# 정보보안세칙

제정 2012.11. 28
개정 2013. 2. 18
개정 2022. 3. 18

## 제 1 장 총 칙

제1조(목적) 이 세칙은 포항공과대학교(이하 '대학'이라 한다)의 '보안업무규정'에 의거하여 대학의 정보보안 활동과 효율적인 정보보안업무 수행을 위하여 필요한 세부사항을 규정함을 목적으로 한다.

제2조(역할과 책임) ① 정보보안책임자는 대학의 정보보안 업무를 효율적으로 수행하기 위하여 정보보안실무부서와 정보보안실무관련자를 두어야 한다.

② 정보보안실무부서는 대학의 정보보안 업무를 총괄하는 부서로서 다음 각 호의 역할을 수행한다.

1. 정보보안 계획 이행 및 예산 수립
2. 정보보안 관련규정의 관리
3. 정보보안시스템 운영 및 관리
4. 정보보안 위험평가 및 정보보안감사 활동
5. 정보보안 교육 및 훈련 업무
6. 대외 정보보안 업무의 실무창구
7. 기타 정보보안 제반 사항에 대한 업무

③ 정보보안 실무를 담당하는 정보보안실무관련자로는 정보보안관리자, 정보보안담당자, 정보보안분임관리자, 정보보안분임담당자가 있으며 다음 각 호의 역할을 수행한다.

1. 정보보안관리자는 정보보안실무부서의 장으로 대학의 정보보안 실무업무에 대한 관리감독을 수행하며, 정보보안 관련 주요사항을 정보보안책임자에게 보고하는 등의 역할을 수행한다.
2. 정보보안담당자는 정보보안실무부서장의 명을 받아 정보보안 실무를 담당하는 자로서, 수립된 정보보안 계획을 이행하는 등의 역할을 수행한다.

3. 정보보안분임관리자는 단위조직의 장으로 정보보안책임자의 지휘, 감독을 받아 소속 부서 내에서 정보보안 실무를 관리감독하는 등의 역할을 수행한다.
4. 정보보안분임담당자는 단위조직의 장의 명을 받아 정보보안 실무를 담당하는 자로 정보보안분임관리자의 지휘, 감독을 받아 현업 부서에서 정보보안 실무를 수행한다.

제3조(용어의 정의) 이 세칙에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. “정보자산”이란 좁은 의미로는 정보 그 자체만을 의미하지만 넓은 의미로는 그 정보를 포함해 정보를 생성, 가공 및 저장하는 설비를 모두 포함하는 것을 말한다.
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 비 인가된 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. “취약점”이란 웜/바이러스 패치 미적용, 패스워드 및 네트워크 접근 설정의 미흡 등과 같이 정보자산에 직접적인 해는 없으나 정보자산의 손실을 입힐 수 있는 상태를 말한다.
8. “적용성보고서(Statement of Applicability )”란 위험평가와 위험처리 프로세스 및 결론에 근거하여 대학의 정보보호관리체계에 적용 가능한 통제목표 및 통제항목을 기술한 문서를 말한다.
9. “위험관리계획서”란 적용성보고서에 의하여 구체적인 위험관리 방안을 나타낸 보고서를 말한다.
10. “시스템”이라 함은 지정된 정보 처리 기능을 수행하기 위하여 조직화되고 규칙적으로 상호 작용하는 하드웨어와 소프트웨어의 집합물로 서버, 네트워

크, PC, DB 등을 포함한다.

11. “시스템운영자”라 함은 시스템을 운영하고 관리하기 위하여 선임된 운영담당자를 말한다.
12. "응용프로그램(Application Program)"이라 함은 대학 구성원 또는 외부 기관에 의하여 제작된 프로그램 또는 응용 소프트웨어(어플리케이션)를 구현하는 프로그램을 말한다.
13. "응용시스템(Application System)"이라 함은 특정 업무나 목적을 위하여 만들어진 응용프로그램들의 집합과 그와 관련된 하드웨어의 집합을 말한다.
14. “응용시스템운영자”라 함은 응용시스템을 운영하고 관리하기 위하여 선임된 운영담당자를 말한다.
15. “침해사고”라 함은 악성코드 감염, 해킹, 서비스 방해 등의 공격행위에 의한 정보통신망(네트워크) 또는 정보시스템의 기능저하, 데이터 변조 또는 유출 등의 사고를 말한다.
16. “포스텍 침해사고대응조직(POSTECH-CERT : POSTECH Computer Emergency Response Team)”이라 함은 대학 내 침해사고 발생 시 분석 및 대응 절차를 통해 사고 원인 규명 및 대응 조치를 수행하기 위한 조직을 말한다.
17. “보안감사” 란 정보보호를 위해 준수해야 할 보안기준 및 절차들의 이행여부 확인을 위해 다양한 방법으로 증거를 수집하고 분석하여 결과를 보고하는 활동을 말한다.
18. “감사증적”이란 적절한 정책이나 표준에 따라 기록관리가 이루어졌는지를 검사하기 위하여 기록관리 과정에서 행해진 모든 조치를 기록하여 남기는 정보를 말한다.
19. “부적합 사항” 이란 정보보호 정책 및 관련 보안 규정에 정의된 바와 다르게 수행된 사항으로 보안위험을 증가시킬 수 있는 문제점을 말한다.

