정보보호 규정

한국항공대학교

개정 기록표

번호	개정일자	개정자 (서명)	번호	개정일자	개정자 (서명)
1	2014.4.22.		16		
2	2021.12.13		17		
3			18		
4			19		
5			20		
6			21		
7			22		
8			23		
9			24		
10			25		
11			26		
12			27		
13			28		
14			29		
15			30		

정보보호 규정

제 1 장 총 칙

제1조 (목적) 본 규정은 한국항공대학교(이하 ”본 대학교“라 한다.)의 보안요구사항에 대한 정보보호 관리체계의 방향성을 제시하고, 이를 바탕으로 관련 법규 및 기타 계약상의 요구에 대응하며, 비 인가자에 의한 정보의 오남용, 훼손, 변조, 유출 등의 위협으로부터 중요 정보 자산을 보호하여 업무의 연속성을 보장하고, 정보보호 사고로 인한 시스템 및 자원의 피해를 최소화하기 위한 기본 방침을 정립하는 것을 목적으로 한다.

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

1. “정보”라 함은 본 대학교 업무와 관련하여 생성 또는 입수하여 소유하고 있는 지적 자산 등의 자료로서, 컴퓨터나 저장매체에 기록된 자료를 말한다.
2. “정보시스템”이라 함은 다양한 서비스 제공을 위해 사용 또는 관리하는 모든 컴퓨터 하드웨어와 시스템 소프트웨어, 응용프로그램 등을 통칭하며, PC를 포함한다.
3. “전산망”이라함은 본 대학교 내에 설치한 유무선 전산망 및 CCTV망 설비를 통칭한다. 단, 각 단위 기관에서 임의로 설치 운영하는 LAN설비 등은 제외하며, 만약 이를 전산망에 접속할 경우는 전산망측 접속장치까지만 전산망으로 간주한다.
4. “보안시스템”이라함은 정보시스템 및 전산망을 침해사고로부터 보호하기 위해 설치한 각종 하드웨어 및 소프트웨어를 말한다.
5. “정보자산“이라 함은 정보와 정보시스템, 전산망, 보안시스템 등을 통칭한다.
6. “정보 관련 자산”이라 함은 정보자산 구축 및 운영에 필요한 인력, 시설, 장비, 관련 도서(설계서, 매뉴얼 등) 등을 말한다.
7. "이용자"라 함은 대학이 제공하는 정보서비스를 이용하는 자를 말한다.
8. "정보보호책임자(이하 "CSO"라 한다.)라 함은 정보서비스의 안정성 확보 및 정보보호 업무를 총괄하는 자를 말한다.
9. "정보보호관리자"라 함은 정보서비스에 이용되는 정보시스템을 총괄 관리하는 자를 말한다.
10. “외부자”라 함은 본 대학교와 계약에 의해 용역 및 서비스를 제공하는 외부 전문가 및 외부용역업체, 기타 본 대학교 정보자산에 접근이 허용된 자 및 업체를 말한다.
11. "침해사고"라 함은 외부 또는 내부의 악의적인 사용자에 의한 비인가 된 시스템 사용, 사용자 계정의 도용, 악성코드(웜/바이러스) 유입 및 실행, 정보시

스템 방해 등 시스템의 서비스를 왜곡 또는 지연시키거나 시스템을 파괴, 데이터를 변조, 삭제하는 등의 행위를 말한다.

12. “취약점”이라함은 시스템의 기능명세, 설계 또는 구현단계의 오류나 시동, 설치 또는 운용상의 문제점으로 인하여 시스템이 지니게 되는 보안상의 약한 부분을 말한다.

제3조 (수범자 및 적용대상) ① 본 규정은 본 대학교 전 구성원 및 외부자를 수범자로 한다.

② 본 규정은 본 대학교가 보유 및 운영하고 있는 정보자산 및 정보 관련자산을 대상으로 한다.

제4조 (정보보호 요구사항) 본 대학교의 정보자산은 다음과 같은 요구사항을 충족하여야 한다.

1. 기밀성 : 정보가 권한이 없는 사람에게 공개되지 않아야 한다.
2. 무결성 : 정보가 권한이 없는 사람에 의해 변경되지 않고, 정확하고 완전한 상태로 유지되어야 한다.
3. 가용성 : 권한이 있는 사람이 정보에 대한 접근을 필요로 할 때, 적정한 시간 내에 이용 가능해야 한다.

제5조 (정보보호 기능 요구사항) 정보자산에 대한 정보보호 요구사항을 충족하기 위하여 보안 관리는 다음과 같은 기능 요구사항을 충족하여야 한다.

1. 권한 관리 : 정보자산을 업무특성 및 중요도에 따라 분류하고 사용자별로 업무수행에 따른 역할에 따라 정보자산에 대한 접근권한을 부여하고 관리하여야 한다.
2. 식별 및 인증 : 정보자산에 접근하고자 하는 사용자를 식별하고 확인하여야 한다.
3. 접근 통제 : 식별된 사용자에게 주어진 권한에 따라 정보자산에 대한 접근을 통제하여야 한다.
4. 책임 추적 : 정보 및 정보시스템의 소유자, 운영자, 사용자의 의무 및 책임을 명확히 하고 특정 활동의 책임을 추적할 수 있어야 한다.
5. 기타 기능 : 정보자산에 따라 기밀성, 무결성, 가용성 및 준법성 요구에 적합한 기능이 제공되고 관리되어야 한다.

제6조 (정보자산 사용자) 인가된 정보 자산만을 이용할 권한을 가지며, 본 규정을 준수할 의무와 불법 사용에 대한 최종 책임을 갖는다.

제7조 (준수 확인) ① 정보자산 사용자의 본 규정 위반은 본 대학교 인사규정에 따라 징계되며, 사안에 따라서는 고발 조치 될 수 있다.

② 정보자산 사용자가 본 규정을 위반하여 본 대학교에 재산상의 손실을 입히거나 이미지를 훼손시킬 경우에는 민·형사상의 모든 책임을 진다.

제 2 장 정보보호 조직

제8조 (정보보호심사위원회) ① 대학 보안업무의 효율적인 운영과 업무계획의 수립과 기

타 보안에 관한 중요한 사항을 심의하기 위하여 정보보호심사위원회를 운영한다.

② 정보보호심사위원회는 대학 정보화추진위원회에서 겸한다.

③ 정보보호심사위원회는 다음 각 호의 사항을 심의 및 의결하고 결과를 총장에게 보고한다.

1. 정보보호 규정 및 내규의 수립 및 그 개정에 관한 사항
2. 분야별 정보보호대책의 수립에 관한 사항
3. 정보보호 위반자 심사와 처리에 관한 사항
4. 연간 정보보호 업무 지침 수립과 그 이행 상태의 확인 처리에 관한 사항
5. 각 부서로부터 제청된 각종 정보보호사항
6. 정보보호 업무 심사 분석 및 정보보호 업무 수행상 조정과 협의를 요하는 사항
7. 기타 위원장이 필요하다고 인정하는 사항

제9조 (정보보호전문위원회) ① 정보보호심사위원회 산하에 정보보호전문위원회를 다음 각 호와 같이 둔다.

1. 위원장을 포함하여 6인 내외의 위원으로 구성한다.
2. 위원은 정보보호를 취급하는 관련 주요부서들의 팀장(총무팀장, 교무팀장, 학생지원팀장)을 당연직으로 하고, 위원장이 추천하는 전문 자문위원 2인 내외로 구성한다.
3. 위원장의 역할은 정보보호책임자가 수행하고, 간사의 역할은 정보보호관리자가 수행한다.
4. 위원장을 포함한 각 위원의 임기는 보직 재임기간 및 해당업무기간으로 한다.

② 정보보호전문위원회는 다음 각 호의 사항을 전문적으로 심의 및 검토하고 의결안을 도출하여 정보화추진위원회에 상정한다.

1. 정보보호 정책·규정 및 대책 수립에 관한 사항
2. 정보보호 신규 추진 사업 및 연간계획 수립에 관한 사항
3. 정보보호 위반자 심사 및 처리 사항
4. 기타 위 각호에 부수되는 제반 사항

제10조 (정보보호 조직) ① 정보보호 조직은 정보보호책임자와 정보보호 담당부서로 구성한다.

② 정보보호 담당부서는 정보보호관리자(정보보호 실무 책임자) 및 정보보호담당자(정보보호 실무 운영자), 침해사고대응팀(침해사고예방/탐지/대응 전담)으로 구성한다.

③ 정보보호책임자는 전산정보원장, 정보보호관리자는 전산정보전략팀장이 겸임한다.<개정 2014.4.22.>

④ 정보보호 담당부서는 전산정보원 전산정보전략팀이 된다.<개정 2014.4.22.>

제11조 (정보보호책임자의 책무) 정보보호책임자는 정보보호 관련 업무를 총괄하며, 다음

과 같은 업무를 수행한다.

1. 정보보호전문위원회 위원장으로 참여
2. 정보보호 정책 및 규정의 검토
3. 정보보호 대책의 수립
4. 정보보호 업무의 지휘 감독 등

제12조 (정보보호관리자의 책무) ① 정보보호관리자는 정보보호 담당부서의 부서장이 담당한다.

② 정보보호관리자는 정보보호담당자의 업무를 관리 감독하여야 한다.

③ 정보보호관리자는 시스템관리자가 타부서로 전보되거나 퇴직할 경우 계정삭제 등 정보보호를 위한 적절한 조치를 취하여야 한다.

④ 정보보호관리자는 정보침해사고 발생에 대비하여 비상연락망, 응급조치 절차 및 복구대책을 포함하는 정보침해사고대응계획을 수립하고 이를 시행하여야 한다.

⑤ 정보보호관리자는 정기적으로 정보시스템의 보안취약점을 점검 분석하여 그 결과를 정보보호책임자에게 보고하여야 한다.

⑥ 정보보호관리자는 정기적으로 이용자접속기록을 분석하여 정보침해사고를 예방하고, 정보침해사고가 발생한 경우에는 즉시 필요한 조치를 취하여야 한다.

⑦ 정보보호관리자는 정보통신 설비 및 정보통신시설에 대한 부정한 접근을 방지하기 위한 적절한 조치를 취하여야 한다.

제13조 (정보보호담당자의 책무) 정보보호담당자는 정보보호관리자가 선임하며, 다음과 같은 정보보호 관련 실무업무를 담당한다.

① 시스템관리자는 정보통신망에 운용되는 데이터를 그 중요도에 따라 분류하고 적절한 관리기준 및 절차를 수립 시행하여야 한다.

② 시스템관리자는 중요데이터는 암호화하거나 파일 잠금 기능을 사용해 관리하여야 하며 필요한 경우 이용자 접근을 통제하여야 한다.

③ 시스템관리자는 침해사고, 시스템 장애, 정전 등으로부터 정보를 보호하기 위해 정기적으로 데이터백업 등 적절한 조치를 취하여야 한다.

⑤ 시스템관리자는 주요자산이 정상적인 가동상태로 운영되도록 노력하여야하며, 정보침해사고나 시스템장애가 발생했을 경우 이를 즉시 정보보호관리자에게 보고하여야 한다.

제14조 (침해사고대응팀의 역할) ① 정보보호관리자는 정보보호 사고를 사전에 탐지하고 예방하며, 침해사고 발생 시 신속하고 효과적으로 사고를 처리하고 복구하기 위해 침해사고대응팀을 구성하여 운영하며, 다음과 같은 업무를 담당한다.

1. 침해사고 예방을 위한 정기적인 취약점 분석
2. 침해사고 예방기술 연구 및 교육
3. 침해사고 발생 접수 및 처리
4. 침해사고 복구
5. 외부 기관과의 협력창구 마련

② 침해사고대응팀은 대외 유사기관과의 협력체계 유지 및 침해사고에 대한 전문적 기술 확보를 위해 외부 전문 인력을 이용하여 별도 조직으로 구성할 수 있다.

③ 침해사고대응팀원은 정보보호담당자를 중심으로 구성하며 필요에 따라 정보보호 업무 이외의 업무담당자를 포함할 수 있다.

제 3 장 정보보호

제1절 정보자산관리

제15조 (정보자산 분류) ① 정보 : 데이터베이스(DB)나 파일의 형태로 저장된 전자정보 및 정보자산 운영에 필요한 문서 등

② 소프트웨어 : 운영체제(OS), 시스템소프트웨어(웹서버, 웹어플리케이션서버, 데이터베이스관리시스템 등), 사무자동화 소프트웨어, 업무용 응용프로그램, 보안소프트웨어, 통신소프트웨어, 기타 개발 및 관리용 소프트웨어 등

③ 하드웨어 : 컴퓨터 및 컴퓨팅자원(서버, PC 등), 스토리지장비, 백업장비, 전산망장비(스위치, 라우터, 허브, 전화교환기 등), 보안장비, 기록매체 등

④ 부대설비 : 전원공급장치, 항온항습기, 출입통제장비, UPS, CCTV 등의 부대설비 자산 등

제16조 (정보자산의 등급) 정보자산의 등급은 정보자산의 기밀성, 무결성, 가용성에 대하여 평가하고 침해사고 발생시, 재정적, 이미지손실, 사생활침해, 경쟁력, 업무운영 면에서의 손실을 측정하여 다음과 같이 분류한다.

