	정보보안규칙	규정번호	8-0-2		
		제정일자	2013.03.01		
		개정일자	2016.07.01		
		개정번호	Ver.1	총페이지	17

제1장 총칙

제1조(목적)

이 규칙은 동양미래대학교(이하 "본 대학"이라 한다)의「보안규칙」에 따라 정보보안을 위하여 수행하여야 할 기본활동 규정을 목적으로 한다.

제2조(적용범위)

이 규칙은 본 대학의 전 교직원 및 본 대학을 위해 종사하는 외부업체 직원 모두에게 적용된다.

제3조(용어정의)

이 규칙에서 사용하는 용어의 정의는 다음과 같다.

1. "정보시스템"이라 함은 서버·PC 등 단말기, 보조기억매체, 네트워크장치, 응용프로그램 등 정보의 수집·가공·검색·송수신에 필요한 하드웨어 및 소프트웨어를 말한다.
2. "정보자산"이라 함은 정보 및 정보시스템을 통칭하며, 정보시스템에는 서버, 네트워크, 보안시스템, 시설 등이 포함된다.
3. "위협"이라 함은 자산에 손실을 초래할 수 있는 원치 않는 사건의 잠재적 원인 또는 행위자를 말한다.
4. "취약성"이라 함은 자산의 잠재적 속성으로서 위협의 이용 대상이 되는 것을 말한다. 때로 정보보안 대책의 미비로 정의되기도 한다. 자산에 취약성이 없다면 위협이 발생해도 손실이 나타나지 않는다.
5. "위험분석"이라 함은 자산, 위협, 취약성, 기존 보호대책 등을 분석하여 위험의 종류와 규모를 결정하는 것을 말한다.
6. "위험평가"라 함은 분석된 위험을 수용 가능한 위험수준과 대비하여 위험의 대응여부와 우선순위를 결정하는 것을 말한다.
7. "잔여위험"이라 함은 위험분석 후 위험을 수용하기로 결정하고 별도의 보안대책을 적용하지 않는 위험정도를 말한다.
8. "위험감소"라 함은 위험을 감소시킬 수 있는 대책을 채택하여 구현하는 것을 말한다.
9. "보안시스템" 이라 함은 정보의 수집·가공·저장·검색, 송수신 중에 나타나는 정보의 훼손·변조·유출 등을 방지하기 위한 기술적 수단으로써 침입차단시스템, 침입탐지시스템, VPN(가상사설망) 등이 이에 해당한다.
10. "정보통신실"이라 함은 서버·PC 등 전산장비와 스위치·교환기·라우터 등 통신 및 전송장비 등이 설치 운용되는 장소를 말하며, 전산실·통신실 및 전산자료 보관실

등을 말한다.
11. "저장매체"라 함은 자기저장장치·광저장장치·반도체저장장치·보조기억장치(USB 등) 등 자료기록이 가능한 전자장치를 말한다.
12. "보조기억매체"라 함은 디스켓·CD·하드디스크·USB 메모리 등 자료를 저장할 수 있는 것으로 정보시스템과 분리할 수 있는 기억장치를 말한다.
13. "정보보안" 또는 "정보보호"라 함은 정보시스템 및 정보통신망을 통해 수집·가공·저장·검색·송수신 되는 정보의 유출·위변조·훼손 등을 방지하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위로서 사이버안전을 포함한다.
14. "전자정보"라 함은 대학 내 업무와 관련하여 취급하는 전자문서 및 전자기록물을 말한다.
15. "RFID(Radio Frequency IDentification)시스템"이라 함은 대상이 되는 사물 등에 RFID 태그를 부착하고 전파를 사용, 해당 사물 등의 식별정보 및 주변 환경정보를 인식하여 각 사물 등의 정보를 수집·저장·가공 및 활용하는 시스템을 말한다.
16. "사이버공격"이라 함은 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스방해 등 전자적 수단에 의하여 정보통신망을 불법 침입·교란·마비·파괴하거나 정보를 절취·훼손하는 공격행위를 말한다.
17. "보안감사"라 함은 정보보호 및 개인정보보호와 관련된 통제절차의 기록과 행동을 독립적으로 조사·관찰하고 관련 증거를 수집하여 분석함으로써 주요 정보자산의 무결성, 가용성 및 기밀성을 확인하고자 하는 일련의 정보보안 관리 활동을 말한다.
18. "분야별보안담당관"이라 함은 보안담당관, 정보보안담당관, 부서별보안담당관을 총칭하여 말한다.
19. 기타 용어정의는「보안규칙」및「개인정보보호규칙」과 관계 지침에 따른다.

제4조(정보보안 정책의 준용)
본 대학의 정보 자산에 대한 정보보안 업무는 이 규칙을 준용하며, 이 규칙에 명시되지 아니한 사항은「보안규칙」에서 정하는 바에 따른다.

