정보보안 관리규정

□ 제정 : 2011. 10. 01.
□ 개정 : 2013. 10. 01.
□ 개정 : 2016. 04. 01.
□ 개정 : 2017. 01. 01.
□ 개정 : 2017. 05. 01.

제1장 총칙

제1조(목적)
이 규정은 수원대학교(이하 ‘학교’라 한다) 정보자산이 불법 유출 · 파괴 · 변경 되는 것으로부터 안전하게 보호하며, 네트워크 및 각종 정보시스템등 정보운영 환경과 응용프로그램을 보다 안전하고 신뢰성 있게 운영하여 학교 전산망 사용자에게 원활한 서비스를 제공하고자 함을 그 목적으로 한다.

제2조(적용 대상과 범위)
이 규정은 학교 교직원, 업무위탁회사의 임직원 및 내방객 등 교내를 출입하는 모든 사람에게 적용되며, 학교가 보유하고 있는 모든 유무형의 정보자산을 대상으로 한다.

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, 정보 보호 시스템 등 정보통신에 이용되는 컴퓨터 기능을 보유한 모든 시스템을 말한다.

③ “시스템관리자”라 함은 각 부서에 소속되어 시스템의 루트(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 “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.

⑦ “시스템실“이라 함은 서버 · PC 등 전산장비와 스위치 · 교환기 · 라우터 등 통신 및 전송장비 등이 설치 운용되는 장소를 말하며, 정보전산원 서버실, 전산자료 보관실 등을 말한다.

⑧ ‘개인정보’라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명 · 주민등록번호 등의 사항에 의하여 당해 개인을 식별 할 수 있는 정보(당해 정보만으로는 특정개인을 식별 할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을

포함한다)를 말한다.

⑨ “침해사고”라 함은 해킹, 컴퓨터 바이러스, 악성코드, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등에 의하여 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태를 말한다.

제2장 정보보안 조직

제4조(정보보안조직 구성)

① 학교 내 정보보호 활동을 관리하기 위한 정보보호 조직을 구성 및 운영하며, 각 구성원은 본인에게 부여된 정보보호 책임과 역할을 성실히 이행하여야 한다.

② 정보보안을 담당하는 부서는 정보보호센터로 하며 정보보안에 관한 업무를 진행하는 정보보안담당관은 정보보호센터장으로 한다.

③ 정보보호관리자는 정보보안담당관의 업무를 보좌하며, 정보보안 전문지식을 보유한자로 정보보안담당관이 임명하여 운영할 수 있다.

④ 정보보안담당관은 주요자산을 관리·운영하는 자(이하 “시스템관리자”라 한다)를 임명하여 운영할 수 있다.

제5조(정보보안심사위원회)

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

② 위원회의 운영에 관하여 필요한 사항은 ‘정보보안 세부관리 지침’으로 정한다.

제3장 정보보안

제6조(기본 수칙)

① 정보시스템 사용자는 개인별 사용자 계정 및 패스워드의 기밀을 유지해야 하며, 본래의 발급 목적으로만 사용하여야 한다. 패스워드는 9자리 이상 영문자, 숫자, 특수문자를 혼용해야하고 다음 각 호 사항을 반영하여 쉽게 유추할 수 없는 문자순으로 구성해야함을 원칙으로 하며 분기 1회 변경해야 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 학교 교 · 직원 및 학생은 허가받은 정보시스템의 권한이 부여된 영역에 대하여 본래의 목적으로만 사용할 수 있으며 직원의 경우 보안서약서를 작성해야한다.

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 정보자산과 연관된 저작권 · 특허권 및 소프트웨어 라이선스의 사용 조건을 숙지하고 이를 준수하여야 한다. 또한 교내에서는 구매증서가 있는 합법적인 소프트웨어만 사용 할 수 있다. 또한 불법적인 소프트웨어의 사용을 방지하기 위하여 각 부서의 장은 연간 1회 이상 부서내의 시스템을 점검해야 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.

⑧ 모든 정보자산은 보안등급에 따라 분류 · 관리한다.

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

⑩ 학교 정보자산 및 업무와 관련해 습득한 정보자산을 본교의 허가 없이 외부에 유출해서는 아니 된다.

⑪ 교내 각종 민감 정보 및 주요 연구 자료의 교외이관 시 인터넷 메일과 같은 사적 E-Mail을 사용할 수 없다.

⑫ 정보보안 사고를 예방하기 위한 목적으로 학교의 승인을 득한 정보보안시스템 및 정보보안 활동은 즉시 시행 할 수 있다.

