문서번호	GCH-규정-01-16	정보보안업무규정	총장
제정일자	2013.09.01.		
개정일자	2020.08.13.		
면 수	13		

제1장 총칙

제1조 (목 적) 이 규정은 교육부 정보보안기본지침에 따라 정보보안을 위하여 경북보건대학교(이하 '본 대학' 이라 칭함)에서 수행하여야 할 기본활동 규정을 목적으로 한다.

제2조 (정 의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

1. '사용자'라 함은 총장으로부터 정보통신망 또는 정보시스템 등에 대한 접근 또는 사용 허가를 받은 모든 인원을 말한다.
2. '인터넷서비스망'(이하 '인터넷망'이라 칭함)이라 함은 본 대학의 네트워크 중에서 인터넷을 사용할 수 있도록 연결되어 있는 인터넷 전산망을 말한다.
3. '정보통신망'이라 함은 전기통신기본법 제2조 제2호의 규정에 따라 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송수신하는 정보통신체제를 말하며 정보시스템 일체를 포함한다.
4. '정보시스템'이라 함은 서버·PC 등 단말기, 보조기억매체, 전산·통신장치·정보통신긱, 응용프로그램 등 정보의 수집·가공·저장·검색·송수신에 필요한 하드웨어 및 소프트웨어를 말한다.
5. '휴대용 저장매체'라 함은 디스켓·CD·외장형 HDD(SSD)·USB메모리 등 정보를 저장할 수 있는 것으로 PC 등의 정보시스템과 분리할 수 있는 기억장치를 말한다.
6. '정보보안' 또는 '정보보호'라 함은 정보시스템 및 정보통신망을 통해 수집·가공·저장·검색·송수신 되는 정보의 유출·위변조·훼손 등을 방지하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위로서 사이버안전을 포함한다.
7. 'RFID'라 함은 대상이 되는 사물 등에 RFID 태그를 부착하고 전파를 사용, 해당 사물 등의 식별정보 및 주변 환경 정보를 인식하여 각 사물 등의 정보를 수집·저장·가공 및 활용하는 시스템을 말한다.
8. '정보통신실'이라 함은 서버·PC 등과 스위치·교환기·라우터 등 네트워크 장치 등이 설치 운용되는 장소를 말하며, 본 대학에서는 전산실을 말한다.
9. '안전측정'이라 함은 정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 해킹·컴퓨터바이러스·서비스방해 등으로부터 정보통신망과 정보를 보호하기 위하여 정보보안 취약점을 진단하는 제반활동의 일체를 말한다.
10. '정보보호시스템'이라 함은 정보의 수집·저장·검색·송신·수신시 정보의 유출, 위·변조, 훼손 등을 방지하기 위한 하드웨어 및 소프트웨어를 말한다.
11. '사이버공격'이라 함은 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스맹해, 랜섬웨어 등

전자적 수단에 의하여 정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 공격 행위의 일체를 말한다.

제3조 (적용범위) ① 본 대학 정보보안업무에 관하여는 따로 정한 경우를 제외하고는 본 규정에 의한다.

② 본 규정은 본 대학 교직원과 학생 및 본 대학에 출입하는 관련업체 및 개인에게 적용한다.

제2장 정보보안 기본활동

제4조 (보안담당관 운영) ① 총장은 효율적·체계적인 정보보안 업무를 수행하기 위하여 정보보안 전문지식을 보유한 인력을 확보하고 관련 전담조직을 구성·운영하여야 한다.

② 제1항과 관련한 정보보안 조직을 지휘하고 소속 및 산하기관에 대한 정보보안 업무를 총괄하기 위하여 '보안담당관'을 임명하여야 한다.

③ 보안담당관은 전산담당자가 소속된 부서의 장이 보직과 동시에 임명되며, 전산·시설에 관한 분임 보안담당관을 임명할 수 있다.

④ 총장이 보안담당관에게 부여하는 기본활동은 다음 각 호와 같다.