제5조(정보보안 규칙의 유지관리)
① 본 대학 정보보안 관련 규칙은 최고보안담당관의 승인을 득한 후 인쇄물 형태나 본 대학의 전자게시판 등을 통하여 전체 교직원에게 공표한다.
② 전체 교직원은 정보보안 관련 문서(규칙, 지침, 절차 등)를 충분히 숙지하고 준수한다.
③ 최고보안담당관은 위험분석 및 평가를 실시하여 필요한 대책을 강구하고 정보보안 관련 문서에 대하여 정기적으로 타당성을 검토하여 정보보안 관련 규정을 개정한다.
④ 정기적인 타당성 검토 이외에 중대한 보안사고 발생, 새로운 위협 또는 취약성의 발생, 정보보안 환경의 중대한 변화 등이 발생했을 경우에는 관련 사항에 대하여 추가로 검토하여 개정한다.

제2장 정보보안 조직

제6조(정보보안 조직의 구성)
① 본 대학은 정보보안 관리 업무를 체계적이고 효율적으로 수행하기 위하여 정보보안 전문지식을 보유한 인력을 확보하고 관련 전담조직을 구성하여 운영하여야 한다.
② 최고보안담당관은 보안실무를 담당할 분야별보안담당관을 선임하여야 하며, 정보보안담당관 및 부서별보안담당관은 해당 조직의 정보보안 실무에 대한 책임을 진다.
③ 정보보안담당관은 보안담당관의 업무 중 정보통신 및 정보시스템 관련 전자정보의 수집·저장·검색·송수신 등에 대한 보안업무를 지원한다.
④ 본 대학은 정보보안 활동을 효과적으로 수행하기 위하여 정보보안위원회를 구성·운영할 수 있다.
⑤ 정보보안 조직 구성의 세부사항은「보안조직관리지침」으로 따로 정한다.

제7조(역할과 책임)
① 본 대학 전체 교직원은 자신의 업무와 관련하여 이 규칙 및 관계 지침을 이해하고 준수하여야 한다.
② 정보보안 조직의 직무별 역할과 책임은「보안조직관리지침」으로 따로 정한다.

제3장 정보보안관리 체계의 구축 및 운영

제8조(정보자산 식별)
① 부서별보안담당관은 정보자산을 서버, 보안시스템, 네트워크, 소프트웨어, PC, 시설장비 등으로 구분하여 다음 각 호로 분류하고 별지 제4호 서식 '정보자산목록(표)'을 작성·유지하여야 한다.
1. 서버: 서버운영체제(윈도우, 유닉스, 리눅스 등)를 사용하고 있는 정보시스템 장비
2. 보안시스템: 침입차단시스템, 침입탐지시스템 등 정보 자산의 보호를 위한 시스템 장비
3. 네트워크: 라우터, 스위치 장비 등 네트워크 통신에 필요한 주요 장비
4. 소프트웨어: OS, DBMS, 그룹웨어 등 정보시스템에서 실행되는 시스템소프트웨어 및 응용소프트웨어
5. 기타 시설장비, PC, 상용소프트웨어 등을 포함한다.
② 부서별보안담당관은 정보자산 별 보안등급, 소유자, 관리자 등 정보자산 관리를 위하여 필요한 식별정보가 최신의 상태로 유지되도록 하여야 한다.

제9조(위험분석 및 평가)
① 부서별보안담당관은 정보자산의 중요도를 평가하고 보안등급을 분류하여 관리하여야 한다.
② 부서별보안담당관은 등급이 분류된 정보자산 보안등급을 별지 제4호 서식 '정보자산목록(표)'에 유지하여 관리하여야 한다.
③ 부서별보안담당관은 년 1회 이상 정보자산의 보안등급을 재검토하여 용도 및 세부내역이 변경된 정보자산의 경우 보안등급을 재분류하여야 한다.

제10조(정보보안 대책 수립)
① 위험감소를 위해서 적절한 통제를 선택하고 구축한다.
② 선택한 통제를 구축하기 위해서 필요한 자산의 조달, 역할의 할당, 절차의 문서화, 교육 훈련 등을 병행한다.
③ 구축된 통제를 일목요연하게 관리하기 위해 정보보안 대책을 수립하여야 한다.
④ 잔여위험 및 통제절차에 대하여는 각 정보자산의 보안관리를 위해 마련한 지침 및 절차에 따라 지속적으로 관리한다.

제11조(정보보안 계획 수립 및 대책 구현)
① 정보보안 대책의 수립 이후 주요 정보보안 대책의 구현 일정, 예산, 책임, 운영계획 등이 포함된 정보보안 계획을 수립하여야 한다.
② 정보보안계획은 연간 정보보안 계획서로 문서화하여야 하며, 최고보안담당관 및 총장의 승인을 득하여야 한다.
③ 정보보안 계획에 근거한 관리적 대책, 기술적 대책, 물리적 대책을 구현하고 운영하여야 한다.