## 제2장 정보자산관리

제4조(분류 및 등록) ① 정보보안분임관리자는 단위조직 정보자산에 대해서 정보자산코드 및 분류체계(별지 제1호 서식)에 의하여 정보자산을 분류하고 정보자산관리대장(별지 제3호 서식)을 작성하여 보관한다.

② 정보보안분임관리자는 정보자산의 신규, 변경, 폐기 등 정보자산의 변경이 발생 한 경우 정보자산관리대장에 기입하고 그 결과를 7일 이내 정보보안관리자에 통보한다.

③ 정보자산분류기준과 정보자산관리대장은 대학이 보유하고 있는 정보자산의 종류와 유형에 따라 추가 및 삭제될 수 있으며, 변경 시 단위조직에 통보한다.

제5조(중요도 평가 및 등급 분류) ① 정보보안분임관리자는 단위조직 정보자산에 대해서 정보자산 중요도 평가 및 등급(별지 제2호 서식)에 따라 정보자산관리대장에 기록한다.

② 정보자산 중요도 평가기준은 기밀성, 무결성, 가용성 원칙에 따라 각각 1부터 3까지의 값을 평가하여, 매년 정보자산의 중요도를 산정한다.

③ 정보자산 중요도 등급은 중요도 평가수치를 합산한 결과에 따라 VL, L, M, H, VH의 5단계로 구분한다.

제6조(정보자산 관리) ① 정보보안관리자는 단위조직에서 제출한 정보자산에 대한 식별 및 분류의 적절성을 점검하고, 정보자산관리대장을 취합하여 통합 관리한다.

② 정보보안관리자는 단위조직에서 제출한 정보자산의 중요도 평가의 적절성을 점검하고, 중요도 평가와 연계하여 취약점 분석 및 위험 평가를 정기적으로 수행한다.

③ 정보보안관리자는 위험평가 실시 후 분석결과를 단위조직에 통보하여 대학의 정보자산이 적합하게 관리되도록 유지시킨다.

## 제3장 위험평가 및 관리

제7조(취약점진단 실시) ① 정보보안관리자는 대학의 정보자산관리대장의 정보자산 중요도 등급 중 등급이 높은 대상을 선정하여 취약점 진단을 실시한다.

② 정보보안관리자는 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 대학 환경에 중대한 변화가 발생되었을 경우에는 별도 실시할 수 있다.

④ 정보보안관리자는 정보자산 별로 파악된 취약점 점검 결과를 근거로 다음

각 호와 같은 사항이 포함된 취약점진단 결과보고서를 작성하여 정보보안책임자에게 보고한다. 1. 정보자산관리 목록 2. 정보자산 중요도 평가표 3. 취약점 진단 결과

제8조(위험평가 실시) 정보보안관리자는 취약점진단 결과보고서를 바탕으로 다음 각 호의 사항이 포함된 위험평가를 실시하고, 위험평가결과보고서를 작성하여 정보보안책임자에게 보고한다.

1. 위험평가 점검리스트 내용
2. 각 영역 별 잠재위험 평가기준
3. 각 영역 별 노출위험 평가기준
4. 각 영역 별 위험평가 결과

제9조(위험관리 절차) 정보보안관리자는 위험평가결과보고서에 의하여 다음 각 호의 위험관리 절차를 수행한다.

1. 위험평가결과보고서를 바탕으로 수용가능 위험수준을 정하여 관리대상 위험을 식별하여 적용성보고서를 작성한다.
2. 적용성보고서에 의하여 위험관리계획서를 작성하여 정보보안책임자에게 보고한다.
3. 위험관리계획서에 의하여 취약점진단 결과 및 위험평가 결과를 해당 단위조직으로 통보한다.

제10조(사후 관리) 정보보안관리자는 위험관리계획서에 따라 단위조직에서 위험관리가 적절히 이루어지고 있는지를 점검하고 그 결과를 정보보안책임자에게 보고한다.

## 제4장 시스템보안관리

제11조(도입 및 설치) ① 정보보안분임관리자는 시스템 도입 시 장비설치내역을 정보보안관리자에게 통보하여야 하며, 다음 각 호에 해당하는 경우 반드시 보안취약성 점검요청을 하여야 한다.

