정보 보안 규정

제 1 장 총 칙

제1조 (목적) 본 규정은 성결대학교(이하 “본 대학교”라 한다)의 보안요구사항에 대한 정보보안 관리체계의 방향성을 제시하고, 이를 바탕으로 관련 법규 및 기타 계약상의 요구에 대응하며, 정보의 오남용, 훼손, 변조, 유출 등의 위협으로부터 중요 정보 자산을 보호하고 업무의 연속성을 보장하고, 정보보안 사고로 인한 시스템 및 자원의 피해를 최소화하기 위한 기본 방침에 관한 사항을 규정함을 목적으로 한다.

제2조 (정의) 규정에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. “정보”라 함은 본 대학교 업무와 관련하여 생성 또는 입수하여 소유하고 있는 지적 자산 등의 자료로서, 컴퓨터나 저장매체에 기록된 자료를 말한다.
2. “시스템”이라 함은 다양한 서비스 제공을 위해 사용 또는 관리하는 모든 컴퓨터 하드웨어와 시스템 소프트웨어, 응용프로그램 등을 통칭하며, PC를 포함한다.
3. “정보통신망”이라함은 본 대학교내에 설치한 유무선 전산망 설비를 통칭한다.
4. “정보 관련 자산”이라 함은 정보 구축 및 운영에 필요한 인력, 시설, 장비, 관련 도서(설계서, 매뉴얼 등) 등의 유형, 무형의 자산을 말한다.
5. “정보보안담당관”이라 함은 정보보안과 관련한 제반사항을 총괄하는 책임자를 말한다.
6. “정보보안담당자”이라 함은 정보보호와 관련한 실무책임자를 말한다.
7. “정보취급자”라 함은 정보통신망 및 기타 시스템을 이용하여 정보보호 및 정보를 취급하는 일과 이와 관련한 일을 하는 자를 말한다.
8. “휴대용 저장매체”라 함은 디스켓, CD, 외장형 하드디스크, USB 메모리, 노트북 등 정보를 저장할 수 있는 휴대용 기억장치를 말한다.

제 2 장 조직체계

제3조 (정보관리책임관 지정 및 임무) ① 정보보안담당관은 기획처장으로 한다.

② 정보보안담당관의 임무는 다음 각 호와 같다.

1. 정보보안 정책 및 기본계획 수립・시행・심사・분석
2. 자체 정보보안 업무 수행에 관한 총괄 업무 관장
3. 교내 구성원에 대한 자체 정보보안 교육 관리감독

4. 교내 정보보안 진단 실시 및 감사
5. 정보보안을 위한 기술적 보안조치 사항 조정 및 감독
6. 관련규정의 제정, 개정
7. 정보보안을 위한 조직 구성 및 역할 분담
8. 사이버공격 초동조치 및 대응
9. 사이버위협정보 수집·분석 및 보안관제
10. 정보보안 예산 및 전문인력 확보
11. 위 각 호에 부수되는 업무

③ 정보보안담당관은 “정보 관련 자산”의 보호를 위해 각 전문 분야의 전담부서 및 전문분야 정보보안담당관을 지정하여 운영할 수 있다.

제4조 (정보보안심사 위원회) ① 정보보안업무의 효율적인 운영과 계획 수립, 기타 보안에 관한 중요사항을 심의하기 위하여 정보보안심사 위원회(이하 “위원회”라 한다)를 두며, 정보보안과 관련한 사항의 심의는 “정보화추진위원회”에서 정보보안업무를 담당하게 할 수 있다.

② 위원회는 다음 각 호의 사항을 심의 결정한다.

1. 정보보안 내규의 수립 및 개정에 관한 사항
2. 분야별 정보보안 대책 및 정보보안 계획 수립에 관한 사항
3. 정보보안위반자 심사 및 처리에 관한 사항
4. 정보보안업무 심의 및 정보보안업무 수행 상 조정과 협의를 요하는 사항
5. 기타 총장의 지시나 정보보안담당관이 필요하다고 인정하는 사항

제 3 장 정보보안 관리

제5조 (보안 교육 기본원칙) ① 정보보안 교육은 정보보안교육 계획에 따라 전 교직원을 대상으로 연간 1회 이상 실시한다. 단, 정보보안담당자는 연간 15시간이상 정보보안 교육(개인정보보호법 제28조 제2항의 교육 등 포함)을 이수하여야 한다.

② 제 1항의 규정에 의한 교육을 실시할 때 외부의 정보보안 전문기관에 이를 위탁할 수 있다.

③ 정보보안담당관은 정보보안 관련 전문기관 교육 및 기술 세미나 참석을 장려하는 등 정보보안담당자의 업무 전문성을 제고하기 위하여 노력하여야 한다.

④ 다음과 같은 사항의 발생 시 비정기적인 교육을 실시 할 수 있다.

