정보보안관리규정

제 정 : 2012 . 6. 1

제1장 총 칙

제1조(목적) 본 규정은 금강대학교(이하 “본교”라 한다) 정보자산을 훼손, 변조, 도난, 유출 등의 위협으로부터 보호하기 위해 필요한 사항을 규정함을 목적으로 한다.

제2조(적용범위) 본 규정은 본교 정보통신망 및 정보시스템 보안운영 및 관리업무를 대상으로 적용한다.

제3조(용어 정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

① “정보통신망”이라 함은 유·무선을 매개로 하는 다양한 정보통신수단에 의하여 부호, 문자, 음향, 영상 등의 정보를 수집·가공·저장·검색·송수신하는 정보 통신 체계를 말한다

② “정보보호”또는“정보보안”이라 함은 정보통신수단으로 수집·가공·저장·검색·송수신 되는 정보의 유출·위변조·훼손 등을 방지하거나 정보통신망을 보호하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위를 말한다

③ “국가용 정보보안시스템(이하 ”국가용 보안시스템“이라 한다)”이라 함은 국가정보원장(이하 ‘국정원장’이라 한다)이 기밀 등 중요자료를 보호하기 위하여 승인한 암호장비·암호자재 또는 암호논리·사이버 안전기술이 적용된 프로그램이나 장치 등을 말한다

④ “전산기계실”이라 함은 서버·PC등 전산장비와 스위치·교환기·라우터 등 통신 및 전송장비 등이 설치 운용되는 장소를 말한다.

⑤ “전산자료”,“전자문서”라 함은 전산장비에 의하여 전자기적인 형태로 입력·보관되어 있는 각종 정보(data)를 말하며, 그 자료가 입력되어 있는 USB, 디스크 등 보조기억매체를 포함한다.

⑥ “보조기억매체”라 함은 디스켓·CD·하드디스크·USB 메모리 등 정보를 저장할 수 있는 것으로 정보통신시스템과 분리할 수 있는 기억장치를 말한다.

⑦ “정보보안시스템”이라 함은 정보의 수집・저장・검색・송신・수신시 정보의 유출, 위・변조, 훼손 등을 방지하기 위한 하드웨어 및 소프트웨어를 말한다

⑧ “비밀번호”라 함은 전산장비에 저장되어 있는 자료를 무단열람하거나 부정출력하지 못하게 하기 위하여 사용하는 패스워드를 말한다.

⑨ “기밀성”이라 함은 정보가 인가되지 않은 개인이나, 처리과정 등에 누설되거나 공개되지 않는 속성을 말한다.

⑩ “무결성”이라 함은 정보가 고의적 또는 우발적으로 변경, 파괴되지 않고 일관성을 유지하는 속성을 말한다.

⑪ “가용성”이라 함은 인가자가 정보나 정보시스템을 사용 또는 접근하고자 할 때 사용 또는 접근이 가능하게 하는 속성을 말한다.
⑫ “접근통제”라 함은 인가된 사용자, 프로그램, 프로세스, 시스템 등의 주체만이 정보시스템의 자원에 접근할 수 있도록 제한하는 것을 말한다.
⑬ “중요정보”라 함은 노출, 변경, 파괴되면 본교에 지대한 영향을 미칠 수 있는 정보를 말한다.
⑭ “로그”라 함은 시스템 사용에 관련된 전체의 기록, 즉 입출력 내용, 프로그램 사용 내용, 데이터 변경 내용, 시작시간, 종료시간 등의 기록을 말한다.
⑮ “프로젝트담당자”라 함은 정보시스템 개발 등의 외부용역사업시 본교의 해당 업무담당자를 말하며, 해당 용역사업 및 용역업체 직원에 대한 관리 책임이 있다.
⑯ “내부망”이라 함은 본교의 보안관리 하에 있는 네트워크 중 라우터를 경계선으로 하여 보호받는 본교의 주요 네트워크를 말한다.
⑰ “외부망”또는 “상용망“이라 함은 내부망을 제외한 모든 네트워크를 말한다.
⑱ “웹 페이지(Web Page)”라 함은 인터넷의 월드 와이드 웹에 접속했을 때 나타나는 웹브라우저(Web Browser)를 통해 사용자들에게 제공되는 인터넷 서비스를 말한다.
⑲ “웹 서버”라 함은 웹서비스 제공을 위한 웹페이지 등 웹 프로그램의 작업수행 및 주된 정보를 제공하는 컴퓨터시스템을 말한다.
⑳ “단말기”라 함은 시스템에 연결되어 단순히 입·출력 기능만 수행하는 전용단말기와 내부망에 연계되어 운용하고 있는 개인용 컴퓨터를 포함한다.
㉑“암호장비”라 함은 정보통신수단으로 처리, 저장, 송수신되는 정보자료를 보호할 목적으로 암호프로그램을 내장하여 제작된 장비나 장치를 말한다.
㉒“암호자재”라 함은 Ⅱ급비밀 이하의 통신내용 및 정보자료를 비닉할 목적으로 사용하는 문자·숫자·기호 등으로 구성된 환자표와 난수 또는 암호논리 등을 저장한 문서나 도구를 말한다..
㉓“암호프로그램”이라 함은 암호장비·암호자재에 적용되거나 자체적으로 자료를 암·복호화하기 위하여 작성된 프로그램을 말한다.
㉔“보조기억매체”라 함은 디스켓·CD·하드디스크·USB 메모리 등 자료를 저장할 수 있는 것으로 정보통신시스템과 분리할 수 있는 기억장치를 말한다.
㉕“개인정보”라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다.
㉖“내부심사”라 함은 정보보호 관련 규정과 정보보호관리체계 지침·매뉴얼의 준수 여부를 확인하고, 개선사항을 제시하며 이행을 권고하는 활동을 말한다.
㉗“침해사고”라 함은 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등에 의하여 정보통신망 또는 이와 관련된 정보시스템을 공격하는

