[붙임2]

부경대학교 정보보안 기본지침

제정 2014. 11. 12.

제1장 총 칙

제1조(목적) 이 지침은 부경대학교의 정보보안활동에 필요한 세부사항을 규정함을 목적으로 한다.

제2조(적용범위) ① 이 지침은 부경대학교 내의 모든 부서(학과)에 적용한다.
② 이 지침에 없는 사항에 대해서는 교육부 정보보안 기본지침을 적용한다.

제3조(정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. “공공기관”이라 함은 「공공기관의 운영에 관한 법률」제4조에 의해 공공기관으로 지정된 기관을 말한다.
2. “사용자”라 함은 부경대학교 구성원으로서 정보통신망 또는 정보시스템을 사용하는 자를 말한다.
3. “정보통신망”이라 함은 전기통신기본법 제2조제2호의 규정에 의한 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, 네트워크 장치, 응용 프로그램 등 정보의 수집 · 가공 · 저장 · 검색 · 송수신에 필요한 하드웨어 및 소프트웨어를 말한다.
5. “휴대용 저장매체”라 함은 디스켓 · CD · 외장형 하드디스크 · USB 메모리 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. “전자정보”라 함은 업무와 관련하여 취급하는 전자문서 및 전자기록물을 말한다.
8. “정보통신실”이라 함은 서버 · PC 등과 스위치 · 교환기 · 라우터 등 네트워크장치 등이 설치 운용되는 장소를 말하며, 전산실 · 통신실 · 전자문서 및 전자기록물(전자정보) 보관실 등을 말한다.
9. “국가용 보안시스템”이라 함은 비밀 등 중요자료 보호를 위하여 국가정보원장이 개발하거나 안전성을 검증한 암호장비 · 보안자재 · 암호논리 등을 말한다.
10. “암호모듈”이라 함은 정보의 유출, 위 · 변조, 훼손 등을 방지하기 위해 암호논리를 활용하여 구현한 수단이나 도구를 말한다.
11. “정보보호시스템”이라 함은 정보의 수집 · 저장 · 검색 · 송신 · 수신시 정보의 유출, 위 · 변조, 훼손 등을 방지하기 위한 하드웨어 및 소프트웨어를 말한다.
12. “사이버공격”이라 함은 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스방해 등 전자적 수단에 의하여 정보통신망을 불법침입 · 교란 · 마비 · 파괴하거나 정보를 절취 · 훼손하는 공격 행위를 말한다.

제2장 정보보안 기본활동

제4조(정보보안 책임) 부경대학교 정보보안의 총괄 책임은 총장에게 있으며, 교내 각 부서(학과) 소관 정보보안에 관한 책임은 교내 각 부서(학과)의 장에게 있다.

제5조(정보보안담당관 운영) ① 부경대학교 보안업무시행규정 제3조제1항에 의거 임용된 정보통신보안담당관(이하 "정보보안담당관"이라 한다)은 부경대학교의 정보보안 업무를 총괄한다.

② 정보보안담당관의 임무는 다음과 같다.

1. 정보보안 기본계획 수립 · 시행
2. 정보보안 관련 규정 · 지침 등 제 · 개정
3. 정보보안 업무 지도 · 감독, 교육, 정보보안 감사 및 심사분석
4. 사이버위협정보 수집 · 분석 · 대응 및 보안관제
5. 정보보안 교육
6. 기타 정보보안업무 관련 사항

③ 정보보안담당관을 임면한 경우에는 7일 이내에 소속 · 직책 · 직급 · 성명 · 연락처 등을 교육부장관에게 통보하여야 한다.

제6조(활동계획 수립 및 심사분석) ① 정보보안담당관은 정보보안업무 세부 추진계획을 수립 · 시행하고 이에 대한 심사분석을 실시하거나, 총무과에서 작성하는 보안업무 추진계획에 정보보안을 포함하여 실시할 수 있다.

② 정보보안담당관은 세부 추진계획 및 심사분석을 제1호 및 제2호 서식에 따라 작성 보고하거나, 총무과에서 작성하는 보안업무 계획 및 심사분석에 포함하여 실시할 수 있다.

제7조(사용자 관리) ① 교내 각 부서(학과)에서 사용자가 보직변경, 퇴직 등 인사이동이 있을 경우 관련 정보시스템(PC · 서버 · 네트워크장비 등 포함) 접근권한을 조정하여야 한다.