1. 보안심사위원회에 정보보안분야 안건 심의 주관
2. 정보보안 업무 지도·감독
3. 정보보안 수준진단
4. 사이버위협정보 수집·분석 및 보안관제
5. 교직원을 대상으로 한 정보보안 교육 및 정보협력
6. 정보보안 예산 및 전문인력 확보
7. 정보보안 사고조사 결과처리

8 그 외 본 규정에서 정하는 정보보안업무에 대한 총괄을 포함

제5조 (활동계획 수립 및 심사분석) ① 보안담당관은 본 대학의 정보보안업무 세부 추진계획을 수립·시행하고 그 추진결과를 심사분석·평가하여 총장에게 보고하여야 한다.

② 제1항의 경우 보안담당관은 세부추진계획 및 심사분석을 「정보보안업무 세부 추진계획」 서식 및 「정보보안업무 심사분석」 서식에 따라 작성하며 관련문건은 기획처에서 자체 보관한다.

문서번호	GCH-규정-01-16	정보보안업무규정	총장
제정일자	2013.09.01.		
개정일자	2020.08.13.		
면 수	13		

1. 보안업무 세부 추진계획 : 3. 25 까지(해당 연도 추진계획)

2. 보안업무 심사분석 : 7. 31 까지(전년도 3/4분기 ~ 해당연도 2/4분기 내용 종합)

제6조 (본 규정 제·개정) 보안담당관은 정보 및 정보통신망 보호를 위한 자체 정보보안 내규(지침·시행세칙 등)를 이 규정에 저촉되지 아니하는 범위에서 작성·운용할 수 있다.

제7조 (사용자 관리) ① 총장은 소관 정보통신망(정보시스템 포함) 사용과 관련하여 사용자의 직위·임무별 정보통신망 접근 자격부여 심사 등 인적보안에 관한 절차 및 방법을 마련하여야 한다.

② 총장은 정보통신망을 통하여 비밀 등 중요정보를 취급하는 사용자에 대해서는 보안서약서 징구 등의 보안조치를 하여야 한다.

③ 보안담당관은 직원이 보직변경, 퇴직, 신규임용 등 인사이동이 있을 경우 관련 정보시스템(웹메일, 통합정보시스템 등) 접근권한을 조정하여야 한다.

④ 총장은 외부인력을 활용하여 정보시스템의 개발, 운용, 정비 등을 수행할 경우에는 해당 인력의 고의 또는 실수로 인한 정보유출이나 파괴를 방지하기 위하여 보안조치를 수행하여야 한다.

제8조 (시스템 보안책임 범위) ① 본 대학의 운영에 관한 일체의 시스템을 도입·사용할 경우, 사용자·시스템관리자 및 관리책임자를 지정 운용하여야 한다.

② 사용자는 PC 등 소관 정보시스템을 사용하거나 본인 계정으로 정보통신망에 접속하는 것과 관련한 보안책임을 가진다.

③ 시스템관리자는 서버·네트워크 장비 등 부서 공통으로 사용하는 정보시스템의 운용과 관련한 보안책임을 가진다.

④ 제1항부터 제3항까지 정보시스템을 실제 운용하는 부서의 처장 또는 센터장이 정보시스템 '관리책임자'가 되며, 관리책임자는 「정보시스템 관리대장」 서식을 수기 또는 전자적으로 운용 관리하여야 한다.

⑤ 관리책임자는 해당 부서의 정보시스템 관리대장에 정보시스템의 변경 최종 현황을 유지 및 관리하여야 한다.

⑥ 보안담당관은 제1항부터 제5항까지 명시된 정보시스템 운용과 관련한 보안 취약점을 발견하거나 보안대책 강구가 필요하다고 판단할 경우, 사용자·시스템관리자 및 관리책임자에게 시정을 요구할 수 있다.

제9조 (정보통신시설 보안) ① 총장은 다음 각 호의 중요 정보통신시설 및 장소를 보호구역으로 설정·관리하여야 한다.

