

대구예술대학교 보안관리규정

(제정 2010.09.10. 교무위원회)

(개정 2019.06.20. 교무위원회/자구수정)

(개정 2020.03.09. 교무위원회/자구수정)

제 1 장 총칙

제1조 (목적) 본 지침은 「보안업무규정」(대통령령), 「정보 및 보안업무 기획·조정규정」(대통령령), 「국가사이버안전관리규정」(대통령훈령), 및 국가정보원의 「국가정보보안기본지침」에 의거 대구예술대학교의 보안활동에 필요한 세부사항 규정을 목적으로 한다.

제2조 (적용범위) 이 규정은 우리 대학교 내 정보자산과 해당 자산을 관리·운영하는 우리 대학교 교직원 및 우리 대학교 운영을 위해 종사하는 외부업체 직원에게 모두 적용된다.

제3조 (용어정의) 이 규정에서 사용되는 용어정의는 다음과 같다.

1. “보안”이라 함은 인원·문서·자재·시설·정보시스템 등을 관리, 보호하기 위하여 강구하는 일체의 행위를 말한다.
2. “정보보호”라 함은 정보통신수단으로 수집·처리·가공·저장·검색·송수신되는 정보의 유출·위변조·훼손 등을 방지하거나 정보통신망을 보호하기 위하여 관리적, 물리적, 기술적 수단을 강구하는 일체의 행위를 말한다.
3. “정보통신망”이라 함은 유·무선을 매개로 하는 다양한 정보통신 수단에 의하여 부호·문자·음향·영상 등의 정보를 수집·가공·저장·검색·송수신하는 정보 통신체제를 말한다.
4. “정보보안” 또는 “정보보호”라 함은 정보통신수단으로 수집·가공·저장·검색·송수신 되는 정보의 유출·위변조·훼손 등을 방지하거나 정보통신망을 보호하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위를 말한다.
5. “국가용 정보보안시스템(이하 ‘보안시스템’이라 한다)”이라 함은 국가정보원장(이하 ‘국정원장’이라 한다)이 기밀 등 중요자료를 보호하기 위하여 승인한 암호장비·암호자재 또는 암호논리·사이버안전기술이 적용된 프로그램이나 장치 등을 말한다.
6. “보안적합성 검증필 정보보호시스템(이하 ‘검증필 정보보호시스템’이라 한다)”이라 함은 상용 정보보호시스템 중 국정원장이 각급기관에서 사용하는 것이 적합하다고 승인한 것을 말한다.
7. “정보통신실”이라 함은 서버·PC 등 전산장비와 스위치·교환기·라우터 등 통신 및 전송장비 등이 설치 운영되는 장소를 말하며, 전산실·통신실 및 전산자료 보관실 등을 말한다.
8. “전산자료”라 함은 전산장비에 의하여 전자기적인 형태로 입력·보관되어 있는 각종 정보(data)를 말하며, 그 자료가 입력되어 있는 자기테이프, 디스크 등 보조기억매체를 포함한다.
9. “정보보안측정”이라 함은 해킹·컴퓨터바이러스, 도청 등 각종 위협요소로부터 정보통신망에 대한 정보보안 취약성을 진단하기 위한 제반활동을 말한다.
10. “보조기억매체”라 함은 디스켓·CD·하드디스크·USB 메모리 등 자료를 저장할 수 있는 것으로 정보통신시스템과 분리할 수 있는 기억장치를 말한다.

11. “사이버공격”이라 함은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스 방해 등 전자적 수단에 의하여 국가정보통신망을 불법 침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 말한다.
12. “사이버안전”이라 함은 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 말한다.
13. ‘보조기억매체 관리책임자’라 함은 각 부처 또는 과별 보조기억매체 관리상의 책임을 맡은 그 팀장 또는 과장, 계장을 말한다.
14. ‘보조기억매체 취급자’라 함은 해당 보조기억매체를 사용하는 자를 말한다.
15. ‘보조기억매체 관리시스템’이라 함은 보조기억매체의 등록, 파기, 재사용, 반출·입, 불용 처리 현황 등에 관하여 전자적으로 처리하는 시스템을 말한다.
16. 공인인증서보관용 보조기억매체 중 ‘업무용’ 이라 함은 업무와 관련하여 신분확인 등에 활용되는 것을 말한다.
17. 공인인증서보관용 보조기억매체 중 ‘개인용’ 이라 함은 인터넷 뱅킹 등 사적인 목적으로 활용되는 것을 말한다.
18. “저장매체”란 자기저장장치·광 저장장치·반도체 저장장치 등 자료기록이 가능한 전자장치를 말한다.
19. “정보시스템”이라 함은 정보의 수집·가공·저장·검색·송신·수신에 활용되는 전자기기와 소프트웨어의 조직화된 체계를 말하며, 저장매체를 내장한 복사기·팩스 등 사무용 기기를 포함한다.
20. “완전포맷”이라 함은 저장매체 전체의 자료저장 위치에 새로운 자료(0 또는 1)를 중복하여 저장하는 것을 말한다.
21. “지도감독 기관”이라 함은 대구예술대학교의 지도 감독을 하는 교육과학기술부를 말한다.

제 2 장 조직

제4조 (최고보안책임관) ① 최고보안책임관은 우리 대학교의 보안 및 정보보호 업무를 전담·총괄하며 각 부서(팀)별 보안 및 정보보호 업무를 지도·감독한다.

② 최고보안책임관은 교무처장이 보직과 동시에 당연 임명된다.

제5조 (보안담당관) ① 보안담당관은 사무처 총무팀장이 보직과 동시에 당연 임명된다.

(개정 2020.03.09.)

② 보안담당관은 다음 각 호의 업무를 담당한다.

