	정보보안규정	제 정 일	2015. 6. 1
		개 정 일	2019. 8. 1
		개정차수	1차
		담당부서	전산정보과

제 1 장 총 칙

제 1조 (목적) 이 규정은 동서울대학교(이하 '본교'라 한다) 정보자산이 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 본교 전산망 사용자에게 원활한 서비스를 제공하고자 함을 그 목적으로 한다.

제 2조 (적용 대상과 범위 및 의무와 책임) ① 적용 대상은 교내 정보자산을 사용하는 모든 정보시스템 및 구성원으로 한다. (개정 2019. 8. 1)

② 본교의 정보자산 보호와 정보운영환경 및 응용프로그램의 운영과 제공에 관하여는 이 규정에 따른다.

③ 정보보안규정을 준수할 의무는 본교의 정보자산을 사용하는 구성원 모두에게 있으며 본 규정을 준수하지 않아 발생한 사고의 책임은 원칙적으로 사용자 본인에게 있다. (개정 2019. 8. 1)

제 2 장 조 직

제 3조 (담당관 지정) 정보보안담당관은 총장의 임명을 받은 자로서, 정보보안 업무를 총괄하며 효율적인 관리·감독을 위해 각 부서 계·과장 및 학부(과)장은 당연직으로서 분야별 담당자가 된다. (개정 2019. 8. 1)

제 4조 (담당관) 정보보안담당관의 업무는 다음 각 호와 같다.

1. 정보보안 정책 및 기본계획 수립·시행
2. 정보보안 관련 규정·지침 등 제·개정
3. 보안심사위원회에 정보보안 분야 안건 심의 주관
4. 정보보안 업무 지도·감독, 정보보안 감사 및 심사분석
5. 정보통신실, 정보통신망 및 정보자료 등의 보안관리
6. 정보보안 수준진단
7. 사이버공격 초동조치 및 대응
8. 사이버위협정보 수집·분석 및 보안관제
9. 정보보안 예산 및 전문인력 확보
10. 정보보안 사고조사 결과 처리
11. 정보보안 교육 및 정보협력
12. 주요정보통신기반시설 보호활동

13. 국가용 보안시스템 및 암호키의 운영・보안관리
14. 국가정보원장이 개발하거나 안전성을 검증한 암호모듈・정보보호시스템의 운용 및 보안관리
15. 정보통신망 보안대책의 수립・시행
16. 그 밖에 정보보안 관련 사항

[전문개정 2019. 8. 1]

제 5조 (분야별 담당자) 정보보안 분야별 담당자의 업무는 다음 각 호와 같다.

1. 정보자산의 유지보수
2. 정보자산의 보안성 검토
3. 정보자산 보안실태 관리감독 및 보안 위배사항에 관한 조치 (개정 2019. 8. 1)
4. 기타 위 각호에 부수되는 제반 사항

제 3 장 위 원 회

제 6조 (구성) ① 체계적이고 효율적인 보안정책의 수립·심의 및 관리를 위하여 정보보안위원회(이하 '위원회'라 한다)를 둔다.

② 위원회는 위원장을 포함하여 8인 내외의 위원으로 구성한다.

③ 위원장은 정보보안담당관이 되고 위원은 위원장의 제청으로 총장이 임명한다.

제 7조 (기능) 이 위원회는 제1조의 목적을 달성하기 위하여 다음 각 호의 사항을 심의·결정한다.

1. 정보보안규정 제정 및 개정
2. 정보보안업무 세부추진계획 수립
3. 정보보호 수준진단 자체평가 (신설 2019. 8. 1)
4. 기타 정보보안과 필요하다고 인정하는 사항

제 4 장 정보시스템 보안

제 8조 (사용자 정의) 정보시스템을 사용할 수 있는 자는 본교 구성원으로 정한다. (개정 2019. 8. 1)

제 9조 (접근 권한의 관리) ① 정보시스템에 대한 접근 권한은 서비스 제공에 필요한 최소한의 인원에게만 부여한다.

② 개인정보를 취급하는 담당업무에 따라 개인정보취급 권한을 부여하며, 부서별/직급별에 따라 개인정보에 대한 접근권한(읽기/쓰기/수정 및 삭제 권한)을 차등 부여한다.

③ 개인정보취급자가 전보 또는 퇴직 등 인사이동으로 변경되었을 경우 즉시 정보시스템의 접근권한을 변경 또는 말소한다.