1. 대학 전체 구성원을 대상으로 서비스를 제공하기 위해 도입되는 시스템
2. 중앙전산실 내에 설치되는 시스템
3. 기타 정보보안관리자가 필요하다고 판단한 경우

② 정보보안관리자는 보안취약성 점검을 수행하여 분석결과를 통보하고 보안설

정 환경을 점검하여야 한다.

③ 시스템운영자는 장비가 설치된 경우 다음 각 호와 같이 기본 보안설정을 하여야 한다.

1. 콘솔(Console)에서 시스템작업을 수행하는 것을 원칙으로 하나 원격접속이 필요한 경우 해당 IP 주소만 허용한다.
2. 시스템운영자 단말 또는 보안이 설정된 장소 이외의 모든 IP 주소는 차단한다.
3. 서비스에 필요한 포트 만 허용하고 그 이외의 포트는 모두 차단한다.
4. 외부기관에 시스템작업을 의뢰하는 경우 해당 IP주소와 서비스 포트만 허용하고, 목적 이외의 사용에 대한 경고 배너를 설정하며, 사용 허용기간이 만료되면 즉시 해당 IP주소 및 서비스 포트를 삭제한다.

제11조의2(정보보안시스템 운영) ① 정보보안관리자는 시스템의 안전한 관리를 위하여 정보보안시스템을 운영할 수 있으며, 정보보안시스템 운영 및 관리 정책을 수리하고 주기적으로 검토한다.

② 정보보안관리자는 정보보안시스템 정책(룰셋 등) 등록, 변경, 삭제 절차를 마련하고, 대학 내•외부 이용자의 정보보안시스템 신청에 대한 검토 기준을 마련한다.

③ 정보보안관리자는 정보보안시스템별 정책(룰셋 등) 등록, 변경, 삭제 요청이 있을 시, 대학 정보보안 및 네트워크 영향성을 검토하여 이를 승인/반려한다.

④ 정보보안담당자는 정보보안시스템별 이벤트를 모니터링하고, 현행 정보보안 시스템 정책의 타당성 및 적정성을 주기적으로 검토한다. (신설: 2022.03.18)

제12조(운영 및 관리) ① 시스템관리용 계정을 생성하여 관리하는 것을 원칙으로 하며, 필요시에만 root 계정을 사용하여야 하고, 중요 보안 패치 및 보안관련 업그레이드는 수시로 적용한다.

② 보안사고 발생 시 증거 추적성을 확보하기 위해 다음 각 호의 로그정보를 3개월 이상 보존하여야 하며 임의 변경하지 않는다.

1. 시스템의 접근내역에 관한 로그 (사용자 계정, 로그온/오프의 날짜/시간)
2. 데이터 및 자원에 대한 모든 접근 시도
3. 패스워드 변경 등과 같은 중요 시스템 명령어의 수행에 관한 로그
4. 시스템 이벤트 로그

③ 시스템 로그정보는 업무용 이외에 공식적인 요청이나 법률에 의한 협조 요

청 없이는 제공할 수 없다.

④ 시스템운영자는 보안사고로 인하여 시스템복구가 불가능한 경우를 대비하여 중요한 데이터를 백업하여야 한다.

⑤ 최초 장비설치 시 용도가 변경된 경우 정보보안관리자에 변경내역을 통보하여야 한다.

제13조(철수 및 폐기) ① 정보보안분임담당자는 장비철수 및 폐기시, 데이터가 저장되어 있는 하드디스크 등의 매체는 분리하여 별도 보관하거나 정보보안관리자에 파쇄 의뢰 후 장비철수 및 폐기를 한다.

② 정보보안분임담당자는 장비철수 및 폐기 후 해당 내역을 전자우편 또는 유선 등의 방법으로 정보보안관리자에 통보한다.

제13조의1(정보시스템 저장매체 불용처리) ① 사용자 및 시스템운영자는 하드디스크 등 전자정보 저장매체를 불용처리(교체・반납・양여・폐기 등) 하고자 할 경우에는 정보보안분임담당자의 승인 하에 저장매체에 수록된 자료가 유출되지 않도록 보안조치 하여야 한다.

② 정보시스템의 사용자가 변경된 경우, 비밀처리에 사용한 정보시스템은 완전포맷 3회 이상, 그 외의 정보시스템은 완전포맷 1회 이상으로 저장자료를 삭제하여야 한다.

③ 정보시스템 저장매체 불용처리 세부절차는 자산관리부서와 별도로 협의하여 시행한다.

