정보보호규정개정이력 현황표

번호	개정일자	소속	담당자	개정내용
01	2022. 12. 27	정보지원부	송**	규정 제정

정보보호규정

제 정 : 2022. 12. 27.

제1장 총 칙

제1조(목적) 본 규정은 금강대학교(이하 “본교”라 한다) 정보자산을 훼손, 변조, 도난, 유출 등의 위협으로부터 보호하기 위해 필요한 사항을 규정함을 목적으로 한다.

제2조(적용범위) 본 규정은 본교 정보통신망 및 정보시스템 보안운영 및 관리업무를 대상으로 적용한다.

제3조(용어 정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

① “정보통신망”이라 함은 유·무선을 매개로 하는 다양한 정보통신수단에 의하여 부호, 문자, 음향, 영상 등의 정보를 수집·가공·저장·검색·송수신하는 정보 통신 체계를 말한다

② “정보보호”또는“정보보안”이라 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

③ “전산기계실”이라 함은 서버 등 전산장비와 스위치·교환기·라우터 등 통신 및 전송장비 등이 설치 운용되는 장소를 말한다.

④ “전산자료”,“전자문서”라 함은 전산장비에 의하여 전자기적인 형태로 입력·보관되어 있는 각종 정보(data)를 말하며, 그 자료가 입력되어 있는 USB, 디스크 등 보조기억매체를 포함한다.

⑤ “보조기억매체”라 함은 디스켓·CD·하드디스크·USB 메모리 등 정보를 저장할 수 있는 것으로 정보통신시스템과 분리할 수 있는 기억장치를 말한다.

⑥ “정보보안시스템”이라 함은 정보의 수집 · 저장 · 검색 · 송신 · 수신시 정보의 유출, 위 · 변조, 훼손 등을 방지하기 위한 하드웨어 및 소프트웨어를 말한다.

⑦ “비밀번호”라 함은 전산장비에 저장되어 있는 자료를 무단열람하거나 부정출력하지 못하게 하기 위하여 사용하는 패스워드를 말한다.

⑧ “기밀성”이라 함은 정보가 인가되지 않은 개인이나, 처리과정 등에 누설되거나 공개되지 않는 속성을 말한다.

⑨ “무결성”이라 함은 정보가 고의적 또는 우발적으로 변경, 파괴되지 않고 일관성을 유지하는 속성을 말한다.

⑩ “가용성”이라 함은 인가자가 정보나 정보시스템을 사용 또는 접근하고자 할 때 사용 또는 접근이 가능하게 하는 속성을 말한다.

⑪ “접근통제”라 함은 인가된 사용자, 프로그램, 프로세스, 시스템 등의 주체만이

정보시스템의 자원에 접근할 수 있도록 제한하는 것을 말한다.
⑫ “중요정보”라 함은 노출, 변경, 파괴되면 본교에 지대한 영향을 미칠 수 있는 정보를 말한다.
⑬ “로그”라 함은 시스템 사용에 관련된 전체의 기록, 즉 입출력 내용, 프로그램 사용내용, 데이터 변경 내용, 시작시간, 종료시간 등의 기록을 말한다.
⑭ “프로젝트담당자”라 함은 정보시스템 개발 등의 외부용역사업시 본교의 해당 업무담당자를 말하며, 해당 용역사업 및 용역업체 직원에 대한 관리 책임이 있다.
⑮ “내부망”이라 함은 본교의 보안관리 하에 있는 네트워크 중 라우터를 경계선으로 하여 보호받는 본교의 주요 네트워크를 말한다.
⑯ “외부망”또는 “상용망“이라 함은 내부망을 제외한 모든 네트워크를 말한다.
⑰ “웹 페이지(Web Page)”라 함은 인터넷의 월드 와이드 웹에 접속했을 때 나타나는 웹브라우저(Web Browser)를 통해 사용자들에게 제공되는 인터넷 서비스를 말한다.
⑱ “웹 서버”라 함은 웹서비스 제공을 위한 웹페이지 등 웹 프로그램의 작업수행 및 주된 정보를 제공하는 컴퓨터시스템을 말한다.
⑲ “단말기”라 함은 시스템에 연결되어 단순히 입·출력 기능만 수행하는 전용단말기와 내부망에 연계되어 운용하고 있는 개인용 컴퓨터를 포함한다.
⑳ “암호프로그램”이라 함은 암호장비·암호자재에 적용되거나 자체적으로 자료를 암・복호화하기 위하여 작성된 프로그램을 말한다.
㉑ “개인정보”라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다.
㉒ “침해사고”라 함은 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등에 의하여 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태를 말한다.
㉓ “외부용역인력”이라 함은 본교의 정보자산을 이용하여 서비스와 기타 업무를 대행하는 자를 말하며 그 예는 아래와 같다.
1.본교에서 일정의 계약을 체결하여 계약조건에 부합되는 업무를 담당하고 지원하는 업체 및 직원
2.하드웨어와 소프트웨어의 개발, 유지보수를 담당하고 지원하는 업체 및 직원
3.아르바이트생 고용 등 단기간 동안 임시 채용된 업체 및 직원
㉔ “외부용역업체”라 함은 ’제3자(Third Party)’ 및 ’외부위탁’ 업체를 총칭한다.
㉕ “정보보호 전문 교육”이라 함은 정보시스템 운영자를 포함한 정보보안책임관, 정보보안담당관, 분임정보보안담당관이 정보보호 기술을 습득하기 위한 전문교육을 말한다.
㉖ “정보보호 기본 교육”이라 함은 전 직원이 정보보호관리체계의 지속적인 운영을 위해 필요한 사항을 습득하기위한 내부교육을 말한다.

㉗ “보호구역”이라 함은 비밀보호와 중요시설 장비 및 자재를 불순분자로부터 보호하고 지속적인 기능 유지를 위해 일정한 장소에 일정한 범위를 지정하여 관리하는 구역으로 제한지역, 제한구역 및 통제구역이 있다.
㉘ “통제구역”이라 함은 보안상 극히 중요한 구역으로 비인가자 출입금지 지역을 말한다.
㉙ “E-mail 시스템”이라 함은 본교에서 대내외적으로 송수신되는 E-mail을 운영, 관리하기 위하여 구축한 하드웨어, 소프트웨어를 총칭한다.

제2장 정보보안 목표 및 기본활동

제4조(기본목표) 본교 정보보안의 기본목표는 본교가 보유하고 있는 중요정보 유출을 방지하고 정보통신시스템 및 정보통신망의 기밀성 · 무결성 · 가용성을 확보하는데 있다.

제5조(활동방향) 본교는 정보보안을 위하여 다음 각 호의 기본활동을 수행한다.

