정보보안관리규정

2010.04.01.제정 2011.04.18.일부개정 2012.08.01.일부개정 2014.03.01.일부개정
2016.04.28.일부개정 2018.07.01.일부개정 2021.06.01.일부개정

<정보인프라팀>

제 1 장 총 칙

제1조(목적) 이 규정은 동명대학교(이하 '본 대학교'라 한다) 정보자산을 학내 전산망을 이용하는 내·외부의 무단사용자에 의해 불법·유출·파괴·변경되는 것으로부터 안전하게 보호하며, 네트워크, 정보시스템 및 데이터베이스를 포함한 정보운영환경과 응용프로그램을 보다 안전하고 신뢰성 있게 운영하여 본 대학교 전산망 사용자에게 원활한 서비스를 제공하고자 함을 그 목적으로 한다.

제2조(적용 대상과 범위 및 의무와 책임) ① 적용 대상은 교내 전산자원을 사용하는 모든 정보시스템 및 구성원으로 한다.

② 본 대학교의 정보자산 보호와 정보운영환경 및 응용프로그램의 운영과 제공에 관하여는 따로 규정되는 경우를 제외하고는 이 규정에 따른다.

③ 정보보안에 대한 의무는 본 대학교의 전산자원을 사용하는 구성원 모두에게 있으며, 본 규정을 준수하지 않아 발생한 사고의 책임은 원칙적으로 사용자 본인에게 있다.

제3조(용어의 정의) ① "전산망"이라 함은 각종 정보시스템을 통신회선으로 연결하여 자료를 처리, 보관하거나 전송하는 조직망을 말한다.

② "정보시스템"이라 함은 PC, 노트북 PC, PDA, 서버시스템, 네트워크시스템, 정보보호시스템 등 정보통신에 이용되는 컴퓨터 기능을 보유한 모든 시스템을 말한다.

③ "시스템관리자"라 함은 각 부서에 소속되어 시스템의 슈퍼유저(administrator, root) 권한을 가지고 시스템을 운영·관리하는 자를 말한다.

④ "데이터베이스관리자"라 함은 데이터베이스를 운영·관리하는 자를 말한다.

⑤ "전산자료"라 함은 전산장비에 의해 입력·보관되어 있는 정보자료를 말하며, 백업 미디어 등 저장매체를 포함한다.

⑥ "정보자산"이라 함은 전산망을 이용하여 정보의 생성, 조회, 유지관리에 이용되는 정보시스템과 데이터베이스를 포함한 일체의 자산을 말한다.

⑦ "정보보안" 또는 "정보보호"라 함은 정보통신 수단으로 수집, 가공, 저장, 검색, 송수신 되는 정보의 유출·위변조·훼손 등을 방지하거나 정보통신망을 보호하기 위하여 관리적, 물리적, 기술적 수단을 강구하는 일체의 행위를 말한다.

⑧ "시스템실 또는 기계실"이라 함은 서버, PC 등 전산장비와 스위치·교환기·라우터 등 통신 및

전송장비 등이 설치 운용되는 장소를 말하며, 전산자료 보관실 등을 말한다.(개정 2016.4.28.)

제 2 장 위원회 및 정보보안담당부서

제4조(위원회 구성) ① 체계적·효율적인 보안정책 수립·심의 및 관리를 위하여 정보보안심사위원회(이하 '위원회'라 한다)를 둔다.

② 위원회는 위원장을 포함하여 8인 내외의 위원으로 구성한다. (개정 2016.4.28.)

③ 위원은 정보전산원장 및 기획처장, 사무처장, 정보전산원 팀장을 당연직으로 하고 그 외는 총장이 임명하는 교직원으로 구성한다. (개정 2016.4.28., 2018.07.01., 2021.6.1.)

④ 위원장은 정보전산원장으로하고, 본 대학교의 정보보안담당관이 된다. (개정 2012.8.1.)

