정보보안 내규

제정일 : 2015. 12. 31.
담당부서 : 원주학술정보원 정보통신팀(033-760-2512)

제1장 총 칙

제1조(목적) 이 내규는 연세대학교 원주캠퍼스(이하 '대학교'이라 한다)의 '정보보안규정'에 의거하여 대학교의 정보보안 활동과 효율적인 정보보안 업무 수행을 위하여 필요한 세부사항을 규정함을 목적으로 한다.

제2조(적용범위) 이 내규는 대학교 학칙에 정한 교내 행정조직, 대학(원) 학부, 부속기관, 캠퍼스통신망에 물리적으로 연결하여 정보통신망 자원을 이용하는 기관, 단체 및 개인을 모두 포함한다.

제3조(용어의 정의) 이 내규에서 사용되는 용어의 정의는 다음 각 호와 같다.
1. "정보보호"란 개인정보와 정보보안을 통칭하는 용어로 이 내규에서는 정보보안
2. "위험평가"란 정보자산의 중요도와 정보자산의 기밀성, 무결성, 가용성 측면에서의 취약점 수준에 따라 위험 크기를 측정하고, 위험도를 산출하는 행위를 말한다.
3. "기밀성"이라 함은 비인가자가 정보를 사용하거나 비인가자에게 정보가 노출되지 못하도록 하는 특성을 말한다.
4. "무결성"이라 함은 비인가 된 방법을 통해 정보를 변경 또는 파괴하지 못하도록 하는 특성을 말한다.
5. "가용성"이라 함은 권한을 가진 개체의 요구에 따라 정보자산을 지속적으로 접근하고 사용이 가능하도록 하는 특성을 말한다.
6. "위험평가결과보고서"란 취약점 분석 결과를 바탕으로 위험 등급에 따라 평가한 결과를 말한다.
7. "적용성보고서(Statement of Applicability)"란 위험평가와 위험처리 프로세스 및 결론에 근거하여 대학교의 정보보호관리 체계에 적용 가능한 통제목표 및 통제항목을 기술한 문서를 말한다.
8. "위험관리계획서"란 적용성보고서에 의하여 구체적인 위험관리 방안을 나타 낸 보고서를 말한다.
9. "시스템"이라 함은 지정된 정보처리 기능을 수행하기 위하여 조직화되고 규칙적으로 상호 작용하는 하드웨어와 소프트웨어의 집합물로 서버, 네트워크, PC, DB 등을 포함한다.
10. "응용프로그램(Application Program)"이라 함은 대학교 구성원 또는 외부 기

관에 의하여 제작된 프로그램 또는 응용 소프트웨어(어플리케이션)를 구현하는 프로그램을 말한다.
11. “응용시스템(Application System)”이라 함은 특정 업무나 목적을 위하여 만들어진 응용프로그램들의 집합과 그와 관련된 하드웨어의 집합을 말한다.
12. “침해사고”라 함은 악성코드 감염, 해킹, 서비스 방해 등의 공격행위에 의한 정보통신망(네트워크) 또는 정보시스템의 기능저하, 데이터 변조 또는 유출 등의 사고를 말한다.

제2장 정보보안 조직

제4조(역할과 책임) 정보보안 조직은 ‘정보보안규정’ ‘제2장 정보보안 조직’의 내용을 기본적으로 준수한다.
① 대학교의 정보보안 책임자는 원주학술정보원장이 겸임한다.
② 대학교의 정보보안 담당부서는 원주학술정보원 정보통신팀이 되고 정보보안 업무를 총괄하는 부서로서 다음 각 호의 역할을 수행한다.
1. 정보보안 계획 이행 및 예산 수립
2. 정보보안 관련 규정의 관리
3. 정보보안 시스템 운영 및 관리
4. 정보보안 위험평가 및 정보보안 감사 활동
5. 정보보안 교육 및 훈련 업무
6. 대외 정보보안 업무의 실무창구
7. 기타 정보보안 제반 사항에 대한 업무
③ 정보보안 실무를 담당하는 정보보안 실무 관련자로는 정보보안 관리자, 정보보안 담당자가 있으며 각 호의 역할은 ‘정보보안규정’ 에 따른다.
④ 각 기관 및 부서별 정보보안 및 IT 실무를 담당하는 정보보안 실무 관련자로는 정보분임 관리자, 정보분임 담당자가 있으며 각 호의 역할은 다음과 같다.
1. 정보분임 관리자는 단위조직의 장으로 정보보안 책임자의 지휘, 감독을 받아 소속 부서 내에서 정보보안 실무 및 IT관련 업무를 관리감독 하는 등의 역할을 수행한다.
2. 정보분임 담당자는 단위조직의 장의 명을 받아 정보보안 실무를 담당하는 자로 정보분임 관리자의 지휘, 감독을 받아 현업 부서에서 정보보안 실무 및 IT관련 업무를 수행한다.