1. 1등급(VL) : 재정적 손실만이 있으며 그 정도가 미미함
2. 2등급(L) : 재정적, 이미지손실 등의 면에서 약간의 손실은 있으나. 법에 위배되지 않음
3. 3등급(M) : 법에 위배되며, 소규모 재정적 손실과 조직운용과 관리 등에 지장을 초래함
4. 4등급(H) : 법에 위배되며, 중규모 재정적 손실과 운용업무 등에 심각한 영향을 초래함
5. 5등급(VH) : 법에 위배되며, 대규모 재정적 손실과 경쟁력에 심각한 영향을 미처, 조직 자체의 존립에 영향을 초래함

제17조 (정보자산 목록관리) ① 정보보호담당자는 본 대학교 자산목록을 바탕으로 정보자산목록을 작성하여 관리하여야 한다.

② 정보보호담당자는 정보자산목록에 등록된 자산에 대해 자산 평가를 실시하고 자산의 등급을 파악한다.

③ 정보보호담당자는 해당부서의 정보시스템, 보안시스템, 전산망 장비 등의 도입, 설치, 변경, 매각, 폐기 등의 사유로 보안성 검토 요청 시, 정보자산목록도 갱신하여 최신의 상태로 유지하여야 한다.

④ 정보보호관리자는 연 1회 정보자산목록을 토대로 자산현황을 점검하고 변경사항을 갱신 한다. 자산실사 결과 및 변경사항에 대해서는 정보보호책임자에게 보고한다.

제18조 (정보자산의 도입 시 보안성 검토) ① 안전성 및 침해사고의 방지를 위해 보안시스템, 소프트웨어 등과 같이 보안성 검토가 요구되는 정보자산의 도입 시에는 규정된 구매절차와 더불어 보안성에 대한 검토를 실시한다.
단, 공신력 있는 기관의 인증된 제품에 대해서는 생략할 수 있다.

② 보안성 검토는 정보보호담당부서에 의해 수행되어야 하며, 필요 시 외부보안 전문가 및 전문 업체를 통한 협력검사를 실시한다.

③ 보안성에 대한 검토 결과를 장비선택에 대한 평가 자료에 반영한다.

제19조 (정보자산의 설치 및 변경) ① 정보자산의 설치 및 변경으로 인하여 서비스 연속성에 영향이 있을 경우는 이를 사전에 공지하여야 한다.

② 정보자산의 설치 및 변경 시에는 보안관련 기술적 보안 조치사항을 고려하여 적용한다.

③ 정보자산의 관리부서는 설치 또는 변경되는 정보자산에 대한 보유현황을 최신의 상태로 유지하여야 한다.

④ 보안시스템, 정보시스템, 전산망 장비 등 보안성이 요구되는 정보자산의 설치가 종료된 후에는 관리 담당자는 보안설정 및 보안기능 등이 정상적으로 설치되었는지 확인하고, 정보보호부서에 검토를 요청한다.

⑤ 보안시스템과 기밀정보를 처리하는 서버, 주요 전산망 장비는 설치 시 다음 사항을 준수하여야 한다.

1. 제한 구역 내에 설치하여야 하며, 24시간 X 365일 모니터링 가능한 곳에 설치 운영 하고 비인가자의 불법접근 및 오용이나 남용을 방지하기 위하여 물리적인 출입 통제가 시행되도록 한다.
2. 설치 위치를 설정함에 있어 화재, 침수, 홍수, 지진 등 발생 가능한 다양한 형태의 위험을 고려하여야 한다.
3. 장비가 위치한 곳에서의 음식물, 인화성물질 등의 반입 및 흡연을 금지한다.

제20조 (정보자산의 매각 및 폐기) ① 하드웨어의 매각이나 폐기 시 해당 하드웨어 관리자는 반출 전에 하드웨어에 적재된 모든 구성설정정보, 로그정보, 비밀번호 등을 포함한 일체의 내용을 초기화 또는 삭제하여야 한다.

② 하드디스크 등의 저장장치가 부착된 하드웨어(서버, 스토리지, PC 등)는 매각이나 폐기 시, 분리하여 별도 파기하거나 기록된 데이터를 삭제하고 포맷하여야 한다.

③ 하드웨어 관리자는 매각이나 폐기장비 반출 전에 정보보호담당부서에 확인을 요청하여야 한다.

④ 백업 미디어 등과 같은 기록매체는 폐기 시 데이터 삭제 및 포맷 후 폐기하여야 하며, 필요한 경우 물리적으로 완파하여야 한다.

⑤ 정보자산 운영에 필요한 문서 등은 안전하게 파쇄 또는 소각해야 한다.

⑥ 정보자산의 폐기를 전문 업체를 통해 시행할 경우, 정보의 유출과 관련한 보안사항을 계약서에 반영하여야 한다.

제21조 (위험 분석) 보호하여야 할 정보자산에 대한 효과적인 보호대책 수립을 위하여 매년 1회 정보보호 감사 수행 시 실시한다. 본 대학교의 위험분석 방안은 다음과 같다. 단, 위험분석을 위해 외부 전문기관에 의뢰한 경우 해당 전문기관의 위험분석 방법론에 따라 자산분석 및 위험분석을 수행할 수 있다.

1. 자산평가 : 본 규정 제 16조에 따른다.
2. 위협평가 : 대상 자산에 피해를 가 할 수 있는 잠재적인 위협 요소를 파악하고 , 이러한 위협의 발생 확률 또는 빈도와 자산에 대한 해를 입는 정도 등을 기준으로 평가한다.
3. 취약성평가 : 정보자산이나 조직 목표에 손해를 끼치는 원인이 될 수 있는 각종 시스템, 소프트웨어, 조직, 절차 등의 약점을 확인하고 평가한다.
4. 위험평가 : 자산, 위협, 취약성 평가 결과에 따라 6등급으로 평가한다.

제22조 (보호대책 수립) ① 보호대책 구현의 효과적인 이행을 위하여 수용 가능한 위험의 수준(DoA: Degree of Assurance)을 정하고, DoA 이하의 심각도가 낮은 위험은 수용 가능한 위험으로, DoA를 초과하는 심각도가 높은 위험은 수용 불가능한 위험으로 분류한다.

② 수용 불가능한 위험에 대하여, 위험을 완화시키기 위한 통제방안을 국내·외 보안관리 기준의 통제항목에서 차용하고, 이를 구체적으로 구현하기 위한 보호대책을 수립한다.

제2절 인사 보안 및 보안 교육

제23조 (인사 보안) ① 정보보호의 위협과 취약점에 대해 관련자들이 해당 내용을 충분히 이해하고, 정보보호 정책에 따라 업무를 수행해야 한다.

② 정보 시스템을 사용하는 모든 구성원 및 제 3자에 의한 실수, 사기, 도난, 오용 등으로부터 초래되는 위험을 제거하거나 최소화하기 위한 방안들을 수립해야 한다.

③ 이와 관련된 사항은 본 대학교의 “보안업무에 관한 규정”(이하 보안업무규정) 제 3장 에서 정한 바에 따른다.

제24조 (정보보호 교육) ① 정보보호 교육은 전 교직원을 대상으로 정보보안 교육 및 개인정보보호 교육을 각 연 1회 실시한다.<개정 2021.12.13.>

② 교직원의 채용/전보(인사이동) 시 보안업무 규정 제 52조에 의거하여 정보보호 교육을 실시하여야 하며, 이후에는 연간 정보보호교육계획에 따라 시행한다.

③ 다음과 같은 사항의 발생 시 비정기적인 교육을 실시 할 수 있다.

1. 정보보호 정책·규정 또는 직무 등의 변경
2. 새로운 보안위협의 발생

3. 법적 요구사항에 대한 대책수립
4. 기타, 본 대학교의 정보보호 관리업무와 관련한 교육의 필요성이 있는 경우

④ 정보보호 교육계획수립은 정보보호 담당부서가 하며, 교육의 시행은 교육전담부서(사무처 총무팀)가 맡는다.

⑤ 정보보호 담당부서는 정책 및 규정, 보안가이드라인의 제·개정 등이 이루어진 경우, 필요에 따라 비정기 보안교육을 시행할 수 있다.

⑥ 정보보호 담당부서는 정보보호 교육계획을 충실히 이행하고 교육실적을 관리하여야 한다.

⑦ 정보보호 담당부서는 전자 게시판 등을 활용하여 직원의 정보보호 인식제고를 위한 지속적인 홍보를 실시한다.

⑧ 외부자에 대한 교육은 정보보호 담당부서 및 업무주관부서의 협의에 따라, 업무수행 시작 시점과 업무수행 중 필요 시 시행하며, 교육의 내용은 해당 외부자의 업무에 따라 정의한다.

제25조 (정보보호 교육 계획 수립) ① 정보보호 담당부서는 전 교직원을 대상으로 정보보안 교육 및 개인정보보호 교육을 각 연 1회 실시가 가능한 연간 정보보호 교육계획을 수립하여 정보보호책임자의 승인을 득하여야 한다.<개정 2021.12.13.>

② 보안교육 계획에는 교육 종류, 대상, 내용, 강사, 시행 일시 및 장소 등이 포함되어야 한다.

③ 필요 시 외부 전문가에게 위탁하여 해당 보안 교육을 실시할 수 있으며, 위탁교육을 실시하여야 하는 경우 사전에 해당 전문가를 선정하여 교육 계획을 협의하도록 한다.

④ 보안교육 실시 후 피교육자에게 설문을 실시하여 결과를 추후 교육계획 진행에 반영하도록 한다.

⑤ 보안 교육 이수 여부를 관리하여 누락 및 중복이 발생하지 않도록 한다.

제26조 (정보보호 교육 평가) ① 정보보호 담당부서는 피교육자에게 작성 받은 설문을 토대로 교육의 효과 및 문제점을 분석하여 추후 보안교육 진행에 반영하도록 한다.

② 보안교육 시행 결과에는 교육 대상, 일시, 장소, 내용, 참석자 명단(미참석자 표시), 설문 결과 등의 내용을 포함한다.

제27조 (정보보호 교육 내용) ① 정기 및 비정기적인 교육은 피교육자의 업무 영역과 수준에 따라 세부 내용을 조정하고 가능한 최신의 상위 정책 및 규정, 보안가이드라인, 보안관리 동향 등이 전달될 수 있도록 구성한다.

② 교직원 대상 시 정기 및 비정기적인 교육은 해당 업무의 특성을 고려하여 다음과 같은 내용으로 구성 할 수 있다.

1. 정보보호 정책, 규정의 소개 및 설명
2. 정보보호 관련 법률
3. 업무용 PC관련 보안
4. 기타 보안관련 사항 등

③ 외부자 대상 시, 계약서상의 보안요구사항, 본 대학교의 보안정책 및 업무수행에 필요한 보안준수 사항 등을 교육하도록 한다.

제3절 외부자 정보보호

제28조 (외부자 보안관리 역할 및 책임) ① 계약업무담당자는 외부업체와 계약 시 계약서에 정보보호 요구사항을 명시하여 계약 당사자 간에 합의하여야 한다.

② 업무주관부서는 정보보호 준수 사항 및 사고 시 보고 절차 등을 명확히 외부자에게 공지하여야 하며, 필요 시 외부자에 대해서 정보보호 요구사항의 이행여부를 감사할 수 있다.

③ 정보보호 담당부서는 계약업무담당자 및 업무주관부서에서 요청 시 외부자가 정보보호 요구사항을 이행하고 있는지 검토하여야 한다.

제29조 (외부용역 추진 시 검토사항) 중요 정보시스템의 개발 및 운영업무를 외부용역으로 대체하는 경우, 업무주관부서는 다음 사항을 충분히 검토하여야 한다.

1. 정보시스템 서비스 외부용역에 따른 정보 관리의 취약점을 최소화하고 정보보호를 위하여 내부 통제방안을 수립 및 운영하여야 한다.
2. 재난상황에서도 최소한의 업무기능 유지를 위해 백업자료를 보존하고, 백업설비를 확보하는 방안을 강구해야 한다.
3. 외부자가 제공하는 서비스의 품질수준을 주기적으로 평가할 수 있다.

제30조 (계약 시 정보보호 요구사항) ① 외부자의 계약서에는 정보보호를 위한 다음과 같은 요구조건을 포함하거나 관련사항이 언급된 문서가 명시되어야 하며, 계약은 정보시스템 접근 허가 전에 공식 체결되어야 한다.

1. 법적 요구사항의 충족 여부
2. 모든 계약 당사자들에게 정보보안 책임을 주지시키는 절차
3. 정보자산의 무결성 및 비밀성 유지
4. 전산매체에 저장된 데이터의 보호 및 소유권
5. 중요 정보 사용권한이 없는 자의 접근제한에 관한 사항
6. 재해 발생 시 서비스의 가용성 유지 방법
7. 외부자 장비에 대한 물리적 보안 허용 수준
8. 자료 제출 및 감사 권한
9. 서비스수준협약(SLA)의 정의
10. 본 대학교와 외부자의 위험 및 의무 등

② 외부자는 원칙적으로 재 위탁을 금한다. 단, 부득이하게 재 위탁이 필요할 경우는 대학의 허가를 반드시 득하고 관리감독을 받아야한다.