⑬ 비인가 IT기기에 대하서는 원칙적으로 사용을 금지하며, 전산장비나 휴대용 저장매체는 각 부서장의 사전승인에 의하여 사용을 하고, 사용 후 폐기 및 재사용 여부를 반드시 승인받는다.

제7조(이용자 제한조치)

① 정보보호관리자는 다음 각 호에 해당하는 행위를 한 이용자에 대하여 계정해지, 접속제한 등 정보통신서비스를 제한할 수 있다.

1. 부당한 방법으로 정보통신망에 의하여 처리·보관·전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하는 행위
2. 트로이목마, 컴퓨터바이러스 등 악성 프로그램을 유포하는 행위
3. 음란물, 폭력물 등의 불건전한 자료를 게재·유포하는 행위
4. 전자우편시스템 장애를 유발시킬 목적으로 다량의 전자우편을 전송하는 행위
5. 수신자의 명시적 수신거부 의사에 반하는 광고성 전자우편을 전송하는 행위
6. 기타 정보보호에 해가 되는 행위

② 정보보호관리자는 제1항에 의한 제한을 하고자 하는 경우에는 사전에 이를 이용자에게 고지하거나 학내 정보망에 게시하여야 한다.

제8조(이용자 고지)

① 정보보호관리자는 제7조 제1항의 각 호에 해당하는 행위가 발생하였을 때에는 그 사실을 이용자에게 고지하여야 한다. 다만, 이용자에게 경미한 영향을 미치거나 신속히 처리해야 하는 등의 긴급한 상황일 경우에는 고지하지 아니할 수 있다.

제9조(이용자 제재)

① 제7조에 규정된 사항에 해당할 경우에는 이용자의 계정을 회수·삭제하여 정보시스템의 이용을 제한 또는 금지하며, 그에 따른 구체적 제재사항은 위원회에서 심의·결정한다.

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

1. 「개인정보 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등에 의한 법적 조치
2. 학칙 따른 징계 조치
3. 정보시스템의 손해발생에 대한 손해배상 청구

제10조(이용자 구제조치)

① 정보보호관리자는 이용자의 불만사항 및 침해사고 피해발생시 처리절차 등을 홈페이지 등에 고지하여야 한다.

제4장 정보보안 교육

제11조(교직원 교육)

① 교직원의 보안역량을 강화를 위해 적절한 교육 프로그램을 개발하고, 필요한 정보보호 교육 및 홍보 계획을 매년 수립하여 시행하여야 한다.

② 정보보호 교육 담당부서는 정보보호 관련 규정의 변경이 발생한 경우 해당 교직원을 대상으로 전달교육 및 공지를 실시한다.

③ 교육내용은 최근 정보보호에 이슈화되고 있는 사항들과 교육받은 대상자들의 설문평가를 통하여 차기 교육에 반영한다.

④ 정보보안담당관, 정보보안관리자는 연간 15시간 이상 정보보안 교육(개인정보보호법 제28조 제2항의 교육 등 포함)을 이수하여야 한다

⑤ 정보보안담당관은 정보보안 관련 전문기관 교육 및 기술 세미나 참석을 장려하는 등 정보보호관리자, 시스템관리자 등 정보보안 담당자의 업무 전문성을 제고하기 위하여 노력하여야 한다.

⑥ 정보보안담당관은 필요한 경우 정보보안 교육을 외부의 정보보안 관련 전문교육기관에 위탁할 수 있다.

제12조(위탁업체 교육)

① 위탁업체 임직원에 대하여 계약서 상의 보안요구사항과 학교의 보안규정, 지침, 절차의 준수 및 보안책임을 주지시기 위해 필요한 교육을 실시한다.

제5장 인원보안

제13조(교직원 보안)

① 모든 교직원은 입사 시 정보보호서약서를 제출하여야 하며, 업무 상 취득한 학교 또는 제3자 소유의 정보를 학교의 사전승인 없이 누설해서는 아니된다.

② 정보보안와 관련된 교직원은 본 규정, 지침, 절차서를 준수하며 해당 담당 업무에 적용한다.

③ 정보보안담당관는 본 규정, 지침, 절차서를 정보보호 활동에 필요한 교직원에게 전달하여 정보보호관리체계가 원활히 이루어지도록 한다.

④ 담당 업무의 변경 및 퇴직 시에는 해당 교직원의 물리적·기술적 접근권한을 즉시 변경한다.

