이버안전기술이 적용된 프로그램이나 장치 등을 말한다.

12. “휴대용 저장매체”라 함은 디스켓, CD, 하드디스크, USB 메모리 등 자료를 저장할 수 있는 것으로 정보통신시스템과 분리할 수 있는 기억장치를 말한다.
13. “휴대용 저장매체 관리책임자”(이하 ‘관리책임자’라 한다)라 함은 각 소속 부서 및 단체의 장을 말한다.
14. “휴대용 저장매체 취급자”(이하 ‘취급자’라 한다)라 함은 해당 휴대용 저장매체를 사용하는 자를 말한다.
15. “휴대용 저장매체 관리시스템”(이하 ‘관리시스템’이라 한다)이라 함은 보조기억매체의 등록파기, 재사용, 반출, 반입, 불용처리 현황 등에 관하여 전자적으로 처리하는 시스템을 말한다.
16. “저장매체”라 함은 자기저장장치, 광 저장장치, 반도체 저장장치 등 자료기록이 가능한 전자장치를 말한다.
17. “소자”라 함은 저장매체에 역자기장을 이용해 매체의 자화값을 0으로 만들어 저장자료의 복원을 불가능하게 만드는 것을 말한다.
18. “완전삭제”라 함은 저장매체 전체의 데이터가 어떠한 방법으로도 복구 불가하도록 수행하는 것을 말한다.
19. “저장매체 완전삭제장비”(이하 ‘완전삭제장비’이라 한다)라 함은 저장매체의 자료를 복구 불가능하게 완전 삭제하는 국가정보원이 인증한 장비를 말한다.
20. “무선통신망”이라 함은 무선접근(무선랜, 휴대폰, 스마트폰, PDA, 태블릿 PC 등)이 가능한 기기와 통신장비 및 통신망을 말한다.

## 제2장 조직

**제4조(책임)** 본교의 정보보안에 관한 책임은 총장에게 있다.

**제5조(조직)** ① 총장은 학술정보원장을 정보보안담당관으로 임명하고 각 소속 부서 및 단체의 장을 분임정보보안담당관으로 임명하여야 한다. 다만, 별도로 임명하지 않는 경우 당연직으로 임명한 것으로 본다.

② 정보보안담당관은 정보보안담당자(정보보안 실무책임자)와 정보보안실무자(정보보안 실무운영자)를 지정한다.

③ 정보보안에 관한 업무의 전담부서는 학술정보원 전산정보팀으로 한다.

**제6조(임무)** ① 정보보안담당관의 임무는 다음 각 호와 같다.

1. 정보보호에 관한 지휘 감독
2. 정보보안 정책 및 규정의 검토
3. 정보보안 대책의 수립
4. 정보보호에 관한 감사 및 의견 제시
5. 정보자산 신·증설 시 보안대책 수립 및 보안성 검토
6. 정보보안 침해사고 조사, 처리, 대응
7. 사이버 위협정보 수집, 분석, 경보발령 및 보안관제
8. 외부 유관기관과 협력 창구 마련
9. 기타 정보보안을 위해 필요한 사항

② 전산정보팀의 업무는 다음 각 호와 같다.

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. 정보보안 위규 적발 및 사고조사 처리
11. 소관분야 정보보안 업무조정 및 감독
12. 기타 정보보안 관련 사항

## 제3장 위원회

**제7조(구성)** ① 총장은 체계적이고 효율적인 보안정책 수립, 심의 및 관리를 위하여 정보보안심사위원회(이하 '위원회'라 한다)를 둔다.
② 위원회는 정보보안담당관을 위원장으로 하며 위원장을 포함하여 7인 내외의 위원으로 구성한다.
③ 위원회는 학술정보원장, 기획처장을 당연직으로 하되, 정보보안담당관이 필요로 하는 경우 외부 보안전문위원을 포함할 수 있다.
④ 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.