1. 정보보안 정책·규정 또는 직무 등의 변경

2. 새로운 보안위협의 발생
3. 법적 요구사항에 대한 대책수립
4. 기타, 본 대학교의 정보보안 관리업무와 관련한 교육의 필요성이 있는 경우

④ 정보보안 담당부서는 정보보안 교육계획을 충실히 이행하고 교육실적을 관리하여야 한다.

제6조 (인적보안) ① 정보보안담당관은 교원, 직원 및 보조인력(용역인력 포함)에게 정보보호 및 보안에 대한 별표1의 "보안서약서"를 청구할 수 있으며 필요한 경우 관련부서에 청구를 위임할 수 있다.

② 정보보안담당관은 교원 및 직원의 인사변동이 발생하면 해당자의 개인계정 및 권한을 관리감독 한다.

③ 정보보안담당관은 본 대학교 정보보안을 위하여 정보 시스템 구축 및 그와 유사한 행위에 대해 다음과 같은 사항을 요구 또는 관련사항이 언급된 문서를 요구할 수 있다.

1. 법적 요구사항의 충족 여부
2. 모든 당사자들에게 정보보안 책임을 주지시키는 절차
3. 정보시스템의 무결성 및 비밀성 유지
4. 전산매체에 저장된 데이터의 보호 및 소유권
5. 권한이 없는 자의 시스템 접근제한에 관한 사항
6. 재난 발생 시 서비스의 가용성 유지 방법
7. 요구 자료 제출 및 감사 권한
8. 본 대학교가 필요하고 인정하는 조치 사항

④ 정보보안담당관은 정보 시스템 구축 및 그와 유사한 행위는 원칙적으로 재 위탁을 금하며 다만, 재 위탁 시 반드시 정보보안 요구사항을 준수하도록 명시하며 이를 관리/감독한다.

제7조 (개인정보 이용 및 관리) ① 개인정보취급자가 민원 등 행정서비스 업무를 수행함에 있어 홈페이지에 게시된 "개인정보보호방침"을 따라 안전하게 처리해야 한다.

② 기타 사항은 공공기관의 개인정보보호에 관한 법률을 준용한다.

③ 개인을 식별할 수 있는 정보를 담고 있는 전자적인 문서에는 암호를 부여하여 관리한다.

④ 개인을 식별할 수 있는 정보를 담고 있는 문서에는 "정보 취급자"가 사용한 PC정보, 프로그램, 성명 및 문서 생산자의 정보가 표시될 수 있다.

⑤ 개인을 식별할 수 있는 정보를 담고 있는 문서는 그 사용용도가 다하면 폐기하는 것을 원칙으로 한다.

제8조 (보안성 검토) ① 보안성 검토는 정보 시스템이 운영 단계 이전에 보안요구사항을 기반으로 실시하는 것을 원칙으로 한다. 다만 정보시스템이 방대하거나 기타의 필요성이 인정되는 경우 외부기관이나 전문가의 도움(전문 기관, 감리 등)을 얻어 보안성 검토를 실시할 수 있다.

② 보안성 검토와 관련된 사항은 문서화하여 관리하도록 한다.

제9조 (사이버보안진단의 날) ① 매월 세 번째 수요일을 '사이버보안진단의 날'로 지정·운영한다.

② '사이버보안진단의 날'에 PC 자가 진단 프로그램을 통해 백신, 운영체제 최신버전체크, 패스워드 적합성 여부, 폴더공유 사용여부 등을 점검하여 인터넷 사용을 금지할 수 있다.

제10조 (정보자산관리) ① 정보자산은 허가 없이 외부로 반출하여서는 아니된다. 정보자산을 외부로 반출할 경우 별표6의 "휴대용 저장매체 반·출입 대장"에 기입하고 정보보안담당관의 승인 후 반출하여야 한다.

② 정보자산의 유지보수 및 수리시 외부로 자료 유출을 방지하기 위하여 저장장치(HDD)를 분리하여 반출하여야 한다.

③ 정보자산 반출입시 최신 백신으로 악성코드를 점검하여야 한다.

④ PC, 노트북, 스마트기기 등 단말기는 아래와 같은 보안조치를 수행하여야 한다.

1. CMOS 비밀번호 및 로그온 비밀번호(9자리 이상) 설정
2. 10분 이상 작업 중단시 비밀번호 등이 적용된 화면보호 설정
3. 문서자료 암호화 또는 비밀번호 설정
4. 사용 후 업무자료 완전 삭제(윈도우즈 휴지통 비우기 등)
5. 공유 폴더 삭제
6. 운영체제 및 응용프로그램 최신 보안패치 유지
7. 불필요한 프로그램 설치 금지

제11조 (정보보안 문서관리) ① 정보보안담당관은 다음 각 호에 해당하는 정보통신망 관련 현황·자료 관리를 하여야 한다.

1. 정보시스템 운용현황
2. 정보통신망 구성현황
3. IP 할당현황
4. 주요 정보화사업 추진현황

② 정보통신망, 보안취약점 점검 결과물 등 중요 정보통신망 관련 자료는 대외비 문서로 관리한다.

