정보보안 규정

시행: 2022. 06. 13.

제1장 총칙

제1조 (목적) 본 규정은 경희대학교(이하 '본교'라 한다) 정보보안 관리체계의 수립 및 운영과 정보통신망의 안정성과 정보보호를 위해 필요한 사항을 규정함을 목적으로 한다.

제2조 (용어 정의) 본 규정에서 사용하는 용어의 정의는 다음과 같다.

1. "정보자산"이란 본교 내·외에 서비스를 제공하기 위해 정보의 수집·가공·저장·검색·송수신에 사용되는 서버·PC 등 단말기, 보조기억매체, 전산·통신장비·정보통신기기, 응용프로그램 등 정보시스템과 정보시스템의 운영·관리에 필요한 시설, 전자정보 등 본교 자산을 총칭한다.
2. "정보시스템"이란 PC·서버 등 단말기, 보조기억매체, 전산·통신장치, 정보통신기기, 응용프로그램 등 정보의 수집·가공·저장·검색·송수신에 필요한 하드웨어 및 소프트웨어 일체를 말한다.
3. "사용자"란 본교 전산망 및 전산자원을 사용하는 업무 담당자, 시스템 관리자 및 정보서비스를 이용하는 구성원을 말한다.
4. "정보보안" 또는 "정보보호"라 함은 정보통신 수단으로 수집·가공·저장·검색·송수신되는 정보의 유출, 위변조, 훼손 등을 방지하거나 정보자산을 보호하기 위하여 강구하는 관리적, 물리적, 기술적 수단 일체의 행위를 말한다.
5. "보안사고"란 외부 또는 내부의 악의적인 사용자에 의한 비 인가된 시스템 사용, 사용자 계정의 도용, 악성코드(웜, 바이러스 등) 유입 및 실행, 정보시스템방해 등 시스템의 서비스를 왜곡 또는 지연시키거나 정보자산을 유출, 파괴하거나 데이터를 변조, 삭제하는 등의 일체의 행위를 말한다.
6. "전산망"이란 각종 정보시스템을 통신회선으로 연결하여 자료를 처리·보관하거나 전송하는 조직망을 말한다.

제3조 (적용 대상 및 의무) ① 본교의 교원, 직원 및 보조인력(용역인력 포함)과 학생(이하 "구성원"이라 한다)에게는 본교 내에서 자신이 속하는 소속(부서)의 정보자산, 시설과 기기에 대하여 본 규정과 본 규정에 따른 지침을 준수할 의무가 있다.

② 각 기관(부서)의 장(이하 "부서장"이라 한다)에게는 관할 부서에서 생산, 가공, 유통, 관리, 파기되는 정보자산 및 다른 부서 또는 외부에 접근이 허용된 정보자산에 대하여 보안책임이 있다.

제4조 (준수 확인) ① 사용자가 본 규정을 위반하면 관련 법규 및 내부 규정에 따라 징계할 수 있으며, 사안에 따라서는 고발 조치할 수 있다.

② 사용자가 본 규정을 위반하여 본교에 재산상의 손실을 입히거나 이미지를 훼손시킬 경우에는 민·형사상의 모든 책임을 진다.

제2장 정보보안위원회

제5조 (구성) ① 체계적・효율적 보안정책의 수립・심의를 위하여 정보보안위원회(이하 "위원회"라 한다)를 둔다.

② 위원회는 정보보안담당관, 서울·국제캠퍼스 교무처장, 서울·국제캠퍼스 총무관리처장, 인사처장의 당연직 위원과 위원장의 추천으로 총장이 임명하는 전문직 위원으로 구성한다.

③ 위원회 위원장은 정보보안담당관으로 한다.

④ 위원회의 간사는 정보처 보직자 중 위원장이 임명하며, 위원회의 제반 사무를 처리하고 회의록을 작성하여 보관한다.

⑤ 위원회 회의는 연 1회 이상 실시하고 그 결과를 기록·관리하여야 한다.

제6조 (기능) ① 본 위원회는 다음 각 호의 사항을 전문적으로 심의 및 의결한다.

