사이버보안 관리규정

공포 제2026-3호(개정 2026. 7. 24.)

제1장 총칙

제1조(목적) 이 규정은 장안대학교(이하 “본교”라 한다)의 정보자산을 사이버공격·위협 및 침해사고로부터 안전하게 보호하고, 사이버보안 대응체계를 구축·운영함으로써 본교 구성원에게 안전하고 원활한 정보서비스를 제공함을 목적으로 한다.

제2조(적용 대상과 범위) ① 이 규정의 적용 대상은 교내 전산자원을 사용하는 모든 정보시스템 및 그 이용자로 한다.
② 본교의 정보자산 보호와 정보운영환경 및 응용프로그램의 운영과 제공에 관하여는 따로 규정되는 경우를 제외하고는 이 규정에 따른다.
③ 본교의 전산자원을 사용하는 모든 구성원은 이 규정을 준수하여야 하며, 이를 준수하지 않아 발생한 사고의 책임은 원칙적으로 사용자 본인에게 있다.

제3조(정의) 이 규정에서 사용하는 용어의 뜻은 다음 각 호와 같다.

1. “전산망”이란 각종 정보시스템을 통신회선으로 연결하여 자료를 처리·보관하거나 전송하는 조직망을 말한다.
2. “정보시스템”이란 정보의 수집, 가공, 저장, 검색, 송신·수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 말한다.
3. “시스템관리자”란 각 부서에 소속되어 시스템의 관리 권한을 가지고 전자적 민원처리 및 행정업무의 원활한 수행을 위하여 정보시스템을 운영·관리하는 사람을 말한다.
4. “데이터베이스관리자”란 데이터베이스를 운영·관리하는 자를 말한다.
5. “전산자료”란 전산장비에 의해 입력·보관되어 있는 정보자료를 말하며, 백업미디어 등 저장매체를 포함한다.
6. “사이버보안”이란 사이버공격·위협 및 침해사고로부터 정보통신망 및 정보시스템을 보호하고 그 기능을 유지하기 위한 관리적·물리적·기술적 활동의 일체를 말한다.
7. “사이버공격·위협”이란 해킹, 컴퓨터바이러스, 서비스거부(DDoS), 전자기파 등 전자적 수단에 의하여 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템을 침입·교란·마비·파괴하거나 정보를 위조·변조·훼손·절취하는 행위 및 그와 관련된 위협을 말한다.
8. “침해사고”란 해킹, 컴퓨터바이러스, 악성코드, 메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태를 말한다.
9. “시스템실”이란 서버·PC 등 전산장비와 스위치·라우터 등 통신 및 전송 장비 등이 설치·운용되는 장소를 말한다.
10. “정보이용자”(이하 “이용자”라 한다)란 본교 전산망을 통하여 전자적 민원처리 또는 행정업무를 수행하거나 웹 기반 서비스를 이용하는 민원인 및 시스템관리자를 말한다.
11. “업무담당자”란 전자적 민원처리 또는 행정업무를 담당하는 사람을 말한다.
12. “민원인”이란 전자적 민원처리를 신청하는 주체로서, 개인 또는 사업자, 법인 등 단체 및 그 기관의 담당자 등을 말한다.
13. “본인확인”이란 정보통신망을 통하여 정보시스템 또는 행정정보를 이용하는 업무담당자, 민원인 또는 시스템관리자가 가지고 있거나 알고 있는 정보를 이용하여 본인임을 확인하는 것을 말한다.
14. “접근권한”이란 정보시스템에 접속하여 정보자원을 활용할 수 있는 권한과 행정정보를 생성·변경·열람·삭제 등을 할 수 있는 권한을 말한다.
15. “개인정보”란 「개인정보 보호법」 제2조제1호에 따른 정보를 말한다.
16. “클라우드컴퓨팅서비스”란 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조에 따른

서비스를 말한다.

17. “인공지능(AI) 시스템”이란 학습·추론 기능을 갖춘 정보시스템으로서 본교가 도입·이용하는 시스템을 말한다.
18. “사물인터넷(IoT) 기기”란 통신 기능을 갖추어 네트워크에 연결되는 센서, CCTV, 출입통제장치 등 기기를 말한다.
19. “시험데이터”란 정보시스템의 개발, 변경, 테스트, 검증 등의 목적으로 사용하는 데이터를 말한다.
20. “위험평가”란 정보자산의 식별, 위협 및 취약점 분석, 영향도 평가 등을 통하여 보호 필요 수준을 결정하는 활동을 말한다.

제4조(정보보안담당관의 지정) ① 총장은 효율적·체계적인 사이버보안 업무를 수행하기 위하여 사이버보안 전문지식을 보유한 인력을 확보하고 관련 전담조직을 구성·운영한다.
② 사이버보안 조직을 지휘하고 본교 및 소속기관에 대한 사이버보안 업무를 총괄하는 “정보보안담당관”으로 정보전산원장을 지정하여 운영한다.
③ 총장은 관계기관의 지침 또는 요청이 있는 경우 정보보안담당관의 소속·직책·직급·성명·연락처(전자우편 주소 포함) 등을 통보하여야 한다.
④ 총장이 정보보안담당관에 부여하는 기본활동은 다음 각 호와 같다.