1. 연도별 보안업무추진계획 수립 및 심사분석(보안관련 주요 성과 및 실적 분석)
2. 보안(인원, 시설, 문서, 자재 등 일반보안) 진단
3. 보안교육(일반보안 및 보안인식 교육)에 관한 사항
4. 비밀소유 및 취급인가자 현황 조사
5. 보안서약의 집행
6. 시설보안 및 보호구역 관리 등

- 7. 보안규정 수립(지침·절차서 총괄) 및 보안업무 기획·조정
- 8. 보안업무 지도, 감독 및 개선 대책 수립
- ③ 제1항의 경우에도 불구하고 보안담당관이 교체되었을 경우에는 교체 후 7일 이내에 총장 임회하에 인계인수를 하여야 한다.

제6조(정보보호담당관) ① 정보보호담당관은 학술정보원 전산운영팀장이 보직과 동시에 당연 임명된다.(개정 2020.03.09.)

② 정보보호담당관은 다음 각 호의 업무를 담당한다.

1. 정보보안 정책 및 활동 세부계획 수립·시행
2. 정보보안 감사·지도점검 실시
3. 취약 정보통신망 보안대책 수립 추진
4. 정보보안 위규적발 강화 및 사고조사 처리
5. 산하기관에 대한 정보보안 업무조정 및 감독
6. 사이버위협정보 수집·분석 및 보안관제
7. 사이버공격 관련 경보 발령시 대응활동
8. 침해사고 대응·복구
9. 정보보안수준 평가·관리
10. 정보보안 교육계획 수립·시행
11. 정보보안업무 심사분석 시행
12. 도청 위해요소 제거
13. 정보보안 관련 규정·지침 등 제·개정
14. 기타 정보보안 관련 사항

제7조 (분임보안담당관) 각 부서의 팀장은 분임보안담당관으로서 해당 부서의 보안 및 정보보호 업무를 전담·총괄하며 보안담당관 및 정보보호담당관의 업무요청에 협조할 수 있다. (개정 2020.03.09.)

제 3 장 보안심사위원회

제8조 (보안심사위원회) ① 보안업무의 효율적인 운영과 보안에 관한 중요한 사항을 심의하기 위하여 보안심사위원회(이하, “위원회”라 한다.)를 정한다.

② 위원회는 다음 각 호의 사항을 심의한다.

1. 보안 관련 규정의 수립 및 그 개정에 관한 사항
2. 분야별 보안대책의 수립에 관한 사항
3. 신원특이자의 임용 등 인사관리에 관한 사항
4. 보안위규자의 심사 및 처리에 관한 사항
5. 연간보안업무 지침수립과 그 이행상태의 확인처리에 관한 사항
6. 보안업무심사분석 및 보안업무 수행상 조정과 협의를 요하는 사항
7. 보안성 검토에 관한 사항
8. 기타 위원장이 필요하다고 인정하는 사항

③ 위원회의 운영은 별도로 정하는 바에 따른다.

제9조 (위원회 구성) ① 위원회는 위원장을 포함하여 5인 이상으로 구성한다.

② 위원장은 회의의 의장으로서 최고보안책임관이 되며 위원회의 회무를 통할하며 위원회를 대표한다.

③ 위원장이 부득이한 사유로 직무를 수행할 수 없는 경우에는 위원장이 위원 중에서 지명한 자가 그 직무를 대행한다.

④ 위원은 각 처장과 학술정보원장을 당연직 위원으로 하고, 당연직이 아닌 위원은 위원장이 위촉한다.

⑤ 위원회의 사무를 처리하기 위하여 간사 1인을 두되, 간사는 보안담당관이 된다.

⑥ 위원회의 회의를 소집하고자 하는 때에는 회의일시·장소 및 부의사항을 회의개최 7일 전까지 각 위원에게 서면 또는 전자문서로 통지해야 한다. 다만, 긴급을 요하거나 부득이한 사유가 있는 경우에는 그러하지 아니하다.

제 4 장 보안 업무

제10조 (보안점검) ① 우리 대학교의 각 부서에서는 보안업무 수행 시 관련 규정 및 지침을 준수하여야 한다.

② 보안점검은 보안담당관이 주관이 되어 실시하는 것을 원칙으로 하며, 보안점검 수행 조직에는 외부에서 기술지원을 받을수 있다.

③ 보안담당관은 연 1회 이상의 보안점검을 실시하며, 정보보호관리체계 전 부분이 포함되도록 점검을 시행하여야 한다.

④ 보안담당관은 보안점검의 목적, 대상, 방법 및 실시 시기 등을 포함하는 연간 보안점검 계획을 수립하여야 한다.

⑤ 연간 보안점검 계획에 의해 보안점검 또는 특별, 정기점검을 실시할 때에는 “정보보호관리체계 점검항목(별표 1)”을 기준으로 보안점검 계획을 수립·시행한다.

제11조 (보안점검 보고 및 조치) ① 보안담당관은 점검을 위한 취약점 점검 도구, 보안점검항목 등의 점검 시 사용되는 소프트웨어 및 점검항목 원문은 접근통제를 철저히 하여 기밀성·무결성·가용성을 보호하여야 한다.

② 보안담당관은 보안점검 수행 후 보안점검결과보고서는 다음 각 호의 사항을 포함하여 작성하여야 한다.

1. 보안점검의 범위
2. 보안점검의 실시방법
3. 부적합사항 및 조치 계획

제 5 장 정보보안관리

제12조 (정보보안 교육) ① 정보보안 교육계획을 수립하고 년2회 이상 시행하여야 한다.

② 정보보안교육의 효율성을 제고시키기 위하여 정보보안 교안을 작성 활용하여야 한다.

③ 제1항에 의한 교육계획 수립 시 정보보안담당관이 최신 정보보안 정책 및 기술 등을 습득하기 위하여 국가에서 인증하는 기관에서 개설하는 정보보안 관련 교육과정을 이수하는 내용을 포함할 수 있다.

