정보보안규정

제정 : 2012. 11. 12
개정 : 2015. 05. 08
개정 : 2020. 06. 05

담당자 : 전산지원팀(02-950-5468)

제1조(목적) 본 규정은 한국성서대학교(이하 “본 대학교”라 한다.)내의 네트워크, 정보시스템, 응용프로그램, 데이터베이스 등 정보자산을 안전하게 보호하며, 정보환경을 보다 안전하고 신뢰성 있게 운영하기 위하여 필요한 제반 사항에 관한 내용을 정의함을 목적으로 한다.

제2조(정의) 이 규정에서 사용하는 용어의 정의는 다음 각 호와 같다.(개정2020.04.28)

1. “정보시스템”이라함은 본 대학교에서 학사행정을 목적으로 보유하고 있는 데이터를 등록, 수정, 변경, 조회할 수 있는 서버·PC 등 단말기, 보조기억매체, 전산·통신장치·정보통신기기, 응용 프로그램 등 정보의 수집·가공·저장·검색·송수신에 필요한 소프트웨어와 하드웨어를 총괄하여 말한다.
2. “정보보안담당관”이라 함은 각급기관의 정보보안업무를 총괄하기 위하여 각급기관의 장이 임명한 사람을 말한다.(개정15.02.06)
3. “사용자”라 함은 각급기관의 장으로부터 정보통신망 또는 정보시스템 등에 대한 접근 또는 사용 허가를 받은 자를 말한다.
4. “휴대용 저장매체”라 함은 디스켓·CD·외장형 하드디스크·USB 메모리 등 정보를 저장할 수 있는 것으로 PC 등의 정보시스템과 분리할 수 있는 기억장치를 말한다.
5. “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.
6. “전자정보”라 함은 각급기관이 업무와 관련하여 취급하는 전자문서 및 전자기록물을 말한다.
7. “정보통신실”이라 함은 서버·PC 등과 스위치·교환기·라우터 등 네트워크 장치 등이 설치 운용되는 장소를 말하며, 전산실·통신실·전자문서 및 전자기록물(전자정보) 보관실 등을 말한다.
8. “안전측정”이라 함은 정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 해킹·컴퓨터바이러스·서비스방해 등으로부터 정보통신망과 정보를 보호하기 위하여 정보보안 취약점을 진단하는 제반활동을 말한다.
9. “암호장비”라 함은 정보통신망으로 처리·저장·송수신되는 정보를 보호할 목적으로 암호논리를 내장하여 제작된 장비를 말한다.
10. “암호논리”라 함은 정보의 유출, 위·변조, 훼손 등을 방지하기 위하여 기밀성·무결성·인증·부인봉쇄 등의 기능을 제공하는 수학적 논리 또는 알고리즘을 말한다.
11. “암호모듈”이라 함은 정보의 유출, 위·변조, 훼손 등을 방지하기 위해 암호논리를 활용하여 구현한 수단이나 도구를 말한다.
12. “정보보호시스템”이라 함은 정보의 수집·저장·검색·송신·수신시 정보의 유출, 위·변조, 훼손 등을 방지하기 위한 하드웨어 및 소프트웨어를 말한다.

13. “정보보안 수준진단”라 함은「전자정부법」제56조 등에 따라 각급기관의 국가정보 보안 정책에 대한 이행여부를 확인하기 위하여 실시하는 평가를 말한다.
14. “사이버공격”이라 함은 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스방해 등 전자적 수단에 의하여 정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 공격 행위를 말한다.
15. “보안관제”라 함은 사이버공격 정보를 실시간으로 탐지 및 분석, 대응하는 일련의 활동을 말한다.
16. “보안관제센터”라 함은 일정한 수준의 시설 및 장비와 이를 운영하기 위한 전문 또는 전담인력을 갖추고 보안관제업무를 수행하는 조직을 말한다.

제3조(정보보안심사위원회) ① 본 대학교의 정보보호에 관한 중요한 사항을 심의하기 위하여 정보보안심사위원회(이하 “위원회”라 한다)를 둔다.
② 위원회의 위원장은 총장이 임명하며 교목실장, 교학처장, 전산지원팀장과 위원장이 추천하는 3인으로 하며, 이때 정보보호전문가를 포함하여야 한다.(개정2015.05.08)
③ 위원회의 위원장이 정보보안담당관을 겸한다.

제4조(정보보안심사위원회 기능) ① 위원회는 다음 각 호의 사항을 심의한다.
1. 정보화 추진 정책 및 계획 수립
2. 정보화 추진을 위한 재정 및 투자에 관한 사항
3. 정보보호 정책 및 계획 수립
4. 정보보호 관련 지침의 수립, 이행 상태의 확인 처리
5. 정보보호 사고의 처리
6. 기타 정보보호 관련사항
② 위원회의 운영에 관한 사항은 회의록으로 남기고, 의결사항을 보관한다.

