정보보안 관리 규정

2005. 07. 05. 최초제정
2011. 03. 01. 부분개정

제1장 총칙

제1조(목적) 이 규정은 대전보건대학(이하 '본 대학'이라 함) 정보자산이 학내 정보통신망을 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 대학 정보통신망 사용자에게 원활한 서비스를 제공하고자 함을 그 목적으로 한다.

제2조(적용 대상 및 범위) ①적용대상은 본대학 전부서(부속기관, 연구기관, 부설기관 포함)로 한다.

②본대학의 정보자산보호와 정보운영 환경 및 응용프로그램의 운영과 제공에 관하여는 따로 규정되는 경우를 제외하고는 이 규정에 따른다.

제3조(용어의 정의) ①정보통신망이라 함은 각종 정보시스템을 통신회선으로 연결하여 자료를 처리·보관하거나 전송하는 조직망을 말한다.

②정보시스템이라 함은 네트워크장비·PC·컴퓨터 서버 및 프린터 등을 말한다.

③시스템관리자라 함은 각 부서에 소속되어 시스템의 관리자(root) 권한을 가지고 시스템을 운영·관리하는 자를 말한다.

④데이터베이스 관리자라 함은 데이터베이스를 운영·관리하는 자를 말한다.

⑤전산자료라 함은 전산장비에 의해 입력·보관되어 있는 정보자료를 말하며, 백업미디어 등 저장매체를 포함한다.

⑥정보보안이라 함은 제3조 1항~5항까지 운영,활용함에 있어 정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 방법을 의미한다.

제2장 위원회

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

②위원회는 위원장을 포함하여 10인 내외의 위원으로 구성하며, 위원장은 경영기획실장(이하 '실장'이라 함)이 겸직한다.

③위원의 임명은 본교 교원 중에서 위원장의 제청으로 총장이 임명한다.

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

1. 정보보안정책 심의와 학내 정보보안 총관장
2. 정보보호정책 및 총괄 계획 심의

3. 정보보안사고 처리의 책임을 심의・결정
4. 정보보안교육 및 정보보안 준수 사항 감사
5. 기타 정보보안 관련 제반 업무의 총괄

제6조(정보보안 전담팀 구성과 역할) ①경영기획실 정보기술과(이하 '정보기술과'이라 함)에 정보보안 전담팀을 구성하여 본교에 관련된 정보보안 제반사항을 담당한다.
②어떤 상황에서도 교육과 연구에 지장이 발생하지 않도록 정보시스템을 유지, 관리한다.
③세부적인 정보보안 전담팀은 위원장이 별도로 구성할 수 있다.

제3장 보안

제7조(기본 수칙) ①정보시스템 사용자는 개인별 사용자 계정 및 비밀번호의 기밀을 유지해야 하며, 본래의 발급 목적으로만 사용하여야 한다.
②교직원 및 학생은 허가받은 정보시스템의 권한이 부여된 영역에 대하여 본래의 목적으로만 사용할 수 있다.
③정보시스템 사용자는 정보시스템의 성능저하 및 보안상 위험을 초래할 수 있는 행위를 해서는 안된다.
④제3항의 규정에 언급된 행위를 한 자가 발견된 경우에는 소속부서의 장 또는 정보에 알려야 한다.
⑤정보 자산과 연관된 저작권・특허권 및 소프트웨어 라이센스의 사용 조건을 숙지하고 이를 준수하여야 한다.
⑥학내 정보통신망을 신설・변경 및 폐기하고자 하는 경우에는 본교의 사전승인을 얻어야 한다.
⑦외부 정보통신망에서 학내정보통신망으로의 접근은 대학에서 승인한 정보시스템을 제외하고는 원칙적으로 허용하지 아니한다.
⑧모든 정보자산은 보안등급에 따라 분류・관리한다.
⑨본댁은 주기적인 보안점검을 통해 학내 정보통신망 및 정보시스템의 안전성을 점검하고, 정보보안정책 및 규정의 준수여부를 평가한다. 다만, 학내 모든 사용자는 이에 적극 협조하여야 한다.
⑩업무와 관련해 습득한 정보자산을 본교의 허가 없이 외부에 누출해서는 안 된다.
⑪정보보안 사고의 책임은 원칙적으로 사용자 본인에게 있다.

제8조(보안등급 기준) ①보안등급의 분류기준은 다음의 각 호에 따라 정한다.