제13조 (비상통신 보안대책) 전시 또는 비상사태 발생에 대비하여 비상통신망을 운영하고 있거나 중요한 정보통신시설을 관리 감독하는 기관의 장은 평상시 이에 대한 정보통신보안 대책을 강구하여야 한다.

제14조 (전산자료 보안관리) ① 전산자료에 대한 유출이나 파괴 또는 변조 등에 대비하여 다음 각 호에 정하는 보호대책을 강구하여야 한다.

1. 자료복사본(예비) 확보 및 안전지역 별도 보관
2. 전산자료(보조기억매체) 보유현황 관리
3. 전산자료 및 장비의 반출 또는 반입 통제
4. 불법접근 및 컴퓨터바이러스(이하 '악성코드'라 한다) 피해 예방
5. 전산자료 접근권한 구분·통제
6. 예비(Back up)체계 수립·시행

② 보조기억매체를 활용하는 부서의 보안담당자는 월1회 이상 보유현황 및 관리실태를 점검하고 관리책임자의 확인을 받아야 한다.

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

제15조 (정보통신망 관련자료 관리) ① 다음 각 호의 자료를 대외비로 분류하여 관리하여야 한다. 다만, 국가안보와 직결되는 중요한 정보통신망 관련 세부자료는 해당 등급의 비밀로 분류 관리하여야 한다.

1. 정보통신망 세부 구성현황(IP 세부 할당현황 포함)
2. 중요 보안시스템 운용현황
3. 보안취약성 분석·평가 결과물
4. 기타 보호할 필요가 있는 정보통신망 관련 자료

② 제1항의 명시되지 않은 정보통신망 관련 자료의 분류 관리는 국정원장이 제정한 「비밀 세부분류지침」(대외비)을 따른다.

제16조 (비공개자료 보호) ① 정보보안과 관련된 행정정보는 비공개로 분류·관리한다.

② 소속직원 중 비밀 및 중요업무 담당자의 인적사항, 세부 담당업무와 전자우편 주소 등을 인터넷 등에 공개하여서는 아니 된다.

③ 제1항 및 제2항의 경우에도 불구하고 지도감독기관의 장과 공개범위·요건 등을 사전 협의하여 관련내용을 공개할 수 있다.

제17조 (재난복구 대책) ① 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애 발생에 대비하여 시스템 이원화, 백업관리, 복구 등 종합적인 재난복구 대책을 수립·시행하여야 한다.

② 재난복구 대책을 정기적으로 시험하고 검토해야 하며 업무 연속성에 대한 영향평가를 실시하여야 한다.

③ 정보통신망 장애에 대비한 백업시설을 확보하고 정기적으로 백업을 수행하여야 한다.

④ 제3항에 의거 백업시설을 설치할 경우에는 정보통신실과 물리적으로 일정거리 이상 위치한 안전한 장소에 설치하여 재난에 대비하여야 한다.

제18조 (PC 보안관리) ① 단말기를 포함한 PC 등을 사용하고자 할 경우에는 사용자 및 관리 책임자를 지정하여야 한다.

② 비인가자가 PC를 무단으로 조작하여 전산자료를 유출, 위·변조 및 훼손시키지 못하도록 다음 각 호에 정한 보호대책을 강구하여야 한다.

1. 장비별·자료별·사용자별 비밀번호 사용
2. 10분 이상 PC 작업 중단시 화면보호 조치
3. 백신 및 PC용 침입차단시스템 등 운용
4. P2P 등 업무와 무관하거나 보안에 취약한 프로그램의 사용 금지
5. 실습용 PC의 경우 제1항과 제2항의 적용을 받지 아니한다.

③ 정보보안담당관은 PC를 교체·반납·폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 하드디스크에 수록된 자료가 유출, 훼손되지 않도록 보안조치를 하여야 한다.

④ PC에 적용되는 사용자계정(ID) 및 비밀번호의 취급관리는 제19조(사용자계정 관리)의 지침을 준용한다.

⑤ 정보보안담당관은 해당기관의 업무용 노트북 PC, PDA 등 휴대용 단말기의 운용현황을 파악하여 관리하고, 해당부서 장은 반출 또는 반입시 최신 백신을 활용하여 해킹프로그램 및 웜·바이러스 감염여부를 점검하여야 한다.

⑥ 개인소유의 PC(노트북 PC 등)는 각급기관 내부로 반출 또는 반입하여 사용하여서는 아니 된다. 다만, 부득이한 경우에는 해당부서 장의 책임 하에 보안조치를 한 후 반출·반입할 수 있으며, 정보보안담당관에게 통보하여야 한다.

제19조 (사용자계정 관리) ① 사용자계정(ID)은 비인가자 도용 및 정보통신시스템 불법접속에 대비하여 다음 각 호의 사항을 반영하여 관리하여야 한다.

1. 사용자별 또는 그룹별로 접근 권한 부여
2. 외부 사용자의 계정부여는 불허하되 부득이한 경우에는 유효기간을 설정하는 등 보안조치강구한 후 허용
3. 비밀번호가 없는 사용자계정은 사용 금지

② 시스템관리자는 사용자계정의 등록·변경·폐기시 정보보안담당관에 그 결과를 보고하여야 한다.

③ 3회에 걸쳐 사용자인증 실패시 정보통신시스템 접속을 중지시키고 비인가자 침입 여부를 확인 점검하여야 한다.

④ 시스템관리자는 퇴직 또는 보직변경 등으로 사용하지 않는 사용자 계정이 발생할 경우 이를 신속히 삭제하여야 한다.

제20조 (비밀번호 관리) ① 비밀번호는 정보통신시스템의 무단사용 방지를 위하여 다음과 같이 구분 사용하여야 한다.