1. 정보보안 정책 및 활동 세부계획 수립 · 시행
2. 취약 정보통신망 보안대책 수립 추진
3. 사이버위협정보 수집 · 분석 및 보안관제
4. 침해사고 대응 · 복구
5. 정보보안 교육계획 수립 · 시행
6. 정보보안 관련 규정 · 지침 등 제 · 개정
7. 기타 정보보안 관련 사항

제6조(연도 정보보안 추진계획 수립) ① 정보보안책임관 및 정보보안담당관은 년간 정보보안 추진계획을 수립 · 시행한다.

제7조(사이버 보안진단의 날 운영) ① 정보보안담당관은 매월 셋째주 수요일을 ‘사이버보안 진단의 날’로 지정한다. 다만, 부득이한 사유로 해당일에 시행하지 못할 경우 같은 달 다른 날에 시행한다.
② 사이버보안진단의 날은 교직원의 보안인식을 제고하고, 해킹 및 정보유출을 사전에 예방하는데 목적이 있다.

제3장 정보보안 조직 체계

제8조(정보보안심사위원회) ① 정보보안 업무에 관한 중요한 사항을 심의・의결하기 위한 정보보안심사위원회는 정보통신자원 운영규정 제2장 제5조에 의하여 정보화추진위원회 (이하 ‘심사위원회’라 한다)가 역할을 대신한다.
② 심사위원회는 다음의 사항을 심의・의결한다.
1. 정보보안과 관련하여 필요하다고 인정하는 사항

제9조(정보보안 조직 구성) ① 본교 정보보안 업무를 원활히 수행하기 위하여 정보보안 조직을 구성하여 운영한다.

② 정보보안 조직은 다음과 같이 구성・지정한다.

1. 정보보안책임관 : 경영관리처장
2. 정보보안담당관 : 정보지원부 팀장
3. 분임정보보안담당관(기술) : 각 담당분야별 담당자
4. 부서정보보안담당관 : 부서 각 팀장

제10조(정보보안책임관) ① 경영관리처장은 보직에 임명됨과 동시에 본교 정보보안책임관으로 지정한다.

② 정보보안책임관은 정보보안업무를 총괄한다.

제11조(정보보안담당관) ① 정보보안담당관은 정보지원부 팀장으로 지정한다.

② 정보보안담당관은 다음 각 호의 임무를 수행한다.

1. 정보보안책임관의 업무를 보좌
2. 분임정보보안담당관 및 부서정보보안담당관들의 업무를 관리감독
3. 정보보호규정, 시행규칙 제・개정 총괄
4. 기타 정보보안업무 전반에 관한 지도, 조정 및 기타 감독에 관한 사항

제12조(분임정보보안담당관) ① 분임정보보안담당관은 다음 각 호의 임무를 수행한다.

② 분임정보보안담당관은 다음 각 호의 임무를 수행한다.

1. 정보보안담당관 업무를 보좌하여 실무 수행
2. 정보보안업무 분야별 연간 정보보안 활동계획 수립 및 이행
3. 정보보안 관리규정 등 정보보안 문서에 대한 변경 관리
4. 정보자산 목록에 대한 관리 및 통제
5. 침해사고 대응체계 수립 및 이행
6. 정보보안 교육 계획 수립 및 이행
7. 정보보안 홍보활동(게시판, e-mail공지 등)
8. 정보보안시스템 보안정책 등록 및 변경
9. 정보통신망 및 정보자료 등의 보안관리 주관

제13조(부서정보보안담당관) ① 각 부서 및 부속기관 부서정보보안담당관은 부서별 담당팀장이 되며 팀장이 없는 경우 선임팀원을 지정한다.

② 부서정보보안담당관은 다음 각 호의 임무를 수행한다.

1. 부서(팀) 직원에 대한 정보보안 인식제고 활동
2. 부서(팀) 보조기억매체 관리 및 이동식 저장장치 관리
3. 부서(팀) 중요문서, 개인정보 관리 감독
4. 부서(팀) PC 보안관련 사항
5. ‘사이버・보안 진단의 날’ 부서(팀) 진단 결과 취합 및 보고
6. 침해사고 발생시, 침해사고대응팀 구성원으로 포함되어 활동

③ 각 처의 처장은 부서의 부서정보보안담당관을 지정하고, 정보보안책임관에게 보

고해야 하며, 변경 시에도 보고해야 한다.

제4장 정보자산 관리

제14조(정보자산 관리 유형) ① 분임정보보안담당관은 다음의 자산에 대한 최신 현황을 관리해야 한다.

1. 서버(스토리지)
2. 네트워크, 정보보안시스템
3. 어플리케이션(소프트웨어)
4. PC, 노트북, 보조기억매체(USB, 외장형하드디스크)
5. 부대설비(항온항습기, UPS)
6. 기타 정보자산 관리를 위해 필요하다고 판단되는 자산

② 경영관리부서는 다음의 자산에 대한 최신 현황을 관리해야 한다.

1. 디지털 OA기기
2. 문서정보, 비밀취급 관련 문서
3. CCTV 관련 장비 및 설비
4. 기타 정보자산 관리를 위해 필요하다고 판단되는 자산

③ 시설관리부서는 다음의 자산에 대한 최신 현황을 관리해야 한다.

1. 물리적 시설(소화설비, 냉.난방 설비, 비상발전기 등)
2. 출입통제 설비
3. 기타 정보자산 관리를 위해 필요하다고 판단되는 자산

제15조(정보자산의 보안관리) ① 본교 내부직원 및 사업단을 포함한 외부 용역직원들은 본교 내부 정보자산을 개인의 목적으로 외부 반출 및 타인에게 전송 할 수 없다.

② 전자적 형태의 정보자산을 업무상 목적으로 전송 또는 배포하고자 하는 경우에는 승인된 정보기기 및 전송망을 사용해야 한다.

③ 정보보안담당관은 중요 정보자산에 대하여 비인가자의 무단접근을 통제할 책임을 지닌다.

④ 정보보안담당관은 관련 규정에 따라 정보자산이 적절하게 사용 및 운용되고 있는지 관리·감독한다.

제16조(정보자산의 폐기) ① 부서정보보안담당관은 정보자산의 폐기사유가 발생하면 정보보안담당관의 승인을 받은 후 폐기한다.

② 정보자산 재사용 또는 폐기 시 에는 다음 사항을 준수해야 한다.

구 분	출력물	보조기억매체
재사용	대외비 이상 정보의 재사용 (이면지 사용)금지	덮어쓰기 또는 신뢰할 수 있는 방법으로 데이터 완전 소거
폐기	문서 수거함이나 문서 파쇄기를 통한 폐기	물리적으로 매체의 완전 파괴

제17조(정보자산의 반·출입 관리) ①중요 정보자산의 외부 반출은 소속팀장의 사전 승인 후 반출한다.

1. 소속팀장은 감사를 위해 관련내용을 기록 관리하고, 저장매체 내의 데이터를 확인한다.
2. 소속팀장은 외부로 반출·입 되는 정보자산의 승인여부를 확인하고, 관련내용을 기록 관리한다.

제5장 정보보안 교육 및 홍보

제18조(정보보안 교육) ① 정보보안담당관은 전 교직원을 대상으로 년 1회 이상 정보보안 교육을 실시하여야 한다.

