정보보안 규정

2016. 9. 23. 제정

제1조(목적) 이 규정은 이화여자대학교(이하 “본교”라 한다) 정보통신망의 안정성과 정보보안을 위해 필요한 사항을 규정함을 목적으로 한다.

제2조(용어의 정의) 이 규정에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. “정보통신서비스”라 함은 정보통신설비 및 시설을 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다.
2. “정보통신설비”라 함은 정보통신서비스를 제공하기 위한 기계, 기구, 선로 등의 설비를 말한다.
3. “정보통신시설”이라 함은 정보통신설비가 집적되어 있는 시설 및 부대시설을 말한다.
4. “주요자산”이라 함은 정보통신설비 중 정보통신서비스에 중요한 역할을 하는 라우터, 스위치, 웹서버, DNS서버, DB서버, PC 등의 설비와 관련 S/W를 말한다.
5. “정보통신서비스제공자”라 함은 정보통신설비 및 정보통신시설을 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.
6. “이용자”라 함은 정보통신서비스제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
7. “정보보안담당관”이라 함은 정보통신서비스의 안정성 확보 및 정보보안 업무를 총괄하는 자를 말한다.
8. “정보보안담당자”라 함은 정보통신서비스의 안정성 확보 및 정보보안 실무 업무를 담당하는 자를 말한다.
9. “시스템관리자”라 함은 정보통신서비스에 이용되는 정보통신설비와 정보통신시설을 관리·운영하는 자를 말한다.
10. “사이버침해사고”라 함은 해킹 및 컴퓨터바이러스의 유포 등에 의해 정보통신시스템이 정상적으로 운영되지 않거나 정보의 유출·파괴 또는 정보의 위조·변조 등이 발생한 사태를 말한다.

제3조(보안책임) ① 본교의 교원, 직원 및 보조인력(용역인력 포함) (이하 "구성원"이라 한다)에게는 학교 내에서 자신이 속하는 기관의 정보자산, 시설과 기기에 대하여 이 규정과 이 규정에 따른 지침을 준수할 의무가 있다.

② 모든 구성원에게는 교내 게시판 및 전자메일 등을 통한 정보보안 규정의 제·개정 내용, 보안 취약점 안내, 계도 사항 등 보안 공지를 열람 후 숙지할 의무가 있다.

③ 각 기관의 장(이하 "기관장"이라 한다)에게는 관할기관에서 생산, 가공, 유통, 관리, 파기되는 정보자산 및 다른 기관 또는 외부에 접근이 허용된 정보자산에 대하여 보안책임이 있다.

④ 각 기관의 정보보안담당자는 소속 기관의 정보보안업무를 수행할 책임이 있다.

제4조(정보보안조직의 구성) ① 정보보안조직은 정보보안담당관, 정보보안담당자, 시스템관리자로 구성한다.

② 정보보안담당관은 정보통신처장이 겸한다.

③ 정보보안담당자와 시스템관리자는 정보보안담당관이 임명한다.

④ 정보보안담당관은 정보보안 업무를 효과적으로 수행하기 위하여 기관별 정보보안 담당자를 지정할 수 있다.

제5조(내부지침의 수립 및 시행) 정보보안담당자는 업무 수행에 필요한 내부지침을 수립하여 시행할 수 있다.

제6조(정보보안담당관의 책무) ① 정보보안담당관은 정보보안담당자, 시스템관리자의 업무를 관리·감독하여야 한다.

② 정보보안담당자나 시스템관리자의 업무수행과 관련해 오류 또는 불법행위가 있을 경우 정보보안담당관은 이를 즉시 총장에게 보고하여야 한다.

③ 정보보안담당관은 정보화추진위원회에 정보보안업무에 필요한 심사 및 자문을 의뢰할 수 있다.

제7조(정보보안담당자의 책무) ① 정보보안담당자는 시스템관리자의 업무를 관리·감독하여야 한다.

② 정보보안담당자는 시스템관리자가 타기관으로 전보되거나 퇴직할 경우 계정삭제 등 정보보안을 위한 적절한 조치를 취하여야 한다.

