정보통신자원 운영규정 개정이력 현황표

번호	개정 공포 일자	담당부서	담당자	개정내용
1	2020.6.15	정보지원팀	송**	**제정**
2	2020.9.24	정보지원팀	송**	
3	2022.12.27.	정보지원부	송**	**폐지**

정보통신자원 운영규정(폐지)

제 정 : 2020. 6. 15
개 정 : 2020. 6. 15
폐 지 : 2022. 12. 27

제1장 총 칙

제1조(목적) 이 규정은 금강대학교(이하 "본교"이라 한다)의 정보통신자원 운영에 관하여 필요한 사항 및 서버, 네트워크, 그룹웨어, 홈페이지, 종합정보시스템, 데이터베이스, 컴퓨터류 등을 포함한 전산운영환경과 응용프로그램을 보다 안전하고 신뢰성 있게 운영하여 전산자원이 불법 유출, 파괴, 변경됨이 없이 원활한 서비스를 제공함을 그 목적으로 한다.

제2조(용어의 정의) ① 정보통신자원이라 함은 본교 내의 모든 전산관련 하드웨어와 소프트웨어를 말한다.

② 정보시스템이라 함은 정보의 수집·저장·검색·송신·수신 등 정보관리를 위한 하드웨어 및 소프트웨어를 말한다

③ 시스템 관리자라 함은 시스템의 루트(root) 권한을 가지고 시스템을 운영관리하는 자를 말한다.

④ 데이터베이스 관리자라 함은 데이터베이스를 운영관리하는 자를 말한다.

⑤ 전산자료라 함은 전산장비에 의해 입력보관되어 있는 정보자료를 말하며, 백업미디어 등 저장 매체 등을 포함한다.

⑥ 보안 관리자라 함은 보안관련 시스템을 운영관리하는 자를 말한다.

⑦ 홈페이지 관리자라 함은 홈페이지 시스템을 운영관리하는 자를 말한다.

⑧ 네트워크 관리자라 함은 네트워크 시스템을 운영관리하는 자를 말한다.

제3조(정보통신자원 주관부서) 시스템 개발 / 운영, 홈페이지, 전산망 관리 등 정보통신자원 총괄은 정보지원팀이 담당한다.

제2장 위원회

제4조(위원회) 본교의 체계적이고 효율적인 정보화사업의 추진 및 정책결정을 수립·심의 및 관리하기 위해 정보화추진위원회(이하 "위원회"라 한다)를 둔다.

제5조(기능) 위원회는 다음 각호와 같은 사항에 관하여 심의·조정 한다.

1. 종합적인 정보화 및 인프라 구축에 관한 사항
2. 정보화사업 추진에 따른 제도 및 업무개선에 관한 사항
3. 정보화실무위원화 처리결과 및 건의사항 심의
4. 정보통신 윤리에 관한 사항

5. 정보보안 및 보안업무에 관한 사항
6. 기타 정보화의 관련된 주요 사항

제6조(구성) ①위원회는 당연직 위원 8명 내외로 구성한다.
②당연직 위원은 기획관리(부)처장, 교학지원(부)처장, 원각도서관장, 경영지원팀장, 기획조정팀장, 교무지원팀장, 학생지원팀장, 정보지원팀장 이상8명으로 한다.
③위원회 사무를 처리를 위한 간사는 정보지원팀장이 겸하며, 위원장의 지시를 받아 회의록을 작성하고 보존한다.

제7조(위원장) ①위원장은 기획관리처장으로 한다
②위원장은 위원회를 대표하며 회의를 총괄한다.
③위원장은 위원회를 소집하고 그 의장이 된다.

제8조(임기) ①위원장 및 당연직위원의 임기는 보직재임기간으로 하며 위촉위원의 임기는 2년으로 한다.
②결원에 의해 새로 위촉되는 위원의 임기는 전임위원의 잔임 기간으로 한다.

제9조(회의의 소집) 위원장은 필요하다고 인정될 때 위원회를 소집할 수 있다.