② 정보보안담당관은 정보보안 교육의 효율성, 전문성을 높이기 위해 외부전문가의 지원을 요청할 수 있다.

③ 분임정보보안담당관은 업무 전문성을 제고하기 위해 년 1회, 10시간 이상의 정보보안전문기관 교육 또는 정보보안 관련 세미나에 참석해야 한다.

④ 정보보안담당관은 외부 정보보호 전문교육과 세미나 참석을 위한 예산을 확보해야 하며, 관련 정보를 수집하여 해당 팀에 전파한다.

제6장 인적보안

제19조(채용시 보안) ① 교직원(계약직 포함) 채용 시에는 재직 중에 취득한 정보에 대한 보안을 유지하도록 '[별지 제1호 서식] 정보보안 서약서(교직원용)'를 작성해야 한다.

제20조(보직변경 등 인사이동시) ① 보직변경 등 인사이동시 업무시스템에 대한 접근권한을 인사발령과 함께 신속하게 변경 또는 조정하여야 한다.

② 인사이동시 PC에 저장된 업무관련 파일은 삭제해야하며, 업무관련 파일이나 정보유출에 대한 책임은 해당PC 사용자에게 있다.

제21조(퇴직 및 계약해지시) ① 퇴직자는(계약직 포함)재직 중 보유한 모든 정보자산(사용PC, 보조기억매체, 업무자료 및 문서, 출입증 등)을 반환해야 할 의무가 있으며, 해당 부서장은 퇴직자의 정보자산을 부서에 귀속시킬 수 있도록 할 책임이 있다.

② 인사담당자는 퇴직자의 정보자산 반납 등을 확인한다.

③ 인사담당자는 퇴직 절차가 완료된 퇴사자에 대해 인사발령을 시행하고, 정보지원부서에 통보하여 퇴직처리 된 퇴사자의 계정이 삭제될 수 있도록 조치한다.
④ 분임정보보안담당관은 퇴직자에 의한 정보유출이 의심되거나 위험이 있는 경우 퇴직 처리 전에 사용자의 계정을 삭제 조치할 수 있다.

제7장 물리적 보안

제1절 보호구역 설정 및 통제

제22조(보호구역 설정) ① 본교의 물리적 보안을 위해 보호구역을 설정하여 관리한다.
② 보호구역은 그 중요도에 따라 통제구역, 제한구역, 일반구역으로 구분하며, 본교의 보호구역은 보안업무규정 제 33조에 의한 설정에 따른다.

제23조(통제구역의 통제) 통제구역으로 지정된 장소는 다음과 같은 통제를 적용한다.
① 출입통제 및 감시를 위해 출입통제시스템, 감시카메라(CCTV) 등을 설치한다.
② 비인가자의 출입이 제한되는 '통제구역' 표시를 하여야 한다.
③ 통제구역의 출입권한 등록은 최소한의 인원으로 제한하고, 인가자 외의 인원 출입 시 담당자 인솔하에 출입한다.

제24조(장비 설치 및 보호) ① 장비는 물리적·환경적 위협이나 위험, 또는 외부인의 접근으로부터 위험을 줄일 수 있도록 설치하고 보호한다.
② 비밀정보를 다루는 원격터미널 또는 모니터는 비인가자가 외부로부터 투시가 될 수 없도록 배치하며, 특별한 보호가 요구되는 정보시스템은 격리된 장소에서 별도로 관리한다.
③ 비상시 사용될 백업장비 및 자산은 원격지에 보관한다.
④ 정보시스템은 화재 등에 대비하여 건물 외벽과 거리를 두고 배치하고, 가능한 취사시설, 화장실 등으로부터 거리를 두고 배치한다..

제25조(전원 공급) ① 장비는 정전이나 기타의 전기적 장애로부터 보호한다.
② 장비 제조업체에서 권장하는 규격에 맞는 적합한 전력이 공급되도록 한다.
③ 일시적인 전력중단이나 기타 전기적 이상으로부터 정보시스템의 가용성을 확보하기 위한 대체 전력 공급원을 확보한다.
④ 비상시를 대비하여 핵심 업무활동을 지원하는 정보시스템에는 UPS(무정전전원공급장치)를 설치한다.

제2절 전산기계실 보안관리

제26조(전산장비실 환경) ① 전산기계실은 다른 업무 장소와 분리하여 물리적 보안성이 보장된 곳에 위치하여야 한다.
② 전산기계실은 중요 정보통신장비 및 정보자료가 상존하는 곳이므로 차광, 환풍, 냉·온방등의 시설이 구축되어야 한다.

③ 전산기계실은 정보통신장비의 원활한 운영 · 관리를 위하여 필요한 공간이 충분히 확보되어야 한다.
④ 재난에 대비하여 열 감지기, 연기감지기, 누수감지기 등의 방화시설, 소화설비, 기타 방재설비를 적절히 보유해야 하며 항시 작동 가능한 상태로 유지해야 한다.
⑤ 전산기계실 운영 · 관리에 필요한 정보통신장비 및 도구 이외의 사물을 보관하거나 비치하지 않도록 통제, 감독 및 관리하여야 한다.
⑥ 항온 · 항습을 유지할 수 있는 설비를 설치하며, 항상 적정온도 및 습도를 유지하도록 한다.
⑦ 비인가 행위 적발, 전산기계실 물리적 감시를 위해 CCTV를 설치하여 운영할 수 있다.

제27조(출입권한 관리) ① 전산기계실 출입권한은 전산관련 직원에 한하여 허가된다.
② 전산기계실 출입권한이 신규로 필요로 한 경우 정보보안담당관의 승인 후, 해당 인원의 출입권한을 등록한다.
③ 정보보안담당관은 퇴사 및 보직변경으로 인하여 전산기계실 출입권한의 변동이 발생한 경우 우선적으로 해당인원의 전산기계실 출입권한을 삭제한다.

제28조(외부인 출입통제) ① 전산기계실은 비인가자의 출입을 통제하여야 하며 “기계실 출입관리 대장’ 을 비치하여 모든 출입자를 기록해야 한다.
② 외부인이 전산기계실을 출입하는 경우 출입권한자가 동행하도록 한다.
③ 외부인의 전산기계실 출입 시 목적, 출입 및 퇴실시간 등을 출입관리대장에 기록하고 동행한 출입권한자가 확인서명을 하여야 한다.
④ 정보보안담당관은 매월 출입관리대장을 확인하고, 출입관리대장의 보관은 1년 이상으로 한다.

제29조(정보통신장비의 반입 · 출입 통제) ① 정보보안담당관은 정보통신장비의 수리, 교체 및 대체, 대여 등으로 정보통신장비가 반입 · 반출되는 경우, 정보통신장비의 반입 · 반출을 통제하여야 한다.
② 정보보안담당관은 정보시스템 장비의 반입 · 반출을 하는 경우 관련 기록을 “정보화기기 외부 반출입 관리대장’ 에 기록한다.
③ 장비 반출일 경우 해당 장비내의 저장매체에 저장된 정보가 복구 가능하지 않도록 삭제되었는지 확인한 후 장비를 반출 하도록 한다.