④ 전자정보 저장매체의 불용처리에 관한 구체적인 사항은 교육과학기술부「정보시스템 저장매체 불용처리지침」을 따른다. (신설: 2013.2.18)

제14조(보안관리지침) 정보보안관리자는 시스템 관리운영에 필요한 보안관리지침을 정보보안분임담당자에게 제공하며, 세부 보안항목 적용은 보안관리지침을 따른다.

## 제5장 응용시스템보안관리

제15조(개발환경의 분리) 응용시스템은 개발시스템과 운영시스템을 분리하는 것을 원칙으로 하며, 분리가 어려운 경우는 개발환경이 운영환경의 보안에 영향을 주지 않도록 구성한다.

제16조(보안 기능의 설계) ① 응용프로그램을 구축하는 경우 개발 시점부터 프로

그램 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 접근권한부여와 접근통제가 가능하도록 한다.
4. 중요한 응용프로그램의 경우 관리자와 사용자의 활동에 대한 사용 로그를 생성하여 보안사고 발생시 증거자료로 활용할 수 있도록 한다.

② 응용프로그램의 안전성 및 보안성 확보를 위해 행정안전부장관이 정하는 “소프트웨어 개발보안 가이드”를 포함하여 “정보화 용역사업 표준 및 법적 제약사항(별지 제7호 서식)”에서 지정한 정부 중앙부처 및 공공기관의 관련지침 및 가이드라인을 준수하고, 소스코드 등의 보안취약점을 점검하고 제거한다. (개정: 2022.03.18)

제17조(응용시스템 가동) ① 내부 또는 외주로 구축된 응용시스템은 가동 전에 보안취약성 점검을 자체 실시한다.

② 필요 시 보안취약성 점검요청을 할 수 있으며, 정보보안관리자는 보안취약성 점검을 즉시 실시하고 분석결과를 통보하며 보안설정 환경을 점검한다.

제18조(응용시스템 감시) ① 응용시스템운영자는 침해사고가 발생하지 않도록 응용프로그램과 운영환경에 대한 안전성과 신뢰성에 대하여 지속적으로 감시하여야 한다.

② 침해사고 발생시에는 응용시스템의 즉시 가동중단 또는 네트워크 분리 등의 선 조치 후 정보보안관리자에 신고한다.

③ 정보보안관리자는 제6장 침해사고대응에 의하여 침해사고 원인 및 결과를 통보한다.

제19조(응용시스템 외주개발) ① 응용시스템을 외주 개발 시 보안기능의 설계요구사항(별지 제6호 서식)과 외주 용역사의 보안준수사항을 용역제안서 또는 계약서에 반영한다. 단, 외주 용역사의 보안준수사항은 교내 관련 규정으로 정한다. (개정: 2022.03.18)

② 응용시스템의 프로그래밍 보안에 대한 위험요소를 관리하여야 하며 개발된 응용프로그램들이 유출되지 않도록 보안통제를 실시한다.

③ 응용시스템 구축에 참여하는 외주개발자에 대해서 보안서약서를 받아야 한다.

④ 그 외 사항은 일반보안관리세칙 및 교내 관련 규정을 따른다. (개정: 2022.03.18)

## 제6장 침해사고대응

제20조(사고유형) 침해사고 유형의 종류는 다음 각 호와 같다.

1. 서비스 거부공격(DoS), 웜/바이러스 등으로 인한 정보시스템, 네트워크 등의 일부 또는 전체의 서비스가 중단되는 경우
2. 교내 주요 서버 등 정보시스템이 해킹을 당하여 홈페이지 변조 또는 파괴된 경우
3. 연구자료 또는 대학 기밀정보가 저장된 시스템의 해킹으로 인한 정보의 유출
4. 대학 내부의 정보자산이 외부로 공격을 시도하거나 경유지로 사용된 경우
5. 외부로부터 지속적인 공격 시도가 탐지된 경우
6. 기타 정보보안 침해사고가 발생된 경우

제21조(위험등급) 침해사고는 피해상황과 업무 영향도에 따라 침해사고위험등급표(별지 제5호 서식)와 같이 구분한다.

제22조(신고절차) 침해사고 발생 시 침해사고발생신고서(별지 제4호 서식)를 작성하여 정보보안관리자에 신고하며 신고유형은 다음 각 호와 같다.

1. 대학 내에서 사용자가 침해사고를 인지한 경우
2. 외부기관을 통하여 침해사고가 접수된 경우
3. 기타 보안 장비를 통하여 침해사고가 탐지된 경우

제23조(사고대응) 정보보안관리자는 침해사고가 접수되면 침해사고 위험등급에 따라 다음 각 호와 같은 대응 조치를 한다.

1. 1등급 사고 발생시 대상시스템 네트워크 격리(IP/MAC주소 차단) 및 POSTECH-CERT를 통한 침입경로, 취약점 파악 및 분석 등 긴급 대응 조치를 한다.
2. 2등급 사고 발생시 대상시스템 네트워크 격리(IP/MAC주소 차단) 및 원인분석과 취약점 점검 실시 후 결과를 안내한다.

