정보보안 규정(3-1-16)

제1장 총 칙

제1조**(목적)** 본 규정은 건양대학교(이하 “본 대학교”라 한다) 구성원들의 정보보안을 위하여 수행하여야 할 기본활동에 관한 사항을 규정함을 목적으로 한다.

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

1. “정보보안” 또는 “정보보호”라 함은 정보시스템 및 정보통신망을 통해 수집·가공·저장·검색·송수신 되는 정보의 유출·위변 조·훼손 등을 방지하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위로서 사이버안전을 포함한다.
2. “사용자”라 함은 총장으로부터 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 자를 말한다.
3. “정보통신망”이라 함은 전기통신기본법 제2조 제2호의 규정에 의한 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송수신하는 정보통신체제를 말하며 정보시스템 일체를 포함한다.
4. “정보시스템”이라 함은 서버·PC 등 단말기, 보조기억매체, 네트워크 장치, 응용 프로그램 등 정보의 수집·가공·저장·검색·송수신에 필요한 하드웨어 및 소프트웨어를 말한다.
5. “휴대용 저장매체”라 함은 디스켓·CD·외장형 하드디스크·USB 메모리 등 정보를 저장할 수 있는 것으로 PC 등의 정보시스템과 분리할 수 있는 기억장치를 말한다.
6. “전자문서”라 함은 컴퓨터 등 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 정보를 말한다.
7. “전자기록물”이라 함은 정보처리능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 기록정보자료를 말한다.
8. “전자정보”라 함은 각급기관이 업무와 관련하여 취급하는 전자문서 및 전자기록물을 말한다.
9. “정보통신실”이라 함은 서버·PC 등과 스위치·교환기·라우터 등 네트워크 장치 등이 설치 운용되는 장소를 말하며, 전산실·통신실·전자문서 및 전자기록물(전자정보) 보관실 등을 말한다.

10. “안전측정”이라 함은 정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 해킹·컴퓨터바이러스·서비스방해·도청 등으로부터 정보통신망과 정보를 보호하기 위하여 정보보안 취약점을 진단하는 제반활동을 말하며, 대도청(對盜聽)측정 활동을 포함한다.
11. “암호장비”라 함은 정보통신망으로 처리·저장·송수신되는 정보를 보호할 목적으로 암호논리를 내장하여 제작된 장비를 말한다.
12. “정보보호시스템”이라 함은 정보의 수집·저장·검색·송신·수신 시 정보의 유출, 위·변조, 훼손 등을 방지하기 위한 하드웨어 및 소프트웨어를 말한다.
13. “사이버공격”이라 함은 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스방해 등 전자적 수단에 의하여 정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 공격 행위를 말한다.
14. “인터넷PC”라 함은 인터넷망에 접속이 가능한 PC를 말한다.
15. “업무PC”라 함은 업무·인터넷망이 분리된 기관에서 내부 업무망 접속을 위해 사용하는 PC를 말한다.
16. “IP(Internet Porotocol)주소”라 함은 정보통신망으로 서버와 클라이언트간 연결을 가능하게 하기 위하여 부여되는 주소체계를 말한다.
17. “이용자계정(ID)”이라 함은 이용자의 식별과 자료이용을 위하여 이용자가 생성한 영문자와 숫자가 조합된 고유계정을 말한다.

제2장 정보보안 기본활동

제3조**(책무)** 정보통신원장은 국가안보 및 국가이익 관련 정보(전자정보를 포함한다. 이하 같다)와 정보통신망을 보호하기 위한 보안대책을 마련하여야 하며 정보보안에 대한 책임을 진다.

제4조**(정보보안담당관 운영)** ① 정보통신원장은 효율적인 정보보안업무를 수행하기 위하여 '정보보안담당관'을 임명 운영하여야 하며, 부서의 원활한 정보보안업무 수행을 위하여 필요한 경우 과·팀 단위 부서에 '부서 정보보안담당관'을 임명 운영할 수 있다.

② 정보보안담당관을 임명한 경우에는 7일 이내에 소속·직책·직급·성명·연락처(전자우편 주소 포함) 등을 교육부장관에게 통보하여야 한다.

③ 정보보안담당관은 그 기관의 본부 및 소속·산하 공공기관에 대한 정보보안

업무를 총괄한다.

제5조**(활동방향)** ① 정보보안담당관은 정보보안을 위하여 다음 각 호의 기본활동을 수행하여야 한다.

1. 정보보안 정책 및 기본계획 수립・시행
2. 정보보안 관련규정・지침 등 제・개정
3. 보안심사위원회에 정보보안 분야 안건 심의 주관
4. 정보통신원 보안업무 지도·감독, 정보보안 감사 및 심사분석
5. 정보통신실, 정보통신망 및 정보자료 등의 보안관리
6. 정보보안 관리실태 평가
7. 사이버공격 초동조치 및 대응
8. 사이버위협정보 수집·분석 및 보안관제
9. 정보보안 예산 및 전문인력 확보
10. 정보보안 사고조사 결과 처리
11. 정보보안 교육 및 정보협력
12. 도청 위해 요소 측정·제거
13. 주요 정보 통신기반 시설 보호활동
14. 정보통신망 보안대책의 수립·시행
15. '사이버보안진단의 날' 계획 수립·시행
16. 정보보안 위규 적발 강화 및 사고조사 처리
17. 정보보안 감사・지도점검 실시
18. 그 밖에 정보보안 관련 사항

② 정보보안담당관은 제1항에 따라 부서 / 학부에 대한 정보보안 감사・지도점검을 실시할 경우에는 "정보보안점검 체크리스트"(별지 제1호) 등을 적극 활용한다.

제6조**(활동계획 수립 및 심사분석)** ① 정보보안담당관은 제5조에 따라 당해 대학 정보보안업무 세부 추진계획을 수립・시행하고 그 추진결과를 심사분석 및 평가하여야 한다.

② 정보보안담당관은 세부 추진계획 및 심사분석을 별지 제3호 및 제4호 서식에 따라 다음 각 호의 기한 내에 작성하여 별도 보관하고 증빙자료서 요청시 제출한다.

1. 정보보안업무 추진계획 : 매년 2월 28일 까지
2. 정보보안업무 심사분석 : 매년 2월 28일 까지(전년도 1/4분기~4/4분기)

제7조**(모의훈련)** 정보보안담당관은 자체 정보통신망을 대상으로 매년 정기 또는 수시 사이버위기 대응 모의훈련을 실시하여야 한다.

제8조**(정보보안 감사)** ① 정보보안담당관은 연 1회 이상 부서 / 학부에 대하여 정보보안감사를 실시하여야 한다.

② 정보보안담당관은 정보보안감사 실시계획과 감사결과를 작성하여 별도 보관하고 증빙자료서 요청시 제출한다.

제9조**(정보보안 교육)** ① 정보보안담당관은 자체 정보보안 교육계획을 수립하여 아래 대상으로 하여금 관련 교육을 실시하여야 한다.

1. 대학 전 교직원 : 연 2회 이상
2. 교원 / 학생 : 연 1회 이상
3. 외부 용역업체 직원 : 상주인력(분기 1회 이상), 비상주인력(연 1회 이상)

단, 정보통신원 직원들은 연간 15시간 이상 정보보안 교육(개인정보보호법 제28조 제 2항의 교육 등 포함)을 이수하여야 한다.

② 정보보안담당관은 정보보안 교육의 효율성 제고를 위해 기관별 자체 실정에 맞는 정보보안 교안을 작성 활용하여야 한다.

③ 정보보안 담당자는 업무 전문성을 제고하기 위하여 정보보안 관련 전문기관 교육 및 기술 세미나 참석을 필하여야 한다.

제10조**(사이버보안 진단의 날)** ① 본 대학교는 매월 세 번째 수요일을 '사이버보안진단의 날'로 지정·운영한다.

② 정보보안담당관은 '사이버보안진단의 날'에 소관 정보보안업무 전반에 대하여 체계적이고 종합적인 보안진단을 실시하고 악성코드 감염여부와 정보시스템의 보안 취약여부 등을 진단 및 문제점을 발굴 개선하여야 한다.

③ 본 대학교의 교직원은 '사이버보안진단의 날'에 국가정보원에서 배포한 '내PC 지키미'를 시행·조치 후 시행 보고서를 정보보안담당관에게 제출하여야 한다.

제11조**(정보보안 사고조사)** ① 정보보안담당관은 정보보안 사고가 발생한 때에는 즉시 피해확산 방지를 위한 조치를 취하고 다음 각 호의 사항을 교육부장관 에게 통보하여야 한다. 이 경우, 사고원인 규명 시까지 피해 시스템에 대한 증거를 보전하고 임의로 관련 자료를 삭제하거나 포맷하여서는 아니 된다.

1. 일시 및 장소
2. 사고 원인, 피해현황 등 개요
3. 사고자 및 관계자의 인적사항
4. 조치내용 등

② 정보보안담당관은 규정에 따른 관련자 징계, 재발방지를 위한 보안대책의 수립·시행 등 사고 조사 결과에 따라 필요한 조치를 이행하고 결과를 교육부장관에게 제출하여야 한다.

제12조**(재난방지)** ① 정보보안담당관은 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애 발생에 대비하여 정보시스템 이원화, 백업관리, 복구 등 종합적인 재난방지 대책을 수립·시행하여야 한다.

② 정보보안담당관은 재난방지대책을 정기적으로 시험하고 검토해야 하며 업무 연속성에 대한 영향평가를 실시하여야 한다.

③ 정보보안담당관은 정보시스템 장애에 대비한 백업시설을 확보하고 정기적으로 백업을 수행하여야 한다.

④ 제3항에 의거 백업시설을 설치할 경우에는 네트워크 서버실과 물리적으로 일정거리 이상 위치한 안전한 장소에 설치하여야 하며 전력공급원 분리 등 정보시스템의 가용성을 최대화 할 수 있도록 하여야 한다.

제13조**(정보통신망 현황·자료 관리)** ① 정보보안담당관은 다음 각 호에 해당하는 정보통신망 관련 현황자료를 관리하고 보안에 유의하여야 한다.