1. 정보의 중요도
2. 정보(시스템)의 절취 및 불법 변경시 손실 가치
3. 정보(시스템)의 파괴시 복구비용
4. 정보의 사용권자

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

제9조(보안 점검) ①정보보안 전담팀은 교내주요서버 및 각 연구실의 서버에 대해 보안

사항 점검을 년1회 이상의 정기점검과 필요시 수시점검을 실시한다.
②보안점검 대상 및 분야를 해당부서나 학과에 통보하고, 해당 부서(학과)에서는 보안점검에 필요한 자료 및 제반요청사항을 준비하여 보안점검에 대비한다.
③보안점검을 실시한 후 그 결과를 정보실장에게 보고한 후 해당부서에 통보한다.
④해당 부서에서는 지적사항을 즉각 시정하고 그 결과를 실장에게 보고한다.
⑤정보보안 전담팀은 필요시 각부서의 보안점검 지적사항에 대한 시정 여부를 확인할 수 있다.

제10조(보안사고의 처리) 보안사고가 발생할 경우 정보보안 전담팀은 다음 각 호의 단계에 따라 적절한 조치를 취하여야 한다.

1. 침입자의 침입예방을 위하여 침입가능성이 있는 부분을 수시로 점검하여 불법침입자의 침입을 사전에 예방한다.
2. 시스템 관리자는 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 몰아냈거나 로그 파일의 분석을 통해 침입한 흔적이 발견된 경우 즉시 보고하고, 보안진단 도구나 체크리스트를 이용하여 정보자료의 이상 유무를 점검하여야 한다.

제11조(보안교육) ①학내 의사결정자·사용자 및 시스템 관리자를 대상으로 정보보안 교육을 실시한다.
②보안에 대한 인식을 제고하고 사용자와 시스템관리자의 부주의나 고의에 의한 보안사고를 최소화한다.
③보안 교육은 년 1회의 정기교육과 필요에 따라 수시 교육을 실시한다.

제4장 정보 시스템관리

제12조(사용자 정의) 정보시스템을 사용할 수 있는 자는 다음 각 호와 같다.

1. 본교 교원·직원·재학생 및 졸업생
2. 연구기관 및 부설기관의 장이 사용을 인정한 자

제13조(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 비밀번호를 허가 없이 사용한 경우
2. 타 사용자의 정당한 사용을 방해한 경우
3. 타 사용자의 자료를 허가 없이 유출하거나 읽고 쓰는 행위
4. 일반 사용자가 "root" 비밀번호 또는 타사용자의 비밀번호를 획득하고자 해킹하는 행위
5. 내부의 중요 전산정보를 불법으로 외부에 유출한 경우
6. 외부의 불법 사용자에게 계정 및 비밀번호를 제공한 경우

7. 사용자 계정 및 비밀번호를 상호 공유하는 행위
8. 시스템 관리자가 특별한 사유없이 "root" 비밀번호를 일반 사용자와 공유한 경우
9. 허가된 보안등급 이상의 자료를 무단유출하거나 읽고 쓰는 행위
10. 인터넷을 통해 자살 사이트나 음란 사이트 등 반사회적인 유해 사이트에 접속·개설·열람하는 경우
11. 보안점검의 지적 사항에 대해 즉각적인 시정을 취하지 않는 경우

제14조(사용자 제재) ①제13조에 규정된 사항에 해당할 경우에는 사용자의 계정을 회수·삭제하여 정보시스템의 사용을 제한 또는 금지하며, 그에 따른 구체적 제재 사항은 위원회에서 심의·결정한다.

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

1. "정보통신망 이용촉진 등에 관한 법률"에 의한 법적 조치
2. 개인정보보호법에 의한 법적조치
3. 규정에 따른 징계 조치
4. 정보시스템의 손해 발생에 대한 손해배상 청구

제5장 네트워크 관리

제15조(정보통신망 관리) ①네트워크 관리는 일관성과 기밀성을 위해 통합관리를 원칙으로 한다.

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

③네트워크 IP ADDRESS는 사용자가 임의로 변경할 수 없다.

④라우터 비밀번호는 제19조에 규정된 계정관리에 따른다.

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

⑥외부접속자의 "root" 로그인은 허용하지 않는다.

⑦일정횟수 접속실패 시 접속을 차단하고 관련 정보를 로그에 기록한다.

