목 차

작성부서	정보전산센터	제정일자	2018. 05. 04.

구 분	작 성	검 토				승 인
직 책	담 당	정보전산센터장	기획처장			총 장
서 명						
일 자						

개정이력		
개정 번호	개정일자	개정내용
1	2018. 05. 04.	정보보호 규정 제정

제1장 총칙

제1조(목적) 이 규정은 동원대학교(이하 “이 대학교”라 한다)의 정보통신서비스 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치 등에 관한 구체적 내용을 정하는 것을 목적으로 한다.

제2조(정의) 이 규정에서 사용하는 용어의 뜻은 다음과 같다.

1. “정보통신서비스”란 정보통신설비(정보통신서비스를 제공하기 위한 기계, 기구, 선로 등의 설비) 및 시설(정보통신설비가 집적되어 있는 시설 및 부대시설)을 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다.
2. “주요자산”이란 정보통신설비 중 라우터, 스위치, 웹서버, DNS, DB서버, 컴퓨터, 무선AP 등의 H/W 및 S/W를 포함한 정보통신서비스 제공에 중대한 영향을 미치는 설비를 말한다.
3. “정보통신서비스제공자”란 정보통신설비 및 시설을 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.
4. “이용자”란 정보통신서비스제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
5. “침해사고”란 해킹 및 컴퓨터바이러스의 유포 등으로 인하여 정보시스템의 정상적인 운영에 대한 방해, 정보의 유출, 파괴, 위조 및 변조 등이 발생한 사태를 말한다.

제3조(정보보호조직의 구성 및 역할) ① 정보보호를 위한 조직으로 정보보안담당관, 정보보안담당자, 시스템 관리자를 둘 수 있다.

② 정보보안담당관은 정보보호와 관련한 제반 업무를 총괄하는 자로 정보보안담당자 및 시스템관리자의 업무를 관리·감독하며 정보전산센터장이 당연 겸직한다.

③ 정보보안담당자는 주요자산의 정보보안을 총괄 관리한다.

④ 시스템관리자는 주요자산을 관리, 운영한다.

제4조(정보보안심사위원회) ① 체계적이고 효율적인 보안정책 수립, 심의 및 관리를 위하여 정보보안심사위원회(이하 “위원회”라 한다)를 둔다.

② 위원회 조직은 다음 각 호와 같다

1. 위원회는 위원장 1인을 포함한 위원 5인 이내로 구성한다.
2. 위원장은 정보전산센터장을 당연직으로 하며 관련 업무를 총괄한다.
3. 위원은 내부인원 중에서 총장이 임명하며 필요한 경우 외부인을 포함 할 수 있다.
4. 위원회의 원활한 사무처리를 위하여 간사 1명을 둔다.

③ 위원회는 다음 각 호의 사항을 심의·의결한다.

1. 보안내규의 수립 및 그 개정에 관한 사항
2. 분야별 보안대책의 수립에 관한 사항
3. 보안위반자 심사 및 처리에 관한 사항
4. 연간 보안업무 지침수립 및 그 이행 상태의 확인 처리에 관한 사항

5. 보안업무 심사분석 및 보안업무 수행 상 조정과 협의를 요하는 사항
6. 각 부서로부터 제청된 각종 보안사항
7. 기타 위원장이 보안상 필요하다고 인정하는 사항

④ 위원장은 위원회의 회의를 소집하고 그 의장이 되며, 위원장이 사고가 있을 때에는 위원 중에서 위원장이 지정한 자가 그 직무를 대행한다.

⑤ 위원회는 총장의 요청이 있을 때 또는 기타 위원장이 필요하다고 인정할 때 소집 할 수 있다.

⑥ 위원회의 소집이 곤란하거나 긴급을 요할 때에는 서면 결의로 대체 할 수 있다.

⑦ 위원회의 의사는 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 결정하며 가부동수인 경우에는 위원장이 결정한다.

⑧ 위원회는 회의록을 작성하여 총장에게 보고한다.

제2장 정보보안담당관

제5조(내부방침의 수립 및 시행) ① 정보보안담당관은 이 대학교의 정보통신서비스의 안정성과 정보의 신뢰성을 확보하는데 필요한 정보보호조치를 내용으로 하는 정보보호내부지침(이하 “내부지침”이라 한다)을 다음과 같이 수립·시행하여야 한다.