1. 정보시스템 운용현황
2. 정보통신망 구성현황
3. IP 할당현황
4. 주요 정보화사업 추진현황

② 정보보안담당관은 다음 각 호의 자료를 대외비로 분류하여 관리하여야 한다.

1. 정보통신망 세부 구성현황(IP 세부 할당현황 포함)
2. 보안취약점 분석·평가 결과물
3. 기타 보호할 필요가 있는 정보통신망 관련 자료

제14조**(표준적용)** 정보보안담당관은 정보보안 대책을 강구하는 경우 정보보안에 필요한 기술의 호환성 유지 및 안전성 확보를 위하여 국가정보원장이 제정한 「국가표준기본법」의 표준을 우선 적용하여야 한다.

제15조**(정보협력)** 정보보안담당관은 정보보안 업무의 발전을 도모하고 교직원들의 상호 교류협력을 증진하기 위하여 협의기구를 구성·운영할 수 있다.

제3장 정보시스템 보안

제16조**(정보통신시설 보안)** ① 다음 각 호의 중요 정보 통신시설 및 장소를 「보안업무규정」(대통령령) 제30조에 따른 보호구역으로 설정 관리한다.

1. 명곡정보관 305호 중앙 네트워크 서버실
2. 정보 통신지원센터 사무실
3. 각 건물 네트워크 서버실
4. 그 밖에 보안관리가 필요하다고 인정되는 정보시스템 설치 장소

② 정보보안담당관은 제1항에서 지정된 보호구역에 대한 보안대책을 강구할 경우 다음 각 호 사항을 참고하여야 한다.

1. 방재대책 및 외부로부터의 위해 방지대책
2. 상시 이용하는 출입문은 한 곳으로 정하고 이중 잠금장치 설정
3. 출입자 인증·식별 등을 위한 출입문 보안장치 설치 및 주야간 감시대책
4. 휴대용 저장매체를 보관할 수 있는 용기 비치
5. 정보시스템 안전지출 및 긴급파기 계획 수립
6. 관리책임자 및 자료·장비별 취급자 지정 운용
7. 정전에 대비한 비상전원 공급, 시스템의 안정적 중단 등 전력관리 대책
8. 비상조명 장치 등 비상탈출 대책
9. 전자파 누설 방지 대책
10. 카메라 장착 휴대폰 등을 이용한 불법 촬영 방지대책 등

제17조**(정보시스템 보안관리)** ① 정보보안담당관은 정보시스템의 효율적인 보안관리를 위하여 정보시스템별로 관리책임자(이하 '시스템관리자'라 한다)를 지정 운영하여야 한다.

② 시스템관리자는 운영되는 정보시스템이 비인가자에게 불필요한 서비스를 허용하지 않도록 보안기능을 설정하여야 하며, 보안취약점을 제공할 수 있는 다음 각 호의 프로그램의 설치를 제한하여야 한다.

1. P2P, 웹하드 등 파일 공유 프로그램
2. 상용 메신저 프로그램 등

③ 시스템관리자는 정보시스템을 도입할 경우 별지 제10호 서식의 정보시스템 관리대장에 따라 그 하드웨어 목록을 유지·관리해야 하며, 비인가자가 접근할 수 없도록 물리적인 접근통제 장치가 마련된 공간에 서버를 설치해야 한다.

④ 시스템관리자는 소관 시스템의 안정적 운영을 위해 다음 각호에 따라 관리해야 한다.

1. 신규로 설치되는 시스템의 취약점 점검 및 조치
2. 시스템의 운영체제 등 최신 패치 실행
3. 설치·운영 중인 시스템의 수시 보안취약점 점검 및 조치

⑤ 외부자가 전산실에 출입하여 서버와 관련된 작업을 할 경우 시스템관리자가 입회·감독해야 한다.

제18조**(웹서버 등 공개서버 관리)** ① 정보보안담당관은 외부인에게 공개할 목적으로 설치되는 웹서버 등 각종 공개서버는 내부망과 분리된 영역(DMZ)에서 운영하고 보안적합성이 검증된 침입차단·탐지시스템을 설치하는 등 보안대책을 강구하여야 한다.

② 정보보안담당관은 공개서버에 접근할 수 있는 사용자계정을 제한하여야 하며 불필요한 계정은 삭제하여야 한다.

③ 정보보안담당관은 공개서버에 비공개 자료 및 개인정보가 유·노출, 위·변조되지 않도록 보안조치를 하여야 한다.

④ 정보보안담당관은 공개서버의 서비스에 필요한 프로그램을 개발하고 시험하기 위해 사용된 도구(컴파일러 등)는 개발 완료 후 사용이 제한되도록 보안기능을 설정하거나 삭제하여야 한다.

⑤ 정보보안담당관은 공개서버의 보안취약점을 수시로 점검하고, 자료의 위·변조, 훼손 여부를 확인하여야 한다.

제19조**(사용자계정 관리)** ① 시스템관리자는 사용자계정(ID)의 비인가자 도용 및 정보시스템 불법접속 등을 방지하기 위해 다음 각 호 사항을 반영·관리하여야 한다.

1. 신규 사용자계정 생성 시 신청서 작성, 신원확인 등의 절차를 거쳐 발급
2. 퇴직 또는 보직변경 등으로 사용자계정을 해지해야할 때에는 신속히 삭제

3. 사용자별 또는 그룹별로 접근권한 부여, 사용자계정을 공동으로 사용 금지
4. 외부 사용자의 계정부여는 불허하되, 부득이한 경우에는 각급기관의 정보보안담당관의 책임 하에 유효기간을 설정하는 등 보안조치를 강구한 후 허용
5. 비밀번호 등 사용자 식별·인증 수단이 없는 사용자계정은 사용 금지
6. 장시간 사용하지 않는 휴면계정을 점검하여 필요하지 않은 경우 삭제
7. 계정을 주기적(사용자계정 6개월, 관리자계정 3개월)으로 점검하여 접근권한을 재검토하고 권한 남용을 감시

② 정보시스템의 계정은 사용목적 및 권한에 따라 관리자계정과 사용자계정으로 분류하여 관리하여야 한다.

③ 관리자계정은 관리자로 지정된 자만이 사용할 수 있으며, 그 외의 자에게는 대여할 수 없다. 다만, 업무상 필요에 의해 부득이하게 타인에게 대여한 경우에는 회수 후 즉시 비밀번호 변경 등의 보안조치를 해야 한다.

④ 시스템관리자는 정보시스템별로 계정발급현황을 별지 제11호 서식의 사용자계정 관리대장에 현행화하여 관리해야 한다.

제20조**(비밀번호 관리)** ① 비밀이나 중요자료에는 반드시 자료별 비밀번호를 부여하여야 한다.

② 비밀번호는 다음 각 호 사항을 반영하여 숫자와 문자, 특수문자 등으로 9자리 이상으로 정하고 분기1회 이상 주기적으로 변경 사용하여야 한다.

1. 사용자계정(ID)과 동일하지 않은 것
2. 개인 신상 및 부서명칭 등과 관계가 없는 것
3. 사전에 등록된 단어 또는 추측하기 쉬운 단어는 사용하지 말 것
4. 이미 사용된 또는 직전에 사용된 비밀번호는 재사용하지 말 것
5. 패스워드의 전달 시 팩스, 전자우편을 사용하지 말 것
6. 패스워드의 입력 횟수는 최대 5회로 제한
7. 동일 비밀번호를 여러 사람이 공유하여 사용하지 말 것
8. 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용금지

③ 서버에 등록된 비밀번호는 암호화하여 저장하여야 한다.

제21조**(악성코드 방지대책)** ① 정보보안담당관은 웜·바이러스, 해킹프로그램, 스파이웨어 등 악성코드 감염을 방지하기 위하여 다음 각 호와 같은 대책을 수립·

시행하여야 한다.

1. 사용자는 개인PC에서 작성하는 문서·데이터베이스 작성기 등 응용프로그램을 보안패치하고 백신은 최신상태로 업데이트·상시 감시상태로 설정 및 주기적인 점검을 실시하여야 한다.
2. 사용자는 출처, 유통경로 및 제작자가 명확하지 않은 응용프로그램 사용을 금지하고 인터넷 등 상용망으로 자료 입수 시 신뢰할 수 있는 인터넷사이트를 활용하되 최신 백신으로 진단 후 사용하여야 한다.
3. 사용자는 인터넷 파일공유 프로그램과 메신저·대화방 프로그램 등 업무상 불필요한 프로그램의 사용을 금지하고 시스템 관리자는 인터넷 연동구간의 침입차단시스템 등에서 관련 사이트 접속을 차단하도록 보안설정 하여야 한다.
4. 사용자는 웹브라우저를 통해 서명되지 않은(Unsigned) Active-X 등이 PC 내에 불법 다운로드 되고 실행되지 않도록 보안 설정하여야 한다.

② 시스템관리자 또는 PC 등의 사용자는 시스템에 악성코드가 설치되거나 감염된 사실을 발견하였을 경우에 다음 각 호의 조치를 취하여야 한다.

1. 악성코드 감염원인 규명 등을 위하여 파일 임의삭제 등 감염 시스템 사용을 중지하고 전산망과의 접속을 분리한다.
2. 악성코드의 감염확산 방지를 위하여 정보보안담당관에게 관련 사실을 즉시 통보한다.

③ 정보보안담당관은 악성코드가 신종이거나 감염피해가 심각하다고 판단할 경우에는 관련사항을 교육부에 신속히 통보하여야 한다.

제22조**(보안성 검토)** ① 정보보안담당관은 다음 각 호에 해당하는 경우에는 자체 보안대책을 강구한다.

1. 유·무선 네트워크를 신·증설하거나 서버 등 정보시스템을 구축 또는 교체하고자 하는 경우
2. 내부 정보통신망을 외부망과 연결하고자 하는 경우
3. 국정원장이 개발하거나 안정성을 검증한 암호장비·보안자재·암호논리·암호모듈·정보보안시스템을 도입·운용하고자 할 경우
4. 원격근무 지원 등을 위해 시스템을 도입하는 경우
5. 외부기관 및 업체의 보안감리 또는 보안컨설팅(보안취약점 분석·평가를 포함한다)을 받거나 정보처리·보안관제 등의 업무를 위탁할 경우

6. 그 밖에 정보통신망 및 정보시스템 운용환경 변화로 인하여 별도의 보안대책 수립이 필요하다고 인정되는 경우

② 그 밖에 명시되지 않은 사항은 「국가 정보보안 기본지침」에 따른다.