제16조(침입차단시스템 및 침입탐지시스템 관리) ①침입차단시스템 및 침입탐지시스템에는 슈퍼유저 이외의 어떤 계정도 두지 않음을 원칙으로 하고, 관리자를 제외한, 예외적인 사항에 한하여는 위원장이 결정한다.

②침입차단시스템 및 침입탐지시스템에는 침입차단과 침입탐지 기능이외에는 어떤 소프트웨어도 설치하지 않는다.

③외부에서 내부로의 모든 접속시도는 LOG 파일로 관리되어야 하며, 관리자용 컴퓨터 외에는 해당 사용자로부터의 접속시도를 차단한다.

④침입차단시스템 및 침입탐지시스템의 기록된 LOG 파일은 정보보호담당자에 의해서 정기적으로 점검되어야 한다.

⑤침입차단시스템 및 침입탐지시스템의 LOG 파일은 일주일 단위로 백업하며, 점검이

이루어진 3개월 이상의 LOG 파일은 정기적으로 삭제되어야 한다.

제6장 서버 관리

제17조(운영 및 관리) ①신규 임용된 교원과 직원의 계정 등록요구 시 시스템 관리자에게 사용목적 및 연락처 등을 제출하도록 한다.
②휴직자의 계정은 휴직기간동안 잠정 폐쇄를 원칙으로 한다.
③퇴직자의 사직원 제출 시 경영기획실 정보기술과장은 사용자 계정을 반드시 중단 및 반납하도록 한다.
④시스템 관리자는 최소 월 단위로 사용자의 비밀번호를 체크해 취약한 비밀번호가 발견될 경우 당사자에게 통보하여 변경을 요구할 수 있다.
⑤취약한 비밀번호를 사용한 계정에 대해서는 경고를 하되, 2회 이상의 경고를 받고도 변경하지 않을 경우에는 1개월 동안 계정을 폐쇄할 수 있다.
⑥시스템 개발 및 운영부서의 장은 응용 프로그램 개발계획 단계에서 보안정책에 근거한 응용 프로그램 개발을 지시하고, 이를 위반할 경우에는 개발을 중지시킬 수 있다.
⑦관리자(슈퍼 유저)의 권한은 정보보안업무 담당자/시스템관리자로 제한한다.
⑧장애복구나 점검을 위해 관리자 권한을 위임할 경우에는 시스템 관리자 입회하에 작업을 실시하고, 작업종료 후 루트계정과 비밀번호를 변경한다.
⑨백업 규정에 의거하여 반드시 규정에 따라 주기적인 백업을 실시한다.
⑩각 부서는 백업 미디어별로 적절한 사용 연수를 정하여 노후된 백업 미디어에 대해서는 사용하지 않는다.

제18조(보안관리) ①전체 시스템에 대한 보안관리와 전반적인 방향설정 및 주기적인 보안 점검은 정보보안 전담팀에서 실시한다.
②개별서버에 대한 보안관리는 각 서버의 관리자가 담당한다.

제19조(계정관리) ①사용자계정 분류는 그 사용목적에 따라 분류하고 그 기준은 따로 정한다.
②사용자별 또는 그룹 별로 접근권한을 부여한다.
③외부사용자의 계정은 유효기간을 설정한다.
④특별한 사유 없이 1학기 이상 사용하지 않는 계정은 학기 시작 일주일 이내에 말소 한다.
⑤비밀번호가 없는 계정은 사용을 금지한다.
⑥일정회수 접속 실패 시 사용을 금지한다.
⑦관리자는 콘솔 및 지정 단말기에서만 접속을 허용한다.
⑧사용자 계정절차의 등록·변경 및 폐기는 다음을 따른다.

가. 사용자 계정은 사용자등록이나 변경 또는 폐기신청서를 작성한 후에 시스템 관리자에게 통보하되, 외부사용자는 반드시 사용기간 및 목적 등의 사유를 명확히 해야 한다.

나. 시스템관리자는 내용을 검토한 후에 사용자 계정을 등록이나 변경 또는 폐기하고

사용자에게 그 사실을 통보한다.

다. 사용자 계정을 등록하거나 변경 또는 폐기할 경우에 일반적인 사항은 월 단위로 실장에게 사후 보고한다. 다만, 특별한 상황이 발생할 경우에 한하여 실장의 허가를 받은 후에 작업을 실시한다.

