정보보안 규정

2016. 9. 23. 제정
2020. 8. 19. 개정

제1장 총 칙

제1조(목적) 이 규정은 이화여자대학교(이하 "본교"라 한다) 정보통신망의 안정성과 정보자산의 신뢰성을 확보하기 위해 필요한 사항을 정하는 것을 목적으로 한다.

제2조(적용대상 및 범위) ① 적용대상은 정보자산을 이용하거나 관리하는 본교 구성원과 관련 외부자로 한다.

② 적용범위는 관리적·기술적·물리적 보호가 필요한 본교의 주요 정보자산 및 관련 자산으로 한다.

제3조(용어정의) 이 규정에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "정보보호 관리체계"란 조직의 주요 정보자산을 보호하기 위해 정보보호 관리절차와 과정을 체계적으로 수립하여 지속적으로 관리·운영하기 위한 종합적인 체계를 말한다.
2. "정보보안"이란 정보시스템 및 정보통신망을 통해 수집·가공·저장·검색·송수신되는 정보의 유출·위변조·훼손 등을 방지하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위로 사이버안전을 포함한다.
3. "정보시스템"이란 PC·서버 등 단말기, 보조기억매체, 전산·통신장치, 정보통신기기, 응용프로그램 등 정보의 수집, 가공, 저장, 검색, 송·수신에 필요한 하드웨어 및 소프트웨어 일체를 말한다.
4. "정보자산"이란 본교의 서비스를 제공하기 위한 정보시스템과 정보시스템의 운영·관리에 필요한 시설, 전자정보 등 자산을 총칭한다.
5. "기밀성(Confidentiality)"이란 비인가자가 임의의 정보를 사용하거나 정보가 노출되지 못하도록 하는 특성으로 자산 또는 데이터가 전송, 백업, 보관 중에 허가 받지 않은 사람에게 노출되지 않아야 함을 말한다.
6. "무결성(Integrity)"이란 비인가된 방법을 통해 정보를 변경 또는 파괴하지 못하도록 하는 특성으로 정보가 전송되고 저장되는 과정에서 완전성과 정확성을 유지하는 것을 말한다.
7. "가용성(Availability)"이란 권한을 가진 개체의 요구에 따라 정보자산을 지속적으로 접근하고 사용이 가능하도록 하는 특성을 말한다.
8. "중요정보"란 노출, 변경, 파괴 시 업무에 중대한 영향을 미칠 수 있는 정보로서, 암호화대상은 개인정보보호법에 따른다.

제4조(정보보안 기본 수칙) ① 정보자산을 이용·관리하는 본교 구성원과 관련 외부자는 다음

각 호의 정보보안 활동의 기본 수칙을 준수하여야 한다.

1. 개인별 사용자 계정 및 비밀번호의 기밀을 유지하여야 하며, 본래의 발급 목적으로만 사용하여야 한다.
2. 허가받은 정보시스템의 권한이 부여된 영역에 대하여 본래의 목적으로만 사용하여야 한다.
3. 정보시스템의 성능저하 및 보안상 위험을 초래할 수 있는 행위를 해서는 아니 된다.
4. 정보자산과 연관된 저작권·특허권 및 소프트웨어 라이선스의 사용 조건을 숙지하고 이를 준수하여야 한다.
5. 업무와 관련해 습득한 정보자산을 임의로 외부에 누출해서는 아니 된다.

② 정보보안 담당부서는 정보통신망과 정보시스템의 안전성 및 정보보안 규정의 준수 여부를 주기적으로 점검하여야 하며 본교 구성원과 관련 외부자는 이에 적극 협조하여야 한다.

③ 정보보안 담당부서는 정보보안 사고를 예방하기 위한 목적으로 정보보안 활동을 즉시 시행할 수 있다.

제2장 정보보안 규정 관리

제5조(정보보안 목표 및 역할) ① 정보보안은 본교 업무의 연속성을 보장하고, 정보보안 사고 시 시스템 및 자원의 피해를 최소화하는 것을 목표로 한다.

② 정보보안의 역할은 정보의 생성, 저장, 처리, 송신, 수신시에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하여 정보에 대한 기밀성, 무결성, 가용성을 확보하는 것이다.