③ 본 대학교는 업무와 관련된 사항에 대하여 외부자를 감사할 수 있는 권한을 가지며, 이를 계약서에 명시할 수 있다.

제31조 (비밀유지 서약) ① 외부자가 법인일 경우는 대표가 서명한 업무 전반에 비밀 보

장을 서약하는 정보보안 서약서 [별지 제1호 서식]를 작성하여야 한다.

② 외부자가 법인일 경우 대표의 정보보안 서약서 이외에 업무를 수행할 인원 개개인에 대해서도 비밀보장을 위해 정보보안 서약서를 작성하여야 한다.

제32조 (외부자의 의무) ① 외부자는 내부직원과 동일한 정보보안 책임과 의무를 가진다.

② 업무주관부서는 외부자에게 정보보호 준수 사항 및 사고 시 보고 절차 등을 명확히 공지하고, 외부자는 이를 숙지하여야 한다.

③ 외부자는 다음의 책무를 다 하여야 한다.

1. 계약서에 기술한 정보보안 요구사항을 포함하여 계약사항에 대해 성실히 이행하여야 한다.
2. 업무의 수행 중 발생하는 추가적인 정보보안 요구사항에 대하여 협의 및 합의하고 이를 준수하여야 한다.

④ 외부자가 법인일 경우는 외부용역인력에 대한 정보보안 교육을 정기적으로 실시하여야 한다.

제33조 (외부자 사용자 관리) ① 본 대학교의 시스템에 접근할 경우, 별도 사용자 계정을 발급받아야 한다.

② 운영 중인 정보시스템에 대한 작업을 승인한 경우 이용시간과 작업지역을 제한하여 접근통제를 실시할 수 있다.

③ 업무담당 부서는 외부자에게 제공하는 각종 통제 방법 등을 평가하고, 필요 시 추가적인 통제방안을 요구하여야 한다.

제34조 (외부자 접근통제) ① 외부자는 직무에 필요한 정보만 접근할 수 있도록 하여야 한다.

② 시스템의 계정에 적절한 접근권한을 설정하여 필요 이상의 접근이 가능하지 않도록 소프트웨어적 통제를 실시한다.

③ 외부자가 사용하는 통신망은 전산망과 분리하여 주요시스템의 접근이 제한되도록 한다. 단, 업무상 부득이한 경우 예외로 하며 담당자 입회하에 작업하는 것을 원칙으로 한다.

제35조 (외부자 업무 완료 시) ① 외부자는 보유 중인 본 대학교 소유의 모든 정보자산을 반환해야 하며, 특별한 허가를 받지 않는 한, 개인PC/노트북/저장장치 등에 포함된 본 대학교의 지적재산과 관련된 모든 정보는 삭제한다.

② 본 대학교로부터 부여받은 물리적, 논리적 권한의 삭제 요청과 정보자산에 대한 반납에 대해 외부자는 외부용역 업무완료 보안 점검표 [별지 제2호 서식]를 작성하여 업무주관부서의 확인을 받아야 한다.

③ 업무주관부서로부터 특별한 허가를 받지 않는 한, 본 대학교에서 취득한 어떤 정보자산도 외부자가 보유해서는 아니 된다.

제36조 (위배사항의 처리) 계약상의 정보보호 요구사항과 관련하여 외부자의 위배사항이 발생할 경우 제도적, 법적 대응책을 강구해야 한다.

1. 경미한 위배사항일 경우, 외부자와의 협의를 통해 피해를 구제한다.
2. 중요한 위배사항일 경우, 계약서 및 관련 법률에 따라 피해보상을 강구해

야 한다.

제37조 (외부자 장비 반입/반출) 외부자 소유 정보자산의 반입/반출시는 본 규정 제19조에 명시된 점검을 하여야 한다.

제4절 응용프로그램 개발 보안

제38조 (정보보호 요건 분석 및 적용) 응용프로그램 개발부서는 본 대학교의 정보보호정책이나 정보 소유자의 정보보호 요건을 분석하여 응용프로그램 설계 단계에서부터 테스트 후 운용될 때까지 응용프로그램 개발자에 의해 일관성 있게 적용될 수 있도록 관리 한다.

제39조 (필수 사용자 보안 요건 정의) 업무와 관련한 사용자 보안 요건 정의 시 다음의 정보보호 요건은 반드시 함께 정의하도록 한다.

1. 사용자 인증 방법
2. 암호화 및 접근 권한 통제 방법
3. 로깅 방법
4. 응용프로그램 개발 및 운영 시 정보보호 통제 방법
5. 기타 정보보호 관련 사항

제40조 (개발 환경 보안) ① 개발 및 테스트 시스템과 운영시스템은 분리하는 것을 원칙으로 한다. 단, 개발 환경이 운영환경에 영향을 주지 않도록 대책이 수립되었을 경우에는 예외로 한다.

② 개발시스템은 실 운영 시스템의 보안성을 유지하여야 한다.

제41조 (데이터 보안) ① 응용프로그램의 개발 및 테스트 시 운영 데이터의 노출을 방지하기 위해 임의의 테스트 데이터를 생성하여 활용하거나 운영 데이터를 변경하여 사용하는 것을 원칙으로 한다.

② 운영 데이터의 사용이 불가피할 경우 해당 개발 업무 부서장의 통제 하에 실시한다.

제42조 (개발 프로그램 보안) ① 응용프로그램 및 라이브러리의 침해를 예방하기 위해 개발 중인 응용프로그램 및 라이브러리/소스코드는 운영시스템에 저장하지 않도록 한다.

② 응용프로그램 개발 시 정보보호 요구사항을 우회하거나 응용프로그램 자체 기능에 위협을 줄 수 있는 악성코드의 삽입은 금지한다.

③ 필요한 경우, 응용프로그램의 변경 이력 및 버전 관리 등을 위해 형상관리 도구를 사용하여 소스코드를 관리할 수 있다.

제43조 (사용자 인증) ① 본 대학교에서 개발되는 모든 응용프로그램은 사용자의 권한을 확인한 후 작동되도록 한다.

② 응용프로그램에 대한 인증 수단은 응용프로그램에서 다루어지는 정보의 중요도, 인증에 대한 위협 등을 고려하여 정보보호담당부서, 응용프로그램 개발부서, 개발을 의뢰한 현업 부서 등 관련 조직과의 협의 하에 최적의 인증 수단

을 선택하도록 한다.

제44조 (사용자 계정) ① 사용자 계정은 사용자 신상(주민등록번호 등)과 관련된 정보가 포함되지 않도록 하며, 부득이하게 포함되어야 하는 경우 주요 정보에 대해서는 숨김이나 보이지 않는 형식으로 표현해야 한다.

단, 업무 편의상 교직원 번호/학생번호 등은 예외 적용할 수 있다.

② 사용자 계정명은 응용프로그램에서 유일성을 가져야 한다.

③ 응용프로그램 개발자는 응용프로그램의 소스 내에 사용자 계정이 포함되지 않도록 해야 한다.

제45조 (비밀번호) ① 응용프로그램의 인증 시스템은 비밀번호의 최소 길이(최소 8자리 이상, 영문자/숫자 혼용)를 통제할 수 있도록 한다.

② 응용프로그램의 인증시스템은 비밀번호를 사용할 수 있는 최대기간(최대 6개월)을 설정할 수 있도록 한다.

③ 비밀번호는 입력 시 타인이 추측할 수 없도록 화면상에 표시하지 않거나 인식 불가능한 문자로 표시하여 나타내도록 한다.

④ 비밀번호는 평문으로 저장되어서는 안 되며, 반드시 암호화된 형태로 저장되어야 한다.

⑤ 응용프로그램 개발자는 응용프로그램의 소스 내에 비밀번호가 포함되지 않도록 해야 한다.

⑥ 응용프로그램 사용자가 비밀번호를 잘못 입력하는 횟수에 대한 제한 설정 기능을 구현하여 설정된 횟수에 도달하는 경우, 일시적으로 사용을 중지시키거나 세션을 종료시키도록 한다. 이러한 경우 해당 응용프로그램의 인증시스템은 다음과 같은 기능을 수행할 수 있도록 설계한다. 단, 수강신청 시스템은 예외로 한다.

1. 응용프로그램 관리자에 의해 비밀번호가 재설정될 때까지 해당 계정 사용 중지
2. 잘못된 비밀번호 5회 이상 입력 시 최소 30분 이상 사용자 계정을 일시 중지 또는 담당자 확인 전까지 사용 중지한다.

제46조 (로그인) ① 로그인 화면에서는 단지 로그인 관련 정보만 표시될 수 있도록 한다. 기타 정보는 로그인 과정을 성공적으로 마친 후 표시될 수 있도록 한다.

② 응용프로그램 사용자의 로그인 실패 시 로그인 실패 이유를 표시하지 말고, 단순히 로그인 절차가 잘못되었다는 정보만 표시하고 세션을 종료 시키거나 정확한 로그인 정보가 입력되기를 기다리도록 한다.

단, 로그인 실패 이유를 상세하게 표시할 필요성이 인정되는 경우는 예외로 할 수 있다.

제47조 (암호화) ① 응용프로그램 설계 및 개발 시 암호화 기법을 사용할 필요가 있는 경우에는 정보보호조직으로부터 승인을 받은 암호화 기법을 사용하도록 한다.

② 정보의 유형과 기밀성에 따라 정보를 더욱 안전하게 관리할 필요성이 있을 경우에는 정보를 암호화하여 보관하도록 설계한다.

③ 응용프로그램에서 학사 관련 정보 등 노출 시 사용자에게 피해를 줄 수 있는 중요 정보가 전산망을 통해 전송될 때에는 암호화 대상을 정의한 후, 반드시 암호화된 상태로 전송되도록 한다.

제48조 (접근 권한) ① 응용프로그램의 설계 및 개발 시 업무 성격상 또는 업무 흐름상으로 적절하도록 화면 및 메뉴별로 접근 권한을 통제한다.

② 응용프로그램의 사용자를 사용자별, 직책별, 부서별, 인가된 등급 등으로 구분하여 접근 권한을 관리할 수 있도록 한다.

③ 필요한 경우 날짜, 시간, IP 주소 별로 사용자의 접근을 통제할 수 있도록 기능을 구현한다.

④ 응용프로그램을 운영 단계로 이관하기 전 응용프로그램 개발자는 공식화된 접근 권한을 제외한 모든 접근 권한을 제거한 후 운영단계로 이관하도록 한다.

제49조 (로그의 기록) 본 대학교의 개인정보를 취급하는 응용프로그램은 중요 정보의 입력, 수정, 삭제와 관련한 사용자의 활동에 대하여 로그를 기록하도록 설계한다.

제50조 (보안성 평가) ① 보안성 평가는 운영 단계로 이관하기 전에 개발담당부서의 요청으로 정보보호담당부서가 응용프로그램 개발 시 요구된 보안요구사항을 기반으로 실시하는 것을 원칙으로 한다. 단, 응용프로그램의 양이 방대하거나 기타의 필요성이 인정되는 경우 외부전문가의 도움(전문 감리 등)을 얻어 보안성 평가를 실시 할 수 있다.

② 보안성 평가가 완료되면 정보보호담당부서는 평가결과를 검토하여 해당 응용프로그램의 정보보호 기능의 적절성 여부를 판단하고, 개선의 필요성이 요구되는 부분을 제시하고 개선활동 결과를 재평가 하여야 한다.

③ 보안성 평가와 관련된 사항은 모두 문서화하여 관리하도록 한다.

제51조 (운영 및 변경관리) ① 응용프로그램 소스프로그램은 실 운영서버에 저장하지 말아야 하며, 해당 응용프로그램 운영자가 소스에 대한 모든 통제를 우선 담당한다.

② 응용프로그램에 대한 보안상 중대한 변경이 필요한 경우 정보보호담당부서에 의뢰하여 발생 가능한 위험과 취약성에 대한 분석을 실시해야 한다.

③ 개발자는 위험과 취약성 분석에 따른 결과 값에 따라 변경작업을 수행하도록 한다.

제52조 (개발 및 변경 내역의 문서화) 응용프로그램 개발 및 변경에 관련된 사용자의 요건 분석, 응용프로그램 설계 및 개발 사항, 정보보호 요건 정의 및 구현 등에 대한 사항들은 문서화하여 관리하여야 한다.

제53조 (기존시스템의 보안적용) ① 기존 시스템의 경우 본 규정의 보안요구사항에 해당하는 유지보수 사항이 발생할 경우에는 본 규정의 기준이 반영되는 것을 원칙으로 한다.

② 본 규정의 보안요구 사항을 기존 시스템에 적용하기 어려운 경우, 해당 유지보수 책임자는 개발담당자와의 협의를 거쳐 미적용 사유 및 대안방안을 세우

고, 정보보호조직의 검토와 승인을 통해 유지보수를 진행하도록 한다.

제5절 물리적 보안

제54조 (제한구역의 설정) 정보자산 보안을 위한 제한구역의 설정은 정보보호책임자가 지정한다.