제10조(의결) ①위원회 회의는 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 의결한다. 다만, 가부동수인 때에는 의장이 이를 결정한다.
② 의결은 원칙적으로 출석에 의한 방법으로 하나, 예외적으로 위원 중 정당한 사유로 의결에 출석할 수 없을 사유 등이 발생한 때는 전자메일 등의 통신수단을 통하여도 가능한 것으로 한다.
③ 의결사항이 경미한 경우 의원장의 판단에 의하여 위원서면결의로 대신할 수 있다.

제3장 업무 · 기능

제11조(업무) 정보지원팀은 시스템 개발 / 운영, 홈페이지 관리 및 운영, 네트워크 관리운영, 정보보안 운영관리, 교내 컴퓨터류 관리운영 등에 관한 업무를 수행한다.

제12조(기능) 정보지원팀의 기능은 다음 각 호와 같다.

1. 시스템 운영 : 교내 정보시스템 구축 및 운영, 서버장비유지관리, 소프트웨어관리, 교내 컴퓨터류 관리, 행정부서 전산업무지원, 전자우편 운영
2. 시스템 개발 : 종합정보시스템 운영 및 개발, 각종 데이터베이스 구축 및 백업, 전산자원 활용에 따른 개발
3. 전산망 관리 : 교내 전산망 유지보수 및 관리, 전산망 사용자 지원, 해킹 및 보안사고 예방
4 홈페이지 관리 : 교내 홈페이지 개발 및 운영, 서버관리, 게시판 관리
5. 정보보호 : 정보보안 기술적 보호조치, 네트워크 보안, PC보안

제4장 정보시스템 개발 · 유지 · 관리

제13조(프로그램 개발) ① 프로그램을 개발하거나 수정하고자 할 경우에는 다음의 각호

에 의한다.
1. 실무부서가 새로운 프로그램의 개발을 요청할 경우 정보지원팀과 6개월 전에 협의해야 하며, 이미 개발한 프로그램을 수정할 경우에는 1개월 전에 협의해야 한다.
2. 업무에 대한 전문성이 필요한 경우 정보지원팀은 실무부서의 인원지원을 요청할 수 있다.
3. 개발대상 업무의 규모, 소요기간, 인원 등의 부족으로 인해 정보지원팀에서 자체 개발이 곤란할 때에는 개발업무의 일부 또는 전부를 외부 용역으로 개발할 수 있다.
4. 프로그램에 대한 개발, 수정이 필요한 경우 실무부서장 명의의 문서로 개발 및 수정을 의뢰한다. 다만 경미한 사항의 경우에는 구두로 의뢰한다.
② 프로그램 개발기간에는 다음의 각호 사항을 준수해야 한다.
1. 모든 프로그램은 접근하는 데이터의 정보등급에 따라 해당 프로그램의 보안등급을 설정한다.
2. 프로그램의 계획서 및 설계서는 보안업무규정에 근거해 보안대책이 마련되어야 하며, 프로그램 개발 시에 이를 반영해야 한다.
3. 별도지침에 의해 중요자료로 분류된 프로그램은 정보보안을 위해 사용자 계정 및 패스워드를 설정해야 한다.
4. 프로그램에서 사용하는 사용자계정. 패스워드 및 기타 전산망 접근과 관계된 중요정보는 소스코드로부터 분리해 1차 인식이 불가한 암호화된 형태로 존재해야 한다.
5. 별도지침에 의해 중요자료로 분류된 프로그램은 개발 시 시스템 사용에 대한 로그정보를 관리함을 원칙으로 한다.
제14조(프로그램 관리) ①전산자료(데이터베이스) 처리(입력, 수정, 출력 포함)는 해당 실무부서에서 관리, 운영하며 이에 대한 책임은 실무부서장에 있다.
② 중요자료로 분류된 프로그램은 정보보안을 위해 사용자 계정 및 비밀번호를 설정한다.
③ 사용자 계정 및 비밀번호는 1차 인식이 불가한 암호화된 형태로 존재해야 한다.
④ 사용자 로그인 정보를 관리한다.
⑤ 소스프로그램은 해당서버와 별도의 백업 서버에 보관한다.
제15조(프로그램 운영) ① 프로그램 운영자는 프로그램 사용자 계정에 대한 패스워드 변경을 최소 6개월에 1회 이상 실시해야 한다.
② 프로그램 운영자는 시스템 사용에 대한 로그 정보를 주기적으로 분석해 자료의 불법접근 및 변조에 대한 위험성을 사전에 방지해야 한다.
③ 프로그램의 추가, 삭제, 변경은 부서장의 허가를 받은 후에 시스템 관리자에 의해 실시되어야 한다.
④ 운영중인 시스템 내에 소스프로그램을 설치하지 않는 것을 원칙으로 한다.
⑤ 별도지침에 의해 중요자료로 분류된 프로그램은 가동 전 정보지원팀의 보안검증을 받아야 한다.
제16조(적절성 확보) 정보시스템 이용자는 시스템 사용에 있어 적절성을 유지해야 한