제30조(촬영금지) 전산기계실 내에서의 휴대폰, 디지털카메라 등을 이용한 촬영은 금지 한다. 단, 업무적으로 필요한 경우 정보보안담당관의 승인을 득해야한다.

제8장 PC 보안

제31조(PC 관리책임자 · 취급자 지정) ① 개인용컴퓨터(노트북 포함)에 대한 총괄책임자는 정보보안담당관으로 하며, 부서별 관리책임자는 해당 부서의 팀장 (팀장이 없는 경우는 선

임팀원)으로 하고, 취급자는 해당 PC 사용자로 한다.

제32조(유해 소프트웨어에 대한 통제) 공식적으로 인가되지 않은 프로그램의 사용은 바이러스, 트로이 목마와 같은 악성 코드들이 포함되어 있을 가능성이 높으며 이러한 악성코드 들은 조직의 중요 정보 노출, 파괴 등을 유발할 수 있으므로 사용자는 프로그램 사용에 대해 다음 사항을 준수한다.

① 사용자는 업무에 불필요 또는 불법 소프트웨어를 사용하지 않고, 정품 소프트웨어만을 사용한다.

② 불확실하거나 출처가 명확하지 않은 파일, 신뢰할 수 없는 네트워크로부터 획득된 파일은 사용하기 전에 바이러스 검사를 한다.

③사용자는 월 1회 악의적인 바이러스, 불법 소프트웨어 등이 설치되어 있는지를 점검한다.

제9장 E-mail, 인터넷 보안관리

제33조(E-mail 사용의 제한) ① E-mail 사용자는 부서장의 허가를 받지 않은 정보 또는 외부에 공개할 수 없는 내부 정보를 외부에 발송하지 않는다.

② 스팸메일 등 불법 메일 등을 송신하거나 타 직원의 E-mail 계정을 도용할 수 없다.

③ 정보시스템 자원의 낭비를 초래하는 스팸메일, 반복메일 등은 전송 및 배포를 금지한다.

④ 모든 E-mail 사용자는 제3자의 지적재산권, 저작권을 침해하는 내용, 명예훼손, 사기, 바이러스 유포 등의 불법적인 행위에 대한 내용을 E-mail에 포함하지 않는다.

⑤ 타인의 E-mail 내용 및 비밀번호를 중간에서 전자적으로 도청하지 않는다.

⑥ E-mail이 암호화되지 않은 경우, E-mail 사용자들은 신용카드번호, 패스워드 등 개인의 중요한 정보를 E-mail 내용에 포함시켜 보내지 않아야 한다.

⑦ 내부정보를 외부로 송신하기 위해서는 사전에 그 타당성에 대해 해당 전결권자의 승인을 득해야 하며, 내용의 중요성에 따라 선택적으로 암호화하여 전송한다.

⑧ 직원은 외부의 네트워크 주소로 E-mail을 자동전달(Forwarding)해서는 안 된다.

제10장 서버 보안

제34조(정보시스템 보안관리) ① 정보보안담당관은 정보통신시스템(정보통신망 포함)의 효율적인 보안관리를 위하여 분임정보보안담당관을 두어 정보통신시스템별로 관리운영하여야 한다.

② 시스템관리자는 각종서버 · PC · 정보통신장비 등 정보통신시스템이 비인가자에게 불필요한 서비스를 허용하지 않도록 보안기능을 설정하여야 한다.

③ 시스템관리자는 보안도구를 이용하여 년1회 이상 정보통신시스템의 보안취약성을 진단하여야 한다.

④ 시스템관리자는 주기적으로 불필요한 포트의 사용여부를 점검하여, 불필요한 포트 사용이 확인되는 즉시, 해당 포트를 삭제하는 등의 보안조치를 수행한다.
⑤ 중요정보를 취급하는 정보시스템은 관리자 권한으로 시스템에 접근하는 경우, 지정된 IP에서만 접근할 수 있도록 한다.

제35조(서버 시스템의 설치) ① 서버시스템 설치 아래의 각호의 사항을 준수하여야 한다.

1. 신규 시스템을 도입 시 시스템 보안설정, 서버백신, 장애관리 등의 도구를 설치해야 한다.
2. 시스템관리자는 신규로 도입 설치되는 서버 시스템에 서버 취약점 점검도구를 설치하여 시스템 및 OS의 취약점 점검을 수행하며, 점검결과 발견된 취약점에 대해 발주부서에 통보하여 조치토록 한다.
3. 시스템관리자는 신규 시스템 설치 및 변경 사항을 정보자산 관리목록에 갱신해야 한다.

제36조(시스템 접근 기록 관리) ① 시스템 접속기록은 접속일시, 사용자 ID, 접속 IP 등이 포함되어야 한다.
② 시스템 접근 및 사용에 대한 책임 추적성을 확보하기 위하여 시스템 가동 및 종료, 설정 변경, 중요파일 접근로그, 관리자 계정 명령어 사용내역 등의 로그를 기록한다.
③ 사고발생시 책임추적이 가능하도록 시스템 접근기록을 3개월 이상 보관하여야 한다.
④ 정보보안담당관의 사전 승인이 없는 한 모든 시스템 로그에 대해 비인가자가 접근할 수 없으며 시스템 로그를 비인가자가 열람하거나, 훼손하는 경우 심사위원회를 통해서 처벌하거나, 외부자의 경우 민.형사상 법적 조치를 취한다.
⑤ 시스템관리자는 정기적으로 시스템 접근기록을 검토하여 비인가자의 접속시도, 정보 위・변조 및 무단삭제 등의 의심스러운 활동이나, 침입흔적 발생시 정보보안담당관에게 보고하고 조치를 취해야 한다.

제37조(권한관리) ① 서버 내 정보에 대한 접근 권한은 정보보안담당관이 검토 후 부여한다.
② 시스템관리자는 개인의 계정으로 접속한 후에 관리자 권한을 획득한다.
③ 일반사용자는 다른 사용자의 홈디렉터리 혹은 시스템 관리에 관한 파일 혹은 디렉터리에는 접근할 수 없도록 제한한다.
④ 일반사용자가 서비스 중지 등을 일으킬 수 있는 시스템 명령어 혹은 컴파일러를 사용할 수 없도록 제한한다.
⑤ 일반사용자는 시스템관리자 및 정보보안담당관의 사전 승인 없이 운영체제의 접근통제를 우회할 수 있는 프로그램을 사용할 수 없도록 제한한다.
⑥ 관리자 권한 등의 중요 권한을 일반 사용자에게 생성해주지 않는다.

⑦ 슈퍼유저 계정을 이용한 FTP 접속권한을 해제한다.
⑧ 불필요한 RPC통신 권한을 해제한다.