② 교내 각 부서(학과)에서 외부 인력을 활용하여 정보시스템의 개발, 운용, 정비 등을 수행할 경우 해당 인력의 고의 또는 실수로 인한 정보유출이나 파괴를 방지하기 위하여 보안조치를 수행하여야 한다. 용역사업에 관한 세부 사항은 제33조(용역사업 보안관리)를 따른다.

제8조(시스템 보안책임 범위) ① 교내 각 부서(학과)에서 필요한 일체의 정보시스템(PC · 서버 · 네트워크장비 등 포함)을 도입 · 사용할 경우, 사용자 · 시스템관리자 및 관리책임자를 지정 운용하여야 한다.

제9조(정보통신시설 보안) ① 교내 각 부서(학과)에서 다음 각 호의 중요 정보통신시설 및 장소를 운영할 경우 「보안업무규정」(대통령령) 제30조에 따른 보호구역으로 설정 관리하여야 한다.

1. 주전산기실 · 정보통신실 · 통신실
2. 그 밖에 보안관리가 필요하다고 인정되는 정보시스템 설치 장소

② 교내 각 부서(학과)에서 제1항에서 지정된 보호구역에 대한 보안대책을 강구할 경우 다음 각 호 사항을 참고하여야 한다.

1. 방재대책 및 외부로부터의 위해(危害) 방지대책
2. 상시 이용하는 출입문은 한 곳으로 정하고 이중 잠금장치 설치
3. 출입자 인증 · 식별 등을 위한 출입문 보안장치 설치
4. 관리책임자 및 자료 · 장비별 취급자 지정 운용
5. 정전에 대비한 비상전원 공급, 시스템의 안정적 중단 등 전력관리 대책

제10조(지도방문) ① 정보보안담당관은 정보통신망 운용 관리에 따른 보안취약성 개선을 위하여 교내 각 부서(학과)를 지도방문을 할 수 있다.

② 교내 각 부서(학과)에서 정보통신망의 보안취약성을 개선하기 위하여 정보보안담당관에게 지도방문을 요청할 수 있다.

제11조(정보보안 감사) ① 정보보안담당관은 연1회 이상 대학 자체 정보보안 감사를 실시하거나, 대학 자체 행정감사 시 정보보안 감사를 포함하여 실시하여야 한다.

② 정보보안담당관은 정보보안감사 결과를 보안담당관을 경유하여 총장에게 보고하거나, 대학 자체 행정감사 시 정보보안 감사를 하였을 경우에는 행정감사 보고로 대체 할 수 있다.

제12조(정보보안 교육) ① 정보보안담당관은 정보보안 교육을 연1회 이상 교직원을 대상으로 실시하여야 한다.

제13조(사이버보안진단의 날) ① 부경대학교는 매월 세 번째 수요일을 '사이버보안진단의 날'로 지정·운영 한다.

② 교내 각 부서(학과)에서는 '사이버보안진단의 날'에 자체점검을 통한 보안진단을 실시하여야 하며, 그 결과를 정보보안담당관에게 제출하여야 한다.

③ 정보보안담당관은 교내 각 부서(학과)의 보안진단을 지원하기 위하여 점검도구를 제공할 수 있다.

제14조(재난방지) ① 정보시스템 관리자는 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애 발생에 대비하여 정보시스템 이원화, 백업관리, 복구 등 종합적인 재난방지 대책을 수립·시행하여야 한다.

제3장 요소별 보안관리

제15조(PC 등 단말기 보안관리) ① 단말기 사용자는 PC·노트북·PDA 등 단말기(이하 "PC 등"이라 한다) 사용과 관련한 일체의 보안관리 책임을 가진다.

② PC 등을 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손시키지 못하도록 사용자는 다음 각 호를 준수하여야 한다.

1. 장비(CMOS 비밀번호)·자료(중요문서자료 암호화 비밀번호)·사용자(로그온 비밀번호)별 비밀번호를 주기적(3개월)으로 변경 사용
2. 10분 이상 PC 작업 중단 시 비밀번호가 적용된 화면보호 조치
3. PC용 최신백신 운용·점검, 운영체제(OS) 및 응용프로그램(한컴 오피스, MS Office, Acrobat 등)의 최신 보안패치 유지
4. 업무상 불필요한 응용프로그램 설치 금지 및 공유 폴더의 삭제

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

④ 사용자는 PC 등 단말기를 기관 외부로 반출하거나 내부로 반입할 경우에 최신 백신 등을 활용하여 웜·바이러스 감염여부를 점검하여야 한다.