다. 다만, 다음 각 호에 해당하는 경우에는 부적절한 사용으로 간주해 제재 조치를 취할 수 있다.
1. 타 사용자의 계정 및 패스워드를 허가 없이 사용한 경우
2. 타 사용자의 정당한 사용을 방해한 경우
3. 타 사용자의 자료를 허가 없이 유출하거나 읽고 쓰는 행위
4. 일반사용자가 관리자 또는 타 사용자의 패스워드를 획득하고자 해킹하는 행위
5. 내부의 중요 전산정보를 불법으로 외부에 유출한 경우
6. 외부의 불법사용자에게 계정 및 패스워드를 제공한 경우
7. 사용자 계정 및 패스워드를 상호 공유하는 행위
8. 허가된 보안등급 이상의 자료를 무단유출 하거나 읽고 쓰는 행위
9. 보안점검의 지적사항에 대해 즉각적인 시정을 취하지 않는 경우

제17조(사용자 제재) ① 제16조에 규정된 사항에 해당할 경우에는 사용자의 계정을 회수•삭제해 정보시스템의 사용을 제한 또는 금지하며, 그에 따른 구체적 제재 사항은 위원회에서 심의한다.
② 정보시스템의 불법사용으로 학교에 해를 끼치거나 명예를 훼손시켰을 경우에는 다음 각호의 제재 조치를 취할 수 있다.
1. “정보통신망 이용촉진 등에 관한 법률” 및 “개인정보보호법” 위반에 의한 법적 조치
2. 정보시스템의 손해발생에 대한 손해배상 청구

제18조(소프트웨어 패키지관리) ①연구지원, 문서작성, 자료처리 등 이미 개발되어 있는 소프트웨어 패키지가 필요한 경우에는 정보지원팀에 의뢰하여 해당 목적에 적합한 프로그램 정품을 구입하여야 하며, 구입한 프로그램은 정보지원팀 자산으로 등록 관리 한다.
②교내 공공목적으로 구입한 프로그램은 개인이 임의의 목적으로 설치 사용하거나 프로그램을 훼손시켜서는 안된다.

제5장 유·무선 네트워크 관리

제19조(네트워크 장비관리) ① 네트워크 장비가 설치, 운영 중인 건물별 층별 IDF실은 네트워크 담당자외 출입을 금하며, 잠금장치를 통해 출입을 제한한다.
② 장비관리 및 운영을 위해 담당자 외에 출입을 해야 할 경우 “IDF실 출입자 관리대장” 기록 후 담당직원 입회하에 출입한다.
③ 출입 시 개인 휴대장비(노트북, 보기기억매체 등)는 소지할 수 없으며 장비점검 및 수리를 위해 필요한 경우 정보지원팀 내에서 원격접속을 통하여 점검할 수 있다. 단 휴대장비 점검(OS버젼 및 백신버젼 확인, 본교IP 설정 등)을 확인한 후 “외부업체 개인 휴대장비 점검 일지” 작성 후 담당직원 입회하에 점검을 실시한다.
④ 교내 네트워크 장비의 예방정비는 정비보수 업체와 유지보수 계약을 체결하여 계약조건에 준하여 실시하되 실시 후 “정기. 수시 점검보고서”를 받아 보관한다.