제23조 **(정보보호시스템의 도입 등)** ① 정보보안담당관은 정보 및 정보통신망 등을 보호하기 위해 정보보호시스템을 도입할 수 있다. 다만, 별지5에 규정된 유형의 시스템에 대해서는 해당 도입요건을 만족하는 경우로 한정한다.

② 정보보호시스템 유형별 도입요건을 변경은 국가정보원장이 하며, 변경시 각급 기관장에게 관련 사항을 통보하여야 한다.

제24조**(정보시스템 저장매체 불용처리)** ① 사용자 및 시스템관리자는 하드디스크 등 전자정보 저장매체를 불용처리(교체·반납·양여·폐기 등) 하고자 할 경우에는 정보보안담당관의 승인 하에 저장매체에 수록된 자료가 유출되지 않도록 보안조치 하여야 한다.

② 자료의 삭제는 해당 정보가 복구될 수 없도록 별지 2의 기준에 따라 저장매체별, 자료별 차별화된 삭제방법을 적용하여야 한다.

③ 당해 기관 내에서 정보시스템의 사용자가 변경된 경우, 비밀처리용 정보시스템은 완전포맷 3회 이상, 그 외의 정보시스템은 완전포맷 1회 이상으로 저장자료를 삭제하여야 한다.

④ 정보보안담당관은 정보시스템 저장자료의 삭제를 외부업체에 의뢰할 경우 작업 장소에 입회하여 삭제 절차 및 방법의 준수여부 등을 확인·감독하여야 한다.

⑤ 정보보안담당관은 저장장치의 자성을 완전히 소멸시키거나 데이터를 완전히 삭제시키는 전용 장비 또는 소프트웨어를 도입하는 경우 국가정보원의 보안 적합성 검증을 필한 제품을 도입하여야 한다.

⑥ 정보보안담당관은 정보시스템 외부 반출 시 다음 각 호에 따라 보안조치를 하여야 한다.

1. 불용처리 등을 위해 정보시스템을 외부로 반출할 경우 현황을 기록·유지하여야 한다.
2. 정보보안담당관은 저장매체의 고장수리·저장자료 복구 등을 외부에 의뢰할 경우 저장매체에 저장된 자료의 유출 방지를 위해 수리 또는 복구 참여자에 대해 보안서약서 징구, 교육 등 필요한 보안조치를 하여야 한다.
3. 정보보안담당관은 정보시스템을 불용 처리할 경우 당해 시스템의 사용기관·

부서・사용자 등을 인식할 수 있는 표시를 모두 제거하여야 한다.

제4장 사용자 정보보안

제25조**(PC보안관리)** ① 정보보안담당관은 단말기를 포함한 PC 등을 사용하고자 할 경우에는 관리책임자를 지정하여야 한다.

② 정보보안담당관은 비인가자(퇴직자 등)가 PC를 무단으로 조작하여 전자정보를 유출하거나, 위・변조 및 훼손시키지 못하도록 다음 각 호에 따른 보호대책을 강구하여야 한다.

1. 장비별・사용자별 비밀번호 사용
2. 백신 및 PC용 침입차단시스템 등 운용
3. P2P 등 업무와 무관하거나 보안에 취약한 프로그램의 사용 금지

③ 정보보안담당관은 PC를 교체・반납・폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 하드디스크에 수록된 자료가 유출, 훼손되지 않도록 보안조치를 하여야 한다.

④ PC에 적용되는 사용자계정(ID) 및 비밀번호의 취급관리는 제17조(사용자계정 관리)와 제18조(비밀번호 관리)의 규정을 준용한다.

⑤ 사용자는 사용자PC 보안관리를 위한 다음 각 호의 사항을 준수하여야 한다.

1. PC부팅 시 패스워드 설정
2. 컴퓨터명은 사용자 실명으로 설정하고 작업그룹명은 과(팀)명으로 설정
3. 최대 10분을 초과하지 않도록 화면보호기 설정
4. IP주소 임의변경 금지
5. PC에 대한 최신 보안업데이트, 바이러스 치료 프로그램 등 보안프로그램 설치 및 주기적인 바이러스검사 실시

⑥ 퇴직 / 보직 종료자의 인수인계시 아래의 사항을 준수하여야 한다.

1. 보안서약서(확약서) 작성
2. 개인(민감)정보를 포함한 불필요 문서는 삭제
3. PC내 저장파일에 대한 목록을 작성
4. PC 및 파일 인수인계시 비밀번호는 즉시 변경토록 조치

제26조**(IP주소 관리)** ① 업무용 PC 사용자는 교내 망접속을 위해 정보통신원에 IP사용신청을 해야한다.(학과 및 연구 PC는 학부 행정실에서 일괄신청 가능)

② 정보보안담당관은 IP 임의 도용 사용자 발견시 아래 규정에 의해 처리해야한다.

1. 진술서 작성
2. 개인PC(데스크탑, 노트북 등) 사용자 : MAC주소 영구차단(교내망접속 불가)
3. 대학PC(데스크탑, 노트북 등) 사용자 : IP차단 / PC 회수

③ 정보보안담당관 주관하 사실정도에 따른 처리기간을 판단하고 재사용권한 부여시 보안서약서 집행을 병행한다.

제27조**(스마트폰 등 모바일 행정업무 보안관리)** 스마트폰 등을 활용하여 내부행정업무, 학사관련 모바일 업무환경을 구축할 경우 보안대책을 아래와 같이 수립·시행하여야 한다.

1. 정식앱마켓이 아닌 다른출처(블랙마켓)의 앱 설치 제한
2. SMS 도는 SNS에 포함된 인터넷 주소 또는 URL 클릭 금지
3. 공인인증서는 USIM 등 안전한 저장소에 보관
4. 스마트폰 내 백신 설치 및 실시간 탐지 기능 활성화
5. 스마트폰 체제를 항상 최신으로 업데이트(보안패치 등)
6. 스마트폰 보안잠금(비밀번호 또는 화면패턴)
7. 스마트폰 플랫폼의 구조를 임의로 변경하지 않기(루팅, 탈옥 등)
8. KISA에서 배포하는 폰키퍼를 설치하여 정기적으로 보안점검 실시

제28조**(클라우드시스템 보안관리)** ① 정보보안담당관은 클라우드 컴퓨팅시스템을 구축할 경우「국가·공공기관 클라우드 컴퓨팅 보안가이드라인」(2013.1, 국가정보원)을 준용한 보안대책을 강구하여야 한다.

② 정보보안담당관은 상용 클라우드 컴퓨팅 시스템을 활용하고자 할 경우에는 교육부장관을 경유하여 국가정보원장에게 보안성 검토를 요청하여야 한다.

제29조**(소프트웨어의 설치 제한)** ① 각급기관의 소프트웨어는 업무상 인가된 프로그램만 사용하여야 한다.

② 각급기관의 정보시스템을 침해하거나 우회할 수 있는 소프트웨어를 임의로 설치하거나 시스템 운영상 설치된 프로그램을 임의로 삭제하여서는 아니 된다.

제30조**(인터넷 서비스 차단)** ① 인터넷PC에서 내부정보유출가능성이 있는 다음

각 호에 해당하는 경우 서비스를 차단할 수 있다.

1. 웹메일을 이용한 메일 발송 시 메일제목, 본문내용, 첨부파일내용에 사전 정의된 키워드(기관 중요정보 키워드 및 주민등록번호, 신용카드정보 등 개인정보)가 포함될 경우
2. 웹메일(상용이메일) 사용 시 대용량 첨부기능으로 메일을 송신할 경우
3. 침입차단시스템을 우회하여 접속하는 프로그램을 이용하여 서비스 연결할 경우
4. 웹하드 등에 파일 업로드를 시도하는 경우
5. 상용 메신저 S/W를 설치하여 연결을 시도할 경우
6. 비업무용사이트(인터넷파일공유 및 음악 사이트 등)에 접속할 경우
7. 그 밖에 정보보안을 위하여 서비스 차단이 필요하다고 판단되는 경우

② 업무·인터넷망이 분리된 부서/학부의 인터넷PC에서는 업무와 관련된 자료를 작성·저장·편집하여서는 아니 된다. 다만, 업무상 필요할 경우 정보통신원의 정보보안담당관의 승인을 통하여 외부 공개가 가능한 자료에 한하여 편집을 허용할 수 있다.

제31조**(업무PC 사용제한)** 인터넷망이 분리된 업무PC로 인터넷 서비스를 사용하기 위한 물리적 우회접속 시도 등을 하여서는 아니 된다.(단 업무망, 인터넷망 분리시에만 적용)

제32조**(보안프그램 설치·운영)** 정보보안담당관은 사용자 PC의 안정성을 강화하기 위하여 다음 각 호의 필수 보안프로그램 설치 및 운용방안을 강구하여야 한다.

1. 바이러스백신 소프트웨어
2. 패치관리 소프트웨어
3. 보안USB 통합관리 소프트웨어
4. PC보안 및 접근통제 소프트웨어 등

제33조**(방문자 PC의 사용제한)** 방문자 휴대용컴퓨터(일반 PC포함)는 내부 업무망 접속을 원칙적으로 금지한다. 단, 사전에 정보통신원의 정보보안담당관 승인을 받은 사용자에 한하여 접속을 허용할 수 있다.

제34조**(PC 반·출입 제한)** 내부 업무용PC는 외부로의 반출을 금지하며 외부 업무용으로 사용하는 휴대용 컴퓨터에 한하여 부서장 책임하에 반출할 수 있다.

제35조**(사용자 패스워드 관리)** ① 사용자PC의 패스워드 관리는 제20조 “비밀번호 관리” 에 관한 규정을 준용한다.

② 사용자는 PC에 접근하기 위해 사용하는 모든 패스워드에 대하여 비밀을 유지해야 하며, 타인에게 고의로 패스워드 정보를 제공하거나 노출시켜서는 아니 된다.

③ PC에 접근하기 위해 사용되는 패스워드가 노출되었거나 노출이 의심되는 경우, 패스워드를 즉시 변경하여야 한다.