⑤ 사용자는 개인소유의 PC 등 단말기를 무단 반입하여 사용하여서는 아니 된다. 다만, 부득이한 경우에는 관리책임자의 승인을 받아 사용할 수 있다.

제16조(인터넷PC 보안관리) ① 인터넷과 연결된 PC 사용자는 비인가자가 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손시키지 못하도록 다음 각 호를 준수하여야 한다.

1. 메신저·P2P·웹하드 등 업무에 무관하거나 불필요한 Active-X 등 보안에 취약한 프로그램과 비인가

프로그램 · 장치의 설치 금지
2. 음란 · 도박 등 업무와 무관한 사이트 접근차단 조치

② 그 밖에 인터넷 PC의 보안관리에 관련한 사항에 대해서는 제15조(PC 등 단말기 보안관리)를 따른다.

제17조(서버 보안관리) ① 서버 관리자는 서버를 도입 · 운용할 경우, 해킹에 의한 자료 절취, 위 · 변조 등에 대비한 보안대책을 수립 · 시행하여야 한다.

② 서버 관리자는 서버의 운용에 필요한 서비스 포트 외에 불필요한 서비스 포트를 차단하여 운영한다.

③ 서버 관리자는 서버에 저장된 자료에 대해서는 정기적으로 백업을 실시하여 복구 및 침해사고에 대비하여야 한다.

④ 데이터베이스 관리자는 데이터베이스에 대하여 사용자의 직접적인 접속을 차단하고 개인정보 등 중요정보를 암호화하는 등 데이터베이스별 보안조치를 실시하여야 한다.

제18조(웹서버 등 공개서버 보안관리) ① 공개서버 관리자는 비인가자의 서버 저장자료 절취, 위 · 변조 및 분산서비스거부(DDoS) 공격 등에 대비하기 위하여 침입차단 · 탐지시스템 및 DDoS 대응시스템을 설치하는 등 보안대책을 강구하여야 한다.

② 서버 관리자는 비인가자의 공개서버 내에 비공개 정보에 대한 무단 접근을 방지하기 위하여 서버에 접근 사용자를 제한하고 불필요한 계정을 삭제하여야 한다.

③ 공개서버의 보안관리에 관련한 그 밖에 사항에 대해서는 제17조(서버 보안관리)에 따른다.

제19조(홈페이지 게시자료 보안관리) ① 홈페이지 관리자는 개인정보를 포함한 중요 업무자료가 홈페이지에 무단 게시되지 않도록 홈페이지 게시자료의 범위 · 방법 등을 명시한 자체 홈페이지 정보공개 보안지침을 수립 · 시행하여야 한다.

② 사용자는 개인정보, 비공개 공문서 및 민감 자료가 포함된 문서를 홈페이지에 공개하여서는 아니 된다.

③ 사용자는 인터넷 블로그 · 카페 · 게시판 · 개인 홈페이지 또는 소셜네트워크 서비스 등 일반에 공개된 정보통신망에 업무관련 자료를 무단 게재하여서는 아니 된다.

제20조(사용자계정 관리) ① 시스템관리자는 사용자에게 정보시스템 접속에 필요한 사용자계정(ID) 부여 시 비인가자 도용 및 정보시스템 불법 접속에 대비하여 다음 각 호의 사항을 반영하여야 한다.

1. 사용자별 또는 그룹별로 접근권한 부여
2. 외부인에게 계정 부여는 불허하되 업무상 불가피 시 교내 각 부서(학과)장 책임 하에 필요업무에 한해 특정기간 동안 접속토록 하는 등 보안조치 강구 후 허용
3. 비밀번호 등 사용자 식별 및 인증 수단이 없는 사용자계정 사용 금지

② 시스템관리자는 교직원의 퇴직 또는 보직변경 발생 시 사용하지 않는 사용자 계정을 삭제하고, 특별한 사안이 없는 한 유지보수 등을 위한 외부업체 직원에게 관리자계정 제공을 금지하여야 한다.

제21조(비밀번호 관리) ① 비밀번호는 다음 각 호 사항을 반영하여 숫자와 문자, 특수문자 등을 혼합하여 9자리 이상으로 정하고, 분기(3개월) 1회 이상 주기적으로 변경 사용하여야 한다.