제38조(접근통제관리) ① 업무상 접속할 필요가 있는 사용자를 파악한 후 보안도구를 이용해 IP주소 기반의 접근제어를 한다.
② 시스템관리자는 서버가 정상적으로 동작하지 않을 경우 정상적으로 동작될 때까지 사용자의 접근을 제한할 수 있다.
③ 시스템관리자는 비인가자의 불법적인 접근 및 서비스 중지 등을 예방하기 위해 업무적으로 불필요하거나, 침해의 위협이 있는 네트워크 서비스를 제공하지 않는다.

제39조(원격접근 보안관리) ① 일반사용자가 서버에 접속할 경우 반드시 사용자 계정과 패스워드 또는 보다 강화된 인증방법을 적용하여 접근 가능하도록 한다.

제40조(외부망에 대한 접근보안관리) 시스템관리자 등 정보시스템관리자는 정보시스템을 외부에서의 네트워크를 통해 원격으로 접속하여 정비하는 것을 원칙적으로 금지하여야 한다. 다만, 부득이한 경우에는 아래의 각호에 해당하는 보안대책을 강구하고 정보보안담당관과 협의한 후 한시적으로 허용하여야 한다.

1. 원격접속 수행자에게 임시 접근권한 부여
2. 접근권한의 사용시간 명시, 시간경과 후 접근권한 삭제
3. 원격정비 시스템의 IP사전 파악, 지정된 시스템에서만 수행
4. 원격시스템과의 통신정보를 점검하여 실행코드에 악성코드 유입 방지
5. 원격정비를 수행할 때 대상 정보시스템을 내부망과 분리
6. 원격정비기록을 유지, 정비결과 서버관리자에게 보고
7. 원격 정비자가 네트워크를 통해 원격지 컴퓨터 파일을 자신의 컴퓨터 파일처럼 접근하여 작업할 수 있도록 하는 등 해킹에 취약한 방식으로 원격정비 금지

제41조(백신설치 및 운영) ① 시스템관리자는 윈도우 시스템의 경우 최신버전의 백신을 설치하고 운영하여 컴퓨터바이러스 등에 의한 해킹 및 사이버테러에 대응해야 한다.
② 출처, 유통경로 및 제작자가 명확하지 않은 응용프로그램은 바이러스 검색 프로그램으로 진단한 후 사용한다.
③ 바이러스 서버를 설치하여 외부에서 들어오는 메일 등에 대하여 사전 검색을 한다.
④ 정기적으로 일제점검이 가능하도록 특정일을 지정하여 점검을 실시한다.
⑤ 중요 실행파일은 읽기 전용으로 속성을 변경하여 관리한다.
⑥ 최신의 검색 프로그램을 활용하고 최신의 패치프로그램 배포 시 즉시 보정작업을 실시한다.
⑦ 바이러스 감염 시 피해를 최소화할 수 있도록 아래와 같이 조치한다.

1.감염사실을 부서정보보안담당관에게 신속히 신고
2.부서정보보안담당관은 정보보안담당관 신속히 보고

3.감염된 시스템 사용 중지

4.백신프로그램을 이용하여 바이러스 퇴치

5.원인분석 후 예방조치 권고사항의 수행

제42조(웹서버 등 공개서버 관리) ① 외부인에게 공개할 목적으로 설치되는 웹서버 등 각종 공개서버는 내부망과 분리하여 운영하고 보안적합성이 검증된 침입차단시스템을 설치하는 등 보안대책을 강구하여야 한다.

② 서버에 접근할 수 있는 사용자계정을 제한하며 불필요한 계정은 삭제하여야 한다.

③ 홈페이지 게재내용은 자체 해당팀장의 심의를 거쳐 비밀내용 등 비공개 자료가 포함되지 않도록 해야한다.

④ 공개서버는 업무서비스를 제외한 모든 서비스 및 시험 · 개발도구 등의 사용을 제한하도록 보안기능을 설정하여야 한다.

⑤ 공개서버의 보안취약성을 수시로 점검하고 자료의 위 · 변조, 훼손여부를 확인해야 한다.

⑥ 보안사고에 대비하여 서버에 저장된 자료의 철저한 백업체계를 수립 · 시행하여야 한다.

⑦ 공개서버를 통해 개인정보가 유출, 위 · 변조되지 않도록 보안조치를 해야 한다.

제43조(취약점 점검) ① 시스템관리자는 시스템 불법 접근 및 해킹 프로그램(백도어 및 스파이웨어 등)의 설치여부 점검 등 일상적인 보안활동을 수행한다.

제44조(백업 관리) ① 정보보안담당관은 정보화자료 백업 및 소산계획을 수립하고 백업을 실시한다.

② 백업대상 선정 및 주기는 시스템별 중요도 및 자료 건수, 사용빈도, 사용시간 등을 검토하여 결정한다.

③ 백업시스템 도입 후 최초 적용 시 정기적인 항목들(보관기간, 방식, 데이터베이스 백업 모드, 소산백업 여부)을 결정하여야 하며, 운영도중 변경사항이 발생하면 충분한 검토 및 승인을 통해 이를 반영하여야 한다. 그리고 백업데이터의 중요도에 따라 백업주기를 결정한다.

제11장 네트워크 보안

제45조(외부망 연동) ① 다른 기관과의 정보통신망을 연결 사용하고자 할 경우에는 보안관리 책임한계를 설정하고 다음과 같은 보안대책을 수립 · 시행하여야 한다.

1. 네트워크 취약성 점검

2. 침입차단 · 탐지 시스템 설치 운용 등

② 외부망과 접속하는 경우에는 전산자료 제공범위 및 이용자의 접근제한 등에 대해 정보보안책임관의 승인을 받아야 한다.

③ 외부망 연결에 따른 보안취약성 해소를 위하여 접속자료를 주기적으로 분석하고

보안도구를 이용하여 정보통신망의 취약성을 수시 점검하여야 한다.
④ 인터넷 등 상용망 및 타 기관과의 정보통신망 연동 시 불법침입(해킹)을 방지하고 효율적인 보안관리를 위하여 연결지점을 지정 운용함으로써 임의 접속을 차단하여야한다.
제46조(네트워크 장비 계정 및 권한 관리) ① 네트워크 장비에는 관리자 계정 등 최소한의 계정만을 생성해야 한다.
② 네트워크 장비 설치 시 기본적으로 생성되는 불필요한 계정을 삭제해야 하며 해당 계정이 필요한 경우 기본 패스워드를 변경하여 사용한다.
③ 네트워크 장비의 패스워드는 영문과 숫자를 조합하여 최소 8자 이상으로 설정하고 주기적으로 변경해야 한다.
제47조(로그 및 백업관리) ① 네트워크관리자는 모든 네트워크 시스템에 대해 시간을 동기화하여 로그 생성 시 정확한 시간이 기록되도록 한다.
② 주요 네트워크 장비의 로그정보는 실시간으로 로그가 저장될 수 있도록 한다. 단. 기능을 제고하지 않는 장비는 제외한다.
③ 네트워크 로그파일 및 구성정보는 일반사용자 권한으로 수정 및 삭제할 수 없도록 설정한다.
제48조(유지관리) ① 라우터 및 스위치는 가용성 보장을 위해 유지보수를 해야 하며 최소 1개월마다 정기점검을 실시해야 한다.
② 네트워크관리자는 라우터 및 스위치의 주요 패치정보를 수집하고 패치 시 안전성이 확보되는 시점에 패치 적용을 수행한다.