⑤ 총장이 위촉하는 비당연직 위원의 임기는 2년으로 하되 연임할 수 있다. 당연직위원의 임기는 보직재임기간으로 한다. (개정 2016.4.28.)

제5조(위원회 기능) 이 위원회는 제1조의 목적을 달성하기 위하여 다음 각 호의 사항을 심의 결정한다. (개정 2016.4.28.)

1. 정보보안 업무 총괄 및 자문
2. 정보보안 정책 및 계획 심의, 보안장비 도입 적합성 심사
3. 정보보안사고 처리의 책임여부(중대사건) 심의
4. 정보보안교육 및 정보보안준수 사항 감사
5. 기타 정보보안관련 제반업무

제6조(정보보안담당부서) ① 정보보안업무를 체계적, 효과적으로 추진하기 위하여 정보보안전반에 대한 계획수립 및 업무를 담당하는 전담부서를 두어야하는 것을 원칙으로 하며, 전담부서가 없을시 담당부서의 업무분장 및 조직구성은 본 대학교의 사무분장규정에서 정한다. (개정 2016.4.28.)

② 정보보안담당부서는 정보보안 업무의 특수성으로 인하여 해당분야의 전문지식과 경험을 갖춘 전문가를 확보하여야 한다.

③ 정보보안담당부서는 정보보안업무 자체 보안감사(혹은 실태점검) 계획서를 작성하여 정보보안담당관의 승인을 받아야 하며, 자체보안감사 실시 후 결과를 보고하여야한다.

④ 정보보안담당부서는 사이버 침해사고에 대비하여 유관기관과의 연락처를 포함한 침해사고 대응 및 절차를 문서화하여 유지 관리하여야 한다.

제 3 장 보 안

제7조(기본 수칙) ① 정보시스템 사용자는 개인별 사용자 계정 및 패스워드의 기밀을 유지해야 하며, 본래의 발급 목적으로만 사용하여야 한다.

② 교직원 및 학생은 허가받은 정보시스템의 권한이 부여된 영역에 대하여 본래의 목적으로만

사용할 수 있다.

③ 정보시스템 사용자는 정보시스템의 성능저하 및 보안상 위험을 초래 할 수 있는 행위를 해서는 아니 된다.

④ 제3항의 규정에 언급된 행위를 한 자가 발견된 경우에는 소속부서의 장 또는 정보보안 담당부서에게 알려야 한다.

⑤ 정보 자산과 연관된 저작권. 특허권 및 소프트웨어 라이선스의 사용 조건을 숙지하고 이를 준수하여야 한다.

⑥ 학내 전산망을 신설, 변경 및 폐기하고자 하는 경우에는 정보보안담당부서의 사전승인을 얻어야 한다.

⑦ 외부 전산망에서 학내 전산망으로의 접근은 학교에서 승인한 정보시스템을 제외하고는 원칙적으로 허용하지 아니 한다. 단, 필요시 적법한 절차에 의해 요청하며, 승인된 경우 제한적으로 허용 될 수 있다.

⑧ 모든 정보자산은 정보자산 보안등급표(정보보안 기본지침)에 따라 분류, 관리한다.(개정 2016.4.28.)

⑨ 정보보안담당부서는 주기적인 보안점검을 통해 학내 전산망 및 정보시스템의 안전성을 점검하고, 정보보안정책 및 규정의 준수 여부를 평가하며 학내 모든 사용자는 이에 적극 협조하여야 한다.

⑩ 정보보안 사고를 예방하기 위한 목적으로 학교의 승인을 득한 정보보안시스템 및 정보보안 활동은 즉시 시행 할 수 있다.

⑪ 정보통신망 및 주요 정보시스템 및 서비스에 대한 원격유지보수 및 진단활동이 필요한 경우 외부자 인력현황 및 외부장비 반출입에 대한 정보보안담당관의 사전승인을 득한 후 실시하여야 하며, 해당업무내역과 사용기간이 명시된 보안서약서와 계정사용신청서를 제출 받아야 한다.

