10. 정보보호규정

제 1 장 총 칙

제1조 (목적) 이 규정은 가톨릭꽃동네대학교(이하 ‘본교’라 한다)의 정보자산을 다루는 정보시스템을 내·외부의 위협으로부터 안전하게 보호하여 사용자에게 원활한 서비스를 제공하고자 함을 그 목적으로 한다.(2021.6.22.개정)

제2조 (적용범위와 의무) ①적용범위는 본교의 모든 정보시스템 및 구성원으로 한다.

② 정보보호에 대한 의무는 본교의 전산자원을 사용하는 구성원 모두에게 있으며 정보보호규정을 준수할 의무가 있다.

제3조 (용어의 정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

① “정보자산”이라 함은 정보처리 및 이와 관련된 설비, 소프트웨어, 데이터 등 정보화에 필요한 자원으로써 특정조직에 소유권이 부여된 것을 말한다.

② “정보시스템”이라 함은 PC, 노트북, 스마트폰, 서버, 네트워크시스템 등 정보통신에 이용되는 컴퓨터 기능을 보유한 모든 시스템을 말한다.

③ “전산망” 또는 “네트워크”라 함은 각종 정보시스템을 통신회선으로 연결하여 자료를 처
리·보관하거나 전송하는 조직망을 말한다.

④ “시스템 관리자”라 함은 시스템의 루트(root) 권한을 가지고 시스템을 관리. 운영하는 자
를 말한다.

⑤ “전산자료”라 함은 전산장비에 의해 입력·보관되어 있는 정보자료를 말하며, 백업미디어 등 저장매체를 포함한다.

⑥ “정보보호” 또는 “정보보안”이라 함은 정보통신 수단으로 수집·가공·저장·검색·송수신 되
는 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, 전산자료 보관실 등을 말한다.

⑧ “정보보호 담당부서”라 함은 전산과를 말한다.

제 2 장 정보보호심사위원회

제4조 (구성) ①정보보안의 체계적이고 효율적인 정책을 수립하기 위하여 정보보호심사위원회(이하 “위원회”라 한다)를 둔다.

② 위원회는 제1조의 목적을 달성하기 위하여 다음 각 호의 사항을 심의한다.

1. 정보보안정책 심의와 학내 정보보안의 총 관장
2. 정보보안사고 처리의 책임을 심의·결정
3. 정보보안교육 및 정보보안준수 사항 감사

4. 기타 정보보안관련 제반업무의 총괄

③ 위원회는 본교의 교직원을 포함하여 7인 이내로 구성하며 당연직 위원으로 기획관리처장, 총무차(과)장, 전산과장이 된다. 위원장은 개인정보보호 책임관이 되며 위원은 위원장의 추천으로 총장이 임명한다. 위원의 임기는 보직 재임기간으로 한다. (2019.2.8.개정)

④ 위원장은 위원회의 회무를 총괄하고 위원회를 대표한다.

⑤ 위원회의 회무를 처리하기 위하여 간사 1인을 두며 위원장이 임명한다.

제 3 장 보 안

제5조 (기본 수칙) ① 교·직원 및 학생은 허가받은 정보시스템의 권한이 부여된 영역에 대하여 본래의 목적으로만 사용할 수 있다.

② 정보시스템 사용자는 정보시스템의 성능저하 및 보안상 위험을 초래할 수 있는 행위를 해서는 안 된다.

③ 외부 전산망에서 본교 전산망으로의 접근은 본교에서 승인한 정보시스템을 제외하고는 허용하지 않는다. 단, 필요시 적법한 절차에 의해 요청하여 승인된 경우 제한적으로 허용될 수 있다.

④ 업무와 관련하여 습득한 정보자산을 본교의 허가 없이 외부에 유출해서는 안 된다.

제6조 (보안 점검) 정보보호 담당부서는 교내 정보시스템에 대해 필요시 수시점검을 실시할 수 있다.

제7조 (보안 사고의 처리) 보안사고가 발생할 경우 정보보호 담당부서는 다음 각 항의 단계에 따라 적절한 조치를 취하여야 한다.

① 정보시스템을 수시로 점검하여 침입을 사전에 예방한다.