제6조(정보보안 규정 등의 수립) ① 정보보안 규정의 제·개정 시 정보화추진위원회의 심의를 거친 후 총장의 승인을 받아야 한다.

② 정보보안 규정에서 정의한 정보보안 업무를 수행하기 위한 시행세칙을 체계적으로 수립하여 정보보안 담당관의 승인을 받아야 한다.

③ 정보보안 담당관은 정보보안 규정 및 시행세칙을 모든 본교 구성원에게 공지하고 적용하여야 한다.

제7조(정보보안 규정 등의 유지 및 관리) 정보보안 관리자는 정보보안 규정 및 시행세칙의 타당성을 매년 1회 정기적으로 검토하여야 하며, 정보보안 관련 법령 제·개정 및 대내외 환경에 중대한 변화 발생 시 추가 검토를 수행할 수 있다.

제3장 정보보안 조직 체계

제8조(정보화추진위원회) 보안업무의 효율적인 운영과 업무계획수립 및 기타 보안에 관한 중요한 사항은 정보화추진위원회에서 심의한다.

제9조(정보보안 담당부서의 구성) ① 총장은 효율적·체계적인 정보보안 업무를 수행하기 위하여 정보보안 담당부서를 구성 운영하여야 한다.

② 정보통신처장은 당연직으로 정보보안 담당관이 된다.

③ 본교의 정보보안 총괄업무는 정보통신처에서 수행하고, 정보통신처 정보인프라팀을 정보보안 담당부서로 하며 정보인프라팀장이 정보보안 관리자가 된다. 정보보안 관리자는 팀원 중에서 정보보안 담당자를 지정한다.

제10조(정보보안 담당관 등의 책임 및 역할) ① 정보보안 담당관의 책임 및 역할은 다음 각 호와 같다.

1. 정보보안 계획 수립에 대한 관리 감독
2. 정보보안 규정 및 시행세칙의 수립, 운영에 대한 관리 감독
3. 정보자산의 관리 및 위험 분석, 평가 활동에 대한 관리 감독
4. 정보보안 관련 예산 편성 및 집행에 대한 관리 감독
5. 정보보안 사고의 예방 및 대응에 대한 관리 감독

② 정보보안 관리자의 책임 및 역할은 다음 각 호와 같다.

1. 정보보안 계획 수립 및 수행
2. 정보보안 규정 및 시행세칙의 수립, 운영
3. 정보자산의 관리 및 위험 분석, 평가 활동 관리
4. 정보보안 관련 예산 편성 및 집행
5. 정보보안 사고 등 비상상황 시 대응 활동 관리

③ 정보보안 담당자의 책임 및 역할은 각 호와 같다.

1. 정보자산의 관리 및 위험 분석, 평가 활동 수행
2. 정보보안 사고 예방 및 대응 활동
3. 정보보안 실무 활동

제11조(활동 평가) 정보보안 활동의 평가는 「교원인사 규정」, 「사무직원인사 규정」에서 정하는 포상 및 징계기준에 따르며 정보보안 활동 및 성과를 주기적으로 평가한다.

제4장 정보보호 관리체계 운영 및 검토

제12조(운영 검토) ① 정보보호 관리체계의 효과를 지속적으로 보장하기 위하여 연1회 이상 정보보호 관리체계 운영 전반에 대한 검토를 실시한다.

② 정보보호 관리체계 운영 검토사항은 다음 각 호와 같다.

1. 정보보호 관리체계 내부심사 결과
2. 정보보안 업무계획 및 실적
3. 정보보안 시스템 도입에 관한 사항
4. 위험평가 및 조치에 관한 사항
5. 과년도 개선 조치 사항

제13조(운영기록의 유지 및 통제) ① 정보보안 담당자는 정보보호 관리체계 운영에 따른 기록을 유지하고 체계적으로 관리한다.

② 정보보안 담당자는 제1항에 의한 운영기록의 열람, 복사 등에 대하여 통제한다.

제5장 인적보안 관리

제14조(채용 시 보안) ① 본교 교직원은 채용 시 재직 중에 취득한 정보에 대한 보안을 유지하도록 보안서약서를 작성하여야 한다. (개정 2020.8.19.)

② 정보보안 담당부서는 인사담당 부서와 협의하여 신규 교직원 채용 시 본교의 정보보안 규정 및 시행세칙이 정하는 바에 따라 정보보안 교육을 시행하여야 한다.