1. 전산실

2. 그 밖에 보안관리가 필요하다고 인정되는 정보시스템 설치 장소

② 총장은 제1항에서 지정된 보호구역에 대한 보안대책을 강구할 경우 다음 각 호 사항을 학교 운영실정에 맞춰 시행한다

1. 방재대책 및 외부로부터의 위해 방지대책

2. 상시 이용하는 출입문은 한 곳으로 정하고 이중 잠금장치 설치

3. 정전에 대비한 비상전원 공급

제10조 (정보보안 교육) ① 보안담당관은 자체 정보보안 교육계획을 수립하여 연 1회 이상 전 교직원을 대상으로 관련 교육을 실시하여야 하며, 정보보안 담당 대상인원은 연간 15시간 이상 관련 전문기관의 교육, 기술세미나에 참석하여야 한다.

제11조 (사이버·보안 진단의 날) ① 보안담당관은 본 대학의 실정에 맞게 매월 세 번째 수요일을 '사이버·보안 진단의 날'로 지정·운영하여야 한다.

② 보안담당관은 '사이버·보안 진단의 날' 운영에 대하여 계획을 수립하고 소관 정보보안업무 전반에 대하여 체계적이고 종합적인 보안진단을 실시하여야 한다.

제12조 (재난방지) ① 보안담당관은 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애 발생에 대비하여 정보시스템 백업관리, 복구 등 종합적인 재난방지 대책을 수립·시행하여야 한다.

② 정보시스템 장애에 대비한 백업시설을 확보하고 정기적으로 백업을 수행하여야 한다.

③ 제3항에 따른 백업시설을 설치할 경우에는 전산실과 물리적으로 일정거리 이상 떨어진 안전한 장소에 설치하여야 하며 전력공급원 이원화 분리 등 정보시스템의 가용성을 최대화 할 수 있도록 하여야 한다.

제3장 요소별 보안관리

제13조 (PC 등 단말기 보안관리) ① 단말기 사용자는 PC·노트북·스마트기기 등 업무수행에 필요한 단말기(이하 'PC'라 칭함) 사용과 관련된 일체의 보안관리 책임을 가진다.

② 보안담당관은 비인가자가 PC등을 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손시키지 못하도록 다음 각 호의 보안대책을 학교의 운영여건에 맞도록 보안대책을 사용자에게 지

원하며, 사용자는 이를 준수하여야 한다.

1. 장비(CMOS 비밀번호)·자료(개인정보 등 중요문서 자료 비밀번호)·사용자(PC 로그인 비밀번호) 에 대한 비밀번호를 월 1회 변경 사용한다.
2. 10분이상 PC작업 중단 시 비밀번호가 적용된 화면보호기 적용
3. 내PC지키미를 활용한 운영체제(OS) 및 응용프로그램의 최신 보안패치 유지
4. 업무상 불필요한 응용프로그램 설치 및 공유 폴더의 삭제
5. 그 밖에 교육사이버위협 정보공유시스템 상 안전성을 확인하여 배포·승인한 프로그램의 운용 및 보안권고문

③ 사용자는 PC 등 단말기를 교체·반납·폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 관리책임자와 협의하여 하드디스크에 수록된 자료가 유출, 훼손되지 않도록 보안조치하여야 한다.

④ 사용자는 PC등을 기관 외부로 반출하거나 내부로 반입할 경우에 관리책임자와 협의하여 최신 백신 등을 활용하여 해킹프로그램 및 웜바이러스 감염여부를 점검하여야 한다.

⑤ 개인소유의 스마트폰을 제외한 PC 등 단말기를 무단 반입하여 사용하여서는 아니된다. 다만, 부득이한 경우에는 보안담당관의 승인을 받아 사용할 수 있다.

제14조 (서버 보안관리) ① 전산담당자는 서버를 도입·운용할 경우, 보안담당관과 협의하여 해킹에 의한 저료 절취, 위·변조 등에 대비하여 다음 각 호의 내용을 포함한 보안대책을 수립·시행하여야 한다.