1. 사이버보안 정책 및 기본계획 수립·시행
2. 사이버보안 관련 규정·지침 등의 제정 및 개정
3. 정보보안운영위원회 및 대학정보화위원회에 부의되는 사이버보안 관련 안건의 사전 검토 및 상정
4. 사이버보안 업무 지도·감독, 감사 및 심사분석
5. 정보통신실, 정보통신망 및 정보자료 등의 보안관리
6. 사이버보안 수준진단 및 위험평가
7. 사이버공격 초동조치 및 대응
8. 사이버위협정보 수집·분석 및 보안관제
9. 사이버보안 예산 및 전문인력 확보
10. 침해사고 조사 결과 처리 및 재발방지 대책 수립
11. 사이버보안 교육 및 정보협력
12. 주요정보통신기반시설 보호활동
13. 국가용 보안시스템 및 암호키의 운용·보안관리
14. 국가정보원장이 개발하거나 안전성을 검증한 암호모듈·정보보호시스템의 운용 및 보안관리
15. 정보통신망 보안대책의 수립·시행
16. 클라우드·AI·IoT 등 신기술 환경의 사이버보안 대책 수립·시행
17. 사이버위협 정보 공유 및 유관기관 협력
18. 그 밖에 사이버보안 관련 사항

⑤ 정보보안담당관은 사이버보안 전문지식을 보유하고 제4항의 업무를 보좌하는 정보보안담당자를 지정하여 운영할 수 있다.

제2장 정보보안운영위원회

제5조(정보보안운영위원회) ① 제4조제4항의 업무를 체계적·효율적으로 수행하기 위하여 정보보안운영위원회(이하 “위원회”라 한다)를 둔다.
② 위원회는 위원장 1인을 포함한 7인 이내의 위원으로 구성한다.
③ 위원장은 정보보안담당관으로 하고, 위원은 위원장의 추천으로 총장이 위촉한다.
④ 위원의 임기는 1년 이내로 하되, 중임할 수 있으며, 위원장은 그 직에 있는 동안 재임한다.
⑤ 위원회는 다음 각 호의 사항을 심의한다.

1. 본교의 사이버보안 정책 및 제도 개선
2. 사이버보안 관련 규정·지침의 수립 및 개정
3. 본교 규정 및 관련 법령에서 정한 사이버보안 사항의 이행 실태 확인

4. 각 부서로부터 심의 요청을 받은 각종 사이버보안 관련 사항
5. 사이버보안 업무에 대한 심사분석 및 그 수행상 조정과 협의를 요하는 사항
6. 사이버보안 기능 강화를 위한 전산망 신·증설계획과 정보화 용역개발 사업에 관한 사항
7. 사이버보안 위험평가 결과 및 자체 진단·점검 결과
8. 중대 침해사고 조사 결과 및 재발방지 대책
9. 외부 위탁·용역사업의 보안 요구사항
10. 사이버보안 위반사항의 심사와 처리
11. 그 밖에 위원장 또는 총장이 본교의 사이버보안을 위하여 필요하다고 인정하는 사항

제5조의2(대학정보화위원회 심의) ① 다음 각 호의 사항은 「대학정보화위원회 규정」에 따른 대학정보화위원회에서 심의한다.
1. 클라우드컴퓨팅서비스 도입의 보안성 심사
2. 인공지능(AI) 시스템 도입의 보안성 심사
3. 사물인터넷(IoT) 기기 도입의 보안성 심사
4. 사이버보안 관련 정보화 예산 및 사업계획에 관한 사항
5. 그 밖에 정보보안담당관이 필요하다고 인정하여 부의하는 사항

② 정보보안담당관은 제1항 각 호의 사항에 대하여 대학정보화위원회에 안건을 부의할 수 있으며, 그 심의 결과를 사이버보안 업무에 반영한다.

제6조(활동계획 수립 및 심사분석) ① 총장은 매 학년도 사이버보안업무 추진계획을 수립·시행하고, 직전 학년도 추진결과를 정리한 이행보고서를 작성·보관하여야 한다.
② 추진계획 및 이행보고서의 작성 시기는 교육부 등 관계기관의 지침에 따르되, 별도 지침이 없는 경우 다음 각 호와 같다.
1. 추진계획: 매년 3월 31일까지
2. 이행보고서: 매년 3월 31일까지

③ 추진계획 및 이행보고서의 서식은 정보보안담당관이 따로 정한다.

제3장 사이버보안

제7조(기본 수칙) ① 정보시스템 또는 행정정보 사용자는 개인별 사용자 계정 및 암호의 기밀을 유지하여야 하며, 본래의 발급 목적으로만 사용하여야 한다.
② 교직원 및 학생은 허가받은 정보시스템 또는 행정정보의 사용 권한이 부여된 영역에 대하여 본래의 목적으로만 사용할 수 있다.
③ 정보시스템 사용자는 정보시스템의 성능저하 및 보안상 위험을 초래할 수 있는 행위를 하여서는 아니 되며, 이러한 행위를 한 자를 발견한 경우에는 소속 부서의 장 또는 정보보안담당관에게 알려야 한다.
④ 정보시스템 또는 행정정보와 연관된 저작권·특허권 및 소프트웨어 라이선스의 사용조건을 숙지하고 이를 준수하여야 하며, 교내에서는 구매증서가 있는 합법적인 소프트웨어만 사용할 수 있다.
⑤ 학내 전산망을 신설·변경 또는 폐기하고자 하는 경우에는 정보보안담당관의 사전승인을 받아야 한다.
⑥ 외부 전산망에서 학내 전산망으로의 접근은 학교에서 승인한 정보시스템을 제외하고는 원칙적으로 허용하지 아니한다. 다만, 필요 시 적법한 절차에 따라 승인된 경우에는 제한적으로 허용할 수 있다.
⑦ 모든 정보시스템 또는 행정정보는 보안등급에 따라 분류·관리한다.
⑧ 정보시스템 관리자는 주기적인 보안점검을 통해 학내 전산망 및 정보시스템의 안전성을 점검하고, 사이버보안 정책 및 규정의 준수 여부를 평가하여야 하며, 학내 모든 사용자는 이에 적극 협조하여야 한다.
⑨ 업무와 관련하여 습득한 정보자산을 본교의 허가 없이 외부에 누출하여서는 아니 된다.
⑩ 교내 각종 민감 정보 및 주요 연구자료의 교외 이관 시 인터넷 메일과 같은 사적 전자우편을 사용할 수 없다.
⑪ 침해사고를 예방하기 위한 목적으로 학교의 승인을 받은 사이버보안시스템 및 사이버보안 활동은 즉시 시행할 수 있다.