제5조(정보보안 조직) ① 본 대학교의 정보보호 제반 업무는 담당부서인 전산지원팀에서 처리한다.(개정 2015.05.08.)
② 조직 내 “정보보안담당관”은 「교육부 정보보안 기본지침」 제5조에 근거하여 본 대학교 총장이 임명하며 정보보안 조직을 지휘하고 소속 및 산하기관에 대한 정보보안 업무를 총괄하는 자를 말한다.(신설 2020.04.28)
③ “정보보안담당관”은 다음 각 호의 업무를 수행한다.(신설2020.04.28)
1. 정보보호 활동계획 수립, 시행 및 정보보안 관련 규정, 지침, 시행세칙 등 제·개정
2. 정보보호 전담조직 구성 및 관리
3. 정보보안심사위원회에 정보보안 안건 심의 주관
4. 정보보호 관리실태 평가 및 정보보안 수준진단 총괄
5. 정보보호 예산 및 전문 인력 확보
6. 사이버 침해사고 초동조치 및 대응
7. 재난방지 대책 수립 및 대외 협의기구 정보협력
8. 정보보안교육 총괄 및 ‘사이버보안진단의 날’ 계획 수립, 시행
9. 해당 기관에 대한 정보보안 감사
10. 기타 교내 정보시스템 보안을 위하여 필요한 행위

제6조(정보보호 관련 사업계획서, 예산계획서) 본 대학교의 정보보안 담당관은 정보보호 관련된 당해

연도 사업계획서, 예산계획서를 수립하여야 한다.

제7조(정보보안 규정자료 배포) 본 대학교의 위원회를 거쳐 정해진 사항들 중, 교내 구성원들에게 필요한 사항은 내부게시판, 그룹웨어 등을 통해 공지, 배포한다.

제8조(정보보호 교육계획) 정보보호 교육은 매년 1회 이상 전체 교원, 직원을 대상으로 진행하며 교육주제는 담당부서에서 교육시점을 기준으로 적절한 주제를 선정한다.

제9조(개인정보 파기) ① 개인정보 파기는 별지서식(3)의 양식에 따라 해당 부서 팀장의 감독 하에 개인정보 파기대장을 작성하고 파기결과를 상급자에게 보고하도록 한다.
② 개인정보가 저장되어 있는 하드디스크 저장매체를 파기하는 경우에는 공장 로우포맷(Low Format)방법으로 재생 불가능하게 파기하며 저장매체의 파기는 전산지원팀에서 총괄하여 진행한다.(개정 2015.05.08)

제10조(홈페이지 개인정보노출 방지) ① 부서별로 첨부파일 게시 전에 상급자의 확인을 받도록 한다.
② 첨부파일 업로드 시 경고문구, 경고창을 띄워서 확인한다.
③ 자체 모니터링은 부서별로 다음과 같이 담당구역을 지정하여 진행하며 노출방지 가이드라인에 다른 취약점 점검은 총괄적으로 전산지원팀에서 담당한다.(개정2015.05.08) (개정2020.04.28)

부 서	자체 모니터링 구역	모니터링 내용	주요 개인정보
교목실	공지사항 게시판 일반 게시판	본문 및 첨부파일에 개인정보 기재여부	학번, 이름, 주민등록번호, 휴대폰번호, 금융관련정보 등
교학팀	공지사항 게시판, 장학/등록금 게시판, Q&A 게시판, 총학생회 게시판		
교수학습센터	교수학습센터 홈페이지		
대외협력실	발전기금 홈페이지		
대학원 교학팀	대학원 홈페이지		
사무관리팀	공지사항 게시판, 장학/등록금 게시판, Q&A 게시판		
일립생활관	공지사항 게시판 일반 게시판		
도서관	도서관 홈페이지		
취창업지원센터	취창업 홈페이지		

평생교육원	평생교육원 홈페이지		
전산지원팀	해당 부서 외의 영역		

(개정2020.04.28)

제11조(정보시스템 접근권한 관리) 정보시스템의 접근권한은 다음과 같이 하며 필요시 해당 부서장의 요청으로 임시권한을 특정인에게 특정기간 부여할 수 있다.

부서	관련데이터	수정/삭제권한	조회권한
교학팀	학부 학적, 수업성적, 장학, 교원업적, 학생카드, 교육통계	팀장, 업무담당자	업무외 담당자
대학원 교학처	대학원 학적, 수업성적, 장학, 학생카드, 교육통계	팀장, 업무담당자	업무외 담당자
사무관리팀	인사, 급여, 등록금, 회계, 수익사업, 학생카드	팀장, 업무담당자	업무외 담당자
한국어 교육원	어학원 학적, 외국인	원장, 부원장 업무담당자	업무외 담당자
평생교육원	평생교육원 학적, 수업	원장, 팀장, 업무담당자	업무외 담당자
기획실	예산, 회계, 결산, 교육통계	팀장, 업무담당자	업무외 담당자
대외협력실	기부금	팀장, 업무담당자	업무외 담당자
교수학습센터	교수학습	팀장, 업무담당자	업무외 담당자
전산지원팀	시스템 관리	팀장, 업무담당자	업무외 담당자

(개정2020.04.28)

제12조(정보처리구역 출입통제) ① 정보통신 및 정보보호시스템이 설치되어 있는 전산지원팀은 보호구역 및 출입통제구역으로 지정하고 별지서식(1)의 양식에 따라 전산지원팀 팀장의 관리 하에 출입대장을 작성한다.(개정2015.05.08)(개정2020.04.28)

② 출입통제구역에는 물리적 보안장치를 설치하여 정보시스템을 보호한다.

③ 출입통제구역에 출입 시 정보보안담당자의 의해 승인된 전산장비(노트북 등) 및 휴대용 저장매체(USB 메모리, 외장하드, SD카드, CD, DVD 등) 이외는 반입을 허가하지 않는다.