1. 정보보안 정책·규정 및 대책 수립에 관한 사항
2. 정보보안 신규 추진 사업 및 연간계획 수립에 관한 사항
3. 정보보안 위반자 심사 및 처리에 관한 사항
4. 주요 정보보안 이슈 대책 및 사업에 관한 사항
5. 중대 정보보안 침해사고에 대한 검토, 평가 협의 및 결정에 관한 사항
6. 정보보호 관리체계 관련 환경 변화 검토 및 개선 사항
7. 기타 위 각호에 부수되는 제반 사항

제7조 (임기) ① 위원장 및 간사의 임기는 보직재임기간으로 한다.
② 전문직 위원의 임기는 2년으로 하되 연임할 수 있다.
③ 위원의 임기 중 결원이 생겼을 때에는 신규로 위촉하되, 그 임기는 전임자의 잔여기간으로 한다.

제8조 (회의소집) 위원장은 제6조의 심의 안건이 있는 경우 위원회를 소집한다.

제9조 (의결) 위원회 회의는 재직위원 과반수의 출석과 출석위원 3분의 2 이상의 찬성으로 의결한다.

제3장 정보보안 조직

제10조 (정보보안담당관) ① 본교의 효율적인 정보보안 업무를 수행하기 위하여 '정보보안담당관'을 둔다.
② 정보보안담당관은 정보처장으로 한다.
③ 정보보안담당관은 정보처 정보기획팀장을 정보보안관리자로 선임할 수 있으며, 정보보안 활동에 필요한 업무를 지시할 수 있다.

제11조 (정보보안 활동) 정보보안담당관은 정보보안를 위하여 다음 각 호의 정보보안 활동을 수행하여야 한다.

1. 정보보호 관리체계의 수립 및 관리·운영
2. 정보보안 취약점 분석·평가 및 개선
3. 침해사고의 예방 및 대응
4. 정보보안을 위한 사전 대책 마련 및 보안조치 설계·구현 등
5. 정보보안 관련한 사전 보안서 검토
6. 중요 정보의 암호화 및 보안서버 적합성 검토
7. 그 밖에 본교의 정보보안을 위하여 필요한 조치의 이행

제12조 (정보보안 조직의 구성 및 운영) ① 본교의 정보보안 조직은 위원회, 정보보안실무협의회, 정보보안담당관, 정보보안관리자, 정보보안담당자 등으로 구성하여 체계적으로 운영하도록 한다.
② 정보보안 조직의 구성 및 운영에 관한 세부 사항은 '정보보안 조직 지침'을 따른다.
③ 위원회의 기능은 사안에 따라 정보보안담당관의 승인으로 정보보안실무협의회에 위임하여 심의·의결할 수 있다.

제4장 정보보안 준수

제13조 (기본수칙) ① 사용자는 계정 및 패스워드의 기밀을 유지해야 하며, 본래의 목적으로만 사용하여야 한다.
② 사용자는 정보시스템의 사용권한이 부여된 영역에 대하여 본래의 목적으로만 사용하여야 한다.

③ 사용자는 정보시스템의 성능저하 및 보안상 위험을 초래할 수 있는 행위를 해서는 안되며 위험을 초래할 수 있는 행위를 발견한 경우에는 소속부서의 장 또는 정보보안담당자에게 즉시 알려야 한다.
④ 사용자는 정보시스템과 연관된 저작권·특허권 및 소프트웨어 라이선스의 사용 조건을 숙지하고 이를 준수하여야 한다.
⑤ 본교 내 전산망을 신설·변경 및 폐기하고자 하는 경우에는 정보보안담당관의 사전승인을 얻어야 한다.
⑥ 외부 전산망에서 본교 내 전산망으로의 접근은 본교에서 원칙적으로 허용하지 아니한다. 단, 필요시 적법한 절차에 따라 승인된 경우에 제한적으로 허용할 수 있다.
⑦ 정보자산(정보시스템, 정보보호시스템, 정보)은 보안등급에 따라 분류·관리한다.
⑧ 정보보안관리자는 주기적인 보안점검을 통해 본교 전산망 및 정보시스템의 안전성을 점검하여 정보보안 규정 등의 준수 여부를 평가하고 필요한 조치를 취할 수 있으며 모든 사용자는 이에 적극 협조하여야 한다.
⑨ 업무와 관련해 습득한 정보자산을 본교의 허가 없이 외부에 누출해서는 아니되며, 정보보안 관련 사고의 책임은 원칙적으로 사용자 본인에게 있다.
⑩ 보안사고 예방을 위한 정보보안 활동은 정보보안담당관의 승인을 얻은 후 즉시 시행할 수 있다.