⑫ 주요 정보자산의 경우 시스템관리자는 최소 최근 3개월의 시스템 접속 및 사용 로그를 보관하여야 한다.

제8조(정보통신실 보안관리) ① 정보통신실(기계실, 통신실 등)에 대하여 다음과 같은 보호대책을 강구하여야 한다.(개정 2016.4.28.)

1. 방재대책 및 외부로부터의 위해방지대책
2. 이용하는 출입문은 가능한 한 곳으로 정하고 이중 잠금장치 또는 이중문 설치 (개정 2016.4.28.)
3. 출입문 보안장치 설치 및 주야간 감시대책
4. 보조기억매체를 보관할 수 있는 잠금장치가 달린 용기 비치(개정 2016.4.28.)
5. 보조기억매체에 대한 안전지출 계획 수립
6. 관리책임자 및 자료·장비별 취급자 지정 운용

② 정보통신실의 관리책임자는 자료보호를 위하여 다음과 같은 보안대책을 강구하여야 한다.

1. 자료별로 접근권한이 있는 자를 제한
2. 작업은 소관업무에 따라 입력·출력·열람 등으로 제한
3. 열람은 필요에 따라 기본항목·전항목 등으로 제한

제9조(보안등급 기준) ① 보안등급의 분류기준은 다음의 각 호에 따라 정한다.

1. 정보의 중요도
2. 정보(시스템)의 절취 및 불법변경 시 손실 가치
3. 정보(시스템)의 파괴 시 복구비용
4. 정보의 사용권자

② 정보자산의 보안등급 및 사용자인가는 전항의 기준에 따라 정보자산을 보유한 부서의 장이 별도로 정한다.

제10조(보안 점검) ① 정보보안담당부서는 교내 주요서버 및 각 연구실의 서버에 대해 필요시 수시 점검을 실시 할 수 있다.

② 보안점검 대상 및 분야를 해당 부서에 통보하고, 해당 부서에서는 보안점검에 필요한 자료 및 제반 요청사항을 준비하여 보안점검에 대비한다.

③ 보안점검을 실시한 후 그 결과를 위원회 위원장에게 보고한 후 해당 부서에 통보한다.

④ 해당 부서에서는 지적사항을 즉각 시정하고 그 결과를 위원회 위원장에게 보고한다.

⑤ 정보보안담당부서는 필요시 각 부서의 보안점검 지적사항에 대한 시정 여부를 확인할 수 있다.

제11조(보안사고의 처리) 보안사고가 발생할 경우 정보보안담당부서는 다음 각 호의 단계에 따라 적절한 조치를 취하여야 한다.

1. 침입자의 침입예방을 위하여 침입 가능성이 있는 부분을 수시로 점검하여 불법침입자의 침입을 사전에 예방한다.
2. 시스템관리자는 자신의 시스템에 비정상적인 활동이나 징후가 보이면 무단 침입자의 유무를 즉각 점검해야 한다.
3. 침입자가 현재 시스템에 침투해 해킹을 하고 있을 경우 필요한 조치를 즉각 취하고 보고하여야 한다.
4. 침입자를 발견하여 차단하였거나 로그파일의 분석을 통해 침입한 흔적이 발견된 경우 즉시 보고하고, 보안진단 도구나 체크리스트를 이용하여 정보자료의 이상 유무를 점검하여야 한다.

제12조(보안교육) ① 학내 의사결정자. 사용자 및 시스템 관리자를 대상으로 정보보안 교육을 실시하여 보안에 대한 인식을 제고하고 사용자와 시스템 관리자의 부주의나 고의에 의한 보안 사고를 최소화한다.

② 보안교육의 기본계획은 교육계획을 매년 수립하여야 하며, 총장 또는 정보보안담당관의 승인을 받아야 한다.