③ 대외비 문서는 별표8의 “비밀관리 기록부”에 기입하고 지정된 보안USB에 저장 보관하여야 한다.

제12조 (용역사업 보안관리) ① 정보화·정보보호사업 및 보안컨설팅 수행 등을 외부용역으로 추진할 경우 사업 관리책임자는 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 용역사업 계약 시 계약서에 참가직원의 보안준수 사항과 위반 시 손해배상 책임 등 명시
2. 용역사업 수행 관련 보안교육·점검 및 용역기간 중 참여인력 임의교체 금지
3. 정보통신망도·IP현황 등 용역업체에 제공할 자료는 자료 인계인수대장을 비치, 보안조치 후 인계·인수하고 무단 복사 및 외부반출 금지
4. 사업 종료 시 외부업체의 노트북·휴대용 저장매체 등을 통해 비공개 자료가 유출되는 것을 방지하기 위해 복구가 불가능하도록 완전삭제
5. 용역업체로부터 용역 결과물을 전량 회수하고 비인가자에게 제공·열람 금지
6. 용역업체의 노트북 등 관련 장비를 반입·반출시마다 악성코드 감염여부, 자료무단반출 여부를 확인하고 별표6의 “휴대용 저장매체 반·출입 대장”을 기입하여 관리한다.
7. 용역사업 참가자에게 정보보호 및 보안에 대한 별표1의 “보안서약서”를 청구할 수 있으며, 용역사업 종료시 관련 자료 회수 및 삭제조치 후 복사본 등 용역사업 관련 자료를 보유하고 있지 않다는 별표11의 “보안확약서”를 용역업체 대표명의로 징구하여야 한다.
8. 그 밖에 정보보안담당관이 보안관리가 필요하다고 판단하는 사항

② 용역사업 추진 시 과업지시서·입찰공고·계약서에 다음 각 호의 누출금지 대상정보를 명시해야 하며 해당정보 누출 시 입찰 참가자격 제한을 위한 부정당업자로 등록하여야 한다.

1. 기관 소유 정보시스템의 내·외부 IP주소 현황
2. 세부 정보시스템 구성 현황 및 정보통신망 구성도
3. 사용자계정·비밀번호 등 정보시스템 접근권한 정보
4. 정보통신망 취약점 분석·평가 결과물
5. 정보화 용역사업 결과물 및 관련 프로그램 소스코드(유출시 피해가 우려되는 중요 용역사업에 해당)
6. 침입차단시스템(FW)·침입방지시스템(IPS) 등 정보보호제품 및 라우터·스위치 등 네트워크 장비 설정 정보
7. 「공공기관의 정보공개에 관한 법률」 제9조제1항의 비공개 대상 정보에 준하는 내부문서

8. 「개인정보보호법」 제2조제1호의 개인정보
9. 비밀에 해당하는 대외비 자료
10. 그 밖에 공개가 불가하다고 판단한 자료

③ 정보보안담당관은 비밀 및 중요 외주 용역사업을 수행할 경우, 외부인원에 대한 비밀취급인가, 보안교육 및 외부유출 방지 등 보안조치를 수행하여야 한다.

④ 사업 관리책임자는 제1항부터 제3항까지 규정한 보안대책의 시행과 관련한 이행 실태를 주기적으로 점검하고 미비점 발견 시 사업담당자로 하여금 보완토록 조치하여야 한다.

⑤ 그 외의 사항은 외부용역 관리지침에 따른다.

제13조 (원격근무 보안관리) ① 재택·파견·이동근무 등 원격 근무를 지원하기 위한 정보시스템을 도입·운영할 경우 기술적·관리적·물리적 보안대책을 수립하고 제8조(보안성 검토)에 따라 보안성 검토를 실시하여야 한다.

② 각 부서의 장은 원격근무 가능 업무 및 공개·비공개 업무 선정기준을 수립하되 대외비 이상 비밀자료를 취급하는 업무는 원격근무 대상에서 원칙적으로 제외하되 반드시 수행해야 하는 경우 보안대책 강구 후 정보보안담당관과 협의하여 수행여부를 결정한다.

③ 각 부서장은 모든 원격근무자에게 별표9의 보안서약서(원격근무)를 징구하고 원격근무자의 업무변경·인사이동·퇴직 등 상황 발생 시 정보시스템 접근권한 재설정 등 관련 절차를 수립하여야 한다.

④ 원격근무자는 원격근무 시 해킹에 의한 업무자료 유출을 방지하기 위하여 작업수행 전 백신으로 원격근무용 PC 점검·업무자료 저장금지 등 보안조치를 수행하여야 한다.

⑤ 원격근무자는 정보시스템 고장 시 정보유출 방지 등 보안대책을 강구한 후 정보보안담당관과 협의하여 정비·반납 등 조치를 취하여야 한다.

⑥ 각 부서의 장은 주기적인 보안점검을 실시하여 원격근무 보안의 이행 여부를 확인하여야 한다.