1. 비인가자의 정보통신시스템 접근방지를 위한 장비 접근용 비밀번호(1차)
2. 정보통신시스템 사용자가 서버 등 정보통신망 접속시 인가된 인원인지 여부를 확인하는 사용자인증 비밀번호(2차)

3. 문서에 대한 열람·수정 및 출력 등 사용권한을 제한할 수 있는 자료별 비밀번호(3차)
- ② 비밀이나 중요자료에는 반드시 자료별 비밀번호를 부여하되, 공개 또는 열람 자료에 대해서는 부여하지 아니할 수 있다.
- ③ 비밀번호는 다음 각 호 사항을 반영하여 숫자와 문자, 특수문자 등으로 7자리 이상으로 정하고 분기1회 이상 주기적으로 변경 사용하여야 한다.
1. 사용자계정(ID)과 동일하지 않은 것
 2. 개인 신상 및 부서명칭 등과 관계가 없는 것
 3. 일반 사전에 등록된 단어는 사용을 피할 것
 4. 동일단어 또는 숫자를 반복하여 사용하지 말 것
 5. 이미 사용된 비밀번호는 재사용하지 말 것
 6. 동일 비밀번호를 여러 사람이 공유하여 사용하지 말 것
 7. 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지
- ④ 서버에 등록되어 있는 비밀번호는 암호화하여 보관하여야 하고, 단말기·PC 등의 비밀번호를 종합기록 관리하고자 할 경우에는 전산장비 관리대장에 등재하여 대외비 이상으로 분류 관리하여야 한다.

제21조 (‘사이버보안 진단의 날’ 운영) ① 매월 셋째주 수요일을 ‘사이버보안 진단의 날’로 지정·운영하여야 한다.

- ② 정보보안담당관은 ‘사이버보안 진단의 날’에 소관 정보통신망을 대상으로 악성코드 감염여부와 정보통신시스템의 보안 취약여부 등을 진단, 문제점을 발굴 개선하여야 한다.
- ③ 제1항 및 제2항에 따라 보안취약성을 발굴·개선한 실적을 정보보안담당관에게 보고하여야 한다.

제22조 (웹서버 등 공개서버 관리) ① 외부인에게 공개할 목적으로 설치되는 웹서버 등 각종 공개서버는 보안적합성이 검증된 침입차단·탐지시스템을 설치하는 등 보안대책을 강구하여야 한다.

- ② 서버에 접근할 수 있는 사용자계정을 제한하며 불필요한 계정은 삭제하여야 한다.
- ③ 홈페이지 게재내용은 비밀내용 등 비공개 자료가 포함되지 않도록 하여야 한다.
- ④ 공개서버는 업무서비스를 제외한 모든 서비스 및 시험·개발도구 등의 사용을 제한하도록 보안기능을 설정하여야 한다.
- ⑤ 공개서버의 보안취약성을 수시로 점검하고, 자료의 위·변조, 훼손 여부를 확인하여야 한다.
- ⑥ 보안 사고에 대비하여 서버에 저장된 자료의 철저한 백업체계를 수립·시행하여야 한다.
- ⑦ 공개서버를 통해 개인정보가 유출, 위·변조 되지 않도록 보안조치를 하여야 한다.

제23조 (외부 용역사업 보안관리) ① 정보화사업 및 보안컨설팅 수행 등 외부 용역사업을 추진할 경우 보안성 검토를 하여야 한다.

- ② 제1항에 의한 용역사업 계약 시 계약서에 용역사업 참여직원의 보안준수 사항과 위반 시 손해배상 책임 등을 명시하여야 한다.
- ③ 비밀 관련 용역사업을 수행할 경우, 외부인원에 대한 비밀취급인가 등 보안조치를 수행하여야 한다.

- ④ 정보통신망도·IP현황 등 용역업체에 제공할 자료는 자료 인계인수대장을 비치, 보안 조치 후 인계인수하고 무단 복사·외부반출을 금지한다.
- ⑤ 정보보안담당관은 용역 참여직원을 대상으로 보안교육 및 보안점검을 실시하여야 한다.
- ⑥ 정보보안담당관은 용역 참여직원이 노트북 등 관련 장비를 반출 또는 반입할 때마다 악성코드 감염여부, 자료 무단반출 여부를 확인하는 등 보안조치를 하여야 한다.
- ⑦ 정보보안담당관은 용역사업 종료 시 외부업체의 노트북·보조기억매체 등을 통해 기관 내부자료 및 용역 결과물이 유출되는 것을 방지하기 위하여 복구가 불가능하도록 완전 소거하는 등 보안조치를 하여야 한다.
- ⑧ 용역업체로부터 용역 결과물을 전량 회수하고 비인가자에게 제공·대여·열람을 금지하는 등 관리를 철저히 한다.

제 6 장 문서보안

제1절 문서등급 분류

제24조 (등급분류의 기준) ① 보안담당관 및 정보보호담당관은 문서자료를 중요도에 따라 다음 각 호와 같이 4단계로 분류하여 관리한다.

1. 비밀

가. 「보안업무규정시행세칙(교육과학기술부)」에 따라 분류된 III급 이상의 비밀

나. 비밀취급인가자 이외의 접근이 통제되어야 하는 것

다. 보안담당관에 의하여 「보안업무규정시행세칙(교육과학기술부)」에 따라 분류·관리하여야 함

2. 대외비

가. 중요 시설 및 정보통신망의 구조 등에 관한 세부정보 및 개인정보가 대량으로 집적되어 있는 문서 및 전산자료로서 해당 업무 이외의 자에게 배포 및 유출이 제한되는 문서

나. 해당 업무 이외의 자에게는 접근이 통제되어야 하는 것

다. 보안담당관 및 정보보호담당관에 의하여 본 규정에 따라 분류·표시하며 비밀에 준하여 보관·관리하여야 함

3. 비공개

가. 우리 대학교 외부로의 배포 및 유출이 제한되는 문서

나. 우리 대학교 교직원 이외의 자에게 접근이 통제되어야 하는 것

다. 별도의 분류·표시 없이 우리 대학교 내에서 보관·관리할 수 있음

4. 공개

가. 우리 대학교 외부 및 일반에 배포될 수 있는 문서

나. 문서 생산자가 자유롭게 취급·관리할 수 있음

다. “공개자료”로 분류·표시·관리할 수 있음

- ② 각 부서장은 문서자료의 분류 및 관리책임이 있다.
- ③ 문서보안관리의 자세한 사항은 「정보보호관리체계 지침」에서 별도로 정한다.