1. 서버 내 저장자료에 대해 업무별·자료별 중요도에 따라 사용자의 접근권한을 차등 부여
2. 사용자별 자료의 접근범위를 사버에 등록하여 인가여부를 식별토록 하고 인가된 범위 이외의 자료접근을 통제
3. 서버 운용에 필요한 서비스 포트 외에 불필요한 서비스 포트 제거 및 관리용 서비스와 사용자용 서비스를 분리 운용
4. 서버 관리용서비스 접속 시 특정IP와 MAC주소가 부여된 관리용 단말을 지정·운용
5. 서버 설정 정보 및 서버에 저장된 자료에 대해서는 정기적으로 백업을 실시하여 복구 및 침해행위에 대비
6. 데이터베이스에 대하여 사용자의 직접적인 접속을 차단하고 개인정보와 같은 중요정보를 암호화하는 등 데이터베이스별 보안조치를 실시

② 전산담당자는 제1항의 각 호에서 수립한 보안대책의 적절성을 수시로 확인하고, 연1회 이상 보안도구를 이용하여 서버설정 및 저장자료의 절취, 위·변조 가능성 등 보안취약점을 점검하여야 한다. 이 경우 보안담당관은 서버 관리자가 수행한 사항이 적절한지 확인하고 시정조치를 권고할 수 있다.

제15조 (학교 홈페이지 게시자료 보안관리) ① 사용자는 개인정보 등 민감내용을 포함한 자료를 홈페이지에 공개하여서는 아니된다.

② 홈페이지에 정보를 게시하고자 하는 부서의 장은 홈페이지 관리책임자와 사전 협의하여 비밀 등 비공개 자료가 홈페이지에 게시되지 않도록 하여야 한다.

③ 사용자는 인터넷 블로그·카페·게시판·개인 홈페이지 도는 소셜네트워크 서비스(SNS) 등 일반에 공개된 전산망에 업무관련 자료를 무단 게재하여서는 아니된다.

④ 전산담당자는 홈페이지 등에 비공개 내용이 게시되었는지 여부를 주기적으로 확인하여야 하며, 개인정보를 포함한 중요정보가 홈페이지에 공개되지 않도록 보안교육을 주기적으로 실시하여야 한다.

⑤ 전산담당자는 홈페이지 중요정보가 공개된 것을 인지할 경우 이를 즉시 차단·삭제하는 등의 보안조치를 강구·시행하고, 신속히 보안담당관에게 보고하여야 한다.

⑥ 위의 제1항부터 6항까지의 사항은 학교 메인홈페이지를 포함한 동일한 도메인을 사용하는 모든 학과(부)를 포함한 홈페이지에 동일하게 적용된다.

제16조 (사용자 계정관리) ① 전산담당자는 사용자에게 정보시스템 접속에 필요한 사용자계정(ID) 부여 시 비인가자 도용 및 정보통신시스템 불법 접속에 대비하여 다음 각 호의 사항을 반영하여야 한다.

1. 사용자별 또는 그룹별로 접근권한 부여
2. 외부인에게 계정 부여는 불허하되 업무상 불가피 한 경우 총장 책임하에 필요업무에 한해 특정기간 동안 접속토록 하는 등 보안조치 강구 후 허용
3. 비밀번호 등 사용자 식별 및 인증수단이 없는 사용자계정 사용 금지

② 전산담당자는 사용자가 5회 이상에 걸쳐 로그인 실패 시 정보시스템 접속을 중단시키도록 시스템을 설정하여야 한다.

③ 전산담당자는 사용자의 퇴직 또는 보직변경 발생 시 사용하지 않는 사용자계정을 신속히 삭제하고, 특별한 사안이 없는 한 유지보수 등을 위한 외부업체 직원에게 관리자계정 제공을 금지하여야 한다.

④ 시스템관리자는 사용자계정의 부여 및 관리가 적절한지 연2회 이상 점검하여야 한다. 이 경우 보안담당관은 시스템관리자가 수행한 사항이 적절한지 확인하고 시정조치를 권고할 수 있다.

제17조 (비밀번호 관리) ① 사용자는 비밀번호 설정 사용 시 정보시스템의 무단사용 방지를 위하여 다음 각 호와 같이 구분하여야 한다.