제8조(보안등급 기준) ① 보안등급의 분류기준은 다음 각 호에 따라 정한다.

1. 정보의 중요도
2. 정보시스템 또는 행정정보의 절취 및 불법변경 시 손실 가치
3. 정보시스템 또는 행정정보의 파괴 시 복구비용
4. 행정정보의 사용권자

② 정보시스템 또는 행정정보의 보안등급 및 사용자 인가는 제1항의 기준에 따라 행정정보를 보유한 부서의 장이 따로 정한다.

제9조(사이버보안 점검 및 위험평가) ① 정보보안담당관은 교내 주요 서버 및 각 연구실의 서버에 대하여 필요 시 수시 점검을 실시할 수 있으며 다음 각 호의 절차에 따른다.

1. 보안점검 대상 및 분야를 해당 부서에 통보한다.
2. 해당 부서에서는 보안점검에 필요한 자료 및 제반 요청사항을 준비하여 보안점검에 대비한다.
3. 보안점검을 실시한 후 그 결과를 정보보안담당관에게 보고하고 해당 부서에 통보한다.
4. 해당 부서에서는 지적사항을 즉시 시정하고 그 결과를 정보보안담당관에게 보고한다.
5. 정보보안담당관은 필요 시 각 부서의 보안점검 지적사항에 대한 시정 여부를 확인할 수 있다.

② 홈페이지 침해사고 및 개인정보 노출사고 등을 예방하고 대응하기 위하여 정보보안담당관은 다음 각 호에 따라 보안점검을 실시하거나 요구할 수 있다.

1. 보안점검 대상은 본교의 모든 홈페이지로 한다.
2. 보안점검은 홈페이지를 구축할 때와 점검 사유가 발생할 때 실시한다.
3. 보안점검은 원칙적으로 정보보안담당관이 시행하되, 사전 협의된 경우 구축·관리 주체가 자체적으로 보안점검을 실시하고 그 결과를 정보보안담당관에게 통보할 수 있다.
4. 제1항의 절차를 준용한다.

③ 정보보안담당관은 연 1회 이상 본교 정보자산에 대한 위험평가를 실시하여야 하며, 그 결과를 위원회에 보고하여야 한다.

④ 각 부서의 장은 제3항의 위험평가 결과에 따라 필요한 보호조치를 시행하여야 한다.

제10조(사이버 침해사고 대응) ① 침해사고가 발생한 경우 정보보안담당관은 다음 각 호의 단계에 따라 적절한 조치를 하여야 한다.

1. 침입 가능성이 있는 부분을 수시로 점검하여 침해사고를 사전에 예방한다.
2. 시스템관리자는 비정상적인 활동이나 징후를 발견한 경우 침해 여부를 즉시 점검하고 정보보안담당관에게 보고하여야 한다.
3. 침해사고가 진행 중인 경우에는 계정 차단, 네트워크 분리, 악성코드 제거 등 피해 확산 방지를 위한 조치를 즉시 실시하여야 한다.
4. 침해 흔적이 확인된 경우 로그파일, 관련 장비 정보 등 증적자료를 확보하고 정보자료의 이상 유무를 점검하여야 한다.

② 정보보안담당관은 중대한 침해사고를 인지한 경우 지체 없이 초동조치를 수행하고, 특별한 사유가 없는 한 24시간 이내에 총장에게 보고하여야 한다.

③ 침해사고가 관계기관 보고 대상에 해당하거나 외부 지원이 필요한 경우에는 관계 법령·지침에 따라 교육부, 한국인터넷진흥원(KISA) 등 관계기관에 통보하거나 기술지원을 요청할 수 있다.

④ 총장은 침해사고 대응을 위하여 필요한 경우 침해사고 대응체계 또는 대응조직(CERT)을 운영할 수 있으며, 연 1회 이상 모의훈련을 실시하여야 한다.

⑤ 침해사고 관련 로그 및 증적자료는 별도 지침이 없는 한 1년 이상 보존한다.

제11조(사이버보안 교육) ① 총장은 자체 사이버보안 교육계획을 수립하여 연 1회 이상 전 교직원을 대상으로 관련 교육을 실시하여야 한다. 다만, 정보보안담당자는 연간 15시간 이상 사이버보안 교육(「개인정보 보호법」에 따른 교육을 포함한다)을 이수하여야 한다.

② 총장은 사이버보안 교육의 효율성 제고를 위하여 본교 실정에 맞는 사이버보안 교안을 작성·활용하여야 하며, 필요 시 관계기관에 전문인력 및 자료 지원을 요청할 수 있다.

③ 총장은 사이버보안 관련 전문기관 교육 및 기술세미나 참석을 장려하는 등 정보보안담당자의 업무 전문성을 제고하기 위하여 노력하여야 한다.

④ 교육 내용에는 사이버위협 사례, 클라우드·AI 이용 보안수칙, 개인정보 보호에 관한 사항을 포함하여야 한다.
⑤ 교육 실시 결과(교육일지, 이수자 명단 등)는 3년간 보관하여야 한다.

제12조(사이버보안진단의 날) ① 매월 세 번째 수요일을 "사이버보안진단의 날"로 지정·운영한다.
② 총장은 "사이버보안진단의 날" 운영에 대한 계획을 수립하고 소관 사이버보안업무 전반에 대하여 체계적이고 종합적인 보안진단을 실시하여야 한다.
③ 총장은 제1항 및 제2항에 따른 보안진단 결과를 제6조에 따른 이행보고서에 포함하여야 한다.