제15조(직무 변경 등 인사이동 시 보안) 인사담당 부서는 본교 교직원의 부서 및 직무변경, 휴직, 퇴직 시 인사변경 내용을 관련 부서와 공유하여 사용자 계정 권한을 변경하여야 한다.

제16조(퇴직 시 보안) ① 퇴직자는 퇴직 시 재직 중 보유한 모든 정보자산(사용PC, 보조기억매체, 업무자료 및 문서, 출입증 등)을 반납하고 이에 대해 소속기관장의 승인을 받아야 한다.

② 퇴직자에게 발급한 모든 사용자 계정 권한을 즉시 삭제 또는 사용중지하여야 한다.

③ 본교 교직원은 퇴직 시 보안서약서를 작성하여야 한다. (신설 2020.8.19.)

제17조(직무 분리 및 주요 직무자 관리) ① 정보자산에 대한 비인가된 변조 또는 권한 오남용을 예방하기 위하여 권한과 책임을 분리하는 직무 분리를 하여야 한다.

② 직무 분리를 다음 각 호와 같이 하며 주요 직무자를 최소한의 범위로 지정하여야 한다.

1. 정보시스템 운영
2. 정보시스템 개발
3. 데이터베이스시스템 관리
4. 정보보안 업무

③ 주요 직무자의 지정 현황 및 권한 부여의 적정성을 연1회 이상 검토하여야 한다.

④ 개발과 운영 업무는 직무 분리를 하여 수행하는 것을 원칙으로 한다.

⑤ 직무 분리가 어려운 경우 직무자의 책임 추적성 확보를 위한 보완통제 방안을 마련하여야 한다.

제18조(위반 시 조치) 본교 교직원과 관련 외부자가 정보보안 규정 및 시행세칙을 위반할 경우 관련 법령 및 규정에 따라 필요한 조치를 할 수 있다.

제19조(외부자 보안 관리) ① 정보보안 담당부서는 유지보수를 포함한 각종 용역사업의 업무 위탁 및 외부 시설·서비스의 이용 현황을 식별하여 관리한다.

② 용역사업 책임자는 업무 위탁 및 외부 시설·서비스의 이용에 따른 법적 요구사항과 위험을 파악하고 적절한 보호대책을 마련한다.

제6장 보안점검 및 감사

제20조(보안점검) 정보보안 담당부서는 매월 하루를 「사이버보안 진단의 날」로 지정하여 정보보안의 중요성을 인지시키고, PC의 보안상태를 주기적으로 점검하여야 한다.

제21조(보안감사) ① 정보보안 담당부서는 매년 보안감사 인력, 대상, 범위, 기준, 일정, 방법 등을 포함한 보안감사계획을 수립한다.

② 보안감사 인력은 독립성과 전문성을 갖추어야 하며, 외부업체를 활용할 수 있다.

③ 연1회 이상 보안감사를 시행하여야 하며, 필요 시 수시 점검을 시행할 수 있다.

④ 보안감사를 실시한 후 발견된 문제점에 대한 개선대책을 수립하여 보완조치를 완료하고, 그 결과를 정보보안 담당관에게 보고하여야 한다.

제7장 정보보안 교육

제22조(정보보안 교육) ① 정보보안 관리자는 연간 정보보안 교육계획을 수립하여야 하며, 연1회 이상 본교 교직원 및 관련 외부자를 대상으로 정보보안 교육을 시행하여야 한다.

② 정보보안 담당자는 정보보안 담당관의 승인을 얻어 교육시기, 기간, 대상, 내용, 방법이 포함된 교육 계획을 수립하여야 한다.

③ 정보보안 담당자는 교육 시행 후 결과를 문서화하여야 하며 교육 효과와 적정성을 평가하여 다음 교육 계획에 반영한다.

제8장 정보보안 활동

제23조(보안성 검토) ① 정보통신망 및 정보시스템의 신·증설 시 시스템의 성능 및 보안에 미치는 영향을 사업 계획단계에서 검토하여야 한다.

② 정보시스템 단순 교체 등 사안이 경미하다고 판단하는 경우에는 보안성 검토를 생략할 수 있다.