3. 3등급 사고 발생시 대상시스템 네트워크 격리(IP/MAC주소 차단)후 점검방법을 안내하여 사용자 자체 점검을 실시한다.

제24조(후속조치) 정보보안관리자는 침해사고 대응 완료 후 다음 각 호와 같은 후속 조치를 하여야 한다.

1. 침해사고발생신고서 양식에 대응 조치결과를 기록한다.
2. 침해사고 재발 방지에 대한 대책을 마련하여 신고자에게 통보하고, 필요 시 교내 구성원에게 공지한다.

제25조(제재절차) ① 대학의 정보자산이 내·외부의 무단사용자에 의해 침해를 받는 경우 보안을 위해 제재조치를 할 수 있다.

② 제재조치의 범위는 대학의 정보자산 이용제한 또는 서비스 제한 등을 가할 수 있다.

③ 제재조치가 발생된 경우 즉시 당사자 또는 관련자에게 제재 내용을 고지하여야 하며, 긴급한 경우 선 조치 후 고지할 수 있다.

④ 대학의 정보자산 이용제한 또는 서비스 제한 이상의 징계조치가 필요한 경우 대학의 관계 규정에 의하여 처리한다.

제26조(조직구성) ① 보안업무규정 제6조 제4항에 의거 정보보안책임자는 대학 정보시스템 및 정보통신망 해킹 등 침해사고에 대응하기 위하여 침해사고대응조직 (이하 'POSTECH -CERT'라 한다.)을 둔다.

② POSTECH-CERT'는 정보보안책임자를 책임자로 하여 정보보안관리자, 정보보안담당자 등의 행정지원 인력과 정보보안 동아리인 PLUS 등의 기술지원 인력으로 구성한다.

③ POSTECH-CERT는 다음 각 호의 역할을 수행한다.

1. 침해사고 예방활동-자체점검, 모의해킹, 교육전파
2. 실질적인 침해사고 대응 및 분석, 피해복구기술
3. 타 기관 CERT와의 정보공유 및 협조체제지원
4. 사이버관제 등 침해사고대응을 위한 단일창구 역할

제27조(조직운영) POSTECH-CERT 운영은 별도로 정한다.

## 제7장 정보보안감사

제28조(감사의 종류) ① 정보보안감사는 정기적으로 실시하는 일반감사와 비정기

적으로 실시하는 특별감사로 구분한다.

② 특별감사는 다음 각 호와 같은 사안이 발생하는 경우 실시한다.

1. 심각한 정보보안 침해사고가 예상되거나 발생한 경우
2. 정보보안책임자가 특별히 필요하다고 결정하는 경우

제29조(인력의 구성) ① 정보보안감사는 정보보안책임자 지휘 하에 그 직무를 수행한다.

② 정보보안 감사인력은 정보보안실무부서의 소속직원이 수행하는 것을 원칙으로 하며, 필요 시 내·외부 보안전문가를 포함시킬 수 있다.

제30조(감사실시) 정보보안관리자는 감사의 대상, 항목, 일정, 감사인력 등을 정한 정보보안감사 기본계획을 수립하여 정보보안책임자에게 보고 후 다음 각 호에 의하여 보안감사를 실시한다.

1. 정보보안감사 시 감사 항목에 대해 담당자 인터뷰, 시스템 설정사항, 시스템 로그, 취약점 진단, 위험평가 분석 등을 통하여 필요한 보안 감사증적을 확보한다.
2. 운영되고 있는 시스템에 대한 감사 시 업무 프로세스의 중단 위험을 최소화 시킬 수 있도록 신중히 수행한다.
3. 정보보안감사 결과 부적합 사항에 대하여 정보보안분임관리자에게서 해당 사항의 이행계획을 받고 이와 관련된 사후관리를 실시한다.

제31조(결과보고) ① 정보보안감사 결과는 정보보안책임자에게 보고하며, 보안감사 수행 중 중대한 보안 사고를 발견한 경우 신속한 대응 조치를 실시한 후 정보보안책임자에게 보고한다.

② 정보보안감사결과보고서에는 다음 각 호와 같은 항목을 포함한다.

1. 정보보안감사의 목적/범위
2. 정보보안감사 기간
3. 정보보안감사 실시 방법
4. 점검 체크리스트 및 점검 결과
5. 부적합 사항 및 조치계획

제32조(후속조치) ① 정보보안관리자는 보안감사 결과에 따른 개선사항을 피 감사자 및 피 감사부서에 통보한다.