제 4 장 물리적 보안

제14조 (제한구역의 설정 및 운영) ① 정보보안담당관은 “정보 관련 자산”의 보안을 위해 제한구역을 설정하고 보안책임자를 지정할 수 있다.

② 제한구역에는 적당한 곳에 관리책임자의 표지를 부착하여야 하며 중요시설에 대해 외부노출을 피하기 위해 그 표지를 생략 할 수 있다.

③ 제한구역에는 별도의 출입통제 장치를 설치하여야 하며, 필요 시 감시시스템 등을 설

치하여 운영한다.

④ 제한구역에 출입하는 자는 별도 별표2의 “출입자관리대장”에 기입하며, 출입통제 시스템 운영 시는 생략 할 수 있다.

⑤ 정보보안담당관은 정보통신실을 통제구역으로 설정하고, 아래와 같은 보안조치를 수행하여야 한다.

1. 정보통신실 출입문 CCTV 등 보안장치 설치 및 주야간 감시
2. 카메라 내장 휴대폰, 디지털 카메라 등의 소지 및 촬영 금지
3. 정보통신실 출입시(CARD KEY, 열쇠)이중 잠금장치로 출입통제

제14조의 2(보호구역설비 및 운영) ① 보호구역은 각종 재해에 대비하여 다음과 같이 필요한 보호설비를 갖추고 운영절차를 수립 및 운영하여야 한다.

1. 온도·습도 조절기(항온항습기·에어컨등)
2. 화재감지기 및 소화설비
3. 누수감지기
4. 비상발전기, 무정전전원장치(UPS)
5. 감시카메라(CCTV)
6. 비상등·비상로 안내 표시

제 5 장 캠퍼스통신망 및 전자정보 보안

제15조 (캠퍼스통신망 관리 및 운영) 캠퍼스통신망 관리 및 운영에 대한 사항은 “정보화 업무 처리 규정”의 “제 4 장 캠퍼스 전산망 운영”에 따른다.

제16조 (캠퍼스통신망 이용자 준수사항) ① 본 대학교 유·무선 정보통신망의 서비스를 이용하려는 이용자는 자신의 컴퓨터 및 그에 준하는 디바이스에 대한 최신 패치 및 바이러스의 방역에 대한 의무를 가진다.

② 본 대학교 유·무선 정보통신망의 서비스에 접근하기 위해서는 교내 백신·PMS를 설치해야 하며 미 설치시는 접근을 제한 할 수 있다. 단, 백신·PMS가 지원하지 않는 컴퓨터 및 그에 준하는 디바이스는 제외한다.

제17조 (정보시스템 운영) ① 각 담당자는 정보시스템의 하드웨어 및 소프트웨어의 지속적인 가용성과 무결성 확보를 위해 취약점 점검을 실시한다.

② 각 담당자는 정보시스템 공급업체의 보안관련 패치나 권고안이 발생되는 것을 지속적으로 모니터링하여 보안패치를 적용하여야 한다. 단, 유지보수 계약이 체결되어 있는

경우 정보시스템 담당자의 관리아래 유지보수 업체에 위탁할 수 있다.

③ 각 담당자는 중요 보안관련 패치를 적용하기 전에 중요정보에 대한 백업을 수행한다.

④ 각 담당자는 기존 운영체제의 정보보안 취약점이 보완되고, 향상된 정보보안 기능이 포함되어 있는 새로운 버전의 운영체제가 출시되어 업그레이드의 필요성이 있을 경우 해당 운영체제에 대한 보안성을 검토 한 후에 업그레이드를 실시한다.

⑤ 정보시스템에는 업무용 목적으로 사용되는 프로그램 이외의 프로그램 설치를 제한한다.

⑥ 원격작업은 원칙적으로 금지하나 원격으로 접속하여 유지보수를 하는 경우 별도의 별표4 “원격 접속 신청서”를 제출 하고 정보보안담당자의 승인 후 원격으로 접속 할 수 있다.

⑦ 정보시스템 비밀번호는 숫자와 영문자, 특수문자 등을 혼합하여 9자리 이상으로 설정하고 분기 1회 이상 주기적으로 변경하여야 한다.

⑧ 네트워크 장비 등 신규 전산장비 도입시 생성되는 기본(default) 계정을 삭제 또는 변경하고 시스템 운영을 위한 관리자 계정을 별도 생성·관리하여야 한다.

제18조 (DB암호화) ①기밀성이 요구되는 DB 시스템 내의 중요 필드에 대해 암호화되어 있어야 한다.

② 암호화를 지원할 수 있는 암호화 기술이 DB 시스템에 도입되어야 한다.

③ 필요 시 DB 암호화 강화를 위해 별도 보안솔루션(DB암호화 툴 등)을 이용할 수 있다.

④ 암호키 관리는 “암호키 관리 지침”을 따른다.

제19조 (DB감사) ① 중요 로그파일은 DBA에 의해서 정기적으로 점검하고 그 내용을 별표10 “데이터베이스 점검 일지” 에 기록한다.

② 로그파일의 조작 및 읽기 권한은 DBA에게만 부여하는 것을 원칙으로 한다.