제2절 비밀자료 보안

제25조 (비밀의 취급) 비밀을 취급하는 자는 비밀의 안전관리를 위하여 「보안업무규정」, 「보안업무시행규칙」 및 「보안업무규정시행세칙(교육과학기술부)」에 따른 보안조치를 취하여야 한다.

제26조 (비밀취급의 한계) 비밀취급인가자라 할지라도 인가받은 비밀등급보다 상위 등급의 비밀 및 업무상 관계가 없는 비밀을 취급할 수 없다.

제27조 (비밀세부분류지침) 비밀의 세부분류는 보안담당관이 분류함을 원칙으로 하되 그 내용을 정확히 분류할 수 없을 때에는 위원회의 심의를 거쳐 분류하여야 한다.

제28조 (비밀자료 보안관리) ① 각 해당 부서의 담당자는 비밀 및 대외비로 분류된 문서자료에 “라벨링 표시” 및 “비밀관리기록부를 작성하여 내화금고에 보관한다.

② 보안담당관은 한 학기에 최소 1회 이상 비밀을 검토하여야 하며, 관련 사항을 총장에게 보고하여야 한다.

③ 비밀 및 대외비는 각 해당 부서(팀)에서 총괄 보관 관리하여 비밀의 일체 관리사항을 기록하기 위하여 “비밀열람기록전”을 작성 비치하여야 한다.

④ 비밀 및 대외비 파기는 소각·용해 또는 기타 방법으로 원형을 완전히 소멸시켜야 한다. 파기가 끝나면 즉시 비밀관리기록부의 파기란에 파기 집행자가 일시를 기입한 후 파기 확인란에는 입회자의 확인을 받아 파기 사실을 증명토록 하여야 한다.

⑤ 비밀 및 대외비로 출력된 자료는 외부로 유출되지 않도록 취급관리 하여야 하며 부득이하게 외부에 제공해야 할 경우 보안담당관에게 자료 검토 후 이루어져야 한다.

⑥ 비밀의 세부분류 기준 및 기타 세부사항은 「보안업무규정시행세칙(교육과학기술부)」 제26조(비밀 세부분류 지침)에 따른다.

제29조 (정보통신 자료관리) ① 정보통신 관련 비밀 및 대외비 분류는 정보보호담당관이 보안업무의 특성에 따라 분류하여 지정한다.

② 비밀 및 대외비로 분류된 입·출력자료 및 데이터베이스 관리는 관련 업무자 이외에는 비밀 및 대외비의 입·출력 자료 및 데이터베이스의 작성·열람 등의 업무에 참여할 수 없으며 통제구역으로 지정된 곳에서 입·출력 및 열람하는 것을 원칙으로 한다.

③ 정보보호담당관은 정보통신 자료에 대한 유출이나 파괴 또는 변조 등에 대비하여 다음 각 호에 정하는 보호대책을 강구하여야 한다.

1. 자료 복사본(예비) 확보 및 안전지역 별도 보관
2. 불법접근 및 컴퓨터 바이러스 피해 예방
3. 예비(Backup) 체계 수립 시행

④ 정보보호담당관은 비인가자가 무단으로 조작하여 정보통신 자료를 열람·출력·변조 및 훼손시키지 못하도록 시스템관리자 계정의 암호설정, 작업 중단 시 화면보호조치를 강구하여야 한다.

제30조 (대외비 관리) ① 직무상 특별히 보호가 요구되는 다음 각 호의 사항은 대외비로서 비밀에 준하여 취급할 수 있다.

1. 장기발전계획 등의 대외유출 제한이 요구되는 경영상 중요 정보
2. 정보통신 현황(IP주소가 포함된 네트워크 구성도) 등의 중요 시설 정보
3. 입학전형 등의 업무상 극히 제한적인 접근이 요구되는 정보
4. 심사분석 등의 우리 대학교 자체 또는 외부에 의한 점검/평가/감사 정보
5. 학적부 등의 집적된 개인정보

② 대외비 문서는 표면 중앙상단에 적색으로 다음 각 호와 같이 표시하여야 한다.

대 외 비
20 . . . 일반문서, 파기

1. 보호기간 경과 후 대외비의 효력이 소멸되어 일반문서로 재분류할 수 있는 문건에는 "일반문서"에 ○표시
2. 보호기간 경과 후에도 대외비의 효력이 지속되나 계속 보관할 필요가 없어 폐기할 문건일 경우에는 "파기"에 ○표시

제31조 (안전지출 및 파기계획) ① 보안담당관은 비상시 비밀보관을 철저히 유지관리하기 위한 비밀 및 중요문서에 대하여 안전지출 및 파기 계획을 수립 시행한다.

② 제1항의 규정에 의한 계획은 평상시보다 공휴일 또는 일과 후 등 평상시의 지휘계통이 없을 때 발생된 비상사태에 대비하기 위한 계획이어야 하며 실천 가능성 여부를 신중히 검토하여야 한다.

③ 보안담당관은 수립된 계획에 의해서 수시훈련을 실시하여야 한다.

제 7 장 시설보안

제32조 (보호구역 관리) ① 보안담당관은 우리 대학교 시설의 기능과 특성을 고려하여 다음 각 호의 기준에 따라 필요한 장소에 일정한 범위를 정하여 보호구역을 설정한다.