제24조(정보서비스 현황 및 흐름분석) ① 관리체계 전 영역에 대한 정보서비스 현황을 식별하고 업무 절차와 흐름을 파악하여 문서화한다.

② 정보보안 담당자는 서비스 및 업무, 정보자산 등의 변화에 따른 업무절차를 주기적으로 검토하여 관련 문서의 최신성을 유지하도록 관리한다.

제25조(정보자산 관리) 주요 정보자산 식별, 각 자산의 중요도 평가 수행, 접근권한 관리, 위협 및 취약점 분석 수행, 위험평가를 다음 각 호와 같이 수행하고 보호대책을 관리하는 등 정보자산을 관리하여야 한다.

1. 정보시스템을 포함한 주요 정보자산을 연1회 이상 식별하고 관리한다.
2. 정보자산에 대한 접근권한의 타당성을 주기적으로 점검하고 관리하여야 한다.
3. 정보자산에 대한 위험평가를 연1회 이상 수행하고 보호대책을 수립하여 이행하여야 하며, 미이행 시 보완대책을 포함한 이행결과를 정보보안 담당관에게 보고하여야 한다.

제26조(정보시스템 보안) 정보시스템의 안정적인 운영을 위하여 다음 각 호와 같은 활동을 수

행하여야 한다.

1. 주요 정보시스템의 보안성 검증, 운영관리, 접근통제, 패치, 로그 감사, 백업 등 보안 관리를 수행한다.
2. 주요 정보시스템의 정기적 취약점 점검을 수행하고 발견된 취약점을 제거한다.
3. 저장매체의 폐기 또는 재사용 시 처리 절차를 수립하여 중요정보의 유출을 방지한다.
4. 중요정보의 전송 및 저장 시 정보의 유출을 방지하기 위하여 암호화 적용 및 암호통제를 수행한다.
5. 비인가자의 접근을 방지하기 위하여 정보시스템 영역별로 접근통제를 수행한다.

제27조(응용프로그램 개발보안) 응용프로그램의 개발, 유지보수 및 운영에 필요한 보안사항을 정하고 운영·관리함으로써 정보자산을 안전하고 효율적으로 보호하여야 한다.

제28조(물리적 보안) 정보자산의 안전한 유지와 보호를 위해 각 호와 같은 물리적 보안활동을 수행하여야 한다.

1. 통제구역, 제한구역 등 물리적 보호구역을 설정 및 관리한다.
2. 각 보호구역별로 출입통제를 하고 출입기록 및 출입권한을 주기적으로 검토한다.
3. 중요정보가 저장된 저장매체는 파기 또는 재사용 시 중요정보의 유출을 방지하도록 관리한다.

제29조(침해사고 대응) 침해사고 발생 시 효율적인 처리 및 복구를 위한 대응체계를 갖추어 피해를 최소화하고, 업무수행 및 서비스 제공의 연속성을 확보하여야 한다.

② 정보보안 담당부서는 침해사고 발생 시 신속한 대응을 위하여 침해사고대응팀을 구성·운영할 수 있고 비상연락체계를 수립하여야 한다.

제30조(침해사고 보고) ① 본교 교직원은 침해사고 징후 또는 발생을 인지한 경우 이를 즉시 정보보안 담당부서에 보고하여야 한다.

② 정보보안 담당부서는 침해사고 발생 시 그 내용을 기록하고 처리 결과를 정보화추진위원회에 보고하여야 한다.

제31조(재해복구) ① 재난 발생 시 최소한의 주요 업무 연속성 확보를 위한 재해복구계획을 수립하여야 한다.

② 환경 및 업무 변화에 따라 정기적으로 재해복구계획을 시험하고 변경관리를 수행하여야 한다.

제9장 기타

제32조(준용) 기타 이 규정에 명시되지 아니한 사항은 다음 각 호의 법령에 따른다.

1. 「개인정보 보호법」및 동법 시행령
2. 「교육부 정보보안 기본지침」

부칙(2016. 9. 23. 제정)

제1조(시행일) 이 규정은 공포일부터 시행한다.

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

부칙(2019. 4. 4. 전문개정)

본 규정은 공포한 날부터 시행한다.

부칙(2020. 8. 19. 개정)

이 규정은 공포한 날부터 시행한다.