제12장 어플리케이션 보안

제1절 설계 및 개발 단계

제49조(개발보안 일반) ① 정보보안담당관은 업무용 어플리케이션 및 홈페이지 등의 정보시스템을 개발하는 경우 보안대책을 수립하고 보안요구사항을 정의해야 한다.
② 해당 프로젝트담당자는 정보시스템 개발 과정을 감독하고, 개발된 코드에 대한 점검과 테스트를 실시해야 한다.
③ 정보보안담당관은 안전한 코딩방법을 프로젝트 담당자에게 제시하여야 하며 프로젝트 담당자는 해당 기준에 따라 어플리케이션을 개발하도록 감독해야 한다.
④ 해당 프로젝트담당자는 모든 개발자에 대하여 사전에 보안서약서를 요구하고, 보안교육을 실시해야 한다.
제50조(개발 환경) ① 개발공간은 비 인가자의 출입이 물리적으로 통제된 작업공간에서 개발이 이루어져야 한다.
② 개발서버가 위치한 네트워크는 인터넷과 분리되어야 하고, 네트워크에 연결된 경우에는 비인가자의 접근으로부터 보호하기 위한 보안대책을 강구해야 한다.
③개발시스템과 운영시스템은 물리적 또는 논리적으로 분리되어야 한다.

④개발자의 PC는 컴퓨터 바이러스나 각종 보안 침해사고로부터 보호되어야 한다.
⑤개발자의 시스템 및 소스코드 접근은 공식적으로 허가된 경로만을 사용하여야 한다.
제51조(보안기능 요건 반영) ① 본교 프로젝트담당자는 어플리케이션 설계 및 개발 시 '어플리케이션 보안기능 요건'을 반영하여야 한다. 단, 업무적으로 반드시 필요하거나 정보보안담당관의 승인을 득한 경우에는 그 사유를 기록하고 보안기능 요건을 반영하지 않을 수 있다.
② 본교 프로젝트담당자는 설계 및 개발 완료시 '어플리케이션 보안기능요건' 반영 여부에 대해서 정보보안담당관에게 보고해야 한다.
③ 중요 정보의 전송 및 저장 시 국정원으로부터 승인을 얻은 암호화 기법을 사용하여 암호화해야 한다.
④ 다음과 같은 정보는 네트워크를 통해 전송될 수 없도록 해야한다. 단 불가피하게 전송을 필요로 할 경우 반드시 암호화된 상태로 전송해야 한다.

1.비밀번호, 주민등록번호 등 사용자와 관련된 민감한 정보
2.금융거래 정보 등 노출 시 사용자에게 피해를 줄 수 있는 정보

⑤ 암호화 Key의 접근은 인가된 사람으로만 제한하도록 하며 암호화 Key는 일정주기마다 변경하여야 한다.

제13장 정보보안시스템 관리

제52조(선정 및 설치) ① 정보보안시스템을 설치·운용하고자 하는 경우 아래와 같은 사항을 반영하여 선정하여야 한다.

1. 정보보안시스템 평가인증 지침 및 공통평가기준에 의해 인증된 제품이나 국정원장이 그와 동등한 효력이 있다고 인정한 제품
2. 소관업무 및 정보통신망 특성을 지원할 수 있는 제품

제14장 침해사고 대응

제53조(침해사고대응팀 구성) ① 침해사고를 효과적으로 대응하기 위해서 침해사고대응팀을 구성하며, 침해사고대응팀은 침해사고 발생시, 한시적으로 운영한다.
② 침해사고 발생시, 본교의 정보보안 조직은 침해사고대응팀으로 전환되어 운영되며, 각 부서의 부서정보보안담당관을 포함한다.
③ 침해사고대응팀의 총괄 책임자는 정보보안책임관으로 한다.
④ 침해사고대응팀의 실무 총괄자는 정보보안담당관으로 하며, 침해사고 대응 및 보고 업무를 총괄 수행한다.
⑤ 분임정보보안담당관은 분야별 담당업무 및 시스템에 대해 침해사고 현황 및 대응방안 등을 실무 총괄자에게 보고, 수시로 상황에 대처한다.
⑥ 분야별 시스템을 유지관리하고 있는 외부업체 주요 담당자는 분임정보보안담당관

과 침해사고 대응책을 마련하여 시스템에 적용한다.
⑦ 침해사고대응 실무 총괄자는 침해사고대응팀 및 유관기관 등의 연락처를 기록하고 현행화해야 한다.

제15장 용역사업 보안관리

제54조(계약시 보안관리 등) ① 정보화, 정보보안사업, 정보시스템 등을 외부 용역으로 외부업체와 계약할 경우에 계약서에 정보보안 준수 의무 및 위반할 경우에 손해배상 책임 등을 명시하여야 한다.
② 계약서에 정보보안 준수 의무 및 위반에 대한 사항을 명시하는 경우 [별표 1]의 내용을 참조한다.
제55조(참여인원 보안관리) ① 사업주관부서는 모든 참여인원에 대하여 각 개인의 친필 서명이 들어간 보안서약서를 요구해야 한다.
② 사업주관부서는 용역업체 자체 보안관리 및 직원 관리감독 강화를 독려하고 보안의중요성 인식제고를 위해 업체대표 명의 '[별지 제3호 서식]정보보안 서약서(용역업체 대표자용)' 을 제출 받아야 한다.
③ 사업주관부서 담당자는 사업시작 전 참여인원에 대한 보안준수 의무 등의 보안교육을 실시하고, 교육 참가에 대한 자필서명을 받는다.
④ 사업수행시 사업수행업체의 대표자(PM)를 정보보안책임관으로 지정·운영하며, 사업수행업체 대표자(PM)는 사업전반에 대한 인원・장비・자료・정보 등을 관리하며 보안사고 방지를 위한 자체 활동을 수행해야 한다.
제56조(자료에 대한 보안관리 등) ① 용역사업 관련자료 및 사업과정에서 생산된 모든 산출물은 본교의 파일서버에 저장하거나 정보보안담당관이 지정한 PC에 저장/관리한다.
② 용역사업 관련 자료는 인터넷, 웹하드 등 인터넷 자료공유사이트 및 웹 메일 등의 외부메일함에 저장을 금지하고, 전자우편을 이용해 자료전송이 필요한 경우에는 본교 전자우편을 이용하여 첨부자료를 암호화한 후 수・발신한다.
③ 본교와 관련된 자료를 출력물로 제공한 경우에는 시건장치가 된 보관함에 보관하여야 한다.
④ 사업수행업체는 사업수행으로 생산되는 산출물 및 기록은 본교의 해당사업 주관부서장 또는 정보보안담당관이 인가하지 않은 비인가자에게 제공・대여・열람을 금지한다.
제57조(장비・사무실에 대한 보안관리) ① 사업수행업체의 노트북, PC는 반입시 마다 최신의 바이러스 백신프로그램 설치와 바이러스 감염여부를 점검·확인해야 한다.
② 반입된 노트북 PC는 사업 종료 시까지 반출을 금지한다. 다만 부득이하게 외부반출이 필요한 경우에는 최소한의 장비만 반출승인하고 자료유출에 대비한 보안조치(부