1. “제한구역”이란 비인가자의 불필요한 접근을 방지하기 위하여 출입자에게 안내가 요구되는 구역을 말한다.
2. “통제구역”이란 인가받은 자 이외의 불필요한 인원의 출입이 금지되는 구역을 말한다.

② 보호구역의 관리를 위해 다음 각 호의 사항을 준수한다.

1. 보호구역은 외부인에게 공개하지 않는 것을 원칙으로 한다.
2. 외부 게시물 및 건물 구조도에는 통제구역의 위치를 표시하지 않는다.
3. 통제구역은 각종 재해 및 장애에 대비하여 안정성을 높이기 위한 별도의 전원설비 및 방재, 공조 설비를 갖춘다.

제33조 (보호구역 지정) ① 우리 대학교의 보호구역은 다음 각 호와 같다.

1. 제한구역 : 총장실, 부총장실, 각 처장실, 전산실 및 개인정보 취급 등으로 업무상 관계자 외의 출입이 주의 요구되는 구역
2. 통제구역 : 통신실, 강의제작실, 전산서버실 및 업무상 관계자와 출입이 제한되는 구역

② 지정된 보호구역에 대하여는 “보호구역대장”에 관계 사항을 기록 유지하여야 한다.

제34조 (출입통제) ① 보안담당관은 출입통제 등 보호대책을 강구하여야 한다.

- ② 제한구역의 출입통제는 비밀번호 키 혹은 ID카드 등의 출입통제장치를 설치한다.
- ③ 통제구역의 출입통제는 다음 각 호의 설비를 통하여 상시 출입자로 등록된 자에 한해 출입이 허가될 수 있도록 운영해야 하며 출입통제의 기록을 남기기 위해 출입대장을 이용, 관리할 수 있다. 다만, 전자적으로 출입통제 기록이 남길 수 없는 제한구역일 경우에는 “출입관리대장”에 작성하여 출입통제를 관리할 수 있다.

1. CCTV
2. ID카드 혹은 정맥 인식 기반 출입통제장치

④ 정보보호담당관은 구역별 출입관리의 기준을 수립하여 관리하여야 한다.

제35조 (시설방호) ① 보안담당관은 우리 대학교 시설방호에 대한 기본계획을 수립하여야 한다.

- ② 시설방호계획에는 외래인 출입통제방안을 포함하여야 한다.
- ③ 공휴일 또는 일과후 등에 발생하는 비상사태에 대비하기 위한 비상연락망을 각 부서별로 작성하여야 한다.

제36조 (소방관리) 보안담당관은 방화 또는 소화 작업의 신속하고도 효과적인 실시를 위하여 기준에 의한 소화시설을 완비하고 수시점검을 실시하여야 하며 자체 소방계획에 의하여 점검 및 훈련을 실시한다.

제37조 (사무실 보안관리) 분임보안담당관은 다음 각 호에 따른 사무실 보안사항을 점검하고 관리하여야 하며 우리 대학교 내 모든 사무실 근무자는 이를 준용하여야 한다.

1. 책상 위에 중요 문서나 저장매체를 방치해서는 안 된다.
2. 책상 위, 벽면 등에는 대외비 이상의 정보가 기록된 자료를 게시하거나, 접근통제를 위해 부여된 계정 정보를 책상 주변에 노출시켜서는 안 된다.
3. 공용 캐비닛에는 정·부책임자를 지정하고 퇴실 시 항상 잠금 상태를 확인 후 열쇠는 안전한 곳에 보관한다.
4. 개인서랍은 시건이 가능해야 하며 퇴근 시 시건 상태를 확인하고 열쇠는 안전한 곳에 보관한다.
5. 최종 퇴실자는 매일 퇴근 전 사무실의 보안점검을 실시하고 “사무실 보안점검 일지”를 작성한다.

제 8 장 기타

제38조 (정보보호정책의 준용) 이 규정에 명시되지 않는 정보보호 관련 업무에 대하여는 「정보보호정책」을 정한다.

제39조 (오·남용) 정보보호담당관은 사용자가 우리 대학교 정보통신망 및 그에 연결된 정보 및 자원을 다음 각 호와 같이 오용할 경우 정보통신망의 사용을 즉시 취소할 수 있으며, 보안담당관을 경유하여 사고경위에 대한 확인서를 사용자에게 요구하고 제37조에 의하여 손해배상 및 징계를 요청할 수 있다.

1. 사용권한 없이 컴퓨터 계정을 사용한 경우나 컴퓨터 계정 주인의 허락 없이 비밀번호를 취득하거나 해킹한 경우
2. 우리 대학교 정보통신망 제공목적 이외의 용도로 사용하거나 자신의 사용권한을 무단으로 타인에게 양도한 경우
3. 컴퓨터 시스템에 접근하기 위하여 권한 없이 우리 대학교 정보통신망을 사용한 경우
4. 허가받지 않은 시스템의 우리 대학교 정보통신망 연결이나 허가받지 않은 IP주소의 사용
5. 고의로 컴퓨터 및 전산망의 정상적인 운용을 방해한 경우
6. 데이터보안을 무시하거나 보안취약점을 노출시킨 경우
7. 원하지 않는 전자우편을 발송 등으로 다른 사용자들에게 피해를 주는 경우
8. 저작권에 의해 보호받는 소프트웨어 및 콘텐츠의 불법적 유통 및 사용 시
9. 학교이념과 규정에 어긋나는 내용을 전자게시판에 공지한 경우
10. 소유자의 허락 없이 통신내용을 감청하거나 복사, 변조, 삭제한 경우
11. 우리 대학교 정보통신망 사용에 있어서 교육·연구·행정 등 고유목적 이외로 사용하여 우리 대학교의 명예를 손상시키거나 재산상의 피해를 끼친 경우
12. 우리 대학교 정보통신망을 이용하여 사이트를 개설 교육·연구·행정 이외의 목적으로 사용되어 민·형사상의 법적 문제를 발생시킨 경우
13. IP 주소관리 주무부서에 등록된 자료와 시스템 관련정보가 불일치할 경우

제40조 (손해배상 및 징계) 오용에 대한 처벌의 종류는 다음 각 호와 같으며 보안담당관과 관련 부서장과 협의하여 징계를 요청할 수 있다.