제5조(정보보안 조직) ① 정보보안규정에 의거하여 매년 정보보안 책임자, 정보보안 관리자, 정보보안 담당자를 지정 또는 갱신하여 문서화 한다.
② 정보보안 책임자는 TF조직의 조직도와 사무분장표 등을 제작하고 전담인원에 대한 정보보안 임무 및 역할을 문서화 한다.

제3장 정보보안정책 및 활동

제6조(세부추진 계획수립) ① 정보보안 담당자는 사이버안전 대책을 포함한 해당 년도 정보보안 세부추진 계획을 1분기에 수립하여 정보보안 관리자, 정보보안 책임자에게 보고하고 문서화 한다.
② 정보보안 책임자 및 정보보안 관리자는 세부추진 계획에 대한 추진사항, 건의사항 등을 심사분석 및 평가하여 문서화 및 보관한다.
③ 정보보안 책임자 및 실무자는 전년도 보안평가를 기반으로 개선방안을 수립 및 시행한다.
④ 정보보안업무 세부추진 계획에는 활동목표, 기본방침, 세부추진계획, 보안감사 시 지적사항과 조치계획 등의 내용을 포함한다.
⑤ 정보보안 업무 심사분석 시 총평, 주요성과 및 추진사항, 세부사업별 실적 분석 및 부진(미진) 사업, 애로 및 건의사항, 기타 정보통신망 및 검증필 정보보호시스템 운용현황 등의 내용을 포함한다.

제7조 (정보보안 활동) ① 정보보안 담당자는 매달 '사이버보안진단의 날'에 캠퍼스통신망 자원을 사용하고 있는 모든 PC에 대해 월별중점 점검사항을 점검하고, 문제점 및 미비점을 조치한다. ('사이버보안진단의 날'은 매월 세 번째 수요일로 정하고, 대학교 행사나 부득이 시행이 어려운 경우는 세 번째 주중에 시행한다.)
② 시스템 관리자는 담당 시스템에 대한 정보보안 활동내용을 정보보안 담당자에게 매월 보고한다.
③ 시스템 관리자가 변경될 시 정보보안 실무자에게 보고하고 '보안업무규정 시행내규'에 따라 조치한다.

제4장 위험평가 및 관리

제8조(취약점진단 실시) ① 정보보안 관리자는 대학교의 정보자산 관리대장의 정보자산 중요도 등급 중 등급이 높은 대상을 선정하여 취약점 진단을 실시한다.
② 정보보안 관리자는 관리체계 진단, 서버 진단, 네트워크 진단, 모의해킹, 물리적 취약점 진단 및 응용프로그램 진단 등 6개 분야에 대한 취약점 진단을 실시한다.
③ 정보자산에 대한 취약점 진단은 정기적으로 실시하는 것을 원칙으로 하며 대학교 환경에 중대한 변화가 발생되었을 경우에는 별도 실시할 수 있다.
④ 정보보안 관리자는 정보자산 별로 파악된 취약점 점검 결과를 근거로 다음 각 호와 같은 사항이 포함된 취약점진단 결과보고서를 작성하여 정보보안 책임자에게 보고한다.

1. 정보자산관리 목록
2. 정보자산 중요도 평가표
3. 취약점 진단 결과

제9조(위험평가 실시) 정보보안 관리자는 취약점진단 결과보고서를 바탕으로 다음 각 호의 사항이 포함된 위험평가를 실시하고, 위험평가결과보고서를 작성하여 정보보안 책임자에게 보고한다.
1. 위험평가 점검리스트 내용
2. 각 영역 별 잠재위험 평가기준
3. 각 영역 별 노출위험 평가기준
4. 각 영역 별 위험평가 결과

제10조(위험관리 절차) 정보보안 관리자는 위험평가결과보고서에 의하여 다음 각 호의 위험관리 절차를 수행한다.
① 위험평가결과보고서를 바탕으로 수용가능 위험수준을 정하여 관리대상 위험을 식별하여 적용성보고서를 작성한다.
② 적용성보고서에 의하여 위험관리계획서를 작성하여 정보보안 책임자에게 보고한다.
③ 위험관리계획서에 의하여 취약점진단 결과 및 위험평가 결과를 해당 단위조직으로 통보한다.