행위로 인하여 발생한 사태를 말한다.
㉘“외부용역인력”이라 함은 본교의 정보자산을 이용하여 서비스와 기타 업무를 대행하는 자를 말하며 그 예는 아래와 같다.
1.본교에서 일정의 계약을 체결하여 계약조건에 부합되는 업무를 담당하고 지원하는 업체 및 직원
2.하드웨어와 소프트웨어의 개발, 유지보수를 담당하고 지원하는 업체 및 직원
3.청소, 경비 및 기타 서비스를 지원하는 업체 및 직원
4.아르바이트생 고용 등 단기간 동안 임시 채용된 업체 및 직원
㉙“외부용역업체”라 함은 '제3자(Third Party)' 및 '외부위탁' 업체를 총칭한다.
㉚정보보안 업무를 합리적이고 체계적으로 관리하기 위하여 아래와 같이 담당자를 지정하여 운영한다.
1.정보보안책임관은 정보지원센터장으로 하며 정보보안에 대한 전반적인 업무를 총괄한다.
2.정보보안담당관은 정보지원센터팀장으로 하며 정보보안책임관을 지원하여 정보보안업무를 진행한다.
3.분임정보보안담당관으로 정보시스템담당자, 정보통신망담당자, 웹시스템담당자 등을 둘 수 있다.
4.부서정보보안담당관으로 각 부서별 정보보안담당관를 두어 원활한 정보보안업무를 진행한다.
㉛“정보보호 전문 교육”이라 함은 정보시스템 운영자를 포함한 정보보안책임관, 정보보안담당관, 분임정보보안담당관이 정보보호 기술을 습득하기 위한 전문교육을 말한다.
㉜“정보보호 기본 교육”이라 함은 전 직원이 정보보호관리체계의 지속적인 운영을 위해 필요한 사항을 습득하기위한 내부교육을 말한다.
㉝“보호구역”이라 함은 비밀보호와 중요시설 장비 및 자재를 불순분자로부터 보호하고 지속적인 기능 유지를 위해 일정한 장소에 일정한 범위를 지정하여 관리하는 구역으로 제한지역, 제한구역 및 통제구역이 있다.
㉞“제한지역” 비밀 및 재산의 보호를 위해 울타리 또는 경비원에 의하여 일반인의 출입감시가 요구되는 지역을 말한다.
㉟“제한구역” 비밀 또는 중요시설 및 자재에 대한 비인가자의 접근을 방지하기 위해 출입에 안내가 요구되는 지역을 말한다.
㊱“통제구역”이라 함은 보안상 극히 중요한 구역으로 비인가자 출입금지 지역을 말한다.
㊲“E-mail 시스템”이라 함은 본교에서 대내외적으로 송수신되는 E-mail을 운영, 관리하기 위하여 구축한 하드웨어, 소프트웨어를 총칭한다.
㊳“E-mail 계정”이라 함은 E-mail 시스템을 이용하는 각 사용자에게 부여된 E-mail 송수신자의 고유 식별자(Identification)를 말한다.

㊴“E-mail 사용자”라 함은 E-mail 시스템을 이용하여 E-mail을 사용하는 직원을 말한다.
㊵“대출”이라 함은 비밀보관소에 보관된 비밀 또는 대외비를 비밀취급자(대외비는 취급자)가 본교 내 사무실에서 볼 수 있도록 대여하여 주는 것을 말한다.
㊶“지출”이라 함은 비밀보관소에 보관된 비밀 또는 대외비를 비밀취급자(대외비는 취급자)가 본교 밖으로 가지고 나가는 것을 말한다.

제2장 정보보안 목표 및 기본활동

제4조(기본목표) 본교 정보보안의 기본목표는 본교가 보유하고 있는 중요정보 유출을 방지하고 정보통신시스템 및 정보통신망의 기밀성・무결성・가용성을 확보하는데 있다.

제5조(활동방향) 본교는 정보보안을 위하여 다음 각 호의 기본활동을 수행한다.

1. 정보보안 정책 및 활동 세부계획 수립・시행
2. 정보보안 감사・지도점검 실시
3. 취약 정보통신망 보안대책 수립 추진
4. 정보보안 위규 적발 및 사고조사 처리
5. 사이버위협정보 수집・분석 및 보안관제
6. 사이버공격 관련 경보 발령 시 대응활동
7. 침해사고 대응・복구
8. 정보보안 교육계획 수립・시행
9. 정보보안업무 심사분석 시행
10. 정보보안 관련 규정・지침 등 제・개정
11. 기타 정보보안 관련 사항

제6조(정보보안 추진계획 수립 및 검토) ① 정보보안책임관 및 정보보안담당관은 년간 정보보안 추진계획을 수립・시행하고 그 추진결과를 심사분석을 해야 한다.
② 정보보안담당관 및 분임정보보안담당관은 세부추진계획 및 심사분석을 ‘[별지 제1호 서식] 정보보안업무 추진계획’ 및 ‘[별제 제2호 서식] 정보보안업무 심사분석’에 따라 작성하여 관리해야 한다. 필요한 경우 별도의 서식을 사용할 수 있다.