1. 우리 대학교 정보통신망의 일부 또는 전체에 대하여 접근제한 및 사용권한의 박탈
2. 손해배상의 청구
3. 규정에 의한 징계

부 칙

이 규정은 2010년 9월 10일부터 시행한다.

부 칙

제1조 (시행일) 이 규정은 2019년 6월 20일부터 시행한다.

부 칙

제1조 (시행일) 이 규정은 2020년 3월 10일부터 시행한다.

정보보안업무 세부 추진계획

1. 활동목표

2. 기본방침

3. 세부 추진계획

분야별	사 업 명	세 부 추 진 계 획	주 관· 관련부서	비 고

4. 전년도 보안감사·지도방문시 도출내용과 조치계획

도 출 내 용	조 치 계 획	담당부서

정보보안업무 심사분석

1. 총 평

2. 주요성과 및 추진사항

추진계획	추진실적	문제점	개선대책

3. 세부 사업별 실적분석

* 추진실적은 목표량과 대비하여 성과 달성도를 계량화

4. 부진(미진)사업

지적사항	조치계획	담당부서

5. 애로 및 건의사항

6. 첨부(정보통신망 및 검증필 정보보호시스템 운용현황 등)

정보보호관리체계 점검항목

1. 통제구역 정보보안감사 점검항목

점검내용	상태	확인자
전산실의 물리적 보안을 위한 지침서 등이 마련되어 있고 적절히 활용되고 있는지 확인		
전원, 온도 등 전산실 내 환경의 조절은 정해진 기준치 내에서 잘 이루어지고 있는지 확인		
방재시설은 적정하며 잘 관리되고 있는지 확인		
전산실을 비롯한 각 부서의 네트워크 케이블이 안전하게 설치되어 관리되고 있는지 확인		
백업테이프 등 전산 보조기억매체 보관 및 입출 관리가 잘 행해지고 있는지 확인		
보조기억매체의 반 출입에 대하여 승인권자의 승인 등 적절한 절차를 통해 이루어지는지 확인		
상시 근무자 이외에 전산실에 출입하는 사람에 대한 출입관리기록이 지침에 의거 잘 이루어지고 있으며 관리자에 의해 정기적으로 검토가 이루어지고 있는지 확인		
문서가 보안등급에 적절하게 시건 장치가 된 문서함에 보관되고 있는지 확인		
비밀문건으로 정의된 정보자산의 입출 및 프린트 등이 적절히 통제되어 대학외부나 대학내부의 비인가자에게 유출되지 않도록 관리되고 있는지 확인		
이면지 사용 등에 의해 비밀정보가 비 인가자에게 유출되지 않도록 관리되고 있는지 확인		

2. 네트워크 정보보안감사 점검항목

점검내용	상태	확인자
장비의 도입 및 설치는 서버보안관리 절차에 따라서 이루어지고 있는지 확인		
장애가 발생하는 경우 발생 일시, 유형, 조치사항 등을 요약한 장애 일지를 적시에 기록하고 있는지 확인		
계정은 지침에 따라 권한을 부여하고 있으며 패스워드는 안전하게 설정되고 있는지 확인		
장비에 대한 접근통제 및 불필요한 서비스 제공여부 확인		
패치나 파라미터 변경은 관련절차에 따라서 이루어지고 있는지 확인		
취약점 점검은 정기적으로 이루어지고 있는지 확인		
네트워크의 성능 및 부하 등이 실시간으로 관리되어 장애 등을 적시에 발견하여 조치를 취하고 있는지 확인		
네트워크 운영자의 콘솔이나 통신회선 등이 인가되지 않은 제3자에 의해 액세스되지 않는지 확인		
통신회선 등의 장애에 대한 대책은 수립되어 있으며 적절히 운영되고 있는지 확인		
네트워크 주소의 발급, 회수 및 현황관리가 이루어지고 있는지 확인		
외부 및 내부의비 인가자에 의한 부정접속, 회선침입, 도청 및 파괴 행위 등에 대한 적절한 대책 및 이의 시행여부를 확인		
대학교의 내부망에서 인터넷을 접속하는 경우 인가된 경로만을 사용하고 있는지 확인		
대학교의 정보보안을 위해 중요한 정보통신시스템의 운영현황을 파악하고 관리상태의 적정성을 확인		

3. 시스템 정보보안감사 점검항목

점검내용	상태	확인자
시스템의 도입 및 설치, 소프트웨어 설치는 서버보안관리절차에 따라서 이루어지고 있는지 확인		
컴퓨터 동작, 작업일정 및 작성 행위, 운용자, 작업제어 언어, 외부 서비스, 테이프 및 디스크 등의 관리, 프로그램 라이브러리 관리 등이 보안체계에 맞게 운영되고 있는가를 확인		
정보통신시스템의 데이터와 프로그램에 대하여 백업이 수행되고 있으며 필요 시 복구가능성을 확보하기 위해 정기적으로 복구테스트가 행해지고 있는지 확인		
주요 데이터 및 프로그램 백업은 소산 보관하는지 확인		
시스템 장애가 발생하는 경우 발생 일시, 유형, 조치사항 등을 요약한 장애일지를 적시에 기록하고 있는지 확인		
사용자 계정은 지침에 따라 권한을 부여하고 있으며 패스워드는 안전하게 설정되고 있는지 확인		
시스템에 대한 접근통제 및 불필요한 서비스 제공여부 확인		
외부에 접속된 컴퓨터 시스템인 경우 데이터의 무결성 확보대책, 장애대책, 오류방지 대책의 수립 및 적절한 운영여부를 확인		
백신 프로그램을 설치하여 악의적 소프트웨어에 대응하고 있는지 확인		
패치나 시스템 파라미터 변경은 관련절차에 따라서 이루어지고 있는지 확인		
시스템의 정상적 운영에 대한 상시 모니터링이 이루어지고 있는지 확인		
취약점 점검은 정기적으로 이루어지고 있는지 확인		
시스템 운영 및 주요 정보에 대한 로그는 적절히 관리되고 있는지 확인		
홈페이지 게재내용은 비밀내용 중요자료가 공개되지 않도록 하고 있는지 확인		