1. 개인정보처리방침
2. 네트워크 보안지침
3. PC 및 바이러스 보안지침
4. E-mail 관리 및 보안지침
5. 데이터베이스 보안지침
6. 응용프로그램 보안지침
7. 침입탐지 및 차단 보안지침
8. 백업 및 복구처리 지침
9. 침해사고 대응지침

② 제1항의 내부지침을 년 1회 이상 검토 및 보완하여야 한다.

제6조(침해사고 대응관리) ① 긴급한 침해사고 발생 시 모든 이용자에게 대응책을 신속하게 알릴 수 있는 체계를 마련하여야 한다.

② 불법행위나 이상 징후가 탐지되었을 때에는 제13조 제1항의 규정에 의하여 수립된 대응·복구계획에 따라 즉각적인 대응조치를 취하고, 침해사고와 관련한 접속기록 등 적절한 증거자료를 수집·보관하여야 한다.

제7조(정보보호 교육) ① 정보보안담당관은 자체 정보보안교육계획을 수립하여 연 1회 이상 전 직원을 대상으로 관련 교육을 실시하여야 한다. 다만, 정보보안담당자는 연간 15시간 이상 정보보안교육(개인정보보호법 제28조 제2항의 교육 등 포함)을 이수하여야 한다.

② 제1항의 규정에 의한 교육을 실시할 때 외부의 정보보호관련 전문기관에게 이를 위탁할 수 있다.
③ 정보보안담당관은 정보보안 관련 전문기관 교육 및 기술 세미나 참석을 장려하는 등 정보보안 담당자의 업무 전문성을 제고하기 위하여 노력하여야 한다.

제8조(인적보안) ① 교·직원의 전보 또는 퇴직 발령 시 인사 대상자에 대한 계정 및 공용계정에 대한 접근 권한을 즉시 제거한다.
② 아웃소싱으로 인한 제3자의 인력 활용 시 정보보호 서약서를 수령하여 보관하게 한다.
③ 정보통신설비 및 시설의 관리 운영을 외부에 위탁할 때에는 계약서에 정보보안관련 사항(보안사고 책임범위, 비밀준수 의무, 위탁업무 중단시 비상대책)을 반영한다.

제9조(전산실 운영관리) 다음 각 호와 같이 전산실을 통제구역으로 지정하고 운영·관리한다.
1. 전산실에 위치한 장비에 대한 도난, 파손, 변경, 불법적인 사용 등의 방지 대책수립
2. 정전 등으로 인해 제19조 제3항의 규정에 의한 중요 데이터의 손상 및 손실을 방지하기 위하여 데이터 백업 등 필요한 대책 수립
3. 전산실의 출입을 통제하는 장치를 설치하고, 인가된 출입자에 대한 '전산실 출입 대장' 기록 관리

제10조(정보보호시스템 등의 운영관리) ① 다음 각 호와 같이 정보통신서비스의 안정성과 정보의 신뢰성 확보를 위한 관리적·기술적 수단을 갖추고 이를 운영, 관리하여야 한다.
1. 침입차단시스템 등의 정보보호시스템을 설치하여 운영하거나 이에 상응하는 정보보호조치 수립
2. 라우터의 접근제어기능 또는 접근제어시스템 설치 등을 이용하여 외부 접근에 대한 시스템 보호조치 수립
② 프로그램의 보안취약점을 발견한 때에는 필요한 대책을 수립 하여야 한다.
③ 정보보안시스템의 도입 목적이 아닌 타 용도로 설정을 변경하거나 운용되는 행위를 하여서는 안된다. 만약 변경이 필요한 경우 보안심사위원회의 승인을 받아야 한다.

제11조(이용자 개인정보 보호) 이용자의 개인정보를 수집·이용 또는 제공하는 경우에는 홈페이지에 게시된 '개인정보처리방침'을 따른다.