1. 비인가자의 정보통신시스템 접근방지를 위한 장비 접근용 CMOS 비밀번호(1차)

2. 정보시스템 사용자가 서버 등 정보통신망에 접속 인가된 인원인지 여부를 확인하는 WINDOW 사용자인증 비밀번호(2차)
3. 개인정보를 포함한 중요문서에 대한 열람·수정 및 출력 등 사용권한을 제한할 수 있는 자료별 비밀번호(3차)
4. 10분 이상 PC작업 중단 시 비밀번호가 적용된 화면보호기 적용(4차)

② 중요자료에는 자료별 비밀번호를 반드시 부여하되, 공개 또는 열람자료에 대해서는 부여하지 아니할 수 있다.

③비밀번호는 다음 각 호의 사항을 반영하여 영문 대문자, 소문자, 숫자, 특수문자 중 2가지 종류 조합은 10자리 이상, 3종류 이상 조합은 8자리 이상으로 설정하고 주기적으로 변경·사용하여야 한다.(단, 장비접근용 CMOS 비밀번호에는 해당하지 아니한다.)

1. 사용자계정(ID)과 동일하지 않은 것
2. 개인 신상 및 부서 명칭 등과 관계가 없는 것
3. 동일단어 또는 숫자를 반복하여 사용하지 말 것
4. 동일 비밀번호를 여러사람이 공유하여 사용하지 말 것
5. 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지

제18조 (네트워크 보안관리) ① 전산담당자는 라우터, 스위치 등 네트워크 장비 운용과 관련하여 다음 각 호의 보안조치를 강구하여야 한다.

1. 네트워크 장비에 대한 원격접속은 원칙적으로 금지하되, 유지보수업체의 원격작업이 필요할 경우 보안담당관 승인하에 「외부업체 원격작업 신청(승인)서」를 작성하고 필요한 보안조치를 적용한다.
2. 물리적으로 안전한 장소에 설치하여 비인가자의 무단접근 통제
3. 네트워크장비 등 신규 전산장비 도입 시 생성되는 기본계정을 삭제 또는 변경하고 시스템 운영을 위한 관리자 계정 별도 생상
4. 전산실에 도입된 소프트웨어·운영체제 등의 최신 업데이트 여부를 주기적으로 확인하여 항상 최신버전으로 유지
5. 전산담당자는 라우터 등 중요 네트워크 장비의 문제점을 주기적으로 점검하고 보안담당관에게 관련결과를 보고하여야 한다.

제19조 (웹메일 보안대책) ① 총장은 각종 바이러스 등 악성코드로부터 사용자 PC 등 웹메일 시스템 일체를 보호하기 위하여 안전성이 확인된 백신, 바이러스 월(Wall), 해킹메일 차단시스템을 구축하는 등 보안대책을 강구하여야 한다.

② 사용자는 메일에 포함된 첨부파일을 다운로드 시 최신백신으로 악성코드 은닉여부를 검사하

여야 한다.

③ 사용자는 출처가 불분명하거나 의심되는 제목의 전자우편은 열람을 금지하며 악성코드가 포함되어있다고 의심되는 메일 수신시에는 즉시 인터넷망(LAN)을 물리적 분리하고, 보안담당관 또는 전산담당자에게 알려야 한다.

④ 사용자는 웹메일을 사용하는 PC에 대하여 제25조(PC 등 단말기 보안관리)에 명시된 보안조치 사항을 따른다.

제20조 (휴대용 저장매체 보안대책) ① 우리학교에 근무하는 모든 교직원들이 업무상 휴대용 저장매체를 반입이 필요하다고 판단될 경우에는 훼손·분실 등에 대비한 보안대책을 강구하여 「컴퓨터 및 주변장치 반입 신청(승인)서」를 작성하여 보안담당관의 승인 후 반입하여야 한다.

② 반입된 저장매체는 각 부서·학과(부)별로 「저장매체 관리대장」에 등재함을 원칙으로 한다.

