일반보안관리세칙

제정 2012. 11. 28

제1장 총 칙

제1조(목적) 이 규정은 포항공과대학교(이하 “본 대학”이라 한다)의 ‘보안업무규정’ 및 국가의 ‘보안업무규정’ 및 ‘보안업무규정시행세칙’에 의거하여 본 대학의 일반보안관리에 필요한 세부사항을 규정함을 목적으로 한다.

제2장 인 적 보 안

제2조(용어의 설명) 사용하는 용어의 정의는 다음 각 호와 같다.

1. “비밀”이라 함은 관련법령에 의하여 국가안전보장에 유해로운 결과를 초래할 우려가 있는 국가기밀 또는 대학의 존립에 관련된 기밀로서 이 세칙에 의하여 분류된 것을 말한다.
2. “외부인력”이라 함은 대학 소속의 구성원 이외의 모든 인력을 통칭하며, 대학의 정보자산 이용여부에 따라 외주용역인력, 외부 연구참여인력, 위탁매장 소속인력, 기타 외부인력 등으로 구분할 수 있다.
3. “계약직원”이라 함은 대학의 필요에 의해서 일정기간 고용을 한 직원으로 정규직원을 제외한 자를 말한다.

제3조(대학구성원 기본보안) 대학구성원으로의 채용, 면직 및 퇴직 시까지 다음 각 호와 같은 보안 기준을 준수하여야 한다.

1. 대학구성원으로 채용된 자는 대학의 보안업무규정과 관련법률 준수를 명기한 정보보호서약서(별지 제1호 서식)를 인사관련 주무부서에 제출하여야 한다.
2. 대학구성원으로 재직중인 자는 보안점검활동을 지원하여야하며, 보안교육 및 보안사고대응절차 등에 대한 교육을 정기적으로 받아야 한다.
3. 대학구성원에서 면직 및 퇴직한 자는 대학의 정보보호 활동에서 제시한 법적, 도덕적 의무를 지켜야 한다.

4. 대학구성원 중 연구과제를 수행하는 연구자에 대한 인적보안은 연구보안관리세칙에서 별도로 정한다.

제4조(신원조사) ① 신원조사 대상이 되는 자는 다음 각 호와 같다.

1. 교직원 임용예정자
2. 비밀취급인가예정자
3. 기타 보안상 필요하다고 인정하는 자

② 신원조사는 인사관련 주무부서에서 실시하며 신원조사 요청시 관련법령에 의거하여 시행한다.

③ 신원조사회보서는 개인의 인사기록서류와 함께 관리하여야 한다.

제5조(계약직원의 관리) ① 계약직원 중 특수 분야에 종사하는 자(비밀업무취급자, 통제구역 근무자, 경비근무자)와 기타 신원조사가 필요한 자는 임용 전에 실시함을 원칙으로 한다.

② 계약직원에게는 비밀취급인가를 하지 않는 것을 원칙으로 하며, 비밀취급인가 필요시 보안실무협의회의 심의를 거쳐 인가할 수 있다.

③ 계약직원의 감독책임은 임용권자 및 단위조직의 부서장과 당해 업무의 담당자가 진다.

제6조(외국인 임용 관련 보안대책) ① 업무상 자문 및 기타의 목적을 위하여 외국인과 고용계약을 체결할 경우에는 임용 30 일전 신원조사를 의뢰하여야하며, 신원특이자는 보안실무협의회의 심의를 거쳐 임용여부를 결정하여야 한다.

② 보안총괄책임자는 단위조직에서 고용할 외국인과 고용계약을 체결할 때에는 근무 중 알게 된 기밀사항을 계약기간 중이나 계약만료 후에 누설할 경우의 손해배상책임과 피고용인 업무의 한계설정 등 보안유의사항을 계약서에 명시토록 감독하여야 한다.

③ 보안총괄책임자는 재직중인 외국인이 퇴직할 경우에는 업무기간 중 취득한 비밀 등 중요자료에 대한 누설 및 사적 이용 금지를 내용으로 하는 정보보호서약서를 작성하여야 하며, 각종 자료의 무단반출 여부를 확인하여야 한다.

제7조(비밀취급의 인가 및 해제) 대학의 문서보안관리세칙에서 정의 된 비밀을 취급하는 자는 비밀의 안전관리를 위하여 다음 각 호와 같은 절차를 준수하여 한다.

1. 비밀취급 인가의 대상은 총장, 보안총괄책임자, 정보보안관리자 및 기타 정보보안업무 수행자로 한다.
2. 비밀취급 인가를 신청할 때에는 비밀취급인가사유서, 서약서, 신원진술서 4부, 호적등본 2부와 사진 6매(2cm X 2.5cm)를 첨부하여야 한다.

3. 비밀취급 인가를 받은 자가 보직이동 또는 퇴직하였을 경우에는 즉시 인사관련 주무부서에 비밀취급 인가증을 반납하여야 한다.
4. 비밀취급 인가증을 분실하였을 때에는 지체 없이 분실사유서를 인사관련 주무부서에 제출하고 사고 발생 시 책임을 진다는 본인의 서약서와 함께 재발급을 요청하여야 한다.