제7장 전산자료 및 데이터베이스 관리

제20조(자료의 관리) ①데이터베이스 로그인 계정관리기준은 데이터베이스 관리자(DBA)·응용프로그램 개발자 및 사용자에 따라 권한을 차등 부여하고, 비밀번호는 암호화된 형태로 존재하도록 한다.

②데이터베이스의 무결성 유지를 위해 데이터베이스의 수정은 적법한 인가자에 의해서만 이루어져야 하며, 물리적인 재해로부터의 보호를 위해 주기적으로 백업하여야 한다.

③데이터베이스에 대한 모든 접근은 감사기록을 유지하되, 일반사용자의 감사기록에 대한접근은 제한해야 한다.

④데이터베이스 관리자(DBA)는 누가 어떤 필드, 레코드 수준에서 접근할 수 있는가를 정의해야 한다.

⑤DBMS는 시스템과는 별도의 사용자 인증기능을 수행해야 한다.

⑥데이터베이스의 데이터는 응용프로그램을 통해서만 접근한다.

⑦별도 지침에 의해 중요자료로 분류된 자료 및 데이터베이스는 데이터의 접근정보를 기록하여 주기적인 점검 및 분석을 실시한다.

제21조(자료의 보관) ①별도 지침에 의해 중요자료로 분류된 자료는 별도의 보호된 장소에 보관하고, 재해 및 비상시에 대비해 계획을 수립하여 운영한다.

②별도 지침에 의해 중요자료로 분류된 자료의 이용 및 변경은 실장의 허가와 관리책임자의 입회하에 이용 및 변경할 수 있다.

제22조(자료의 파기) ①별도 지침에 의해 중요자료로 분류된 자료의 파기는 자료 보관 책임자의 입회하에 담당자가 파기를 실시하고, 자료관리대장의 파기 확인란에 입회자는 파기확인을 한다.

②자기 테이프 등의 자기매체 자료의 파기는 컴퓨터를 이용하여 내용을 완전히 삭제하고, 자료접근이 불가능해 내용을 지울 수 없는 자기 매체의 자료는 소각 또는 용해 등의 방법으로 파기한다.

③소규모의 전산파지는 분쇄기를 이용하고, 대규모의 파지는 소각장에서 소각시킨다.

제8장 응용 프로그램 관리

제23조(응용 프로그램 개발) ①모든 응용 프로그램은 접근하는 데이터의 정보 등급에 따라 해당 응용 프로그램의 보안등급을 설정한다.

②응용 프로그램의 계획서 및 설계서는 보안관리규정에 근거하여 보안 대책이 마련되어야 하며, 프로그램 개발 시에 이를 반영해야 한다.

③별도 지침에 의해 중요 자료로 분류된 응용 프로그램은 정보보안을 위해 사용자 계정 및 비밀번호를 설정해야 한다.
④응용 프로그램에서 사용하는 사용자 계정 · 비밀번호 및 기타 정보통신망 접근과 관계된 중요 정보는 소스코드로부터 분리하여 1차 인식이 불가한 암호화된 형태로 존재해야 한다.
⑤별도 지침에 의해 중요 자료로 분류된 응용 프로그램은 개발 시 시스템 사용에 대한 로그 정보를 관리함을 원칙으로 한다.

제24조(응용 프로그램 운영) ①응용 프로그램 운영자는 응용 프로그램 사용자 계정에 대한 비밀번호 변경을 최소 6개월에 1회 이상 실시해야 한다.
②응용 프로그램 운영자는 시스템 사용에 대한 로그 정보를 주기적으로 분석하여 자료의 불법 접근 및 변조에 대한 위험성을 사전에 방지해야 한다.
③응용 프로그램의 버전 관리는 소스 프로그램과 실행 프로그램의 버전이 일관성을 유지하도록 한다.
④개발된 응용 프로그램의 복제는 시스템관리자의 사전 양해와 입회하에 실시해야 한다.
⑤응용 프로그램의 추가·삭제 또는 변경은 실장의 허가를 받은 후에 시스템 관리자에 의해 실시되어야 한다.
⑥운영 중인 시스템에는 응용 프로그램의 소스 프로그램을 설치하지 않는 것을 원칙으로 한다.
⑦별도 지침에 의해 중요 자료로 분류된 응용 프로그램은 가동전 정보보호 전담팀의 보안검증을 받아야 한다.

