

보안업무규정(안)

※ 문장의 통일감과 일관성을 위해 수정한 문구상의 표현은 따로 표기하지 않았음을 양해해주시기 바랍니다.

정보보호규정	개정안 보안업무규정	비고
2008. 7. 17 제정	2012. 0. 0 제정	
<p>제1조(목적) 이 규정은 포항공과대학교(이하 '대학'이라 한다)의 정보자산을 보호하고, 정보보호 활동에 필요한 사항을 규정함을 목적으로 한다.</p> <p>제2조(적용대상과 범위) ① 이 규정의 적용대상은 정보자산을 이용하거나 관리하는 대학 구성원과 관련 외부 인력으로 한다. ② 적용범위는 관리적, 물리적, 기술적 보호가 필요한 모든 정보자산과 그 부대시설로 한다.</p> <p>제3조(의무와 책임) 대학의 정보자산을 사용하고 관리하는 모든 구성원과 관련 외부 인력은 대학의 정보보호 규정·세칙과 관계법령을 준수하며, 자신에게 부여된 사용권한과 관리권한 내에서 정보자산을 보호할 의무와 책임을 가진다.</p> <p>제4조(용어의 정의) 이 규정에서 사용하는 용어의 정의는 다음 각 호와 같다.</p> <p>1. "정보자산"이라 함은 대학이 보유하고 있는 전자적 정보 및 데이터, 하드웨어, 소프트웨어, 물리적 환경, 인적 자산과 문서, 지적 재산권, 기술 관련, 학술연구 관련 등의 정보를 포함하고 있는 유·무형의 자산을 의미한다.</p> <p>2. "외부인력"이라 함은 대학 소속의 구성원 이외의 모든 인력</p>	<p>제1조(목적) 이 규정은 관계법령에 의거하여 포항공과대학교(이하 '대학'이라 한다)의 모든 유·무형 정보자산을 보호하고, 보안업무 처리 및 활동에 관한 사항을 규정함을 목적으로 한다.</p> <p>제2조(적용대상 및 범위)) ① 대학의 유·무형 정보자산을 이용하거나 관리하는 모든 구성원과 대학의 필요에 의해 계약된 외부인력을 적용대상으로 한다.</p> <p>② 관리적, 물리적, 기술적 보안이 필요한 대학의 모든 유·무형 정보자산과 그 부대시설을 적용범위로 한다. 단, 대학 네트워크망을 이용하는 별도법인은 자체 보안규정을 수립하여야 하며, 보안사고 발생 시 대학의 보안업무규정을 따른다.</p> <p>제3조(의무와 책임) 대학의 유·무형 정보자산을 사용하고 관리하는 모든 구성원과 관련 외부 인력은 대학의 보안업무규정과 관계법령을 준수하여야 하며, 자신에게 부여된 사용권한과 관리권한 내에서 대학의 정보자산을 보호할 의무와 책임을 지닌다.</p> <p>제4조(용어의 정의) 이 규정에서 사용하는 용어의 정의는 다음 각 호와 같다.</p> <p>1. "정보자산"이라 함은 대학이 보유하고 있는 전자적 정보 및 데이터, 하드웨어, 소프트웨어, 물리적 환경, 인적 자산과 문서, 지적 재산권, 기술 관련, 학술연구 관련 등의 정보를 포함한다.</p> <p>2. "정보보안" 또는 "정보보호"라 함은 정보시스템 및 정보통신</p>	<p>▪규정의 범위를 확대하여 하부세칙을 총괄하게 함</p> <p>▪용어에 대한 세부설명 추가</p> <p>▪엄격해진 상위법령의 반영을 위해 새로이 추가된 용어 정의</p>