제12조(모니터링 및 보안감사)
① 정보보안관리가 효과적으로 운영되고 있는지 지속적으로 모니터링하여야 하며, 이를 위해 다음 각 호와 같은 활동을 수행한다.
1. 발견된 취약점 및 부적합 사항에 대한 적절한 조치를 위한 통제 실시
2. 정보보안관리의 적정성에 대한 주기적인 검토
3. 정보보안관리의 유효성 확인을 위한 문서 및 자료 기록·유지
② 정보보안 관련 감사에 관한 세부사항은 「보안감사지침」으로 따로 정한다.

제13조(유지 및 개선)
① 정보보안관리의 효과성 유지를 위하여 주기적으로 기술적, 환경적 변화 및 업무 요구조건의 변화 등을 반영하여 필요한 변경조치를 취한다.
② 정보보안관리 체계를 개선하기 위하여 지속적인 활동을 수행하여야 한다.

제4장 문서보안 관리

제14조(전산자료 보안)
① 정보보안담당관은 다음 각 호의 전산자료를 대외비로 분류하여 관리하여야 한다.
1. 최초로 정보통신망을 신설하여 전산자료의 보호등급 구분이 필요한 경우
2. 현재 운용중인 정보통신망을 재구성할 경우
3. 정보통신망 세부 구성현황(IP 주소 세부 할당현황 포함)
4. 보안취약성 분석·평가 결과물
5. 총장이 필요하다고 인정하는 경우
② 부서별보안담당관은 전산자료의 효율적 보호를 위하여 자체 실정에 맞는 전산자

료 보호등급을 분류하여 운영하여야 한다.
③ 부서별보안담당관은 전산자료를 보호하기 위해서는 자료별 비밀번호 사용과 시스템 접근권한 설정 등 보안대책을 적용, 관리하여야 한다.
④ 전산자료의 보존기간이 경과한 이후 심의를 거쳐 더 이상의 필요성이 없는 것으로 평가된 경우에는 소각, 파쇄, 용해 등 재사용이 불가능한 상태로 완전 파기하여야 한다.

제15조(문서 보존기간)
문서의 보유기간이 만료되면 보존기간은「문서관리규칙」을 준용한다.

제5장 보안성 검토

제16조(보안성 검토)
① 최고보안담당관은 정보화 사업 추진 및 정보통신망의 신ㆍ증설 등 보안대책 강구 등에 대한 적절성 확인을 위하여 중요하다고 판단되는 경우 보안심사위원회에 보안성 검토를 요청하여야 한다. 다만, 경미한 사항에 대해서는 자체적인 보안성 검토를 수행할 수 있다.
② 다음 각 호의 정보화 사업 추진 시 안정성 확보를 위하여 보안성 검토를 수행할 수 있다.
1. 비밀 등 중요 자료의 생산, 등록, 보관, 사용, 유통 및 재분류, 이관, 파기 등 비밀업무와 관련된 정보시스템 및 네트워크 구축
2. 대규모 정보시스템 또는 다량의 개인정보를 처리하는 정보시스템 구축
3. 내부 정보통신망을 인터넷이나 타기관 전산망 등 외부망과 연동하는 경우
4. 원격근무 시스템 구축
5. 업무망과 인터넷망 분리 사업
6. 기타 총장이 보안성 검토가 필요하다고 판단하는 정보화 사업

제17조(제출문서)
① 보안심사위원회에 보안성 검토를 요청하는 경우 제출하는 문서는 다음 각 호와 같다.
1. 기술제안요청서(RFP)
2. 정보통신망 구성도(IP주소체계 포함)
3. 자체 보안대책 강구사항

제18조(결과조치)
① 최고보안담당관은 보안성 검토 의견을 준수하여 시정이 필요하다고 판단되는 경우에 보안대책을 강구하여야 한다.
② 최고보안담당관은 정보화 사업 및 정보통신망과 관련한 보안대책이 적절히 수행되었는지 등의 이행여부를 확인하여야 한다.

제6장 정보보안 교육

제19조(정보보안 교육계획 수립)

① 최고보안담당관은 교내의 업무담당자 및 업무관계자를 대상으로 보안인식 및 직무능력 향상을 위하여 연간 보안교육 시행계획을 수립하여야 한다.

② 정보보안 교육시행에 필요한 업무 역할은 다음 각 호와 같다.