제55조 (제한구역 구분) ① 제한구역에는 그 출입문에 다음 예시와 같은 표시를 한다. 다만, 중요시설에 대해 외부에 노출 위험이 있을 경우 그 표지를 생략할 수 있다. [제한구역 표지]

② 제한구역에는 적당한 곳에 다음 예시와 같은 관리책임자의 표지를 부착하여야 한다. [관리책임자 표지]

제56조 (출입 통제) ① 제한구역에는 비인가 된 접근이나 손상을 방지하기 위하여 별도의 출입통제 장치를 설치하여야 하며, 필요 시 감시시스템 등을 설치하여 운영한다.

② 제한구역 출입은 정보보호책임자의 인가를 득한 자에 한 한다.

③ 제한구역에 대해 허가된 자 외의 교직원 및 외부인이 출입하는 경우에는 인가된 직원이 동행하여야 한다.

④ 제한구역에 출입하는 비인가자는 출입자관리대장 [별지 제3호 서식]에 기입한다. 단, 출입통제 시스템 운영 시는 생략 가능하다.

제57조 (정보자산 보유 시설 기준) ① 방수, 방화, 방진 및 외부 침입 방지 등 설비 요건에 맞도록 시설을 구비한다.

② 지진지대, 침수지대, 위험물(폭발물, 가스, 유류 등) 보관 장소 등 재난발생우려 지역이 아닌 곳에 구축한다.

③ 출입사항에 대하여 사후 확인이 가능하도록 기록하여야 하며, 필요한 경우, 무인 감시카메라 또는 출입통제시스템을 설치한다.

④ 재난에 대비하여 열감지기, 연기감지기, 누수감지기 등의 방화시설, 하론가스 등 소화설비, 기타 방재설비를 보유하며, 소방점검 시 작동상태를 점검하여 항시 사용할 수 있는 상태로 유지한다.

⑤ 일정한 온도 및 습도가 유지되어야 하는 장비 설치장소에는 항온항습장비를 설치·운영한다.

⑥ 정전 등 비상시에 대비하여 전산실은 타 사무실용과 분리하여 전원배선을 하여야 하며, 최소 30분간 유지할 수 있는 무정전장비를 설치하고, 대학의 비상발전설비에 연결하여 전력 공급 중단 사태를 예방한다.

⑦ 화재 시 사람이 대피할 수 있도록 경고, 비상벨 등이 먼저 울리고 일정시간 이후에 자동소화 설비가 작동되도록 설정한다.

⑧ 비상사태 발생 시 빠른 복구를 위해 비상 연락망을 비치한다.

제58조 (사무실 보안 기본 원칙) ① 책상 위에 중요 정보 및 저장매체를 방치하지 않는

다.

② 개인 사물함은 잠금 장치를 설치하고, 퇴근 시 항상 잠금을 확인한다.

③ 중요정보가 담긴 저장매체, 출력된 문서 또는 PC 등은 비인가자의 접근으로부터 보호되어야 한다.

④ 당장 필요하지 않은 중요정보가 담긴 인쇄물, 저장매체, 휴대용 전산장비는 시건 장치가 설치된 캐비닛 또는 서류함에 보관한다.

⑤ 중요정보가 담긴 출력 문서는 타인이 가져가게 하거나 프린터 주위에 방치되지 않도록 한다.

⑥ 신원이 파악되지 않은 자에 의해 내부직원의 신상정보, 조직정보, 시스템 정보 등을 묻는 전화를 받았을 경우, 반드시 상대의 신원을 확인하여야 하며, 신원이 불분명한 상대와 통화를 하는 경우는 정보가 유출되지 않도록 한다.

⑦ 팩스로 전송된 원본 문서는 즉시 회수하도록 한다.

⑧ 복사기 사용 후 원본 및 복사본이 복사기에 남겨져 있지 않도록 반드시 회수한다.

제6절 보안시스템 보안

제59조 (보안시스템 일반 원칙) ① 공개 서버로의 접속은 침입차단시스템을 통하도록 한다.

② 공개서버는 인터넷을 통해 외부에서 내부 망으로의 접속 시 신뢰할 수 있는 호스트 및 통신망으로 제한하며, 서비스를 제공하지 않는 포트와 프로토콜은 차단한다.

제60조 (보안시스템 운영 및 관리) ① 보안시스템을 운영하는 부서는 보안시스템 담당자를 선임하여야 한다.

② 보안시스템 설정(Rule)에 의해 허가된 서비스에 대해서만 연결을 허용하며 구성 상황의 변동을 지속적으로 관리한다.

③ 보안시스템의 접근은 규정된 콘솔 또는 경로를 통해서만 접속하여야 한다.

④ 시스템 자체에서 제공하는 모든 불필요한 서비스 및 포트는 관리 상 필요한 경우 외에는 모두 중지 및 차단하며, 보안시스템 외의 어떠한 프로그램이나 소프트웨어의 설치를 금한다.

⑤ 보안시스템 담당자는 보안시스템의 설정(Rule)에 대한 유효성 검증을 위해 매 6개월마다 해당 설정(Rule)에 대한 실제 사용유무/보안상 취약점 등에 대한 분석을 수행한다.

제61조 (인증) ① 보안시스템에는 관리자 계정 이외의 모든 계정을 삭제한다.
단, 가상사설망(VPN) 사용자 계정에 대해서는 예외 적용한다.

② 보안시스템의 관리자 계정 및 비밀번호는 보안시스템 담당자 외에 유출되어서는 안 된다.

③ 보안시스템의 관리자 비밀번호는 6개월 마다 변경하여야 하며, 영문자/숫자가 혼용된 최소 8자리 이상으로 설정한다.

제62조 (접근통제 정책) ① 외부로부터의 불법적인 트래픽 유입을 차단하고, 명백히 허가되고 인증된 트래픽만을 허용하는 설정(Rule)이 설정되고 적절히 적용되어야 한다.

② 외부와의 모든 통신은 침입차단시스템을 경유하도록 설정 및 운영되어야 한다.

③ 업무상 필요한 경로를 단계적으로 허용하는 방법으로 접근통제 정책을 구현하여야 한다.

④ 웹 서버와 같이 공개용 서버들이 존재하는 경우에는 외부망과 전산망의 중간 영역(DMZ)에 설치되어야 하고 불필요한 서비스 포트를 차단 설정한다.

⑤ 업무 목적 상 외부에서 본 대학교 내부망에 위치한 업무용 서버에 원격 접속하고자 할 경우(Telnet, Windows Terminal Service 등)는 VPN을 통한 암호화 통신 채널 형성 및 사용자 인증을 반드시 수행한다.

제63조 (로그 관리 및 분석) ① 공개용 시스템에 접속하는 모든 시도는 로그를 남기도록 설정한다. 단, 내부용량의 한계 및 불필요하다고 판단되는 로그에 대해서는 정보보호담당부서의 검토를 걸쳐 제한적으로 선택할 수 있다.

② 로그는 최소 3개월 보관하며, 필요 시 별도 백업 미디어에 보관할 수 있다.

③ 로그 파일들은 별도의 로그서버를 지정하여 통합 저장하여 운영할 수 있으며, 로그에 대한 매월 정기적인 백업을 실시하여 로그 변조행위에 대응한다.

④ 보안시스템 담당자는 로그 및 보안 설정(Rule)을 점검하고, 이상 징후 발생 및 분석 결과 특이 사항을 발견한 경우 정보보호담당부서에 알린다.

제64조 (설정(Rule) 등록 및 변경 절차) ① 보안시스템 담당자는 보안시스템 정책 등록 및 변경 요청 신청서 [별지 제4호 서식]를 작성하여 정보보호담당부서에 승인을 요청한다.

② 정보보호담당부서는 보안시스템 정책 등록 및 변경 요청 신청서를 검토 후 요청 사항의 적정성 평가 후 적용을 허용한다.

③ 보안시스템 담당자는 보안시스템 정책 등록 및 변경 요청 신청서 상에 지정된 기한이 경과하면 해당 설정(Rule)을 삭제하여야 한다.

제65조 (백업주기 설정) 보안시스템의 장애나 불량, 침입에 의한 설정 소실 등으로부터 보호하기 위하여 해당 보안시스템의 설정(Rule)을 포함한 주요 설정사항을 매월 백업하여야 하며, 백업된 정보를 3개월 이상 기간 동안 보관한다.

제7절 전산망 보안

제66조 (전산망 관리 및 운영) 전산망 관리 및 운영에 대한 사항은 대학 “안전관리지침-정보화자원 관리에 관한 지침”에 따른다.

제67조 (전산망 운영보안) ① 전산망 담당자는 장비 공급업체의 보안관련 패치나 권고안이 발생되는 것을 지속적으로 모니터링하며 사안에 따라 긴급한 대응이 필요한 경우 패치를 적용한다.

② 전산망담당자는 보안관련 패치를 적용하기 전에 중요정보(접근통제리스트를

포함한 설정 사항 등)에 대한 백업을 수행 후 패치를 적용한다.

③ 정보보호관리자의 허가 없이 본 대학교 전산망의 구성도, 주소, 구성환경, 관련 시스템 정보 등을 무단으로 유출하여서는 안 된다.

④ 전산망 구성도, 현황 자료, 전산망 주소할당자료 및 전산망 관련 모든 자료는 인가된 자만이 접근 가능하도록 제한한다.

⑤ 전산망 관련 자료를 폐기하는 경우 폐지는 반드시 파쇄 해야 하며 이면지로 활용할 수 없다.

⑥ 라우팅 테이블이 존재할 경우 주기적(매 6개월)으로 점검하며 비인가 된 라우팅 정보 또는 불필요한 라우팅 정보는 삭제한다.

⑦ 전산망담당자는 장애의 원인이 보안관련 사안이라고 판단하는 경우 즉시 해당사항을 관련 로그와 함께 정보보호담당자에게 전달하고 그 대책을 협의해야 한다.

제68조 (전산망 장비 접근 통제 및 사용자 인증) ① 중요 전산망 장비에 접속을 위한 비밀번호의 인증은 SSH(Secure Shell)을 사용하여 스니핑(Sniffing)의 위험으로부터 보호할 수 있도록 암호화된 통신 채널을 사용한다.

② 로그인 화면에서는 로그인 관련 정보만 표시하고, 불법적인 접근을 경고하는 보안 배너를 삽입해야 한다.

③ 전산망 장비에 하나의 사용자 계정으로 여러 터미널에서 동시에 여러 세션을 열어 접속하는 것을 원칙적으로 통제 한다.

④ 전산망 장비에 접속하기 위한 사용자 계정은 6개월 주기로 비밀번호를 변경하며, 영문/숫자를 혼용한 6자리 이상으로 설정한다.

제69조 (취약성 점검) ① 정보보호담당부서에서는 전산망 취약점 점검을 년 2회 실시 하여야 하며, 필요 시 추가적으로 진단할 수 있다

② 전산망담당자가 전산망 장비의 보안 취약성 또는 결함을 발견하는 경우 정보보호담당자에게 즉시 알려야 한다.

제70조 (접근가능 호스트의 제한) ① 전산망 장비를 관리하기 위한 접근은 본 대학교 내의 접근 가능한 특정 호스트 및 IP를 정의하고 이를 통해서만 로그인 가능하도록 설정한다.

② 전산망 장비 접근에 필요한 권한의 요청 및 변경, 삭제는 공식적인 문서를 통해 이루어져야 하고, 처리 결과는 향후 감사나 문제 발생 시의 자료로 사용할 수 있도록 보관해야 한다.

③ 전산망담당자는 전산망 장비의 정상적인 운영을 방해하거나, 다른 사용자의 사용을 저해하는 행위를 발견 했을 때, 정보보호담당자에게 즉시 알리고, 해당 사용자 IP 및 호스트의 접근 권한 및 전산망 사용을 제한 또는 취소할 수 있다.

④ 전산망 장비 접속 후 10분 이상 키보드 입력이 없을 경우 자동으로 해당 연결이 차단되도록 설정한다.

단, 장비 모니터 등의 운영 목적상 필요한 경우 예외 적용할 수 있다.

제71조 (구성설정 값의 일관성 유지) 본 대학교 모든 전산망 장비 자산의 구성 설정 값을 일관성 있게 유지하여 보안 수준이 동일하게 적용될 수 있도록 한다. 다만, 특정 세그먼트의 보안을 강화할 필요가 있는 경우 동 세그먼트에 대해서는 설정 값을 다르게 유지할 수 있다.

제72조 (접근제어 리스트 적용) ① 중요 전산망 장비의 경우 IP, 프로토콜 및 서비스 포트에 대해 접근제어리스트를 관리한다.

② 전산망담당자는 전산망 장비에 적용된 접근통제리스트를 매 6개월마다 검토하고 재평가 한다.

제73조 (백업주기 설정) 전산망담당자는 전산망 장비의 이상동작 및 장애, 그리고 침해사고에 의한 설정 정보 및 관련 정보를 보호하기 위하여, 매 6개월 백업 주기를 설정하여 주요 구성 설정상태를 백업저장 관리하여야 하며 최소 6개월 이상 보관한다.

제74조 (주기적인 모니터링) 전산망담당자는 전산망 장비의 사용 현황 및 이상 유무를 주기적으로 확인하며, 중요 보안 이상 상황 발생 시 신속히 조치한 후 정보보호담당자에게 통보한다.