제20조(유·무선 사용방법) ① 본교 네트워크를 사용하기 위해서는 정보지원팀에서

IP주소 또는 무선ID를 발급 받아야 한다.
② 정보지원팀의 승인 없이 IP를 변경하거나 랜 카드를 변경한 경우에는 이를 불법 사용자로 간주해 네트워크 사용을 제한한다.
③ 유선네트워크를 사용을 위해 본교에서 운영중인 보안Agent인 APC Agent를 설치하여야 하며 설치에 관한 지원은 정보지원팀에서 한다. 단 . 기숙사 네트워크망 이용시에는 적용되지 않는다.
제21조(LAN 설치) ① 신규 및 이전설치를 요구할 경우에는 부서장의 결재를 득한 "전산작업의뢰서(홈페이지 종합정보시스템에서 작성)"를 정보지원팀에 제출한다.
② 신규 및 추가 설치 신청은 수시로 접수하며 학기 시작 전 설치를 원칙으로 한다. 단, 긴급을 요하는 경우에는 이를 정보지원팀과 협의 후 처리한다.
③ 정보지원팀의 사전 허가없이 무단으로 공유기를 사용할 수 없으며, 이로 인하여 발생되는 네트워크 장애에 대한 책임은 공유기를 무단으로 설치자 한 자에게 있다.
④ IP주소 및 무선ID의 사용료
1. 교직원, 학생은 IP주소 및 무선ID를 무료로 사용할 수 있다.
2. 단, 교직원, 학생 외에 교내전산망을 사용하고자 하는 외부업체 또는 개인은 정보지원팀의 허가를 받아 사용할 수 있다
제22조(장애 접수) ① 네트워크 사용 중에 문제가 발생할 경우에는 장애 내용을 신고해야 한다.
② 네트워크 장애 신고 방법은 전화 또는 "전산작업의뢰서"에 의한다.
제23조(IP주소 할당) ① IP주소 할당은 다음과 같다.
1. 본교 자산으로 등록된 컴퓨터류에 한해 부여하는 것을 원칙으로 하며 개인 컴퓨터류에 IP를 부여 받기위해서는 정보지원팀에서 할당 받아야 한다.
2. IP주소는 소유가 아닌 대여로 사용되며 할당받은 IP주소를 타 기관 또는 개인에게 위임하거나 판매할 수 없다.
② IP주소 할당은 지속적으로 변경, 보완될 수 있으며 이후의 변경된 내용은 전화 또는 E-Mail로 통보한다.
제24조(IP주소 신청) IP주소 및 무선ID의 신청, 변경, 반납은 다음 각 호와 같다.
1. IP주소의 경우에는 "IP주소 신청서"를 작성하여 정보지원팀에 제출해야 한다.
2. 무선ID의 경우에는 공지된 해당 웹서버에서 온라인으로 신청을 한다.
제25조(IP주소 회수 및 반납) ① 다음 각 호의 1에 해당할 경우에는 IP주소를 회수 할 수 있다.
1. 정해진 절차에 따라 IP주소를 반납하는 경우
2. IP주소 신청서나 증빙서류의 내용을 허위로 작성한 경우
3. IP주소를 무단 사용하는 경우, 기존 부여된 IP주소를 회수 할 수 있다.
② IP주소를 반납 할 경우에는 "IP주소 신청서"를 정보지원팀에 제출해야 한다.
제26조(도메인 네임의 등록) ① 도메인 네임 등록 원칙은 다음과 같다.
1. 도메인 신청은 정보지원팀와 사전 협의 후 문서접수를 통하여 처리한다.

2. 도메인 네임은 소유권이 아니라 인터넷을 이용하기 위한 이용권으로 간주한다.
3. 전세계 인터넷주소 관련 권고문서(RFC-2181, RFC-2182)를 준수해야 한다.
4. 도메인 이름은 본교 교내 네트워크에 연결 확인 후 인터넷 연결과 도메인 네임서비스가 가능한 상태에서 인터넷 서비스 이용(web, ftp, mail 등)을 목적으로 신청한다.
② 도메인 네임을 등록, 변경, 반납 하고자할 경우에는 도메인 네임 등록 신청서를 작성해 부서장 또는 학부장의 결재를 득한 후 정보지원팀에 제출해야 한다.
③ 도메인 네임 등록 결과는 전화 또는 메일로 통보한다.