제8조(외부인력 보안관리) 대학의 단위조직에서는 필요에 의해 계약 된 외부인력에 대해서 다음 각 호와 같은 인적보안 관리활동을 하여야 한다.

1. 외부인력 계약 시 계약서에는 계약 일반사항 이외에, 보안 및 내부통제 사항, 비상대책, 소유권 문제, 보안 교육 요건, 보안 위반 조건과 정보보호서약서 등이 포함되어야 하며, 기타 외부 인력 계약 또는 아웃소싱 계약에 따라 필요한 보안 요건이 추가로 포함시켜야 한다.
2. 외부 인력이 대학 내부의 정보자산에 접근이 필요한 경우에는 정보보안세칙 및 계정 및 패스워드 관리지침에 따라 적절한 접근통제 및 보안 관리가 이루어져야 한다.
3. 외부 인력이 대학에 상주하여 프로젝트를 수행할 경우 정보유출 방지를 위해 별도의 업무공간을 제공하는 것을 원칙으로 한다.
4. 대학에서 실시하는 정기적인 보안교육 참여와 대학의 보안점검 활동에 참여시켜야 한다.

제3장 문 서 보 안

제9조(용어의 정의) 사용하는 용어의 정의는 다음 각 호와 같다.

1. “비밀문서”라 함은 관련법령에 의하여 국가안전보장에 유해로운 결과를 초래할 우려가 있는 국가기밀문서 또는 대학에서 비밀문서로 정하는 경우를 말한다.
2. “대외비”라 함은 비밀에는 해당되지 않으나 대학의 업무수행 상 특별히 보호가 필요한 문서를 말한다.
3. “전자문서”라 함은 일반종이문서가 아닌 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태로 작성, 송·수신 또는 저장된 문서를 말한다.

제10조(등급분류 기준) ① 정보자산 분류 및 관리세칙에서 정의한 대학의 모든 문서는 다음 각 호와 같은 보안등급으로 분류한다.

1. 공개(Public Use)
2. 대외비(Internal Use Only)

3. 비밀(Confidential)
4. 극비(Strictly Confidential)

② 공개(Public Use)문서는 유출 또는 손상되더라도 대학의 연구 및 업무수행 또는 개인 신상에 아무런 영향을 미치지 않은 문서를 말한다.

③ 대외비(Internal Use Only)문서는 외부로의 유출을 제한하며, 유출 또는 손상되는 경우 대학의 연구·업무수행 및 대학의 이미지에 영향을 줄 수 있는 문서를 말하며 다음 각 호와 같은 유형을 말한다.

1. 공개이전의 대학의 중장기 운영계획, 정책수립 및 경영문서
2. 연구보안과제 중 한시제한(B급) 이상의 연구과제 또는 연구기록물
3. 학생성적 등의 학사정보 및 교직원 인사정보
4. 공개이전의 위원회 또는 업무회의 등의 회의문서
5. 각종 프로젝트 성격의 업무와 관련된 문서
6. 보안총괄책임자가 지정하는 문서 등

④ 비밀(Confidential)문서는 외부로의 유출을 엄격히 금지하며, 유출 또는 손상되는 경우 대학의 경영상에 심각한 영향을 줄 수 있거나 관련법령에서 정의하는 국가기밀에 해당되는 문서를 말하며 다음 각 호와 같은 유형을 말한다.

1. 관련법령에서 정하는 Ⅱ급 이하의 비밀문서
2. 국가적으로 가치 있는 정보를 내포하고 있는 문서 교범 및 보고를 요하는 연구발표계획
3. 총장 또는 보안심사위원회에서 비밀로 지정하는 문서 등

⑤ 극비(Strictly Confidential)문서는 엄격히 제한된 자만의 접근을 허용하며, 유출 또는 손상되는 경우 대학의 존립에 심각한 영향을 줄 수 있거나 대학 정책상 극비처리가 필요한 문서를 말한다.

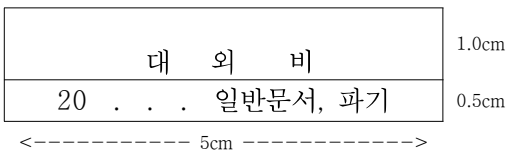
제11조(문서 기본보안) 제11조에 의해 분류된 보안문서는 다음 각 호와 같은 보안기준를 준수하여야 한다.

1. 대외비문서는 제13조의 절차에 의거하여 외부 유출 및 외부자의 접근을 금지시키고 변조가 발생하지 않도록 주기적으로 점검하여야 하며, 전송 시 암호화하고 관련담당자에 의하여 관리되어져야 한다.
2. 비밀(Confidential)문서는 제14조의 절차에 의거하여 비밀취급인가자에 한해서만 관리되어져야 하며, 문서의 보존기한이 만료되었을 경우에는 안전하게 파기되어져야 한다.

3. 극비(Strictly Confidential)문서는 모든 내부·외의 접근을 엄격히 금지하고, 암호화하며, Email등의 파일 전송을 허용하지 않고, 원본파일은 컴퓨터나 휴대용 저장장치에 담을 수 없으며, 경영진만이 열람이 가능하도록 한다.