제36조**(바이러스 감염 시 조치사항)** 사용자는 사용자PC가 바이러스에 감염되었거나 감염이 의심 될 경우 즉시 네트워크 접속을 차단하고 정보통신원의 정보보안담당자에게 바이러스 감염사실을 신속하게 통보하고 필요한 조치를 받아야 한다.

제37조**(휴대용저장매체 관리)** ① "휴대용저장매체 관리책임자"(이하 ‘관리책임자’라 한다)라 함은 각 과 또는 팀별 휴대용저장매체 관리상의 임무를 맡은 부서장을 말한다.

② 관리책임자는 휴대용저장매체의 등록, 파기, 재사용, 반출·입, 불용처리 현황 등의 업무를 수행하는 휴대용저장매체 실무책임자를 지정·운영하여야 한다.

③ 그 밖에 명시되지 않은 사항은 국가 정보보안 기본지침의「USB메모리 등 휴대용저장매체 보안관리 지침」에 따른다.

제38조**(전자우편 보안대책)** ① 정보보안담당관은 웜·바이러스 등 악성코드로부터 사용자 PC 등 전자우편 시스템 일체를 보호하기 위하여 백신, 바이러스 월, 해킹메일 차단시스템 구축 등 보안대책을 강구하여야 한다.

② 사용자는 상용 전자우편을 이용한 업무자료 송·수신을 금지하며 대학자체 전자우편으로 송·수신한 중요 업무자료는 열람 등 활용 후 메일함에서 즉시 삭제하여야 한다.

③ 사용자는 출처가 불분명하거나 의심되는 제목의 전자우편은 열람을 금지하고 해킹메일로 의심되는 메일 수신시에는 즉시 정보통신원 내 정보보안담당자에게 신고하여 필요한 조치를 받아야 한다.

④ 정보보안담당관은 수신된 전자우편의 발신지 IP주소와 국가명이 표시되고 해킹메일 원본을 신고할 수 있는 기능을 갖춘 웹메일시스템을 구축하여야 한다. 다만 웹메일시스템을 직접 구축·운영하지 않은 경우에는 그러하지 아니한다.

제5장 정보화 용역사업 관리

제39조**(용역사업 계획단계)** ① 정보보안담당관은「국가계약법」시행령 제76조 제1항 제18호에 따라 용역사업 추진 시 과업지시서·입찰공고·계약서에 다음 각 호의 누출금지 대상정보를 명시해야 하며 해당정보 누출 시 입찰 참가자격 제한을 위한 부정당업자로 등록하여야 한다.

1. 대학 소유 정보시스템의 내·외부 IP주소 현황
2. 세부 정보시스템 구성 현황 및 정보통신망 구성도
3. 사용자계정·비밀번호 등 정보시스템 접근권한 정보
4. 정보통신망 취약점 분석·평가 결과물
5. 정보화 용역사업 결과물 및 관련 프로그램 소스코드(유출 시 안보·국익에 피해가 우려되는 중요 용역사업에 해당)
6. 정보보호시스템 도입 현황
7. 침입차단시스템·방지시스템(IPS) 등 정보보호제품 및 라우터·스위치 등 네트워크 장비 설정 정보
8.「공공기관의 정보공개에 관한 법률」제9조 제1항에 따라 비공개 대상 정보로 분류된 대학의 내부문서
9.「개인정보보호법」제2조 제1호의 개인정보
10.「보안업무규정」제4조의 비밀 및 동 시행규칙 제7조 제3항의 대외비
11. 기타 정보보안담당관이 공개가 불가하다고 판단한 자료

② 정보보안담당관은 사업수행을 위한 제안요청서 및 계약서에 참가직원의 보안준수 사항과 보안 위규자 처리기준 및 위약금 부과기준을 명시할 수 있다.

③ 정보보안담당관은 제안평가요소에 자료·장비·네트워크 보안대책 등 보안관리 계획의 평가항목 및 배점기준을 마련하여야 한다.

제40조**(용역사업 입찰·계약단계)** ① 정보보안담당관은 입찰 공고 시 누출금지대

상정보, 부정당업자 제재조치, 기밀유지 의무 및 위반 시 불이익 등 보안준수사항을 공지하여야 한다.

② 정보보안담당관은 제안업체가 제시한 보안관리 계획의 타당성을 검토하여 사업자 선정 시 반영하여야 한다

③ 정보보안담당관은 사업에 투입되는 자료·장비 등에 대해 대외보안이 필요한 경우 보안의 범위·책임을 명확히 하기 위하여 사업수행계약서와 별도로 비밀유지계약서를 작성하여야한다. 비밀유지계약서에는 비밀정보의 범위, 보안준수사항, 위반 시 손해배상 책임, 지적재산권 문제, 자료의 반환 등이 포함되도록 명시하여야한다.

④ 정보보안담당관은 외부용역을 추진할 경우 사업 책임자로 하여금 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 용역사업 계약서에 참가직원의 보안준수사항과 위반 시 손해배상 책임 등 명시
2. 용역사업 수행 관련 보안교육·점검 및 용역기간 중 참여인력 임의교체 금지
3. 정보통신망도·IP현황 등 용역업체에 제공할 자료는 자료 인계인수대장을 비치, 보안조치 후 인계·인수하고 무단 복사 및 외부반출 금지
4. 사업 종료 시 외부업체의 노트북·휴대용 저장매체 등을 통해 비공개 자료가 유출되는 것을 방지하기 위하여 복구가 불가능하도록 완전삭제
5. 용역업체로부터 용역 결과물을 전량 회수하고 비인가자에게 제공·열람 금지
6. 용역업체의 노트북 등 관련 장비를 반출·반입 시 마다 악성코드 감염여부, 자료 무단반출 여부를 확인
7. 기타, 정보보안담당관이 보안관리가 필요하다고 판단하는 사항이나 국정원장이 보안조치를 권고하는 사항

⑤ 정보보안담당관은 용역업체가 사업의 일부 또는 전부에 대하여 하도급 계약을 체결하는 경우에 용역업체로 하여금 하도급 계약서에 본 사업계약 수준의 비밀유지 조항을 포함하도록 조치하여야 한다.

⑥ 정보보안담당관은 용역사업에 대한 보안관리를 위하여 사업관리담당과 보안관리담당을 분리하여야 한다. 다만, 사업규모가 작아 분리가 곤란한 경우에는 사업관리담당이 보안관리를 병행할 수 있다.

제41조**(용역사업 수행단계)** ① 정보보안담당관은 참여인원에 대하여 다음 각 호에 따라 보안 관리를 하여야 한다.

1. 용역사업의 참여인력에 대하여 보안서약서(별지 제7, 8호 서식) 징구
2. 용역업체 참여인원에 대해 법적 또는 발주기관 규정에 따른 비밀유지 의무준수 및 위반 시 처벌 내용 등에 대한 보안교육
3. 대학은 사업수행 중 업체 인력에 대한 보안점검 실시, '누출금지 대상 정보' 외부 누출여부 확인
4. 비밀관련 용역사업을 수행할 경우, 참여인원에 대한 비밀취급인가 등 보안조치를 수행하고 국가정보원에게 보안측정을 요청

② 정보보안담당관은 용역업체에게 자료를 제공하거나 용역사업수행 중에 생산된 산출물에 대하여 다음 각 호에 따라 보안 관리를 하여야 한다.

1. 계약서 등에 명시한 누출금지 대상정보를 업체에 제공할 경우 자료관리대장을 작성, 인계자·인수자가 직접 서명한 후 제공하고 사업완료 시 관련자료 회수
2. 용역사업 관련자료 및 사업과정에서 생산된 산출물은 대학의 파일 서버에 저장하거나 사업의 보안담당이 지정한 PC에 저장·관리
3. 용역사업 관련 자료는 인터넷 웹하드·P2P 등 인터넷 공유사이트 및 개인메일함에 저장을 금지하고 대학과 용역업체간 전자우편을 이용해 자료전송이 필요한 경우에는 자체 전자우편을 이용, 첨부자료 암호화 수발신
4. 대학내 사무실에서 용역사업을 수행할 경우, 제공한 비공개 자료는 매일 퇴근 시 반납하고 비밀문서를 제외한 일반문서는 시건장치가 된 보관함에 보관
5. 용역사업 수행으로 생산된 산출물 및 기록은 보안담당관이 인가하지 않은 비인가자에게 제공·대여·열람 금지

③ 정보보안담당관은 용역사업을 수행하는 사무실과 장비에 대하여 다음 각 호에 따라 보안관리를 하여야 한다.

1. 시건장치가 구비되고 비인가자 출입통제가 가능한 사무실 사용
2. 용역업체의 사무실과 인원·장비를 대상으로 정기적으로 보안점검 실시
3. 대학 내부에서 용역사업을 수행하는 경우 용역 참여직원이 노트북 등 관련 장비를 외부에 반출·입시마다 악성코드 감염여부 및 자료 무단반출 여부 확인
4. 인가받지 않은 USB 등 휴대용 저장매체 사용을 금지하며 산출물 저장을 위하여 휴대용 저장매체가 필요한 경우 정보통신원 정보보안담당자의 승인하에 사용

④ 정보보안담당관은 용역업체가 이용하는 전산망에 대하여 다음 각 호에 따라 보안관리를 하여야 한다.

1. 용역업체 사용전산망은 방화벽 등을 활용하여 대학 업무망과 분리구성하고 업무상 필요한 서버에만 제한적 접근
2. 사업참여 인원에 대한 사용자 계정은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 차등 부여하되 대학 내부문서 접근 금지하고 불필요 시 곧바로 권한을 해지하거나 계정을 폐기
3. 참여인원에게 부여한 패스워드는 사업 보안 담당자가 별도로 기록·관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력 확인
4. 용역사업 보안관리담당은 서버 및 장비운영자로 하여금 내부서버 및 네트워크 장비에 대한 접근 기록을 매일 확인하여 이상유무 보고
5. 용역업체에서 사용하는 PC는 인터넷 연결을 금지하되, 사업수행상 연결이 필요한 경우에는 대학의 보안통제 하에 제한적 허용
6. 대학 및 용역업체 전산망에서 P2P, 웹하드 등 인터넷 자료공유사이트로의 접속을 방화벽 등을 이용해 원천차단

⑤ 그 밖의 사항에 대해서는"정보화사업 용역관리 매뉴얼"에 따른다.