제27조(도메인 네임의 회수) ① 다음 각 호의 1에 해당할 경우에는 도메인 네임을 회수할 수 있다.
1. 공문에 의해 도메인 네임을 반납하는 경우
2. 도메인 네임 등록 신청서를 허위로 작성한 경우
3. 도메인 네임과 관련해 변경내용을 통보하지 않은 경우
② 도메인 네임의 회수는 이용자에게 사전에 통보하고 5일 이내에 해당 도메인 네임을 자동 삭제하는 것을 원칙으로 하나 이용자 확인이 안 될 경우 바로 삭제한다.

제6장 전산자료 및 데이터베이스 관리

제28조(자료의 관리) ① 데이터베이스 로그인 계정 관리기준은 DBMS관리자(DBA), 프로그램 개발자 및 사용자에 따라 권한을 차등 부여하고, 패스워드는 암호화된 형태로 존재하도록 한다.
② 데이터베이스의 무결성 유지를 위해 데이터베이스의 수정은 적법한 인가자에 의해서만 이루어 져야 하며, 물리적인 재해로부터의 보호를 위해 주기적으로 백업해야 한다.
③ 데이터베이스에 대한 모든 접근은 감사기록을 유지하되, 일반사용자의 감사기록에 대한 접근은 제한되어야 한다.
④ 데이터베이스 관리자(DBA)는 누가 어떤 필드, 레코드 수준에서 접근할 수 있는가를 정의해야 한다.
⑤ DBMS는 시스템과는 별도의 사용자 인증 기능을 수행해야 한다.
⑥ 데이터베이스의 데이터는 프로그램을 통해서만 접근한다.
⑦ 별도지침에 의해 중요자료로 분류된 자료 및 데이터베이스는 데이터의 접근 정보를 기록해 주기적인 점검 및 분석을 실시한다.
⑧ 데이터베이스의 보안 및 안정성 확보를 위해 데이터베이스 유지관리업체와 계약을 체결하여 데이터 유지 및 관리를 실시하며, 매월 “정기. 수시 점검보고서”를 받아 보관한다.

제29조(자료의 보관) ① 별도지침에 의해 중요자료로 분류된 자료는 별도의 보호된 장소에 보관하고, 재해 및 비상시를 대비한 계획을 수립해 운영한다.
② 별도지침에 의해 중요자료로 분류된 자료의 이용 및 변경은 부서장의 허가와 관리책임자의 입회하에 이용 및 변경할 수 있다.

제30조(자료의 파기) ① 별도지침에 의해 중요자료로 분류된 자료의 파기는 자료 보관책임자의 입회하에 담당자가 파기를 실시하고, 자료관리 대장의 파기 확인란에 입회자는 파기 확인을한다.
② 자기테이프 등의 자기매체 자료의 파기는 컴퓨터를 이용해 내용을 완전히 삭제하고, 자료접근이 불가능해 내용을 지울 수 없는 자기매체의 자료는 소각 또는 용해 등의 방법으로 파기한다.
③ 소규모의 전산파지는 분쇄기를 이용하고, 대규모의 파지는 소각장에서 소각시키거나 분쇄업체를 통해 분쇄확인서를 발부 받아 부서장의 결재를 받는다.
제31조(자료의 사용) ①데이터베이스 자료관리(입력, 수정, 삭제, 출력 등)는 해당 부서의 업무 담당자가 정보시스템을 통하여 관리함을 원칙으로 한다.
②데이터베이스 자료에 대한 출력은 해당부서(데이터 권한 또는 사용부서)에서 직접 행할 수 있도록 한다.
③데이터베이스 자료를 출력물인 아닌 화일 형태로 변환하여 사용할 경우 부서장의 결재를 득한 후 사용하여야 하며, 보조기억매체에 저장하여 사용할 경우 "USB메모리 등 보조기억매체 보안관리지침"에 준하여 사용해야 한다.