**제8조(기능)** 위원회는 제1조의 목적을 달성하기 위하여 다음 각 호의 사항을 심의 · 의결한다.
1. 정보보호 정책 및 총괄 계획 수립에 관한 사항
2. 정보보안사고 처리에 관한 주요 사항
3. 정보보안교육 계획 및 정보보안 준수사항 감사 계획 수립에 관한 사항
4. 정보보안 관련 심의요청에 관한 사항
5. 본 위원회 규정의 제 · 개정 및 운영에 관한 사항
6. 기타 정보보안담당관이 인정하는 정보보안에 필요한 제반사항

**제9조(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 날인하여야 하며, 위원회 심의 · 의결된 사항은 총장에게 보고한다.
④ 이 규정에 명시되지 아니한 세부 운영에 관한 사항은 위원회의 심의를 거쳐 위원장이 정한다.

## 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 보안등급을 지정하여야 하며, 세부사항은 「상지대학교 정보보안 기본지침」으로 정한다.

**제12조(정보자산관리)** 정보보안담당관는 정보자산목록을 작성 관리하여야 하며 정기적으로 정보자산을 점검하여 최신성을 유지하여야 한다.

**제13조(정보자산의 도입)** ① 정보보안담당관은 보안시스템 및 소프트웨어의 도입 시 안전성과 침해사고 방지를 위하여 규정된 구매절차와 보안성에 대한 검토를 실시하여야 하며, 필요시 위원회 심의를 거친다. 다만, 공신력 있는 기관의 인증된 제품에 대하여 생략할 수 있다.
② 본교에서 보안성 검토를 시행하여야 하는 정보화 사업과 관련한 세부사항은 「상지대학교 정보보안 기본지침」으로 정한다.
③ 정보보안담당관은 정보자산 중 보안시스템과, 기밀시스템, 개인정보처리시스템 등의 상시 모니터링이 가능하여야 하며, 비인가자의 불법접근, 인가자의 오·남용을 방지하기 위하여 물리적인 출입통제가 시행되도록 한다.
④ 정보보안담당관은 보안시스템의 본래 도입 목적에 맞게 설치 및 사용하여야 하며 허가 없이 변경할 수 없다.

**제14조(정보자산 폐기 또는 매각)** ① 정보자산의 폐기 또는 매각 시 저장매체는 완전포맷 또는 저장매체 완전파기 시스템을 통하여 복구 불가능하도록 하여야 한다.
② 백업 미디어와 같은 기록매체는 폐기 전 데이터 삭제 및 포맷 후 폐기하며, 필요시 물리적으로 완전파기 하여야 한다.
③ 하드웨어의 매각 폐기는 반출 전 모든 구성정보, 로그정보, 비밀번호 등을 초기화 또는 삭제 하여야 한다.
④ 개인정보가 포함된 문서 또는 정보자산 운영에 필요한 문서는 파쇄 또는 완전 소각하여야 하며, 폐기 전문 업체를 통하여 매각할 경우 정보유출과 관련한 보안사항을 계약서에 명시하여야 한다.

### 제2절 보안교육

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

**제16조(보안교육)** ① 정보보안담당관은 전체 교직원을 대상으로 하는 정보보안 교육을 매년 정기적으로 실시하며 필요시 비정기적 교육을 실시할 수 있다.
② 정보보안담당관은 교직원의 채용, 전보 시 직무와 관련된 정보보안 교육을 실시한다.
③ 정보보안담당관은 외부자에 대한 정보보안 교육 시 정보보안 담당부서와 업무주관부서의 협의에 따라 시행한다.
④ 정보보안담당관은 다음 각 호에 따른 정보보호 교육내용을 업무 특성에 맞게 교육하여야 한다.
1. 정보보안 정책, 규정
2. 정보보안 관련 법률
3. 업무용 PC 보안
4. 외부자 교육, 보안요구사항 계약 시 준수사항 등
5. 정보보호 윤리
6. 기타 보안관련 사항

⑤ 정보보안담당관은 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)** 외부자 관리와 감독의 책임은 주관부서에 있으며, 정보보안담당관은 외부자의 정보보안 준수사항에 대한 이행여부에 대하여 지도, 감독, 감사할 수 있다.

**제18조(보안서약)** ① 외부자가 법인일 경우 대표자의 보안서약서 이외에도 업무를 수행할 개인에 대하여 보안서약서를 작성하여야 한다.

② 보안서약서를 작성한 외부자는 본교 직원과 동일한 정보보안 책임과 의무를 가진다.