제75조 (로그 관리) ① 전산망담당자는 정보보호 사고 발생 시 추적성을 확보하기 위해 사용자 로그인 및 사용자의 명령어 사용에 대해 중요 캠퍼스 통신망 장비 로그를 최소 3개월 이상 기록하도록 설정하고 저장 관리한다. 이를 위하여 별도 로그서버를 구축할 수 있다.

② 전산망담당자가 로그대상을 변경하는 경우에는 정보보호담당부서의 의견을 수렴하여 보안에 미치는 영향을 검토한 후에 행한다.

③ 전산망담당자는 승인이 없는 사용자의 접근정보를 반드시 로그에 저장하여 관리 분석한다.

④ 전산망담당자는 전산망 장비의 접속 내역을 기록한 로그에 대해 공식적인 요청이나 법률에 의한 협조 요청에 의하지 않고는 타인에게 공개할 수 없다.

제8절 서버 보안

제76조 (서버 보안 일반 원칙) ① 외부에서 공개서버로의 접속은 침입차단시스템을 통과하도록 한다.

② 외부에서 내부 망으로의 접속은 신뢰할 수 있는 호스트 및 통신망으로 제한하며, 서비스를 제공하지 않는 포트와 프로토콜은 차단한다.

③ 공개서버 자체 또는 별도 보안제품 등을 이용하여 인터넷을 통한 바이러스, 웜, 트로이 목마 등의 유통을 방지하는 기능을 갖추어야 한다.

제77조 (서버 운영) ① 정보보호담당부서는 서버의 하드웨어 및 소프트웨어의 지속적인 가용성과 무결성 확보를 위해 년 2회 이상 취약점 점검을 실시한다.

② 서버 담당자는 서버 공급업체의 보안관련 패치나 권고안이 발생되는 것을 지속적으로 모니터링하여 보안패치를 적용하여야 한다.

③ 서버 담당자는 보안관련 패치를 적용하기 전에 중요정보에 대한 백업을 수행한다.

④ 서버 담당자는 기존 운영체제의 정보보호 취약점이 보완되고, 향상된 정보보호 기능이 포함되어 있는 새로운 버전의 운영체제가 출시되어 업그레이드의 필요성이 있을 경우 해당 운영체제에 대한 보안성을 검토 한 후에 업그레이드를 실시한다.

⑤ 서버에는 업무용 목적으로 사용되는 프로그램 이외의 프로그램 설치를 제한한다.

⑥ 본 대학교의 정보시스템을 침해할 수 있는 Backdoor, Trojan등의 소프트웨어를 테스트 목적으로도 설치를 제한한다.

⑦ 원격터미널(Remote Terminal)과 같은 원격접속 소프트웨어 설치를 원칙적으로 금한다. 단, 업무적으로 필요한 경우 정보보호 담당부서의 승인을 득하여야 한다.

제78조 (사용자 ID관리) ① 시스템 OS에 대한 사용자 ID의 등록, 변경, 삭제 요청은 사용자계정신청서 [별지 제5호 서식]를 통하여 이루어져야 한다.

② 유지보수, 장애처리 등의 목적으로 제3자에게 ID를 부여할 필요성이 있을 경우 서버 담당자는 해당 ID에 대한 생성 및 관리를 수행하며 작업종료 시 삭제한다.

③ 사용자 ID는 개인정보를 포함하고 있지 않도록 한다.

④ 공용 ID는 사용하지 않는 것을 원칙으로 한다. 단 업무 특성 상 사용해야 하는 경우, 해당 부서장의 승인을 득한 후에 사용한다.

⑤ 서버 설치 시 기본적으로 포함되어 있는 제품 공급 ID 중 업무적으로 불필요한 ID는 삭제 또는 변경한다. 단 삭제가 불가하거나, 서비스 및 업무에 영향을 미치지 않는다고 판단하는 경우에는 제외한다.

⑥ 서버담당자는 해당 시스템별로 사용자계정에 대한 시스템 계정 관리 대장 [별지 제6호 서식]을 작성한다.

제79조 (비밀번호 관리) ① 사용자는 비밀번호 생성 시 다음과 같은 추측 가능한 비밀번호를 사용하지 않도록 한다.

1. 사용자 ID와 동일한 비밀번호
2. 생년월일, 전화번호, 이름 및 추측 가능한 비밀번호
3. 주기성 문자 및 키보드상의 연속된 배열로 구성된 비밀번호 등

② 사용자는 비밀번호의 길이를 최소 8자 이상으로 사용하여야 하며, 매 6개월마다 변경하여야 한다.

단, 데이터베이스관리시스템(DBMS) 및 어플리케이션 등에서 사용되는 비밀번호의 경우 예외 적용할 수 있다.

③ 비밀번호 입력 시 타인이 추측할 수 없도록 화면상에 표시하지 않거나 인식불가능한 문자로 Marking 하여 표시하도록 설정한다.

④ 서버 설치 또는 소프트웨어 설치 시 기본적으로 제공되는 비밀번호는 설치

후 즉시 변경하여야 한다.

⑤ 사용자 ID 발급 후 부여된 초기 비밀번호는 사용자가 처음 접속 시에 자신의 비밀번호로 변경을 해야 하며, 서버 담당자는 그러한 기능이 서버에서 강제화 되도록 구성한다.

단, DBMS 및 어플리케이션 등에서 사용되는 비밀번호의 경우 예외 적용할 수 있다.

⑥ 서버 담당자는 서버에 저장된 비밀번호 파일에 대해 서버 담당자의 관리 목적으로 접근하는 경우를 제외하고는 어느 누구도 읽을 수 없도록 제한을 한다.

⑦ 사용자는 비밀번호가 타인에게 노출되었거나 노출이 의심될 경우 즉시 변경해야 한다. 서버 담당자는 해킹 및 침해사고로 인해 비밀번호가 노출되었다고 판단될 경우 정보보호부서에 통보하고 지시에 따라 처리하여야 한다.

⑧ 서버 담당자는 사용자 ID의 신규 등록 또는 비밀번호 변경으로 인해 사용자에게 비밀번호를 전달하는 경우 본인임을 확인하는 과정을 거쳐야 하며, 팩스나 전화상으로 비밀번호를 전달하지 않는다.

⑨ 사용자는 비밀번호를 메모 또는 문서의 형태로 남기지 않는다.

제80조 (로그인 프로세스) ① 사용자가 서버에 접속할 경우 사용자 ID와 비밀번호 또는 보다 강화된 인증 방법을 통한 후 접근해야 하며, 사용자 ID 및 비밀번호를 스니핑(Sniffing)으로부터 보호할 수 있도록 SSH(Secure Shell)와 같은 암호화된 통신 채널을 사용 한다.

② 로그인 화면에서는 로그인 관련 정보만 표시한다. 조직이나 운영체제, 전산망 환경, 내부적인 사항과 같은 정보는 제공하지 않는다.

③ 사용자가 시스템에 로그인 실패 시 시스템 침해의 원인이 될 만한 정보를 사용자에게 제공하지 않게 설정한다. 로그인이 실패하면 로그인 절차가 잘못되었다는 정보만 표시하고, 세션을 종료시킨다.

④ 서버에 접속한 후 사용자나 다른 시스템으로부터 10분 이상 키 입력이 발생하지 않으면 자동적으로 로그오프 시키거나 세션을 중단시키는 것을 원칙으로 한다.

단, 서버 모니터링 등 지속적인 연결이 필요할 경우 예외 적용할 수 있다.

⑤ 하나의 사용자 ID로 여러 장소(터미널)에서 동시에 여러 온라인 세션을 연결하지 않는 것을 원칙으로 한다.

⑥ 시스템관리자(root 등) 계정으로의 직접 원격 접속은 허용하지 않으며, 일반 사용자로 로그인 후 시스템관리자 계정으로 스위치 한다.

제81조 (권한관리 및 접근통제) ① 특정 수준의 정보에 대한 접근 권한을 부여 받은 사용자는 해당 수준 또는 그 이하의 정보에만 접근 가능하도록 해야 하며, 그 이상의 권한이 필요한 정보에 대해서는 접근을 제한한다.

② 유지보수, 장애처리 및 기타 업무적인 필요성에 의하여 제3자에게 접근 권한을 부여해야 할 경우, 부서장의 승인을 득한 후 사용되도록 관리한다.

③ 서버 담당자는 사용자가 서비스 중지 및 장애를 일으킬 수 있는 시스템 명령어를 사용할 수 없도록 권한을 제한한다.

④ 서버 담당자는 서버의 정상적인 운영을 방해하거나, 다른 사용자의 사용을 저해하는 행위가 발견되거나 의심이 될 때, 부서장의 승인 후 사용자의 권한을 제한 또는 취소한다.

⑤ 사용자는 서버 담당자 및 정보보호담당부서, 해당 부서장의 사전 승인이 없는 한 운영체제의 접근 통제 기능 또는 접근 통제 도구를 우회할 수 있는 프로그램을 이용한 접근은 차단한다.

⑥ 서버 담당자는 서버가 정상적으로 동작하지 않을 경우 정상적으로 동작될 때까지 사용자의 접근을 제한할 수 있다.

제82조 (파일시스템 및 네트워크 서비스 관리) ① 서버 담당자는 파일시스템을 구성할 때 시스템 데이터와 일반 데이터를 논리적 또는 물리적으로 나누어 설치되도록 한다.

② 서버 담당자는 비인가자의 불법적인 접근 및 서비스 중지 등을 예방하기 위해 업무적으로 불필요하거나, 침해의 위협이 있는 네트워크 서비스를 제공하지 않도록 한다.

제83조 (웹서버 구축) ① 웹서버 운영자는 새로운 웹서버 소프트웨어의 신규 업데이트 및 보안패치를 확인하여야 하며, 최신 버전의 보안패치를 유지하도록 하여야 한다.

② 웹서버는 계획된 서비스만을 제공하도록 구축 및 운영되어야 한다.

③ 데이터베이스 서버의 경우는 웹서버와 분리하여 서로 다른 시스템에서 운영하는 것을 원칙으로 한다.

④ 웹서버에서 사용되지 않는 모든 불필요한 소프트웨어는 반드시 제거한다.

⑤ 웹서버와 같은 외부 공개서버는 침입차단시스템을 경유하도록 설치, 운영한다.

⑥ 웹서버를 통하여 개인정보와 같은 민감한 데이터가 전달되는 경우, 암호화 전송을 적용하여야 한다.

제84조 (웹서버 운영) ① 웹서버 운영자는 웹서버 로그와 OS 로그를 수시로 점검하여 침입, 침입시도, 또는 보안 문제점을 발견하여야 한다.

② 웹서버 장애로 인하여 시스템의 복구가 필요한 경우를 위해서 설정파일에 대한 백업을 매월 정기적으로 실시한다. 단, 백업의 필요성이 없다고 판단되는 경우에는 제외한다.

③ 웹서버에서 불특정 다수에게 공개되는 정보를 게시하는 경우, 개인정보 등의 민감한 정보가 공개되지 않도록 하여야 한다.

제85조 (전자우편 보안) ① 전자우편 시스템은 업무적인 목적을 위하여 사용하는 것을 원칙으로 하며, 불법적인 용도나 불순한 목적으로 사용해서는 안 된다.

② 내부 사용자는 본 대학교의 대외비 정보를 전자우편을 통하여 외부 전자우편 시스템으로 송신하여서는 안 된다.

③ 내부 사용자는 본 대학교 및 제3자의 지적재산권을 침해하는 내용, 명예훼손,

사기, 바이러스 등 불법적인 행위에 대한 내용을 포함하는 전자우편을 사용해서는 안 된다.

④ 업무상 중요한 자료를 송수신 할 경우에는 내용의 중요성에 따라 암호를 설정하여 전송하여야 한다.

⑤ 시스템 자원의 낭비를 초래하는 스팸메일, 반복메일 등의 전송 및 배포를 금지한다.

제86조 (전자우편의 열람 및 정보제공) ① 전자우편 시스템은 운영담당자를 제외한 비인가자의 접근을 금지하며 특별한 업무 목적 이외에 그 누구도 전자우편의 내용을 열람해서는 안 된다.

② 개인의 전자우편은 법적 증거자료로 정부기관으로부터 제출을 요구 받을 경우 법률에서 정하는 기준과 절차에 따라 제출할 수 있다.

제87조 (전자우편 서버 및 데이터 보호) ① 전자우편의 수신 시 사전에 바이러스 감염여부를 체크해야 한다.

② 전자우편 시스템의 안정성을 확보하기 위하여 전자우편 시스템에 스팸메일 차단기능을 설치해야 한다. 또한 전자우편 시스템이 허가되지 않은 외부기관의 중계서버로 이용되지 않도록 시스템을 구성한다.

③ 전자우편 시스템은 전자우편 수신 시 발신지의 주소가 확인된 전자우편만 수신하도록 구성되어야 한다.

④ 전자우편 시스템의 안정성을 위하여 필요 시 계정의 크기와 송수신되는 전자우편의 최대크기를 제한할 수 있다.

제88조 (백업주기 설정) 서버 담당자는 서버의 장애나 저장매체의 불량으로부터 중요정보와 소프트웨어를 보호하기 위해 해당 서버 운영자와의 협의를 거친 후 최소 월 1회 이상 백업을 실시하고, 저장된 백업 정보를 3개월 이상 보관한다.