제7장 컴퓨터 관리

제32조(컴퓨터 사용) ① 컴퓨터 기동 시 OS 및 화면보호기에서 제공하는 패스워드를 설정한다.
② OS 및 바이러스 백신 프로그램의 최신 보안 패치를 유지해야 하며, 무단으로 백신 Agent를 삭제할 수 없으며, 정보지원팀에서 지정한 백신프로그램 외에는 무단으로 설치할 수 없다.
③ 장시간 자리를 비울 때는 전원을 끈다.
④ 자신의 업무에 사용하는 응용 프로그램은 시스템 담당자의 허락 없이 무단으로 타인에게 복사해 주어서는 아니 된다.
⑤ 본교에서 구매하여 정식 라이센서를 취득한 소프트웨어 외에 불법으로 취득한 소프트웨어는 절대 설치할 수 없다.
⑥ USB 등 보조기억매체를 사용할 때 또는 데이터를 전송할 때에는 바이러스 검사를 한다.
⑦ 중요한 정보는 컴퓨터 내에 보관하지 아니 하며, 별도의 USB 등 보조기억매체에 담아 물리적인 보안이 철저한 위치에 보관한다.
⑧ 자산으로 등록 된 교내 모든 컴퓨터는 교외로 반출 될 수 없으며 연구 및 교육을 목적으로 반출 될 경우 해당 부서장의 결재 및 기획관리부처장의 허가를 득한 후 반출할 수 있다.
제33조(컴퓨터 관리) ① 자산으로 등록 된 교내 모든 컴퓨터 O.S 및 백신프로그램은 최신버젼으로 패치시켜야 하며, 수시 점검을 통하여 컴퓨터 사용에 지장이 없도

록 해야한다.
② 자산으로 등록 된 교내 모든 컴퓨터류는 매학기별 자산조사를 통하여 컴퓨터류 관리에 철저를 기하여야 한다.
③ 수리불가 및 수리비용 과다발생, 내용년수 초과 등으로 관리가 어려운 컴퓨터류에 대해 "자산관리규정"에 준하여 폐기처리를 진행한다.
제34조(바이러스 예방 및 조치) ① 정보지원팀은 컴퓨터 바이러스 발생이 우려되는 날짜에는 미리 게시판이나 메일 등을 통해 경고 메시지 게시 등의 조치를 취한다.
② 바이러스 감염 및 확산방지를 위해 최신 백신프로그램을 설치하며, 수시로 패치될 수 있도록 백신 Agent를 필히 설치 운영한다.
③ 바이러스에 의한 데이터 손상에 대비해 정기적으로 데이터 백업을 실시한다.

제8장 보안관리

제35조(기본 수칙) ① 정보시스템 사용자는 개인별 사용자 계정 및 패스워드의 기밀을 유지해야하며, 본래의 발급 목적으로만 사용해야 한다.
② 전산자원의 사용을 원하는 자는 허가 받은 정보시스템의 권한이 부여된 영역에 대해 본래의 목적으로만 사용할 수 있다.
③ 정보시스템 사용자는 정보시스템의 성능저하 및 보안상 위험을 초래할 수 있는 행위를 해서는 아니 되며 만약 그런 행위가 발생한 경우 소속 부서의 장 또는 정보지원팀에 이를 즉시 알려야 한다.
④ 정보자산과 연관된 저작권, 특허권 및 소프트웨어 라이센스의 사용 조건을 숙지하고 이를 준수해야 한다.
⑤ 학내 전산망을 신설, 변경 및 폐기하고자 하는 경우에는 정보지원팀의 사전승인을 얻어야한다.
⑥ 외부 전산망에서 학내 전산망으로의 접근은 학교에서 승인한 시스템을 제외하고는 원칙적으로 허용하지 아니한다.
⑦ 모든 정보자산은 보안등급에 따라 분류 관리한다.
⑧ 주기적인 보안점검을 통해 학내 전산망 및 정보시스템의 안전성을 점검하고, 정보보안 정책 및 규정의 준수 여부를 평가한다. 다만, 학내 모든 사용자는 이에 적극 협조해야 한다.
⑨ 업무와 관련해 습득한 자료 및 정보는 본교의 허가 없이 외부에 누출해서는 아니 된다.
⑩ 정보보안 사고의 책임은 원칙적으로 사용자 본인에게 있다.
⑪ 위 사항에 언급되지 않은 내용은 "정보보안관리규정"에 준한다.
제36조(보안등급 기준) ① 보안등급의 분류기준은 다음의 각 호에 따라 정한다.
1. 정보의 중요도
2. 정보(시스템)의 절취 및 불법변경 시 손실 가치
3. 정보(시스템)의 파괴 시 복구비용