④ 출입통제구역에 출입 시 정보보안담당자의 의해 승인된 휴대용 촬영장치에 소지 및 촬영 이외에는 모두 제한한다.

제13조(네트워크 시스템 관리) ① 네트워크 시스템은 전산지원팀에서 통합 관리하며, 관리자는 전산지원팀 근무자로 한다.(개정2015.05.08)
② 관리자는 일정 횟수 접속실패 시 접속을 차단하고 관련 정보를 로그에 기록한다.
③ 사용자는 임의로 네트워크 IP주소를 변경할 수 없다.
④ 라우터 패스워드는 최소의 관리자만 보유하며 매월 변경함을 원칙으로 한다.
⑤ 인터넷을 이용한 모든 외부로부터의 접근은 원칙적으로 방화벽을 통해서만 접근할 수 있도록 한다.
⑥ 외부접속자의 관리자 로그인은 허용하지 아니한다.

제14조(네트워크 시스템 보호) ① 전산지원팀은 본 대학교에 유해하거나 불필요하다고 판단되는 웹사이트의 접속을 통제할 수 있으며, 사용자가 본 대학교 정보보호 기대수준에 미달하는 경우 네트워크 사용을 제한할 수 있다. 또한, 원격 사용자의 공중망 네트워크를 통한 접속은 인증시스템 또는 방화벽에 의해 통제할 수 있다.(개정2015.05.08)
② 전산지원팀은 의심스러운 활동에 대해서는 방화벽, 침입탐지시스템 및 기타 보안 시스템의 로그를 분석하여 해당 내용을 확인하여야 하고, 네트워크 관리 정책에 대한 변경관리를 하여야 한다.(개정2015.05.08)
③ 사용자는 교내 네트워크 사용 시 적법한 사용자임을 인증 받고 사용자의 PC・응용프로그램 등의 무결성 수준 및 보안수준을 점검하여야 한다.

제15조(무선랜 보안 및 운영 정책)
① 「교육부 정보보안 기본지침」제43조 5항에 의거하여 교내 내부망을 제외한 정보통신망에서 학생들의 교육 목적으로 무선랜을 구축, 운용하며 관리자는 전산지원팀 근무자가 된다.(신설2020.04.28)
② 무선랜 장비의 관리는 다음 각 호와 같은 지침을 따른다.(신설2020.04.28)
1. 무선랜 장비(AP)의 암호 변경 주기는 제34조(비밀번호 갱신 주기)를 따른다.
2. 사용 절차는 관리자가 작성하여 교내 구성원들에게 배포한다.
3. 관리자는 무선랜과 관련된 장비 (AP/브릿지/라우터, 단말기 등)의 최신 펌웨어 업데이트를 주기적으로 확인하고 설치를 진행한다.
4. 본 대학교 내에 운영 중인 무선 AP를 접근 하는 휴대용기기(노트북, 스마트폰, PDA 등)는 비밀번호 인증을 통하여 접근 가능하도록 한다.
5. 무선랜 장비(AP)의 WPA2 이상의 안전한 암호를 설정하고 확인한다.
③ 무선랜과 관련된 장비 (AP/브릿지/라우터, 단말기 등)에 대한 현황을 작성하여 유지, 관리한다.(신설2020.04.28)
④ 무선랜에 연결된 사용자 접속 로그를 유지하고, 관리자 접속은 전산지원팀 담당자 관리용PC로 한정하며, 담당자로 지정된 특정IP만 접속한다.(신설2020.04.28)

제16조(침입차단 시스템 관리) ① 본 대학교의 침입차단 시스템은 전산지원팀에서 관리하며, 본 시스템의 관리자는 전산지원팀 근무자로 한다.(개정2015.05.08)
② 본 시스템의 관리자는 침입차단 시스템에 대한 모든 접근정보를 기록하여 주기적인 점검 및 분석을 실시한다.

제17조(보안서버 구축 운영 관리) 본 대학교의 정보시스템은 보안서버로 구축하며 전산지원팀은 보안서버구축 현황을 관리한다.(개정2015.05.08)

제18조(백신 시스템 관리) ① 본 대학교의 백신 시스템은 전산지원팀에서 관리하며, 본 시스템의 관리자는 전산지원팀 근무자로 한다.(개정 2015. 05. 08)
② 본 시스템의 관리자는 백신 시스템에 대한 모든 접근정보를 기록하여 주기적인 점검 및 분석을 실시한다.

제19조(패치관리 시스템 관리) ① 본 대학교의 패치관리 시스템은 전산지원팀에서 관리하며, 본 시스템의 관리자는 전산지원팀 근무자로 한다.(개정2015.05.08)
② 본 시스템의 관리자는 패치관리 시스템에 대한 모든 접근정보를 기록하여 주기적인 점검 및 분석을 실시한다.

제20조(스팸메일 시스템 관리) ① 본 대학교의 스팸메일 시스템은 전산지원팀에서 관리하며, 본 시스템의 관리자는 전산지원팀 근무자로 한다.(개정2015.05.08)
② 본 시스템의 관리자는 스팸메일 시스템에 대한 모든 접근정보를 기록하여 주기적인 점검 및 분석을 실시한다.