③ 정보보안담당자는 사이버침해사고 발생에 대비하여 비상연락망, 응급조치 절차 및 복구대책을 포함하는 사이버침해사고대응절차를 수립하고 이를 시행하여야 한다.

④ 정보보안담당자는 정기적으로 정보시스템의 보안취약점을 점검·분석하여 그 결과를 정보보안담당관에게 보고하여야 한다.

⑤ 정보보안담당자는 정기적으로 이용자접속기록을 분석하여 사이버침해사고를 예방하고, 사이버침해사고가 발생한 경우에는 즉시 필요한 조치를 취하여야 한다.

⑥ 정보보안담당자는 정보통신설비 및 정보통신시설에 대한 부정한 접근을 방지하기 위한 적절한 조치를 취하여야 한다.

제8조(시스템관리자의 책무) ① 시스템관리자는 정보통신망에 운용되는 데이터를 그 중요도에 따라 분류하고 적절한 관리기준 및 절차를 수립·시행하여야 한다.

② 시스템관리자는 중요데이터는 암호화하거나 파일 잠금기능을 사용해 관리하여야 하며 필요한 경우 이용자 접근을 통제하여야 한다.

③ 시스템관리자는 사이버침해사고, 시스템 장애, 정전 등으로부터 정보를 보호하기 위해 정기적으로 데이터백업 등 적절한 조치를 취하여야 한다.

④ 시스템관리자는 주요자산이 정상적인 가동상태로 운영되도록 노력하여야 하며, 사이버침해사고나 시스템 장애가 발생했을 경우 이를 즉시 정보보안담당자에게 보고하여야 한다.

제9조(사이버침해사고 대응관리) ① 정보보안담당관은 긴급한 사이버침해사고가 발생하였을

경우 모든 이용자에게 대응책을 신속하게 알릴 수 있는 체계를 마련하여야 한다.

② 정보보안담당관은 사이버침해사고나 이상징후가 감지되었을 때에는 제7조제3항의 사이버침해사고대응절차에 따라 즉각적인 대응조치를 취하고, 이용자 접속기록 등 적절한 증거자료를 수집·보관하여야 한다.

제10조(정보보안 교육) ① 정보보안담당관은 정보보안담당자, 시스템관리자 등 정보보안과 관련된 업무에 종사하는 자에게 정기적으로 정보보안교육을 실시하여야 한다.

② 정보보안담당관은 필요한 경우 정보보안 교육을 외부의 정보보안 관련 전문교육기관에 위탁할 수 있다.

제11조(인적보안) ① 정보보안담당관은 구성원에게 정보보안 및 보안에 대한 서약서를 징구할 수 있으며 필요한 경우 관련 기관에 징구를 위임할 수 있다.

② 정보보안담당관은 교원 및 직원이 전보되거나 퇴직한 경우 해당자의 개인계정 및 공용계정에 대한 권한을 즉시 제거하여야 한다.

③ 정보보안담당관은 정보통신설비 및 정보통신시설의 관리 운영을 외부에 위탁할 경우 계약서 또는 SLA(서비스 수준 협약)에 정보보안 관련사항(보안사고 책임범위, 비밀준수 의무, 위탁업무 중단시 비상대책)을 반영하여야 한다.

④ 정보보안담당관은 정보보안담당자와 시스템관리자가 정보보안업무 수행에 필요한 정보보안자격증을 취득할 수 있도록 지원한다.

제12조(시스템실 운영관리) 정보보안담당관은 다음 각 호와 같은 조치를 강구하고 시스템실을 운영, 관리하여야 한다.

1. 시스템실내 장비의 도난, 파손, 변경, 불법사용 등에 대한 예방대책
2. 데이터 백업 등 중요 데이터의 손상 및 손실을 방지하기 위한 대책
3. 시스템실 출입 통제장치 설치
4. 출입내역을 기록하는 시스템실 출입 대장 비치

제13조(정보보안시스템 등의 운영관리) ① 정보보안담당관은 다음 각 호와 같은 조치를 강구하고 정보보안시스템을 운영, 관리하여야 한다.