1. 전체 교직원을 대상으로 보안인식 제고 및「정보보안규칙」,「개인정보보호규칙」등의 이행에 필요한 교육 계획 수립
2. 정보보안 기술 향상을 위한 교육 계획 수립
3. 부서별보안담당관은 보안담당관과 협의하여 여타 교육과 중복되지 않는 범위 내에서 부서별 업무담당자를 대상으로 별도의 보안교육 실시

제20조(보안교육 실시)

① 정보보안 교육계획을 수립하여 전체 교직원을 대상으로 정기(년 1회이상)적인 보안교육을 실시하여야 한다.

② 정기 보안교육 미 이수자의 대체교육 시행방안은 다음 각 호와 같다.

1. 미 이수자 소집을 통한 재교육
2. 교육 교안 제공을 통한 자가 학습 평가

제21조(보안교육 평가)

최고보안담당관은 보안교육 훈련 결과를 점검하여 교육 내용 개선을 위한 평가를 실시하여야 한다.

제7장 외부인 보안

제22조(외부인 보안)

외부인의 기밀유지를 위한 보안관리 방안은「인적보안관리지침」에 따르며, 보안서약서는 부서별보안담당관을 통해 보안담당관에게 제출하여야 한다.

제23조(외부인 접근에 대한 보호)

① 보안담당관 및 정보보안담당관은 외부인의 교내 보호구역 출입 등에 관한 사항은「인적보안관리지침」으로 따로 정한다.

② 정보시스템 접근과 관련한 보안관리를 위하여 통제 조치를 하여야 하며, 정보시스템 접근을 위한 접근통제는「응용프로그램보안관리지침」으로 따로 정한다.

제24조(용역사업 보안관리)

① 최고보안담당관은 정보화·정보보안사업 및 컨설팅 수행 등을 외부용역으로 추진할 경우 사업 책임자로 하여금 보안대책을 수립·시행하여야 한다.

② 최고보안담당관은 제1항에서 규정한 보안대책의 시행과 관련한 이행 실태를 주기적으로 점검하고 미비점 발견 시 사업 책임자로 하여금 보완토록 하여야 한다.

③ 기타 세부사항은「인적보안관리지침」으로 따로 정한다.

제8장 시설보안
제1절 보호구역 관리

제25조(정보통신실 보안관리)
① 정보통신실은 통제구역으로 지정, 관리한다.
② 비인가자가 업무상 부득이한 사유로 출입하여야 할 경우에는 정보보안담당관에게 출입요청을 하고 정보보안담당자 또는 담당 교직원의 동행 하에 출입기록을 유지하고, 관리하여야 한다.
③ 정보통신실 운용에 관한 세부사항은「물리적보안관리지침」으로 따로 정한다.

제26조(전산장비의 보안대책)
① 분야별보안담당관은 환경상의 위협을 최소화할 수 있도록 전산장비를 배치하고 비 인가자의 침해를 방지할 수 있는 적절한 대책을 수립·운영한다.
② 전산장비의 유지보수 내역과 의심되는 결함은 부서별보안담당관이 기록·관리하며, 그 내용을 주기적으로 검토하여야 한다.
③ 정보시스템의 사용자가 변경된 경우, 비밀처리용 정보시스템은 완전포맷 3회 이상, 그 외의 정보시스템은 완전포맷 1회 이상 저장 자료를 삭제하여야 한다.
④ 전산장비의 보안 및 저장매체의 불용처리에 관한 세부사항은「물리적보안관리지침」으로 따로 정한다.

제2절 사무실 보안관리

제27조(PC등 단말기 보안관리)
① 본 대학 내에서 사용하는 전체 PC·노트북·PDA·스마트폰 (이하 PC 등) 단말기에 대한 1차적인 보안책임은 단말기 사용자 개인에게 있다.
② 부서별보안담당관은 비인가자가 PC를 무단으로 조작하여 전산자료를 유출, 위·변조 및 훼손시키지 못하도록 백신 및 PC용 침입차단시스템 등의 보호대책을 강구하여야 한다.
③ PC를 폐기 또는 외부로 반출하는 경우는 별지 제2호 서식 '데이터 삭제·폐기 확인서'를 제출하여야 한다.
④ PC 보안관리에 관한 세부사항은「물리적보안관리지침」,「PC보안관리지침」으로 따로 정한다.

제28조(프린터 및 복사기 관리)
① 부서별보안담당관은 프린터로 출력 시 중요 정보(개인정보 포함)가 포함된 문서는 출력한 자를 알 수 있도록 출력물에 워터마킹(로고, IP주소 등)이 표시되도록 하여야 하며, 프린터 주위에 출력물이 방치되지 않도록 관리하여야 한다.
② 문서 생산자가 직접 복사하는 것을 원칙으로 하며 원본 문서는 즉시 회수하도록

한다.
③ 출력 및 복사 시 잘못 인쇄된 용지는 파쇄기를 이용하여 파쇄 하는 것을 원칙으로 하며, 비공개 이상의 정보가 포함된 경우는 이면지로 활용되지 않도록 하여야 한다.