제21조(정보보호시스템 유지보수) 본 대학교의 정보보호시스템의 정책 및 패턴의 업데이트를 위한 유지보수 이력을 관리한다.(개정2020.04.28)

제22조(정보자산 등급화 기준) ① 정보보안담당관은 비밀이 아닌 중요 전자정보의 효율적 보호를 위하여 다음 각 호에 해당하는 전자정보에 대하여 자체 실정에 맞는 보호등급으로 분류하여야 한다.
1. 최초로 정보통신망을 신설하여 전자정보의 보호등급 구분이 필요한 경우
2. 현재 운용중인 정보통신망을 재구성할 경우
3. 각급기관의 장이 필요하다고 인정하는 경우
② 제 1항의 규정에 의한 전자정보의 보호등급 분류는 다음 각 호와 같이 구분한다.
1. '가' 급 : 유출 또는 손상되는 경우 각급기관의 업무수행에 중대한 장애를 초래하거나 개인 신상에 심각한 영향을 줄 수 있는 전자정보
2. '나' 급 : 유출 또는 손상되는 경우 각급기관의 업무수행에 장애를 초래하거나 개인 신상에 영향을 줄 수 있는 전자정보
3. '다' 급 : 유출 또는 손상되는 경우 각급기관의 업무수행 기관의 이미지에 경미한 영향을 줄 수 있는 전자정보

제23조(보안적합성 검증) ① 「교육부 정보보안 기본지침」 제72조, 73조에 의하여 정보보호시스템을 도입할 경우 각급기관의 장은 사전에 보안적합성 검증을 신청하거나 자체적으로 판단하여 검증을 생략하는 보안적합성 검증 수행여부를 확인하여야 한다. 다만, 본 대학의 경우 자체 정보보안심사위원회를 통하여 보안적합성 검증을 수행한다.(개정2020.04.28)
② 보안적합성 검증대상은 다음 각 호와 같다
1. 상용 정보보호시스템
2. 각급기관의 장이 자체 개발하거나 외부업체 등에 의뢰하여 개발한 정보보호시스템
3. 보안성 검토 결과 세부 검증이 필요하다고 판단된 보안기능이 있는 정보시스템 및 제어시스템 등
③ 제2항에도 불구하고, 다음 각 호의 경우에는 검증을 생략할 수 있다.

1. 국가정보원장이 정한 국내용 CC 인증제도에 따라 인증을 받은 정보보호시스템
2. 국가정보원장이 안정성을 확인한 암호제품
3. 그 밖에 국가정보원장이 보안적합성 검증이 불필요하다고 인정한 시스템

제24조(시스템실 운영 및 관리) ① 각 건물별 네트워크 허브 등의 정보통신시설물 비치 장소를 시스템실이라 하고 전산지원팀에서 관리하며 관리자는 전산지원팀 근무자가 된다.(개정 2015. 05. 08)
② 시스템실은 다음 각 호와 같은 설비를 구비하여야 한다.
1. 입실자 식별이 가능한 출입보안장치
2. 자동화재경보 및 할로겐 가스 등 소화 시 장비에 피해를 주지 않는 소화설비
3. 정전에 대비한 별도 전원공급장치
4. 항온항습기
③ 시스템실의 관리자는 운영일지 및 장애일지를 작성해야 하며, 주기적으로 로그파일을 분석하여 이상 발견 시 즉시 조치를 취하고 이를 해당 정보보안담당자에게 보고하여야 한다.
④ 시스템실은 보호구역으로 설정하여 비인가자의 출입을 통제하며, 출입자 명부를 비치한다.
⑤ 보호구역으로 설정된 곳은 분기별 1회 이상 내부 구성원과 일반인과의 접근 권한이 정기적으로 검토 및 갱신되고 있는지 관리한다.

제25조(정보보호시스템의 도입, 운용) ① 본 대학교 내에 정보보호시스템은 정보보안심사위원회의 보안적합성 심사를 통과한 후 시스템 도입, 운용이 가능하다.(개정2020.04.28)
② 위원회의 보안적합성 심사는 제23조를 따른다.
③ 위원회, 정보보안담당관의 허가 없이 보안적합성 검증이 완료된 정보시스템의 형상 및 보안기능을 도입 목적 이외의 용도로 변경, 운용할 수 없다.

제26조(정보시스템 사용자 계정 정보 관리) ① 서버시스템 등의 운영 관리자는 다음 각 호와 같이 계정을 관리하여야 한다.
1. 사용자별 또는 그룹별로 접근권한을 부여한다.
2. 사용자 계정의 등록·변경 및 폐기는 각 시스템 관리자가 실시하며, 특별한 상황이 발생하는 경우에 한하여 부서장의 허가를 받은 후 작업을 실시한다.
3. 외부 사용자의 계정은 유효기간을 설정한다.
4. 특별한 사유 없이 일정기간 이상 사용하지 않는 계정은 학기 시작 일주일 이내에 말소할 수 있다.
5. 일정회수 접속 실패 시 사용을 금지한다.
6. 특정 단말에서만 슈퍼유저의 접속을 허용한다.
② 주요정보시스템의 사용자 계정 관리 이력 대장을 만들고 유지, 관리 한다.

제27조(정보통신망 운영관리) ① 본 대학교 내에 운영 중인 정보시스템의 비상 상황에 대비하기 위하여 정보보안담당관에 의해 이중화(라우터, 서버 이중화) 관리를 한다.
② 안정성 강화를 위하여 네트워크(내부망/외부망, 유선망/무선망)에 대한 관리를 한다.
③ 교내 네트워크를 통한 데이터를 전송할 때 암호화하여(SSL 구축) 전송하고 그 상황을 트래픽 캡처하여 관리한다.