② 정보보안감사를 통하여 도출된 부적합사항에 대하여 피 감사자 및 피 감사부서는 개선방안을 수립하고 조치하여 그 결과를 정보보안책임자에 통보한다.

③ 중·장기적으로 해결되어야 할 보안 개선사항에 대하여 정보보안책임자는 개선방안의 이행 과정을 주기적으로 점검하고, 필요 시 부적합 사항이 완전히 해결되는 시점까지 개선방안을 지원한다.

## 제8장 정보보안교육

제33조(보안교육) ① 정보보안책임자는 정보보호교육계획을 수립하고 교육담당 주무부서에 요청하여 지속적인 교육을 실시하여야 한다.

② 정보보안관리자는 교육관련 주무부서의 시행기준에 따라 정보보호와 관련된 업무 종사자에게 정기적 또는 비정기적 교육을 실시하여야 한다.

③ 정보보안관리자는 교육관련 주무부서와 협의하여 필요시 외부의 정보보호전문교육기관에 교육을 위탁할 수 있다.

④ 제2항에 의한 비정기교육 중 신규임용직원 및 전입자에 대하여는 임용 후 5일 이내 보안 교육을 실시하여야 하며 비밀취급인가예정자에 대하여는 교육실시 후 인가하여야 한다.

## 부 칙

1. 이 세칙은 2012년 11월 28일부터 제정, 시행한다.
2. 이 세칙 시행 이전에 처리된 업무는 이 세칙에 의하여 처리된 것으로 본다.
3. 이 세칙의 제정 시행일 이전의 “정보자산분류 및 관리세칙”, “침해사고대응세칙”, “시스템보안관리세칙”, “응용시스템보안관리세칙”, “위험평가 및 관리세칙”, “정보보호감사세칙”은 이 세칙으로 통합됨으로 제정일 기준으로 폐지한다.

## 부 칙

1. 이 세칙은 2013년 2월 18일부터 개정, 시행한다.
2. 이 세칙 시행 이전에 처리된 업무는 이 세칙에 의하여 처리된 것으로 본다.

## 부 칙

1. 이 세칙은 2022년 3월 18일부터 개정, 시행한다.

(별지 제1호 서식) 정보자산코드 및 분류체계

# 정보자산코드 및 분류체계

| 분 야 | 유형 | 코드 | 세부내역 |
|---|---|---|---|
| 정보자산 | 하드웨어 | HW-SV-0001 (서버) | 클라이언트에게 네트워크를 통해 서비스를 제공하는 장치로서 기본적으로 운영체제와 시스템 소프트웨어가 구동되고 있는 장비이며, 수퍼컴퓨터, 워크스테이션, 스토리지 등을 포함한다. |
| | | HW-NW-0001 (네트워크) | 두 대 이상의 컴퓨터를 케이블 등으로 연결해 서로 데이터를 교환할 수 있도록 만들어 주는 장치로서 라우터, 스위치, AP 등 통신장비를 포함한다. |
| | | HW-SS-0001 (보안시스템) | 여러 가지 위협으로부터 보호하기 위한 장치로서 방화벽, 침입탐지시스템, 침입차단시스템, 위협관리시스템 등을 포함한다. |
| | | HW-PC-0001 (PC&주변기기) | 운영체제(operating system:OS)를 가진 개인용 컴퓨터와 주변기기(프린터, 스캐너 등)를 말한다. |
| | 소프트웨어 | SW-0001 | 컴퓨터 프로그램과 문제 해결에 이용되는 다양한 형태의 응용 프로그램을 말하며, 시스템관리 프로그램, 진단프로그램, 통신프로그램, 유틸리티, 응용어플리케이션, 소스프로그램, 목적프로그램 등을 포함한다. |
| | 데이터 | DA-0001 | 컴퓨터가 처리할 수 있는 문자, 숫자, 소리, 그림 따위의 형태로 된 정보를 말하며, 실행중인 자료, 온라인 저장자료, 오프라인자료, 백업자료, 감시기록자료, 데이터베이스자료, 통신매체상의 전송자료를 포함한다. |
| | 인적자원 | HR-0001 | 생산자원으로서 사람의 노동력을 말하며, 사용자, 관리자, 유지보수자, 고객, 계약자, 외부인력 등을 포함한다. |
| | 문서 | DOC-0001 | 글이나 기호 따위로 일정한 의사나 관념 또는 사상을 나타낸 것으로서 시스템 문서, 사용자 매뉴얼, 운영 및 교육지침서 등을 포함한다. |
| 물리・환경적자산 | | PH-0001 | 눈에 보이는 유형 자산으로 컴퓨터 통신시설, 자기매체, 지원장비, 건물 및 부대설비, 난방, 조명, 편의시설 등을 포함한다. |
| 활동자산 | | ACT-001 | 활동 시 발생하는 자산으로 조직의 이미지와 명성, 운영 등을 포함한다. |