4. 정보의 사용권자
② 정보자산의 보안등급 및 사용자인가는 전항의 기준에 따라 별도로 정한다.
제37조(보안점검) ① 시스템관리자는 "정보보안관리규정"에 의해 담당서버에 대해 년 1회 이상의 정기 점검과 필요시 수시 점검을 실시한다.
② 보안점검을 실시한 후 그 결과를 기획관리처장에게 보고하고 지적된 사항에 대한 조치를 취한다.
제38조(전산자원 보안관리) 전산자원 보안을 위해 방화벽 시스템 및 기타 보안 프로그램 등을 이용하여 외부 통신망에 1차적인 보안체계를 갖추어야 한다.
1. 서버관리 : 시스템 운영실에 설치하여 사용자계정 및 비밀번호에 의하여 관리한다. 다만, 서버를 업무현장에 둘 필요가 있다고 인정된 경우에는 업무현장에 서버를 설치하되 업무부서의 장이 책임 관리 한다.
2. 데이터베이스 자료 : 데이터베이스 관리자를 지정하여 관리 책임을 부여하고 각 계정에 비밀번호를 지정하고 수시로 변경하며, 자료의 중요성에 따라서 매일 백업매체에 자료를 받아 일정한 장소에 보관한다.
3. 개발 프로그램 관리 : 개발 프로그램은 개발자의 컴퓨터에서 개발하며 소스 프로그램 보관을 위하여 매일 백업매체로 이관한다.
4. 정보지원팀 관리 : 시스템운영은 통제구역으로 지정하여 보안장치를 설치해야 하며, 시스템의 안정운영을 위하여 설비자료의 점검과 유지보수를 실행하고, 통제구역 출입자를 관리대장에 기록 하도록 조치한다.
제39조(사용자 보안관리) ①사용자 보안관리를 위해 다음 각호의 업무에 사용자 계정을 발급한다.
1. 정보시스템 사용자계정
2. 웹메일 사용자계정
3. 인트라넷 사용자계정
4. 인터넷디스크 사용자 계정
5. 기타 정보서비스에 필요한 사용자 계정
②개인용 컴퓨터는 항시 네트워크를 통한 외부시스템과 연결되어 있기 때문에 외부침입의 매체로 사용될 수 있으므로 사용자는 정보지원팀에서 제공하는 보안 프로그램 및 백신프로그램을 설치하여 사용해야 한다.
제40조(개인정보 보호) ①업무와 관련된 개인정보를 "개인정보보호법"에서 정한 적법한 승인절차를 거치지 않고 외부에 제공 또는 열람시킬 수 없다.
②개인정보 관리는 관련된 부분별로 해당 부서에서 자료의 수정, 추가, 삭제 등 제반관리를 담당하며, 정보지원팀은 서버에 저장된 데이터베이스 자료 보전을 담당한다.
제41조(보안사고의 처리 및 조치) 보안사고가 발생할 경우 정보지원팀은 다음 각호의 단계에 따라 적절한 조치를 취해야 한다.
1. 침입자의 침입예방을 위해 침입 가능성이 있는 부분을 수시로 점검해 불법침입자의

침입을 사전에 예방한다.
2. 시스템관리자는 자신의 시스템에 비정상적인 활동이나 징후가 보이면 무단 침입자의 유무를 즉각 점검해야 한다.
3. 침입자가 시스템에 침투해 해킹을 하고 있을 경우 “보안사고 대응 절차 및 지침”에 따라 필요한 조치를 취하고 기획관리처장에 보고해야 한다.
4. 침입자를 몰아냈거나 로그파일의 분석을 통해 침입한 흔적이 발견된 경우 즉시 보고하고, 보안 진단 도구나 체크리스트를 이용해 정보자료의 이상 유무를 점검해야 한다.
5. 침해사고 발생에 따른 침해사고 대응 절차에 따라 자체적으로 복구를 수행하고, 자체적인 복구가 어려울 경우 정보통신부, 한국정보보호진흥원 인터넷 침해사고 대응지원센터 등 인터넷 침해사고 대응관련기관에 사고 신고를 한다.
6. 인터넷 사고 중 해킹, 인터넷을 이용한 사기, 주민등록번호의 도용 등 침해 행위에 대해 침해 행위자에 대한 수사 등 법적인 처리를 고려하는 경우에는 경찰청 사이버테러대응센터에 신고해 지원을 받을 수 있다.
7. “개인정보보호법”에 따른 법적 조치를 취한다.