제28조(정보시스템 운영관리) ① 시스템 정보 및 데이터에 대한 백업 및 복구 절차 정책을 관리한다.

② 시스템 정보 및 데이터에 대한 백업 및 복구를 진행하고 소산하여 관리한다.
③ 백업자료 복구에 대한 책임 할당과 모의 훈련에 대한 계획을 수립, 이행한다.
④ 주요 정보시스템(종합정보시스템, 전자결재시스템 등)은 별도의 서버에서 운영하고, 관련 데이터는 분리해서 보관한다.
⑤ 기관 내 인터넷 전화(VoIP)에 대한 실행지침(사용, 제한, 금지 등)을 수립한다.
⑥ 주요 정보시스템에 대한 접근 로그기록을 항상 저장, 점검하고 정보보안담당관의 결재를 한다.
⑦ 정보통신망, 주요 정보시스템 및 서비스에 대한 유지보수, 점검절차를 수립하고, 외부자의 경우 보안서약서 및 보안교육, 사용자 계정 신청서를 작성한다.
⑧ 정보통신망, 주요 정보시스템 및 서비스의 도입 및 개발시스템의 관련에 대한 문서관리대장을 만들고, 보안절차, 운영기록, 계약서등의 내용을 보관한다.
⑨ 본 대학교의 정보시스템의 유지, 보수를 위한 원격접속은 원칙적으로 불허하며 부득이한 경우는 위원회의 심사 후에 한시적으로 허용한다.

제29조(정보시스템 보안관리) ① 정보시스템 관리자(이하 관리자)는 서버를 도입 운용할 경우, 정보보안담당관과 협의하여 해킹에 의한 자료 절취, 위변조 등에 대비한 보안대책을 수립, 시행하여야 한다.
② 관리자는 서버 내 저장자료에 대해 업무별, 자료별 중요도에 따라 사용자의 접근권한을 차등 부여하야야 한다.
③ 관리자는 서버의 운용에 필요한 서비스 포트 외에 불필요한 서비스 포트를 제거하며 관리용 서비스와 사용자용 서비스를 분리, 운용하여야 한다.
④ 관리자는 서버 설정 정보 및 서버에 저장된 자료에 대해서는 정기적으로 백업을 실시하여 복구, 침해 행위에 대비하여야 한다.
⑤ 관리자는 데이터베이스에 대하여 사용자의 직접적인 접속을 차단하고 개인정보 등 중요정보를 암호화하는 등 데이터베이스별 보안조치를 실시하여야 한다.

제30조(외주 용역관리) ① 본 대학교내에 정보시스템을 외주 용역에 위탁하거나 개발할 때에는 계약서에 정보보안관련 사항(보안사고 책임범위, 비밀준수 의무, 위탁업무 중단 시 비상대책)을 반영한다.
② 외주 용역업체의 계약 문서는 용역사업계약서, 서비스수준협약(누출금지 대상정보) 등의 보안준수사항 및 위반 시 손해배상 내용(외부업체 보안서약서) 등을 수립하여 계약서에 첨부한다. (「교육부 정보보안 기본지침」 제26조(용역업체 보안) 참조)(개정2020.04.28)
③ 외주 용역의 계약이 만료된 경우 중요 정보자산의 유출 위험을 최소화하기 위해 보호조치 관련 절차(별도의 그룹으로 지정 접근권한 설정, 내부담당자 통제 하에 작업), 회수 내역 확인 등에 대한 내용을 수립한다.
④ 외부 장비(휴대형저장매체, 노트북PC 등)에 대한 반출입 관리(반출입 대장) 및 비밀유지 계약서, 보안교육 내역을 관리한다.
⑤ 외부자가 본 대학교 내에 정보시스템을 사용하는 경우 개발/운영 업무 수행 내역을 정기적으로 관리하고 보고서로 기록을 보관한다.
⑥ 계약 관계에 있는 제 3자 및 위탁사에 대한 정보보안 요구사항 이행여부를 일일 용역사업 보안점검 리스트를 통해 점검한다.
⑦ 계약이 만료된 후 외부 용역자에 대한 정보자산(ID카드, IP, 사용자계정, 프로젝트 데이터, 임대 노트북 등) 회수 정책을 수립한다.
⑧ 계약 만료 후 비밀유지에 대한 서약서 수취 및 보안 교육을 진행한다.

제31조(정보자산관리) ① 정보시스템 관리를 위한 정보자산 조사를 자산관리대장 현황 파악으로 정기적 수행한다.
② 정보자산 책임자 및 관리자가 교체될 경우에 정보통신망, 주요 정보시스템 및 서비스에 대한 [별지서식10]에 따른 정보시스템 관리대장을 작성하고, 이를 승인 받는다.(개정2020.04.28)
③ 정보자산의 신규 도입 시 필요한 경우, 제25조(정보보호시스템의 도입, 운용)의 내용을 따른다.(개정2020.04.28)