제3장 정보보안담당자

제12조(정보보안담당자의 책무) ① 정보보안담당자는 시스템관리자 업무를 관리·감독하고, 시스템관리자의 인사 발령 시 계정삭제 등 적절한 보안조치를 취하여야 한다.
② 주기적으로 정보시스템의 보안취약점을 점검·분석하여 그 결과를 정보보안담당관에게 보고하여야 한다.
③ 정보시스템에 대한 부정한 접근을 방지하기 위한 제반 보호조치를 취하여야 한다.

④ 정보통신서비스의 제공에 필요한 정보시스템 및 라우터 등의 정보통신망 설비가 설치·운영되는 장소(이하 “전산실”이라 한다)에 대한 부정한 접근을 방지하기 위하여 적절한 조치를 취하여야 한다.

제13조(침해사고 대응·복구) ① 침해사고의 발생에 대비하여 다음 각 호의 사항을 포함하는 대응·복구계획을 수립하여 시행하여야 한다.
1. 비상연락망
2. 응급조치 절차
3. 복구대책

② 주기적으로 접속기록을 분석하여 침해사고를 예방하고, 침해사고를 발견한 경우에는 지체 없이 필요한 조치를 취하여야 한다.

제14조(이용자 계정 등의 관리) ① 이용자 계정 신청, 해지, 변경 및 분실 등이 있을 경우에 대비하여 신원확인 절차를 마련하여야 한다.
② 이용자의 패스워드 누출을 위한 보호조치를 마련하여야 한다.
③ 시스템관리자는 이용자가 5회 이상 로그인 실패 시 정보시스템 접속을 중단시키도록 시스템을 설정하고 비인가자의 침입 여부를 확인, 점검하여야 한다.
④ 시스템관리자는 교·직원의 퇴직 또는 보직변경 시 사용하지 않는 사용자계정을 즉시 삭제하고, 특별한 경우 외에는 유지보수 등을 위한 외부업체 직원에게 관리자계정을 제공해서는 안 된다.

제15조(이용자 서비스 제한조치) ① 다음에 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 프로그램의 유포행위
3. 음란·폭력물 등의 불건전한 자료의 게재·유포행위
4. 전자우편시스템에 장애를 유발시킬 목적으로 다량의 전자우편을 전송하는 행위
5. 수신자의 명시적인 수신거부 의사에 반하는 광고성 전자우편을 전송하는 행위
6. 기타 정보보호에 해가 되는 행위

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

제16조(이용자 제재) ① 제15조에 규정된 사항에 해당할 경우에는 사용자의 계정을 회수·삭제하여 정보시스템의 사용을 제한 또는 금지하며, 그에 따른 구체적 제재사항은 위원회에서 심의·결정한다.
② 정보시스템의 불법사용으로 이 대학교에 해를 끼치거나 명예를 훼손시켰을 경우에는 다음 각 호의 제재 조치를 취할 수 있다.

1. 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 의한 법적 조치
2. 학칙 제62조에 따른 징계 조치
3. 취업규칙 제86조에 따른 징계 조치
4. 정보시스템의 손해발생에 대한 손해배상 청구

제17조(이용자 고지) 제15조 각호 1에 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.

제18조(이용자 구제조치) 이용자의 불만사항 및 침해사고 피해발생시 처리절차 등을 홈페이지 등에 고지하여야 한다.

제4장 시스템관리자

제19조(시스템관리자의 책무) ① 시스템관리자는 데이터의 중요도에 따라 분류하여 적절한 관리기준 및 절차를 수립·시행하여야 한다.
② 제1항의 규정에 의하여 분류된 중요 데이터는 다음 각 호와 같이 관리하여야 한다.
1. 암호화하거나 파일 잠금 기능을 사용할 것
2. 제5조 제1항의 지침에 정한 바에 따라 접근을 통제할 것
③ 침해사고, 시스템의 장애 또는 정전 등으로부터 정보를 보호하기 위하여 주기적으로 데이터의 백업 등 적절한 조치를 취하여야 한다.
④ 제5조 제1항의 각종 지침을 성실히 수행하며, 이상이나 변동사항이 발생할 경우 즉시 정보보안담당자에게 보고하여야 한다.
⑤ 제2조 제2항의 주요자산을 항상 정상적인 가동 상태로 운영하도록 노력하며, 이상이 발생할 경우 정보보안담당자에게 보고하여야 한다.