제12조의2(사이버보안 자체 진단·점검) ① 총장은 본교에 대한 사이버공격·위협의 예방 및 대응에 필요한 자체 진단·점검을 연 1회 이상 실시하여야 한다.
② 각 부서의 장은 자체 진단·점검 결과 취약요소가 발견된 경우 지체 없이 시정조치를 하여야 한다.
③ 정보보안담당관은 자체 진단·점검 결과 및 조치 결과를 종합하여 위원회에 보고하여야 한다.
④ 총장은 관계기관의 요청이 있는 경우 제1항 및 제2항에 따른 결과를 제출할 수 있다.

제12조의3(사이버보안 훈련) ① 총장은 매년 본교에 대한 사이버공격·위협 대응훈련을 실시하여야 한다.
② 정보보안담당관은 관계기관 주관의 통합훈련 또는 합동훈련이 있는 경우 이에 참여할 수 있다.
③ 훈련 결과 시정이 필요한 사항은 즉시 보완하여야 한다.

제13조(용역사업 보안관리) ① 총장은 정보화·정보보호사업 및 보안컨설팅 수행 등을 외부용역으로 추진하는 경우 사업 관리책임자로 하여금 다음 각 호의 사항을 포함한 보안대책을 수립·시행하게 하여야 한다.

1. 용역사업 계약 시 계약서에 참여인력의 보안준수 사항과 위반 시 손해배상 책임 등을 명시할 것
2. 용역사업 수행 관련 보안교육·점검을 실시하고 용역기간 중 참여인력을 임의로 교체하지 못하도록 할 것
3. 정보통신망도, IP 현황 등 용역업체에 제공할 자료는 자료 인계인수대장을 비치하고 보안조치 후 인계·인수하며 무단 복사 및 외부반출을 금지할 것
4. 사업 종료 시 외부업체의 노트북, 휴대용 저장매체 등을 통하여 비공개 자료가 유출되지 않도록 복구가 불가능한 방법으로 완전삭제할 것
5. 용역업체로부터 용역 결과물을 전량 회수하고 비인가자에게 제공하거나 열람시키지 아니할 것
6. 용역업체의 노트북 등 관련 장비를 반입·반출할 때마다 악성코드 감염 여부 및 자료 무단반출 여부를 확인할 것
7. 그 밖에 총장이 보안관리가 필요하다고 판단하는 사항이나 관계기관이 보안조치를 권고하는 사항
8. 수탁사가 클라우드컴퓨팅서비스 또는 인공지능(AI) 시스템을 활용하는 경우 해당 영역의 보안 요구사항을 계약서 등에 명시할 것
9. 용역사업 수행 과정에서 시험데이터를 사용하는 경우 「시험데이터 보안관리 절차 지침」 준수 의무를 명시할 것

② 총장은 용역사업 추진 시 과업지시서, 입찰공고, 계약서 또는 이에 준하는 문서에 다음 각 호의 누출금지 대상정보를 명시하여야 한다. 이 경우 관련 법령이 적용되는 경우에는 해당 법령에 따른 조치를 하고, 그 밖의 경우에는 본교 계약 관련 규정 및 계약조건에 따라 입찰참가 제한, 계약해지, 손해배상 청구 등 필요한 조치를 할 수 있다.

1. 기관 소유 정보시스템의 내·외부 IP주소 현황
2. 세부 정보시스템 구성 현황 및 정보통신망 구성도
3. 사용자 계정·비밀번호 등 정보시스템 접근권한 정보
4. 정보통신망 취약점 분석·평가 결과물
5. 정보화 용역사업 결과물 및 관련 프로그램 소스코드
6. 국가용 보안시스템 및 정보보호시스템 도입 현황
7. 침입차단시스템(FW), 침입방지시스템(IPS) 등 정보보호 제품 및 라우터·스위치 등 네트워크 장비 설정 정보
8. 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따라 비공개 대상정보로 분류된 기관의 내부문

서에 준하는 자료
9. 「개인정보 보호법」 제2조제1호의 개인정보
10. 「보안업무규정」상 비밀 및 대외비에 해당하거나 이에 준하는 자료
11. 그 밖에 총장이 공개가 불가하다고 판단한 자료

③ 총장은 비밀 및 중요 외주 용역사업을 수행할 경우 외부인원에 대한 신원확인, 보안교육 및 외부 유출 방지 등 필요한 보안조치를 하여야 한다.
④ 총장은 국가안보와 관련되거나 이에 준하는 중요 용역자료는 인터넷이 차단된 PC에 비밀번호를 부여하여 별도로 저장하거나 보안 USB 등에 저장하여 유출되지 않도록 조치하여야 한다.
⑤ 사업 관리책임자는 제1항부터 제4항까지의 보안대책 이행 실태를 주기적으로 점검하고, 미비점이 발견된 경우 사업담당자로 하여금 보완하도록 조치하여야 한다.
⑥ 외부 용역업체의 보안관리에 관한 세부사항은 정보보안담당관이 따로 정한다.

제14조(원격근무 보안관리) ① 총장은 재택·파견·이동근무 등 원격근무를 지원하기 위한 정보시스템을 도입·운영하는 경우 기술적·관리적·물리적 보안성 검토를 실시하여야 한다.
② 총장은 원격근무 가능 업무 및 공개·비공개 업무 선정기준을 수립하되, 대외비 이상의 비밀자료 또는 이에 준하는 중요정보를 취급하는 업무는 원격근무 대상에서 원칙적으로 제외한다. 다만, 부득이하게 수행이 필요한 경우에는 별도의 보안대책을 수립하여 시행하여야 한다.
③ 총장은 모든 원격근무자로부터 전자결재 신청양식인 「가상사설망(VPN) 이용 신청서」(보안서약 포함)를 통하여 신청·승인 절차를 거치게 하여야 하며, 원격근무자의 업무 변경·인사이동·퇴직 등 상황 발생 시 정보시스템 접근권한 재설정 등 관련 절차를 마련하여야 한다.
④ 원격근무자는 원격근무 시 해킹에 의한 업무자료 유출을 방지하기 위하여 작업 수행 전 백신으로 원격근무용 PC를 점검하고, 업무자료의 임의 저장 금지 등 보안조치를 하여야 한다.
⑤ 원격근무자는 정보시스템 고장 시 정보유출 방지 등 보안대책을 강구한 후 정보보안담당관과 협의하여 정비·반납 등 조치를 하여야 한다.
⑥ 비공개 원격 업무인 경우에는 암호화, 다중인증 등 보안기술을 사용하여야 한다.
⑦ 총장은 주기적인 보안점검을 실시하여 원격근무 보안대책의 이행 여부를 확인하여야 한다.