<p>을 통칭하며, 대학의 정보자산 이용여부에 따라 외주용역인력, 외부 연구참여인력, 위탁매장 소속인력, 기타 외부인력 등으로 구분할 수 있다.</p> <p>3. "정보보호사고"라 함은 대학의 정보자산이 무단으로 열람, 유출, 훼손, 변경 되는 사고를 말한다.</p> <p>4. "CSO(Chief Security Officer)"라 함은 대학의 정보보호 전담 총괄 보직자를 말한다.</p> <p>5. "위험평가"라 함은 정보자산의 중요도와 정보자산의 기밀성, 무결성, 가용성 측면에서의 취약점 수준에 따라 위험 크기를 측정하고, 위험도를 산출하는 행위를 말한다.</p> <p>6. 이외의 용어의 정의는 정보보호세칙에서 다룬다.</p>	<p>망을 통해 수집·가공·저장·검색·송수신 되는 정보의 유출·위변조·훼손 등을 방지하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위로서 사이버안전을 포함한다.</p> <p>3. "정보시스템"이라 함은 서버·PC 등 단말기, 보조기억매체, 네트워크 장치, 응용 프로그램 등 정보의 수집·가공·저장·검색·송수신에 필요한 하드웨어 및 소프트웨어를 말한다.</p> <p>4. "외부인력"이라 함은 대학 소속의 구성원 이외의 모든 인력을 통칭하며, 대학의 자산 이용여부에 따라 외주용역인력, 외부 연구참여인력, 위탁매장 소속인력, 기타 외부인력 등으로 구분할 수 있다.</p> <p>5. "보안사고"라 함은 대학의 정보자산이 무단으로 열람, 유출, 훼손, 변경 되는 사고를 말한다.</p> <p>6. "위험평가"라 함은 정보자산의 중요도와 정보자산의 기밀성, 무결성, 가용성 측면에서의 취약점 수준에 따라 위험 크기를 측정하고, 위험도를 산출하는 행위를 말한다.</p> <p>7. 이외의 용어는 통상적인 정의에 따른다.</p>	
<p>제6조(정보보호총괄책임자) ① "공공기관의 정보공개에 관한 법률"에 의하여 정보보호총괄책임자(이하 "CSO"라 한다)를 지정하고, 학술정보처장이 겸직한다.</p> <p>② CSO는 대학의 정보보호 활동 전반에 대한 총괄적인 관리 감독의 권한과 책임을 가지며, 다음 각 호의 역할을 수행한다.</p> <ol style="list-style-type: none"> 1. 대학의 정보보호 전략계획에 관한 관리감독 2. 정보보호 정책 및 세칙에 관한 관리감독 3. 정보보호 예산의 편성 및 집행에 관한 관리감독 4. 대학의 정보보호 조직에 관한 관리감독 5. 기타 대학의 정보보호 활동에 관한 관리감독 	<p>제5조(보안총괄책임자) ① 정보보안업무를 총괄하는 보안총괄책임자(Chief Security Officer, 이하 "CSO"라 한다)는 부총장으로 하며 보안심사위원회의 장을 겸한다.</p> <p>② CSO는 다음 각 호의 역할을 수행한다.</p> <ol style="list-style-type: none"> 1. 보안전략 계획수립에 관한 사항 2. 보안관련 정책에 관한 사항 3. 보안 예산의 편성 및 집행에 관한 사항 4. 대학의 보안조직 구성 및 운영에 관한 사항 5. 기타 대학의 보안업무 활동에 관한 사항 <p>③ CSO는 대학의 보안업무를 효율적이고 체계적으로 수행하기 위하여 별지 제1호의 보안업무기구를 두며, 분임보안책임자를 지정하여야 한다.</p> <p>제6조(분임보안책임자) ① 분임보안책임자로는 개인정보보호책임자, 연구보안책임자 및 정보보안책임자 등을 둔다.</p> <p>② 개인정보보호책임자는 각 구성단위별 신분을 대표하는 처장</p>	<p>▪'공공기관의 정보공개에 관한 법률'의 의무사항으로 CSO를 두며, 기존 학술정보처장이 겸직하던 것을 보안업무의 중요성을 반영하고 정보이외의 자산 관리를 총괄할 수 있도록 부총장으로 정함.</p> <p>▪(신설) : 체계적인 보안업무를 위한 직제 신설</p>