제11조(사후 관리) 정보보안 관리자는 위험관리계획서에 따라 단위조직에서 위험관리가 적절히 이루어지고 있는지를 점검하고 그 결과를 정보보안 책임자에게 보고한다.

제5장 인사보안 및 보안교육

제12조(인사보안) 직원 퇴직의 경우 보안서약서를 작성하고, 관계자는 퇴직자의 정보자산, 업무자료반납 등을 점검하여 기록한다.

제13조(보안교육) ① 정보보안 관리자는 교육관련 주무부서의 시행기준에 따라 정보보호와 관련된 업무 종사자에게 정기적 또는 비정기적 교육을 실시하고, 참석을 의무화한다. 또한 해당 교육에 대한 참석확인서, 사진, 인정서류 등을 보관한다.
② 제1항에 의한 비정기 교육 중 신규 임용직원 및 전입자에 대하여는 임용 후 2주 이내 정보보안 교육(개인정보보호 포함)을 실시하는 것을 원칙으로 한다.
③ 정보보안 담당자는 년 2회 이상 15시간 이상의 정보보안 교육(개인정보보호 포함)을 이수해야 한다.

제6장 외부자 정보보안

제14조(외부업체 보안관리) 외부업체와의 계약 시 정보보안규정' '제30조(계약 시 정보보안 요구사항)'를 준수하되 요구조건에 '용역사업 참여자의 임의교체는 불허한다'라는 항목을 추가한다. 만약 부득한 경우로 참여자의 교체가 필요한 경우 비밀유지계약서 및 보안서약서 작성 후 계약담당자와 논의하여 처리한다.

제7장 시스템 보안관리

제15조(응용보안 기능의 설계) ① 응용프로그램을 구축하는 경우 개발 시점부터 프로그램 자체 또는 사용환경에서 이미 알려진 보안취약점을 고려하여 다음 각 호의 보안 기능을 설계한다.

1. 관리자 모듈과 일반 사용자 모듈은 분리한다.
2. 사용자 계정은 개발자 별로 부여하는 것을 원칙으로 하며, 사용자 화면상에 패스워드와 같은 민감한 정보가 평문으로 보이지 않도록 한다.
3. 응용프로그램 상에 생성되는 개발자의 사용자계정에 대하여 접근권한 부여와 접근통제가 가능하도록 한다.
4. 중요한 응용프로그램의 경우 관리자와 사용자의 활동에 대한 사용로그를 생성하여 보안사고 발생 시 증거자료로 활용할 수 있도록 한다.

② 응용프로그램의 안전성 및 보안성 확보를 위해 행정자치부장관이 정하는 "소프트웨어 개발보안 가이드"를 준수하고, 소스코드 등의 보안취약점을 점검하고 제거한다.

제8장 보안시스템 보안

제16조(인증) ① 보안시스템 인증은 '정보보안규정' '제61조'를 준수하되 관리자 계정은 디폴트계정(admin, administrator 등)은 모두 삭제하고 새로운 계정을 할당하여 사용해야 한다.

② 인증을 위한 관리자 비밀번호는 영문자, 숫자, 특수문자가 혼용된(모두 사용) 최소 10자리 이상으로 설정한다.

제17조 (로그 관리 및 분석) 보안시스템의 로그 관리 및 분석은 '정보보안규정' '제63조'를 준수하되 로그는 최소 6개월 보관해야 한다.

제9장 PC보안

제18조(필수 소프트웨어 설치 및 설치 예외) ① 본 대학교의 캠퍼스통신망 자원을 이용하고자 할 경우에는 바이러스백신 프로그램, 패치관리시스템(PMS), PC보안 프로그램을 반드시 해당 PC에 설치하여야 한다.
② 각 개인 PC에 대한 보안점검은 PC보안 프로그램을 통해 매월 1회 정보보안 담당자에 의해 일괄 시행되며 보안점수가 기준점수를 넘지 못하는 PC는 네트워크 격리(IP/MAC주소차단)한다.
③ PC보안 프로그램의 기준 점수는 정보보안 책임자가 정하며 대학교 상황에 따라 유동적으로 정할 수 있다.
④ 특정한 사유에 의해 PC보안 프로그램 설치가 어려운 경우나 패치 또는 보안 업그레이드를 할 수 없는 경우는 'PC보안 프로그램 예외신청서'를 작성 후 정보보안 담당자에게 제출하여 예외처리(IP/MAC주소허용) 하도록 한다.

부 칙

(1) (경과조치) 이 내규 제정 전에 시행된 사항은 이 내규에 의하여 시행된 것으로 본다.
(2) (시행일) 이 내규는 2015년 12월 31일부터 시행한다.