	정보보안 규정	문서번호	MSU-
		제정일자	2014. 4. 21.
		최종개정일자	
		담당부서	교무입학처 정보관리소

제1장 총 칙

제1조(목적) 이 규정은 목포과학대학교(이하 "대학"이라 한다) 정보보안업무에 관하여 필요한 사항을 규정함을 목적으로 한다.

제2조(적용대상 및 범위) 이 규정은 대학의 행정부처와 각 학과, 부속기관, 부설기관 및 산하기관(이하 "당해기관" 이라 한다)에 적용한다.

제3조(정보보안담당관의 지정 및 업무) ①총장은 대학의 정보보안 관리를 위해 정보보안 담당관을 임명하여야 하며, 정보화 총괄부서의 장으로 임명한다.

②정보보안담당관의 임무는 다음과 같다.

1. 정보통신보안대책의 수립
2. 정보관리소 또는 전산망 및 전산자료 등의 보안 유지 관리
3. 정보보안업무 지도, 감독 및 교육
4. 전산보안시스템의 운용 관리
5. 자체 정보보안 감사계획 수립
6. 정보보호 업무추진 및 강화를 위한 중장기 계획 및 당해 연도추진 계획 수립
7. 기타 정보보안업무 관련 사항

제2장 보안심사위원회

제4조(보안심사위원회 구성) 보안심사위원회(이하 "위원회"라 한다.) 구성은 다음 각 호와 같다.

①대학은 보안업무의 효율적인 운영과 업무계획의 수립 및 기타 보안에 관한 중요한 사항을 심의, 결정하기 위하여 위원회를 둔다.

②위원회는 총장이 임명하는 위원장과 7인 이내의 위원으로 구성하며, 개인정보보호책임자, 학사지원처장, 산학취업처장, 기획처장은 당연직으로 한다.

제5조(보안심사위원회 기능) 위원회는 다음 각 호의 사항을 심의 · 의결한다.

1. 정보보안내규의 제정 및 개정에 관한 사항
2. 분야별 정보보안대책 수립에 관한 사항
3. 전산망 신·증설계획 및 전산화 용역개발 사업에 관한 사항
4. 정보보안업무 심사분석 및 보안업무 수행 상 조정과 협의를 요하는 사항
5. 각 당해 기관의 장이 요구하는 사항
6. 기타 위원장 및 정보보안담당관이 필요하다고 인정하는 사항

제6조(임기) 위원의 임기는 2년으로 한다. 단, 당연직 위원의 경우 보직 재임기간으로 한다.

제7조(간사) 위원회의 간사는 정보보안담당자가 된다.

제8조(보안심사위원회 회의) ①위원회는 위원장이 필요하다고 인정할 때 또는 재적위원 과반수의 요구가 있을 때에 위원장이 소집한다.

②위원회는 재적위원 과반수의 출석으로 개회하고, 출석위원 과반수의 찬성으로 의결한다.

제9조(회의록) 위원회는 회의록을 작성하여야 하며, 위원회에서 심의된 사항은 총장에게 보고 하여야 한다.

제3장 정보보안 운영 관리

제10조(사이버 · 보안 진단의 날 실시) ①정보보안담당관은 〃 사이버 · 보안 진단의 날〃 을 실시하여 자체점검을 통한 보안진단을 실시하여야 한다.

②사이버 · 보안 진단의 날은 매월 세 번째 수요일로서 다음 각 호의 사항을 실시하여야 하며,(다만, 진단의 날이 공휴일인 경우나 불가능할 때에는 익일에 실시한다.)그 내용을 기록 · 유지 · 관리하여야 한다.

1. 진단프로그램을 활용한 PC보안 진단
2. 최신 백신프로그램 · 보안패치 설치 및 업데이트 여부
3. 통제구역 출입통제 강화
4. 분야별, 요소별 정보보안관리 실태 진단
5. 정보보안 직무교육 실시

제11조(보안교육) ①정보보안담당관은 정보관련 직원에 대해 충분한 보안교육과 보안조치를 실시하여야 하며, 당해 기관의 보안관리와 보안업무의 향상을 위하여 전 직원에 대하여 연 2회 이상 교육을 실시하여야 한다.

②정보보안담당관은 당해 기관 구성원들의 정보보호 인식 제고를 위해 정보보호 관련 정보, 규정, 실천 수칙 등 정보보호 관련 정보를 정기적으로 공지하는 홍보활동을 하여야 한다.