제42조**(용역사업 종료단계)** ① 정보보안담당관은 최종 용역산출물 중 대외보안이 요구되는 자료는 대외비 이상으로 작성·관리하고 불필요한 자료는 반드시 삭제 및 폐기하여야한다.

② 정보보안담당관은 용역업체에 제공한 자료·장비·문서 및 중간·최종산출물 등 사업 관련 제반자료를 확인하여 전량 회수해야 하며, 업체에 복사본 등 별도 보관을 금지시켜야 한다.

③ 정보보안담당관은 사업완료 후 업체 소유 PC·서버의 하드디스크·휴대용저장매체 등 전자기록 저장매체는 국가정보원장이 안전성을 검증한 삭제 S/W로 완전 삭제 후 반출하여야 한다.

④ 정보보안담당관은 제2항의 용역사업 관련자료 회수 및 삭제조치 후에 용역업체가 용역산출물의 복사본 등 용역사업 관련 자료를 보유하고 있지 않다는 용역업체 대표명의 보안확약서(별지 제9호)를 징구하여야 한다.

제43조**(용역사업 보안관리실태 점검)** 정보보안담당관은 정보화용역사업 관련 규정에서 정한 보안대책에 대한 이행실태를 주기적으로 점검하고 미비점 발견 시 보완 조치하여야 한다.

제6장 정보통신망 관리

제44조**(상용망 등 외부망 연동)** ① 정보보안담당관은 내부 정보통신망을 외부 정보통신망에 연결하고자 하는 경우에 보안관리 책임한계 설정, 전자정보의 제공범위 및 이용자 접근제한 등 정보통신망 보안대책을 수립·시행하여야 한다.

② 정보보안담당관은 정보통신망을 상용망(인터넷 포함)이나 다른 기관과 정보통신망을 연계하기 위한 보안관리 연결지점을 운용할 경우에는 비인가자의 무단침입(불법접속)이나 악성코드 및 사이버공격을 방지하기 위하여 국가정보원장이 검증한 보안시스템의 설치·운용 등 보안대책을 강구하여야 한다.

③ 정보보안담당관은 정보통신망 및 정보시스템에 사용되는 “IP주소”를 체계적으로 관리하여야 한다. 이 경우에 내부 정보시스템을 보호하기 위하여 사설주소체계(NAT : Network Address Translation)를 사용한다.

④ 정보보안담당관은 인터넷을 통한 불법 사이트 접속이나 프로그램 다운로드를 금지하여야 하며, 개인용 장비에서 음란·도박·게임 등 업무와 무관한 인터넷 사이트 접근에 대한 통제대책을 강구하여야 한다.

⑤ 업무망과 인터넷망 간의 자료교환은 망간자료전송시스템을 사용하여야 하고 전송로그는 6개월 이상, 원본파일은 3개월 이상 유지하여야 한다.

⑥ 업무망 관리자는 전송 실패기록을 점검하여 악성코드 유입여부 등을 주기적으로 확인 조치하여야 한다.

⑦ 업무망 PC의 자료를 인터넷 PC로 전송시에는 정보통신원의 정보보안담당자의 사전승인을 받아 진행한다.

제45조**(원격근무 보안관리)** ① 정보보안담당관은 재택·파견·이동근무 등 원격근무를 지원하기 위한 정보시스템을 도입·운영하고자 할 경우에 교육부장관과 사전 협의하여야 한다.

② 원격근무를 지원하고 있는 정보보안담당관은 다음 각 호에 따라 관리하여야 한다.

1. 원격근무 사유(재택, 파견, 이동근무, 출장, 전산망 유지보수 등) 확인
2. 원격근무지원시스템의 사용기록을 보관하고 사용자, 사용자계정, 접속 주소와 시간 및 특이사항 등을 주기적으로 점검
3. 원격근무 완료 후 사용자계정 및 비밀번호의 신속한 회수

③ 정보보안담당관은 제1항 및 제2항에 따라 원격근무를 지원하고 있거나 이를 지원하기 위한 정보시스템을 도입하고자 하는 경우 정부원격접속서비스(GVPN)의 이용 가능 여부를 사전에 확인하여, 활용 가능한 기관의 경우 이를 우선 활용하여야 한다.

제46조**(네트워크장비 보안관리)** ① 정보보안담당관은 라우터, 스위치 등 네트워크 장비 운용과 관련하여 다음 각 호의 보안조치를 강구해야 한다.

1. 네트워크 장비에 대한 원격접속은 원칙적으로 금지하되, 불가피할 경우 장비 관리용 목적으로 내부 특정 IP·MAC 주소에서의 접속은 허용
2. 물리적으로 안전한 장소에 설치하여 비인가자의 무단접근 통제
3. 네트워크 장비 등 신규 전산장비 도입시 생성되는 기본(default) 계정을 삭제 또는 변경하고 시스템 운영을 위한 관리자 계정 별도 생성
4. FTP 등 불필요한 서비스 포트 및 사용자 계정 차단·삭제
5. 접근통제목록(ACL) 적용 및 초기설정 비밀번호 변경으로 비인가자의 네트워크 장비 무단접근 통제
6. 펌웨어 무결성 및 소프트웨어·서버 운영체제 취약점과 최신 업데이트 여부를 주기적으로 확인하여 항상 최신 버전으로 유지

② 정보보안담당관은 네트워크장비의 접속기록을 6개월 이상 유지하여야 하고 비인가자의 침투 여부를 주기적으로 점검하여야 한다.

제47조**(무선랜 보안관리)** ① 정보보안담당관은 무선랜(와이파이 등)을 이용하여 업무자료를 소통하고자 할 경우 자체 보안대책을 수립하여 관련 사업 계획단계(사업 공고 전)에서 교육부에 보안성 검토를 의뢰하여야 한다.

② 정보보안담당관은 제1항의 보안대책 수립 시, 다음 각 호의 사항을 포함하여야 한다.

1. 네트워크 이름(SSID, Service Set Identifier) 브로드캐스팅 중지
2. 추측이 어려운 복잡한 SSID 사용
3. WPA2 이상(256비트 이상)의 암호체계를 사용하여 소통자료 암호화(국가정보원장이 승인한 암호논리 사용)
4. MAC 주소 및 IP 필터링 설정, DHCP 사용 금지

5. RADIUS(Remote Authentication Dial-In User Service) 인증 사용
6. 그 밖에 무선단말기·중계기(AP) 등 무선랜 구성요소별 분실·탈취·훼손·오용 등에 대비한 관리적·물리적 보안대책

③ 정보보안담당관은 제1항 및 제2항과 관련한 보안대책의 적절성을 수시로 점검하고 보완하여야 한다.

제48조**(무선인터넷 보안관리)** ① 정보보안담당관은 무선인터넷(WiBro, HSDPA 등)시스템을 구축하여 업무자료를 소통하고자 할 경우 자체 보안대책을 수립하여 관련 사업 계획단계(사업 공고 전)에서 교육부장관에게 보안성 검토를 의뢰하여야 한다.

② 정보보안담당관은 청사 전역에 무선인터넷 사용을 제한하고 민원실 등 특별히 무선인터넷 사용이 필요한 구역에 한해 기관장 책임하에 운용할 수 있다.

③ 정보보안담당관은 업무용PC에서 무선인터넷 접속장치(USB형 등)가 작동되지 않도록 관련 프로그램 설치 금지 등 기술적 보안대책을 강구하여야 한다.

④ 정보보안담당관은 교내 업무, 학업 관련 무선랜 ID 발급이 필요한 경우 아래와 같이 보안조치를 해야한다.

1. ID 발급 신청서(보안서약 내용 포함) 작성후 정보보안담당관에게 제출
2. 사용기간 미지정 이용자 1년단위 갱신필요.
3. 무선접속으로 인한 보안문제 식별시 관리자가 선조치후 이용자에게 통보

단, 교직원, 재학생(대학원생 포함)은 제외한다.

⑤ 정보보안담당관은 개인 휴대폰을 제외한 무선인터넷 단말기의 사무실 무단 반입·사용을 금지하는 한편 제1항부터 제3항까지와 관련한 보안대책의 적절성을 수시로 점검하고 보완하여야 한다.

제7장 사이버공격 대응 및 조치

제49조**(보안관제센터 구축)** ① 정보보안담당관은 소관 정보통신망에 대한 사이버공격 정보를 수집·분석·대응할 수 있는 자체 보안관제센터를 설치하여야 한다. 다만, 보안관제센터를 설치·운영하지 못하는 경우에는 다른 정보보안담당관 및 관계 공공기관의 장이 설치·운영하는 보안관제센터에 그 업무를 위탁할 수 있다.

② 보안관제센터를 운영하는 기관의 장은 보안관제 업무를 하루 24시간 중단 없이 수행하여야 하며 보안관제센터의 운영에 필요한 전담직원을 배치하여야 한다.

제50조**(보안관제 용역업체 선정)** ① 정보보안담당관은 지식경제부 장관이 지정하는 보안관제 전문업체중에서 '보안관제 용역업체 업무수행 능력평가 기준'등을 참고하여 보안관제 용역업체를 선정한다.

② 보안관제 용역업체 선정을 위하여 작성한 각종 문서는 평가가 끝난 후에도 공개할 수 없으며 3년간 보존하여야 한다. 다만 관계 법규에 따라 정보공개를 요청받은 경우에는 그러하지 아니할 수 있다.

제51조**(보안관제센터 시설보안)** ① 정보보안담당관은 보안관제센터를 통제구역으로 설정하여 관리하여야 한다.

② 정보보안담당관은 다음 각 호의 보안대책을 수립·시행하여야 한다.

1. 출입인가자의 제한범위 설정과 비인가자의 출입통제대책
2. 주·야간 경계대책
3. 방화·항온·항습대책 및 그 밖에 필요한 보안대책

③ 보안관제센터는 상시 출입자에 대하여 항상 출입증을 패용하게 하고 정보시스템 유지보수 등을 위한 임시 출입자의 경우에는 임시출입증을 패용하고 직원이 안내하도록 하여야 한다.