(별지 제2호 서식) 정보자산 중요도 평가기준 및 등급

# 정보자산 중요도 평가기준 및 등급

1. 정보자산 중요도 평가기준

| 평가기준 | 평가수준 | 평가항목 |
|---|---|---|
| 기밀성 | High(3) | 해당 정보자산의 비인가 유출 시 대학 전체적으로 중대한 손실을 미치는 경우 |
| | Medium(2) | 해당 정보자산의 외부 유출 시, 대학에 부분적인 손실을 미치는 경우 |
| | Low(1) | 해당 정보자산의 대학 외부로 공개되어도 관계없거나 손실을 발생시키지 않는 경우 |
| 무결성 | High(3) | 해당 정보자산의 변조 발생시 대학 전체적으로 중대한 손실을 미치는 경우 |
| | Medium(2) | 해당 정보자산의 변조 발생 시 대학에 부분적인 손실을 미치는 경우 |
| | Low(1) | 해당 정보자산이 변조되어도 업무 수행에 미치는 영향이 미흡한 경우 |
| 가용성 | High(3) | 해당 정보자산이 사용 불가능할 때 대학 전체적으로 중대한 손실을 미치는 경우 |
| | Medium(2) | 해당 정보자산이 사용 불가능할 때 대학에 부분적인 손실을 미치는 경우 |
| | Low(1) | 해당 정보자산이 사용 불가능할 때 업무 수행에 미치는 영향이 미흡한 경우 |

2. 정보자산 중요도 등급

| 정보자산 중요도 등급 | 보안 요구사항 평가 지수 |
|---|---|
| VH(Very High) | 9 점 |
| H(High) | 7~8 점 |
| M(Medium) | 6 점 |
| L(Low) | 4~5 점 |
| VL(Very Low) | 3 점 |

(별지 제3호 서식) 정보자산관리대장

# 정보자산관리대장

| 정보자산코드 | 하드웨어 | | | 소프트웨어 | | | 데이터 & 문서 | | | | 부가정보 | | | | | | | 중요도 평가 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 시스템명 | IP 주소 | 수량 | 운영체제 | 어플리케이션명 | 수량 | 데이터및문서명 | 보관방법 | 저장매체 | 보관기간 | 모델명 | 제조사 | 주요용도 | 설치위치 | 관리부서 | 관리자 | 운영자 | 기밀성 | 무결성 | 가용성 | SUM | 등급 |
| HW-NW-0001 | 서버팜 스위치 | 3.99 | 1 | 12.0(3)XE2 | | | | | | | Catalyst 6509 | CISCO | 메인 | 전산실 | 정보시스템 | 박상무 | 홍길동 | 3 | 3 | 3 | 9 | VH |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |

※ 제5조(분류 및 등록)에 의거하여 관련 해당 항목에만 기입

(별지 제4호 서식) 침해사고발생신고서

# 침해사고발생신고서

## ❑ 침해사고 발생 기본사항 (신고자 작성)

○ 이름 :

○ 소속 :

○ 연락처(이메일, 전화번호) :

○ IP 주소 및 용도 :

○ OS 종류 및 버전 :

○ 사고 발견 일시 :

○ 사고 발견 경위 :

○ 사고 피해 증상 :

## ❑ 침해사고 대응 조치 (침해사고대응 담당자 작성)

○ 조치자 :

○ 완료일시 :

○ 공격자 정보 :

○ 피해 내역:

○ 원인 및 조치 방법 :

○ 향후 대책 :

(별지 제5호 서식) 침해사고위험등급표

# 침해사고위험등급표

| 위험등급 | 피해상황 | 업무영향 |
|---|---|---|
| 1 등급 | 1. 중앙전산실의 완전 혹은 상당한 파괴<br>2. 전체 또는 대부분 시스템 작동중단상태<br>3. 통신회선 단절<br>4. 대학업무 관련 서비스에 영향을 미치는 대부분 네트워크 장비의 작동중단 상태<br>5. 전원공급 단절 | 1. 대학업무의 전반적 장애 발생 상태 |
| 2 등급 | 1. 중앙전산실의 부분적 파괴<br>2. 시스템의 일부 작동 중단 상태<br>3. 일부 통신회선 단절<br>4. 대학업무 관련 서비스에 영향을 미치는 네트워크 장비의 부분적인 작동중단 상태 | 1. 대학업무의 부분적 장애 발생 상태<br>2. 그룹웨어 등의 작동 중단으로 인한 대학 또는 부서의 업무 수행에 상당한 지장을 주게 하는 상태 |
| 3 등급 | 1. 정보시스템의 일시적 장애 상태이지만 물리적 손상이 없는 경우<br>2. 일부 통신회선의 불안정 상태 (트래픽 이상 상황)<br>3. 정보자산 목록에 등록된 네트워크 자산의 일시적 장애 상태이지만 물리적 손상이 없는 경우<br>4. 다음 침해사고의 경우<br>- 지속적인 취약점 수집 행위(Scanning)가 발견되는 경우<br>- 계속적인 불법적 접근 시도가 발견되는 경우<br>- 비정상적 패킷 전송량이 증가하는 경우<br>- 확산속도가 빠른 웜/바이러스가 외부에서 발생한 경우 | 1. 대학업무의 일시적 지연 및 불안정 상태<br>2. 그룹웨어 등의 일시적 지연 및 불안정으로 인하여 대학 업무 수행에 지장을 초래하는 상태 |