③정보보안담당관은 정보보호 담당자의 기술고도화를 위하여 연2회 이상 교육을 실시하여야 한다.

제12조(정보보안기본지침) ①정보보안담당관은 정보보안 업무수행을 위하여 이 규정 및 상위 규정에 반하지 아니하는 범위 내에서 자체적으로 정보보안기본지침(이하 "기본지침"이라 한다.)을 정할 수 있다.

제13조(침해사고 대응관리) ①정보보안담당관은 긴급한 침해사고가 발생하였을 때에는 모든 이용자에게 대응책을 신속하게 알릴 수 있는 체계를 마련하여야 한다.

②정보보안담당관은 불법행위나 이상 징후가 탐지되었을 때에는 수립된 대응 · 복구계획에 따라 즉각적인 대응조치를 취하고, 침해사고와 관련한 접속기록 등 적절한 증거자료를 수집 · 보관하여야 한다.

제14조(인적보안) ①정보보안담당관은 교원 및 직원의 신규 채용 시 보안교육을 실시하고, 보안서약서를 받아야 한다.

②정보보안담당관은 교원 및 직원의 전보 또는 퇴직 발생 시 이들에 대한 계정 및 공용 계정에 대한 접근 권한을 즉시 해제하여야 한다.

③정보보안담당관은 외부 위탁으로 인한 제3자의 인력 활용 시 정보보호 서약서를 당해기관에서 수령하여 보관하도록 한다.

④정보보안담당관은 정보통신설비 및 시설의 관리 운영을 외부 위탁 시 계약서에 정보보안 관련 사항(보안사고 책임범위, 비밀준수 의무, 위탁업무 중단 시 비상 대책)을 반영하여야 한다.

제15조(정보관리소 운영관리) 정보보안담당관은 다음 각 호와 같이 전산실을 운영·관리하여야 한다.

1. 정보관리소에 위치한 장비에 대한 도난, 파손, 변경, 불법적인 사용 등의 방지 대책 수립
2. 정전 등으로 인해 중요 데이터의 손상 및 손실을 방지하기 위하여 데이터 백업 등 필요한 대책 수립
3. 정보관리소의 출입을 통제하는 장치를 설치하여 출입자 통제

제16조(정보보호시스템 등의 운영관리) ①정보보안담당관은 다음 각 호와 같이 정보통신서비스의 안정성과 정보의 신뢰성 확보를 위한 관리적·기술적·물리적 수단을 갖추고 이를 운영, 관리하여야 한다.

1. 침입차단시스템 등의 정보보호시스템을 설치하여 운영하거나 이에 상응하는 정보보호 조치 수립
2. 방화벽의 접근제어기능 또는 접근제어시스템 설치 등을 이용하여 외부 접근에 대한 시스템 보호조치 수립

②정보보안담당관은 프로그램의 보안취약점을 발견한 때에는 필요한 조치를 하여야 한다.

③주요 정보시스템 및 서비스와 같은 정보자산에 대한 백업 및 복구 절차를 갖추어야 한다.

제17조(이용자 제한조치 및 고지) ①정보보안담당관은 다음 각 호에 해당하는 행위를 한 이용자에 대하여 계정정지, 접속제한 등 정보통신서비스를 제한 할 수 있다.

1. 부당한 방법으로 정보통신망에 의하여 처리·보관·전송되는 타인의 정보를 훼손 또는 타인의 비밀을 침해·도용 누설하는 행위
2. 트로이목마, 컴퓨터바이러스 등 악성 프로그램 유포행위
3. 음란·폭력물 등의 불건전한 자료의 게재·유포행위
4. 정보시스템에 장애를 유발시킬 목적으로 다량의 데이터 또는 트래픽을 유발·전송하는 행위
5. 수신자의 명시적인 수신거부 의사에 반하는 광고성 전자우편·SMS를 전송하는 행위
6. 기타 정보보호에 해가 되는 행위

②정보보안담당관은 제1항에 의한 제한을 하고자 하는 경우에는 사전에 이를 이용자에게 고지하거나 학내 정보망에 게시하여야 한다.

③정보보안담당관은 제1항에 해당하는 행위가 발생하였을 때에는 그 사실을 이용자에게 고지하여야 한다. 다만, 이용자에게 경미한 영향을 미치거나 신속히 처리

해야 하는 등의 긴급한 상황일 경우에는 고지하지 아니할 수 있다.