② 시스템 관리자는 비정상적인 활동이나 징후가 보이면 무단 침입자의 유무 정보자료의 이상 유무를 점검하여야 한다.

③ 전산자료의 손상이 있을 경우 백업자료를 이용하여 즉시 복구한다.

제8조 (보안 교육) 보안 교육은 연 2회 이상 실시한다.

제 4 장 관 리

제9조 (정보시스템 사용자) 정보시스템을 사용할 수 있는 자는 다음 각 항과 같다.

① 본교 교원·직원·재학생 및 졸업생

② 각 부서의 장이 사용을 허가한 자

제10조 (적절성 확보) 사용자가 정보시스템 사용에 있어 다음 각 항에 해당하는 경우에는 부적절한 사용으로 간주하여 제재조치를 취할 수 있다.

① 타 사용자의 계정 및 패스워드를 허가 없이 사용한 경우

② 타 사용자의 자료를 허가 없이 유출하거나 읽고 쓰는 행위

③ 정보시스템 및 타 사용자 계정을 해킹하는 행위

④ 외부의 불법사용자에게 계정 및 패스워드를 제공한 경우

⑤ 보안점검의 지적사항에 대해 즉각적인 시정을 취하지 않는 경우

제11조 (네트워크 관리) ① 인터넷을 이용한 모든 외부접근은 방화벽을 통해서만 접근 가

능 하도록 한다.
② 네트워크 주소는 사용자가 임의로 변경할 수 없다.
③ 정보보호 담당부서는 본교에 유해하거나 불필요하다고 판단되는 웹사이트 접속을 통제할 수 있다.

제12조 (서버 관리) ① 시스템관리자는 서버의 상태(트래픽, 로그, 무단접속 등)를 수시로 확인하고 이상을 발견한 경우 전산과장에게 보고 후 즉시 조치를 취한다.
② 패스워드가 없는 계정은 사용을 금지하며 퇴직자는 즉시 계정을 회수한다.
제13조 (PC 관리) ① 화면 보호기를 작동시켜야 하며 패스워드를 설정한다.
② 자신의 업무에 사용하는 응용 프로그램은 시스템 관리자의 허락 없이 무단으로 타인에게 복사해 주어서는 안 된다.
③ 보조기억매체를 사용할 때 또는 데이터를 전송할 때에는 바이러스 검사를 한다.
④ 중요한 정보는 PC내에 보관하지 않도록 하고, 별도의 보조기억매체(디스켓, USB, CD 등)에 담아 보관한다.
⑤ 정보보호 담당부서는 컴퓨터바이러스 감염 등으로 심각한 피해가 우려되는 경우 게시판이나 메일 등을 통해 경고 메시지 게시 등의 조치를 취한다.
⑥ 본교 전산망을 사용하는 모든 PC는 웜, 바이러스 감염을 예방하기 위해 아래와 같이 조치해야 하며, 정보보호 담당부서는 필요하다고 판단될 경우 이를 강제할 수 있다.
1. 본교 정보보호 담당부서에서 인증한 백신 프로그램을 설치하여야 한다.
2. 설치된 백신 프로그램을 항상 최신 버전으로 유지해야 한다.
3. 정기적인 바이러스 검색을 통해 예방과 치료에 노력해야 한다.
⑦ 외부에서 반입한 보조기억매체(디스켓, USB, CD 등), 인터넷에서 다운로드 받은 파일, 외부로부터 전송된 메일의 첨부파일 등은 실행 또는 열기 전에 반드시 바이러스 검사를 해야 한다.
제14조 (시스템실 관리) ① 출입구에 입실자의 식별이 가능한 출입 보안장치를 설치한다.
② 정전에 대비하여 별도의 전원공급 장비를 설치한다.
③ 온·습도에 민감한 기기의 보호를 위하여 항온습기를 운용한다.

제 5 장 보 칙

제15조 (준용) 이 규정에 정하지 않은 사항에 대하여는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」,「개인정보보호법」, 동법 시행령 및 시행규칙을 준용한다.

부 칙
① (시행일) 이 규정은 2012년 7월 1일부터 시행한다.

부 칙
① (시행일) 이 개정된 규정은 2019년 3월 1일부터 시행한다.

부 칙
① (시행일) 이 개정된 규정은 2021년 6월 22일부터 시행한다.