제7조(위험분석) ① 정보보안담당관은 기존에 운영 중인 정보자산뿐만 아니라 새로 도입되는 정보자산에 대해서도 위험분석을 실시한다.
② 정보자산에 대한 위험분석은 년 1회 실시하는 것을 원칙으로 한다.
③ 본교의 정보보호관리체계를 구성하는 환경의 중대한 변화가 발생했을 경우, 정보보안책임관의 결정에 따라 위험분석을 실시할 수 있다.

제8조(위험관리) ① 정보보안담당관은 위험분석 결과를 바탕으로, '위험수용기준(DoA)'에 따라 관리대상 위험을 식별한다.
② 정보보안담당관은 '위험수용기준(DoA)'에 따라 해당 위험을 감소, 수용할 것인지를 결정한다.

③ 정보보안담당관은 부서정보보안담당관과 협의하여 DoA 수준 초과 위험에 대하여 보호대책을 선정한다.
④ 정보보안담당관은 각 부서의 위험분석 및 단계별 위험관리방안을 참고하여 '정보보호 대책명세서'를 작성하여 관리한다.

제9조(사이버 보안진단의 날 운영) ① 정보보안담당관은 매월 셋째주 수요일을 '사이버보안 진단의 날'로 지정한다.
② 사이버보안진단의 날은 교직원의 보안인식을 제고하고, 해킹 및 정보유출을 사전에 예방하는데 목적이 있다.

제10조(정보보안 점검 활동) ① 정보보안책임관은 서버, 네트워크, 어플리케이션등 정보시스템에 대한 기술적 보안취약점 점검을 년 1회 이상 실시하고, 발견된 주요 취약점에 대한 조치를 수행한다.
② 정보보안책임관은 교직원이 본 정보보안 규정을 준수하고 있는지에 대해 년1회 이상 점검을 수행한다.
③ 정보보안 점검 활동을 위해 필요한 경우 외부 지식정보보호 전문업체를 통하여 점검을 수행할 수 있다.

제3장 정보보안 조직 체계

제11조(정보보안심사위원회) ① 정보보안 업무에 관한 중요한 사항을 심의·의결하기 위한 정보보안심사위원회는 정보지원센터규정 제2장 제5조에 의하여 정보화추진위원회 (이하 '심사위원회'라 한다)가 역할을 대신한다.(별표 1)
② 심사위원회는 다음 각·호의 사항을 심의·의결한다.
1. 정보보안 규정 제·개정에 관한 사항
2. 기타 이사장이 정보보안과 관련하여 필요하다고 인정하는 사항

제12조(정보보안 조직 구성) ① 본교 정보보안 업무를 원활히 수행하기 위하여 정보보안 조직을 구성하여 운영한다.
② 정보보안 조직은 다음과 같이 구성·지정한다.
1. 정보보안책임관 : 정보지원센터장
2. 정보보안담당관 : 정보지원센터팀장
3. 분임정보보안담당관(기술) : 정보지원센터 각 분야별 담당자
4. 부서정보보안담당관 : 부서(팀)의 각 팀장

제13조(정보보안책임관) ① 정보지원센터장은 보직에 임명됨과 동시에 본교 정보보안책임관으로 지정한다.
② 정보보안책임관은 정보보안업무를 총괄한다.

제14조(정보보안담당관) ① 정보보안담당관은 정보지원센터팀장으로 지정한다.
② 정보보안담당관은 다음 각 호의 임무를 수행한다.
1. 정보보안책임관의 업무를 보좌
2. 분임정보보안담당관 및 부서정보보안담당관들의 업무를 관리감독

3. 정보보안 관리규정, 시행규칙 제·개정 총괄
4. 정보보안 내·외부 감사 및 보안점검 총괄(교육과학기술부, 국가정보원, 행정안전부 등)
5. 기타 정보보안업무 전반에 관한 지도, 조정 및 기타 감독에 관한 사항

제15조(분임정보보안담당관) ①분임정보보안담당관은 다음 각 호의 임무를 수행한다.
② 분임정보보안담당관은 다음 각 호의 임무를 수행한다.
1.정보보안담당관 업무를 보좌하여 실무 수행
2.정보보안업무 분야별 연간 정보보안 활동계획 수립 및 이행
3.정보보안 관리규정 등 정보보안 문서에 대한 변경 관리
4.정보자산 목록에 대한 관리 및 통제
5.정보보안 기술을 숙지·적용
6.침해사고 대응체계 수립 및 이행
7.보안취약성, 위험 분석 및 보안대책 적용
8.정보보안 교육 계획 수립 및 이행
9.신규 정보시스템 개발 시 자체 보안대책 적용
10. 상위기관(교육과학기술부, 국가정보원, 행정안전부) 보안성 심의 요청
11. 정보보안 홍보활동(게시판, e-mail공지 등)
12. 정보보안시스템 보안정책 등록 및 변경
13. 정보통신망 및 정보자료 등의 보안관리 주관
14. 정보통신망 신·증설시 보안대책 수립
15. 정보시스템 보안관리 감독
16. 취약성진단 수행 및 관리 주관

제16조(부서정보보안담당관) ① 각 부서 및 부속기관 부서정보보안담당관은 부서별 담당팀장이 되며 팀장이 없는 경우 선임팀원을 지정한다.
② 부서정보보안담당관은 다음 각 호의 임무를 수행한다.
1. 부서(팀) 직원에 대한 정보보안 인식제고 활동
2. 부서(팀) 보조기억매체 관리 및 이동식 저장장치 관리
3. 부서(팀) 중요문서, 개인정보 관리 감독
4. 부서(팀) PC 보안관련 사항
5. '사이버·보안 진단의 날' 부서(팀) 진단 결과 취합 및 보고
6. 침해사고 발생시, 침해사고대응팀 구성원으로 포함되어 활동
③ 각 처의 처장은 부서(팀)의 부서정보보안담당관을 지정하고, 정보보안책임관에게 보고해야 하며, 변경 시에도 보고해야 한다.