제32조(PC 등 단말기 보안, 관리 규정) ① PC, 노트북, PDA 등 사이버 보안 진단의 날 행사를 시행하고, 점검 결과에 대한 후속 조치를 점검한다.
② 정보보안담당관은 비인가자가 PC 등을 무단으로 조작하여 전산자료를 절취, 위변조 및 훼손시키지 못하도록 각 보안대책을 수립한다.
③ 불법 소프트웨어 사용을 차단하기 위한 점검 계획을 수립, 정기적(연간 1회 이상)으로 진행한다.
④ 본 대학교 내의 사용되는 PC 및 시스템에서 불특정 대상과의 파일 공유를 위한 P2P, 웹하드, 폴더 공유 등의 비인가 프로그램과 접속을 차단한다.
⑤ 단말기 사용자는 PC 등 단말기를 교체, 반납, 폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 관리책임자와 협의하여 하드디스크에 수록된 자료가 유출, 훼손되지 않도록 보안조치 하여야 한다.
⑥ 관리책임자는 사용자가 PC 등을 기관 외부로 반출하거나 내부로 반입할 경우에 최신 백신 등을 활용하여 해킹프로그램 및 웜바이러스 감염여부를 점검하여야 한다.
⑦ 개인소유의 PC 등 단말기를 무단 반입하여 사용해서는 안 된다. 다만, 부득이한 경우 관리책임자의 승인을 받아 사용할 수 있다.

제33조(행정실 PC사용) ① 본 대학교 행정실의 PC 사용 시 P2P, 외부 웹디스크의 사용 및 PC 간의 폴더공유를 금지한다.
② 본 대학교 행정실의 PC에는 원격제어 프로그램을 설치할 수 없으며 퇴근시 전원을 반드시 끄도록 한다.

제34조(비밀번호 갱신 주기) ① 정보시스템 접근 시에 사용되는 비밀번호는 3개월 마다 갱신하도록 하며, 전산지원팀에서 갱신주기를 필수 항목으로 설정하여 관리 한다.(개정2015.05.08)(개정2020.04.28)
② 비밀번호 관리 체계는 영문, 숫자, 특수문자 포함해서 8자리, 영문, 숫자로는 10자리 이상으로 한다.(개정2015.05.08)

제35조(이동식 저장매체 관리) ① 이동식 저장매체(USB, CD, DVD등)를 공용으로 사용하고 있는 부서의 경우 별지서식(2)의 양식에 따라 일반용, 비밀용, 공인인증서용으로 해당부서 팀장의 감독 하에 반·출입대장을 작성하여 관리 한다.
② 이동식 저장매체는 공용 외에 개인용품 사용을 금지한다.
③ 이동식 저장매체에 대한 사전승인 절차, 부서별 관리 책임자를 지정한다.
④ 이동식 저장매체는 사용자가 USB메모리를 PC 등에 연결 시 자동 실행되지 않도록 하고 최신 백신으로 악성코드 감염여부를 자동 검사하도록 보안 설정한다.
⑤ 이동식 저장매체에 대한 폐기, 재사용에 대한 절차와 보안대책 지침을 확인한다.
⑥ 이동식 저장매체에 대한 문제발생(분실, 삭제, 훼손 등)에 대한 대처방안을 확인한다.

⑦ 이동식 저장매체를 파기 등 불용처리 하거나 비밀용을 일반용 또는 다른 등급의 비밀용으로 전환하여 사용할 경우 저장되어 있는 정보의 복구가 불가능하도록 완전삭제 프로그램을 사용하여야 한다.

제36조(첨단 정보통신기기 보안관리) ① 각부서의 장은 개인휴대단말기, PDA 및 스마트폰, 전자제어장비 등 첨단 정보통신기기를 활용하여 업무자료 등 중요정보를 소통, 관리하고자 할 경우 관리대책을 수립한다.
② 정보보안담당관은 개인이 소지한 첨단 정보통신기기가 업무와 무관하더라도 업무자료 유출에 직, 간접적 악용될 소지가 있다고 판단될 경우, 반 출입 통제 등 관련 대책을 강구할 수 있다.
③ 각부서의 장은 정보통신기기를 업무에 안전하게 활용하고자 할 경우, 인증 및 암호화 기술을 적용하고 보안 요구 사항을 준수하여야 한다.

제37조(인적보호) ① 기관 구성원(내부자)에 대한 보안요구사항 공지 및 서약서 수취 등의 이력을 관리한다.
② 기관 구성원의 임용, 퇴직, 부서이동시 권한변경, 자산회수 등 통제절차를 수립한다.
③ 보안관리 규정에 경각심 고취를 위한 담당자(보안 우수자) 포상 및 징계조치 사항을 수립한다.
④ 기관 구성원의 정보보안 인식제고를 위한 연간 교육 계획을 수립하고 연간 1회 이상 집체교육을 실시한다.
⑤ 정보보안담당자의 기술 고도화를 위하여 연간 2회 이상 교육 프로그램에 참여한다.
⑥ 기관 구성원의 정보보안 인식제고를 정보보안 관련 정보, 실천 수칙 등의 홍보활동을 추진한다.
⑦ 각부서의 장은 외부 인력을 활용하여 정보시스템의 개발, 운용, 정비 등을 수행할 경우에는 해당 인력의 고의 또는 실수로 인한 정보유출이나 파괴를 방지하기 위하여 제30조 (외주 용역관리)를 참고하여 보안조치를 수행한다.