③ 보안교육은 주제별, 대상별 필요에 따라 수시/정기교육을 실시하되, 전체 구성원 대상 집체교육을 연간 2회 이상 실시하여야 하며, 교육결과를 보고한다.

④ 보안담당부서의 실무 담당자는 연간 30시간 이상의 정보보호관련 교육훈련을 이수하여야 한다.

제 4 장 정보자산의 취득 및 관리

제13조(보안성 심사) ① 모든 정보자산은 취득 시 보안성 심사를 실시하여야한다. 단, 업무의 효율성을 위하여 국가정보원 인증기준 K4등급 또는 CC인증을 받은 제품은 별도의 보안성 심사를 생략할 수 있다.

②정보자산의 보안성 심사 실시는 정보보안담당부서에서 실시하나, 주요정보자산에 대해서는 위원회의 승인을 거쳐야 하되 주요정보자산의 범위는 1등급 이상의 정보자산을 의미한다. (개정 2016.4.28.)

제14조(유지관리) 정보자산은 매년 1회 이상 현황조사를 실시하여야 하며, 실시방법 및 시기는 따로 정한다.

제15조 (폐기절차) 주요 정보자산의 폐기 시 정보의 유출방지를 위하여 1등급 이상의 정보자산은 위원회의 승인을 득하여야 한다. (개정 2016.4.28.)

제 5 장 정보시스템 관리

제16조(사용자 정의) 정보시스템을 사용할 수 있는 자는 다음 각 호와 같다.

1. 본 대학교 교원. 직원. 재학생 및 졸업생
2. 연구소 및 부속기관의 장이 사용을 인정한 자

제17조(적절성 확보) 학내 정보시스템 이용자는 정보시스템 사용에 있어 적절성을 유지하여야 한다. 다만, 다음 각 호에 해당하는 경우에는 부적절한 사용으로 간주하여 제재조치를 취할 수 있다.

1. 타 사용자의 계정 및 패스워드를 허가 없이 사용한 경우
2. 타 사용자의 정당한 사용을 방해한 경우
3. 타 사용자의 자료를 허가 없이 유출하거나 읽고 쓰는 행위
4. 일반사용자가 관리자 패스워드 또는 타 사용자의 패스워드를 획득하고자 해킹 하는 행위
5. 내부의 중요 전산정보를 불법으로 외부에 유출한 경우
6. 외부의 불법사용자에게 계정 및 패스워드를 제공한 경우
7. 사용자 계정 및 패스워드를 상호 공유하는 행위
8. 시스템관리자가 특별한 사유 없이 관리자 패스워드를 일반사용자와 공유한 경우
9. 허가된 보안등급 이상의 자료를 무단유출 하거나 읽고 쓰는 행위
10. 인터넷을 통해 자살 사이트나 음란 사이트 등 반사회적인 유해사이트에 접속. 개설. 열람하는 경우
11. 보안점검의 지적사항에 대해 즉각적인 시정을 취하지 않는 경우

제18조(사용자 제재) ① 제17조에 규정된 사항에 해당할 경우에는 사용자의 계정을 회수. 삭제하여 정보시스템의 사용을 제한 또는 금지하며, 그에 따른 구체적 제재사항은 위원회에서 심의. 결정한다.

② 정보시스템의 불법사용으로 학교에 해를 끼치거나 명예를 훼손시켰을 경우에는 다음 각 호의 제재 조치를 취할 수 있다.

1. “정보통신망 이용촉진 등에 관한 법률”(법률 제5,835호)에 의한 법적 조치
2. 학칙 제52조에 따른 징계 조치
3. 정보시스템의 손해발생에 대한 손해배상 청구

제 6 장 네트워크 관리

제19조(전산망 관리) ① 네트워크관리는 일관성과 기밀성을 위해 통합관리를 원칙으로 한다.

② 운영부서의 관리자는 네트워크 신규설치 및 변경 시 정보보안담당부서에 변경정보를 통보해야 한다.