제4장 정보시스템 관리

제15조(사용자 정의) 정보시스템 또는 행정정보를 사용할 수 있는 자는 다음 각 호와 같다.
1. 본교 교원, 직원, 재학생 및 졸업생
2. 연구소 및 부속기관의 장이 사용을 인정한 자

제16조(적절성 확보) 정보시스템 또는 행정정보 이용자는 정보시스템 사용에 있어 적절성을 유지하여야 한다. 다만, 다음 각 호에 해당하는 경우에는 부적절한 사용으로 간주하여 제재조치를 할 수 있다.
1. 타 사용자의 계정 및 암호를 허가 없이 사용한 경우
2. 타 사용자의 정당한 사용을 방해한 경우
3. 타 사용자의 자료를 허가 없이 유출하거나 읽고 쓰는 행위
4. 일반 사용자가 관리계정 암호 또는 타 사용자의 암호를 획득하고자 해킹하는 행위
5. 내부의 중요 전산정보를 불법으로 외부에 유출한 경우
6. 외부의 불법 사용자에게 계정 및 암호를 제공한 경우
7. 사용자 계정 및 암호를 상호 공유하는 행위
8. 시스템관리자가 특별한 사유 없이 관리계정 암호를 일반 사용자와 공유한 경우
9. 허가된 보안등급 이상의 자료를 무단 유출하거나 읽고 쓰는 행위
10. 인터넷을 통하여 자살 또는 음란 사이트 등 반사회적인 유해사이트에 접속·개설·열람하는 경우
11. 보안점검의 지적사항에 대하여 즉각적인 시정을 하지 아니한 경우
12. 정보시스템을 이용한 개인정보 침해사고(불법유출, 훼손, 갈취, 불법 열람 등)가 발생한 경우

제16조의2(대학정보시스템 권한관리 및 비밀번호관리) ① 대학정보시스템을 사용하고자 하는 전체 교직원

및 재적 학생은 본 조에서 정하는 권한관리 및 비밀번호 관리에 관한 사항을 준수하여야 한다.
② 재직 중인 교직원으로서 대학정보시스템의 업무 권한을 부여받고자 하는 자는 부서장의 승인을 받아 필요한 업무 권한을 신청하여 업무에 활용할 수 있다.
③ 대학정보시스템의 권한을 부여받은 자는 다음 각 호의 비밀번호 정책을 준수하여야 한다.
1. 사용자 계정과 동일하지 아니할 것
2. 개인신상 및 부서 명칭 등과 관계가 없을 것
3. 일반 사전에 등록된 단어는 피할 것
4. 동일 단어 또는 숫자를 반복하여 사용하지 아니할 것
5. 한 번 사용된 비밀번호는 재사용하지 아니할 것
6. 비밀번호는 문자, 숫자, 특수문자를 혼합하여 9자리 이상으로 설정할 것
7. 설정된 비밀번호는 절대 타인과 공유하지 아니할 것
④ 시스템관리자 및 부서의 장은 인사이동, 퇴직, 휴학, 졸업, 업무변경 등 권한 조정 사유가 발생한 경우 지체 없이 접근권한을 변경 또는 회수하여야 하며, 정기적으로 권한 부여 현황을 점검하여야 한다.

제17조(위반행위에 대한 조치) ① 정보보안담당관은 위반행위를 발견한 경우 피해 확산 방지를 위하여 다음 각 호의 조치를 즉시 시행할 수 있다.
1. 계정 회수 또는 사용 제한
2. 시스템 접근 차단
3. 네트워크 접속 제한
4. 그 밖에 필요한 긴급 보호조치
② 정보보안담당관은 중대한 위반행위에 대하여 총장에게 보고하고 다음 각 호에 따라 처리한다.
1. 교직원 및 학생: 본교 관련 규정에 따른 인사·징계 절차에 회부
2. 외부 용역업체 및 외부 사용자: 계약조건, 본교 관련 규정 및 관계 법령에 따라 처리
③ 위반행위로 인한 손해에 대하여는 관계 법령 및 본교 규정에 따라 손해배상을 청구할 수 있다.
④ 정보보안담당관은 제2항에 따른 처리 결과를 위원회에 보고한다.

제5장 네트워크 관리

제18조(전산망 관리) ① 네트워크 관리는 일관성과 기밀성을 위하여 통합관리를 원칙으로 한다.
② 운영부서의 관리자는 네트워크 신규 설치 및 변경 시 정보보안담당관에게 변경정보를 통보하여야 한다.
③ 네트워크 IP 주소는 사용자가 임의로 변경할 수 없다.
④ 인터넷을 이용한 외부로부터의 접근은 원칙적으로 금지한다. 다만, 다음 각 호의 사유와 승인절차를 거친 경우에 한하여 허용할 수 있다.
1. 연구를 목적으로 원격 접속이 필요한 경우
2. 정보시스템과 관련한 원격 업무지원이 필요한 경우
⑤ 정보시스템에 대한 원격 접속을 허용할 경우 다음 각 호를 준수하여야 한다.
1. 원격 접속 작업자는 전자결재 신청양식인 「가상사설망(VPN) 이용 신청서」(보안서약 포함)를 제출하여 승인을 받아야 한다.
2. 원격 접속 작업자에게는 작업에 필요한 최소 권한만을 부여한다.
3. 원격 접속 작업자는 해당 시스템관리자 또는 업무담당자의 관리·감독 아래에서만 접근하게 한다.
4. 원격 접속은 업무시간 범위에서만 허용한다.
5. DB서버와 같은 보안등급 최상위 정보시스템은 원격 접속 대상에서 제외한다.
⑥ 일정 횟수 이상 접속에 실패한 경우 접속을 차단하고 관련 정보를 로그에 기록한다.
⑦ 보안상 취약한 무선통신망의 신설 또는 증설은 억제한다.