제12조(대외비의 보호) 대외비문서는 비밀에 준하여 대외비문서관리기록부를 비치하고 다음 각 호와 같이 관리하여야 한다.

1. 대외비를 생성, 보관, 이용하는 단위조직에서 일반문서와 별도로 대외비문서수발부를 비치하여 접수 및 발송번호를 별도로 부여한다.
2. 대외비 문서를 발간하고자 할 때에는 비밀문서 발간의 예에 의하여 정보보호총괄책임자의 협조를 거쳐 발간한다.
3. 보호기간이 경과한 대외비문서는 다음과 같이 처리한다.
   가. 일반문서로 재분류할 경우에는 대외비표지를 대각선을 그어 삭제하고 문서보관, 보존요령에 의하여 보관한다.
   나. 파기하기로 결정한 문서는 비밀문서에 준하여 소각 처리한다.
   다. 보호기간의 표지가 없는 대외비문서는 그 생산처에 조회하여 처리하고, 조회할 수 없는 경우에는 단위조직 장의 내부결재를 받아서 일반문서로 재분류 또는 파기한다.
4. 대외비문서는 비밀에 준하여 비밀보관함에 보관하여야 하며, 일반문서와 혼합 보관하지 말아야 한다.
5. 대외비문서 소유현황은 정기보안 감사 시 정보보호전담부서장에게 통보하고, 그 제출서식은 비밀소유현황 조사서에 의한다.
6. 대외비 문서를 생산하는 경우 그 보호기간을 다음과 같이 구분하여 기입한다.



   가. 보호기간 경과 후 대외비의 효력이 소멸되어 일반문서로 재분류할 수 있는 문건에는 "일반문서"에 O 표시
   나. 보호기간 경과 후에도 대외비의 효력이 지속되나 계속 보관할 필요가 없어 폐기할 문건일 경우에는 "파기"에 O 표시

제13조(비밀의 보호) 비밀의 보호는 다음 각 호와 같이 수행한다.

1. 비밀의 취급, 비밀의 분류 및 재분류는 관련법령에서 정하는 바에 의한다.
2. 비밀문서수발부서는 문서규정 주무부서에서 담당하며 비밀문서 수발담당자는 소속 직원 중 비밀취급이 인가된 직원으로 정한다.
3. 비밀보관부서는 문서규정 주무부서로 하며 집중보관 관리함을 원칙으로 한다.
4. 비밀보관 용기는 철제 2중 캐비넷을 원칙으로 하며 반드시 이중 시건장치를 하여야 한다.
5. 비밀보관책임자는 비밀보관실무부서의 장이 정이 되고 부는 보안담당자가 된다. 다만, 비밀을 분산 보관하였을 경우에는 보관단위 부서장이 보관책임자 정이 되며 별도 부책임자를 임명하여야 한다.
6. 비밀의 인계인수는 비밀관리기록부의 최종 기입란 밑에 2개의 주선으로 마감하고 다음과 같이 인계인수 내용을 기재한다.

비 밀 인 계 인 수

급 비밀 건

위와 같이 정히 인계인수함.

20 년 월 일

인계자	직	성명	(인)
인수자	직	성명	(인)
확인자	정보보호총괄책임자	성명	(인)

7. 비밀을 열람하고자 하는 모든 자는 열람에 앞서 비밀열람기록 전에 관계사항을 기재하고 서명 또는 날인한 후 열람하여야 하며 비밀문서를 결재할 때에도 또한 같다.
8. 보안총괄책임자는 비상시 비밀보안을 철저히 유지 관리하기 위하여 비밀문서 안전지출 및 파기계획을 수립하여야 한다.
9. 보안총괄책임자는 매년 6월말과 12월말 일을 기준하여 비밀취급인가자 및 비밀소유현황을 조사하여 별도관계 서식에 의거 7월 10일 및 차년도 1월 10일까지 교육과학기술부 보안담당관에게 통보하여야 한다.
10. 비밀표지는 관련규정의 서식을 준용한다.

제 4 장 시 설 보 안

제 1 절 일반시설보안

제14조(용어의 정의) 사용하는 용어의 정의는 다음 각 호와 같다.

1. “전산실”이라 함은 각종 정보자산과 부대설비가 전용으로 운영되는 장소를 말하며 관제실과 기계실도 포함될 수 있다.
2. “출입통제시스템”이라 함은 보안이 필요한 장소의 출입 및 퇴실을 자동으로 통제하는 장치를 말한다.

제15조(시설보안 책임) 대학의 시설보안 총괄은 시설보안 주무부서의 장이, 각 단위조직은 소관부서장 또는 소속기관장이 담당한다.

제16조(보호구역 지정) ① 대학의 보호구역은 다음 각 호와 같이 구분한다.

1. 제한지역 : 본 대학 및 부속기관 전역
2. 제한구역 : 총장실, 보직자실, 연구실, 교환실, 보일러실, 방송실, 전산실, 변전소, 첨단산업관련연구소
3. 통제구역 : 비 인가자의 출입이 금지되는 보안상 극히 중요한 지역

② 지정된 보호구역에 대하여는 별도관계 서식에 의한 보호구역대장에 관계사항을 기록 유지하여야 한다.