제4장 정보자산 관리

제17조(정보자산 관리 유형) ①분임정보보안담당관은 다음의 자산에 대한 최신 현황을 관리해야 한다.

1. 서버(스토리지)
2. 네트워크, 정보보안시스템
3. 어플리케이션(소프트웨어)
4. PC, 노트북, 보조기억매체(USB, 외장형하드디스크)
5. 부대설비(항온항습기, UPS)
6. 기타 정보자산 관리를 위해 필요하다고 판단되는 자산

② 경영지원팀은 다음의 자산에 대한 최신 현황을 관리해야 한다.

1. 디지털 OA기기
2. 문서정보, 비밀취급 관련 문서
3. CCTV 관련 장비 및 설비
4. 기타 정보자산 관리를 위해 필요하다고 판단되는 자산

③ 시설관리팀은 다음의 자산에 대한 최신 현황을 관리해야 한다.

1. 물리적 시설(소화설비, 냉.난방 설비, 비상발전기 등)
2. 출입통제 설비
3. 기타 정보자산 관리를 위해 필요하다고 판단되는 자산

제18조(정보자산 식별) ① 분임정보보안담당관은 정보시스템과 관련된 정보자산들에 대해서는 총괄책임을 지고 부서정보보안담당관은 각 팀,·처별로 정보자산을 관리한다.

② 분임정보보안담당관은 정보자산 식별 및 분류 작업을 수행하며 정보자산의 소유자, 관리자, 사용자 및 정보자산 보호등급을 정의하고 정보자산에 대한 목록을 관리하도록 한다.

③ 부서정보보안담당관은 분임정보보안담당관의 위임에 따라 대상 정보자산들을 관리하여야 하며, 정해진 관리 및 운영절차에 따라 권한 있는 사용자만이 접근하여 사용할 수 있도록 보안 관리를 수행한다.

제19조(정보자산 목록 유지 및 관리) ① 분임정보보안담당관은 정보자산의 중요도, 용도, 소유자, 관리자 등을 포함하여 '[별지 제3호 서식] 정보자산목록'을 관리해야 한다.

② 분임정보보안담당관은 정보 자산의 도입, 추가 및 폐기로 인해 변경사항이 발생한 즉시 정보자산목록을 변경해야 한다.

③ 각 부서(팀)의 부서정보보안담당관은 소속부서의 정보자산현황을 작성하여 관리해야 하며, 해당 정보자산의 현황이 변경된 경우 소속부서의 정보자산 현황을 분임정보보안담당관에게 통보해야 한다.

제20조(자산의 중요도 평가 및 재검토) ① 분임정보보안담당관은 중요도 평가 기준을 수립하여 평가 기준에 따라 정보자산에 대한 중요도를 평가한다

② 분임정보보안담당관은 정보시스템 운영 환경의 변화에 따라 자산의 중요도 평가 기준을 변경할 수 있다.

③ 분임정보보안담당관은 주기적으로(년 1회 이상) 또는 자산의 용도 및 세부내역이 변경된 경우 자산의 중요도를 재검토하여 재분류 한다.

제21조(정보자산의 보안관리) ① 본교 내부직원 및 사업단을 포함한 외부 용역직원들은 본교 내부 정보자산을 개인의 목적으로 외부 반출 및 타인에게 전송 할 수 없다.
② 전자적 형태의 정보자산을 업무상 목적으로 전송 또는 배포하고자 하는 경우에는 승인된 정보기기 및 전송망을 사용해야 한다.
③ 정보보안담당관은 중요 정보자산에 대하여 비인가자의 무단접근을 통제할 책임을 지닌다.
④ 정보보안담당관은 관련 규정에 따라 정보자산이 적절하게 사용 및 운용되고 있는지 관리·감독한다.

제22조(정보자산의 폐기) ① 부서정보보안담당관은 정보자산의 폐기사유가 발생하면 정보보안담당관의 승인을 받은 후 폐기한다.
② 정보자산 재사용 또는 폐기 시 에는 다음 사항을 준수해야 한다.

구 분	출력물	보조기억매체
재사용	대외비 이상 정보의 재사용 (이면지 사용)금지	덮어쓰기 또는 신뢰할 수 있는 방법으로 데이터 완전 소거
폐기	문서 수거함이나 문서 파쇄기를 통한 폐기	물리적으로 매체의 완전 파괴

제23조(정보자산의 반·출입 관리) ①중요 정보자산의 외부 반출은 소속팀장의 사전 승인 후 반출한다.
1. 소속팀장은 감사를 위해 관련내용을 기록 관리하고, 저장매체 내의 데이터를 확인한다.
2. 소속팀장은 외부로 반출·입 되는 정보자산의 승인여부를 확인하고, 관련내용을 기록 관리한다.