1. 침입차단시스템 등 정보보안시스템의 설치·운영 및 이에 상응하는 정보보안조치
2. 라우터의 접근제어기능 또는 침입차단시스템의 필터링 기능 등을 이용한 정보시스템의 외부 네트워크와의 분리조치

② 정보보안담당관은 정보보안시스템의 보안취약점이 발견된 때에는 필요한 대책을 강구하여야 한다.

제14조(이용자 계정 등의 관리) ① 정보보안담당관은 이용자 계정 신청, 해지, 변경 및 분실 등에 대비한 신원확인 절차를 마련하여야 한다.

② 정보보안담당관은 이용자의 패스워드를 보호하여야 한다.

제15조(이용제한) 정보보안담당자는 다음 각 호에 해당하는 행위를 한 이용자에 대하여 정보통신서비스 이용을 제한할 수 있다.

1. 부당한 방법으로 정보통신망의 타인정보를 훼손하거나 침해·도용 또는 누설하는 행위

2. 컴퓨터바이러스 등 악성 프로그램 유포행위
3. 음란·폭력물 등 불건전한 자료의 게재·유포행위
4. 전자우편시스템의 장애유발을 목적으로 다량의 전자우편을 전송하는 행위
5. 수신자의 거부의사에도 불구하고 광고성 전자우편을 전송하는 행위
6. 불명확한 사유로 교내 업무 처리를 방해하거나 중단시키는 행위
7. 기타 정보보안에 해가 되는 행위

제16조(이용제한 고지) ① 정보보안담당자는 제15조의 이용제한 사유로 인해 정보통신서비스 이용을 제한하고자 할 경우 그 사실을 즉시 이용자에게 고지하여야 한다. 다만, 이용제한과 동시에 시스템안정성 확보를 위한 신속한 조치가 필요한 경우 사후 고지할 수 있다.

② 이용제한 고지는 학내 정보망에 이용제한 사유와 내역을 게시하는 것으로 한다.

제17조(이용자 개인정보 이용) 정보보안담당관이 이용자의 개인정보를 수집·이용할 경우에는 홈페이지에 게시된 「개인정보 처리방침」을 따른다.

제18조(이용자 개인정보 관리) ① 이용자가 개인정보를 제공할 경우에는 홈페이지에 게시된 「개인정보 처리방침」에서 정하는 개인정보의 수집목적, 관리방법 등을 확인하여야 한다.

② 이용자가 정보공유가 가능하고 다양한 이용자가 공동으로 이용하는 전기통신설비를 이용하는 경우에는 개인정보, 사생활정보 등의 보호를 위하여 공유해지 등 필요한 조치를 하여야 한다.

제19조(PC 등 단말기 보안관리) ① 이용자는 PC·노트북·PDA 등 단말기 (이하 PC 등) 사용과 관련한 일체의 보안관리 책임을 가진다.

② 이용자는 비인가자가 PC 등을 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손시키지 못하도록 다음 각 호의 보안대책을 준수하여야 한다.

1. 장비(CMOS 비밀번호)·자료(중요문서자료 암호화 비밀번호)·사용자(로그온 비밀번호)별 비밀번호를 주기적으로 변경 사용
2. 10분 이상 PC 작업 중단 시 비밀번호가 적용된 화면보호 조치
3. 운영체제(OS) 및 응용프로그램 (한컴오피스, MS Office 등)의 최신 보안패치 유지
4. PC에 최신 바이러스 방지프로그램을 설치하여 침투여부를 수시로 점검하고, 침투한 경우에는 이를 제거·복구
5. 업무상 불필요한 응용프로그램 설치 금지 및 공유 폴더의 삭제
6. 업무에 무관한 메신저·P2P·웹하드, 불필요한 Active-X 등 보안에 취약한 프로그램과 비인가 프로그램·장치의 설치 금지

③ 이용자는 PC 등 단말기를 교체·반납·폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 정보보안담당자와 협의하여 하드디스크에 수록된 자료가 유출 되지 않도록 보안조치 하여야 한다.