제9장 정보통신 보안
제1절 시스템 보안

제29조(서버보안 등 정보시스템 운용)
① 정보보안담당관은 서버를 도입·운용 할 경우 보안대책을 수립·시행하여야 하며, 비인가자에게 불필요한 서비스를 허용하지 않도록 보안기능을 설정하여야 한다.
② 정보보안담당관은 정보시스템을 안정적으로 운영하기 위한 운영계획을 수립하고, 운영에 필요한 구성 및 변경관리, 성능관리, 장애관리 등의 체계적인 기준 및 대책을 마련하여야 한다.
③ 정보보안담당관은 각종 정보시스템의 보유 자료에 대해 업무별, 자료별 중요도에 따라 사용자의 접근권한을 차등 부여하여야 한다.
④ 사용자별 자료 접근범위는 정보시스템에 등록하여 인가된 권한범위 이외의 자료 접근은 통제하여야 한다.
⑤ 기타 관련된 세부사항은 「서버보안관리지침」,「응용프로그램보안관리지침」으로 따로 정한다.

제30조(데이터베이스 접근 관리)
① 본 대학에서 운영되는 데이터베이스에는 다음 각 호의 접근통제가 적용되어야 한다.
1. 데이터베이스관리자(DBA) 및 사용자 인증 강화
2. 뷰, 레코드 또는 필드 수준의 사용자 접근통제
3. 데이터사전 및 유틸리티에 대한 접근통제
② 서버보안관리자는 데이터베이스에 대하여 사용자의 직접적인 접속을 차단하고, 중요 개인정보를 암호화하는 등 데이터베이스 별 보안조치를 강구하여야 한다.
③ 기타 보안조치에 관한 세부사항은「서버보안관리지침」으로 따로 정한다.

제31조(접근기록 관리)
① 정보보안담당관은 정보시스템의 효율적인 통제 및 보안사고 발생 시 추적 등을 위하여 사용자의 정보시스템 접근기록을 유지·관리하여야 한다.
② 접근기록은 정보보안 사고 발생 시 확인 등을 위하여 최소 6개월 이상 보관하여야 하며, 접근기록 위·변조 및 외부유출 방지 대책을 강구하여야 한다
③ 기타 접근기록 관리 등에 관한 세부사항은「서버보안관리지침」으로 따로 정한다.

제32조(보안시스템 운용)
① 정보보안담당관은 내부 정보통신망을 인터넷 등 외부망과 접속할 때에는 내부망

을 보호하기 위하여 보안시스템 도입, 보안시스템 이중화 등 보안 대책을 강구하여야 한다.
② 정보보안담당관은 보안시스템에 대하여 보안기능을 설정하여 주기적인 점검 및 관리를 하여야 한다.
③ 기타 보안시스템에 관한 세부사항은「보안시스템관리지침」으로 따로 정한다.

제33조(사용자계정 관리)
① 사용자계정은 비인가자 도용 및 정보시스템 불법접속에 대비하여 주기적인 점검을 하야 한다.
② 정보보안담당관은 퇴직 또는 보직변경 등으로 사용하지 않는 사용자 계정이 발생할 경우 신속히 권한을 변경하여야 한다.
③ 사용자계정에 관한 세부사항은「응용프로그램보안관리지침」으로 따로 정한다.

제34조(비밀번호 관리)
① 사용자는 비밀번호 설정 사용 시 정보시스템의 무단사용 방지를 위하여 다음과 같이 구분하여야 한다.
② 비밀이나 중요자료에는 자료별 비밀번호를 반드시 부여하되 공개 또는 열람 자료에 대해서는 부여하지 아니할 수 있다.
③ 비밀번호 관리를 위한 세부사항은「응용프로그램보안관리지침」으로 따로 정한다.

제35조(홈페이지등 공개용 웹서버 관리)
① 정보보안담당관은 외부인에게 공개할 목적을 설치되는 웹서버 등 각종 공개서버에 대하여 내부망과 분리하여 운영하고 보안적합성이 검증된 침입차단·탐지시스템을 설치하는 등 보안대책을 강구하여야 한다.
② 웹서버에 접근할 수 있는 사용자 계정은 사전 신청 후 승인 받아야 접근할 수 있으며, 불필요한 계정은 주기적으로 삭제하여야 한다.
③ 공개용 웹서버는 내부사용자의 네트워크와 구별된 별도의 네트워크 및 보안구역(DMZ)을 지정하여 설치하며 내부망의 정보자산을 보호하여야 한다.
④ 홈페이지 내용이 불법 변조, 삭제되지 않도록 주기적으로 웹서버의 보안점검을 실시하여야 한다.
⑤ 기타 세부사항은「응용프로그램보안관리지침」,「서버보안관리지침」,「보안시스템관리지침」등 관계 지침으로 따로 정한다.