③ 네트워크 IP ADDRESS는 사용자가 임의로 변경할 수 없다.

④ 라우터 패스워드는 제19조에 규정된 계정관리에 따른다.

⑤ 인터넷을 이용한 모든 외부로부터의 접근은 원칙적으로 방화벽을 통해서만 접근 가능하도록 한다.

⑥ 외부접속자의 시스템관리자 권한으로 로그인은 허용하지 않는다.

⑦ 일정횟수 접속실패 시 접속을 차단하고 관련 정보를 로그에 기록한다.

제20조(네트워크의 보호) ① 정보보안담당부서는 본 대학교에 유해하거나 불필요하다고 판단되는 웹사이트 접속을 통제 할 수 있다.

② 원격 사용자의 공중망 네트워크를 통한 접속은 인증 시스템 또는 방화벽에 의해 통제 할 수 있다.

③ 신뢰할 수 없는 정보시스템 및 서버로의 접속을 보호하기 위해 네트워크 정책을 설정하여 통제 할 수 있다.

④ 네트워크 보안 담당자는 의심스러운 활동에 대해서는 방화벽, 침입탐지시스템(IDS) 및 기타 보안 시스템의 로그를 분석하여 해당내용을 확인하여야 하며 필요 시 부서장에게 보고해야 한다.

⑤ 교내 네트워크 사용 시 적법한 사용자임을 인증 받아야 하며, 사용하는 정보시스템 역시 적정 무결성 수준 및 보안수준을 점검하여 본 대학교 정보보안 기대수준에 미달 시 네트워크 사용을 제한 할 수 있다.

제 7 장 서버 관리

제21조(운영 및 관리) ① 신규 임용된 교원과 직원의 계정 등록요구 시 시스템 관리자에게 사용목적. 사용기간 및 연락처 등을 제출하도록 한다.

② 휴직자의 계정은 휴직기간동안 잠정 폐쇄를 원칙으로 한다.

③ 퇴직자는 사직원 제출 시 사용자 계정을 반납하도록 한다.

④ 시스템 관리자는 최소 월 단위로 사용자의 패스워드를 체크해 취약한 패스워드가 발견 될 경우 당사자에게 통보하여 변경을 요구할 수 있다.

⑤ 취약한 패스워드를 사용한 계정에 대해서는 경고를 하되, 2회 이상의 경고를 받고도 변경하지 않을 경우에는 1개월 동안 계정을 폐쇄할 수 있다.

⑥ 시스템 개발 및 운영부서의 장은 응용프로그램 개발계획 단계에서 보안정책에 근거한 응용프로그램 개발을 지시하고, 이를 위반할 경우에는 개발을 중지시킬 수 있다.

⑦ 슈퍼유저의 권한은 정보보안업무 담당자/시스템 관리자로 제한한다.

⑧ 장애복구나 점검을 위해 루트 권한을 위임할 경우에는 시스템 관리자 입회하에 작업을 실시하고, 작업종료 후 루트계정과 패스워드를 변경한다.

⑨ 백업지침은 별도로 정하며, 반드시 지침에 따라 주기적인 백업을 실시한다.

⑩ 각 부서는 백업 미디어별로 적절한 사용연수를 정하여 노후한 백업미디어에 대해서는 사용하지 아니 한다.

⑪ 백업관리자는 정보자산의 주요데이터에 대하여 백업 계획을 수립하여 정보보안담당관의 승인을 받아야 하며, 주기적으로 데이터 백업 및 복구 테스트를 실시하고 실시결과를 보고하여야 한다.

제22조(보안관리) ① 전체 시스템에 대한 보안관리와 전반적인 방향설정 및 주기적인 보안점검은 정보보안담당부서에서 실시한다.

② 개별 서버에 대한 보안관리는 각 서버의 관리자가 담당한다.