제19조(네트워크의 보호) ① 정보보안담당관은 본교에 유해하거나 불필요하다고 판단되는 웹사이트 접속을 통제할 수 있다.
② 원격 사용자의 공중망 네트워크를 통한 접속은 인증시스템 또는 방화벽에 의하여 통제할 수 있다.

③ 신뢰할 수 없는 정보시스템 및 서버로의 접속을 보호하기 위하여 네트워크 정책을 설정하여 통제할 수 있다.
④ 네트워크 보안 담당자는 의심스러운 활동에 대하여 방화벽, 침입탐지시스템(IDS/IPS) 및 기타 보안시스템의 로그를 분석하여 해당 내용을 확인하여야 하며, 필요 시 부서장에게 보고하여야 한다.
⑤ 교내 네트워크 사용 시 적법한 사용자임을 인증받아야 하며, 사용하는 정보시스템 역시 적정 무결성 수준 및 보안 수준을 점검하여 본교 사이버보안 기대 수준에 미달하는 경우 네트워크 사용을 제한할 수 있다.
⑥ 무선통신 네트워크를 구축하는 경우 무선중계기(AP)의 전파 범위 조정, 사용자 인증, 패킷 암호화 등 보안대책을 적용하여야 한다.

제6장 서버 관리

제20조(운영 및 관리) 서버 관리자는 서버를 도입·운용하는 경우 정보보안담당관과 협의하여 해킹에 의한 자료 절취, 위·변조 등에 대비한 다음 각 호의 보안대책을 수립·시행하여야 한다.

1. 서버 내 저장자료에 대하여 업무별·자료별 중요도에 따라 사용자의 접근권한을 차등 부여할 것
2. 사용자별 자료의 접근 범위를 서버에 등록하여 인가 여부를 식별하게 하고 인가된 범위 이외의 자료 접근을 통제할 것
3. 서버 운용에 필요한 서비스 포트 외에 불필요한 서비스 포트를 제거하고 관리용 서비스와 사용자용 서비스를 분리하여 운용할 것
4. 서버 관리용 서비스 접속 시 특정 IP 주소 또는 관리용 단말을 지정하여 운용할 것
5. 서버 설정정보 및 서버에 저장된 자료에 대하여 정기적으로 백업을 실시하여 복구 및 침해행위에 대비할 것
6. 데이터베이스에 대하여 사용자의 직접적인 접속을 차단하고 개인정보와 같은 중요정보를 암호화하는 등 데이터베이스별 보안조치를 실시할 것

제21조(보안관리) ① 서버 관리자는 제20조에 따라 수립한 보안대책의 적절성을 수시로 확인하고, 연 1회 이상 보안도구를 이용하여 서버 설정정보 및 저장자료의 절취, 위·변조 가능성 등 보안 취약점을 점검하여야 한다. 이 경우 정보보안담당관은 서버 관리자가 수행한 사항이 적절한지 확인하고 시정조치를 권고할 수 있다.
② 개별 서버에 대한 보안관리는 각 서버의 관리자가 담당한다.

제22조(계정관리) ① 사용자 계정 분류는 그 사용 목적에 따라 분류하고 그 기준은 따로 정한다.
② 사용자별 또는 그룹별로 접근권한을 부여한다.
③ 외부 사용자의 계정은 유효기간을 설정한다.
④ 암호가 없는 계정은 사용을 금지한다.
⑤ 일정 횟수 이상 접속에 실패한 경우 사용을 금지한다.
⑥ 슈퍼유저는 콘솔(Console) 및 특정 단말기에서만 접속을 허용한다.
⑦ 사용자 계정의 등록·변경 및 폐기는 다음 각 호를 따른다.

1. 사용자 계정은 사용자 등록·변경 또는 폐기 신청서를 작성한 후 시스템관리자에게 통보하되, 외부 사용자는 반드시 사용기간 및 목적 등의 사유를 명확히 하여야 한다.
2. 시스템관리자는 내용을 검토한 후 사용자 계정을 등록·변경 또는 폐기하고 사용자에게 그 사실을 통보한다.
3. 사용자 계정을 등록·변경 또는 폐기하는 경우 일반적인 사항은 월 단위로 부서장에게 사후 보고한다. 다만, 특별한 상황이 발생한 경우에 한하여 부서장의 허가를 받은 후 작업을 실시한다.

제7장 전산자료 및 데이터베이스 관리

제23조(자료의 관리) ① 데이터베이스 로그인 계정 관리기준은 DBMS 관리자(DBA), 응용프로그램 개발자 및 사용자에 따라 권한을 차등 부여하고, 패스워드는 암호화된 형태로 존재하도록 한다.

② 데이터베이스의 무결성 유지를 위하여 데이터베이스의 수정은 적법한 인가자에 의해서만 이루어져야 하며, 물리적인 재해로부터의 보호를 위하여 주기적으로 백업하여야 한다.
③ 데이터베이스에 대한 모든 접근은 감사기록을 유지하되, 일반 사용자의 감사기록에 대한 접근은 제한하여야 한다.
④ 데이터베이스관리자(DBA)는 누가 어떤 필드, 레코드 수준에서 접근할 수 있는지를 정의하여야 한다.
⑤ DBMS는 시스템과는 별도의 사용자 인증기능을 수행하여야 한다.
⑥ 데이터베이스의 데이터는 응용프로그램을 통해서만 접근하도록 하여야 한다.
⑦ 별도 지침에 의하여 중요자료로 분류된 자료 및 데이터베이스는 데이터의 접근 정보를 기록하여 주기적인 점검 및 분석을 실시하여야 한다.