⑤ 정보보안담당관은 교직원에게 정보보호 및 보안에 대한 서약서를 징구할 수 있으며 필요한 경우 관련부서에 징구를 위임할 수 있다.

⑥ 직무변경 및 정보자산 회수 등 세부사항에 대하여 '정보보안 세부관리 지침'을 따른다.

제14조(외주인력 보안)

① 위탁업체와 계약을 체결하고자 할 경우, 위탁업체의 임직원이 준수해야 할 보안 요구사항과 위반 시 책임을 부과하는 사항을 계약서에 명시하고 보안서약서를 징구 한다.

② 위탁업체 인력의 투입 및 수행, 종료 시 보안관리를 위한 세부사항은 '정보보안 세부관리 지침'을 따른다.

제6장 물리적 보안

제15조(보호구역 접근통제)

① 학교 정보자산의 중요도와 고유특성에 적합한 보호를 위하여 보호구역을 별도로 구분·지정하여 관리하고, 인가 받은 사용자만이 출입할 수 있도록 제한한다.

② 보호구역은 비인가된 접근이나 손상을 방지하기 위하여 별도의 출입통제 장치 및 감시시설, 재해방지시설 등을 갖추워야 한다.

③ 비자격자의 보호구역 출입이 필요할 경우 출입은 반드시 자격자와 동행하여 비자격자의 작업을 종료 시까지 감시하며, 장비의 반출입은 통제 및 관리되어야 한다.

제16조(전산실 운영)

① 전산실은 보호구역으로 지정하여 출입을 통제하고 인가된 출입자에 대한 '전산실 출입대장' 기록 관리해야 한다.

제7장 보안사고 관리

제17조(침해사고 대응)

① 학교의 업무 활동을 방해하는 침해사고가 발생했을 때 이에 대한 효율적인 처리 및 복구를 위한 대응체계를 갖추어 피해를 최소화하고, 업무수행 및 서비스 제공의 연속성을 확보하여야 한다.

② 침해사고 대응은 '사이버위기대응 매뉴얼'을 따른다.

제18조(보안사고 방지)

① 보안에 영향을 줄 수 있는 다양한 취약점에 대해 적시에 보고하고 신속하게 교정 조치가 취해질 수 있도록 한다.

제8장 사이버보안진단의 날

제19조(사이버보안진단의 날)

① 정보보안담당관은 ‘사이버보안진단의 날’에 소관 정보보안업무 전반에 대하여 체계적이고 종합적인 보안진단을 실시하여야 한다.

② 이용자는 매월 세 번째 수요일에 실시하는 사이버보안진단의 날 시행에 협조해야 한다.

③ 이용자는 지정된 정보보호 소프트웨어를 사용하여 사이버 보안진단을 수행해야 하며, 그 결과를 정보보안담당관에게 통보하여야 한다.

④ 사이버 보안진단을 수행하지 않는 이용자의 전산망 접속을 제한할 수 있다.

제9장 시스템 운영 및 관리

제20조(직무 분리)

① 정보자산과 서비스에 대한 비인가된 변조 또는 남용의 발생 가능성을 줄이기 위하여 시스템 운영과 정보보호 활동 직무는 분리하도록 한다.

② 중요한 시스템 및 프로세스에 대한 직무는 분리하도록 한다.

③ 정보시스템에 대한 사용자의 접근권한은 연1회 이상 정기적으로 검토되어야 한다.

제21조(서버 보안)

① 서버를 도입·운용할 경우, 해킹에 의한 정보 유출 및 위·변조 등에 대비한 보안대책을 수립한다.

② 바이러스를 진단·치료할 수 있는 백신프로그램을 설치하여 운영해야 한다.

③ 주관 부서장은 서버시스템 운영관리, 로그관리, 유지보수 등 세부사항에 대해 별도로 마련한다.

제22조(네트워크 보안)

① 비인가자의 불법적인 접근 및 서비스 중지 등을 예방하기 위해 불필요한 서비스 포트 제거, 보안시스템 우회차단 등의 보안조치를 한다.

② 주관부서장은 네트워크시스템 접근통제, 로그관리, 운영관리 등 세부사항에 대해 별도로 마련한다.

제23조(데이터베이스 보안)

① 사용자의 직접적인 접속을 차단하고, 개인정보 등 중요정보를 암호화하는 등 보안조치를 실시한다.

② DBMS 접근권한은 업무 권한에 따라 사용자 그룹 또는 개별 사용자 단위로 부여하고, 사용자의 업무별로 접근권한을 통제한다.

③ 주관부서장은 데이터베이스 접근통제, 로그관리, 운영관리 등 세부사항에 대해 별도로 마련한다.