제9장 PC 보안 및 관리

제25조(PC의 관리) ①PC 기동 시 CMOS에서 제공하는 비밀번호를 설정한다.
②화면보호기를 작동시켜야 하며 비밀번호를 설정한다.
③장시간 자리를 비울 때는 전원을 끈다.
④자신의 업무에 사용하는 응용 프로그램은 시스템 보안관리자의 허락 없이 무단으로 타인에게 복사해 주어서는 안 된다.
⑤디스켓이나 기타 저장매체, 웹디스크를 사용할 때 또는 데이터를 전송할 때에는 바이러스 검사를 한다.
⑥중요한 정보는 PC내에 보관하지 아니하며, 별도의 디스켓이나 기타 저장매체에 담아 물리적인 보안이 철저한 위치에 보관한다.

제26조(바이러스 예방 및 조치) ①정보보안 전담팀은 컴퓨터 바이러스 발생이 우려되는 날짜에는 미리 게시판이나 메일 등을 통해 경고 메시지 게시 등의 조치를 취한다.
②개인용 컴퓨터 사용 시 백신의 시스템 감시 기능을 사용하여, 바이러스를 진단 및 치료할 수 있도록 한다.
③바이러스에 의한 데이터 손상에 대비해 정기적으로 저장매체나 웹디스크에 데이터 백업을 실시한다.

④알려진 바이러스의 경우에는 해당 바이러스를 치료할 수 있는 진단 프로그램을 구비한다.

제10장 장비운영실의 운영・관리

제27조(장비운영실 시설 기준) ①장비운영실 출입구에는 출입보안장치를 설치한다.
②자동 화재경보 설비를 설치하고, 할로겐 가스 등 소화 시 장비에 피해를 주지 않는 자동소화 설비를 설치한다.
③정전에 대비하여 별도의 전원공급 시설을 둔다.
④온・습도를 적절히 유지할 수 있는 항온항습기를 설치한다.
제28조(장비운영실 운영 및 관리) ①장비운영실의 운영을 담당하고 있는 실장은 장비운영실 사용 및 운영에 관한 절차 및 방법을 규정하고, 담당자들이 이를 숙지하도록 한다.
②장비운영실의 서버 운영자는 운영일지 및 장애일지를 작성해야 한다.
③장비운영실 서버 운영자는 주기적으로 로그 파일을 분석해야 하며, 시스템에 이상이 발견되었을 경우에는 보안 사고처리 지침에 따라 즉시 조치를 취하고 이를 정보보안 전담팀 및 실장에게 보고해야 한다.
④장비운영실의 출입은 인가자와 비인가자로 구분하고, 인가자 명단을 작성하여 관리하여야 한다.
⑤비인가자의 장비운영실 출입 시 목적, 입실 및 퇴실시간, 인적시항 등을 장비운영실 출입관리대장에 기록하고, 동행한 출입 자격자가 확인 서명을 하여야 한다.
⑥장비운영실의 장비에 대한 관리 책임자를 지정하고 자료 또는 장비별로 취급자를 지정 운영해야 한다.

제11장 기타

제29조(규정 개정) 이 규정의 개정은 위원회의 의결을 거쳐 총장의 승인을 얻어야 한다.
제30조(시행세칙) 이규정의 운용에 필요한 세부사항은 시행세칙 또는 지침등으로 따로 정할 수 있다.
제31조(준용) 기타 이 규정에 명시되지 아니한 사항은 본교의 관계 규정에 준한다.

제12장 보칙

제32조(정보보안 지침) 이 규정의 시행에 필요한 정보보안 지침은 총장의 승인을 얻어 실장이 따로 정할 수 있다.
제33조(개인정보편람) 이 규정의 시행에 필요한 개인정보편람은 총장의 승인을 얻어 실장이 따로 정할 수 있다.
제34조(사이버 침해사고 대응메뉴얼) 이 지의 시행에 필요한 침해사고 대응메뉴얼은 총

장의 승인을 얻어 실장이 따로 정할 수 있다.

제35조(사이버 침해사고 비상연락망) 이 지의 시행에 필요한 침해사고 비상연락망은 총장의 승인을 얻어 실장이 따로 정할 수 있다.

부 칙

①(시행일) 이 제정의 규정은 공포한 날로부터 시행한다.

부 칙

①(시행일) 이 제정의 규정은 공포한 날로부터 시행한다.