제23조(계정관리) ① 사용자 계정 분류는 그 사용목적에 따라 분류하고 그 기준은 따로 정한다.

② 사용자별 또는 그룹별로 접근권한을 부여한다.

③ 외부 사용자의 계정은 유효기간을 설정한다.

④ 특별한 사유 없이 1학기 이상 사용하지 않는 계정은 학기 시작 일주일 이내에 말소한다.

⑤ 패스워드가 없는 계정은 사용을 금지한다.

⑥ 일정회수 접속 실패시 사용을 금지한다.

⑦ 슈퍼유저는 Console 및 특정 단말에서 만 접속을 허용한다.

⑧ 사용자 계정절차의 등록. 변경 및 폐기는 다음을 따른다.

1. 사용자 계정은 사용자 등록이나 변경 또는 폐기 신청서를 작성한 후에 시스템 관리자에게 통보하되, 외부사용자는 반드시 사용기간 및 목적 등의 사유를 명확히 해야 한다.
2. 시스템관리자는 내용을 검토한 후에 사용자 계정을 등록이나 변경 또는 폐기하고 사용자에게 그 사실을 통보한다.
3. 사용자 계정을 등록하거나 변경 또는 폐기할 경우에 일반적인 사항은 월 단위로 부서장에게 사후 보고한다. 다만, 특별한 상황이 발생할 경우에 한하여 부서장의 허가를 받은후에 작업을 실시한다.

제 8 장 전산자료 및 데이터베이스 관리

제24조(자료의 관리) ① 데이터베이스 로그인 계정 관리기준은DBMS관리자(DBA).응용 프로그램

개발자 및 사용자에 따라 권한을 차등 부여하고, 패스워드는 암호화된 형태로 존재하도록 한다.
② 데이터베이스의 무결성 유지를 위해 데이터베이스의 수정은 적법한 인가자에 의해서만 이루어져야 하며, 물리적인 재해로부터의 보호를 위해 주기적으로 백업하여야 한다.
③ 데이터베이스에 대한 모든 접근은 감사기록을 유지하되, 일반사용자의 감사기록에 대한 접근은 제한해야 한다.
④ 데이터베이스 관리자(DBA)는 누가 어떤 필드, 레코드 수준에서 접근할 수 있는가를 정의해야 한다.
⑤ DBMS는 시스템과는 별도의 사용자 인증기능을 수행해야 한다.
⑥ 데이터베이스의 데이터는 응용프로그램을 통해서만 접근한다.
⑦ 통신망을 통하여 데이터베이스의 데이터 전송 시 반드시 암호화하여야 한다.
⑧ 별도지침에 의해 중요자료로 분류된 자료 및 데이터베이스는 데이터의 접근정보를 기록하여 주기적인 점검 및 분석을 실시한다.

제25조(자료의 보관) ① 별도지침에 의해 중요자료로 분류된 자료는 별도의 보호된 장소에 보관하고, 재해 및 비상시에 대비해 소산계획을 수립하여 운영한다.
② 별도지침에 의해 중요자료로 분류된 자료의 이용 및 변경은 부서장의 허가와 관리책임자의 입회하에 이용 및 변경할 수 있다.

제26조(자료의 파기) ① 별도지침에 의해 중요자료로 분류된 자료의 파기는 자료보관책임자의 입회하에 담당자가 파기를 실시하고, 자료관리대장의 파기 확인란에 입회자는 파기 확인을 한다.
② 자기테이프 등의 자기매체 자료의 파기는 컴퓨터를 이용하여 내용을 완전히 삭제하고, 자료접근이 불가능해 내용을 지울 수 없는 자기매체의 자료는 소각 또는 용해 등의 방법으로 파기한다.
③ 소규모의 전산파지는 분쇄기를 이용하고, 대규모의 파지는 소각장에서 소각시킨다.