제14조 (정보보안 규정 등의 입안) ① 정보보안 규정의 제·개정 시 위원회의 심의를 거치며 『제규정관리규정』 제5조(제정 및 개·폐 절차)에 따라 시행한다.
② 정보보안 업무의 수행을 위하여 하위 지침을 제정할 수 있으며, 지침의 제·개정 시 위원회의 심의를 거쳐 정보보안담당관의 승인을 받아 시행한다.
③ 제2항의 경우에 다음 각 호의 어느 하나에 해당하고 시급성이 인정되는 경우에는 위원회의 심의를 생략할 수 있다.
1. 대내외 감사 관련 조치
2. 상위 법령의 개정에 따른 긴급한 지침 개정

제15조 (정보보안 규정의 준수) ① 사용자는 본 규정을 숙지 및 준수하여야 하며 담당 업무에 적용하여야 한다.
② 사용자가 본 규정 또는 하위 지침을 위반하여 본교에 손실을 입히거나 이미지를 훼손한 경우에는 제4조에 따라 위반자를 징계할 수 있다.

제16조 (정보보안 규정 및 지침의 관리) ① 정보보안 환경 및 정보보호 관리체계의 변화에 따라 필요한 지침을 수립하고 개선하여야 한다.
② 규정 및 지침의 제정, 개정, 배포(시행), 폐기 등의 이력을 관리하여야 한다.
③ 다음 각 호의 사항을 고려하여 연 1회 이상 규정의 변경 필요 여부를 검토하고, 필요시에 규정 및 지침을 변경할 수 있다.
1. 정보보안 목표 및 전략의 변경
2. 정보보안 관련 조직 구조 및 인력의 중대한 변경
3. 중대한 보안사고 또는 새로운 위협·취약성이 발생한 경우
4. 관련 법 요구의 변화 또는 신규 법령의 제정
5. 정보보안 규정 등의 정책 시행 문서간의 일관성 유지를 위한 변경
6. 그 밖에 추가적으로 필요하다고 판단하는 경우
④ 정보보안 규정에서 요구하는 정보보안 수준 유지를 위해 연간 정보보안 업무계획을 수립·시행하고 그 추진결과를 심사·분석 및 평가하여야 한다.
⑤ 정보보안 업무계획의 효과적인 관리를 위해서 '정보보호 운영현황표'를 작성하고 검토하여 최신의 상태가 유지되도록 관리하여야 한다.
⑥ 정보보안 규정을 통하여 정한 정보보안 활동 수행에 관한 운영 기록을 관리하여야 한다.

제5장 정보보안 관리

제17조 (자산분류 및 통제) ① 정보자산에 대한 최신 목록을 유지하고 관리하여야 한다.
② 정보자산의 보호를 위해 보호대책을 마련하고 적용하여야 한다.
③ 관리되는 정보자산은 정보의 중요도를 고려하여 보안등급을 정하여야 한다.
④ 자산분류 및 통제 업무에 관한 세부 사항은 「정보자산관리 지침」으로 정한다.

제18조 (위험평가) ① 서비스 및 업무에서 발생이 예상되는 위험을 평가하고 위험관리 전략을 수립하여 통제하여야 한다.
② 본교에서 발생 가능성이 있는 정보보안 위험은 지속적으로 평가되고 관리되어야 한다.
③ 위험평가에 관한 세부 사항은 「위험평가관리 지침」으로 정한다.

제19조 (인적 보안) ① 교직원에 대한 인사관리 업무상 발생 가능한 정보보안 위험을 식별하고 대책을 적용하여야 한다.
② 외부인력에 의해 발생 가능한 정보보안 위험을 식별하고 대책을 적용하여야 한다.
③ 정보보안 담당부서는 연 단위의 정보보안 교육 및 훈련계획을 수립하고 이를 시행하여야 한다.
④ 교직원은 매년 시행되는 정보보안 교육을 이수하여야 한다.
⑤ 인적 보안에 관한 세부 사항은 「인력보안 지침」 및 「외부인력보안 지침」으로 정한다.

제20조 (물리적 보안) ① 업무상 보호되어야 하는 구역을 제한구역 또는 통제구역으로 구분하여 관리하여야 한다.
② 정보 및 정보자산에 대한 비인가 물리적 접근, 유출, 손상으로부터 보호하기 위한 대책을 적용하여야 한다.
③ 물리적 보안에 관한 세부 사항은 「물리적보안 지침」으로 정한다.