③ 관리책임자는 관리대장에 최종 변경된 휴대용 저장매체의 등록현황을 등재하여야 하며 사본 1부를 보안담당관에게 제출하여야 한다.

④ 관리책임자는 소속직원이 미등록 휴대용 저장매체를 무단 반출하거나 미등록 휴대용 저장매체를 사용하지 않도록 감독하여야 하며 이를 위반한 사실을 발견 또는 확인하는 즉시 보안담당관에게 통지하여야 한다.

⑤ 전산담당자는 사용자가 USB 메모리를 PC등에 연결 시 최신 백신으로 악성코드 감염여부를 자동 검사하도록 보안 설정하여야 한다.

⑥ 휴대용 저장매체를 파기 등 불용처리 할 경우 저장되어 있는 정보의 복구가 불가능하도록 완전삭제 프로그램을 사용하여야 한다.

⑦ 휴대용 저장매체 관리책임자는 사용자의 휴대용 저장매체 무단반출 및 미등록 휴대용 저장매체 사용 여부 등 보안관리 실태를 주기적으로 점검하여야 한다. 이 경우 보안담당관은 휴대용 저장매체 관리책임자가 수행한 사항이 적절한지 확인하고 시정조치를 권고할 수 있다.

⑧ 모든 휴대용 저장매체는 아래와 같은 서식으로 기입·표기하여야 한다.

↑ 2.5cm ↓

일반용	(인)
(관리번호)	
정	부

← 5cm →

<디스켓·이동형HDD>

↑ 1cm ↓

일반용	(인)
(관리번호)	

← 2cm→

<USB·CD 등>

※ (인) 란에 보안담당관 또는 관리책임자의 직인을 날인, 휴대용 저장매체의 크기를 고려하여 서식·글자크기 조정가능

⑨ 관리번호는 연-부서·학과(부)명-연번으로 한다. 이 경우 부서·학과(부)명은 약칭을 사용할

수 있다.(예 : 산학협력처 → 산학, 간호학부 → 간호)

제21조 (악성코드 감염 방지대책) ① 총장은 각종 악성코드 감염을 방지하기 위하여 다음 각 호와 같은 대책을 수립·시행하여야 한다.

1. 사용자는 PC의 백신을 최신상태로 업데이트·상시 감시상태로 설정 및 주기적인 점검을 실시하여야 한다.
2. 사용자는 출처, 유통경로 및 제작자가 명확하지 않은 응용프로그램 사용을 금지하고 인터넷 등 상용망으로 자료 입수 시 신뢰할 수 있는 인터넷사이트를 활용하되 최신 백신으로 진단 후 사용하여야 한다.
3. 사용자는 인터넷 파일공유 프로그램과 메신저·대화방 프로그램 등 업무상 불필요한 프로그램 사용을 지양하고 전산담당자는 인터넷 연동구간의 침입차단시스템에서 관련 사이트 접속을 차단하도록 보안설정 하여야 한다.
4. 사용자는 웹브라우저를 통해 서명되지 않은 Active-X 등이 PC내에 불법 다운로드 되고 실행되지 않도록 보안 설정하여야 한다.
5. 제1호부터 제4호까지의 보안대책과 관련하여 전산담당자는 보안담당관과 협조하여 사용자가 적용할 수 있는 보안기술을 지원하여야 한다.

② 전산담당자 또는 PC사용자는 시스템에 악성코드가 설치되거나 감염된 사실을 발견하였을 경우에 다음 각 호의 조치를 하여야 한다.

1. 악성코드 감염원인 규명 등을 위하여 파일 임의삭제 등 감염 시스템 사용을 중지하고 즉시 인터넷망을 물리적 분리한다.
2. 악성코드의 감염확산 방지를 위하여 보안담당관 혹은 전산담당자에게 관련사실을 즉시 알려야한다.

③ 제2항의 조치가 완료된 후 정보보안사고 조사권한이 보안담당관에게 위임되었을 경우, 보안담당관은 감염PC 등에 대하여 다음 각 호의 조치를 하여야 한다.