제38조(보안사고 대응체계) ① 보안사고 발생 시 신속하고 효율적인 대처를 위한 보안사고 대응 방안 절차 및 매뉴얼을 작성, 확인한다.
② 정보통신망, 주요 정보시스템 및 서비스들에 대한 모의 해킹 및 취약점 진단을 정기적(연간 1회 이상)으로 수행한다.
③ 정보보안담당관은 보안사고 대응방법 및 절차에 관한 교육을 계획에 따라 실시한다.
④ 정보통신망, 주요 정보시스템 및 서비스에 대한 부정 접근이나 정당한 접근에 대한 의심사례, 보안사고 조사과정의 지속적인 모니터링을 유지보수 업체를 통해 수행한다.
⑤ 보안사고가 일어난 경우, 이에 대한 분석과 결과(유형, 비용, 주기)보고를 이행하고 재발방지 대책을 위원회를 통해 작성한다.

제39조(재난관리) ① 본 대학교에 정보통신망, 주요 정보시스템에 대한 재난(자연재해, 기술적, 환경적 재해 등) 발생했을 경우 서비스가 중지된 경우에도 최소한의 업무를 지속 할 수 있도록 재난방지 대책을 관리한다.
② 위원회를 통해 재난 발생 시 기관 내 인원이 취해야 할 보안 절차를 수립하고, 정기적인 전직원 집체교육을 실시한다.

제40조(정보보안감사) 정보보안담당관은 연 1회 이상 자체 정보보안 감사를 실시하여야 한다.

제41조(정보보안 위규자 처리) ① 「교육부 정보보안 기본지침」 제78조(위규자 처리)에 의거하여 교내 정보보안 위규자(보안사고 위반자)가 발생한 경우, 교육부 정보보안 위규자 처리 기준을 바탕으로 정보보안심사위원회에서 위규자에 대한 처리를 진행한다.(신설2020.04.28)

부 칙

1. (시행일) 이 규정은 2012년 11월 12일부터 시행한다.

부 칙

1. (시행일) 이 규정은 2015년 02월 06일부터 시행한다.

부 칙

1. (시행일) 이 규정은 2015년 05월 08일부터 시행한다.

부 칙

1. (시행일) 이 규정은 2020년 ??월 ??일부터 시행한다.

별지서식(1) **출입대장 (장소 :)**

번호	소속	이름	일시 (부터)	일시 (까지)	출입사유	담당자 확인	팀장 확인
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							

별지서식(2) **이동매체 반·출입대장 (부서 :)**

번호	반·출입 매체 이름	사용자	일시 (부터)	일시 (까지)	사용이유	근무자 확인	팀장확인
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							

별지서식(3)　　개인정보 파기대장 (부서 :　　) (개정2020.04.28)

담당	팀장	총괄보호 책임관

번호	파기정보	파기 매체	파기대상자 (ID/이름)	파기 일시	파기 방법	파기사유	파기자 확인
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							

별지서식(4) **보안서약서 양식**

보 안 서 약 서

서약업체(단체) 대표 / 개인
소속 / 직급 :
성명 : (서명)

상기 본인은 _____ 관련 업무/사업(프로젝트)의 수행을 완료함에 있어, 아래의 보안사항에 대하여 준수 책임이 있음을 서약합니다.

1. 본인은 귀 대학에 관한 정보와 비밀유지를 대상으로 지정한 정보를 업무에 한해서만 이용하겠습니다.
2. 본인은 귀 대학으로부터 제공받은 전산장비, 자료, 서류 등 정보를 주의 깊게 사용하고 반납함으로써 무단변조, 복사, 분실 유출 등으로부터 안전하게 관리하겠습니다.
3. 본인은 회사와 무관한 불특정 다수에 대하여 회사의 비밀정보, 소유정보, 경영정보 등 중요한 사항에 대하여 무단사용하거나 누설하지 않겠습니다.
4. 본인은 근무기간 동안 지득한 비밀, 중요사실에 대하여 회사의 허가 없이 상대방과 장소여하를 불문하고 비밀을 준수할 것입니다.

상기 본인은 전술한 바와 같이, 귀 대학의 업무/사업을(를) 수행하는 기간 동안은 물론이고 업무/사업이(가) 종료된 후에도 귀 대학으로부터 지득하게 된 비밀을 허가 없이 사용하거나 누설하지 아니하고 반드시 폐기하겠습니다. 만약, 이를 위반하여 귀 대학에 손해를 야기한 경우에는 어떠한 민, 형사상 책임도 감수하며 지체 없이 배상할 것에 서약하며 본 서약서를 제출합니다.

년 월 일

한국성서대학교총장 귀하

별지서식(5) **일일 용역사업 보안점검 리스트**

일일 용역사업 보안점검 리스트

순번	점 검 항 목	확인 (○, X)
1	용역업체 사용 전산망과 기관 전산망의 분리 여부(VLAN 분리 포함)	
2	용역업체 직원 PC의 내부 정보시스템 접근 통제 여부	
3	P2P, 웹하드, 메신저 등 불필요한 인터넷 접속 차단 여부	
4	용역업체 직원에 주요 계정 비밀번호 제공 여부	
5	용역업체 직원에 비밀번호 부여시 관련사항 별도 기록 여부	
6	용역업체 직원에 시스템 관리자 계정 단독 접근 여부	
7	노트북PC 등 휴대형 정보시스템을 시스템 관리용 PC로 활용 여부	
8	용역업체 직원 등에 의한 기관 외부에서의 원격 접속・작업 여부	
9	용역업체 정보시스템 접근시 작업이력 로깅 기능 사용 여부	
10	용역업체 PC 및 휴대형 저장매체에 정보시스템 '계정명/비밀번호' 저장 여부	
11	용역업체 PC에 설치된 운영체제 및 응용프로그램 최신상태 유지 여부	
12	용역업체 PC 백신 프로그램 자동 업데이트 및 실시간 감시기능 사용 여부	
13	용역업체 PC USB・CD-RW・무선랜 등 매체 통제 여부	
14	용역업체 PC 비밀번호 및 화면보호기 설정 여부	
15	용역업체 직원의 비인가 정보통신장비(노트북 등) 휴대・반입 여부	

20 . . .