제17조(보호구역의 관리) ① 통제구역에는 관계직원 및 출입이 인가된 자 외에 출입을 통제하여야 하며 별도 관계 서식에 의한 출입자 명부를 기록 유지하여야 한다.

② 제한구역 및 통제구역에는 그 출입문 중앙상부에 다음과 같은 표지를 하여야 한다. 다만, 총장실을 포함한 보직자실과 연구실 등은 표지를 생략할 수 있다.

제 한 구 역		통 제 구 역

15cm × 30cm

③ 보호구역에는 적당한 곳에 다음과 같은 관리책임자의 표지를 부착하여야 한다.

관 리 책 임 자	
정	
부	

100mm

150mm

제18조(보호구역 관리책임) ① 보호구역 관리책임자는 다음 각 호와 같다.

1. 제한지역

가. 총장, 보직자 집무실 : 비서

나. 연구실 : 각 연구실 책임교수

다. 행정사무실 : 소관부서장

라. 교환실, 보일러실, 전산실, 변전소, 지하공동구 : 동 시설 관리 소관부서장

마. 첨단산업관련 연구소 : 동 시설 관리 소관기관장

2. 통제구역 : 동 시설 관리 소관부서장

② 보호구역 관리책임자는 소속부서 직원 중에서 관리 부책임자를 지정하여야 한다.

③ 보호구역 관리책임자는 매월 1회 이상 자체점검을 실시하여 관리상의 문제점 및 취약개소를 파악하고 이에 대한 대책을 수립하여 보호구역 관리에 철저를 기해야 한다.

제19조(접근통제) ① 보호구역 내 시설물에 대한 출입은 스마트카드를 소지한 인가된 자만의 출입을 허용한다.

② 외부인력의 일시적인 출입 등 정규출입 ID를 발급받지 못한 자의 업무상 출입은 출입허용자의 동반을 수반하여야 한다.

③ 임시출입을 허가 받은 외부인력은 보호구역 출입시 임시출입증을 패용하여야 한다.

④ 스마트카드를 분실 또는 도난당한 자는 즉시 스마트카드 운영 주무부서에 신고하고 재발급 받아야 한다.

⑤ 스마트카드시스템을 관리 운영하는 주무부서는 보호구역출입자에 대한 입·퇴실 정보를 3개월 이상 보관하여야 한다.

⑥ 비인가자의 불법접근 및 시도 발견시 시설보안 주무부서 업무담당자 또는 경비에게 신고하여야 한다.

제20조(중앙전산실 보안) ① 중앙전산실 출입은 대학구성원에 한해 출입카드를 발급받은 인가자를 원칙으로 하며 인가자 이외의 자로서 중앙전산실의 업무와 관련하여 전산실 출입이 필요한 경우에는 시설보안 주무부서의 장의 허가를 얻은 후 출입할 수 있다.

② 중앙전산실의 출입 및 퇴실 관련 기록을 남기고 통제 및 관리를 위해 출입통제시스템을 설치, 운영하여야 한다.

③ 중앙전산실 외측에 과도한 외부 장식을 피하고, 시설물의 기능 및 목적(전산실, 기계실 등)을 표시하는 내/외부의 표시를 최소화한다.

④ 중앙전산실은 재해방지를 할 수 있는 시설을 갖추어야 한다.

제21조(사무실 및 연구실 보호) 최종 퇴실자는 퇴실 시 다음 각 호의 사항을 확인 점검하여야 한다.

1. 캐비넷, 책상, 출입문 등의 잠금 여부

2. 사무용 OA(컴퓨터, 프린터, 복사기 등) 및 전열기의 전원 차단 여부

3. 실내소등 여부

4. 보안기록부 기록 여부
5. 기타 제 보안조치

제 2 절 출입통제시스템 보안

제22조(용어의 정의) 사용하는 용어의 정의는 다음 각 호와 같다.

1. “출입통제시스템”라 함은 건물의 출입구에 설치된 통제장치로서 ”RF출입통제기, 지문인식리더기”로 구분되며 출입자의 신분을 스마트카드로 확인 후 출입지역 입실 허용/불가를 제어하는 장치를 말한다.
2. “스마트카드”라 함은 출입, 출석, 전자지불 등의 목적으로 제작된 구성원의 신분증(모바일 신분증 포함)이라 한다.
3. “출입통제 보유부서”라 함은 출입통제시스템이 설치 된 부서를 말한다.
4. “출입통제 총괄부서”라 함은 출입통제시스템 관련업무를 총괄하는 부서를 말한다.

제23조(역할과 책임) ① 출입통제시스템 총괄책임자는 안전관리 총괄부서장으로 하며 대학의 출입통제에 대한 총괄책임자로서 아래와 각 호의 역할을 수행한다.