1. 사용자계정(ID)과 동일하지 않은 것
2. 개인 신상 및 부서 명칭 등과 관계가 없는 것
3. 일반 사전에 등록된 단어는 사용을 피할 것
4. 동일단어 또는 숫자를 반복하여 사용하지 말 것
5. 사용된 비밀번호는 재사용하지 말 것
6. 동일 비밀번호를 여러 사람이 공유하여 사용하지 말 것
7. 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지

② 서버에 등록된 비밀번호는 암호화하여 저장하여야 한다.

제22조(네트워크장비 보안관리) ① 네트워크 관리자는 라우터, 스위치 등 네트워크장비 운용과 관련하여 다음 각 호의 보안조치를 강구해야 한다.

1. 네트워크 장비에 대한 원격접속은 원칙적으로 금지하되, 불가피할 경우 장비 관리용 목적으로 내부 특정 IP · MAC 주소에서의 접속은 허용
2. 물리적으로 안전한 장소에 설치하여 비인가자의 무단접근 통제
3. 신규 전산장비 도입시 기본(default) 계정을 삭제 또는 변경하고 관리자 계정 별도 생성
4. FTP 등 불필요한 서비스 포트 및 사용자 계정 차단・삭제

② 네트워크 관리자는 라우터 등 중요 네트워크장비의 접속기록을 6개월 이상 유지하여야 하고 비인가자에 의한 침투 여부를 주기적으로 점검하여야 한다.

제23조(전자우편 보안대책) ① 전자우편 관리자는 전자우편 시스템 일체를 보호하기 위하여 백신, 해킹메일 차단시스템을 구축하는 등 보안대책을 강구하여야 한다.

② 사용자는 상용 전자우편을 이용한 업무자료 송·수신을 금지하며 기관 전자우편으로 송·수신한 업무자료는 열람 등 활용 후 메일함에서 즉시 삭제하여야 한다.

③ 전자우편 관리자 및 사용자는 메일에 포함된 첨부파일이 자동 실행되지 않도록 설정하고 첨부파일 다운로드 시 반드시 최신백신으로 악성코드 은닉여부를 검사하여야 한다.

④ 사용자는 출처가 불분명하거나 의심되는 제목의 전자우편은 열람을 금지하고 해킹메일로 의심되는 메일 수신시에는 즉시 정보보안담당관에게 신고하여야 한다.

제24조(휴대용 저장매체 보안대책) ① 휴대용 저장매체는 비밀용, 일반용으로 구분하고 중요정보는 비밀용 USB에 저장하여 금고 속에 보관한다.

② 일반용 USB를 사용할 경우 PC 등에 연결 시 자동 실행되지 않도록 하고 최신 백신으로 악성코드 감염 여부를 자동 검사하도록 보안 설정한다.

제25조(악성코드 방지대책) ① 사용자는 웜 · 바이러스, 해킹프로그램, 스파이웨어 등 악성코드 감염을 방지하기 위하여 다음 각 호를 준수하여야 한다.

1. 사용자는 PC 등에서 작성하는 문서 · 데이터베이스 작성기 등 응용프로그램을 보안패치하고, 백신은 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.

② 사용자는 감염 PC 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 사용자는 악성코드가 신종이거나 감염피해가 심각하다고 판단할 경우에는 관련사항을 정보보안담당관에게 신속히 통보하여야 한다.

제26조(접근기록 관리) ① 시스템관리자는 정보시스템의 효율적인 통제 · 관리, 사고 발생 시 추적 등을 위하여 사용자의 정보시스템 접근기록을 유지 관리하여야 한다.

② 제1항의 접근기록에는 다음 각 호의 내용이 포함되어야 한다.

1. 접속자, 정보시스템 · 응용프로그램 등 접속 대상
2. 로그 온 · 오프, 파일 열람 · 출력 등 작업 종류, 작업 시간
3. 접속 성공 · 실패 등 작업 결과

③ 접근기록은 정보보안 사고발생 시 확인 등을 위하여 최소 6개월 이상 보관하여야 한다.

제27조(정보시스템 개발보안) ① 시스템 개발사업 담당자는 정보시스템을 자체적으로 개발하고자 하는 경우에는 다음 각 호의 사항을 고려하여 보안대책을 수립하여야 한다.