제23조의2(시험데이터 보안관리) ① 정보시스템의 개발, 변경, 테스트, 검증 등의 목적으로 사용하는 시험데이터는 유출, 변조, 훼손 및 오·남용이 발생하지 않도록 안전하게 관리하여야 한다.
② 개인정보 또는 중요정보가 포함된 데이터를 시험데이터로 사용하는 경우에는 가명처리, 익명처리, 마스킹 등 필요한 보호조치를 우선 적용하여야 하며, 부득이하게 원본에 준하는 데이터를 사용하는 경우에는 접근권한 통제, 반출 금지, 저장 위치 제한 등 강화된 보호조치를 적용하여야 한다.
③ 시험데이터는 업무상 필요한 최소 범위에서 생성·제공·이용하여야 하며, 목적 달성 후에는 지체 없이 삭제 또는 파기하여야 한다.
④ 시험데이터의 생성, 제공, 이용, 보관, 삭제 및 파기에 관한 세부사항은 「시험데이터 보안관리 절차 지침」에 따른다.

제24조(자료의 보관) ① 별도 지침에 의하여 중요자료로 분류된 자료는 별도의 보호된 장소에 보관하고, 재해 및 비상시에 대비하여 소산 계획을 수립·운영하여야 한다.
② 별도 지침에 의하여 중요자료로 분류된 자료의 이용 및 변경은 부서장의 허가와 관리책임자의 입회 아래 이용 및 변경할 수 있다.

제25조(자료의 파기) ① 별도 지침에 의하여 중요자료로 분류된 자료의 파기는 자료보관 책임자의 입회 아래 담당자가 파기를 실시하고, 자료관리대장의 파기 확인란에 입회자는 파기 확인을 하여야 한다.
② 자기테이프 등의 자기매체 자료의 파기는 컴퓨터를 이용하여 내용을 완전히 삭제하고, 자료 접근이 불가능하여 내용을 지울 수 없는 자기매체의 자료는 소각 또는 용해 등의 방법으로 파기한다.
③ 출력된 자료는 사용 목적이 완료되어 폐기할 때에는 반드시 문서파쇄기를 이용하여야 한다.

제8장 PC 관리

제26조(PC의 관리) ① PC 기동 시 BIOS 또는 UEFI에서 제공하는 부팅 암호를 설정한다.
② PC에는 로그인 비밀번호 및 비밀번호가 설정된 화면보호기를 작동시켜야 하며, 화면보호기의 설정 시간은 10분 이내로 한다.
③ 장시간 자리를 비울 때에는 전원을 끄거나 잠금 상태로 전환하여야 한다.
④ 자신의 업무에 사용하는 응용프로그램은 시스템 보안관리자의 허락 없이 무단으로 타인에게 복사해 주어서는 아니 된다.
⑤ 휴대용 저장매체를 통한 자료의 전송은 금지한다. 다만, 업무상 부득이한 경우에는 등록된 휴대용 저장매체를 활용하여야 하고, 그 사용 내역을 대장에 작성하여 부서장의 통제를 받아야 한다.
⑥ 업무상 중요한 정보는 PC 내에 보관하지 아니하며, 별도의 등록된 저장매체에 담아 물리적 보안이 철저한 위치에 보관한다.
⑦ 단말기 사용자는 PC·노트북·PDA 등 단말기(이하 “PC 등”이라 한다) 사용과 관련한 일체의 보안관리 책임을 가진다. 또한 운용 중인 운영체제(OS) 및 응용프로그램의 최신 보안패치를 유지하여야 한다.
⑧ 업무상 불필요한 응용프로그램의 설치를 금지하고, PC의 시스템 자원(폴더, 파일 등)에 대한 공유는 모두 제거하여야 한다. 다만, 필요에 따라 공유하는 경우에는 비밀번호 설정, 보안인증, 암호화 등의 보안대책을 하여야 한다.
⑨ 사용자는 PC 등을 교체·반납·폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우 관리책임자와

협의하여 저장자료가 유출·훼손되지 않도록 보안조치를 하여야 한다.
⑩ 개인 소유의 PC(노트북 PC 등)는 부서 내부로 반입 또는 반출하여 사용하여서는 아니 된다. 다만, 부득이한 경우에는 정보보안담당관의 승인을 받아 보안조치 후 반입 또는 반출할 수 있다.

제27조(악성코드 예방 및 조치) ① 정보보안담당관 및 담당자는 컴퓨터바이러스, 웜 등으로 심각한 피해가 우려되는 경우 게시판 또는 전자우편 등을 통하여 경고 메시지 게시 등의 조치를 할 수 있다.
② 교내 전산망을 통하여 전산자원을 사용하는 모든 PC는 웜, 바이러스 등의 감염을 예방하기 위하여 다음 각 호의 조치를 하여야 하며, 정보보안담당관은 필요하다고 판단될 경우 이를 강제할 수 있다.
1. 본교 사이버보안 담당부서에서 인증한 백신 프로그램을 설치할 것
2. 설치된 백신 프로그램을 항상 최신 버전으로 유지할 것
3. 정기적인 악성코드 검사를 실시할 것

③ 악성코드에 의한 데이터 손상에 대비하여 정기적으로 데이터 백업을 실시한다.
④ 정보보안담당관은 알려진 악성코드의 경우에는 해당 악성코드를 치료할 수 있는 진단 프로그램을 구비한다.
⑤ 무단 또는 불법 복사된 프로그램을 설치한 정보시스템은 교내 전산망 접속을 제한한다.
⑥ 악성코드 감염이 확인된 경우 즉시 네트워크 접속을 단절시킨 후 백신 프로그램 등으로 치료하여야 한다.
⑦ 외부에서 온 USB, 인터넷에서 다운로드한 파일, 외부로부터 전송된 전자우편의 첨부파일 등은 실행 또는 열기 전에 반드시 악성코드 검사를 하여야 한다.