1. 출입통제시스템 설치・운영 현황관리
2. 출입통제시스템 위탁관리 자격요건 및 절차마련
3. 출입통제시스템 위탁업체 보안 총괄관리
4. 출입통제시스템용 스마트카드 발급/교육
5. 기타 출입자 보호를 위하여 필요한 업무

② 출입통제시스템 운영책임자는 출입통제 보유부서의 장으로 하며 출입통제 보유부서의 관리담당자에 대한 출입정보보호업무의 지도 및 감독, 출입통제시스템의 접속기록 분석 및 오남용 사고 예방 등의 역할을 수행한다.

③ 출입통제 보유부서의 관리담당자는 업무상 출입정보를 다루고 있는 자이며 출입정보가 분실・도난・유출・변조 또는 훼손되지 아니 하도록 안전성 확보에 필요한 조치를 강구하여야 한다.

제24조(사전통보) 출입통제시스템을 설치하려는 단위조직(부서 또는 학과)은 출입통제시스템 총괄책임자에게 출입통제시스템 설치 계획을 사전협의 후 통보 하여야 한다.

제25조(안내판의 설치) ① 출입통제 보유부서의 장은 관리 건물 내에 다수의 출입통제시스템을 설치하는 경우에는 당해 건물 전체가 출입통제시스템 설치지역임을 명시한 안내판을 출입구에 부착할 수 있다.

② 출입통제 보유부서의 장은 출입통제기를 설치할 경우 정보주체가 이를 쉽게 인식할

수 있도록 아래의 각 호와 같은 사항을 기재한 안내판을 설치하는 등 필요한 조치를 취하여야 한다.

1. 이용안내 및 방법
2. 출입범위 및 시간
3. 담당부서 및 담당자 연락처

제26조(수집의 제한) ① 출입통제시스템에 의하여 출입정보를 수집하는 경우에는 그 설치 목적 범위를 넘어 시스템을 임의로 조작해서는 아니 된다.

② 출입통제시스템에 의하여 출입정보를 수집하는 경우에는 복사하여 유출하여서는 아니 된다.

제27조(출입통제시스템 보유대상의 작성) 출입통제 보유부서의 장은 출입통제시스템의 변동 사항 발생시 출입통제시스템 보유대장(별지 제2호 서식)을 작성하여 정보주체자가 열람 할 수 있도록 하여야 한다.

제28조(처리의 제한) 출입통제 보유부서의 장은 출입정보의 보유목적 내에서 최소한의 범위로 출입정보를 열람하게 하거나 제공해야 한다. 단, 아래 호 중에 해당하는 경우에는 당해 출입정보를 보유목적 외의 목적으로 열람하게 하거나 제공할 수 있다.

1. 정보주체의 동의가 있는 경우
2. 정보주체에게 열람·제공되는 경우
3. 법률에 특별한 규정이 있는 경우
4. 범죄예방·시설안전·화재예방 등 안전관리 목적을 위하여 제공되는 경우
5. 법원의 재판업무수행을 위하여 필요한 경우
6. 기타 보안실무협의회에서 필요하다고 인정하는 경우

제29조(출입정보의 열람 및 제공) ① 출입정보를 열람하거나 제공받고자 하는 개인의 경우에는 출입정보 열람신청서(별지 제4호 서식)를 작성하여 출입통제 보유부서의 장에게 제출하여야 한다.

② 출입정보를 열람하거나 제공받고자 하는 기관의 경우에는 열람목적 및 열람하고자하는 출입정보의 범위를 명시하여 출입통제 보유부서의 장에게 공식문서로 요청하여야 한다.

③ 출입통제 보유부서의 장은 출입정보의 열람 또는 제공을 요청한 기관에게 출입정보를 열람하게 하거나 제공하는 경우에는 출입정보 열람·제공대장(별지 제3호 서식)에 기록하고 이를 관리하여야 한다.

제30조(출입통제시스템 설치 및 관리의 위탁) ① 출입통제 보유부서의 장은 출입통제시스

템 총괄책임자와 협의 후 아래 요건을 갖춘 전문기관에 출입통제시스템 설치 및 관리에 관한 사무를 위탁할 수 있다.

1. 출입정보보호에 필요한 전문 장비 및 기술을 갖출 것
2. 수탁 받은 업무를 수행하는 데 필요한 전문 인력을 갖출 것

② 출입통제시스템의 설치 및 관리에 관한 사무를 위탁하려는 출입통제 보유부서의장은 위탁대상이 되는 사무의 범위, 출입정보에 대한 접근제한 등 출입정보보호에 필요한 사항을 세부적으로 정한 후 이를 위탁계약서 등 관련 서류에 기록하여야 한다.

③ 사무를 위탁한 경우에는 안내판에 수탁기관의 명칭, 담당자 및 연락처를 기재하여 야 한다.

제31조(보유 및 저장기간) ① 출입정보에 대한 기록장소는 관련법령에 의거하여 대학의 보호구역에 한해 기록함을 원칙으로 한다.

② 출입통제시스템에 의하여 수집된 출입정보는 수집 후 30일까지 저장한다.

제32조(비밀유지의 의무) 출입정보를 처리하거나 처리하였던 자는 직무상 알게 된 출입정보를 누설 또는 권한 없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적을 위하여 사용하여서는 아니된다.

제 3 절 CCTV보안

제33조(용어의 정의) 사용하는 용어의 정의는 다음 각 호와 같다.