④ 이용자는 사용이 승인된 소프트웨어만을 사용해야 하며, 검증되지 않은 불법 소프트웨어의 사용으로 인한 피해는 본인이 책임을 져야 한다.

⑤ 이용자는 발송자를 확인할 수 없는 전자우편 또는 제공자가 불확실한 컴퓨터프로그램

등에 대해 안전성 여부를 확인하고 실행하여야 한다.

⑥ 이용자는 업무상 필요한 PC내의 데이터는 별도의 저장장치를 통해서 백업을 하여 만일의 사태에 대비해야 하며, 이 저장 매체는 시건장치가 되어있는 장소에 보관한다.

제20조(휴대용 저장매체 보안관리) ① 정보보안담당관은 휴대용 저장매체를 사용하여 중요 업무자료를 보관할 필요가 있을 때에는 위변조, 훼손, 분실 등에 대비한 보안대책을 강구하여야 한다.

② 기관장은 휴대용 저장매체에 업무자료 보관을 원칙적으로 금지하여야 하며 부득이한 경우에는 기관장의 승인을 얻어 한시적으로 허용할 수 있다.

③ 이용자는 USB 메모리를 PC 등에 연결 시 자동 실행되지 않도록 하고 최신 백신으로 악성코드 감염여부를 자동 검사하도록 보안 설정한다.

제21조(네트워크 보안관리) ① 이용자는 보안지침 및 절차에 따라 네트워크 서비스를 요청한다. 인가된 정보만을 취급하며, 보안 침해사고의 발생 시 정보보안담당자 및 시스템관리자에게 연락한다.

② 이용자는 PC의 IP 주소를 임의로 변경할 수 없다.

③ 네트워크 진단·관리 도구들은 관리 담당자에 의해서만 사용되고 일반적인 이용자들에게는 사용이 허가되지 않는다.

④ 이용자는 침입차단시스템 등 보안시스템의 경로를 우회하는 경로를 설정해서는 아니 된다. 원칙적으로 내부사용자는 모뎀을 통하여 인터넷에 접속할 수 없으며, 부득이한 경우 기관장과 정보보안담당관의 승인을 받은 후 사용한다.

⑤ 이용자는 보안 문제를 발생시킬 수 있는 개인 소유의 컴퓨터, 주변장치 또는 소프트웨어를 조직 내로 가져와서 네트워크에 연결해서는 아니 된다.

⑥ 이용자는 인터넷과 같은 개방된 네트워크를 통해 전송하는 비밀 정보를 암호화 적용해야한다.

제22조(이메일 보안관리) ① 이용자는 상용 전자우편을 이용한 업무자료 송수신을 하여서는 아니 된다.

② 외부인은 원칙적으로 본교 E-mail을 사용할 수 없으며, 예외의 경우 그 이유를 문서화한다.

③ 고의로 E-mail을 오용하는 경우 상응하는 징계 등의 조치를 취할 수 있다.

④ 특별히 기밀성을 요하는 정보가 있을 경우 E-mail을 통해 전송되어야 한다면 본교에서 승인한 소프트웨어와 알고리즘을 사용하여 지정 수신인만 읽을 수 있도록 암호화한다.

제23조(아이디 및 패스워드 관리) ① 이용자는 자신의 아이디 및 패스워드가 외부로 노출되지 않도록 관리에 유의하여야 한다.

② 비밀번호는 다음 각 호 사항을 반영하여 숫자와 문자, 특수문자 등을 혼합하여 8자리 이상으로 정하고, 분기 1회 이상 주기적으로 변경 사용하여야 한다.

1. 사용자계정(ID)과 동일하지 않은 것
2. 개인 신상 및 기관 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 입력기능을 사용하지 말 것

③ 서버에 등록된 비밀번호는 암호화하여 저장하여야 한다.

제24조(홈페이지 게시자료 보안관리) ① 이용자는 개인정보, 비공개 공문서 및 민감 정보가 포함된 문서를 홈페이지에 공개하여서는 아니 된다.