제2절 정보통신망 보안

제36조(정보통신망 관리)
① 정보통신망에 연결 된 장비가 정보보안담당관의 승인을 얻지 아니하고 사용될 경우 정보통신망 보호를 위하여 그 장비의 정보통신망 사용을 엄격히 제한하여 통제하여야 한다.
② 정보보안담당관은 네트워크 접근통제 규칙을 수립·운영하여야 하며 변경 전·후의

내용을 확인할 수 있도록 한다.
③ 기타 세부사항은「네트워크보안관리지침」으로 따로 정한다.

제37조(전자메일 보안관리)
① 전자메일 사용자는 보안조치 없이 전자메일을 이용한 비밀 및 중요자료 전송을 금지하고 출처가 불분명한 전자메일의 경우 열람하지 말고 삭제한다.
② 본 대학에 상주 또는 비상주 외부직원의 경우 전자메일 계정은 발급하지 않는 것을 원칙으로 한다.
③ 전자메일에 첨부된 파일은 웜·바이러스 검사를 실시하여 이상 유무를 확인한 뒤 열람토록 한다.

제38조(악성코드 방지대책)
① 정보보안담당관은 웜·바이러스, 해킹프로그램, 스파이웨어 등 악성코드 감염을 방지하고 정보시스템을 운영·관리를 위하여 주기적인 모니터링 및 백신 소프트웨어의 업데이트를 실시하여야 한다.
② 바이러스 관리 등에 관한 세부사항은 「서버보안관리지침」,「PC보안관리지침」으로 따로 정한다.

제39조(인터넷 접속관리)
① 정보보안담당관은 인터넷에 접속하고자 할 경우에는 비인가자의 무단침입을 방지하기 위하여 보안시스템 설치 운용 등의 보안대책을 강구하여야 한다.
② 인터넷 등의 접속은 해킹 등 불법침해를 방지하고, 외부인으로부터의 인터넷 접속시 효율적인 보안관리를 위하여 보안시스템을 운용하여 임의 접속을 차단하여야 한다.

제40조(휴대용저장매체 보안)
① 부서별보안담당관은 휴대용 저장매체를 사용하여 업무자료를 보관할 필요가 있을 때에는 위·변조, 훼손, 분실 등에 대비한 보안대책을 강구하여야 한다.
② 부서별보안담당관은 비밀용 휴대용 저장매체에 대해서 주기적으로 보관 상태를 점검하며 반출·입을 통제하여야 한다.
③ 비밀용 휴대용 저장매체를 파기 등 불용처리 할 경우 저장되어 있는 정보의 복구가 불가능하도록 조치하여야 한다.

제41조(무선랜 보안관리)
① 정보보안담당관은 무선랜 보안대책을 적용하고 수시로 점검하여야 한다.
② 교내에서 무선 중계기(AP)의 불법적인 설치 및 사용은 원칙적으로 금지한다. 다만, 대학에서 제공하는 무선 서비스가 음영지역인 경우에는 예외로 한다.
③ 무선랜의 안전한 관리를 위한 보안대책에 관한 세부사항은「네트워크보안관리지침」으로 따로 정한다.

제42조(RFID 보안관리)

RFID 보안대책 수립 시 다음 각 호의 사항을 포함하여야 한다.

1. RFID 시스템의 분실·탈취 대비 보안대책 및 백업대책
2. 태그 정보의 최소화 대책
3. 장치 인증, 사용자 인증 및 기밀 등 중요 정보의 암호화 대책

제43조(CCTV운용 보안관리)

① 최고보안담당관은 CCTV운용에 필요한 카메라 중계・관제서버, 관리용 PC 등 관련 시스템을 비인가자의 임의 조작이 물리적으로 불가능하도록 설치하여야 한다.

② CCTV 상황실은 통제구역으로 지정·관리하고, 출입통제 장치를 도입하여야 한다.

③ 최고보안담당관은 CCTV 카메라, 비디오서버, 관제서버 및 관련 전산망 설치 시 업무망 및 인터넷망과 분리 운영하는 것을 원칙으로 한다. 다만, 부득이하게 인터넷망을 이용할 경우에는 전송 내용을 암호화하여야 한다.

④ CCTV 시스템 일체는 사용자 계정·비밀번호 등 시스템 인증 대책을 강구하고 허용된 특정 IP 주소에서만 접속 허용하는 등 비인가자의 침입통제 대책을 강구하여야 한다.

⑤ 최고보안담당관은 제1항부터 제3항까지와 관련하여 보안대책의 적절성을 수시로 점검하고 보완하여야 한다.