제18조(이용자 제재) ①제17조에 규정된 사항에 해당할 경우에는 사용자의 계정을 정지·삭제하여 정보시스템 및 네트워크 사용을 제한 또는 금지하며, 그에 따른 구체적 제재 사항은 위원회에서 심의 · 의결한다.

②정보시스템의 불법사용으로 대학에 해를 끼치거나 명예를 훼손시켰을 경우에는 다음 각 호의 제재 조치를 취할 수 있다.

1. 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 의한 법적 조치
2. 정보시스템의 손해발생에 대한 손해배상 청구

제19조(계정관리) ①정보보안담당관은 이용자의 패스워드 누출 방지를 위한 보호조치를 하여야 한다.

②이용자는 자신의 계정 및 패스워드가 외부로 노출되지 않도록 유의하고 주기적으로 이를 변경하여야 한다.

③주요 정보시스템 및 서비스 대상의 사용자 계정 정보를 관리, 발급, 변경, 삭제 등을 하기 위한 처리절차를 밟아야 한다.

제20조(정보시스템 기본 보안 사항) ①이용자는 발송자를 확인할 수 없는 전자우편 또는 제공자가 불확실한 컴퓨터 프로그램 등에 대해 안정성 여부를 확인하고 실행하여야 한다.

②이용자는 자신의 컴퓨터에 최신의 컴퓨터 바이러스 방지 프로그램을 설치하여 침투여부를 수시로 점검하고, 침투한 경우에는 이를 제거·복구하여야 한다.

③이용자는 자신의 컴퓨터의 운영체계와 응용프로그램에 대해 주기적인 업데이트를 실행하며, 필요한 보안조치를 반드시 적용하여야 한다.

제21조(정보보안 실무담당자) ①정보보안담당관은 대학의 정보보호를 효과적으로 운영하기 위하여 당해 기관에 정보보안실무담당자(이하"실무담당자"하 한다) 1인을 둔다.

②실무담당자는 조교, 직원이어야 한다.

③실무담당자는 정보보안업무 관련 시행 사항에 대해 당해 기관 구성원에게 업무내용을 전파하여야 한다.

④실무담당자는 사이버보안 진단의 날 시행 시 소속한 당해 기관이 적극적으로 참여할 수 있도록 협조 및 시행 결과를 정보보안담당관에게 보고 하여야 한다.

⑤정보보안 관련 특이사항 발생 즉시 정보보안담당관에게 보고하여야 한다.

부 칙

1. (시행일) 이 규정은 2014년 4월 21일부터 시행한다.

〈별지 제1호 서식〉

정보보안업무 세부 추진계획

1. 활동 목표

2. 기본 방침

3. 세부 추진계획

분야별	사업명	세부 추진계획	주관・관련부서	비고

※ 보안성 검토 대상여부 표기

4. 전년도 보안감사・지도방문 시 도출내용과 조치내역

도출내용	조치내역	담당부서

※ 형식위주의 계획수립을 지양하고 소속 및 산하기관의 추진계획을 종합, 자체 실정에 맞게 작성

〈별지 제2호 서식〉

정보보안업무 심사분석

1. 총 평

2. 주요 성과 및 추진사항

3. 세부 사업별 실적 분석

추진계획	추진실적	문제점	개선대책

※ 추진실적은 목표량과 대비하여 성과달성도를 계량화

4. 부진(미진)사업

부진사업	원인 및 이유	익년도 추진계획

5. 애로 및 건의사항

6. 첨부(정보통신망 및 정보보호시스템 운용현황 등)

〈별지 제3호 서식〉

보안 서약서

본인은 ____년 __월 __일부로 _____관련 용역사업(업무)을/를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 _____관련 업무 중 알게 될 일체의 내용이 직무상 기밀 사항임을 인정한다.

2. 본인은 이 기밀을 누설함이 국가안전이나 대학의 이익에 위해가 될 수 있음을 인식하여 업무 수행 중 취득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.

3. 본인이 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다.

4. 본인은 하도급 업체를 통한 사업 수행 시 하도급업체로 인해 발생하는 위반사항에 대하여 모든 책임을 부담한다.

년 월 일

서 약 자 (업체대표)
업 체 명 :
직 위 :
성 명 : (서명)
주민등록번호 :

서약집행자 (담 당 자)
소 속 :
직 위 :
성 명 : (서명)
주민등록번호 :