1. 독립된 개발시설을 확보하고 비인가자의 접근 통제
2. 개발시스템과 운영시스템의 물리적 분리
3. 소스코드 관리 및 소프트웨어 보안관리

② 시스템 개발사업 담당자는 외부용역 업체와 계약하여 정보시스템을 개발하고자 하는 경우에는 다음 각 호의 사항을 고려하여 보안대책을 수립하여야 한다.

1. 외부인력 대상 보안서약서 징구(제3호 및 제4호 서식) 및 보안교육
2. 외부인력의 보안준수 사항 확인 및 위반 시 배상책임의 계약서 명시
3. 외부인력의 정보시스템 접근권한 및 제공자료 보안대책
4. 외부인력에 의한 장비 반입 · 반출 및 자료 무단반출 여부 확인

제28조(정보시스템 유지보수) ① 정보시스템 유지보수 담당자는 다음 각 호에 따라 정보시스템 유지보수와 관련한 절차를 수립하여야 한다.

1. 유지보수 인력에 대해 보안서약서 집행, 보안교육 등을 포함한 유지보수 인가 절차를 마련하고 인가된 유지보수 인력만 유지보수에 참여한다.
2. 결함이 의심되거나 발생한 결함, 예방 및 유지보수에 대한 기록을 보관한다.
3. 정보시스템의 유지보수 일시, 담당자 인적사항, 정비내용 등을 기록 · 유지하여야 한다.

② 시스템관리자는 외부에서 원격으로 정보시스템을 유지보수 하는 것을 원칙적으로 금지하여야 하며 부득이한 경우에는 정보보안담당관과 협의하여 자체 보안대책을 강구한 후 한시적으로 허용할 수 있다.

제29조(전자정보 저장매체 불용처리) ① 사용자 및 시스템관리자는 하드디스크 등 전자정보 저장매체를 불용처리(교체 · 반납 · 양여 · 폐기 등) 하고자 할 경우에는 저장매체에 수록된 자료가 유출되지 않도록 보안조치 하여야 한다.

② 자료의 삭제는 해당 정보가 복구될 수 없도록 저장매체별, 자료별 차별화된 삭제방법을 적용하여야 한다.

제30조(무선랜 보안관리) ① 교내 각 부서(학과)에서 무선랜을 설치할 경우 자체 보안대책을 수립하고 제37조의 절차에 따라 보안성 검토를 받아야 한다.

② 무선랜관리자는 제1항의 보안대책 수립 시, 다음 각 호의 사항을 포함하여야 한다.

1. WPA2 이상(256비트 이상)의 암호체계를 사용하여 소통자료 암호화(국가정보원장이 승인한 암호논리 사용)
2. MAC 주소 및 IP 주소 필터링 설정
3. RADIUS(Remote Authentication Dial-In User Service) 인증 사용
4. 무선망을 통한 업무망 정보시스템 접근을 정보보호시스템 등으로 차단하는 보안 대책
5. 무선단말기 · 중계기(AP) 등 무선랜 구성요소별 분실 · 탈취 · 훼손 · 오용 등에 대비한 관리적 · 물리적 보안대책

③ 문제가 발생할 경우 정보보안담당관에게 즉시 통보하여 대책을 강구하여야 한다.

제31조(CCTV운용 보안관리) ① CCTV를 운영하는 부서(학과)에서는 CCTV운용에 필요한 카메라, 중계 · 관제서버, 관리용PC 등 관련 시스템을 비인가자의 임의 조작이 물리적으로 불가능하도록 설치하여야 한다.

② CCTV 상황실은 보호구역으로 지정 관리하고 출입통제장치를 도입하여야 한다.

제32조(정보통신망 자료 보안관리) ① 정보통신망을 운영하는 부서(학과)에서는 다음 각 호에 해당하는 정보통신망 관련 현황 · 자료 관리에 유의하여야 한다.

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

② 정보통신망을 운영하는 부서(학과)에서는 다음 각 호의 자료를 대외비로 분류하여 관리하여야 한다.

1. 정보통신망 세부 구성현황(IP 세부 할당현황 포함)
2. 국가용 보안시스템 운용 현황
3. 그 밖에 보호할 필요가 있는 정보통신망 관련 자료

제33조(용역사업 보안관리) ① 교내 각 부서(학과)에서 정보화 · 정보보호사업을 외부용역으로 추진할 경우 용역사업 담당자는 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 중요 자료는 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, 자료 무단반출 여부를 확인
7. 그 밖에 보안관리가 필요하다고 판단하는 사항

② 용역사업 담당자는「국가계약법」시행령 제76조 제1항 제18호에 따라 용역사업 추진 시 과업지시서 · 입찰공고 · 계약서에 다음 각 호의 누출금지 대상정보를 명시해야 하며 해당정보 누출 시 입찰 참가자격 제한을 위한 부정당업자로 등록(조달청에 요청)하여야 한다.