제5장 이용자

제20조(계정 관리) ① 이용자는 자신의 계정 및 패스워드가 외부로 노출되지 않도록 유의하고 주기적으로 이를 변경하여야 한다.
② 이용자는 자신의 계정 및 패스워드를 본인이 직접 사용하여야 하며, 타인과 공유하여서는 안된다. 공유로 인하여 발생할 수 있는 각종 손실 및 손해에 대한 책임은 본인에게 귀속된다.

제21조(개인정보 관리) ① 개인정보를 제공할 경우에는 이 대학교 홈페이지에 게시된 '개인정보처리방침'에서 규정하는 개인정보의 수집목적, 관리방법 등을 확인하여야 한다.
② 정보공유가 가능하고 다양한 이용자가 공동으로 이용하는 전기통신설비를 이용하는 경우에는

개인정보 및 사생활정보 등의 보호를 위하여 공유해지 등 필요한 조치를 하여야 한다.

제22조(컴퓨터바이러스 등 주의) ① 발송자를 확인할 수 없는 전자우편 또는 제공자가 불확실한 컴퓨터프로그램 등에 대해 안전성여부를 확인하고 실행하여야 한다.
② 자신의 컴퓨터에 최신의 컴퓨터바이러스 방지프로그램을 설치하여 침투여부를 수시로 점검하고, 침투한 경우에는 이를 제거·복구하여야 한다.
③ 자신의 컴퓨터에 최신의 윈도우 업데이트를 주기적으로 실행하며 필요한 보안패치를 반드시 적용하여야 한다.

제23조(사이버 보안진단의 날) ① 매월 셋째주 수요일에 실시하는 사이버 보안진단의 날의 시행에 협조해야 한다.
② 지정된 정보보호 소프트웨어를 사용하여 사이버 보안진단을 수행해야 하며 그 결과를 정보보안담당관에게 통보하여야 한다.
③ 사이버 보안진단을 수행하지 않는 이용자의 전산망 접속을 제한 할 수 있다.

제24조(패치관리 프로그램 설치) ① 교내 모든 이용자는 개인 PC의 보호를 위해 패치관리 시스템을 설치하여야 한다.
② 패치관리시스템을 설치하지 않은 이용자의 전산망 접속을 제한할 수 있다.
③ 이용자 PC의 보호를 위해 정보보안담당자는 관련된 패치 및 소프트웨어를 배포할 수 있다.
④ 정보보안담당관은 패치관리시스템을 통한 개인정보누출 방지를 위한 점검을 지속적으로 실시하여야 한다.

제25조(불법 소프트웨어 사용 차단을 위한 자가진단 수행) ① 교내 모든 이용자는 불법프로그램으로 인한 악성코드, 바이러스 등의 감염을 차단하고 정보시스템을 안전하게 보호하기 위하여 소프트웨어에 대한 연 2회 주기적인 점검을 수행하여야 한다.
② 이용자 PC의 불법 소프트웨어를 진단하기 위해 정보보안담당자는 관련된 소프트웨어를 배포할 수 있다.
③ 불법 소프트웨어 사용으로 인한 법적 책임은 이용자 본인이 진다.

제26조(홈페이지 게시자료 보안관리) ① 사용자는 개인정보, 비공개 공문서 및 민감 자료가 포함된 문서를 홈페이지에 공개하여서는 안된다.
② 정보보안담당자는 기관의 홈페이지 등에 비공개 내용이 게시되었는지 여부를 주기적으로 확인하고 개인정보를 포함한 중요정보가 홈페이지에 공개되지 않도록 보안교육을 주기적으로 실시하여야 한다.
③ 정보보안담당자는 홈페이지에 중요정보가 공개된 것을 인지할 경우 이를 즉시 차단하는 등의 보안조치를 요청하여야 하며, 해당 부서는 이를 즉시 시행하여야 한다.

부 칙

제1조(시행일) 이 규정은 2018년 4월 10일부터 시행한다.

제2조(준용) 이 규정이 정하는 바 이외의 정보보호업무에 관한 사항은 정부의 「보안업무규정」 및 「보안업무규정 시행규칙」과 「교육부 보안업무규정 시행세칙」을 준용한다.