제20조 (DB 백업) ① 백업에 관한 일반적인 사항은 “정보화 업무 처리규정”의 제9조를 참조한다.

② 영구 보관할 필요성이 있는 자료에 대해서는 절차에 따라 영구보관을 할 수 있다.

제21조 (PC사용자의 책임) PC의 운용 및 관리에 있어서 고의나 부주의 또는 직접적인 실수에 의한 보안 사고 발생 시 각 PC의 해당 사용자가 그 책임을 지며, 그 세부 사항은 다음 각 호와 같다.

1. 개인/업무용 PC의 경우는 PC사용자가 책임을 진다.
2. 실습실 등의 공용 PC는 실제 관리를 수행하는 부서의 장이 그 책임을 진다.

제22조 (불법소프트웨어 사용 제한) ① PC사용자는 사용이 승인된 소프트웨어만을 사

용해야 하며, 불법소프트웨어를 사용한 경우 개인 및 본 대학교가 모두 처벌 받을 수 있음을 양지하여야 한다.

② 불법 소프트웨어를 관리하기 위해 다음 각 호를 준수해야 한다.

1. 소프트웨어의 기본용도 외에 불법 용도 변경을 금지한다.
2. 캠퍼스통신망 및 인터넷을 통한 불법복제를 금지한다.
3. 시리얼 넘버의 공유, 도용, 배포, 전송 등의 행위를 금지한다.

제23조 (바이러스 검사) ① 다음 각 호의 방법 중 하나를 선택하여 관리 책임이 있는 PC에 대하여 주기적으로 바이러스를 검사해야 한다.

1. 부팅 시 검사
2. 주기적인 예약 검사 등

② 주기적인 바이러스 검사를 위해 바이러스백신 프로그램이 PC에 설치되어 있어야 한다.

③ 최소 1주 1회 이상 자동엔진 업데이트 기능 등을 이용하여 바이러스 엔진을 업데이트하여 백신 프로그램은 항상 최신 버전으로 유지해야 한다.

④ 다음 각 호의 외부로부터 받은 파일은 실행 또는 열기 전에 반드시 바이러스 검사를 수행해야 한다.

1. 외부에서 받은 CD나 USB 메모리 같은 저장매체
2. 인터넷에서 다운로드 받은 파일
3. 외부로부터 수신된 메일의 첨부파일 등

⑤ PC 사용자 및 실습실 관리자는 바이러스 예방을 위해 예방조치를 실시해야 할 책임을 진다.

⑥ 바이러스 감염 시 정보통신망 접속을 차단하고 즉시 인가된 바이러스 백신 프로그램으로 바이러스를 치료한다.

⑦ 모든 PC 사용자 및 실습실 관리자는 보안패치 및 서비스 팩을 자발적으로 설치해야 한다.

제24조 (무선장비 보안 관리) 무선장비(AP, 브릿지, 라우터, 단말기 등)를 사용하여 업무자료를 소통하고자 할 경우 “무선장비 관리 지침”을 따라 수행하여야 한다.

제25조 (이용제한) 다음 각 호에 해당하는 행위를 한 이용자에 대하여 캠퍼스통신망 이용을 제한할 수 있다.

1. 부당한 방법으로 정보통신망의 타인 정보를 훼손하거나 침해 도용 또는 누설하는 행위
2. 컴퓨터바이러스, 웜, 밀 웨어 등 악성 프로그램 유포 및 캠퍼스통신망을 위해 하는 프

로그램을 배포하는 행위

3. 음란, 폭력물, 광고 등 불건전한 내용의 게재 및 유포행위
4. 캠퍼스통신망의 장애유발을 목적으로 다량의 패킷을 전송하는 행위
5. 기타 정보보호에 해가 되는 행위 및 그와 유사한 행위

제 6 장 침해사고 대응 및 보안 감사

제26조 (침해사고 보고) 침해사고의 발생 및 침입 흔적을 인지한 경우 "정보보안담당관"에게 문자나 전화로 보고 후 조치결과를 문서로 보고하여야 하며, 침해사고 발생 사실을 지정된 보고자 이외의 사람에게 유출시켜서는 안 된다.

제27조 (침해사고 대응) ① "정보보안담당자"는 시스템에 대한 침입이 확인되면 다음과 같은 사항을 참고하여 사이버위기 대응 매뉴얼에 따라 보고한다.

1. 백도어의 확인
2. 스캐닝 및 스니핑 탐지
3. 허가 받지 않은 서비스의 조사
4. 비밀번호 파일의 변경여부
5. 설정 파일조사
6. 파일공유 및 외부전송 여부
7. 기타 필요한 사항

제28조 (정보보안감사) ① 정보보안감사는 정보보안 기준에 규정된 사항을 확인하기 위한 모든 활동을 말하며 본 대학교가 보유한 "정보", "시스템" 및 "정보 관련 자산"을 그 대상으로 한다.