제 9 장 응용프로그램 관리

제27조(응용프로그램 개발) ① 모든 응용프로그램은 접근하는 데이터의 정보등급에 따라 해당 응용프로그램의 보안등급을 설정한다.
② 응용프로그램의 계획서 및 설계서는 보안관리규정에 근거하여 보안대책이 마련되어야 하며, 프로그램 개발 시에 이를 반영해야 한다.
③ 개발시 중요자료로 분류된 응용프로그램은 정보보안을 위해 사용자계정 및 패스워드를 설정해야 한다. (개정 2016.4.28.)
④ 응용프로그램에서 사용하는 사용자계정. 패스워드 및 기타 전산망 접근과 관계된 중요 정보는 소스코드로부터 분리하여 1차 인식이 불가한 암호화된 형태로 존재해야 한다.
⑤ 중요자료로 분류된 응용프로그램은 개발 시 시스템 사용에 대한 로그 정보를 관리함을 원칙으로 한다. (개정 2016.4.28.)

제28조(응용프로그램 운영) ① 응용프로그램 운영자는 응용프로그램 사용자 계정에 대한 패스워

드 변경을 최소 6개월에 1회 이상 실시해야 한다.
② 응용프로그램 운영자는 시스템 사용에 대한 로그 정보를 주기적으로 분석하여 자료의 불법 접근 및 변조에 대한 위험성을 사전에 방지해야 한다.
③ 응용프로그램의 버전관리는 소스프로그램과 실행프로그램의 버전이 일관성을 유지하도록 한다.
④ 개발된 응용프로그램의 복제는 시스템관리자의 입회하에 실시해야 한다.
⑤ 응용프로그램의 추가, 삭제 또는 변경은 부서장의 허가를 받은 후에 시스템 관리자에 의해 실시되어야 한다.
⑥ 운영 중인 시스템에는 응용프로그램의 소스프로그램을 설치하지 않는 것을 원칙으로 한다.
⑦ 중요자료로 분류된 응용프로그램은 가동전 정보보안담당부서의 보안검증을 받아야 한다. (개정 2016.4.28.)

제 10 장 PC 관리

제29조(PC의 관리) ① PC 로그인시 ID와 패스워드를 설정하여 사용하여야 한다.
② 화면 보호기를 작동시켜야 하며 패스워드를 설정한다.
③ 장시간 자리를 비울 때는 전원을 끈다.
④ 자신의 업무에 사용하는 응용 프로그램은 시스템 보안관리자의 허락 없이 무단으로 타인에게 복사해 주어서는 아니 된다.
⑤ 보조기억장치를 사용할 때 또는 데이터를 전송할 때에는 바이러스 검사를 한다.
⑥ 중요한 정보는 PC내에 보관하지 아니 하며, 별도의 보조기억장치에 담아 물리적인 보안이 철저한 위치에 보관한다.

제30조(노트북및모바일기기의 관리) ① 노크북 및 휴대용 모바일 기기의 분실로 인한 자료 유출을 방지하기 위하여 CMOS 비밀번호 및 로그인 비밀번호를 설정한다.
② 주요 문서를 보호하기 위해 문서 암호화 및 비밀번호를 설정한다.
③ 사용을 다한 기기는 반드시 업무자료를 완전삭제 한다.
[본조신설 2016.4.28.]

제31조(바이러스 예방 및 조치) ① 정보보안담당부서는 컴퓨터 바이러스, 웜 발생으로 심각한 피해가 우려되는 경우 게시판이나 메일 등을 통해 경고 메시지 게시 등의 조치를 취한다.
② 교내 전산망을 통해 전산자원을 사용하는 모든 PC는 웜, 바이러스 감염을 예방하기 위해 아래와 같이 조치해야하며, 정보보안담당부서는 필요하다고 판단될 경우 이를 강제할 수 있다.
1. 본 대학교 정보보안담당부서에서 인증한 바이러스 백신프로그램을 설치하여야 한다.
2. 설치된 바이러스 백신 프로그램을 항상 최신 버전으로 유지해야 한다.
3. 정기적인 바이러스 검색을 통해 예방과 치료에 노력해야 한다.
③ 바이러스에 의한 데이터 손상에 대비해 정기적으로 데이터 백업을 실시한다.
④ 알려진 바이러스의 경우에는 해당 바이러스를 치료할 수 있는 진단 프로그램을 구비한다.