4. 보안시스템 정보보안감사 점검항목

점검내용	상태	확인자
보안시스템 관리를 위한 접속 이외의 접근경로를 차단하였는지 확인		
보안 시스템 관리자용 PC 이외의 IP로부터 접근이 차단되고 있는지 확인		
보안시스템의 장애 시 즉각 관리자에게 연락이 되는지 확인		
보안시스템 용도 이외의 S/W를 설치하지 않았는지 확인		
불필요하거나 현황에 맞지 않은 설정이 존재하지 않는지 확인		
발견된 침입 시도에 대한 통계를 모니터링 하는지 확인		
수집된 로그를 백업하고 일정기간 동안 관리 하는지 확인		
를 변경은 정보보호시스템보안관리 절차에서 제시한 검토 및 승인 절차에 의해 변경되고 있는지 확인		

5. 데이터 정보보안감사 점검항목

점검내용	상태	확인자
정보통신시스템 내에 존재하는 데이터와 문서형태로 관리되는 데이터에 대하여 모두 보안등급을 부여하여 관리하고 있는지 확인		
비밀 유지가 필요한 비밀정보에 대하여 암호화 등이 이루어지고 있는지 확인		
백업과 회복 절차가 적절히 수행되고 있는지 확인		
데이터베이스 운영시스템, 데이터사전, 유틸리티 소프트웨어, 운영체제 등의 시스템 소프트웨어에 대해 무결성이 유지되고 있으며 장애 시에 대책수립 등이 적절히 수행되고 있는지 확인		
학생정보의 보호를 위해 학생 비밀번호 관리를 위한 보안대책이 준수되고 있는지 확인		

6. 응용시스템 정보보안감사 점검항목

점검내용	상태	확인자
응용프로그램 개발 시 계획단계에서 준수하여야 할 사항(보안요구 사항 분석 및 명세화 등)이 적절히 준수되고 있는지에 대한 확인		
응용프로그램 개발 시 프로그래밍 단계에서 준수하여야 할 사항(보안을 고려한 프로그래밍 등)이 적절히 준수되고 있는지에 대한 확인		
응용프로그램 개발 시 테스트 단계에서 준수하여야 할 사항(데이터의 입출력 등)이 적절히 준수되고 있는지에 대한 확인		
테스트 수행 시 사용되는 데이터는 실 업무에 사용 중인 데이터를 변경하여 사용하는지의 여부를 확인		
개발된 응용프로그램이 적절한 통제절차에 의하여 운영환경으로 이전되고 있는지에 대한 확인		
프로그램 소스 라이브러리에 대한 엄격한 접근통제 유지를 확인		
프로그램 변경의 경우 변경절차의 따라 적절한 승인을 거친 후 운영환경에 이관되고 있는지 확인		
운영시스템에서의 직접적인 프로그램 변경 등 긴급한 상황하의 프로그램 변경이 사후의 승인을 득하였는지 등 적절한 통제절차에 의해 이루어 졌는지 확인		
인가된 응용소프트웨어 만을 사용하고 있는지에 대해 확인		
사용자별 접근기록을 감사하고, 로그로 남겨진 변경 사항을 주기적으로 감사하여 불법으로 접근되거나, 변조된 내용이 없는지 확인		

7. PC 정보보안감사 점검항목

점검내용	상태	확인자
개인용 컴퓨터는 비인가자가 부팅을 하거나 접근하지 못하도록 부팅 시 패스워드의 설정사용, 화면보호기 패스워드의 설정사용, 공유폴더 사용제한, 개인용 컴퓨터의 패스워드 관리 등을 규정한 개인용 컴퓨터 보안관리 지침이 준수되고 있는지 실사 등을 통해 확인		
개인소유의 컴퓨터는 적절한 승인절차 없이 중요정보가 처리, 보관되는 기관 내부로 반입하여 사용할 수 없도록 적절한 통제절차가 수립되어 시행되는지 확인		
개인용 컴퓨터에 보관되어 있는 정보일지라도 비밀정보를 저장하고 있는 경우 패스워드의 설정, 암호화 등을 통해 비인가자에 의한 정보의 유출을 방지하기 위한 적절한 대책이 강구되어 있는지 확인		
개인용 컴퓨터에 대하여 불법 소프트웨어의 사용 금지 및 사내 표준 운영체제와 소프트웨어를 사용하도록 하는 지침이 잘 준수되고 있는지 확인		
노트북 등 특히 분실의 염려가 있는 경우 별도의 도난방지 장치를 설치하여 사용하는지 확인		
노트북 컴퓨터를 내부에서 전산망에 연결하여 사용하는 경우에도 개인용 컴퓨터 및 단말기에 적용되는 수준의 보안이 동일하게 적용되고 있는지 확인		
개인용 컴퓨터에 바이러스의 유입을 방지하기 위한 바이러스 방역 지침이 잘 준수되고 있는지 확인		
업무 연락, 사내게시판, 메일 등을 통해 개인용 컴퓨터 보안 및 바이러스 방역을 위한 홍보가 지속적으로 행해지는지 확인		