1. 부서의 소유 정보시스템의 내 · 외부 IP주소 현황
2. 세부 정보시스템 구성 현황 및 정보통신망 구성도
3. 사용자계정 · 비밀번호 등 정보시스템 접근권한 정보
4. 그 밖에 공개가 불가하다고 판단한 자료

제34조(스마트폰 등 모바일 행정업무 보안관리) ① 교내 각 부서(학과)에서 스마트폰 등을 활용하여 내부행정업무와 현장행정업무 및 대민서비스업무 등 모바일 업무환경을 구축할 경우 자체 보안대책을 수립하고 제37조의 절차에 따라 보안성 검토를 받아야 한다.

② 기타 상세한 사항은「국가 · 공공기관의 모바일 활용업무에 대한 보안가이드라인」(2014, 국가정보원)을 준수하여야 한다.

제35조(클라우드시스템 보안관리) ① 교내 각 부서(학과)에서 클라우드 컴퓨팅시스템을 구축할 경우 자체 보안대책을 수립하고 제37조의 절차에 따라 보안성 검토를 받아야 한다.

② 기타 상세한 사항은「국가 · 공공기관 클라우드 컴퓨팅 보안가이드라인」(2013.1, 국가정보원)을 준수하여야 한다.

③ 교내 각 부서(학과)에서 상용 클라우드 컴퓨팅 시스템을 활용하고자 할 경우자체 보안대책을 수립하고 제37조의 절차에 따라 보안성 검토를 받아야 한다.

제4장 안전성 확인

제36조(보안성 검토) ① 교내 각 부서(학과)에서 다음 각 호의 정보화사업을 추진할 경우 자체 보안대책을 강구하고 안전성을 확인하기 위하여 사업 계획단계에서 보안성 검토를 의뢰하여야 한다. 단 정보시스템의 단순 교체 등 사안이 경미하다고 판단되는 경우에는 이를 생략할 수 있다.

1. 비밀 업무와 관련된 정보시스템 및 네트워크 구축
2. 국가용 보안시스템을 도입 운용하고자 할 경우
3. 대규모 정보시스템 또는 다량의 개인정보를 처리하는 정보시스템 구축
4. 정보통신망의 신 · 증설, 내부 정보통신망을 인터넷이나 타 기관 전산망 등 외부망과 연동하는 경우
5. 업무망과 연결되는 대규모의 무선 네트워크 시스템 구축
6. 와이브로 · 스마트폰 등 첨단 IT기술을 업무에 활용하는 시스템 구축
7. 업무망과 인터넷 분리 사업
8. 그 밖에 보안성 검토가 필요하다고 판단하는 정보화사업

제37조(보안성 검토 절차) ① 교내 각 부서(학과)에서 보안성 검토를 의뢰하는 업무 절차는 다음과 같다.

1. 교내 각 부서(학과)에서 자체적으로 수립한 보안대책에 대하여 보안심사위원회 심의를 요청한다.
2. 보안성 검토는 서면 검토를 원칙으로 하되 필요하다고 판단하는 경우에는 현장 확인을 병행 실시할 수 있다.
3. 보안심사위원회 심의 통과 후 교육부장관에게 보안성검토를 요청한다.(다만, 정보화사업 예산 5억원 미만 또는 개인정보 5만건 미만인 정보화사업에 대해서는 보안심사위원회 심의로 갈음한다.)

제38조(제출문서) ① 교내 각 부서(학과)에서 보안성 검토를 요청할 경우에는 다음 각 호의 문서를 제출하여야 한다.

1. 사업계획서(사업목적 및 추진계획 포함)
2. 기술제안요청서(RFP)
3. 정보통신망 구성도(IP주소체계 포함)
4. 자체 보안대책 강구사항

② 제1항 제4호의 자체 보안대책 강구사항에는 다음 각 호를 포함하여야 한다.