④ 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록은 최소 2년간 보관한다.

제10조(접속 기록의 관리) ① 접속 기록의 위·변조 방지를 위해 개인정보를 처리(입/출력, 수정, DB접근 등)하는 경우에는 처리일시, 처리내역 등 접속기록을 저장한다.

② 제1항의 접속기록에 대해 위·변조 방지를 위해 별도의 저장매체에 백업하여 금고에 보관하며, 보관기간은 최소 6개월 이상으로 한다.

제11조 (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. 내부의 중요 전산정보를 불법으로 외부에 유출한 경우
2. 외부의 불법사용자에게 계정 및 패스워드를 제공한 경우
3. 정보시스템을 이용한 개인정보 침해사고(불법유출, 훼손, 갈취, 불법열람 등)가 발생한 경우

제12조 (사용자 제재) 정보시스템 사용과 관련하여 학교에 해를 끼치거나 명예를 훼손시켰을 경우에는 '정보통신망 이용촉진 및 정보보호 등에 관한법률' 등 관련 법령에 의한 법적조치를 취할 수 있다.

제12조의 2 (정보시스템 도입 및 폐기) ① 정보시스템 도입절차, 변경 관리, 재사용 및 폐기에 관한 절차를 수립하고 이행한다.

② 정보시스템은 정기적으로 모니터링하고 장애발생시 조치절차대로 이행한다.

③ 정보시스템 접근기록은 주기적으로 점검하고 시각은 표준시각으로 동기화한다.

④ 정보시스템 개발 시 시험시스템과 운영시스템은 분리하고 시험데이터는 기술적 보안조치를 한다.

⑤ 소스프로그램은 안전하게 관리하고 신규시스템 이관 방안을 마련한다.

[본조신설 2019. 8. 1]

제 5 장 네트워크 보안

제13조 (네트워크 관리) ① 각 부서는 네트워크 신규 설치 또는 변경시 그 사항을 정보보안담당관에게 통보해야 한다.

② 네트워크 IP 주소는 사용자가 임의로 변경할 수 없다.

③ IP 주소는 주기적으로 조사하며 변동에 대해서는 IP관리대장에 기록하거나 그에 상응하는 조치를 취한다.

④ 정보시스템에 대한 원격접속을 허용할 경우 다음을 준수하여야 한다.

1. 원격접속 작업자는 보안서약서를 제출해야 한다.
2. 원격접속 작업자는 정보시스템 원격접속 관리대장을 작성해야 한다.
3. 원격접속 작업자에게는 작업에 필요한 최소 권한만을 부여한다.

제14조 (네트워크의 보호) ① 본교에 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 교내 네트워크 사용 시 적법한 사용자임을 인증 받아야 하며, 사용하는 정보시스템도 적정 무결성 수준 및 보안수준을 점검하여 본교 정보보안 기대수준에 미달 시 네트워크 사용을 제한 할 수 있다.

제14조의 2 (무선네트워크 보안) ① 무선랜(와이파이 등)을 사용하여 업무자료를 소통하고자 할 경우 자체 보안대책을 수립하고 보안성 검토를 실시하여야 한다.

② 시스템관리자는 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. 관리자 페이지 MAC 주소 및 IP 주소 필터링 설정
3. RADIUS(Remote Authentication Dial-In User Service) 인증 사용
4. 무선단말기·중계기(AP) 등 무선랜 구성요소별 분실·탈취·훼손·오용 등에 대비한 관리적·물리적 보안대책
5. 그 밖에 무선랜 보안 대책 강구

[본조신설 2019. 8. 1]

제 6 장 서버 보안

제15조 (운영 및 관리) ① 시스템 관리자는 사용자의 패스워드를 검토하여 취약한 패스워드가 발견될 경우 당사자에게 통보하여 변경을 요구할 수 있다.

② 시스템 개발 및 응용프로그램 개발계획 단계에서 보안정책에 근거한 응용프로그램 개발을 지시하고, 이를 위반할 경우에는 개발을 중지시킬 수 있다.

③ 장애복구나 점검을 위해 루트 권한을 위임할 경우에는 시스템 관리자 입회하에 작업을 실시한다.

④ 정보시스템을 반입/반출 할 경우에는 용역업체 담당자에게 보안조치에 대한 서약을 받고 진행한다.