팅・로그인 패스워드 설정, 자료 암호화 등)를 실시한 후 반출한다.
③ USB 등의 보조기억매체 사용을 금지한다. 다만, 산출물작성 등 보조기억매체가 필요한 경우는 정보보안담당관의 승인하에 허가된 것만 사용한다.
④ 용역사업 수행장소는 시건장치와 출입통제가 가능한 공간을 사용해야 한다.

제58조(내·외부 정보망 접근에 대한 보안관리) ① 용역사업 수행 시 정보시스템에 대한 사용자 계정(ID)이 필요한 경우, 외부인력에게 별도의 계정을 발급하고 접근권한을 부여 후 계정발급 및 접근권한 부여 기록을 별도로 관리 한다.
② 외부인력에게 부여된 접속권한이 불필요한 경우 곧바로 권한을 해지하거나 계정을 삭제한다.
③ 프로그램 개발 용역사업 수행을 위한 작업은 사업수행업체의 자체 개발서버 또는 본교가 제공한 개발서버에서 수행함을 원칙으로 하며, 개발이 완료된 후 실 운영시스템에 설치시는 본교의 해당 시스템 담당자의 감독하에 작업한다.
④ 용역업체 전산망에서 P2P, 웹 하드 등 인터넷 자료공유사이트로의 접속을 차단한다.

제59조(사업완료시 보안관리 등) ① 사업완료 후 생산되는 최종 산출물 중 대외보안이 요구되는 자료는 대외비로 작성・관리하고 불필요한 자료는 삭제 및 세단 후 폐기한다.
② 용역업체에 제공한 제반자료, 장비, 서류와 중간・최종 산출물 등 용역과 관련된 제반자료는 전량 회수하고 업체에 복사본 등 별도보관을 금지한다. 단, 소스코드 등 향후 유지보수를 위해 필요하다고 판단되는 경우 정보보안책임관의 승인 후 용역업체에게 제공할 수 있다.
③ 사업완료시 용역업체의 노트북 PC 및 사용된 보조기억장치는 자료에 대하여 Format 후 반출한다.
④ 노트북・보조기억매체 등 전자적으로 기록된 자료는 복구할 수 없도록 삭제해야 한다.
⑤ 사업완료시 용역사업 관련자료 회수 및 삭제조치 후 업체에게 복사본 등 용역사업 관련 자료를 보유하고 있지 않다는 대표 명의로 '[별지 제4호 서식] 보안자료 반납 및 파기 완료 확약서'를 요구한다.

제16장 백업 및 복구

제60조(백업일반) ① 물리적 재난이나 정보통신설비의 오류 발생으로 긴급 상황이 발생할 경우, 즉각적으로 복구할 수 있도록 주기적으로 백업을 수행한다.
② 정보의 중요성 및 데이터의 성격에 따라 백업주기, 백업방법, 보존기간 등을 포함하여 기록・관리해야 한다.
③ 백업 데이터의 최소 보관기간은 3개월로 한다.

제61조(백업 대상 및 주기) ① 백업대상은 데이터의 파손 시 복구의 필요성이 요구되는 본교의 주요 데이터이며 다음과 같은 정보들이 이에 해당한다.

1. OS및 유틸리티 프로그램
2. 데이터베이스 파일 : 업무데이터 및 데이터베이스 구성파일
3. 네트워크 장비 구성파일 및 로그파일
4. 정보보안시스템 정책 및 로그파일
5. 기타 필요로 하다고 생각되는 파일

② 백업대상에 대한 백업 및 보관주기는 따로 정한다.

③ 백업 데이터는 원격지의 안전한 장소에 분산보관 하고, 그 기록을 관리 한다.

제62조(복구) ① 데이터베이스 및 정보통신시스템 장애 시 백업된 자료를 사용하여 복구한다.

제17장 개인정보보안

제63조(개인정보보안) ① 모든 직원은 업무 목적으로 개인정보를 수집, 이용, 저장하는 경우 개인정보가 유출되지 않도록 유의해야 한다.

② 모든 직원은 업무용도외 개인정보를 사용하지 않아야 하며, 업무상 알게 된 개인정보를 침해 또는 누설하여서는 안된다.

③ 개인정보보안과 관련된 세부사항은 ‘개인정보 내부 관리계획 규정’을 따른다.

④ CCTV와 관련된 세부사항은 ‘CCTV 설치·운영에 관한 지침’을 따른다.

부 칙

(시행일) 이 규정은 2022년 12월 27일부터 시행한다.

[별표 1]

용역사업 계약시 정보보안 준수 및 의무 사항

1.정보자산의 기밀성, 무결성, 가용성보장

가. 본교 정보자산을 허가 없이 외부 또는 제3자에 공개 및 유출하지 말아야 하며, 특히 업무수행 시 취득한 정보를 다른 협력회사 등에 유출되지 않도록 주의한다.

나. 본교 정보자산을 무단으로 변경하지 말아야 하며, 정확하고 완전한 상태로 유지한다.

2.보안관련법적조항 및 보안규정, 지침준수책임

가.개인정보보호법 등의 법적인 요구사항을 준수한다.

나.정보보안 관련 법률에서 금지하고 있는 본교 시스템 및 정보통신망에 대한 해킹 및 침해 행위를 금한다.

다.본교 정보보안관련규정을 숙지하여 위반사항이 발생하지 않도록 준수한다.

라.본교 지적재산에 대한 보호 의무를 성실히 준수한다.

3.계약완료시 정보자산 반환 및 폐기 의무

가.사업수행을 위해 이용한 모든 본교 정보자산은 해당 사업종료 시 반드시 본교에 귀속되어야 한다.

나.계약완료 시 정보자산의 반환 및 폐기는 해당 사업의 본교 책임자에 의해 확인되어야 한다.

4.바이러스 확산 방지

가. 본교 교내로 반입되는 모든 장비에는 반드시 백신이 설치되어 있어야 하며, 바이러스 검역 과정을 거친 후 본교 네트워크에 연결할 수 있다.

나.수시로 반·출입되는 장비에 대한 관리 책임은 협력회사 측에 있으며, 백신의 정상 작동 여부와 바이러스 엔진의 업데이트 여부를 반드시 확인한다.