1. “CCTV”라 함은 일정한 공간에 설치된 촬영기기로 수집한 화상정보를 폐쇄적인 유선 또는 무선 전송로를 통해 특정한 수신자에게만 전송하는 시스템을 말한다.
2. “화상정보”라 함은 CCTV로 촬영된 영상에 의하여 당해 개인의 동일성 여부를 확인할 수 있는 정보를 말한다.
3. “처리”라 함은 CCTV에 의하여 수집되는 화상정보를 입력·저장·전송·편집·삭제 및 재생 그밖에 이와 유사한 행위로서, 수집을 제외한 화상정보의 취급을 말한다.
4. “정보주체”라 함은 화상정보에 의하여 식별되는 사람으로서, 당해 화상정보의 주체가 되는 사람을 말한다.
5. “화상정보 보유부서”라 함은 화상정보를 보유하는 부서를 말한다.
6. “화상정보 총괄부서”라 함은 화상정보보호 업무를 총괄하는 부서를 말한다.

제34조(적용 범위) ① 대학에서 범죄예방·증거확보·시설안전·화재예방 등 공익을 위하여 필요한 경우에 설치·운영하는 CCTV와 이로써 수집·처리되는 화상정보의 보호에 관하여는 법령에 특별한 규정이 있는 경우를 제외하고는 이 내규가 정하는 바에 따른다.

② 대학에서 설치·운영하는 CCTV로서 모조카메라를 부착한 경우에도 실제 화상정보의 취급 여부를 불문하고 이 내규를 적용한다.

제35조(역할과 책임) ① CCTV 총괄책임자는 화상정보 총괄부서장으로 하며 대학의 화상정보보호에 대한 총괄책임자로서 다음과 같은 역할을 수행한다.

1. CCTV 설치·운영 현황관리
2. CCTV 위탁관리 자격요건 및 절차마련
3. CCTV 위탁업체 보안 총괄관리
4. 화상정보보호 교육
5. 기타 화상정보보호를 위하여 필요한 업무

② CCTV 운영책임자는 화상정보 보유부서장으로 하며 화상정보취급 담당자에 대한 화상정보보호업무의 지도 및 감독, 화상정보 시스템의 접속기록 분석 및 오남용 사고 예방 등의 역할을 수행한다.

③ CCTV 운영담당자는 업무상 화상정보를 다루고 있는 자이며 화상정보가 분실·도난·누출·변조 또는 훼손되지 아니 하도록 안전성 확보에 필요한 조치를 강구하여야 한다.

제36조(영상정보처리기기의 설치·운영 제한) ① 다음 각 호의 경우를 제외하고는 대학 내의 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우

제37조(사전통보) CCTV를 설치하려는 부서(또는 학과)는 화상정보 총괄부서장에게 CCTV 설치 계획을 사전 협의 후 통보 하여야 한다.

제38조(안내판의 설치) ① 화상정보 보유부서장 관리 건물 내에 다수의 CCTV를 설치하는 경우에는 당해 건물 전체가 CCTV 설치지역임을 명시한 안내판을 출입구에 부착할 수 있다.

② 화상정보 보유부서장은 CCTV를 설치할 경우 정보주체가 이를 쉽게 인식할 수 있도록 아래와 같은 사항을 기재한 안내판을 설치하는 등 필요한 조치를 취하여야 한다.

1. 설치목적 및 장소
2. 촬영범위 및 시간
3. 담당부서 및 연락처
4. 운영책임자 및 연락처

제39조(CCTV 설치 및 관리의 위탁) ① 화상정보 보유부서장은 다음 각 호의 요건을 갖춘 전문기관에 CCTV 설치 및 관리에 관한 사무를 위탁할 수 있다.

1. 화상정보보호에 필요한 전문 장비 및 기술을 갖출 것
2. 수탁 받은 업무를 수행하는 데 필요한 전문 인력을 갖출 것

② CCTV의 설치 및 관리에 관한 사무를 위탁하려는 화상정보 보유부서장은 위탁대상이 되는 사무의 범위, 화상정보에 대한 접근제한 등 화상정보보호에 필요한 사항을 세부적으로 정한 후 이를 위탁계약서 등 관련 서류에 기록하여야 한다.

③ 사무를 위탁한 경우에는 안내판에 수탁기관의 명칭, 담당자 및 연락처를 기재하여야 한다.

제40조(수집의 제한) ① CCTV에 의하여 화상정보를 수집하는 경우에는 그 설치목적 범위를 넘어 카메라를 임의로 조작하거나 다른 곳을 비추어서는 아니 된다.

② CCTV에 의하여 화상정보를 수집하는 경우에는 녹음기능을 사용하여서는 아니 된다.

제41조(화상정보대장의 작성) 화상정보 보유부서장은 화상정보 생성시 화상정보대장(별지 제5호 서식)을 작성하여 정보주체자가 열람 할 수 있도록 하여야 한다.

제42조(처리의 제한) 화상정보 보유부서장은 보유목적 이외의 용도로 화상정보가 활용되거나 접근권한을 부여받은 자 이외의 타인에게 열람·제공되지 않도록 하여야 한다. 단, 아래의 어느 하나에 해당하는 경우에는 당해 화상정보를 보유목적 외의 목적으로 열람하게 하거나 제공할 수 있다.