제5장 정보보안 교육 및 홍보

제24조(정보보안 교육) ① 정보보안담당관은 전 교직원을 대상으로 년 2회 이상 정보보안 교육을 실시하여야 한다.
② 정보보안담당관은 정보보안 교육의 효율성, 전문성을 높이기 위해 외부전문가의 지원을 요청할 수 있다.
③ 분임정보보안담당관은 업무 전문성을 제고하기 위해 년 2회, 20시간 이상의 정보보안전문기관 교육 또는 정보보안 관련 세미나에 참석해야 한다.
④ 정보보안담당관은 외부 정보보호 전문교육과 세미나 참석을 위한 예산을 확보해야 하며, 관련 정보를 수집하여 해당 팀에 전파한다.

제25조(정보보안 홍보활동 수행) 분임정보보안담당관은 교직원에게 정보보안 인식을 제고할 수 있는 다음과 같은 내용을 활용하여 전자메일(e-mail), 교내 게시판 (홈페이지, 그룹웨어)등을 활용하여 홍보활동을 주기적으로 수행한다.
1.최신 보안사고 사례 및 동향 : 학기별 1회
2.의심스럽거나 출처가 불분명한 외부 전자우편 수신시 열람금지에 대한 공지
3.최신 바이러스에 대한 대응방안 : 필요시(최신 바이러스 발생시)

제6장 인적보안

제26조(채용시 보안) ① 교직원(계약직 포함) 채용 시에는 재직 중에 취득한 정보에 대한 보안을 유지하도록 '[별지 제4호 서식] 정보보안 서약서(교직원용)'를 작성해야 한다.
② 정보보안 서약서의 요구주체는 인사담당이며 제출된 서약서를 인사파일에 포함하여 안전하게 보관해야 한다.
③ 부서정보보안담당관은 신규 입사자에 대해서 내부 보안업무 규정, 정보보안관리규정, 개인정보보호 지침 등의 내용을 포함하여 정보보안 교육을 수행하고, 정보보안담당관은 교육수행 기록을 관리해야 한다.
제27조(보직변경 등 인사이동시) ① 보직변경 등 인사이동시 업무시스템에 대한 접근권한을 인사발령과 함께 신속하게 변경 또는 조정하여야 한다.
② 인사이동시 PC에 저장된 업무관련 파일은 삭제해야하며, 업무관련 파일이나 정보유출에 대한 책임은 해당PC 사용자에게 있다.
제28조(퇴직 및 계약해지시) ① 퇴직자는(계약직 포함)재직 중 보유한 모든 정보자산(사용PC, 보조기억매체, 업무자료 및 문서, 출입증 등)을 반환해야 할 의무가 있으며, 해당 부서장은 퇴직자의 정보자산을 팀에 귀속시킬 수 있도록 할 책임이 있다.
② 인사담당자는 퇴직자의 정보자산 반납 등을 확인한다.
③ 인사담당자는 퇴직 절차가 완료된 퇴사자에 대해 인사발령을 시행하고, 퇴직처리된 퇴사자의 계정이 삭제될 수 있도록 조치한다.
④ 분임정보보안담당관은 퇴직자에 의한 정보유출이 의심되거나 위험이 있는 경우 퇴직 처리 전에 사용자의 계정을 삭제 조치할 수 있다.

제7장 물리적 보안

제1절 보호구역 설정 및 통제

제29조(보호구역 설정) ① 본교의 물리적 보안을 위해 보호구역을 설정하여 관리한다.
② 보호구역은 그 중요도에 따라 통제구역, 제한구역, 일반구역으로 구분하며, 본교의 보호구역은 보안업무규정 제 33조에 의한 설정에 따른다.
제30조(통제구역의 통제) 통제구역으로 지정된 장소는 다음과 같은 통제를 적용한다.
1.출입통제 및 감시를 위해 출입통제시스템, 감시카메라(CCTV) 등을 설치한다.
2.비인가자의 출입이 제한되는 '통제구역' 표시를 하여야 한다.
3.통제구역의 출입권한 등록은 최소한의 인원으로 제한하고, 인가자 외의 인원 출입시 담당자 인솔하에 출입한다.
제31조(제한구역의 통제) 제한구역으로 지정된 장소는 다음과 같은 통제를 적용한다.

1.출입통제를 위해 출입통제시스템을 설치한다.
2.퇴직, 보직 변경된 교직원에 대한 불필요한 출입권한은 즉시 해제되어야 한다.
3.외부인의 제한구역 내 출입은 업무상 필요에 따라 결정되어야 하며, 담당자는 이들의 제한구역 내 활동은 지속적으로 관리·감독되어야 한다.

제32조(중간구역 마련) ①비인가자의 물리적인 불법접근을 방지하기 위해 필요 시 전산기계실 외부접점에 물품배달 및 적재를 위한 중간구역을 마련할 수 있다.
②중간구역의 접근을 위해서는 사전에 책임부서장의 승인을 받는다.
③반입물품은 중간구역에서 전산기계실로 들어가기 전에 잠재적인 위협이 없는지 점검한다.

제33조(장비 설치 및 보호) ①장비는 물리적·환경적 위협이나 위험, 또는 외부인의 접근으로부터 위험을 줄일 수 있도록 설치하고 보호한다.
②비밀정보를 다루는 원격터미널 또는 모니터는 비인가자가 외부로부터 투시가 될 수 없도록 배치하며, 특별한 보호가 요구되는 정보시스템은 격리된 장소에서 별도로 관리한다.
③비상시 사용될 백업장비 및 자산은 원격지에 보관한다.
④정보시스템은 화재 등에 대비하여 건물 외벽과 거리를 두고 배치하고, 가능한 취사시설, 화장실 등으로부터 거리를 두고 배치한다.