확인자 부서명 직급 성명 (인)

별지서식(6)　　노트북 및 휴대용 단말기 보안점검 리스트(신설2020.04.28.)

노트북 및 휴대용 단말기 보안점검 리스트

순번	점 검 항 목	확인 (○, X)
1	CMOS 비밀번호 및 로그온 비밀번호 설정(9자리 이상) 여부	
2	10분 이상 작업 중단시 비밀번호 등이 적용된 화면보호 조치 여부	
3	문서자료 암호화 또는 비밀번호 설정 여부	
4	사용 후 업무자료 완전 삭제(윈도우즈 휴지통 비우기 등) 여부	
5	공유 폴더 삭제 여부	
6	운영체제 및 응용프로그램 최신 보안패치 유지 여부	
7	불필요한 프로그램 설치 금지 여부	
8	백신, 내PC지킴이 등 보안관련 프로그램 설치 여부	

201 .　.　.

노트북명(제조사명, S/N표기) :

담당부서 :

확인자　부서명　　직급　　성명　　(인)

별지서식(7)　　용역업체 자료 인수인계대장 (사업명 :　　)(신설2020.04.28.)

번호	자료명	인계자	인계자 서명	인수자	인수자 서명	인계일자	인수일자	팀장 확인
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								

별지서식(8) 용역사업 이행확약서(신설2020.04.28.)

용역사업 이행확약서

서약업체(단체) 대표
소속 / 직급 :
성명 : (서명)

상기 본인은 _____ 사업(프로젝트)의 수행을 완료함에 따라, 아래의 보안사항에 대하여 준수 책임이 있음을 확약합니다.

1. 본인은 귀 대학에 관한 정보와 비밀유지를 대상으로 지정한 정보를 업무에 한해서만 이용하였습니다.
2. 본인은 귀 대학으로부터 제공받은 전산장비, 자료, 서류 등 특히, 사업 관련자료 및 사업과정에서 생산되는 모든 산출물(소스코드, 시스템구성도, 설계도, 보고서, 정보통신망 구성도, IP주소 현황 등)은 주의 깊게 사용하고 사업담당자에게 반납, 삭제 처리함으로써 무단변조, 복사, 분실 유출 등으로부터 안전하게 관리하였습니다.
3. 본인은 회사와 무관한 불특정 다수에 대하여 회사의 비밀정보, 소유정보, 경영정보 등 중요한 사항에 대하여 무단사용하거나 누설하지 않겠습니다.
4. 본인은 사업 종료 후에도 지득한 비밀, 중요사실에 대하여 회사의 허가 없이 상대방과 장소여하를 불문하고 비밀을 준수할 것입니다.

상기 본인은 전술한 바와 같이, 귀 대학의 사업이 종료된 후에도 귀 대학으로부터 지득하게 된 비밀을 허가 없이 사용하거나 누설하지 아니하고 반드시 폐기하겠습니다. 만약, 이를 위반하여 귀 대학에 손해를 야기한 경우에는 어떠한 민, 형사상 책임도 감수하며 지체 없이 배상할 것에 서약하며 본 확약서를 제출합니다.

년 월 일

한국성서대학교총장 귀하

별지서식(9) 사이버보안 진단의 날 체크리스트(신설2020.04.28.)

no	구분	점 검 항 목	결과 (○/×)
1	PC 보안 진단 실시	「사이버보안 진단의 날」행사가 월계획표에 기록되었는가?	
2		「진단의 날」행사 관련 공지를 사전에 숙지하였는가?	
3		PC진단프로그램(내PC지키미)가 PC에 설치되어 있는가?	
4	진단 결과 보완	PC진단프로그램 실행 후 파악된 취약점을 보완 조치(5~14번)하였는가?	
5		바이러스 백신 설치 및 실행 여부	
6		바이러스 백신의 최신 업데이트 여부	
7		운영체제, MS Office의 최신 보안패치 설치 여부	
8		한글프로그램의 최신 보안 패치 설치 여부 점검	
9		로그인 패스워드 안전성 여부	
10		로그인 패스워드의 분기 1회 이상 변경 여부	
11		화면보호기 설정 여부	
12		사용자 공유 폴더 차단설정 여부	
13		USB 자동 실행 허용 여부 점검	
14		미사용(3개월) ActiveX 프로그램 존재 여부 점검	
16	PC 보안 교육	업무용 PC에서 유해 프로그램 사용하고 있습니까?	
17		업무용 PC에서 P2P, 외부 웹하드 사용하고 있습니까?	
18		업무용 PC에서 불법소프트웨어를 사용하고 있습니까?	
19		업무용 PC에서 원격프로그램을 사용하고 있습니까?	

별지서식(10) 정보시스템 관리대장(신설2020.04.28.)

연번	소속	취급자 (성명)	종류 (서버, PC 등)	관리번호	도입일자	비고