1. 최신 백신 등 악성코드 제거 프로그램을 이용하여 악성코드를 삭제한다.
2. 감염이 심각할 경우 포맷 프로그램을 사용하여 하드디스크를 포맷한다.
3. 악성코드 감염의 확산 및 재발을 위하여 원인을 분석하고 일련의 예방조치를 수행한다.

④ 보안담당관은 해당기관에 악성코드 감염사실을 확인하여 조치를 권고할 경우, 즉시 이행하여야 한다.

제22조 (정보시스템 유지보수) ① 보안담당관은 정보시스템 유지보수와 관련한 절차·주기·문서화 등에 관한 사항을 아래와 같이 준수하여야 한다.

1. 유지보수 인력에 대한 보안서약서 집행, 보안교육 등을 통한 유지보수 인가 절차를 마련하고 인가된 유지보수 인력만 참여한다.
2. 결함이 의심되거나 발생한 결함·예방 및 유지보수에 대한 기록을 보관한다.
3. 정보시스템의 유지보수 시에는 일시, 담당자 인적사항, 출입 통제조치, 정비내용 등을 기록·유지하여야 한다.
4. 전산담당자는 외부에서 원격으로 정보시스템을 유지보수하는 것을 원칙적으로 금지하여야 하며 부득이한 경우에는 「외부업체 원격작업 신청(승인)서」의 양식을 통해 보안담당관의 승인을 구한 후 보안대책을 강구하여 한시적으로 허용할 수 있다.

제23조 (저장매체 불용처리) ① 사용자 및 전산담당자는 하드디스크 등 저장매체를 불용처리(교체·반납·폐기 등) 하고자 할 경우에는 「정보시스템 저장매체 삭제처리 신청서」양식을 작성하여 보안담당관의 승인 후 저장매체에 수록된 자료가 유출되지 않도록 보안조치 하여야 한다.

② 불용처리시에는 보안담당관, 시설보안 분임보안담당관, 보안위원회 간사가 일정을 조율하여 분기당 1회 불용처리한다.(단, 외부업체에 불용처리를 의뢰할 때에는 보안담당관이 입회하여 삭제 절차·방법 준수여부 등을 확인 감독하여야 한다.)

③ 저장매체에 저장된 자료를 삭제할 경우는 다음 각 호와 같다.

1. 정보시스템의 사용연한이 경과하여 폐기 또는 양여할 경우
2. 정보시스템의 무상 보증기간 중 저장매체 또는 저장매체를 포함한 정보시스템을 교체할 경우
3. 정보시스템의 임대기간이 만료되어 반납할 경우
4. 그 밖에 사용자 변경 등으로 저장자료 삭제가 필요하다고 판단되는 경우

④ 저장매체의 고장수리·자료복구 등을 외부에 의뢰할 경우 저장매체에 보관된 자료의 유출방지를 위하여 보안담당관 입회하에 수리·복구 참여자에 대한 보안서약서 집행·교육 등 필요한 보안조치를 하여야 한다.

⑤ 저장매체의 삭제방법은 다음과 같다.

저장매체 / 저장자료	플로피디스크	광디스크	자기테이프	SSD·USB	HDD
공개자료	완전파괴	완전파괴	완전파괴 / 전용 소자장비 이용 저장자료 삭제	완전파괴	완전포맷 1회

제24조 (정보시스템 위탁운영 보안관리) ① 총장은 소관 정보시스템에 대한 외부업체의 위탁

운영을 최소화하되, 위탁 운영과 관련한 관리적·물리적·기술적 보안 대책을 수립하여 시행하여야 한다.

② 정보시스템의 위탁 운영은 여타 기관 또는 업체 직원이 해당기관에 상주하여 수행하는 것을 원칙으로 한다. 다만, 해당기관에 위탁업무 수행 직원이 상주가 불가한 타당한 사유가 있을 경우, 그러하지 아니할 수 있다.