	<p>으로 하고, 다음 각 호의 역할을 수행한다.</p> <ol style="list-style-type: none"> 1. 개인정보보호 계획의 수립 및 시행 2. 개인정보보호 관련 규정의 제·개정 3. 개인정보보호 관련 제반사항 관리 및 총괄 4. 보안심사위원회에 개인정보보호 분야 안건 심의 상정 5. 그 밖에 대통령령으로 정한 업무 <p>③ 연구보안책임자는 연구 관련 업무를 총괄하는 처장으로 하고, 다음 각 호의 역할을 수행한다.</p> <ol style="list-style-type: none"> 1. 연구보안 정책 및 기본계획 수립·시행 2. 연구보안 관련 규정의 제·개정 3. 연구보안 관련 제반사항 관리 및 총괄 4. 보안심사위원회에 연구보안 분야 안건 심의 상정 5. 그 밖에 대통령령으로 정한 업무 <p>④ 정보보안책임자는 정보보안 업무를 총괄하는 처장으로 하고, 다음 각 호의 역할을 수행한다.</p> <ol style="list-style-type: none"> 1. 정보보안 정책 및 기본계획 수립·시행 2. 정보보안 관련 규정의 제·개정 3. 정보보안 관련 제반사항 관리 및 총괄 4. 보안심사위원회에 정보보안 분야 안건 심의 상정 5. 그 밖에 대통령령으로 정한 업무 	<p>■직제들 간의 통일성을 위해 기존 개인정보보호세칙 내의 개인정보총괄책임자의 명칭을 변경하고, 규정에 기록함</p>
<p>제5조(정보보호위원회) ① 대학의 중요한 정보보호 정책 및 사고에 대한 심의를 위하여 "정보보호위원회" (이하 "위원회"라 한다)를 다음 각 호와 같이 구성한다.</p> <ol style="list-style-type: none"> 1. 위원회는 연구부총장을 위원장, 학술정보처장을 간사로 하여 10인 내외의 보직자로 구성한다. 2. 위원장을 포함한 각 위원의 임기는 보직 재임기간으로 한다. <p>② 위원회는 다음 각 호의 사항을 심의한다.</p>	<p>제7조(보안심사위원회) ① 보안업무와 관련한 주요사항을 심의 하기 위하여 CSO 하부에 "보안심사위원회" (이하 "위원회"라 한다)를 두며, 다음 각 호와 같이 구성한다.</p> <ol style="list-style-type: none"> 1. 위원회는 CSO를 위원장, 정보보안실무부서장을 간사로 하여 10인 내외의 보직자로 구성하며, 위원구성은 별지 제2호와 같다. 2. 위원장을 포함한 각 위원의 임기는 보직 재임기간으로 한다. 3. 위원회 소집은 협의 안건이 있는 실무부서에서 공문을 통해 안건 및 협의내용을 7일전에 고지하여야 한다. <p>② 위원회는 다음 각 호의 사항을 심의한다.</p>	<p>■'정보보호위원회'→ '보안심사위원회' : 정보보안 뿐만 아니라 기타 보안업무의 중요사항을 심의 하기 위해 명칭을 변경하고 위원장을 부총장으로 함</p>

<p>1. 대학의 중요한 정보보호정책 심의 2. 민·형사상 또는 대학 규정에 위배되는 중대한 정보보호 사고에 대한 심의 3. CSO가 필요하다고 판단한 정보보호 안건 심의</p> <p>③ 위원회에서 안건 심의가 필요한 경우 CSO가 안건을 상정하고, 재적위원 3분의 2이상 참석에 참석위원 과반수의 찬성으로 의결한다.</p>	<p>1. 보안전략 및 정책의 수립에 관한 사항 2. 보안관련 규정에 관한 주요 사항 3. 보안 위반자 심사 및 처리에 관한 사항 4. 보안업무 심사분석 및 보안업무 수행상 조정과 협의를 요하는 사항 5. 기타 위원장이 필요하다고 인정하는 사항</p> <p>③ 위원회는 재적위원 과반수 이상의 출석과 출석위원 과반수 이상의 찬성으로 의결하며 가부동수인 경우에는 부결된 것으로 본다.</p>	
	<p>제8조(보안실무협의회) ① 보안업무의 효율적인 이행과 조정 및 실무 협의를 하기 위하여 “보안실무협의회”(이하 “협의회”라 한다)를 다음 각 호와 같이 구성한다.</p> <p>1. 협의회 구성은 각 보안업무의 실무 대표부서의 장으로 구성하며, 간사는 협의회를 소집하는 보안업무 실무부서의 담당자로 한다. 2. 협의회 소집은 협의 안건이 있는 실무부서에서 공문을 통해 안건 및 협의내용을 7일전에 고지하여야 한다.</p> <p>② 협의회는 다음 각 호의 사항을 협의한다.</p> <p>1. 보안업무 범위에 관련된 실무 사항 2. 보안예산 수립 및 집행 관련 사항 3. 보안관련 규정 사항 4. 외부 용역 시 하드웨어, 소프트웨어, 물리적 보안 등의 운영계획에 대한 협의 5. 기타 위 각 호에 부수되는 제반 사항</p>	<p>▪ (신설) : 실무자들을 중심으로 하는 실무협의회를 구성함으로써 좀 더 효율적으로 보안업무가 이루어지도록 함</p>
<p>제7조(정보보호전담부서) ① 대학의 정보보호 실무 총괄부서 역할을 수행하고 정보보호 현업 부서의 업무조정 및 지원을 위하여 정보보호전담부서를 둔다. ② 정보보호전담부서는 CSO 산하에 두며, 업무의 독립성과 연속성을 가지고 업무를 수행한다. ③ 정보보호전담부서는 다음 각 호의 역할을 수행한다.</p> <p>1. 정보보호 관리 체계 수립</p>	<p>제9조(보안업무실무부서) ① 보안업무관련 실무부서 역할을 수행하고 단위조직의 보안활동조정 및 지원을 위하여 보안업무실무부서를 둔다. ② 보안업무실무부서는 분임보안책임자 산하에 두며, 업무의 독립성과 연속성을 가지고 업무를 수행한다. ③ 보안업무실무부서는 해당 보안 분야에서 다음 각 호의 역할을 수행한다.</p>	<p>▪ ‘정보보호전담부서’→ ‘보안업무실무부서’ : 정보보호를 전담하는 부서를 포함하는 보안업무실무부서를 둘 수 있음을 명시. (기존의 정보보호전담부서는</p>