⑤ 무단, 불법 복사된 프로그램을 설치한 정보시스템은 교내 전산망 접속을 제한한다.

⑥ 바이러스의 감염이 확인될 경우 즉각 네트워크 접속을 단절 시킨 후 바이러스 백신 프로그램으로 바이러스를 치료한다.

⑦ 외부에서 온 보조기억장치, 인터넷에서 다운로드 받은 파일, 외부로부터 전송된 메일의 첨부파일 등은 실행 또는 열기 전에 반드시 바이러스 검사를 하여야 한다.

[제30조에서 제31조로 조이동 2016.4.28.]

제 11 장 시스템실 운영관리

제32조(시스템실 시설기준) ① 출입구에 입실자를 식별 및 로깅 가능한 출입보안장치를 설치한다.

② 자동화재경보 설비를 설치하고, 할로겐 가스 등 소화 시 장비에 피해를 주지 않는 자동소화 설비를 설치한다.

③ 정전에 대비하여 별도의 전원공급 시설을 둔다.

④ 온·습도를 적절히 유지할 수 있는 항온항습기를 설치한다.

[제31조에서 제32조로 조이동 2016.4.28.]

제33조(시스템실 운영 및 관리) ① 시스템실의 운영을 담당하고 있는 부서장은 시스템실 사용 및 운영에 관한 절차 및 방법을 규정하고, 담당자들이 이를 숙지하도록 한다.

② 시스템실의 운영자는 운영일지 및 장애일지를 작성해야 한다.

③ 시스템 운영자는 주기적으로 로그화일을 분석해야 하며, 시스템에 이상이 발견 되었을 경우에는 보안사고처리 지침에 따라 즉시 조치를 취하고 이를 정보보안담당부서 및 부서장에게 보고해야 한다.

④ 시스템실에는 출입자 명부를 비치하고 비인가자의 출입을 통제해야 한다.

⑤ 시스템실, 자료보관실 및 통신실은 관리책임자를 지정하고 자료 또는 장비별로 취급자를 지정 운영해야 한다.

[제32조에서 제33조로 조이동 2016.4.28.]

제34조 (보호구역 지정) ① 시스템실 및 기계실은 보호구역으로 지정하여 운영한다

보호구역: 전산기계실(경영관315호), 초고속연구망스위칭센터(경영관313호)

② 보호구역으로 지정된 장소는 반드시 CCTV 및 이중잠금장치, 출입금지 안내판를 부착한다.

[본조신설 2016.4.28.]

제 12 장 기 타

제35조(시행세칙) 이 규정의 운용에 필요한 세부사항은 시행세칙 또는 지침서로 따로 정할 수 있다.(개정 2016.4.28.)

[제33조에서 제35조로 조이동 2016.4.28.]

제36조(준용) 기타 이 규정에 명시되지 아니한 사항은 본 대학교의 “보안업무규정”에 따른다.
[제34조에서 제36조로 조이동 2016.4.28.]

부 칙

이 규정은 2010년 4월 1일부터 시행한다.

부 칙

이 규정은 2011년 4월 18일부터 시행한다.

부 칙

이 규정은 2012년 8월 1일부터 시행한다.

부 칙

이 규정은 2014년 3월 1일부터 시행한다. 다만 제4조 제3항 개정규정은 2014년 3월 1일부터 적용한다.

부 칙

이 규정은 2016년 4월 28일부터 시행한다.

부 칙

이 규정은 2018년 7월 1일부터 시행한다.

부 칙

이 규정은 2021년 6월 1일부터 시행한다.