제29조 (정보보안감사 결과) ① 감사결과를 "정보보안담당관"에게 보고하고 문서화하여 보관하며 총장 또는 외부 감독기관의 요청이 있는 경우 이를 제출할 수 있도록 보관하여야 한다.

② 정보보안감사 결과 보고서에는 다음과 같은 내용이 포함될 수 있다.

1. 보고서는 감사의 목적과 범위, 실시 기간 등을 명시하고 주요 결과를 요약하여 기술한다.
2. 지적사항에 대해서는 관련 업무 담당자와 상위관리자의 의견이나 향후 조치 계획 등이 함께 기술되도록 한다.
3. 정보보안 정책·규정의 미흡한 부분이나, 건의 사항 등이 반영되도록 정책·규정의 제반 사항을 정비하도록 한다.

4. 정보보안감사를 외부 전문가를 활용하여 시행한 경우 외부 전문가에 의해 시행된 범위를 명시하며, 정보보안감사의 전부를 외부에 위탁하여 시행한 경우에는 외부전문가의 감사보고서로 대치할 수 있다.

제 7 장 휴대용 저장매체 관리

제30조 (USB메모리 및 관리시스템 도입) ① USB메모리 및 관리시스템을 도입할 경우 그 제품의 안전성을 검증하기 위해 보안성 평가를 받아야 한다. 다만 보안 적합성 검증(CC인증)을 받은 제품은 예외로 둔다.

② 휴대용 저장매체 보안관리를 안전하게 관리하기 위하여 휴대용 저장매체 관리시스템을 구축할 수 있다.

제31조 (휴대용 저장매체 사용) ① USB메모리 등의 휴대용 저장매체를 사용 시에는 별표3의 “휴대용 저장매체 관리대장”에 등록 후 사용한다.

② USB메모리 등의 휴대용 저장매체의 관리책임자는 각 부서의 장이 하며 비밀용, 일반용으로 구분하고 주기적으로 수량 및 보관 상태를 별표5 “휴대용 저장매체 점검대장”에 기입하여 점검하며 별표6 “휴대용 저장매체 반·출입 대장”에 기입하여 반·출입을 통제하여야 한다.

③ 일반용 휴대용 저장매체의 관리요령은 다음과 같다.

1. 일반용에는 업무관련 일반자료(공인인증서 포함)만 보관하여야 하며 별표3 “휴대용 저장매체 관리대장”에 기록하여야 한다.
2. 일반용에는 별표7의 서식과 같이 기입·표시하여야 한다.
3. 관리번호는 팀·과명, 일반, 연번으로 한다. 이 경우 팀·과명은 약칭을 사용할 수 있다. (예 : 총무과-일반-01, 총무과-일반-02, 총무-일반-03 등)

④ 대외비 이상 자료를 보관하는 비밀용 휴대용 저장매체(이하 “비밀용”이라 한다) 관리요령은 다음과 같다.

1. 비밀용을 사용할 경우에는 별표3 “휴대용 저장매체 관리대장”에 기록하여야 하며 대외비 이상의 기밀자료가 수록되어 있는 경우에는 별표8 “비밀관리 기록부”에도 등재·관리하여야 한다.
2. 비밀용은 비밀자료와 동일하게 캐비닛 또는 금고에 보관하여야 한다.
3. 비밀용에는 별표7의 서식과 같이 기입·표시하여야 한다.
4. 비밀용을 사용하여 비밀작업을 하는 경우 그 작업을 완료하거나 일시 중단할 때에는 PC에서 즉시 분리하여야 한다.

5. 관리번호는 팀·과명, 비밀등급, 연번으로 한다. 이 경우 팀·과명은 약칭을 사용할 수 있다.(예 : 총무과-Ⅱ급-01, 총무과-Ⅲ급-01, 총무-대외비-01 등)

제32조 (휴대용 저장매체 불용처리 및 재사용) ① 업무목적으로 사용한 USB메모리 등의 휴대용 저장매체의 불용 처리 시 물리적 파기를 원칙으로 하며 그 사실을 별표3 "휴대용 저장매체 관리대장"에 기입한다.

제 8 장 정보보안 규정의 유지관리

제33조 (규정의 유지관리) ① "정보보안담당관"은 정보보안규정의 타당성을 매년 1회 정기적으로 검토해야 하며, 업무환경의 변화 발생 등과 같은 변화요인 발생 시 추가 검토할 수 있다.

② 정보보안과 관련하여 새로운 요구 사항이 도출되거나 정보보안감사 결과 및 정보보안 정책·지침의 검토 결과 개정이 필요한 경우 정보보안규정을 제·개정할 수 있다.

제 9 장 위반자조치 및 기타

제34조 (위반자조치) 본 규정을 위배한 자는 관계법령과 본 대학의 규정에 의하여 위법조치 및 불이익을 취할 수 있다.

제35조 (준용) 이 규정에 명시되지 않은 사항은 관계법령, 교육부 정보보안 기본지침과 본 대학교의 제반규정에 따른다.

부 칙

(시행일) 이 규정은 2011년 1월 1일부터 시행한다.