다.본교 교내망에 연결된 상태로 E-mail을 이용하거나 인터넷을 통한 자료를 다운로드 받는 경우 반드시 바이러스 점검을 수행한다.

5.보안위반사항 발생 시책임

보안요구사항 및 계약서상에 명시된 준수사항 불이행으로 인해 본교에 피해가 발생한 경우 보상 책임은 용역회사측에 있으며, 현재사업 및 향후 계약에 불이익이 발생할 수 있다

6.보안사고보고 및 조사 동의

용역업체 참여 직원은 본교에서 사업수행 중 보안사고 발견 시 신속히 해당사항을 본교에 보고하여 지속적인 업무 활동이 보장될 수 있도록 협조한다.

7.보안감사수용

가.용역업체 참여 직원은 본교 정보보안관리규정 준수 현황 감독을 위해 본교는 정기적으로 보안감사를 실시할 수 있는 권한이 있으며,용역회사는 이에 적극적으로 협조한다.

나. 본교의 핵심 정보시스템 또는 기밀 정보를 다루는 업무를 수행하는 협력회사 직원에 대해서 E-mail 모니터링 등의 물리적, 논리적 모니터링을 실시할 수 있다.

8.기타사항

가.본교 출입 시 반드시 허가된 지역만 출입한다.

나.사업 수행을 위해 본교 내부 시스템에 대한 사용권한을 부여 받은 경우 용역회사직원은 부여 받은 계정 및 패스워드가 노출되지 않도록 각별히 주의한다.

【별지 제1호 서식】

정보보안 서약서(교직원용)

본인은 본교 (이하 “본교”라 함)에 근무함에 있어서 다음 각 호의 정보보안사항을 충분히 숙지하고, 성실히 준수할 것을 서약합니다.

1. 본인은 본교의 정보보안 규정을 준수하여, 보안 사고가 발생되지 않도록 예방 및 주의에 최선을 다할 것입니다.
2. 본인은 본교에서 근무하는 동안 취득한 본교의 정보, 개인정보, 지적 재산권들을 엄격히 보호할 것이며, 이를 개인적인 용도나 제 3자를 위한 정보로 이용하지 않고 맡은 바 업무수행을 위해서만 사용할 것입니다. 기밀을 누설함이 이적행위가 됨을 명심하고 재직중은 물론 퇴직 후에도 알게된 모든 기밀사항을 「부패방지권익위법」·「공익신고자 보호법」에 따른 신고의 경우를 제외하고는 일절 타인에게 누설하지 아니한다.
3. 본인은 본교의 정보자산(문서서류, 전자파일, 저장매체, 전산망, 전산장비 등)을 무단 변조, 훼손, 분실 등으로부터 안전하게 사용하고 관리할 것이며, 불법적인 목적으로 사용하지 않을 것입니다.
4. 본인은 본교의 업무 수행 과정 중 사용하는 PC에 승인 받은 정품 소프트웨어만을 사용할 것이며, 불법 소프트웨어 사용으로 인한 모든 책임은 본인에게 있음에 동의합니다.
5. 본인은 본교에서 퇴직하는 경우, 재직 시에 취득한 본교 소유의 모든 정보 자산을 반드시 반납할 것이며, 이후에도 개인적으로 이용하지 않을 것입니다.

본인은 상기 사항을 숙지하고 이를 성실히 준수할 것을 동의하며, 본 서약서의 준수사항을 위반한 경우에는 아래의 관계법규에 따라 엄중한 처벌을 받을 것을 서약한다.

가. 「국가보안법」제4조의 제1항 제2호 및 제5호(국가기밀 누설등)

나. 「형법」제99조(일반이적) 및 제127조(공무상 비밀의 누설)

20 년 월 일

서약자 소속 : 주민등록번호(앞자리) 성명 (인)	
서약자 집행자 소속 : 성명 (인)	

【별지 제2호 서식】

정보보안 서약서(용역업체 대표자)

(주) 대표이사 은 20 . . 부터 사업 종료시까지 수행하는 「(사업명) 」의 주관사업자로서 참여함에 있어 사업수행 기간 중 취득한 사항에 대해 비밀을 엄수하고 법인 또는 개인의 영리를 목적으로 이용하지 않으며, 이를 위반하여 발생되는 보안상의 책임과 관련법령에 의한 조치를 따를 것을 각호와 같이 서약합니다.

1. 당사는 금강대학교에서 업무를 수행함에 있어 알게 된 내부정보, 개인정보, 기타 모든 업무에 관련된 정보를 제3자에게 제공하거나, 공개 또는 누설하지 않을 것이며, 금강대학교의 사전 동의 없이 무단 사용하지 않겠습니다.

2. 당사는 금강대학교로부터 업무수행을 위하여 명시적으로 접근을 허가 받은 시설과 정보만을 이용하겠습니다.

3. 당사는 금강대학교의 사전 동의 없이는 내부정보 및 기타 개인정보와 관련된 모든 문서나 자료 및 결과물 등을 어떠한 형태로도 외부로 반출하지 않겠습니다.

4. 당사는 업무가 종결되거나 금강대학교의 요청이 있는 경우, ㅍ대학교가 제공한 모든 자료와 자산을 즉시 반납하겠습니다.

5. 당사는 업무수행의 결과 산출된 모든 결과물(보고서, 도면, 컴퓨터 프로그램, 장치 등)에 대한 제반 권리가 금강대학교에 귀속됨을 인정하고, 금강대학교 이에 대한 권리를 행사하는데 협조하겠습니다.

6. 만일 본 서약 사항을 위반하였을 경우에 당사는 법령이 정한 바에 따라 민.형사상의 모든 책임을 부담하겠으며, 본 서약 위반 행위로 인하여 금강대학교에 발생한 모든 손해를 배상하겠습니다.

20 년 월 일

용역업체명: 대 표 자 : (인)

금 강 대 학 교 총 장 귀 하

【별지 제3호 서식】

보안자료 반납 및 파기 완료 확약서

본인은 금강대학교와 계약한 사업의 수행을 완료함에 있어, 다음 각 호의 보안사항에 대한 준수 책임이 있음을 서약하며 이에 확약서를 제출합니다.

1. 본 업체는 업체 및 사업 참여자가 사업수행 중 지득한 모든 자료를 반납 및 파기하였으며, 지득한 정보에 대한 유출을 절대금지 하겠습니다.

2. 본 업체 직원의 과실은 곧 당사의 과실이며 이로 인해 발생하는 금강대학교의 손해에 대해서는 당사에서 책임지겠습니다.

3. 본 업체는 보안사항을 위반했을 경우에 민.형사상 및 보안상의 책임과 관계법규에 의한 조치에 따를 것을 서약하오며 이에 확약서를 제출합니다.

20 년 월 일

업체 (단체) 명 :
주 소 :
사업자등록번호 :
성 명 : (서명)

금 강 대 학 교 총 장 귀 하