<p>2. 정보보호 중장기 마스터플랜 수립 3. 정보보호 정책 및 세칙 총괄 관리 업무 4. 정보보호 위험평가 및 보안감사 활동 5. 정보보호 교육 및 훈련 업무 6. 대외 정보보호 업무의 창구 7. 기타 정보보호 제반 사항에 대한 업무</p>	<p>1. 보안업무 계획 이행 및 예산 수립 2. 보안업무 관련규정의 관리 3. 보안시스템 운영 및 관리 4. 위험평가 및 보안감사 활동 5. 보안교육 및 훈련 집행 6. 대외 보안업무의 실무창구 7. 기타 보안관련 제반사항에 관한 사항</p>	<p>정보보호세칙에서 정함)</p>
<p>제8조(세칙의 수립 및 시행) ① 정보보호 규정의 시행과 정보 보호 활동에 필요한 세부사항을 세칙으로 정하며, 세칙의 종류와 관리에 관한 사항은 CSO가 별도로 정한다. ② 각 세칙의 제정과 개폐 시에는 대학의 규정 관리 절차에 의하여 정보보호 총괄 책임자인 CSO와 기획처장의 협조를 거쳐 총장의 승인으로 시행한다. ③ 승인 된 각 세칙은 지체 없이 정보 보호 전담 부서와 기획 예산팀으로 통보하여야 하며, 반드시 교내에 공지하여야 한다.</p>	<p>제10조(규정의 수립 및 시행) ① 보안업무규정의 시행과 보안 업무 활동에 필요한 세부사항은 별도로 정한다.</p>	<p>▪규정에 관한 당연사항 삭제</p>
<p>제9조(제재절차) ① 대학의 정보자산이 내·외부의 무단사용자에 의해 침해를 받는 경우 정보보호를 위해 제재조치를 할 수 있으며 구체적인 사항은 각 세칙에서 정한다. ② 제재조치의 범위는 대학의 정보자산 이용제한 또는 서비스 제한을 말한다. ③ 제재 조치가 발생한 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 징계 조치가 필요한 경우 대 학의 관계 규정에 의하여 처리한다.</p>	<p>제11조(제재절차) 대학의 정보자산이 내·외부의 무단사용자에 의해 침해를 받는 경우 보안을 위해 제재조치를 할 수 있으며 구체적인 사항은 따로 정한다.</p>	<p>▪ 조항의 내용상, 정보보안세칙으로 이관.</p>
	<p style="text-align: center;">부칙</p> <p>1. 이 규정은 2012년 0월 0일부터 제정, 시행한다. 2. 이 규정의 제정 시행일 이전의 "정보보호규정"은 이 규정으로 통합됨으로 제정일 기준으로 폐지한다.</p>	<p>(신설)</p>
	<p>(별지 제1호 서식) 보안업무기구표 (생략)</p>	<p>(신설)</p>

	(별지 제2호 서식) 보안심사위원회 (생략)	(신설)
--	-----------------------------	------