정 보 보 호 규 정

제정 2012. 7. 1
개정 2022. 6. 13

제1장 총 칙

제1조(목적) 이 규정은 청강문화산업대학교(이하 “본교”라 한다) 내에서 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치 등의 구체적 내용을 정하는 것을 목적으로 한다.

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

① “정보통신서비스”라 함은 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”이라 함은 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”라 함은 정보통신설비 및 시설을 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

④ “이용자”라 함은 정보통신서비스제공자가 제공하는 정보통신서비스를 이용하는자를 말한다.

⑤ “침해사고”라 함은 해킹 및 컴퓨터바이러스의 유포 등으로 인하여 정보시스템의정상적인 운영에 대한 방해, 정보의 유출, 파괴, 위조 및 변조 등이 발생한 사태를 말한다.

제3조(적용대상) 이 규정은 본교가 보유 및 운영하고 있는 정보자산을 이용하는 사용자 및 구성원을 대상으로 한다.

제2장 정보보호 조직

제4조(정보보호조직) ① 정보보호 총괄책임자는 본교의 정보보호업무를 지휘, 감독하며 정보보호 대책 수립, 수행을 총괄하는 책임자는 전자계산소장을 당연직으로 한다.

② 효율적인 정보보호 업무 수행을 위하여 각급 행정부서장과 스쿨원장은 보직 재임기간 동안 자동으로 소속 부서와 스쿨(이하 부서)의 정보보호책임자가 되며, 정보보호 총괄 책임자는 필요시 업무 분야별로 정보보호 담당자를 추가 지정 할 수 있다.

③ 본교를 대표하는 정보보호관련 행정업무는 전자계산소에서 수행한다. 업무 특성상 업무담당 부서에서 수행해야 하는 경우에는 예외로 할 수 있다.

④ 정보보호 총괄책임자 및 담당부서는 정보보호 총괄책임자의 지휘, 감독을 받아 우리 대학교의 정보보호를 위한 임무를 수행한다.

⑤ 정보보호 총괄책임자는 정보보호 계획수립 및 시행, 정보보호 업무 지도감독 및 교육, 정보보호 침해사고 예방 및 대응, 대외협력 업무 등을 총괄한다.

제5조(정보보호위원회) 본교의 정보보호에 대한 사항을 심의 할 수 있는 위원회를 별도로 구성할 수 있으며, 위원회 운영과 관련된 세부사항은 따로 정한다.

제3장 정보자산 운영관리

제6조(기본수칙) ① 정보시스템 사용자는 허용되지 않은 정보에 접근을 시도하거나 사용권한 이외의 활동을 위해 정보보호 기능을 무력화시키는 시도를 해서는 안된다.

② 제 1항의 규정에 언급된 행위를 한 자가 발견된 경우 소속부서의 장은 지체없이 정보보호책임자에게 알려야 하며, 행위자는 그 결과에 대한 책임을 진다.

③ 정보취급자는 업무와 관련해 습득한 정보자산을 외부에 누출해서는 안된다.

제7조(보안점검) ① 정보보호 총괄책임자는 학내에서 운영중인 서버 및 영역별 정보통신망에 대하여 필요시 보안 점검을 실시할 수 있다.

② 정보보호총괄책임자는 보안점검 대상 및 분야를 해당 부서에 통보하고, 해당부서는 보안점검에 필요한 자료 및 제반 요청사항을 준비하여 보안점검에 대비해야한다.

③ 보안 점검을 실시한 경우, 그 결과를 해당 부서에 통보하며 지적 사항에 대하여 소속 부서장은 시정을 하여야 한다.

제8조(정보보호 교육) ① 정보보호총괄책임자는 정보보호에 대한 인식을 제고하고 사용상의 부주의나 고의에 의한 보안 사고를 최소화하기 위하여 구성원을 대상으로 정기적으로 정보보호 교육을 실시한다.

② 정보보호총괄책임자는 필요한 경우 비정기적인 교육을 실시 할 수 있다.

제9조(물리적 통제 및 제한) ① 중요한 정보자산이 배치된 통제구역에는 비인가자의 출입을 엄격히 통제하여야 하며, 출입대장을 비치하여 관리하여야 한다.

② 외부 전산망에서 본교 내 전산망으로의 접근, 내·외부 사용자의 IP할당, 방화벽 포트 허용 및 도메인 사용 신청 등은 적법한 절차에 의해 정보보호 업무 담당부서에 요청하여야 하며, 승인된 경우에 한하여 제한적으로 허용될 수 있다.

제10조(정보시스템의 설치 및 변경) ① 본교의 전산망을 신설·변경 및 폐기하고자 하는 경우에는 문서로 정보보호총괄책임자의 승인을 얻어야 한다.

제11조(정보자산의 매각 및 폐기) ① 하드디스크 등의 저장장치가 부착된 하드웨어(서버, 스토리지, PC 등) 또는 외장형 저장장치 등은 매각이나 폐기 시, 소속 부서장의 책임하에 분리하여 별도 파기

하거나 기록된 데이터를 삭제하고 포맷하여야 하며, 필요한 경우 물리적으로 완파하여야 한다.

② 본교의 중요 정보화기기의 폐기장비 반출이나 매각 시에는 소속 부서장이 사전에 정보보호총괄책임자에게 통보하여야 한다.

제4장 외부자 정보접근

제12조(외부자의 의무) ① 본 대학의 정보자원에 접근하는 외부자는 본교에서 규정하는 정보보호에 대한 책임과 의무를 가진다.