제34조(케이블 보안) ①전력선과 통신선이 절단 또는 손상되지 않도록 한다.
②모든 배선의 접점은 잠금 장치가 있는 박스 내에 설치한다.
③전력선은 간섭을 방지하기 위해 통신선과 격리하여 간섭현상을 방지한다. 격리에 대한 예외가 발생할 경우 시설관리 책임자의 허가에 따른다.
④인가 받지 않은 장비가 케이블에 연결되지 않도록 통제한다.
⑤정보시스템에 연결된 전력과 통신케이블은 가능한 매설하고, 매설이 어려울 경우 보호를 위한 방안을 마련해야 한다.
⑥공공지역이나, 위험이 예상되는 취약지역은 우회하여 케이블을 설치하도록 한다.

제35조(전원 공급) ①장비는 정전이나 기타의 전기적 장애로부터 보호한다.
②장비 제조업체에서 권장하는 규격에 맞는 적합한 전력이 공급되도록 한다.
③일시적인 전력중단이나 기타 전기적 이상으로부터 정보시스템의 가용성을 확보하기 위한 대체 전력 공급원을 확보한다.
④비상시를 대비하여 핵심 업무활동을 지원하는 정보시스템에는 UPS(무정전전원공급장치)를 설치한다.
1.전원공급시스템 관리부서의 장은 UPS의 적정용량 유지여부 등에 대한 정기점검을 월1회 이상 실시한다.
2.UPS의 고장 시에 취하여야 할 조치에 대해 비상계획을 수립한다.
⑤정전이 장기간 계속되어 전원을 공급할 수 있도록 비상 발전기를 설치하도록 한다.
1.전원공급시스템 관리부서장은 비상발전기에 대한 정기점검을 주1회 이상 실시한다.
2.비상발전기를 장기간 작동하기 위해 최소10시간 분의 연료를 확보한다.

3.비상전력공급 스위치는 비상시 전력을 신속히 차단할 수 있도록 장비가 설치된 장소의 비상구 근처에 설치한다.
⑥주동력선이 단절된 경우 비상등이 자동으로 켜지도록 설치한다.
⑦모든 건물에는 낙뢰로부터 보호 장비를 설치해야 하며, 특히 외부의 통신라인에 낙뢰방호필터를 설치한다.

제36조(장비 폐기 및 재사용) ①중요한 정보를 담고 있는 저장장치의 폐기 및 재사용 시에는 물리적으로 파괴하는 등 적절한 정보보호 대책을 적용한다.
②하드디스크와 같은 저장매체를 포함하는 모든 종류의 장비는 폐기되기 전에 저장매체로부터 중요한 데이터 및 라이센스가 있는 소프트웨어가 제거되었는지 확인한다.
③비밀정보를 포함한 보고서 등의 문서는 안전하게 파지 또는 소각하며, 하드 디스크, 광파일, 마그네틱 테이프 등의 매체를 폐기 처분하고자 할 때에는 인가된 안전한 방법을 사용하여 포맷 또는 삭제한 후 폐기한다.
④비밀정보 폐기와 관련된 기록은 향후 감사를 위해 유지한다.

제37조(보호구역 재해 대비) ①화재대비 소화기를 비치한다.
②적정한 온·습도를 유지하기 위한 항온항습기를 설치 및 운용하도록 한다.
③비상시에 대비하여 휴대용 조명기기를 비치한다.
④재해방지 설비에 대한 점검을 정기적으로 실시한다.
⑤ 기적인 재해대비 훈련에 대한 계획수립 및 훈련을 실시한다.
⑥재해복구를 위한 방안을 마련하도록 한다.

제38조(자료보안) ①비밀정보가 담긴 저장매체, 출력된 문서 또는 PC 등은 비인가자의 접근으로부터 보호한다.
②시설관리 책임부서장은 관할 보호구역 내에서 생성 및 유통되고 있는 종이문서와 비인가자에게 정보가 유출되는 것을 방지하기 위하여, 보호구역 내의 직원들을 대상으로 보안활동을 준수토록 한다.
③주요서류 및 이동형 저장매체(노트북, PDA, 외장형 하드디스크 등)를 사용하지 않을 경우, 시건 장치가 된 캐비닛이나 창고에 보관한다.

제2절 사무실 보안관리

제39조(출입통제) ①본교 각 부서(팀), 연구실, 연구소 등 출입문에는 출입통제 장치를 설치해야하며, 비인가자의 출입을 통제해야 한다.
②근무시간 이후에는 출입통제장치가 잠금상태로 되어 있어야 한다.

제40조(출입증 착용 및 관리) ①전 교직원은 출입시 신분증을 착용해야 한다.
②신분증을 분실 또는 도난당한 경우, 경영지원팀으로 즉시 통보해야 한다.
③교직원은 자신의 신분증이 분실되지 않도록 주의한다.

제41조(사무실 보안 활동) ①전 교직원은 책상 위에 주요 문서나 저장매체를 방치하지 않도록 한다.

②노트북은 퇴근 시 반드시 잠금장치 내에 보관 또는 시건장치를 하여 도난 및 분실에 유의한다.
③쓰레기통은 항상 사무실 내에 있어야 하며 쓰레기통에 주요 문서를 버리지 않는다.
④공용 캐비닛에는 정/부 책임자를 지정하고 퇴실 시 항상 잠근 후 열쇠는 안전한 곳에 보관하여야 한다.
⑤개인서랍은 잠금 장치를 설치하고 퇴근 시 항상 잠금을 확인한다.
⑥최종 퇴실자 또는 팀의 부서정보보안담당관은 매일 퇴근 전 사무실의 보안점검을 실시하고 보안점검 일지를 작성해야 하며, 팀의 부서정보보안담당관은 작성된 보안일지에 대하여 월별 주기로 확인을 수행한다.