② 이용자는 인터넷 블로그·카페·게시판·개인 홈페이지 또는 소셜 네트워크 서비스 등 일반에 공개된 전산망에 업무관련 자료를 무단 게재하여서는 아니 된다.

③ 정보보안담당자는 각 기관의 홈페이지 등에 비공개 내용이 게시되었는지 여부를 주기적으로 확인하고 개인정보를 포함한 중요정보가 홈페이지에 공개되지 않도록 보안교육을 주기적으로 실시하여야 한다.

④ 기관장은 홈페이지에 중요정보가 공개된 것을 인지할 경우 이를 즉시 차단하는 등의 보안조치를 강구 시행하여야 한다.

제25조(홈페이지 구축 및 운영 보안관리) ① 기관장은 홈페이지를 구축 및 운영하고자 하는 경우, 웹 취약점의 존재에 의한 사이버 침해사고가 발생하지 않도록 교육부 및 신뢰할 수 있는 기관의 웹 취약점 대응 가이드를 참조하여 홈페이지를 구축 및 운영하여야 한다.

② 정보보안담당관은 각 기관의 홈페이지 구축이 완료되고 서비스가 개시되기 이전에 보안진단을 실시하고, 취약점이 존재하는 경우 이를 수정한 후 서비스를 할 수 있도록 제한하여야 한다.

③ 기관장은 각 기관의 홈페이지에서 취약점이 존재함을 인지하였거나 통보 받았을 경우, 정보보안담당관과 협의하여 초동조치를 취하고 이를 즉시 수정하여야 하며, 그렇지 아니한 경우에 정보보안담당관은 해당 서비스를 차단할 수 있다.

④ 각 기관의 홈페이지 관리자는 홈페이지 관리자 페이지에 대하여 내부망의 IP·MAC 주소에서만 접근이 가능하도록 제한을 하여야 하며, 제23조제2항을 참조하여 비밀번호의 보안성을 강화하여야 한다.

⑤ 기관장은 홈페이지를 더 이상 운영하지 않을 경우, 정보보안담당관과 협의하여 홈페이지를 즉시 폐기하고 서비스를 차단하여야 한다.

제26조(정보시스템 개발보안) ① 각 기관의 시스템 개발사업 담당자는 정보시스템을 자체적으로 개발하고자 하는 경우에는 다음 각 호의 사항을 고려하여 보안대책을 수립하고 정보보안담당관의 확인을 받아야 한다.

1. 독립된 개발시설을 확보하고 비인가자의 접근 통제

2. 개발시스템과 운영시스템의 물리적 분리

3. 소스코드 관리 및 소프트웨어 보안관리

② 각 기관의 시스템 개발사업 담당자는 외부용역 업체와 계약하여 정보시스템을 개발하고

자 하는 경우에는 다음 각 호의 사항을 고려하여 보안대책을 수립하고 정보보안담당자의 확인을 받아야 한다.

1. 외부인력 대상 신원확인, 보안서약서 징구, 보안교육 및 점검
2. 외부 인력의 보안준수 사항 확인 및 위반 시 배상책임의 계약서 명시
3. 외부 인력의 정보시스템 접근권한 및 제공자료 보안대책
4. 외부 인력에 의한 장비 반입·반출 및 자료 무단반출 여부 확인
5. 제1항제1호부터 제3호까지의 사항

③ 정보보안담당자는 제1항 및 제2항과 관련하여 보안대책의 적절성을 수시로 점검하고 정보시스템 개발을 완료한 경우에는 정보보안 요구사항을 충족하는지 검토하여야 한다.

제27조(정보시스템 유지보수) ① 기관장이 정보시스템 유지보수 절차 및 문서화 수립 시 고려사항은 다음 각 호와 같다.

1. 유지보수 인력에 대해 보안서약서 집행, 보안교육 등을 포함한 유지보수 인가 절차를 마련하고 인가된 유지보수 인력만 유지보수에 참여한다.
2. 결함이 의심되거나 발생한 결함, 예방 및 유지보수에 대한 기록을 보관한다.
3. 유지보수를 위해 원래 설치장소 외 다른 장소로 정보시스템을 이동할 경우, 통제수단을 강구한다.
4. 정보시스템의 유지보수 시에는 일시, 담당자 인적사항, 출입 통제조치, 정비내용 등을 기록·유지하여야 한다.