④ 보안관제센터는 외부인으로부터 시찰견학 요청을 받은 경우에는 시설에 대한 사진 촬영을 제한하고 보안관제와 관련된 세부 정보의 제공을 금지하는 등 출입자에 대한 보안대책을 마련하여야 한다.

제52조**(예방활동)** 정보보안담당관은 소관 정보시스템의 사이버안전을 확보하기 위하여 평시 예방활동을 수행하여야 하며 사이버 침해사고 발생 시 신속하게 대응할 수 있는 긴급연락체계를 상시 관리하여야 한다.

제53조**(초동조치)** 정보보안담당관은 소관 정보시스템 및 정보통신망에 대하여 다음 각 호에 해당하는 사이버공격을 인지할 경우 그 피해실태를 파악하고 관련 로그 자료를 보존하여야 하며, 필요할 경우 정보시스템을 통신망과 분리하는 등 초동조치를 취하여야 한다.

1. 비인가자의 정보시스템·어플리케이션에 대한 접근 및 접근시도
2. 정보자산의 유출(H/W, S/W, DATA 등)
3. 비인가자에 의한 중요 정보의 위·변조 및 삭제에 관한 사항
4. 악성 프로그램(바이러스, 백도어 등) 유포
5. 정보시스템에 대한 서비스 거부공격(DOS 공격 등) 발생
6. 네트워크 장비, 서버 및 PC 등에 대한 해킹
7. 그 밖에 정보보안 사고에 해당하는 사항

제54조**(사고통보 및 복구)** ① 정보보안담당관은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취해야 하며, 지체 없이 전화·팩스·이메일 등 통신수단을 활용하여 그 사실을 교육부장관에게 통보하여야 하며 통보해야할 사항은 다음 각호와 같다.

1. 대규모 사이버공격 발생시
2. 사이버공격으로 인하여 피해가 발생하거나 피해 발생이 예상되는 경우
3. 사이버공격이 확산될 우려가 있는 경우
4. 그 밖에 사이버공격 계획 등 사이버안전에 위협을 초래할 수 있는 정보를 입수한 경우

② 교육부장관은 사이버공격으로 인한 사고의 발생 또는 징후를 발견하거나 통보를 받은 때에는 관계 정보보안담당관에게 사고복구 및 피해의 확산방지에 필요한 조치를 요청할 수 있다. 이 경우 요청받은 관계 정보보안담당관은 특별한 사유가 없는 한 이에 협조하여야 한다.

제8장 보 칙

제55조**(시행세칙)** 정보보안담당관은 정보보안 업무수행을 위하여 이 지침을 준용하여 세부지침을 정하여 운용할 수 있다.

제56조**(준용 또는 위임)** 이 지침에 명시되지 않은 사항은 다음 각 호의 관련 규정 및 지침에 따른다.

1. 대통령령『보안업무규정』

2. 대통령령『보안업무규정시행규칙』
3. 대통령령『보안업무규정시행요강』
4. 국가정보원 『국가 정보보안 기본지침』
5. 국가정보원『USB메모리 등 휴대용저장매체 보안관리 지침』
6. 교육부『정보보안기본지침』
7. 그 밖에 정보보안 관계 법령 및 지침·가이드·메뉴얼

부 칙

이 규정은 2011년 9월 22부터 시행한다.

부 칙

이 규정은 2015년 6월 11부터 시행한다.

【별지 제1호】

정보보안점검 체크리스트

1. 정보보안 기본활동

순번	세부 점검사항	비고
1	기관 자체 실정에 맞는 정보보안업무 내규를 수립하고 있는가?	
2	매년 정보보안업무 활동계획을 수립・시행하고 심사분석 하는가?	
3	정보보안업무 전담 조직 및 직원(정보보안담당관)이 지정되어 있는가?	
4	소속・산하기관 대상 정보보안 감사・점검・지도방문을 실시하는가?	
5	소속・산하기관 대상 정보보안 교육을 실시하고 있는가?	
6	사이버보안진단의 날을 내실 있게 수행하는가?	
7	정보보안 위규・사고, 정보통신망 장애 발생 시 보고체계 및 조치절차가 있는가?	
8	정보시스템 사용자에 대한 심사 등 인적보안 절차・방법을 강구중인가?	
9	보직변경 등 인사이동시 정보시스템 접근권한을 신속하게 조정하는가?	
10	서버・PC 등 정보시스템 현황을 제대로 파악하는가?	
11	정보통신장비(노트북 등) 반출・입 통제를 철저히 하는가?	
12	업무자료를 상용 전자우편으로 전송하고 있지 않는가?	
13	정보통신망 구축 및 유지보수 업무를 수행하는 외부인력에 대한 신원확인 및 보안서약서 징구 등 충분한 보안조치를 하고 있는가?	
14	용역업체 직원의 내부 정보시스템 접근을 통제하고 있는가?	
15	홈페이지에 자료 게재시 자체 보안성검토를 시행하고 있는가?	
16	중요 정보화사업에 대하여 국정원에 보안성검토를 의뢰하는가?	
17	정보보호시스템(암호모듈 포함) 도입시 보안적합성 검증절차를 준수하는가?	

2. PC 및 서버 보안관리

순번	세부 점검사항	비고
1	PC・서버에 설치된 운영체제 및 응용프로그램을 최신 보안업데이트 하였는가?	
2	백신프로그램이 자동 업데이트되고 실시간 감시기능이 설정되어 있는가?	
3	업무용 PC에 비밀이 평문으로 저장되어 있는가?	
4	P2P, 웹하드, 메신저 등 업무에 무관한 서비스가 허용되거나 비인가 프로그램을 사용하지 않도록 보안조치 하는가?	
5	비인가자 접근방지를 위해 PC 부팅 비밀번호를 설정했는가?	
6	서버 내 저장자료는 중요도에 따라 권한설정이 되어 있는가?	
7	공개서버가 DMZ 구간에 위치하는 등 정보통신망 구성측면에서 PC 및 서버 등의 위치가 적정한가?	
8	인가받지 않은 휴대용 저장매체(USB, 이동형 하드디스크, 메모리카드 등)를 반입・휴대하고 있는가?	
9	전자우편 비밀번호 설정 시 특수문자 포함, 9자리 이상으로 설정하고 주기적으로 변경 사용하는가?	
10	서버 등 정보시스템 접근기록을 유지 관리하는가?	
11	PC・서버에 비인가 USB 등 비인가 정보통신기기 연결 시 작동되지 않도록 보안 설정되어 있는가?	
12	PC・노트북 등 저장매체가 있는 기기의 고장 시 저장된 자료의 완전 삭제를 확인하고 외부에 수리를 의뢰하는가?	
13	중요정보가 저장된 매체 불용처리 시 전용 소자장치로 삭제하거나 파쇄・용해 등 물리적으로 완전 파기하고 있는가?	

3. 네트워크 보안관리

순번	세부 점검사항	비고
1	정보시스템 세부 구성도(IP 포함)를 최신으로 유지하면서 대외비 이상 비밀로 관리하고 있는가?	
2	업무자료를 소통하기 위한 내부망은 인터넷과 분리 운영하는가?	
3	업무망・인터넷간 자료공유 방안이 적정한가?	
4	업무자료를 소통하기 위한 내부망 구축 시 사설주소체계(NAT)를 적용하는가?	
5	국가정보원장이 안전성을 검증한 정보보호시스템을 운용하고 있는가?	
6	네트워크를 통한 파일공유를 제한하고 있는가?	
7	스위치・라우터 등 네트워크 장비와 서버는 비인가자가 접속 못하도록 IP・MAC 통제 등 보안설정하고 불필요한 서비스포트를 제거하는가?	
8	와이브로, 무선랜 등 허가받지 않은 인터넷 접속경로가 존재하는가?	
9	첨단 정보통신기기에 의한 내부 업무자료 유출방지 대책이 충분한가?	
10	시스템 최초 설치시 등록된 관리자계정(회사명 등)・패스워드를 변경하였는가?	
11	장비 신규 도입, IP할당내역 등 전산망 구성 변동 시 관련사항을 기록하는가?	
12	중요업무 처리 PC는 인터넷 연결을 금지하고 이상 유무를 수시로 점검하는가?	
13	무선네트워크 구축 시 사전에 국정원의 보안성검토를 받았는가?	
14	홈페이지에 대한 보안취약점을 주기적으로 점검하는가?	
15	불가피한 사정상 무선중계기를 설치하였을 경우 WPA2이상 보안설정을 하였는가?	
16	직원의 재택・파견・이동근무 등 원격근무 시 보안관리 절차가 충분한가?	

4. 보안관제 등 해킹 대응활동

순번	세부 점검사항	비고
1	사이버공격에 대응하기 위한 관제센터를 운영하거나 同 업무를 他기관에 위탁하였는가?	
2	보안관제센터 운영을 총괄 관리하는 전담 공무원이 있는가?	
3	사이버공격 탐지·대응 매뉴얼이 구비되어 있는가?	
4	해킹사고 조사결과, 보안위규자에 대한 처벌이 제대로 이루어지고 있는가?	
5	보안시스템 및 정보시스템에 대한 로그를 일정기간 유지하고 있는가?	
6	보안관제 용역업체 직원에 대한 보안대책이 있는가?	
7	자체 DDoS공격 대응매뉴얼을 구비하였는가?	
8	자체 사이버위기 대응 모의훈련을 주기적으로 실시하는가?	
9	DDoS공격 등 침해사고 발생 시 국가정보원 등 유관기관에 즉시 연락하는가?	
10	시스템 장애 시 유지보수 업체에 연락할 수 있는 비상연락체계가 구비되어 있는가?	
11	보안관제시스템에 대한 물리적인 보안대책을 준수하고 있는가?	
12	침해사고 발생 시 사고조사내역 등 관련 문서(전자문서 포함)를 저장하고 있는가?	
13	해킹메일 대응방안 등 침해사고 대응절차 등을 보안교육을 수행하는가?	
14	보안취약점 발표 시, 대상기관이나 담당직원에게 즉시 배포하는가?	
15	국가사이버안전센터 등과 사이버위협정보, 탐지기술 등 정보를 공유하고 있는가?	
16	사이버공격 발생시 소속·산하기관에 전파할 수 있는 체계가 구비되었는가?	