**제19조(외부자 접근통제)** ① 외부자는 본 대학교 시스템에 접근할 경우, 별도 사용자 계정을 발급 받아야 한다.

② 정보보안담당관이 운영 중인 정보시스템의 접근을 승인한 경우 이용시간과 작업시간을 제한하여 접근 통제할 수 있다.

③ 정보보안담당관은 외부자가 업무에 필요한 정보만 접근할 수 있도록 통제하며 필요 이상의 접근권한을 설정하지 않도록 한다.

④ 정보보안담당관은 외부자에게 원격접근을 허용한 경우 접근통제관리 및 모니터링하고 그 기록을 일정기간 보관하여야 한다.

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

**제20조(외부자의 장비 반·출입)** ① 정보보안담당관은 외부자 소유의 정보자산의 반·출입을 제한한다. 다만, 정보보안담당관이 승인을 득한 경우는 예외로 한다.

② 정보보안담당관은 정보자산의 반·출입에 대한 이력을 관리하여야 한다.

### 제4절 물리적 보안

**제21조(보호구역의 지정)** 총장은 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 : 정보보안담당관

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 동행하여야 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 방재 설비
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 자가 발전기를 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 정보보안 감사

**제24조(정보보안 감사)** ① 정보보안담당관은 제9조의 규정에 따라 매년 정기적 또는 비정기적으로 자체 정보보안 감사 계획을 수립하여 정보보안 감사를 실시하여야 한다.
② 정보보안담당관은 보안감사 또는 불시점검은 업무 수행 시 발생할 문제점 파악에 중점을 두고 실시하여야 하며 도출된 취약요인은 근본적인 대책을 수립하여 시행하여야 한다.
③ 정보보안담당관은 총장에게 정보보안 감사 실시계획과 감사 결과를 제출하여야 한다.
④ 정보보안담당관은 정보보안 감사의 효율적 수행을 위하여 각 처, 원, 실, 센터, 단, 부, 팀의 업무협조를 요청할 수 있다.

**제25조(정보보안 감사위원 구성)** ① 정보보안담당관은 정보보안 감사를 실시하기 위하여 전산분야 전문가로 5인 이내 감사위원을 구성하며 감사위원장은 정보보안담당관으로 한다.
② 정보보안담당관은 객관성과 전문성이 필요하다고 인정되는 경우 감사위원 중 외부 전문가를 포함하거나 위탁할 수 있다.

**제26조(정보보안 감사 결과 기록)** ① 정보보안담당관은 감사 결과를 문서화하여 보관하여야 한다.
② 정보보안담당관은 총장 또는 외부 감독기관의 요청이 있는 경우 정보보안 감사 결과를 제출할 수 있다.
③ 정보보안담당관은 정보보안 감사를 외부 전문가를 활용하거나 위탁한 경우 외부전문가 감사보고서로 대체할 수 있다.

## 제5장 정보보안 규정의 유지관리

**제27조(규정의 검토)** 정보보안담당관은 정보보안 규정의 타당성에 대하여 매년 1회 정기적으로 검토하여야 한다.

**제28조(규정의 제·개정)** 정보보안담당관은 관련 법령, 지침 등이 개정된 경우 관련 전문가 및 실무자에 의해 검토된 결과를 정보보안담당관의 승인을 거쳐 위원회의 심의 후 제·개정 하여야한다.

**제29조(규정의 예고)** 정보보안담당관은 제·개정된 사항을 모든 사용자에게 일정기간 공지하고 유예기간을 고려하여 시행하여야 한다.

**제30조(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** (기획예산팀-511, 2024.02.27.)

**제1조(시행일)** 이 규정은 2024년 2월 27일부터 시행한다.

**제2조(예외적용)** ① 이 규정이 명시한 내용일지라도 다음 각 호의 어느 하나에 해당하는 경우 정보보안담당관의 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

② 기관의 특성에 따라 적용이 불가능한 경우 정보보안 운영내규를 별도 제정 운영할 수 있다.

**제3조(경과조치)** 정보보안담당관은 특별한 사유에 의하여 이 규정을 충족하지 못한 경우 개선방안이 강구될 때까지 일정기간 유예할 수 있다.