⑥ CCTV 시스템의 보안관리에 관한 세부사항은「CCTV설치및운영규칙」으로 따로 정한다.

제3절 응용프로그램 개발 및 유지보수

제44조(응용프로그램 개발 보안)

① 정보보안담당관은 응용프로그램 개발 시 데이터 입·출력의 적합성 여부 등 보안 요건을 확인하여야 한다.

② 정보보안담당관은 응용프로그램 개발 및 유지보수 시 처리되는 데이터의 기밀성, 무결성 및 가용성을 보장하기 위하여 보안대책을 강구하여야 한다.

③ 응용프로그램 개발, 테스트, 유지보수 등의 세부 사항은「응용프로그램보안관리지침」으로 따로 정한다.

제45조(정보시스템 유지보수)

① 정보시스템 유지보수와 관련한 절차, 주기, 문서화 등에 관한 사항은 다음 각 호와 같다.

1. 유지보수 인력에 대해 보안서약서 집행, 보안교육 등을 포함한 유지보수 인가 절차에 따라 인가된 유지보수 인력만 유지보수에 참여하여야 한다.
2. 결함이 의심되거나 발생한 결함, 예방 및 유지보수에 대한 기록은 보관·관리하여야 한다.
3. 유지보수를 위해 현재 설치장소에서 다른 장소로 정보시스템을 이동할 경우 통제수단을 강구하여야 한다.

4. 서버를 폐기 또는 외부로 반출하는 경우는 별지 제2호 서식 '데이터 삭제·폐기 확인서'를 제출하여야 한다.
② 정보보안담당관은 정보시스템의 변경이 발생할 경우 정보시스템의 설계·코딩·테스트·구현 과정에서의 보안대책을 강구하여야 하며, 이를 주기적으로 확인하여야 한다.
③ 대학 외부에서 원격접속을 통한 정보시스템 유지보수는 원칙적으로 금지하며, 부득이한 경우 보안대책을 강구한 후 정보보안담당관의 승인을 득하여 수행할 수 있다.
④ 정보시스템의 응용프로그램 및 서버 등에 대한 유지보수에 관한 세부 사항은「인적보안관리지침」,「응용프로그램보안관리지침」,「서버보안관리지침」등 관계 지침으로 따로 정한다.

제10장 보안사고 대응 및 비상계획 관리

제46조(보안사고)
① 보안사고의 범위는 비밀의 누설 또는 분실, 중요시설 및 장비의 파괴, 보호구역에 대한 불법침입 등이며, 다음 각 호와 같다.
1. 종합정보지원실 및 각 건물의 장비·통신실 파괴, 정보통신망의 해킹
2. 악성 바이러스 유포 또는 비밀번호 파일 유출
3. 응용프로그램 불법복제·복사
4. 중요 정보의 유출·파괴·변조, 보안시스템의 손괴 등
② 보안사고가 발생하였을 때 사고를 범하였거나 이를 인지한 자는 즉시 최고보안담당관 및 부서별보안담당관에게 보고하여야 한다.

제47조(보안사고 대응)
① 최고보안담당관은 보안사고가 발생했을 때 이에 대한 효율적인 처리 및 복구대응체계를 갖추고 그 피해를 최소화하기 위해「보안사고대응관리지침」에 따라 사고대응을 시행하고, 이행실태를 지속적으로 확인·점검하여야 한다.
② 정보보안담당관은 사고조사를 실시하고 동일유형의 사고가 발생하지 않도록 제반 보안조치를 취한다.
③ 기타 보안사고 대응을 위한 세부사항은「보안사고대응관리지침」으로 따로 정한다.

제48조(비상계획 관리)
① 최고보안담당관은 인위적, 자연적으로 발생될 수 있는 시스템 장애, 가동중지 등 비상사태에 대비하여 비상계획 대책 등을 수립·시행하여야 하는 사항은 다음 각 호와 같다.
1. 비상사태에 대비한 조직, 임무 및 업무처리 지침
2. 백업시설 구성, 백업방법, 정상상태로의 복구 내용
3. 비상사태에 대비한 정기적인 훈련과 교육 실시 등
② 최고보안담당관은 정보통신망 장애에 대비한 백업대책을 수립, 적용하고 정기적으로 이를 수행하여야 한다.

제49조(사이버·보안 진단의 날 실시)

① 최고보안담당관은 '사이버·보안 진단의 날'을 지정하여 자체점검을 통한 보안진단을 실시하여야 한다.

② 제1항의 규정에 의한 보안진단은 정보보안담당관이 지휘하고, 일반보안진단은 보안담당관의 책임 하에 실시하여야 한다.

③ 사이버·보안 진단의 날은 매월 세 번째 수요일(다만, 공휴일 또는 불가능할 때는 익일)에 실시하여야 하며, 별지 제3호 서식 '사이버보안 진단일지'에 의거 기록·유지하여야 한다.