【별지 제2호】

정보시스템 저장매체·자료별 삭제방법

저장매체 \ 저장자료	공개자료	민감자료 (개인정보 등)	비밀자료 (대외비 포함)
광디스크 (CD·DVD 등)	㉮	㉮	㉮
자기 테이프	㉮·㉰중 택일	㉮·㉰중 택일	㉮
반도체메모리 (EEPROM 등)	㉮·㉰중 택일	㉮·㉰중 택일	㉮·㉰중 택일
	완전포맷이 되지 않는 저장매체는 ㉮ 방법 사용		
하드디스크	㉱	㉮·㉯·㉰중 택일	㉮·㉯중 택일

㉮ : 완전파괴(소각·파쇄·용해), ㉯ : 전용 消磁장비 이용 저장자료 삭제
㉰ : 완전포맷 3회 수행, ㉱ : 완전포맷 1회 수행

【별지 제3호】

○○년도 정보보안업무 추진계획

1. 활동 목표

2. 기본방침

3. 세부 추진계획

분야별	사업명	세부 추진계획	주관·관련부서	비고

※ 보안성검토 대상여부 표기

4. 전년도 보안감사・지도방문 시 도출내용과 조치내역

도 출 내 용	조 치 내 역	담 당 부 서

※ 형식위주의 계획수립을 지양하고 소속기관의 추진계획을 종합, 자체 실정에 맞게 작성

【별지 제4호】

○○년도 정보보안업무 심사분석

1. 총 평

2. 주요성과 및 추진사항

3. 세부 사업별 실적분석

추 진 계 획	추 진 실 적	문 제 점	개 선 대 책

4. 애로 및 건의사항

5. 첨부(정보통신망 및 검증필 정보보호시스템 운용현황 등)

【별지 제5호】

정보보호시스템 도입 시 확인사항

항목명	점 검 항 목	결 과
인증여부	EAL 2 이상 CC인증서 획득 여부	
	CC인증을 받지 않은 경우, 국가용 암호제품 지정 여부	
	국가정보원장이 검증한 암호모듈 탑재 여부	
일치성	인증보고서 또는 운용정책문서와 도입제품 보안기능 일치성 여부	
	기술제안서(RFP)에서 요구하는 보안기능 구현 여부	
운용환경	도입기관의 시스템관리자 지정여부	
	감사기능 지원 여부	
	네트워크 성능 요구사항 만족 여부	
	시스템 장애 시 대책 수립 여부	
유지보수	보안적합성 검증결과 반영 가능 여부	
	업체 기술지원 전담조직 운영 여부	
	작동중단 등 긴급상황에 대비한 지원절차 마련 여부	
	업체 유지보수 매뉴얼 제공 여부	
	관리자 설치·운영 매뉴얼 제공 여부	
	업체의 제품 운용교육 제공 여부	
	신규취약성에 대한 통보 및 처리절차 마련 여부	

※ 점검결과는 O, X로 표기

【별지 제6호】

보안적합성 검증 신청서

신청기관	기관명		운용부서		
	도입목적				
	운용환경	사용자 수		망 구성	□유선 □무선
		속도(대역폭)			
	운용형태	□단독 설치·운용 □타 보안제품과 연동 □대 국민 배포용			
	연동 시스템	□ ERP □ KMS □ CRM □ 전자결재 □ 기타 그룹웨어			
	사업명				
신청제품	업체명		대표자		
	주소		전화번호		
	제품명	* 신청제품이 2種 이상인 경우, 추가기재	CC 인증번호		
			암호 검증번호		
			용역개발 여부	□ 예 □ 아니오	
	평가기관		인증기관	등급	
	담당자	전화번호			
		휴대폰번호			
		E-mail			
	암호모듈	□없음 □있음 (□검증 □미검증)			

【별지 제7호】

보 안 서 약 서(업체대표)

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

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

2. 본인은 이 기밀을 누설함이 국가안전보장 및 국가이익에 위해가 될 수 있음을 인식하여 업무수행 중 지득한 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 하도급업체를 통한 사업 수행 시 하도급업체로 인해 발생하는 위반사항에 대하여 모든 책임을 부담한다.

년 월 일

서 약 자 (업체 대표)
업 체 명 :
사업자등록번호 :
성 명 : (서명)

서약집행자 (담당공무원)
소 속 :
직 위 :
성 명 : (서명)

【별지 제8호】

보 안 서 약 서(참여직원용)

본인은 년 월 일부로 ____과 관련한 업무(연구개발, 제작, 입찰, 그 밖의 업무)를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 _____과 관련된 소관업무가 기밀 사항임을 인정하고 제반 보안 관계규정 및 지침을 성실히 준수한다.

2. 나는 이 기밀을 누설함이 이적행위가 됨을 명심하고 재직 중은 물론 퇴직 후에도 알게 된 모든 기밀사항을 일절 타인에게 누설하지 아니한다.

3. 나는 기밀을 누설한 때에는 아래의 관계법규에 따라 엄중한 처벌을 받을 것을 서약한다.

   가. 국가보안법 제4조 제1항 제2호・제5호(국가기밀 누설 등)
   나. 형법 제99조 (일반이적) 및 제127조(공무상 비밀의 누설)

년 월 일

서 약 자 소속 직급 성 명 (서명)

서약집행자 소속 직급 성 명 (서명)

【별지 제9호】

보 안 확 약 서

본인은 귀 기관과 계약한 _____ 사업의 수행을 완료함에 있어, 다음 각 호의 보안사항에 대한 준수 책임이 있음을 서약하며 이에 확약서를 제출합니다.

1. 본 업체(단체)는 업체(단체) 및 사업 참여자가 사업수행 중 지득한 모든 자료를 반납 및 파기하였으며, 지득한 정보에 대한 유출을 절대 금지하겠습니다.
2. 본 업체(단체)는 하도급업체에 대해 상기 항과 동일한 보안사항 준수 책임을 확인하고 보안확약서 징구하였으며, 하도급업체가 위의 보안사항을 위반할 경우에 주사업자로서 이에 동일한 법적 책임을 지겠습니다.
3. 본 업체(단체)는 상기 보안사항을 위반할 경우에 귀 기관의 사업에 참여 제한 또는 기타 관련 법규에 따른 책임과 손해배상을 감수하겠습니다.

년 월 일

서약업체(단체) 대표

소 속 :

직 급 :

성 명 : (서명)

○○○○○○○장 귀하

【별지 제10호】

정보시스템 관리대장

연번	시스템명	주요기능(용도)	설치일자	관리책임자	비 고

【별지 제11호】

사용자계정 관리대장

연번	소속	성명	시스템명	계 정	접근권한	처리내용 (등록, 수정, 삭제)	처리일자	확인

【별지 제12호】

용역업체 보안점검 관리대장

☐ 점검일 : 년 월 일

☐ 용역사업 책임자(소속/이름) : / (인)

☐ 분임보안담당관(소속/이름) : / (인)

구분	점 검 항 목	확인
인적	용역 참여 인원 변동사항 현행화 및 보안 서약서 징구	
	참여인원에 대한 보안 교육 실시	
	비인가자 출입 및 접근 통제	
장비	용역업체 전산장비 관리대장 확인(갱신 여부 등 확인)	
	전산장비에 대해 월 1회“내 PC 지키미 수행”결과 확인 및 보완 - 비밀번호 지정 및 정기변경(최소 분기별 1회 이상), 화면보호기 설정여부	
	비인가 휴대용저장매체 사용 여부 확인	
	전산장비 반·출입 대장 확인	
	- 반입시 최신 백신 프로그램 설치여부 및 악성코드 감염여부 확인	
	- 반출시 무단반출 여부 확인	
네트워크	방화벽 등 정보보안시스템을 사용하여 비인가 네트워크 차단	
	정보시스템 접근 대상 인원의 네트워크 허용 리스트 관리	
	정보시스템에 접근 가능한 참여인원은 최소화하고 계정별로 접근 권한을 차등 부여	
	정보시스템 접근 계정과 비밀번호 관리 및 작업 내역 기록	
	정보시스템에서 작업 후 기록한 작업 내역과 정보시스템 로그 확인	
	정보시스템 작업이력 로그는 6개월이상 보유	
	정보시스템 접속 기간이 만료한 계정의 해지 여부	
	정보시스템 운영자는 서버 및 네트워크 장비에 비인가자 접근 여부 매일 확인	
	사용자 계정· 네트워크 사용 승인 관리, 사용 만료 시 즉시 차단	
자료	누출금지대상정보 등 제공자료에 대한 관리대장 작성 및 확인 점검	
	산출물 지정 파일서버 저장·관리, 파일서버 인터넷 연결 금지	
	전자우편 비밀번호 설정시 특수문자 포함, 9자리 이상 설정하고 주기적으로 변경	
	전자우편을 통한 발주기관과 업체간 자료 전송 유무 확인	
	전자우편으로 자료 전송한 경우, 업체 자사메일로 업무자료 송수신 후 메일삭제 조치	

※ 전산장비 종류 : 서버, PC, 노트북, 휴대용 저장매체 등을 모두 포함하며, 특히 휴대용 저장매체는 스마트폰 , MP3 플레이어 등 유사 저장매체 모두 포함

※ 확인 : 분임보안담당관이 점검하고 점검자 란에 이름 및 서명

※ 분임보안담당관은 점검대장을 최종 검토한 후 미흡한 부분 보완지시 및 서명

【별지 제13호】

용역업체 사업 참여인원 현황대장

□ 사업명 : _____

□ 사업기간 : _____년 _____월 _____일 ~ _____년 _____월 _____일

□ 주사업자명 : _____

□ 총 참여인원 : _____(명)

□ 참여인원 현황(※ 하도급업체 포함)

연번	업체명	소속팀 및 직위	이름	전화번호	E-mail	비 고
1						
2						
3						
4						

【별지 제14호】

용역업체 보안교육 결과서

_____업체는 _____년도 발주기관(기관명 : _____)의 정보화사업(사업명 : _____)을 수행함에 있어 용역사업 수행 기간동안 용역사업 참여 인력이 준수해야 할 보안사항에 대한 보안교육을 수료하였으며 그 결과를 제출하는 바입니다.