1. 보안관리 수행체계(조직, 인원) 등 관리적 보안대책
2. 정보시스템 설치장소에 대한 보안관리 방안 등 물리적 보안대책
3. 서버, 휴대용 저장매체, 네트워크 등 정보통신망의 요소별 기술적 보안대책
4. 재난복구 계획 또는 상시 운용계획

제39조(보안적합성 검증) 교내 각 부서(학과)에서 국가용 보안시스템을 제외한 정보보호시스템, 네트워크 장비 등 보안기능이 있는 정보통신제품을 도입할 경우, 안전성 확인을 위하여 정보보안담당관의 협조를 받아 교육부장관에게 보안적합성 검증을 의뢰하여야 한다.

제40조(정보보호시스템의 도입 등) ① 교내 각 부서(학과)에서 정보 및 정보통신망 등을 보호하기 위해 정보보호시스템을 도입할 수 있다. 다만, 별표1에 규정된 유형의 시스템에 대해서는 해당 도입요건을 만족하는 경우로 한정한다.

제41조(보안적합성 검증대상)

① 보안적합성 검증대상은 다음 각 호와 같다.

1. 상용 정보보호시스템

2. 대학 자체 개발하거나 외부업체 등에 의뢰하여 개발한 정보보호시스템
3. 저장매체 소자장비 혹은 완전삭제 소프트웨어 제품
4. 네트워크 장비(L3이상 스위치라우터 등) 및 보안기능이 있는 L2 스위치

② 제1항에도 불구하고, 다음 각 호의 경우에는 검증을 생략할 수 있다.
1. 국가정보원장이 정한 국내용 CC 인증제도에 따라 인증을 받은 정보보호시스템
2. 검증필 제품목록에 등재된 저장매체 소자장비 혹은 소프트웨어 제품
3. 암호모듈 검증제도를 통해 국가정보원장이 안전성을 확인한 제품
4. 그 밖에 국가정보원장이 보안적합성 검증이 불요하다고 인정한 시스템

제42조(정보보호 수준 자가진단) ① 정보보안담당관은 교육부장관이 매년 정하는 진단 대상 · 기준, 진단항목 및 기간에 따라 자체 진단하고 그 결과를 교육부장관에게 제출하여야 한다.

제5장 사이버위협 탐지 · 대응

제43조(보안관제센터 설치 · 운영) ① 정보보안담당관은 소관 정보통신망에 대한 사이버공격 정보를 수집 · 분석 · 대응할 수 있는 보안관제센터를 설치 · 운영하거나 또는 국가 · 공공기관이 운영하는 보안관제센터에 관련 업무를 위탁할 수 있다.

제44조(정보보안 사고조사) ① 교내 각 부서(학과)에서 정보보안 사고가 발생한 때에는 즉시 피해확산 방지를 위한 조치를 취하고 다음 각 호의 사항을 정보보안담당관에게 통보하여야 한다. 이 경우, 사고원인 규명 시까지 피해 시스템에 대한 증거를 보전하고 임의로 관련 자료를 삭제하거나 포맷하여서는 아니 된다.
1. 일시 및 장소
2. 사고 원인, 피해현황 등 개요
3. 사고자 및 관계자의 인적사항
4. 조치내용 등

② 정보보안담당관은 제1항 각 호의 상황을 교육부장관 및 국가정보원장에게 통보하여야 한다.

제6장 보 칙

제45조(다른 법령과의 관계) 이 지침에 명시되지 않은 사항은 다음 각 호의 법령에 따른다.
1.「전자정부법」및 동법 시행령
2.「정보통신기반보호법」및 동법 시행령
3.「국가정보보안기본지침」 및 「교육부 정보보안기본지침」
4. 그 밖의 관계 법규

부 칙

제1조(시행일) 이 지침은 공포일부터 시행한다.

【 제1호 서식 】

정보보안업무 세부 추진계획

<작성 요령>

1. 활동 목표
2. 기본 방침
3. 세부 추진계획

분야별	사업명	세부 추진계획	주관・관련부서	비고

*** 보안성 검토 대상여부 표기**

4. 전년도 보안감사・지도방문 시 도출내용과 조치내역

도 출 내 용	조 치 내 역	담당부서

*** 형식적인 계획수립을 지양하고 자체 실정에 맞게 작성**

【 제2호 서식 】

정보보안업무 심사분석

1. 총　　평
2. 주요 성과 및 추진사항
3. 세부 사업별 실적 분석

추 진 계 획	추 진 실 적	문 제 점	개 선 대 책

*** 추진실적은 목표량과 대비하여 성과 달성도를 계량화**

4. 부진(미진)사업

부 진 사 업	원인 및 이유	익년도 추진계획

5. 애로 및 건의사항

6. 첨부(정보통신망 및 정보보호시스템 운용현황 등)