부 칙

(시행일) 이 개정 규정(제2조, 제3조, 제6조, 제7조)은 2013년 12월 1일부터 시행한다.

부 칙

(시행일) 이 개정 규정(제2조～제6조, 제8조～제35조, 별표 2～3, 5～11)은 2017년 5월 22일부터 시행한다.

부 칙

(시행일) 이 개정 규정(제3조)은 2018년 11월 19일부터 시행한다.

부 칙

(시행일) 이 개정 규정(제3조, 14조의 2)은 2020년 2월 29일부터 시행한다.

부 칙

(시행일) 이 개정 규정(제8조, 제13조, 제14조의 2)은 2023년 02월 28일부터 시행한다.

<별표 1>

보 안 서 약 서

소속 :

직위 :

성명 :

상기 본인은 본교 (　　)시스템 개발과 관련하여 다음 사항에 대해 준수할 것을 엄숙히 서약합니다.

1. 본교 제반규정과 지침 및 관계법령을 준수하겠습니다.

2. 본교 시스템 개발과 관련되어 알게 된 모든 기밀 및 업무상의 자료를 외부로 유출하지 않음은 물론 시스템 개발 완료 후에도 본교에서 획득한 어떠한 자료도 타인에게 누설하지 않겠습니다.

3. 위 사항들을 위반할 시에는 관계법령에 따라 어떠한 처벌도 감수할 것을 서약합니다.

2010년　　월　　일

위 본 인 :　　(인/서명)

성결대학교 총장 귀하

<별표 2>

(　　)실 출입 관리 대장

출입일자	셩명	연락처	작업이력	장비명	시작시간	종료시간	관리자 확인
2017.01.01	홍길O	010-*	정기점검	L4	2017.01.01. 00:00	2017.01.01. 00:00	

<별표 3>

휴대용 저장매체 관리대장

<관리부서 및 관리책임자 : OOOO>

순번	관리번호 (S/N)	일반용/ 비밀용	비밀 등급	매체 형태	등록일자	취급자	불용 처리일자	불용처리방법 (재사용 용도)	비고
1	정보기획과 -일반-01	일반용		USB	2017.01.02	홍길동	2017.02.01	물리적 파괴	고장
2	정보기획과 -일반-02	일반용		외장 하드	2017.01.13	홍길동	2017.02.01	포맷후 재사용 (관리번호)	
3									
4									
5									
6									
7									
8									

<별표 4>

원격 접속 신청서

신청일: 년 월 일

<table>
<tr><td rowspan="2">부서</td><td colspan="2" rowspan="2"></td><td>신청자</td><td></td></tr>
<tr><td>담당자</td><td></td></tr>
<tr><td>연락처
(TEL/CP)</td><td colspan="2"></td><td>이메일</td><td></td></tr>
<tr><td>사용기간</td><td colspan="4">년 월 일 ~ 년 월 일</td></tr>
<tr><td>구분</td><td colspan="4">신규 / 변경 / 연장 / 해지</td></tr>
<tr><td>서비스
요청 사유</td><td colspan="4"></td></tr>
<tr><td rowspan="6">요청 내역</td><td>사용자 IP 주소
(Source IP)</td><td colspan="3"></td></tr>
<tr><td>목적지 IP 주소
(Destination IP)</td><td colspan="3"></td></tr>
<tr><td>프로토콜</td><td colspan="3"></td></tr>
<tr><td>사용포트</td><td colspan="3"></td></tr>
<tr><td>목적지 서버의
주요서비스</td><td colspan="3"></td></tr>
<tr><td>목적시 서버
용도</td><td colspan="3"></td></tr>
<tr><td>기타
요청사항</td><td colspan="4"></td></tr>
<tr><td>검토사항</td><td colspan="4"></td></tr>
<tr><td>비고</td><td colspan="4"></td></tr>
</table>

※ 만료기간 경과 후(최대 1년) 별도 연장 신청이 없을 경우 해당 룰은 자동 삭제됨

<별표 5>

휴대용 저장매체 점검대장

<관리부서 및 관리책임자 : OOOO>

점검일시	현 보유수량				이상 유무	점검관		비고
	Ⅱ급	Ⅲ급	대외비	일반		성명	서명	
2017.1.3	1	1	3	15	이상무	홍길O	홍길O	
2017.1.13	1	1	2	16	이상무	홍길O	홍길O	
2017.2.1	1	1	2	16	이상무	홍길O	홍길O	
2017.2.28	1	1	2	17	이상무	홍길O	홍길O	