1. 정보주체의 동의가 있는 경우
2. 정보주체에게 열람・제공되는 경우
3. 법률에 특별한 규정이 있는 경우
4. 신문・방송을 통한 언론보도의 목적을 위하여 필요한 때로서 특정 개인을 알아 볼 수 없는 형태로 제공하는 경우
5. 범죄의 수사와 공소의 제기 및 유지에 필요한 경우
6. 법원의 재판업무수행을 위하여 필요한 경우
7. 기타 보안실무협의회에서 필요하다고 인정하는 경우

제43조(화상정보의 열람・제공・삭제) ① 화상정보를 열람하거나 제공받고자 하는 기관은 열람목적 및 열람하고자 하는 화상정보의 범위를 명시하여 화상정보 보유부서장에게 문서로 요청하여야 한다.

② 정보주체는 화상정보 보유부서장에게 화상정보 열람 및 삭제 신청서(별지 제7호 서식)를 제출하여 화상정보의 열람이나 삭제를 청구 할 수 있다. 단, 아래의 어느 하나에

해당하는 경우에는 열람 및 삭제를 거부할 수 있다.

1. 화상정보의 보관기간이 경과하여 파기 또는 삭제한 경우
2. 범죄수사・공소유지・재판수행에 중대한 지장을 초래하는 경우
3. 특정 정보주체의 화상정보만을 삭제하는 것이 기술적으로 현저히 곤란한 경우
4. 제1항에 따른 청구에 필요한 조치를 취함으로써 타인의 사생활이 침해될 우려가 큰 경우
5. 기타 열람 등의 청구를 거절할 만한 정당한 공익적 사유가 존재하는 경우

③ 화상정보 보유부서장은 화상정보의 제1항과 2항의 요청에 따라 화상정보를 열람하게 하거나 제공・삭제하는 경우에는 화상정보 관리대장(별지 제6호 서식)에 기록하고 이를 관리하여야 한다.

제44조(보유 및 삭제) CCTV에 의하여 수집된 화상정보는 수집 후 30일 이내 삭제함을 원칙으로 하며, 단, 법령에 보유기간이 명시되어 있는 경우와 특별한 목적이 있을 시에는 예외로 한다.

제45조(비밀유지 의무) 화상정보를 처리하거나 처리하였던 자는 직무상 알게 된 화상정보를 누설 또는 권한 없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적을 위하여 사용하여서는 아니 된다.

부 칙

1. 이 세칙은 2012년 11월 28일부터 제정, 시행한다.
2. 이 세칙 시행이전에 처리된 업무는 이 세칙에 의하여 처리된 것으로 본다.
3. 이 세칙의 제정 시행일 이전의 인적보안관리세칙, 문서보안관리세칙, 시설보안관리세칙은 이 세칙으로 통합됨으로 제정일 기준으로 폐지한다.

정보보호서약서

성 명 :
주민등록번호 :

본인은 포항공과대학교(이하 '대학'이라 함)의 보안업무규정 및 관련 세칙을 충분히 숙지하고 성실히 준수할 것을 서약합니다.

1. 채용 시 정보보호 준수사항
   ① 대학으로부터 취득한 정보 또는 대학과 연관된 업무와 관련하여 취득한 모든 정보는 대학 설립 목적 본연의 업무에 한해 이용한다.
   ② 대학의 구성원으로서 업무를 수행하더라도 이전의 고용인 또는 기타 외부 조직이나 개인의 독점적인 정보를 기밀로 하는 계약 또는 의무를 위반하지 않는다. 대학의 업무를 수행하는데 있어서 이전 고용인 또는 기타 기업, 개인의 서면 위임장 없이 그들의 독점적인 정보를 사용하지 아니한다.
   ③ 업무상 사용하는 각종 서류, 사진, 자기테이프, 전산장비 등 정보를 기록한 매체를 주의 깊게 사용, 보관함으로써 무단변조, 복사, 훼손, 분실, 멸실, 기밀 누설 등의 사고를 미연에 방지할 수 있도록 최선을 다한다.
   ④ 업무상 또는 각종 연구 과정, 회의 및 세미나 등에서 취득한 대학의 중요 운영사항 또는 운영정보, 연구물 등을 누설하지 않는다.
   ⑤ 업무상 허가 받지 않은 정보나 시설에 접근하지 않으며 업무 이외의 용도로 대학이 설립 목적상 보유하고 있는 데이터 처리 및 보관 시설을 사용하지 않는다. 또한 이 시설 내에 사적 정보를 보관하지 아니한다.
   ⑥ 대학에서 제공된 정보자산을 대학의 업무 목적 이외에는 사용하지 아니하며 대학의 정보자산을 대학의 허락 없이 대학 밖으로 유출하지 아니한다.
   ⑦ 대학의 업무관련 문서의 생성, 사용, 폐기시 정보보호규정 및 세칙에 따른다.
   ⑧ 이외 사항에 대해서는 교내 정보보호규정 및 세칙에 정의되어 있는 규정의 내용에 동의하고 준수할 것을 약속한다.