제24조(일반에게 공개된 시스템)

① 일반인에게 공개되는 전자적인 정보에 대한 무결성 확보 방안이 적용되어야 한다.

② 일반인에게 공개되는 전사적 형태의 정보(회사 홈페이지 등에 수록된 정보)는 관련 법

규에 준하여 보호하여야 한다.

③ 정보를 일반인에게 공개할 경우 정보보호관리자의 승인을 득한 후 공개하여야 한다.

④ 민감한 정보의 경우 정보 수집 및 전송 시 또는 저장 시에도 보호되어야 한다.

제10장 시스템 개발 보안

제25조(응용시스템 설계 및 개발 보안)

① 중요 응용프로그램의 신규 개발 또는 변경을 위한 업무 요구사항 내에 보안 통제 사항을 포함한다.

② 응용프로그램의 설계 및 개발 시, 다음 각 호의 사항을 고려하여 보안대착을 수립한다.

1. 화면 및 메뉴 별로 접근 권한을 통제한다.
2. 응용프로그램을 테스트할 때는 임의의 테스트 데이터를 생성하여 활용하고, 실제 운영 데이터의 사용을 금지한다.
3. 독립된 개발시설을 확보하고 비인가자의 접근을 통제한다.
4. 개발시스템과 운영시스템을 물리적으로 분리한다.
5. 소스코드 및 소프트웨어를 보안관리 한다.

③ 외부용역 업체와 계약하여 정보시스템을 개발하고자 하는 경우에는 다음 각 호의 사항을 고려하여 보안대책을 수립하고 시스템 개발사업 관리책임자의 검토를 받아야 한다.

1. 외부인력 대상 신원확인, 보안서약서 징구, 보안교육 및 점검
2. 외부인력의 보안준수 사항 확인 및 위반 시 백상책임의 계약서 명시

④ 정보보안담당관은 제2항 및 제3항과 관련하여 보안대책의 적절성을 수시로 점검하고 정보시스템 개발을 완료한 경우에는 정보보안 요구사항을 충족하는지 시험 및 평가를 수행하여야 한다.

제26조(암호 적용 및 관리)

① 정보보안담당관은 정보자산의 형태, 등급 및 관련 법령에서 요구하는 사항을 고려하여 정보자산 보호에 적합한 방법으로 암호화 기술을 적용해야한다.

② 암호화 기술의 안전한 관리 및 운영을 위하여 '암호화 기술 승인절차(이용・변경포함)', '예외사항 및 오류 발생시 조치절차 및 내용' 등을 기록하고 비인가자의 접근을 통제 한다.

제11장 보안 점검

제27조(보안 점검)

① 정보보안담당부서는 교내 주요서버 및 각 연구실의 서버에 대해 필요시 수시 점검을 실시 할 수 있으며 다음 각 호의 단계를 따른다.

1. 보안점검 대상 및 분야를 해당 부서에 통보한다.
2. 해당 부서에서는 보안점검에 필요한 자료 및 제반 요청사항을 준비하여 보안점검에 대비 한다.
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.

② 홈페이지 침해사고 및 개인정보노출사고 등을 예방 및 대처하기 위해 다음 각 호에 따라 정보보안 담당부서는 보안점검을 실시 또는 요구할 수 있다.

1. 보안점검 대상은 본교 모든 홈페이지로 한다.

2. 보안점검은 홈페이지를 구축 할 때와 점검사유가 발생할 때 실시한다.

3. 보안점검은 원칙적으로 정보보안담당부서에서 시행하나, 사전 협의된 경우 구축·관리 주최에서 자체적으로 보안점검을 진행하고, 그 점검결과를 정보보안담당부서에 통보할 수 있다.

4. 위 ①항에 따라 보안점검을 실시한다.

제12장 기 타

제28조(시행세칙) 이 규정의 운용에 필요한 세부사항은 시행세칙으로 따로 정할 수 있다.

제29조(준용) 기타 이 규정에 명시되지 아니한 사항은 학교의 관계 규정 및 교육부 정보보안 기본지침에 준한다. 교육부 정보보안 기본지침 개정시 교육부 규정을 우선 준용한다.

부 칙

이 규정은 2011년 10월 1일부터 시행 한다.

이 규정은 2013년 10월 1일부터 시행 한다.

이 규정은 2016년 4월 1일부터 시행 한다.

이 규정은 2017년 1월 1일부터 시행 한다.

이 규정은 2017년 5월 1일부터 시행 한다.