<별표 6>

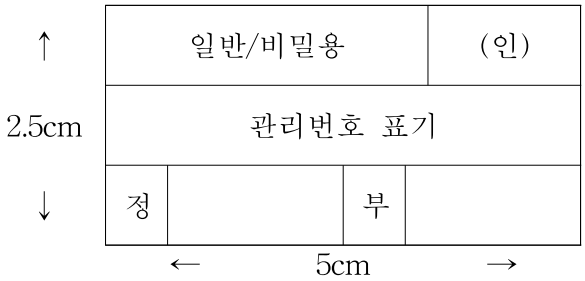
휴대용 저장매체 반·출입 대장

<관리부서 및 관리책임자 : OOOO>

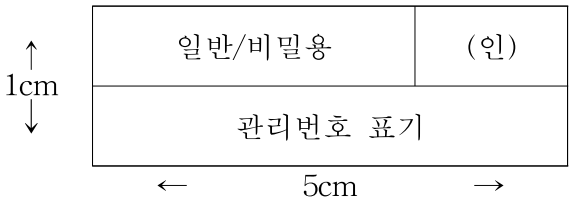
장비명	관리번호	용도	반출입 일시	자료반출여부	백신점검 결과	사용자 확인	관리자 확인
USB	정보기획과-일반-01	회의제출	2017.01.1 11:00 (출)	예	이상없음	홍길O	OOOO
CD	정보기획과-2	회의제출 회수	2017.01.7 09:40 (입)	아니요	이상없음	홍길O	OOOO
노트북	정보기획과-1	세미나 발표	2015.10.7 17:50 (입)	예	이상없음	홍길O	OOOO

<별표 7>

휴대용 저장매체 라벨



<디스켓, 이동형 HDD 서식>



<USB, CD 등 서식>

가. 同 서식을 만들어 휴대용 저장매체 중앙의 적절한 위치에 부착

나. 첫 번째 줄에는 일반/비밀용(인)란에 정보보안담당관 또는 관리책임자의 직인을 날인

다. 두 번째 줄에는 휴대용 저장매체 관리번호 표기

라. 세 번째 줄의 '정'란에 관리책임자, '부'란에 취급자 표기
(USB메모리 및 CD의 경우 생략 가능)

마. 휴대용 저장매체의 크기를 고려하여 서식·글자 크기 조정 가능

<별표 8>

비밀관리 기록부

<관리부서 및 관리책임자 : OOOO>

순번	구분	등재일	내 용	담당자	관리USB (S/N)	비고 (등급)
1	비밀	2017.01.01	성결대 네트워크 구성도	홍길O	정보기획과-Ⅱ급-01	신규
2	비밀	2017.01.05.	성결대 네트워크 구성도	홍길O	정보기획과-Ⅱ급-01	수정
3	비밀	2017.01.06.	사이버 모의훈련 결과 보고서	홍길O	정보기획과-Ⅱ급-02	신규

<별표 9>

보 안 서 약 서(원격근무)

본인은 ____년 __월 __일부로 원격근무를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 나는 부여받은 인증 관련 정보 및 매체를 타인에게 유출하지 아니한다.

2. 나는 원격근무 중 작성·저장·열람·출력한 문서는 업무 목적에만 활용하고 타인에게 유출하지 아니한다.

3. 나는 원격근무용 소프트웨어 및 전산장비를 업무목적에만 활용하며 바이러스백신 프로그램 및 기타 보안 프로그램을 설치하여 최신 상태로 유지한다.

4. 나는 기타 보안사항들을 성실히 준수하며 위반 시 관련 규정에 따라 어떠한 처벌도 감수한다.

년 월 일

서 약 자 소 속 :
직 급 (직위) :
성 명 : 서명(인)

서약집행자 소 속 :
직 급 (직위) :
성 명 : 서명(인)

<별표 10>

데이터베이스 점검 일지

<관리부서 및 관리책임자 : OOOO>

순번	DB구분	작업 구분	이상내용	조치/확인 결과	점검일자	점검자
1	SKY1	로그	특이사항 없음	해당없음	2017.03.02.	홍길O
2	SKY2	백업	ABC DB 백업 오류	조치완료	2017.03.02.	홍길O
3	홈페이지	로그	특이사항 없음	해당없음	2017.03.02.	홍길O

<별표 11>

보 안 확 약 서

본 업체(단체)는 귀 대학과 계약한 _____관련 용역사업(업무)을 완료함에 있어 다음 각 호의 보안사항에 대한 준수 책임이 있음을 서약하며 이에 확약서를 제출합니다.

1. 본 업체(단체)는 업체(단체) 및 사업 참여자가 사업수행 중 지득한 모든 자료를 반납 및 파기하여 복사본 등 용역사업 관련 자료를 보유하지 않으며, 지득한 정보에 대한 유출을 절대 금지한다.

2. 본 업체(단체)는 하도급업체에 대해 상기 항과 동일한 보안사항 준수 책임을 확인하고 보안확약서를 징구하였으며, 하도급업체가 위의 보안사항을 위반할 경우에 주 사업자로서 이에 동일한 법적책임을 지겠습니다.

3. 본 업체(단체)는 상기 보안사항을 위반할 경우에 귀 기관의 사업에 참여 제한 또는 기타 관련 법규에 따른 책임과 손해배상을 감수한다.

년 월 일

서약자 (업체대표)
업 체 명 :
직 위 :
성 명 : (서명)

성결대학교 총장 귀하