제89조 (모니터링 및 로그관리) ① 서버 담당자는 서버의 사용 현황 및 이상 유무를 매월 정기적으로 모니터링 해야 하며, 다음과 같은 사항에 대하여 이상 상황 발생 시 부서장에게 알리고, 신속히 조치한다.

1. 새로운 계정 및 프로그램
2. 파일 또는 디렉터리 신규생성 및 삭제 여부
3. 서버 사용량 부하
4. 파일시스템 용량 초과
5. 프로세스 Looping
6. 비인가자의 접근 등

② 서버 담당자는 정보보호 사고 발생 시 추적성을 확보하기 위해 사용자 로그인 및 사용자의 명령어 사용에 대해 로그를 기록하도록 설정한다.

③ 서버 담당자는 로그의 정확한 기록을 위해 전산망에 연결된 본 대학교의 모든 서버의 내부 시간을 일치시키도록 한다.

④ 서버 담당자는 서버의 성능 및 디스크 용량 등을 고려하여 로그를 남길 대상을 선정한다.

⑤ 중요 서버의 로그 파일들은 별도의 로그서버를 지정하여 통합 저장하여 운영할 수 있으며, 로그에 대한 정기적인 백업을 실시하여 로그 변조 행위에 대응한다.

⑥ 서버 담당자는 서버 접속 내역을 기록한 로그에 대해 공식적인 요청이나 법률에 의한 협조 요청에 의하지 않고는 타인에게 공개하지 않는다.

⑦ 서버 담당자는 침해 사고가 의심되는 사건이 발생했을 때 경고 및 적발이 가능하도록 사용자의 로그 기록을 별도로 보관 관리 할 수 있으며, 그 내역을 정보보호 담당부서에게 알려야 한다.

제9절 데이터베이스 보안

제90조 (DB 인증정책) ① 데이터베이스관리자(DBA)는 계정 및 비밀번호 관리에 대한 책임과 권한을 갖는다.

② DB의 접근 제한을 위해서는 롤(role) 등을 통해 사용자를 관리하여야 한다.

제91조 (계정의 생성 및 폐기) ① DB를 사용하고자 하는 자는 DBA에게 사용자(업무) 정보 및 사용목적, 사용기간, 연락처 등이 포함된 DB사용자 계정 및 권한 신청서 [별지 제7호 서식]를 제출하고, DBA는 타당성 검토를 한 후 부서장의 승인을 득하여 처리한다.

② DBA는 DB사용자를 생성한 후 DB 사용자 관리대장 [별지 제8호 서식]에 반영한다.

③ DBA는 파견자, 휴직자, 퇴직자, 전출자 등 업무에 관계없는 DB 사용자를 삭제하며, DB 사용자 관리대장을 갱신한다.

④ 디폴트 계정은 설치 후 업무에 사용되지 않는다면 삭제하도록 한다.

제92조 (계정 운영) ① 계정 정보에 관한 사용자 관리대장은 모든 사용자에 대해 작성되어야 한다.

② 비밀번호가 없는 계정은 사용을 금한다.

③ DBA 권한을 가지고 있던 사용자가 이/퇴직 등의 사유로 다른 곳으로 옮길 때에는 인수자는 DBA 계정 비밀번호를 신속히 변경한다.

제93조 (비밀번호) ① 신규 사용자가 DB 사용에 대한 권한을 부여 받을 때 반드시 비밀번호를 받도록 한다.

② 사용자 비밀번호는 매 6개월마다 주기적으로 변경한다.

③ 모든 사용자는 비밀번호 인증을 통해서만 DB에 접근할 수 있도록 한다.

④ 모든 사용자 비밀번호는 최소 8자리 이상, 영문자/숫자 혼용으로 부여한다.

⑤ 계정이름과 동일한 비밀번호를 사용하거나 DB서버의 이름을 비밀번호로 사용하는 등의 추측하기 쉬운 비밀번호는 절대 사용하지 않는다.

⑥ DB의 디폴트 비밀번호는 추측하기 어려운 복잡한 비밀번호로 변경하여 사용한다.

제94조 (DB 접근수준 및 권한부여) ① 사용자가 DB 파일에 접근할 수 있는 수준은 최소

한의 접근 권한만 부여하는 원칙에 따라, DBA가 접근 정책을 결정해야 한다.

② DBA는 사용자의 시스템 자원 사용 수준을 결정해야 한다.

③ DBA는 테이블에 입력, 수정, 삭제 등 행위별 권한, 필드 접근 권한 등의 객체 권한을 조정해야 한다.

④ 사용자에게 DB 접근권한을 부여하는 경우, 적절한 롤을 생성하여 필요한 시스템 권한 및 객체 권한을 롤에 부여하고 그러한 롤을 사용자에게 부여한다.

⑤ 시스템 권한은 DBA에게만 부여한다.

⑥ 시스템 오브젝트 권한 부여 시 DBA 또는 권한을 부여 받은 사용자가 또 다른 사용자에게 권한을 부여해야 할 업무상의 필요가 있는 경우에만 권한을 부여한다.

⑦ 업무담당자에 의한 중요 자료 변경은 필요 시 DBA 허가를 통하여 처리할 수 있다.

제95조 (접근제어 설정 갱신 절차) ① 접근 제어에 대한 설정은 DB관리 부서장의 허가를 득하고서만 변경될 수 있도록 한다.

② 접근제어에 대한 설정은 환경의 변화 등을 반영하여 주기적으로 갱신한다.

③ 필요 시 접근제어 강화를 위하여 별도 보안솔루션(DB모니터링 툴 등)을 이용할 수 있다.

제96조 (암호화) ①기밀성이 요구되는 DB 시스템 내의 중요 필드에 대해 암호화되어 있어야 한다.

② 암호화를 지원할 수 있는 암호화 기술이 DB 시스템에 도입되어야 한다.

③ 필요 시 DB 암호화 강화를 위하여 별도 보안솔루션(DB암호화 툴 등)을 이용할 수 있다.

제97조 (로그 관리) ① 사용자의 로그인 시간 및 로그인 지속 시간이 적절한 범위 내에서 로깅 되어야 한다.

② 접속에 실패한 접근 시도가 로깅 되어야 한다.

③ DB 내의 Dead Lock이 로깅 되어야 한다.

④ 모든 사용자의 I/O 통계가 적절한 범위 내에서 로깅 되어야 한다.

⑤ System Table에의 접근이 로깅 되어야 한다.

⑥ 새로운 DB 객체의 생성이 로깅 되어야 한다.

⑦ 데이터 조작(필요할 경우, 날짜, 시간, 사용자와 함께) 이 적절한 범위 내에서 로깅 되어야 한다.

제98조 (감사) ① 중요 로그파일은 DBA에 의해서 정기적으로 점검되어야 하며, 특이 사항 발생 시 정보보호담당부서에 통보한다.

② 로그파일의 조작 및 읽기 권한은 원칙적으로 DBA에게만 부여하며, 필요 시 정보보호담당자에게 부여한다.

③ 로그파일의 무결성을 보장하기 위하여 로그파일 자체에 대한 모니터링을 정기적으로 실시한다.

④ 중요 자료에 대한 정기적 감사를 실시한다.

제99조 (백업주기 설정) ① 매일 이루어지는 변경사항에 대해 백업하고 최소 2개월 이상 보관한다.

② 영구 보관할 필요성이 대두되는 자료에 대해서는 영구보관을 할 수 있다.

③ 업무별 자료에 따라 보관 주기를 따로 정할 수 있다.

④ 과거에 사용했던 백업 매체의 사용불가가 예상될 경우 빠른 시일 내에 백업 매체를 변경하여 이관하도록 한다.

제10절 PC 보안

제100조 (PC사용자의 책임) PC의 운용 및 관리에 있어서 고의나 부주의 또는 직접적인 실수에 의한 보안사고 발생 시 각 PC의 해당 사용자가 그 책임을 지며, 그 세부 사항은 다음 과 같다.

1. 개인/업무용 PC의 경우는 PC사용자가 책임을 진다.
2. 실습실 등의 공용 PC는 실제 관리를 수행하는 PC관리부서의 장이 그 책임을 진다.

제101조 (필수 소프트웨어 설치 및 설치 제한) ① 본 대학교의 전산망 자원을 이용하고자 할 경우에는 바이러스백신 프로그램 및 패치관리시스템(PMS)을 반드시 해당 PC에 설치하여야 한다.

② 본 대학교의 정보자산을 침해하거나 우회할 수 있는 하드웨어나 소프트웨어를 임의로 설치해서는 안 된다.

제102조 (PC 변경 및 반출) PC 또는 부착된 하드웨어를 임의로 변경하거나 부서 밖으로 반출해서는 안 된다.

단, 업무상 필요한 경우, 해당 부서장의 승인을 득한 후 변경 및 반출할 수 있다.

제103조 (불법소프트웨어 사용 제한) ① PC사용자는 사용이 승인된 소프트웨어만을 사용해야 하며, 불법소프트웨어를 사용한 경우 개인 및 본 대학교가 모두 처벌 받을 수 있음을 양지하여야 한다.

② 불법 소프트웨어를 관리하기 위해 다음 각 호를 준수해야 한다.

1. 소프트웨어의 기본용도 외에 불법용도 변경을 금지한다.
2. 전산망 및 인터넷을 통한 불법복제를 금지한다.
3. 소프트웨어 사용권 증명서(라이선스)는 분실되지 않도록 안전한 곳에 보관한다.
4. 시리얼 넘버의 공유, 도용, 배포, 전송 등의 행위를 금지한다.

제104조 (PC 접근제어) ① PC는 CMOS 비밀번호와 부팅 비밀번호를 설정하여, PC를 악의적인 제 3자로부터의 위험으로부터 보호해야 한다. 단, 공용 PC의 경우는 역할과 특성을 감안하여 예외 적용할 수 있다.

② PC 사용자는 비밀번호 설정 시 6자 이상의 문자/숫자를 사용하며 추측이 어려운 단어를 선택한다.

③ 부팅 시 사용하는 비밀번호, 로그인 및 화면보호기에 사용하는 비밀번호는 최

소 6개월마다 변경한다.

④ 모든 PC는 반드시 비밀번호가 설정된 화면 보호기(1~5분)를 설치하여, 운용하여야 한다. 단, 공용 PC의 경우는 역할과 특성을 감안하여 예외 적용할 수 있다.

⑤ 공유 폴더 사용 시 반드시 사용자 ID인증 등을 수행하며, 그 사용이 끝났을 경우 즉시, 공유를 해제한다.

제105조 (비밀정보 및 백업 관리) ① PC내 하드디스크 및 저장매체에 비밀 정보 저장 시는 암호화해야 한다.

② 2인 이상이 공동으로 사용하는 공용PC에 비밀정보를 저장해서는 안 되며, 중요 파일은 비밀번호를 부여하여 접근을 통제해야 한다.

③ 비밀자료 또는 중요자료의 백업은 자료를 압축하거나 원본 그대로를 CD, 하드디스크, USB 메모리 등에 별도로 저장, 보관한다.

제106조 (바이러스 검사) ① 다음 각 호의 방법 중 하나를 선택하여 관리 책임이 있는 PC에 대하여 주기적으로 바이러스를 검사해야 한다.

1. 부팅 시 검사
2. 주기적인 예약 검사 등

② 주기적인 바이러스 검사를 위해 바이러스백신 프로그램이 PC에 설치되어 있어야 한다.

③ 자동엔진 업데이트 기능 등을 이용하여 매일 바이러스 엔진을 업데이트하여 백신 프로그램은 항상 최신 버전으로 유지해야 한다.

④ 다음 각 호의 외부로부터 받은 파일은 실행 또는 열기 전에 반드시 바이러스 검사를 수행해야 한다.

1. 외부에서 받은 CD나 USB 메모리 같은 저장매체
2. 인터넷에서 다운로드 받은 파일
3. 외부로부터 수신된 메일의 첨부파일 등

제107조 (바이러스 예방 조치 및 감염 시 조치사항) ① PC 사용자는 바이러스 예방을 위해 다음 각 호의 예방조치를 실시해야 한다.

1. 실행 전에 중요자료일 경우, 사본을 제작하여 보관하여야 한다.
2. 비 인가된 실행 프로그램(Shareware, Freeware 등)을 설치하지 않는다.
3. 출처가 분명하지 않은 전자우편은 되도록 열지 않도록 한다.

② 바이러스 감염 시 전산망 접속을 차단하고 즉시 인가된 바이러스 백신 프로그램으로 바이러스를 치료한다.

제108조 (각종 보안패치 및 서비스 팩의 공지 및 설치) ① 정보보호담당부서는 지속적으로 업데이트되고 있는 보안패치 및 서비스 팩 중 사용자가 반드시 설치해야 할 필요가 있는 긴급 보안 패치를 공지하여야 한다.

② 모든 PC 사용자는 공지된 보안패치 및 서비스 팩을 자발적으로 설치해야 한다.

제109조 (인터넷 유해사이트 접속금지) ① 본 대학교의 인터넷 사용관련 규정이나 기타

문건 등의 공지를 통해 접속을 제한하는 사이트는 방문하지 말아야 한다.