제4장 정보보안분야 수준진단

제25조 (정보보안 수준진단) 본 대학은 교육부장관의 권한에 따라 매년 정보보안 수준에 대한 진단을 받을 수 있으며 관련사항에 대한 자료를 작성하여 기일 한 제출한다.

제26조 (진단결과 개선대책 강구) ① 진단결과에 대한 교육부의 통보에 대해 개선대책을 강구하여야 한다.

② 총장은 교육부장관이 통보한 수준진단 결과를 자체 정보보안 강화 등의 수립 시에 반영하고 취약요소를 개선·보완하여 정보보안 수준을 제고하여야 한다.

제5장 보 칙

제27조 (다른 법령과의 관계) 이 규정에 명시되지 않은 사항은 다음 각 호의 법령 및 규칙에 따른다.

1. 보안업무규정 및 시행규칙
2. 공공기록물 관리에 관한 법률
3. 정보통신기반보호법 및 동법 시행령
4. 교육부 사이버분야 위기대응 실무매뉴얼

제6장 비밀취급의 인가[신설 2020.08.13.]

제28조(비밀취급인가) ① 비밀취급인가 등급별 부여 대상은 특별한 사유가 없는 한 다음 기

준에 의한다.

1. Ⅱ급 비밀취급인가대상

가. 총장

나. 보안담당관

다. 보안업무 실무자

라. 기타 총장이 필요하다고 인정하는 자

2. Ⅲ급비밀취급인가대상 : 기타 인가권자가 필요하다고 인정하는 자

② 다음의 직위에 보직된 자는 따로 발령 없이 보직과 동시에 Ⅱ급 비밀취급인가를 받은 것으로 간주한다.

1. 총장

2. 기획처장

3. 전산직 실무자

③ 제2항에 의하여 비밀취급인가를 받은 자에 대하여는 경북지방경찰청에 신원조사 후 비밀취급인가증을 교부하여야 한다.

제29조(비밀취급인가의 해제) ① 비밀취급인가를 받은 자가 인가권을 달리하는 타 기관으로 전출(전보)하였거나 퇴직하였을 경우 해당자의 비밀취급인가는 당연 해제된 것으로 보며 별도의 서면 해제 발령을 하지 아니한다.

② 제1항 이외의 경우에 비밀취급인가를 해제하고자 할 때에는 반드시 서면으로 발령하여야 하고, 직원의 인사기록 대장에 그 사실을 포함하여야 한다.

③ 비밀취급인가가 해제된 자는 해제 발령일로부터 3일 이내에 소속 부서에 인가증을 반납하고, 소속부서는 회수한 인가증을 보안담당관에게 반납하여야 한다.

④ 반납된 인가증은 발급권자의 결재를 받아 소각 폐기하고, 별지 제3호 서식의 비밀취급인가증발급대장에 주서로 해제사유, 일시를 기록하여 삭제하여야 하며, 인사기록카드에도 해제 사항을 기록하여야 한다.

제30조(비밀취급인가증의 분실 및 재교부) ① 비밀취급인가증을 분실하였을 때에는 지체 없이 분실사유서(부서장 확인)를 제출하여야 한다. 비밀취급인가증을 분실한 자에 대하여는 그 과실 또는 부주의의 정도에 따라 경고 조치한다.

② 당해 부서장은 분실사유서 제출 후 5일이내에 인가증의 분실로 인하여 야기되는 사고에 대한 책임을 진다는 본인의 서약서와 함께 재발급을 요청하여야 한다.

③ 비밀취급인가의 재발급시에는 서약의 집행을 생략할 수 있다.

문서번호	GCH-규정-01-16	정보보안업무규정	총장
제정일자	2013.09.01.		
개정일자	2020.08.13.		
면 수	13		

부 칙

제1조(시행일) 본 규정은 2013년 9월 1일부터 시행한다[관련근거: 기획-기획-13-038].

부 칙

본 규정은 2019년 3월 1일부터 시행한다.

부 칙

본 규정은 2019년 11월 1일부터 시행한다.

부 칙

본 규정은 2020년 8월 13일부터 시행한다.