제9장 전산시스템실 운영 관리

제28조(시스템실 시설기준) ① 출입구에는 입실자를 식별 및 통제할 수 있는 출입보안장치를 설치한다.
② 자동화재경보설비를 설치하고, 소화 시 장비에 피해를 최소화할 수 있는 자동소화설비를 설치한다.
③ 정전에 대비하여 별도의 전원공급시설을 둔다.
④ 온·습도를 적절히 유지할 수 있는 항온항습기를 설치한다.

제29조(시스템실 운영 및 관리) ① 전산시스템실의 운영을 담당하는 부서장은 시스템실 사용 및 운영에 관한 절차와 방법을 정하고, 담당자가 이를 숙지하도록 하여야 한다.
② 전산시스템실 운영자는 운영일지 및 장애일지를 작성하여야 한다.
③ 전산시스템 운영자는 주기적으로 로그파일을 분석하여야 하며, 시스템에 이상이 발견된 경우에는 침해사고 처리 절차에 따라 즉시 조치를 취하고 이를 정보보안담당관 및 해당 부서장에게 보고하여야 한다.
④ 전산시스템실에는 출입자 명부를 비치하고 비인가자의 출입을 통제하여야 한다.
⑤ 전산시스템실, 자료보관실 및 통신실은 관리책임자를 지정하고 자료 또는 장비별로 취급자를 지정·운영하여야 한다.

제10장 신기술 환경 보안

제29조의2(클라우드 이용 보안) ① 본교가 클라우드컴퓨팅서비스를 도입 또는 이용하는 경우 정보보안담당관은 사전에 보안성 검토를 실시하여야 한다.
② 정보화 사업과 연계되는 클라우드 도입 사항은 제5조의2에 따라 대학정보화위원회의 심의를 거쳐야 한다.
③ 클라우드 도입 계약 또는 이용약정에는 서비스 가용성, 백업, 접근통제, 사고통보, 자료의 반환 및 완전삭제 등에 관한 사항을 포함하여야 한다.
④ 개인정보 및 비공개 중요정보를 클라우드에 저장·처리하는 경우에는 암호화, 접근통제, 접속기록 관리 등 필요한 보호조치를 하여야 한다.
⑤ 클라우드 이용 현황 및 보안조치 이행 여부는 연 1회 이상 점검하여야 한다.

제29조의3(인공지능(AI) 시스템 이용 보안) ① 본교 구성원은 정보보안담당관의 승인 없이 외부 인공지능

서비스에 개인정보, 비공개 자료, 연구·학사 중요정보를 입력하여서는 아니 된다.
② 인공지능(AI) 시스템을 도입하거나 업무에 활용하고자 하는 경우에는 정보보안담당관의 사전 보안성 검토를 받아야 하며, 정보화 사업과 연계되는 경우에는 제5조의2에 따라 대학정보화위원회의 심의를 거쳐야 한다.
③ 인공지능(AI) 시스템의 출력물은 업무담당자가 정확성, 적정성 및 법적 문제 여부를 확인한 후 활용하여야 한다.
④ 총장은 인공지능(AI) 이용 보안수칙 또는 가이드라인을 따로 정할 수 있다.

제29조의4(IoT 기기 보안) ① CCTV, 출입통제장치, 센서 등 사물인터넷(IoT) 기기를 도입·운영하는 경우에는 초기 비밀번호 변경, 불필요한 기능 비활성화, 최신 보안패치 및 펌웨어 적용 등 필요한 보안조치를 하여야 한다.
② 사물인터넷(IoT) 기기는 필요한 경우 업무망과 분리된 네트워크에서 운영하고, 기기별 관리대장과 관리책임자를 지정하여야 한다.
③ 정보보안담당관은 사물인터넷(IoT) 기기의 보안상태를 주기적으로 점검할 수 있다.

제11장 기타

제30조(시행세칙) 이 규정의 운용에 필요한 세부사항은 시행세칙 또는 별도 지침으로 정할 수 있다.

제31조(준용) 이 규정에 명시되지 아니한 사항은 다음 각 호의 법령, 지침 및 본교 관련 규정에 따른다.

1. 「개인정보 보호법」 및 같은 법 시행령
2. 「국가정보원법」
3. 「사이버안보 업무규정」
4. 「보안업무규정」
5. 「전자정부법」 및 같은 법 시행령
6. 「정보통신기반 보호법」
7. 「국가 사이버보안 기본지침」
8. 교육부 및 관계기관의 사이버보안 관련 지침
9. 「대학정보화위원회 규정」

부칙 <2022. 10. 7.>

제1조(시행일) 이 규정은 2022년 10월 7일부터 시행한다.

부칙 <2025. 4. 29.>

제1조(시행일) 이 규정은 2025년 4월 29일부터 시행한다.

부칙

제1조(시행일) 이 규정은 2026년 7월 24일부터 시행한다.

제2조(경과조치) 이 규정 시행 당시 종전의 「정보보안 관리규정」에 따라 지정된 정보보안담당관, 정보보안담당자 및 구성된 정보보안운영위원회는 이 규정에 따라 지정·구성된 것으로 본다.

제3조(다른 규정과의 관계) 이 규정 시행 당시 다른 규정에서 종전의 「정보보안 관리규정」 또는 그 규정을 인용한 경우에는 「사이버보안 관리규정」 또는 이 규정의 해당 규정을 인용한 것으로 본다.