② 기본적인 금지 사이트는 다음과 같다.

1. 국가보안에 위배되는 사이트
2. 본 대학교에서 유해하다고 판단되는 사이트
3. 불법음란 사이트
4. 해킹 사이트
5. 채팅 사이트 등

③ 대용량 파일전송이 가능하고, 불필요한 네트워크 트래픽을 양산하는 P2P프로그램의 사용을 가급적 제한하며, 그 이용여부는 정보보호조직의 결정에 따른다.

제110조 (주기적 PC 보안진단 실시) PC 관리부서 및 사용자는 PC 보안을 위해 주기적으로 PC보안점검을 수행한다.

제111조 (휴대용 컴퓨터 기기 정보보호) 「국가정보보안 기본지침」, 「교육과학기술부 정보보안 기본지침」에 의거 휴대용 컴퓨터기기(Notebook 등), USB 메모리, 보조기억매체 등의 정보보호에 필요한 사항을 다음과 같이 정한다.

① 본 사항은 행정부서(대학본부, 단과대학, 부속 및 부설기관)로 한 한다.

② 본 사항에 사용하는 용어의 정의는 다음과 같다.

1. “휴대용 컴퓨터 기기”라 함은 노트북, 타블렛 PC 등의 휴대 가능한 컴퓨터 장비와 USB, 휴대 가능한 외장하드디스크 등의 보조기억장치를 말한다.
2. “휴대용 컴퓨터 기기 관리책임자”(이하 “관리책임자”라 한다)라 함은 각 팀 또는 단위 부서의 관리상 책임을 맡은 팀장 또는 담당을 말한다.
3. “휴대용 컴퓨터 기기 취급자”(이하 “취급자”라 한다)라 함은 해당 장비를 사용하는 자를 말한다.
4. “보조기억장치 관리시스템”(이하 “관리시스템”이라 한다)이라 함은 보조기억장치의 등록, 파기 등의 사용 현황을 관리하는 전자적으로 처리하는 시스템을 말한다.
5. “휴대용 컴퓨터 기기 관리번호”(이하 “관리번호”라 한다)라 함은 사용 중인 보조기억장치의 식별 및 관리를 용이하게 하기 위하여 부여한 번호를 말한다.

③ 휴대용 컴퓨터 기기의 사용은 각 부서에서 별지 서식 제9호 관리대장에 등재하고 변동사항을 정보보호책임자에게 통보하며, 정보보호담당부서에서는 통보받은 사항을 관리시스템에 일반용, 보안용을 구분하여 등록하고 사용 허가 사항을 부서에 통보한다.

④ 관리책임자는 매 분기 1회 휴대용 컴퓨터 기기 수량 및 보관 상태를 점검하여 별지 제10호 서식에 따라 확인·서명하여야 한다.

⑤ 관리책임자는 휴대용 컴퓨터 기기의 반·출입을 통제하여야 하며 별지 제11호 서식에 따라 기록하여야한다. 이때 반·출입은 업무상 목적에 한 한다.

⑥ 휴대용 컴퓨터 기기의 불용 처리시 관리책임자는 별지 제12호 서식에 따라 기록하여 정보보호책임자에게 통지하며, 정보보호 담당부서에서는 관리시스

템에 해당 사항을 삭제 조치한다.

⑦ 관리책임자는 소속직원이 미등록 휴대용 컴퓨터 기기를 사용하지 않도록 감독하여야 하며 이를 위반한 사실을 발견 또는 확인하는 즉시 정보보호책임자에게 통지하여야 한다.

⑧ 정보보호책임자는 대학 내 행정부서에서 사용하는 휴대용 컴퓨터 기기의 등록 현황을 파악하여야 한다. 이 경우 각 부서의 팀·과별 관리대장 사본을 비치·관리하고 관리시스템에 등록된 현황을 관리하는 것으로 갈음할 수 있다.

제11절 개인정보보호

제112조 (개인정보보호 정책) 본 대학교의 개인정보보호를 위한 정책은 “공공기관의 개인정보보호에 관한 법률(법률 제10465호)” 및 대학의 “보안업무 규정”의 제 9장 “개인정보 보호관리”를 준용하여 적용한다.

제 4 장 침해사고 예방 및 대응

제113조 (침해사고 예방) ① 정보보호담당자는 보안시스템 로그(방화벽/IPS 등 보안관련 로그)에 대하여 매월 1회 이상 점검하고 문제점 발견 시 정보보호관리자에게 보고하여야 한다.

② 침해사고대응팀은 서버 및 전산망 장비 등을 대상으로 연 2회 이상 취약점 점검을 실시한다.

③ 각 시스템/전산망/어플리케이션 운영담당자는 취약점 점검에 따른 결과에 따라 조치를 수행한다.

④ 취약점 점검은 외부 정보보호 전문업체 등을 통하여 수행할 수 있다.

⑤ 취약점 점검도구를 사용하는 경우의 관리는 다음과 같다.

1. 취약점 점검도구의 사용 및 관리는 정보보호담당자 또는 권한을 위임 받은 자로 제한한다.
2. 정보보호담당자는 취약점 점검도구의 접근통제에 대한 관리를 하여야 하며, 새로운 취약점 점검도구의 룰 업데이트를 실시한다.

⑥ 정보보호담당자는 PC, 서버 운영체계, 응용프로그램 및 전산망 장비에 대한 최신 보안 업데이트(patch 등)정보를 수집하고, 다음과 같은 절차에 따라 적용한다.

1. 정보보호담당자는 PC, 서버 OS, 응용프로그램 및 전산망 장비에 대한 최신 버전 및 보안패치 정보를 모니터링 한다.
2. 정보보호담당자는 서버운영담당자 및 어플리케이션 협력업체와 협의하여 보안패치 적용 가능성 여부를 검토한다.
3. 검토된 결과를 바탕으로 서버운영담당자 및 관련 협력업체와 보안패치에 대한 시험적용을 실시한다.

4. 시험적용이 성공한 경우 정보보호관리자의 승인을 거쳐 실제 운영시스템에 반영할 수 있도록 한다.
5. PC에 대한 신규 보안업데이트 발생의 경우, 교직원 및 교내 전 사용자에게 공지하여 적용하도록 한다.

제114조 (침해사고의 탐지) 침해사고의 탐지를 위하여 정보보호담당자 및 침해사고대응팀원, 서버운영자는 다음과 같은 사항들을 확인하여야 한다.

1. 실패한 로그인 시도
2. 비활성화 된 계정으로의 로그인 정보
3. 업무시간 외 동안의 작업 내역
4. 서버 운영자에 의해 생성된 것이 아닌 새로운 계정
5. 새로이 생성된 파일 및 인스톨 되어 있는 프로그램
6. 웹 서버상의 다른 페이지나 변경된 페이지의 유무
7. 사용자의 업무 이외의 기능이나 명령
8. 시스템 로그의 삭제나 삽입
9. 인가되지 않은 라우터나 침입차단시스템의 규칙
10. 특이할 만큼의 속도 및 성능 저하
11. 시스템 장애 등

제115조 (침해사고 보고) 정보보호담당자 및 침해사고대응팀원은 침해사고의 발생 및 침입 흔적을 인지한 경우 정보보호책임자 및 정보보호관리자에게 문서로 보고하여야 하며, 침해사고 발생 사실을 지정된 보고자 이외의 사람에게 유출시켜서는 안 된다.

제116조 (침해사고 대응) ① 정보보호담당자 및 침해사고대응팀원은 시스템에 대한 침입이 확인되면 다음과 같은 사항에 기초하여 긴급 대응을 실시하여야 한다.

1. 백도어의 확인
2. 스캐닝 및 스니핑 탐지
3. 허가 받지 않은 서비스의 조사
4. 비밀번호 파일의 변경여부
5. 시스템 및 전산망 설정 파일조사 등

② 정보보호담당자 및 침해사고대응팀원은 다음과 같은 경우 시스템의 폐쇄, 전산망 감시기능 강화, 전산망 전송의 전면차단, 사용자 계정의 삭제 등 침해사고의 확산을 방지하기 위한 조치를 취하여야 한다.

1. 분산 서비스 거부 공격을 당하고 있어 정상적인 동작이 불가능한 경우
2. 침입자에 의해 시스템의 중요 파일이 삭제되고 있는 경우
3. 트로이 목마, 백도어 등의 악성 프로그램 실행으로, 정상적인 접근제어를 적용하더라도 다른 경로를 통한 침입자의 지속적 공격시도가 있는 경우
4. 기타 침입자의 공격에 대한 대응수단이 없는 경우 등

③ 각 업무별 운영담당자는 침입자를 식별하기 위한 증거를 수집하여야 하며, 법률적 대응을 할 경우 증거물로 활용될 수 있는 해당 시스템의 백업 데이터,

침입차단 시스템 로그, IPS 로그, 라우터 로그 등과 같은 로그파일을 안전하게 저장하여야 한다.

④ 침해사고에 대해서 외부 언론매체에 알려지지 않도록 해야 하며, 외부 언론매체에서 피해사건과 관련된 문의를 해 올 경우 직접 대응 하지 말고, 홍보 담당자에게 연결하여 언론매체에 대응할 수 있도록 한다.

⑤ 정보보호 담당부서는 필요할 경우 관련 국가기관의 협조를 받기 위한 절차를 준비한다.

제117조 (침입자 추적 및 연락) ① 침입자가 시스템 내에 로그인해 있다면, 가능한 도구나 명령어를 이용하여 침입자에 관련된 정보를 수집하여야 한다.

② 내부 침입의 경우 침해사고대응팀원은 침입한 시스템 위치를 확인 후 조치를 취하여야 한다.

③ 다른 사이트를 거쳐 침입했을 경우 해당 사이트 관리자에게 경고를 통해 필요한 조치를 취할 수 있게 한다.

④ 외부에서 침입한 경우 시스템 및 전산망 운영자는 로그를 유지하고 침해사고대응팀원은 로그를 분석하여 침입자를 추적하여야 한다.

⑤ 추적에 성공하여 도메인 주소나 IP 주소를 알아낸 경우 관련 사이트의 연락처 정보(e-Mail 또는 전화 등)를 알아내고, 이에 대한 조치를 요청하여야 한다.

제118조 (침해사고 시스템 복구) ① 침입자에 의해 사용된 시스템 취약점을 수정하고 변경된 정보를 복구 및 삭제하는 것으로는 보안상 완벽한 시스템을 유지하기에는 부적합하므로, 각 업무별 운영담당자는 침해사고가 발생한 시스템 또는 침입이 의심되는 시스템의 운영체제 및 기타 어플리케이션의 재설치를 검토하여야 한다.

② 재설치 시 각 벤더에서 제공하는 최신 보안패치를 적용하여야 한다.

③ 각 업무별 운영담당자는 패치를 적용하기 전에 기존에 운용 중인 어플리케이션 및 서비스에 영향을 미치지는 않는지 검증을 거친 후 적용하여야 한다.

④ 백업에서 데이터를 복구할 경우 침해당하지 않은 시스템에서 데이터에 취약점이나 트로이 목마 프로그램은 없는지 확인 후 복구한다.

⑤ 시스템에서 보안 취약점이나 설정상의 보안문제를 해결하고 보안 패치를 적용한 후에는 모든 사용자 계정에 대해서 비밀번호를 변경한다. 변경 시에는 추측하기 어려운 비밀번호를 설정하도록 하며, 계정정책에서 옵션들을 설정하여 보안을 강화하도록 한다.

제119조 (침해사고 사후활동) ① 정보보호담당자 및 침해사고대응팀원은 침해사고에 대한 대응 및 복구가 완료된 경우, 보고서를 작성하여 정보보호관리자에게 보고하여야 하며, 정보보호관리자는 이를 정보보호책임자에게 보고하여야 한다.

② 필요한 경우, 정보보호담당부서는 침해사고를 방지하는 적절한 기능의 보안도구를 설치하고, 이에 대한 적절한 기준을 적용하여 보안기능을 수용할 수 있도록 한다.

③ 정보보호담당자는 시스템 및 전산망에 대한 취약점 분석도구를 사용하여 보안상 취약점을 수시로 점검·보완하고, 사용자 계정, 사용자 권한, 파일시스템, 환경설정 변수 등에 대한 보안강화를 위한 절차를 수립·배포하여야 한다.

④ 서버운영자는 이벤트 뷰어나 네트워크 모니터, 성능 모니터와 같은 전용 툴을 사용하여 시스템 성능 및 침입시도를 모니터링 한다.

⑤ 침해사고 대응결과에 대하여 정보보호관리자는 재발방지를 위해 조치사항을 각 업무담당자에게 통보한다.

제120조 (보안관련 교직원 교육 및 훈련) 정보보호관리자는 침해사고의 사전 예방 및 사고발생시 신속한 대응 및 조치를 위해 침해사고대응팀, 서버운영자 및 관련 교직원에 대하여 연 1회 이상 침해사고 예방 및 대응 교육을 실시하여야 하며, 교육의 대상자는 이를 숙지하여야 한다.

제 5 장 정보보호감사

제121조 (정보보호감사 영역) ① 정보보호감사는 정보보호 기준에 규정된 사항을 확인하기 위한 모든 활동을 그 범위로 하며 정보자산, 정보자산 관리인력 및 본 대학교 구성원을 그 대상으로 한다.