□ 교육 이수 결과

번호	업체명	소속팀 및 직위	이름	전화번호	E-mail	확인 (서명)
1						
2						
3						
4						

【별지 제15호】

용역업체 제공자료 관리대장

연번	제공정보명	제공사유	제공기간	매 체	인계자	인수자	삭제 및 회수 확인
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

【별지 제16호】

용역업체 제공자료 일일 보안점검

연번	제공정보명	제공기간	매 체	인계자	인수자	점검일자	점검 확인
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

【별지 제17호】

용역업체 전산장비 관리대장

연번	사용자 (성명)	관리 번호	전산장비 종류	네트워크 IP	보안 3종 설치 (백신 등)	산출물저장 PC
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						

※ 관리번호 : 각 부서별로 정보자산을 관리하기 위하여 부여하는 번호
(예:팀명-사업명-IP끝자리)
(각 장비에 해당 관리번호를 라벨링하여 부착하기)

※ 전산장비 종류 : 서버, PC, 노트북, 휴대용 저장매체 등을 모두 포함하며 특히 휴대용 저장매체는 스마트폰 , MP3 플레이어 등 유사 저장매체 모두 포함
특히 산출물 저장용 PC나 파일서버도 모두 기록

【별지 제18호】

용역업체 전산장비 반출·입 대장

전산장비명	관리번호	사용자	용도	입·출 구분	반입시		반출시 자료삭제여부	확인
					백신 설치여부 (프로그램명 및 버전정보)	악성코드 점검여부		

※ 관리번호 : 각 부서별로 정보자산을 관리하기 위하여 부여하는 번호(예:팀명-사업명-IP끝자리)

※ 확인 : 분임보안담당관의 결재 또는 서명

【별지 제19호】

용역업체 정보시스템 접속 관리대장

연번	접속자 (소속/성명)	접속자 컴퓨터 IP	정보시스템 IP	접속 용도	발주기관 승인자 (소속/성명)	접속 허용 일자	접속 해제 일자

【별지 제20호】

원격 접근 허용 신청서

(*표시는 반드시 기입하시기 바람)

1. 관리자(서버 등 책임자)

성명*		직급		E-mail*	@
소속*					
연락처*	사무실 :		핸드폰:		

2. 사용자(원격 유지보수 및 진단 수행자)

성명*		직급		E-mail*	
소속*					
연락처*	사무실 :		핸드폰:		

3. 확인 사항(관리자가 확인 및 각 항목 체크 필수)

① 원격 접속시간을 최소화하였습니까?	□ 예 □ 아니오
② 원격에서 최고권한의 계정으로 원격 접속대상 시스템에 직접 접속할 수 없도록 제한하고 임시 접근권한을 부여하였습니까?	□ 예 □ 아니오
③ 원격 접속할 사용자계정의 비밀번호는 임시로 부여하였습니까? (단 비밀번호는 9자리 이상 문자, 숫자, 특수기호 로 구성되어야 함)	□ 예 □ 아니오
④ 원격 접속 후, 소통내용 암호화 등 보안대책을 적용하였습니까?	□ 예 □ 아니오
⑤ 인가되지 않은 원격관리가 수행되는지 주기적으로 확인 점검하고 원격접속 기록을 유지합니까?	□ 예 □ 아니오
⑥ 원격 점검 종료 후 원격 접속시 사용한 계정의 비밀번호, 원격 접속 허용 IP 등은 회수(포트반납신청 또는 서버 설정삭제 등)하여야 합니다. 회수하시겠습니까?	□ 예 □ 아니오
⑦ 원격 점검용 PC(이하 PC)를 통해 원격 접속대상 시스템으로 악성코드나 바이러스 유입을 예방하기 위해 PC에 백신제품 설치 및 바이러스 감염여부 확인 등의 안전조치를 확인하였습니까?	□ 예 □ 아니오
⑧ 이 외의 사항에 대해서는 「교육기술과학부 정보보안기본지침」 및 「정보화사업 용역업체 보안관리 방안」에 준하는 보안대책을 수립하였습니까?	□ 예 □ 아니오

위 사항을 준수할 것을 약속하며 원격 접속 허용 신청합니다.

신 청 일 20 . . .

신청자(관리자) 서명

부서(팀)책임자 서명

4. 신청 정보

원격 허용 신청 상세 정보							
NO.	원격 접속 IP* 1) (Client IP)	PORT*	원격접속 사유*	접속시간* 2)		원격접속 대상 서버 IP* (Server IP)	비고 (경유 IP 등)
				접속시작시간	접속종료(예정)시간		
1	. . .			2010.10.29 18:00	2010.10.31 12:00	. . .	
2							
기타 특이사항							

1) [원격접속IP]는 반드시 공인 IP만 가능하며 any로 신청 불가능함. 사설 IP 사용시 반드시 공인 IP 확인한 후 작성해야 한다. (※ [참고사항] 공인 IP확인방법 : http://ipconfig.co.kr 접속하면 공인 IP확인 가능)

2) [접속시간]은 반드시 접속시작시간과 접속종료시간을 적되, 종료시간을 예측할 수 없는 경우 반드시 예정시간을 적는다.

【별지 제21호】

용역업체 작업 기록 대장

연번	소속	성명	접근 정보시스템	계 정	처리내용 (등록, 수정, 삭제)	처리일자	확인

※ 처리내용 : 내용이 많은 경우 별도 양식에 상세히 기록

※ 확인 : 분임보안담당관의 결재 또는 서명

【별지 제22호】

휴대용 저장매체 불용처리 확인서

아래와 같이 휴대용 저장매체(　종　점) 불용처리 및 휴대용 저장매체(　종　점) 재사용에 대해 확인을 요청함

연번	관리번호 (S/N)	매체형태	사유	불용처리	재사용
1	총무과-일반-01 (E-D900-04-3705B)	USB	고장	물리적 파기	
2	총무과-Ⅲ급-01 (5101-53RA-12567)	CD	고장	물리적 파기	
3	총무과-Ⅱ급-01 (610-RURQ-61750)	USB	용도전환	자성소거	총무과-일반-09
4					
5					
6					
7					
8					
9					
10					

※ 불용처리 장소 : 정보화본부 102동 207호

확인일자 :　　년　월　일

요 청 자 : 소속・직책　　O급 성명 :　　(인)

확 인 자 : 소속・직책　　O급 성명 :　　(인)

【별지 제23호】

본 표준 개인정보처리위탁 계약서는 「개인정보 보호법」 제26조제1항에 따라 위탁계약에 있어 개인정보 처리에 관하여 문서로 정하여야 하는 최소한의 사항을 표준적으로 제시한 것으로서, 위탁계약이나 위탁업무의 내용 등에 따라 세부적인 내용은 달라질 수 있습니다.

개인정보처리업무를 위탁하거나 위탁업무에 개인정보 처리가 포함된 경우에는 본 표준 개인정보처리위탁 계약서의 내용을 위탁계약서에 첨부하거나 반영하여 사용하실 수 있습니다.

표준 개인정보처리위탁 계약서(안)

OOO(이하 "갑"이라 한다)과 △△△(이하 "을"이라 한다)는 "갑"의 개인정보 처리업무를 "을"에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제1조 (목적) 이 계약은 "갑"이 개인정보처리업무를 "을"에게 위탁하고, "을"은 이를 승낙하여 "을"의 책임아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는 개인정보보호법, 동법 시행령 및 시행규칙, 「표준 개인정보 보호지침」(행정안전부 고시 제2011-45호)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) "을"은 계약이 정하는 바에 따라 (_____) 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.[3)]

1.
2.

제4조 (재위탁 제한) ① "을"은 "갑"의 사전 승낙을 얻은 경우를 제외하고 "갑"과의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.

② "을"이 재위탁받은 수탁회사를 선임한 경우 "을"은 당해 재위탁계약서와 함께 그 사실을 즉시 "갑"에 통보하여야 한다.

제5조 (개인정보의 안전성 확보조치) "을"은 개인정보보호법 제29조, 동법 시행령 제30조 및 개인정보의 안전성 확보조치 기준 고시(행정안전부 고시 제2011-43호)에 따라 개인정보의 안전성 확보에 필요한 관리적・기술적 조치를 취하여야 한다.

제6조 (개인정보의 처리제한) ① "을"은 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

② "을"은 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여

3) 각호의 업무 예시 : 고객만족도 조사 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 이름, 주소, 연락처 처리 등

보유하고 있는 개인정보를 「개인정보보호법」 시행령 제16조에 따라 즉시 파기하거나 "갑"에게 반납하여야 한다.

③ 제2항에 따라 "을"이 개인정보를 파기한 경우 지체없이 "갑"에게 그 결과를 통보하여야 한다.

제7조 (수탁자에 대한 관리·감독 등) ① "갑"은 "을"에 대하여 다음 각 호의 사항을 관리하도록 요구할 수 있으며, "을"은 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속현황
3. 개인정보 접근 또는 접속 대상자
4. 목적외 이용·제공 및 재위탁 금지 준수여부
5. 암호화 등 안전성 확보조치 이행여부
6. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② "갑"은 "을"에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, "을"은 특별한 사유가 없는 한 이행하여야 한다.

③ "갑"은 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 (__)회 "을"을 교육할 수 있으며, "을"은 이에 응하여야 한다.[4)]

④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 "갑"은 "을"과 협의하여 시행한다.

제8조 (손해배상) ① "을" 또는 "을"의 임직원 기타 "을"의 수탁자가 이 계약에 의하여 위탁 또는 재위탁받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 "을" 또는 "을"의 임직원 기타 "을"의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 "갑" 또는 개인정보주체 기타 제3자에게 손해가 발생한 경우 "을"은 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보주체 기타 제3자에게 발생한 손해에 대하여 "갑"이 전부 또는 일부를 배상한 때에는 "갑"은 이를 "을"에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, "갑"과 "을"이 서명 또는 날인한 후 각 1부씩 보관한다.

갑	을
○○시 ○○구 ○○동 ○○번지	○○시 ○○구 ○○동 ○○번지
성 명 : (인)	성 명 : (인)

4) 「개인정보 안전성 확보조치 기준 고시」(행정안전부 고시 제2011-43호) 에 따라 개인정보처리자 및 취급자는 1년에 1회 이상 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.