제21조 (네트워크 및 운영관리) ① 정보시스템의 운영과정에서 발생하는 보안 위협을 예방하고 통제하여야 한다.
② 정보시스템의 신규 도입, 운영 및 폐기 단계에서 보안성을 확보하여야 한다.
③ 네트워크상에서 전송되는 중요 정보에 대한 기밀성, 무결성, 가용성 보장을 위하여 적절한 통제 대책을 수립하여 적용하여야 한다.
④ 매체에 저장된 중요 정보의 보호를 위하여 안전한 보관 및 폐기 관리를 수행하여야 한다.
⑤ 정보시스템 운영보안에 관한 세부 사항은 「정보시스템 운영보안 관리지침」으로 정한다.

제22조 (보안사고 예방 및 대응) ① 본교에서 발생 가능한 보안사고를 사전에 예방하고 대응할 수 있는 통제 대책을 수립하여 운영하여야 한다.
② 보안사고 대응을 위한 조직을 구성하고, 대응책을 수립하여 적용하여야 한다.
③ 보안사고를 인지한 교직원은 정보처 정보기획팀에 이를 즉시 신고하여야 한다.
④ 보안사고 예방 및 대응 업무에 관한 세부 사항은 「정보보안 침해사고 대응지침」으로 정한다.

제23조 (접근 통제) ① 승인된 사용자만 본교의 정보 및 정보자산에 접근할 수 있어야 한다.
② 정보시스템에 대한 접근통제 정책은 사용자 식별, 인증, 활동기록 등의 보안통제 기능을 통하여 이행되어야 한다.
③ 사용자는 안전한 패스워드 설정 및 관리를 통해 정보시스템 대한 비인가 접근이 불가능하도록 하여야 한다.
④ 정보시스템의 접근통제에 관한 세부 사항은 「정보시스템 운영보안 관리지침」, 패스워드에 대한 세부 사항은「PC보안 지침」으로 정한다.

제24조 (응용프로그램 보안관리) ① 응용프로그램의 신규 개발, 변경 및 폐기 시 보안성 검토가 수행되어야 한다.

② 응용프로그램에서 취급하는 민감한 정보의 전송 및 저장에 관한 세부 사항은 「암호관리 지침」으로 정한다.
③ 응용프로그램의 개발 및 보안관리에 관한 세부 사항은 「개발보안 지침」, 데이터베이스 보안관리에 관한 세부 사항은 「정보시스템 운영보안 관리지침」으로 정한다.

제25조 (IT 재해복구 계획) ① 정보시스템의 복구를 위한 비상계획을 수립하여야 한다.
② 인위적 및 자연적으로 발생되는 긴급사태에 대비하여 백업 및 복구절차를 수립하고 시행하여야 한다.
③ 재해복구에 관한 세부 사항은 「정보시스템 재해복구 관리지침」으로 정한다.

제26조 (법적 요구사항의 준수) ① 본교 업무 운영에 적용되는 법적, 제도적 요구사항을 식별하고 준수하여야 한다.
② 정보보안 규정 및 지침의 준수 여부를 확인하기 위해 주기적 준거성 검토를 수행하고 필요시 감사가 수행될 수 있다.
③ 개인정보보호에 관한 사항은 「개인정보 내부관리계획」을 따른다.

제27조 (정보보안 감사) ① 정보보안 감사를 수행하여 정보보안 활동이 적절히 수행되는지 평가하고 개선사항이 발생한 경우에는 개선하도록 하여야 한다.
② 정보보안 감사에 관한 세부 사항은 「정보보안 감사 지침」으로 정한다.

제6장 기타

제28조 (준용) ① 정보보안에 관하여는 본교의 다른 규정에서 특별히 정한 경우를 제외하고는 본 규정이 정하는 바에 따른다.
② 본 규정에 정하지 아니한 사항은 본교 제·규정을 준용한다.

부 칙
본 규정은 2015년 4월 16일부터 시행한다.

부 칙
본 규정은 2017년 11월 17일부터 시행한다.

부 칙
본 규정은 2019년 3월 28일부터 시행한다.

부 칙
본 규정은 2019년 6월 15일부터 시행한다.

부 칙
본 규정은 2020년 5월 11일부터 시행한다.

부 칙
본 규정은 2021년 7월 13일부터 시행한다.

부 칙
본 규정은 2022년 06월 13일부터 시행한다.