② 정보보호감사는 다음과 같은 부문을 포함하며, 정보보호책임자의 검토에 의해 조정이 가능하다.

1. 관리적, 물리적, 기술적 보안 부문
2. 정보자산에 대한 위험분석 부문 등

제122조 (정보보호감사 구분) ① 정보보호감사는 정기 정보보호감사, 특별 정보보호감사, 정기 정보보호진단으로 구분하며 그 내용은 다음과 같다.

② 정기 정보보호감사는 연간 정보보호감사 계획에 따라 실시하는 계획된 감사를 말하며 매년 1회 실시한다.

③ 특별 정보보호감사는 보안사고와 같은 중요 사안의 발생 시 정보보호책임자의 요청에 의해 실시한다.

④ 정기 정보보호진단은 정보시스템 등의 주요 IT자산에 대해 매분기 1회씩 자체점검을 통한 보안진단을 실시한다.

⑤ 정기 정보보호진단은 매월 세 번째 수요일에 실시하며, 정기 정보보호진단일이 공휴일인 때에는 익일에 실시한다.

제123조 (정보보호감사 계획) ① 정보보호책임자는 정보보호감사 계획을 수립 및 공지하여야 한다.

② 정보보호감사 계획은 정보보호 정책·규정의 제·개정 및 공표와 그에 따른 이행 기간을 모두 고려하여 작성되어야 하며, 검사 실시 범위, 시기 및 방법 등이 기술되어야 한다.

제124조 (정보보호감사 조직 구성) ① 정보보호책임자는 정보보호감사를 실시하기 위한 조직을 구성한다.

② 정보보호감사 조직의 구성이 여의치 않을 경우 외부 전문가에게 용역으로 맡길 수 있다.

제125조 (정보보호감사 목표 설정) 본 대학교의 정보보호 정책, 규정 및 절차 또는 관련 법령에 규정된 사항을 확인하기 위하여 각 항목별로 세부검사목표를 설정하고 검사를 실시한다.

제126조 (정보보호감사 증적 수집) ① 정보보호정책 및 규정에 정의된 사항이 부정이나 오류 없이 이행되었다는 것을 확신하기 위한 감사 증적을 수집하여야 한다.

② 효율적인 감사가 되도록 감사를 실시하기 전에 감사계획에 의거 요청할 관련 자료를 담당자에게 서면으로 송부할 수 있다.

③ 감사 증적을 수집하기 위하여 질문, 관찰, 문서검증, 비교 대조, 시사 등의 방법 중에서 단수 또는 복수 개를 선택하여 적용할 수 있다.

④ 정보보호감사 증적의 요건은 다음을 만족하여야 한다.

1. 목표에 적합한 관련 있는 감사 증적을 수집하여야 한다.
2. 목표를 달성하기 위한 충분한 양의 감사 증적을 수집하여야 한다.

제127조 (정보보호감사 결과 기록) ① 감사결과 수집한 증적을 관리하여야 하며 이를 문서화하여 보관한다.

② 감사결과는 총장 또는 외부 감독기관의 요청이 있는 경우 이를 제출할 수 있도록 보관하여야 한다.

③ 정보보호감사 결과 보고서에는 다음과 같은 내용이 포함될 수 있다.

1. 보고서는 감사의 목적과 범위, 실시 기간 등을 명시하고 주요 결과를 요약하여 기술한다.
2. 지적사항에 대해서는 관련 업무 담당자와 상위관리자의 의견이나 향후 조치 계획 등이 함께 기술되도록 한다.
3. 정보보호 정책·규정의 미흡한 부분이나, 운영자들의 건의 사항 등을 반영하여, 정보보호 정책·규정의 제·개정 방향이 반영되도록 한다.
4. 정보보호감사를 외부 전문가를 활용하여 시행한 경우 외부 전문가에 의해 시행된 범위를 명시하며, 정보보호감사의 전부를 외부에 위탁하여 시행한 경우에는 외부전문가의 감사보고서로 대치할 수 있다.

제128조 (정보보호감사 결과 보고) 정보보호감사의 결과는 정보보호관리자가 취합하여 정보보호책임자에게 보고하고, 필요시 정보보호심사위원회의 심의를 거쳐 총장에게 보고한다.

제 6 장 정보보호 규정의 유지관리

제129조 (규정의 검토) 정보보호관리자는 정보보호규정의 타당성을 매년 1회 정기적으로 검토해야 하며, 업무환경의 변화 발생 등과 같은 변화요인 발생 시 추가 검토를 수행할 수 있다.

제130조 (규정의 제·개정) ① 정보보호와 관련하여 새로운 요구 사항이 도출되거나 정보

보호감사 결과 및 정보보호 정책·지침의 검토 결과 개정이 필요한 경우 또는, 사용자에 의해 개선안, 이의, 문제점 등이 제기된 경우에는 정보보호규정을 제·개정해야 한다.

② 정보보호담당부서는 관련 전문가와 해당 실무자들과 함께 제·개정 사항을 검토 후 제·개정한다.

③ 제·개정안은 정보보호관리자의 검토를 거친 후 정보보호책임자의 승인을 받아야 하며, 승인된 정보보호규정에 대하여 정보보호전문위원회 및 정보화추진위원회 심의를 받아야 한다.

④ 정보보호책임자는 제·개정된 규정 사항을 모든 사용자에게 공지하고 유예 기간을 고려하여 적용해야 한다.

제131조 (규칙 등의 준용) 이 규정에 명시되지 않거나 해석의 차이가 발생하는 사항은 상위 기관의 규정, 규칙, 세칙 등을 따르며 그 내용의 범위 내에서 필요한 사항을 준용한다. <본조 신설 2021.12.13.>

부 칙

1. (시행일) 본 규정은 2011년 11월 29일부터 시행한다.
2. (예외적용) 다음 각 호에 해당하는 경우에는 본 규정에서 명시한 내용일지라도 정보보호책임자의 승인을 받아 예외 취급할 수 있다.
   (1) 기술 환경의 변화로 적용이 불가능할 경우
   (2) 기술적, 관리적 필요에 따라 규정의 적용을 보류할 긴급한 사유가 있을 경우
   (3) 기타 재해 등 불가항력적인 상황일 경우
3. (경과조치) 특별한 사유에 의하여 본 규정에서 정하는 요건을 충족하지 못한 경우에는 시행일로부터 1년 이내에 개선방안을 강구한다.
4. (시행일) 이 개정 규정은 2014년 4월 22일부터 시행하되, 2014년 3월 1일부터 적용한다.
5. (시행일) 이 개정 규정은 2021년 12월 13일부터 시행한다.

[별지 제1호 서식] 정보보안서약서(외부자용) <개정 2021.12.13.>

보 안 서 약 서

본인은 년 월 일부로 한국항공대학교와 관련한 업무(용역, 연구개발, 제작, 입찰, 그 밖의 업무)를 수행함에 있어 다음 사항을 준수할 것을 서약 합니다.

1. 본인 한국항공대학교 유지보수 용역 관련 업무 중 취득하게 될 일체의 내용이 직무상 기밀 사항임을 인정한다.

2. 본인은 관련된 소관업무가 국가 기밀(개인정보 포함) 사항임을 인정하고 제반 보안 관계 규정 및 지침을 성실히 준수한다.

3. 본인은 이 기밀(개인정보 포함)을 누설함이 이적행위가 됨을 명심하고 재직 중은 물론 퇴직 후에도 알게 된 모든 기말사항을 [부폐방지권익위법], [공익신고자 보호법]에 따른 신고의 경우를 제외하고는 일절 타인에게 누설하지 아니한다.

4. 본인은 이 기밀 사항을 누설한 때에는 [국가보안법] 제4조제1항제2호 및 제5호(국가기밀 누설 등)와 [형법] 제99조(일반이적) 및 제127조(공무상 비밀의 누설) 관계 법규에 따라 엄중한 처벌을 받을 것을 서약 한다.

5. 본인은 제3자(업체)를 통한 공동의 사업 수행 시 이로 인해 발생하는 위반사항에 대하여 모든 책임을 부담한다.

년 월 일

서약자 소 속 : 직급/직위 :
생년월일 : 성 명 : (인)

서약집행자 소 속 : 한국항공대학교
직 위 : 전산정보전략팀장 (인)

한국항공대학교 총장 귀하

[별지 제2호 서식] - 외부용역 업무완료 보안 점검표

외부용역 업무완료 보안 점검표

1. 사업 개요

외부용역명		**외부용역 수행기간**	
업무주관부서 사업관리자		**외부용역 관리자**	

2. 외부용역 업무 수행시 인적사항

성 명	소 속	직 급

3. 확인 항목

점검항목	완결여부	미결 사항 및 조치 사항	확인책임자	서명
정보시스템 계정 삭제 요청			업무주관부서 사업관리자	
기타 물리적 접근권한 (열쇠 등) 반납				
지급 정보자산 및 지적재산 반납/삭제				
자료 및 문서 반납/폐기				
기밀유지 준수 확인				
기타 보안 관련 정리 사항				

[별지 제3호 서식] 출입 관리 대장 <개정 2021.12.13.>

(　　)실 출입 관리 대장

　　년　월

일자	출 입 자		출입 목적	입 회 자		입실 시간	퇴실 시간	입회자 확인
	소속	성명		소속	성명			

* 서버룸 입 · 출입시 개인정보 유 · 노출 금지 등의 보안관계 규정 일체를 지키고 서버룸 내 카메라 소지 및 촬영을 금 함

* PC · 노트북 등 전산장비 반입이 있는 경우 최신 백신으로 바이러스 및 보안패치, 악성코드를 점검하여 별동의 " 장비 반출입 관리대장"을 작성 해야 함

[별지 제4호 서식] - 보안시스템 정책 요청서

보안시스템 정책 요청서

신청일: 년 월 일

신청부서		**신청자**	
연락처		**이메일**	
사용기간	년 월 일 ~ 년 월 일		
구분	신규 / 변경 / 연장 / 해지		
서비스 요청 사유			
요청 내역	사용자 IP 주소 (Source IP)		
	목적지 IP 주소 (Destination IP)		
	프로토콜		
	사용포트		
기타 요청사항			
정보보안 담당자 의견			

주) - 만료기간 경과 후(최대 1년) 별도 연장 신청이 없을 경우 해당 룰은 자동 삭제됨
- 보안장비 계정 필요시 이메일 아이디와 동일한 계정이 발급됨
- 학내구성원에 한하여 신청이 가능하며, 외부업체의 접속 요청일 경우 [별지 제1호 서식]정보보호서약서(외부자용)를 같이 제출해야함

[별지 제5호 서식] 사용자계정신청서

사용자계정신청서

계정 신청자

신청일	
구 분	신규( ), 추가( ), 삭제( ), 기타( )
사용기간	200 . . . ~ 200 . . , 영구( )
사 유	
부서명	
사용자 ID	
사용자 이름	
사용자 그룹	

시스템 관리자

지정 그룹	
접근 가능 권한	
비 고	

[별지 제6호 서식] 시스템 계정 관리 대장

시스템 계정 관리 대장

시스템 담당자		소속팀	
시스템 명		시스템 운영체계(OS)	

계정 명	사용자	부서	권한	용도	기간	비고

[별지 제7호 서식] - DB사용자 계정 및 권한 신청서

DB사용자 계정 및 권한 신청서

신청일			
신청자	소속	성명	
ID 구분	개인 ID ( ) 공용 ID ( )		
기본 정보	신청 ID	신청 DBMS	유효기간
ID 신청 사유			
필요 권한 내역			
권한 요청 사유			

[별지 제8호 서식] - DB사용자 관리대장

DB사용자 관리대장

시스템 명		시스템 운영체계(OS)	

ID	등록 일자	종료 일자	데이터베이스 사용권한					utility 사용권한	object 생성권한
			object명	select	insert	update	delete		

[별지 제9호 서식] - 휴대용 컴퓨터 기기 관리대장

휴대용 컴퓨터 기기 관리대장

부서명 : 관리책임자 :

순번	관리번호 (S/N)	매체형태	등록일자	취급자	불용 처리일자	불용 처리방법	비고

[별지 제10호 서식] - 휴대용 컴퓨터 기기 점검대장

휴대용 컴퓨터 기기 점검대장

부서명 : 관리책임자 :

점검일시	보유 수량		이상 유무	점검자		비고
	일반용	보안용		성명	서명	

[별지 제11호 서식] - 휴대용 컴퓨터 기기 반·출입대장

휴대용 컴퓨터 기기 반·출입대장

부서명 : **관리책임자 :**

기기명	관리번호 (S/N)	사용자	용도	일시 (입·출 구분)	확인

[별지 제12호 서식] - 휴대용 컴퓨터 기기 불용처리 확인서

휴대용 컴퓨터 기기 불용처리 확인서

아래와 같이 휴대용 컴퓨터 기기 불용처리 대하여 확인을 요청함.

순번	관리번호 (S/N)	매체 형태	사용자	불용처리 사유	비고
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

확인 요청 일자 : 년 월 일

요청부서 : , 요청자 : (인)

확인부서 : , 확인자 : (인)