【 제3호 서식 】

보안 서약서

본인은 년 월 일부로 _____과 관련한 업무(연구개발, 제작, 입찰, 그 밖의 업무)를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 _____과 관련된 소관업무가 기밀 사항임을 인정하고 제반 보안관계규정 및 지침을 성실히 준수한다.
2. 나는 이 기밀을 누설함이 이적행위가 됨을 명심하고 재직 중은 물론 퇴직 후에도 알게 된 모든 기밀사항을 일절 타인에게 누설하지 아니한다.
3. 나는 기밀을 누설한 때에는 아래의 관계법규에 따라 엄중한 처벌을 받을 것을 서약한다.

   가. 국가보안법 제4조 제1항 제2호・제5호(국가기밀 누설 등)

   나. 형법 제99조 (일반이적) 및 제127조(공무상 비밀의 누설)

년 월 일

서약자 소속 직급 생년월일

직위 성 명 인

서 약 소속 직급 성 명 인

집행자 직위

【 제4호 서식 】

보안 서약서

본인은 ____년 __월 __일부로 _____관련 용역사업(업무)을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 _____관련 업무 중 알게 될 일체의 내용이 직무상 기밀사항임을 인정한다.

2. 본인은 이 기밀을 누설함이 국가안전보장 및 국가이익에 위해가 될 수 있음을 인식하여 업무수행 중 지득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.

3. 본인이 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다.

4. 본인은 하도급업체를 통한 사업 수행 시 하도급업체로 인해 발생하는 위반사항에 대하여 모든 책임을 부담한다.

년 월 일

서 약 자	업 체 명 :	
(업체 대표)	직 위 :	
	성 명 :	(서명)
	생 년 월 일 :	
서약집행자	소 속 :	
(담당공무원)	직 위 :	
	성 명 :	(서명)
	생 년 월 일 :	

【 별표1 】

정보보호시스템 유형별 도입요건

제품 유형	도입 요건	비 고
침입차단시스템	CC인증(EAL2이상)	
침입탐지시스템	CC인증(EAL2이상)	
침입방지시스템	CC인증(EAL2이상)	
통합보안관리서버	CC인증(EAL2이상)	
웹 응용프로그램 침입차단제품	CC인증(EAL2이상)	
DDoS 대응장비	CC인증(EAL2이상)	
가상사설망	CC인증(EAL2이상)	* 검증필암호모듈 탑재필요
서버접근통제 제품	CC인증(EAL2이상)	
DB 접근통제 제품	CC인증(EAL2이상)	
네트워크접근통제제품	CC인증(EAL2이상)	
인터넷전화 보안제품	CC인증(EAL2이상)	
무선 침입방지시스템	CC인증(EAL2이상)	
무선랜 인증제품	CC인증(EAL2이상)	
스팸메일차단제품	CC인증(EAL2이상)	
네트워크 자료유출방지제품	CC인증(EAL2이상)	
호스트 자료유출 방지제품	CC인증(EAL2이상)	* 암호화 저장기능이 존재하는 경우 검증필 암호모듈 탑재필요
안티바이러스 제품	CC인증(EAL2이상)	
PC 침입차단제품	CC인증(EAL2이상)	

제품 유형	도입 요건	비 고
패치관리시스템	CC인증(EAL2이상)	
소프트웨어 보안 USB 제품	CC인증(EAL2이상)	* 검증필암호모듈 탑재필요
매체제어제품	CC인증(EAL2이상)	
PC가상화 제품	CC인증(EAL4이상)	
서버기반 가상화 제품	CC인증(EAL2이상)	
망간 자료전송 제품	CC인증(EAL2이상)	
스마트카드	CC인증(EAL2이상)	
복합기(완전삭제모듈 탑재)	CC인증(EAL2이상)	
소스코드 보안약점 분석도구	CC인증(EAL2이상)	* '14.1.1부 의무화
스마트폰 보안관리 제품	CC인증(EAL2이상)	* '14.6.1부 의무화
메일 암호화 제품	해당사항 없음	검증필 암호모듈 탑재필요
구간 암호화 제품		
PKI 제품		
SSO 제품		
디스크·파일 암호화 제품		
문서 암호화 제품(DRM 등)		
키보드 암호화 제품		
하드웨어 보안 토큰		