⑤ 정보시스템을 불용처리 할 경우에는 저장매체에 기록을 복구할 수 없도록 완전 삭제한다.

제 16조 (보안관리) ① 전체 시스템에 대한 보안관리와 전반적인 방향설정 및 주기적인 보안점검을 실시한다.

② 개별 서버에 대한 보안 관리는 각 서버의 관리자가 담당한다.

③ 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 정보처리시스템에 대한 접속권한을 IP 주소 등으로 제한하여 인가받지 않은 접근을 제한한다.

④ 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통해 열람권한이 없는 자에게 공개되지 않도록 정보시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 한다.

제 7 장 전산자료 및 데이터베이스 보안

제 17조 (자료의 관리) ① 데이터베이스 로그인 계정 관리기준은 DBMS관리자(DBA)·응용프로그램 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 재해로 부터의 보호를 위해 주기적으로 백업하여야 한다.

제 18조 (자료의 보관) ① 중요자료로 분류된 자료는 별도의 보호된 장소에 보관하고, 재해 및 비상시에 대비해 소산계획을 수립하여 운영한다. (개정 2019. 8. 1)

② 중요자료로 분류된 자료의 이용 및 변경은 부서장의 허가와 관리책임자의 입회하에 이용

및 변경할 수 있다. (개정 2019. 8. 1)

③ 고유식별번호 및 민감정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

제 18조의 2 (관리방안) ① 중요정보가 포함된 테이블 또는 컬럼에 대해서는 업무상 취급 권한이 있는 자만이 사용할 수 있도록 제한하여야 한다.

② DBMS 관리를 위한 계정은 데이터베이스 관리자(DBA)만이 사용할 수 있도록 하여야 한다.

③ 사용하지 않는 계정, 테스트 계정, 기본 계정 등은 삭제 또는 접근이 불가능하도록 조치하여야 한다.

④ 응용프로그램(웹 등)용으로 부여된 데이터베이스 계정의 경우 데이터베이스 관리자(DBA), 사용자 등이 공용으로 사용하지 않아야 한다.

제 8 장 PC 보안

제19조 (PC의 관리) ① PC 비밀번호는 CMOS와 운영체제에 설정한다.

② 화면 보호기를 작동시켜야 하며 패스워드를 적용한다.

③ 하드디스크 또는 이동형 저장장치는 주기적으로 바이러스 검사를 실시한다.

④ 중요한 정보는 PC내에 보관하지 아니 하며, 별도의 이동형 저장장치에 담아 물리적인 보안이 철저한 위치에 보관한다.

⑤ PC를 폐기하거나 불용시 저장매체의 데이터는 복구가 불가능하도록 삭제하거나 파손시킨다.

⑥ 노트북 또는 이동형저장매체를 사용할 경우 업무용과 개인용으로 구분하여 사용하고 업무용의 경우에는 반입/반출에 대한 관리를 철저히 한다.

⑦ PC의 보안점검 프로그램을 설치·운영하여 사전에 보안사고를 예방한다.

제20조 (바이러스 예방 및 조치) ① 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, 필요하다고 판단될 경우 이를 강제할 수 있다.

1. 본교에서 인증한 바이러스 백신프로그램을 설치하여야 한다.
2. 설치된 바이러스 백신 프로그램을 항상 최신 버전으로 유지해야 한다.
3. 정기적인 바이러스 검사를 통해 예방과 치료에 노력해야 한다.

③ 바이러스에 의한 데이터 손상에 대비해 정기적으로 데이터 백업을 실시한다.

④ 바이러스의 감염이 확인될 경우 즉각 네트워크 접속을 단절 시킨 후 바이러스 백신 프로그램으로 바이러스를 치료한다.

⑤ 외부에서 온 USB, 인터넷에서 다운로드 받은 파일, 외부로부터 전송된 메일의 첨부파일 등은 실행 또는 열기 전에 반드시 바이러스 검사를 해야만 한다.

제 9 장 기 타

제21조 (시행세칙) 이 규정의 운용에 필요한 세부사항은 시행세칙으로 따로 정할 수 있다.
제22조 (준용) 기타 이 규정에 명시되지 아니한 사항은 본교의 관계 규정에 준한다.

부 칙

1. (시행일) 이 규정은 2015년 6월 1일부터 시행한다.

부 칙

1. (시행일) 이 규정은 2019년 8월 1일부터 시행한다.