(별지 제6호 서식) 보안기능의 설계요구사항 (신설: 2022.03.18)

# 정보화 용역사업 보안기능의 설계요구사항

SER-001 보안 통제

- 사업자는 사업수행에 사용되는 인원, 문서, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 "외주 용역사업 보안특약"의 <별표3>의 '누출금지 대상정보'에 대한 보안관리 계획을 사업제안서에 기재하여야 한다.
- 제안사는 입찰 참여 과정 및 본 사업과 관련하여 취득한 일체의 정보를 제3자에게 유출 또는 누설하여서는 안 되며, 이의 위반으로 인한 문제 발생 시 책임을 진다.
- 사업자는 사업 수행 중 인원, 문서 및 전산자료 보안 등 "외주 용역사업 보안특약"에서 정하는 보안관리 사항을 준수하여야 한다. 기타 사항은 포항공과대학교 정보보안규정 및 정보보안세칙에서 정하는 바에 따른다.

SER-002 안전한 소프트웨어 개발

- 웹페이지 및 응용프로그램 등 소프트웨어의 신규 개발 및 수정 업무가 포함되는 용역사업을 수행할 시, 사업자는 행정안전부가 고시하는 "소프트웨어 개발보안 가이드"를 준수하여야 한다.
- 사업자는 행정안전부가 고시하는 "공개SW를 활용한 소프트웨어 개발보안 점검가이드"에 명시된 공개 소프트웨어, 또는 자체적으로 운용하는 상용 소프트웨어를 활용하여 용역사업 최종 산출물의 "소프트웨어 개발보안 가이드" 준수 여부를 점검하고, 점검결과보고서를 제출하여야 한다.
- 사업자는 "소프트웨어 개발보안 가이드"를 포함하여 "정보화 용역사업 표준 및 법적 제약사항(별지 제7호 서식)"에서 지정한 정부 중앙부처 및 공공기관의 관련지침 및 가이드라인을 준수하여야 한다.
- 사업기간 내 관련 법, 지침이 갱신되었을 경우, 최근의 법과 지침에 따른다.

(별지 제7호 서식) 정보화 용역사업 표준 및 법적 제약사항 (신설: 2022.03.18)

# 정보화 용역사업 표준 및 법적 제약사항

| 순번 | 표준 및 법적 제약사항 | 고시기관 |
|---|---|---|
| 1 | 전자정부 웹 표준 준수지침 | 행정안전부 |
| 2 | 전자정부서비스 호환성 준수지침 | 행정안전부 |
| 3 | 한국형 웹 콘텐츠 접근성 지침 2.1 | 한국정보통신기술협회 |
| 4 | 웹 접근성 향상을 위한 국가표준기술가이드라인 | 한국정보문화진흥원 |
| 5 | 행정기관의 코드표준화 추진지침 | 행정안전부 |
| 6 | 공공기관의 데이터베이스 표준화 지침 | 행정안전부 |
| 7 | 행정기관 등 웹사이트 운영 가이드라인 | 행정안전부 |
| 8 | 공공기관 웹사이트 구축·운영 가이드 | 행정안전부 |
| 9 | 표준 개인정보 보호지침 | 개인정보보호위원회 |
| 10 | 웹 응용프로그램 개발보안 가이드 | 행정안전부 |
| 11 | OWASP Top 10 | OWASP |
| 12 | 홈페이지 개인정보 노출방지 안내서 | 개인정보보호위원회 |
| 13 | 전자정부 웹 서비스 취약점 대응 지침 | 행정안전부 |
| 14 | 소프트웨어 개발보안 가이드 | 행정안전부 |
| 15 | 행정공공기관 웹사이트 구축운영 가이드 | 행정안전부 |
| 16 | 행정기관 및 공공기관 정보시스템 구축·운영 지침 | 행정안전부 |
| 17 | 개인정보의 안전성 확보조치 기준 | 개인정보보호위원회 |