② 시스템관리자 등이 유지보수와 관련된 장비·도구 등을 반출입할 경우, 악성코드 감염여부, 자료 무단반출 여부를 확인하는 등 보안 조치하여야 한다.

③ 시스템관리자는 외부에서 원격으로 정보시스템을 유지보수 하는 것을 원칙적으로 금지하여야 하며 부득이한 경우에는 정보보안담당자와 협의하여 자체 보안대책을 강구한 후 한시적으로 허용할 수 있다.

제28조(용역사업 보안관리) ① 기관장은 정보화·정보보안사업 수행 등을 외부용역으로 추진할 경우 사업 책임자로 하여금 다음 각 호의 사항을 포함한 보안대책을 수립. 시행하여야 하며, 이를 계약서에 명시해야 한다.

1. 용역사업 계약 시 계약서에 참가직원의 보안준수 사항과 위반 시 손해배상 책임 등 명시
2. 용역사업 수행 관련 보안교육·점검 및 용역기간 중 참여인력의 보안서약서 징구 및 임의 교체 금지
3. 사업 종료 시 외부업체의 노트북·휴대용 저장매체 등을 통해 비공개 자료가 유출되는 것을 방지하기 위해 복구가 불가능하도록 완전삭제
4. 용역업체로부터 용역 결과물을 전량 회수하고 비인가자에게 제공·열람 금지
5. 용역업체의 노트북 등 관련 장비를 반입·반출시마다 악성코드 감염여부, 자료 무단반출 여부를 확인
6. 그 밖에 기관장이 보안관리가 필요하다고 판단하는 사항이나 정보보안담당관이 보안조치

를 권고하는 사항

② 기관장은 용역사업 추진 시 과업지시서·입찰공고·계약서 등에 다음 각 호의 누출금지 대상정보를 명시해야 한다.

1. 기관 소유 정보시스템의 내·외부 IP주소 현황
2. 세부 정보시스템 구성 현황 및 정보통신망 구성도
3. 사용자계정·비밀번호 등 정보시스템 접근권한 정보
4. 정보통신망 취약점 분석·평가 결과물
5. 정보화 용역사업 결과물 및 관련 프로그램 소스코드
6. 「개인정보 보호법」 제2조제1항의 개인정보

③ 용역업체가 보안관련 사항을 위반하였을 경우 다음 각 호의 사항을 조치해야 한다.

1. 보안관련 위반시 경위 확인
2. 보안위규 처리기준에 따라 조치
3. 재발방지대책 강구 요구
4. 보안조치 이행여부 점검

④ 용역업체가 정보시스템 개발 및 유지보수를 시행할 때 원칙적으로 원격작업을 금지한다.

제29조(정보시스템 위탁운영 보안관리) ① 기관장은 소관 정보시스템에 대한 외부업체의 위탁운영을 최소화하되, 위탁 운영과 관련한 관리적·물리적·기술적 보안대책을 수립하여 시행하여야 한다.

② 정보시스템의 위탁 운영은 여타 기관 또는 업체 직원이 당해 기관에 상주하여 수행하는 것을 원칙으로 한다. 다만, 해당기관에 위탁업무 수행 직원의 상주가 불가한 타당한 사유가 있을 경우, 그러하지 아니할 수 있다.

제30조(다른 법령과의 관계) 이 규정에 명시되지 않은 사항은 다음 각 호의 법령 등에 따른다.

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 동법 시행령
2. 「정보보호조치에 관한 지침」
3. 「교육부 정보보안 기본지침」
4. 교육부 사이버분야 위기대응 실무 매뉴얼
5. 그 밖의 관계 법규

부칙 <2016. 9. 23. 제정>

제1조(시행일) 이 규정은 공포일부터 시행한다.

제2조(폐지규정) 이 규정의 시행과 동시에 「정보보호 규정」은 폐지한다.