제42조(보안 교육) ① 본교 모든 구성원을 대상으로 정보보안 교육을 실시한다.
② 보안에 대한 인식을 제고하고 사용자와 시스템 관리자의 부주의나 고의에 의한 보안 사고를 최소화한다.
③ 보안교육은 년 1회 이상 정기교육과 필요에 따라 수시 교육을 실시한다.

제9장 홈페이지 운영

제43조(홈페이지 관리) 본교 홈페이지는 다음 각 호와 같이 관련 부서와 협조하여 운영한다.
1. 홈페이지 운영의 전체적인 계획수립, 시안결정, 화면구성 등은 기획총괄 부서 및 홍보지원 부서와 협의한다.
2. 프로그램 소스, 데이터베이스 자료, 관련 프로그램 관리, 운영 및 홈페이지 운영에 필요한 기술 지원(프로그램 제작, 수정, 삭제 등)은 정보지원팀에서 담당한다.
3. 홈페이지 사이트 및 페이지별 자료는 해당부서에서 관리하며, 수시로 제공하여 항상 최신의 정보가 게재되도록 해야 한다.

제44조(게시글 관리) ①“게시글”이라 함은 본교 홈페이지에 설정된 각종 패널에 등재된 내용을 말하며, 각 게시글의 등재/삭제는 해당 부서에서 적정한 절차를 거쳐 처리하여야 한다.
②게시글의 원활한 운영을 위하여 해당 부서장은 게시글 담당자를 지정할 수 있으며, 이를 수시로 점검하여 신속한 정보전달 및 의견수렴의 장이 될 수 있도록 운영한다.
③게시글 내용의 투명성 확보를 위하여 실명제를 적용할 수 있으며, 게시판의 목적에 부합되지 않는 내용 등은 다변에 응답하지 않거나 게시자의 동의 없이 삭제할 수 있다.
④ 사용자의 실수로 개인정보가 누출된 경우 이에 대한 책임은 본교가 지지 않는다.

제10장 전자우편 운영관리

제45조(전자우편 주소 및 우편함 할당) ① 본 대학교 재직중인 전임교원 및 직원은 대학교 종합정보시스템의 전자우편 서비스에서 신청하여 관리자의 승인을 거쳐 정해진 전자우편 주소 및 용량을 사용한다.
② 전자우편함의 관리는 사용자 개인의 책임으로 한다.

제46조(사용 대상자 및 이용제한) ① 본 대학교 재직중인 전임교원 및 직원에게 제공을 원칙으로 하며, 퇴직자의 경우 인사발령 사항을 근거로 즉시 회수함을 원칙으로 하며 특별사유 발생시 정보지원팀에 사전승인을 받아 유예할 수 있다.
② 회수된 계정은 메일 수신이 불가하며, 메일 계정과 메일 내용은 삭제되고 복구할 수 없다.
③ 정보지원팀은 다음 각 호의 사항에 대하여 예고 없이 전자우편 주소를 사용 중단 또는 삭제할 수 있다.
1. 불법적인 메일 발송으로 정보자원의 오남용(유출 및 위·변조·불법 행사 등)하는 경우
2. 기타 정보통신 보안유지에 위협이 된다고 판단되는 경우

제47조(준용) 기타 이 규정에 명시되지 아니한 사항은 본교의 관계 규정 및 상위법(관련 국가기관에서 제정한 법)의 관련 항목을 적용한다

부 칙

1.(시행일) 신설되는 이 규정은 2020년 6월 15일부터 시행한다.
2.(경과조치) 이 규정 시행일 이전에 처리된 관련 업무에 대하여는 이 규정에 의하여 처리된 것으로 본다.

부 칙

1. 이 규정은 2022년 12월 27일부터 폐지한다.