④ 진단결과 발견된 문제점에 대하여는 정보보안위원회에 상정하여 대책을 수립 이행하여야 하며, 시행 및 확인·감독에 관한 사항은 서면으로 작성, 보존하여야 한다.

제50조(정보보안 수준진단)

① 정보보안담당관은 정보통신망 보호를 위하여 정보보안관리 체계 및 침해예방활동 등을 진단하여야 한다.

② 수준진단은 교육부 정보보안기본지침 제10조 ①항의 내용에 준하여 실시하도록 한다.

③ 진단결과에서 발견된 문제점은 정보보안위원회에 상정하여 대책을 수립하고, 취약점은 개선·보완하여 정보보안 수준을 제고하여야 한다.

부 칙

(1) (시행일) 이 규칙은 2013년 3월 1일부터 시행한다.

(2) (시행일) 이 규칙은 2016년 7월 1일부터 시행한다.

[별지 제1호 서식] 전산장비 설치·폐기 요청서

전산장비 설치·폐기 요청서

<table>
<tr><td>용도 구분</td><td colspan="2">☐설치 ☐폐기 ☐증설</td><td>신청부서</td><td></td></tr>
<tr><td>요청사유</td><td colspan="4"></td></tr>
<tr><td rowspan="2">사양</td><td>제조사/모델명</td><td colspan="2">설치OS</td><td>비고</td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><td rowspan="2">(설치/폐기)
정보</td><td>(설치/폐기)장소</td><td colspan="2">수량</td><td>비고</td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><td>작업 내용</td><td colspan="4"></td></tr>
<tr><td>폐기 시
처리방안</td><td colspan="4">디스크 데이터 삭제여부, 설정정보 삭제여부

별지 제2호 서식 ‘데이터 삭제·폐기 확인서’ 첨부</td></tr>
</table>

「정보보안규칙」에 따라 위와 같이 전산 장비를 (설치/폐기) 하고자 하오니 검토 후 처리하여 주시기 바랍니다.

신청 부서 결재	
직위	서명

[별지 제2호 서식] 데이터 삭제·폐기 확인서

데이터 삭제·폐기 확인서

신청 구분	□ 삭제 □ 폐기		신청부서/성명		
신 청 일			완료 요청일		
전화번호 (휴대폰)			이메일 주소		
삭제 대상	구분	제조사/모델명	매체유형	수량	OS
	□PC □서버				
	□PC □서버				
사용 기간	20 . . . ~ 20 . . .				
삭제 정보	삭제 장소		삭제 방법	처리 일자	
삭제 처리자	소 속		성 명	서 명	
작업 내용 (폐기 방법)	관련 사진 첨부				

「정보보안규칙」에 따라 위와 같이 요청하오니 재가하여 주시기 바랍니다.

처리 부서 결재	
직위	서명

신청 부서 결재	
직위	서명

[별지 제3호 서식] 사이버보안 진단일지

사이버보안 진단일지

20 . . .

실 태 점 검 항 목		점 검 결과
개인정보	정보보안(개인정보보호) 교육 실시	실시여부 : 교육방법 : 예)집합, 유인물, 방송 등
	홈페이지 개인정보 노출여부 점검	노출건수 : 건
PC 진단 실시	자체 보유중인 PC는 모두 몇 대입니까?	전체 PC : 대
	내PC지키미를 실행한 PC는 몇 대입니까?	실행 PC : 대
	P2P, 증권, 게임사이트 이용 여부 점검	
	PC별 비밀번호 설정 및 화면보호기 설정 여부	설정 PC : 대
	PC별 개인정보 보유여부 및 암호화 저장 여부 점검	설정 PC : 대
저장매체 불용처리	외부업체에 삭제·파기 의뢰 시 부서별보안담당관 입회하 실시	
	시스템 불용처리 시 저장자료 삭제여부 최종 확인	
	창고 등에 저장자료를 삭제하지 않은 불용시스템을 방치하고 있는가?	
	수리의뢰 시 참여자에 대해 보안서약서 집행・교육 등을 수행하는가?	

[별지 제4호 서식] 정보자산목록(표)

정보자산목록(표)

순번	자산 번호	자산 유형	자산명 (시스템명)	모델명	용도	구성정보		응용 프로그램	소유 형태			관리형태			설치위치			취득 일자	자산변경내역	사용자		자산 중요도 평가					
						OS	IP주소		구분	부서	소유자명	구분	부서	관리자명	건물명	설치위치(층, 호)	장소 이름			부서명	사용자명	기밀성	무결성	가용성	합계	평균	등급
1																											
2																											
3																											
4																											
5																											
6																											
7																											
8																											
9																											