2. 퇴직 시 정보보호 준수사항
   ① 퇴직 시 대학에서 제공 받은 모든 대학소유 정보자산을 즉시 대학에 반납한다.
   ② 어떠한 장소에 어떠한 방법으로도 대학의 비밀 및 정보자산을 보유하거나 저장하고 있지 않음을 약속한다.
   ③ 재직기간 중 취득한 대학의 모든 중요 기밀(운영 관련 자료 및 연구결과물 등을 포함)을 퇴직 후에도 대학의 업무 인수. 인계와 관련 없는 어떠한 대학내외 기타 외부 인력에게도 누설하지 않는다.
   ④ 퇴직 후 3년간 기타 외부 인력을 위하여 대학의 비밀을 누설하거나 사용하지 않는다.
   ⑤ 대학의 비밀 보호를 위한 노력에 적극 협조할 뿐 아니라, 그에 따른 법적. 도덕적 의무를 성실히 이행한다.

본인은 위의 사항을 숙지하여 이를 성실히 준수할 것이며 만일 이를 위반하였을 경우 관련 법령 및 대학의 규정에 따라 일체의 책임을 감수할 것을 서약합니다.

200 년 월 일 서약자: (인)

포항공과대학교 정보보호위원장 귀하

(별지 제2호 서식) 출입통제시스템 보유대장

출입통제시스템 보유대장(기존/변동)

(1) 보유부서	
(2) 설치위치	
(3) 성 능	
(4) 설치수량(대)	
(5) 설치(변경)일자	
(6) 위탁기관	
(7) 범 위	
(8) 작동시간	
(9) 안내판부착장소	
(10) 설치목적	
(11) 저장매체	
(12) 보유기간	
(13) 삭제방법	

출입정보 열람·제공대장

(1) 출입정보 명	
(2) 열람·제공기관	
(3) 열람·제공일자	
(4) 열람·제공주기	
(5) 열람·제공형태	
(6) 열람·제공기간	
(7) 열람·제공 목적	
(8) 열람·제공 근거	
(9)열람·제공 요청일	
(10) 비 고	

(별지 제4호 서식) 출입정보 열람신청서

출입정보 열람신청서

<table>
<tr><td rowspan="3">(1) 청구인</td><td>성명</td><td></td><td>전화번호</td><td></td></tr>
<tr><td>생년월일</td><td></td><td>소 속</td><td></td></tr>
<tr><td>e-mail</td><td colspan="3"></td></tr>
<tr><td rowspan="3">(2) 열람내역</td><td>설치장소</td><td colspan="3"></td></tr>
<tr><td>요청일시</td><td colspan="3"></td></tr>
<tr><td>내 용</td><td colspan="3"></td></tr>
<tr><td rowspan="3">(3) 보유부서
(담당자 작성)</td><td>부서명</td><td colspan="3"></td></tr>
<tr><td>담당자 성명</td><td colspan="3"></td></tr>
<tr><td>담당자 서명</td><td colspan="3"></td></tr>
<tr><td colspan="5">년 월 일

청구인: (서명 또는 인)</td></tr>
</table>

화상정보대장

(1) 보유부서			
(2) 설치위치			
(3) 성능	음성녹음	줌인	회전
	(가능/불가능)	(가능/불가능)	(가능/불가능)
(4) 설치수량(대)			
(5) 설치일자			
(6) 위탁기관			
(7) 촬영범위			
(8) 촬영시간			
(9) 안내판 부착장소			
(10) 설치목적			
(11) 저장매체			
(12) 보유기간			
(13) 삭제방법			

(별지 제6호 서식) 화상정보 관리대장

화상정보 관리대장

번호	구분	일시	파일명/형태	담당자	목적/사유	요청자	이용·제공 근거	이용·제공 형태	기간
1	□ 이용 □ 제공 □ 열람 □ 파기								
2	□ 이용 □ 제공 □ 열람 □ 파기								
3	□ 이용 □ 제공 □ 열람 □ 파기								
4	□ 이용 □ 제공 □ 열람 □ 파기								
5	□ 이용 □ 제공 □ 열람 □ 파기								
6	□ 이용 □ 제공 □ 열람 □ 파기								
7	□ 이용 □ 제공 □ 열람 □ 파기								

(별지 제7호 서식) 화상정보 열람 및 삭제 신청서

화상정보 ([] 열람, [] 삭제) 신청서

청구인	성명		전화번호	
	생년월일		정보주체와의 관계	
	주소 /e-mail			
정보주체	성명		전화번호	
	생년월일			
	주소 /e-mail			
청구내용 (구체적으로 요청하지 않으면 처리가 곤란할 수 있음)	요청 화상정보 기록기간	년 월 일(시 분) ~ 년 월 일(시 분)		
	영상정보 처리기기 설치장소			
	청구 목적 및 사유			

「표준 개인정보 보호지침」 제52조에 따라 위와 같이 개인영상정보의 존재확인, 열람을 청구합니다.

년 월 일

청구인 (서명 또는 인)

보유부서	부서명	
	담당자 성명 및 확인서명	(서명 또는 인)