제42조(사무기기 사용) ①전 교직원은 프린터로 출력되는 문서는 즉시 회수함으로써 출력물을 타인이 가져가게 하거나 프린터 주위에 출력물을 방치하지 않도록 한다.
②신원이 파악되지 않은 자에 의해 내부직원의 신상정보, 조직정보, 시스템정보 등을 묻는 전화를 받았을 경우 반드시 상대의 신원을 확인한고, 신원이 불분명한 상대와 전화 통화를 하는 경우 관련 정보를 제공해서는 않된다.
③팩스 사용 시 원칙적으로 문서 생성자 본인이 스스로 팩스를 전송하여야 하며, 전송되는 원본 문서는 즉시 회수하도록 한다.
④개인정보 등 중요정보가 포함된 문서의 팩스 전송을 금지한다.
⑤원칙적으로 문서 생성자 본인 스스로 복사하고, 원본문서는 즉시 회수한다.
⑥개인정보 등 중요정보가 포함된 문서의 스캔 파일은 사용 후 즉시 삭제 및 보관을 원칙적으로 금지한다.

제3절 전산기계실 보안관리

제43조(전산장비실 환경) ①전산기계실은 다른 업무 장소와 분리하여 물리적 보안성이 보장된 곳에 위치하여야 한다.
②전산기계실은 중요 정보통신장비 및 정보자료가 상존하는 곳이므로 차광, 환풍, 냉 · 온방등의 시설이 구축되어야 한다.
③전산기계실은 정보통신장비의 원활한 운영 · 관리를 위하여 필요한 공간이 충분히 확보되어야 한다.
④재난에 대비하여 열 감지기, 연기감지기, 누수감지기 등의 방화시설, 소화설비, 기타 방재설비를 적절히 보유해야 하며 항시 작동 가능한 상태로 유지해야 한다.
⑤전산기계실 운영 · 관리에 필요한 정보통신장비 및 도구 이외의 사물을 보관하거나 비치하지 않도록 통제, 감독 및 관리하여야 한다.
⑥항온·항습을 유지할 수 있는 설비를 설치하며, 항상 적정온도 및 습도를 유지하도록 한다.
⑦비인가 행위 적발, 전산기계실 물리적 감시를 위해 CCTV를 설치하여 운영할 수 있다.

제44조(출입권한 관리) ①전산기계실 출입권한은 전산관련 직원에 한하여 허가된다.
②전산기계실 출입권한이 신규로 필요로 한 경우 정보보안담당관의 승인 후, 해당 인원의 출입권한을 등록한다.
③정보보안담당관은 퇴사 및 보직변경으로 인하여 전산기계실 출입권한의 변동이 발생한 경우 우선적으로 해당인원의 전산기계실 출입권한을 삭제한다.
제45조(외부인 출입통제) ①전산기계실은 비인가자의 출입을 통제하여야 하며 '[별지 제5호 서식] 기계실 출입관리 대장'을 비치하여 모든 출입자를 기록해야 한다.
②외부인이 전산기계실을 출입하는 경우 출입권한자가 동행하도록 한다.
③외부인의 전산기계실 출입 시 목적, 출입 및 퇴실시간 등을 출입관리대장에 기록하고 동행한 출입권한자가 확인서명을 하여야 한다.
④정보보안담당관은 매월 출입관리대장을 확인하고, 출입관리대장의 보관은 1년 이상으로 한다.
제46조(정보통신장비의 반입 · 출입 통제) ①정보보안담당관은 정보통신장비의 수리, 교체 및 대체, 대여 등으로 정보통신장비가 반입 · 반출되는 경우, 정보통신장비의 반입·반출을 통제하여야 한다.
②정보보안담당관은 정보시스템 장비의 반입 · 반출을 하는 경우 관련 기록을 '[별지 제6호 서식] 반입 · 반출 관리대장'에 기록한다.
③장비 반출일 경우 해당 장비내의 저장매체에 저장된 정보가 복구 가능하지 않도록 삭제되었는지 확인한 후 장비를 반출 하도록 한다.
제47조(촬영금지) 전산기계실 내에서의 휴대폰, 디지털카메라 등을 이용한 촬영은 금지 한다. 단, 업무적으로 필요한 경우 정보보안담당관의 승인을 득해야한다.

제8장 PC 보안

제48조(PC 관리책임자 · 취급자 지정) ①개인용컴퓨터(노트북 포함)에 대한 총괄책임자는 정보보안담당관으로 하며, 부서별 관리책임자는 해당 부서의 팀장 (팀장이 없는 경우는 선임팀원)으로 하고, 취급자는 해당 PC 사용자로 한다.
제49조(PC 보안관리) ①부서별 관리책임자는 팀내의 PC 및 노트북 운영 현황을 '[별지 제7호 서식] PC관리대장'에 사용자를 등록하여 관리해야 한다.
②개인이 사용하는 PC의 정보보안 관리에 대한 1차 책임은 PC 사용자에게 있으며, PC사용자는 다음의 보안대책을 강구해야 한다.
1.장비별, 자료별, 사용자별 비밀번호 사용
2.CMOS(부팅), 로그인 및 화면보호기에 각각 비밀번호 설정
3.10분 이상 PC 작업을 중단 시 비밀번호가 적용된 화면보호기 작동
4.바이러스 백신S/W 설치
5. P2P, 원격PC 관리프로그램 등 업무와 무관하거나 보안에 취약한 프로그램의 사용 금지