② 업무 주관부서의 부서장은 외부자에게 정보보호 규정 및 사고 시 보고 절차 등을 명확히 공지하고, 외부자는 이를 숙지하여야 한다.

제13조(외부자 접근통제) ① 외부자는 업무 주관부서에서 승인한 직무에 필요한 정보 만 접근할 수 있도록 하여야 한다.

② 업무상 부득이한 경우를 제외하고 주요 시스템의 접근이 제한되도록 한다.

③ 업무 주관부서로부터 특별한 허가를 받지 않는 한, 본교에서 취득한 어떤 정보자산도 외부자가 보유해서는 아니된다.

제14조(외부자 보안관리 역할 및 책임) ① 본교의 정보자산을 사용하는 외부업체와 계약 시 소속 부서장은 보안 각서를 받아야 하며, 계약서에 정보보호관련 요구사항을 명시하여야 한다.

② 개인정보의 위험성이 크거나 침해가능성이 있는 경우 정보보호총괄책임자는 업무주관 부서장에게 외부로 제공되는 정보자원 목록을 요구할 수 있다.

③ 정보보호총괄책임자에게 사전 통보하지 않은 정보보호관련 문제가 발생할 경우 업무 주관부서에 모든 책임이 있다.

제15조(위배사항의 처리) 계약상의 정보보호 요구사항과 관련하여 외부자의 위배사항 이 발생할 경우 업무주관부서에서는 계약서 및 관련 법률에 따라 제도적, 법적 대응책을 강구하여야 한다.

제5장 사용자의 책임과 의무

제16조(컴퓨터 사용자의 책임) 컴퓨터의 운용 및 관리에 있어서 고의나 부주의 또는 직접적인 실수에 의한 정보보호 사고 발생 시 각 컴퓨터의 해당 사용자가 그 책임을 진다.

제17조(필수 소프트웨어 설치 및 설치 제한) ① 본교의 인터넷망을 이용 할 경우에는 바이러스백신 프로그램 및 보안관련 프로그램을 반드시 해당 컴퓨터에 설치하여야 한다.

② 본교의 정보자산을 침해하거나 보안장비를 무력화 할 수 있는 하드웨어나 소프트웨어를 임의로 설치해서 사용하는 경우 해당 사용자는 모든 책임을 진다.

③ 정보보호총괄책임자는 본교의 정보시스템, 보안장비, 통신망 등의 운영 및 안전한 정보 서비스

제공에 방해를 하는 사용자를 대상으로 IP회수, 방화벽 차단, 사용 시스템의 로그인 차단, 네트워크 격리 등의 조치를 취할 수 있다.

제18조(불법소프트웨어 사용 제한) ① 컴퓨터 사용자는 사용이 승인된 정품 소프트웨어만을 사용해야 하며, 불법소프트웨어를 사용한 경우 그 사용자 및 소속 부서장은 일체의 책임을 진다.

② 불법 소프트웨어 사용을 방지하기 위해 다음 각 호를 준수해야 한다.

1. 소프트웨어의 기본용도 외에 불법적인 용도 변경을 금지한다.
2. 캠퍼스통신망 및 인터넷을 통한 불법복제를 금지한다.
3. 제품 키 및 시리얼 넘버의 공유, 도용, 배포, 전송 등의 행위를 금지한다.

제19조(주기적 PC 점검 실시) PC 사용자 및 관리부서는 PC 보안을 위해 주기적으로 바이러스 체크, OS 보안패치 및 업데이트를 실시하여야 하며, 매월 시행하는 "사이버보안 진단의 날" 중점 점검 사항에 대한 PC점검을 부서장 책임하에 수행 한다.

제6장 기 타

제20조(정보보호 정책) 이 규정에 명시되지 않은 정보보호관련 사항일 경우에는 '공공기관의 개인정보보호에 관한 법률'과 '교육기관 정보보호 지침' 등을 준용하여 처리 할 수 있다.

제21조(시행세칙) 이 규정의 운용에 필요한 세부사항은 따로 정하며, 세칙의 종류와 관리에 관한 사항은 정보보호책임관이 별도로 정하여 공지한다.

제7장 보안사고(위규자) 처리 기준

제22조(보안사고) 개인정보유출 및 외부에 공개되어서는 안되는 모든 문서 및 데이터 등에 대해서 유출시 보안위반 행위 및 피해정도에 그 책임을 진다.

제23조(보안사고 처리 기준) ① 보안사고 발생 시 징계 종류 및 범위는 아래와 같이 정의한다.

1. 경고 : 보안위반 행위나 피해정도가 경미하여 유사 보안위반 재발 방지를 위한 처벌
2. 경징계 : 보안위반으로 인한 피해정도가 경미하나 유사 보안위반 재발 방지를 위한 처벌
3. 중징계 : 보안사고 원인을 제공하거나 보안위반으로 인한 피해정도가 심각하여 엄히 책임을 묻는 처벌
4. 사법처리 : 국가공무원법, 국가보안법, 정보통신기반보호법 등 관련 법률에 의한 보안사고 처벌

② 보안사고 발생 시 징계 대상자에 대한 결정은 정보보호위원회 및 직원인사위원회(교원의 경우 교원인사위원회)에서 결정 후 징계위원회에 회부 혹은 가결 할 수 있다.

③ 징계 종류 및 세부사항은 정보보호위원회 및 직원징계위원회(교원의 경우 교원징계위원회)에서 결정되며 최종 징계처리는 총장의 결재를 득한 후 통보한다

부 칙

이 규정은 2012년 7월 1일부터 시행한다.

부 칙(개정 2022.6.13.)

이 규정은 2022년 6월 16일부터 시행한다.