③공유폴더는 사용하지 않는 것을 원칙으로 하며, 업무상 목적으로 필요한 경우에는 반드시 공유폴더에 패스워드를 설정하고, 사용이 완료된 후에는 공유 설정을 제거해야 한다.
④노트북은 도난 및 분실을 예방하기 위해 물리적 시건장치를 설치하여 사용해야 하며, 외부 출장 시에도 책상위에 방치하지 말고 시건장치를 설치한다.
⑤모든 PC사용자(노트북 포함)는 적법한 절차를 거쳐 취득한 정품 소프트웨어만을 사용해야 하며 사용권한이 없거나 임의로 복제된 불법소프트웨어를 설치해서는 안된다.
제50조(PC 비밀번호 설정 및 관리) ①PC사용자(노트북 포함)는 CMOS(부팅) 로그인, 화면보호기 패스워드를 설정하여 비인가자의 접근을 통제하여야 한다.
②PC에서 사용하는 비밀번호는 다음 각 호 사항을 반영하여 특수문자가 포함된 8자리 이상으로 정하고, 분기 1회 이상 주기적으로 변경 사용하여야 한다.
1.사용자계정(ID)과 동일하지 않은 것
2.개인 신상 및 부서명칭 등과 관계가 없는 것
3.일반 사전에 등록된 단어는 사용을 피할 것
4.동일단어 또는 숫자를 반복하여 사용하지 말 것
5.이전에 사용된 비밀번호는 재사용하지 말 것
6.동일 비밀번호를 여러 사람이 공유하여 사용하지 말 것
7.관리자계정과 사용자계정의 비밀번호를 다르게 부여
8.초기 할당된 임시 비밀번호는 사용자 로그인 후 즉시 변경
제51조(모바일 컴퓨터에 대한 보안) 사용자가 노트북, 넷북, 스마트폰 등과 같은 모바일 컴퓨터를 이용하는 경우에는 다음의 사항을 준수한다.
①모든 모바일 컴퓨터는 일반 PC보안 사항을 준수한다.
②모바일 컴퓨터는 부팅 패스워드가 지정되어 있어야 하며, 저장되어 있는 중요 정보는 암호화하여 저장한다.
④모바일 컴퓨터에 저장되어 있는 중요정보는 백업을 수행한다.
⑤모바일 컴퓨터는 도난을 당하지 않도록 주의한다.
제52조(PC 및 노트북 반 · 출·입 관리) ①PC(노트북)의 반출 또는 반입 시, 해당 부서별 반출·입 내역을 '[별지 제8호 서식] 보조기억매체(전산장비 포함)반출·입 대장'에 기록해야 한다.
②PC 사용자는 반출된 PC(노트북) 반입시 바이러스 백신프로그램으로 바이러스 및 악성코드 감염여부를 점검한다.
③개인소유의 PC(노트북 등)는 본교 내부로 반입 또는 반출하여 사용해서는 안된다. 다만, 부득이한 경우에는 부서장의 승인을 받은 후 반입 또는 반출할 수 있다.
④PC에 설치 또는 부착된 하드웨어를 임의로 변경, 제거하거나 본교 외부로 반출해서는 안 된다.
제53조(PC 유지보수) ①PC 유지보수는 인가된 직원(또는 외부업체 직원)에 의해서만 수행되어야 한다.

②PC 또는 PC내 하드웨어를 유지보수(교체 · 반납 · 폐기)를 위해 본교 외부로 반출할 경우 다음의 보안대책을 강구한다.
1.PC에 저장된 데이터가 복구가 되지 않도록 삭제 또는 하드디스크를 분리
2.PC 수리자에게 [별지 제9호 서식] '정보보안 서약서(외부자용)' 작성 유도

제54조(바이러스 관리) ①본교에서 사용 중인 모든 PC에는 바이러스백신 S/W를 설치하고 최신의 바이러스 백신엔진으로 유지해야 한다.
②신규 보급하는 PC는 백신S/W를 사전에 설치하여 보급하도록 하고, PC 운영체제 재설치 등의 작업 후에도 백신S/W를 설치하여야 한다.
③모든 사용자는 바이러스가 감염된 경우 네트워크 접속을 차단하고 백신S/W로 바이러스를 치료하고, 정보통신보안담당관에게 보고해야 한다.

제55조(네트워크이용 절차) ①내부사용자가 네트워크를 사용하기 위해서는 다음을 따른다.
1.각 팀장은 팀의 전부 및 일부의 이전, 신규 네트워크 증설시 정보보안담당관에게 통보한다.
2.정보보안담당관은 보안사항 미 준수 사용자의 네트워크 사용을 차단할 수 있다.

제56조 (IP관리) ① 팀 · 처에서는 할당된 IP만을 사용한다.
② 퇴사자 및 직무 순환 이동자는 할당받은 IP를 반납한다.

제57조(유해 소프트웨어에 대한 통제) 공식적으로 인가되지 않은 프로그램의 사용은 바이러스, 트로이 목마와 같은 악성 코드들이 포함되어 있을 가능성이 높으며 이러한 악성코드 들은 조직의 중요 정보 노출, 파괴 등을 유발할 수 있으므로 사용자는 프로그램 사용에 대해 다음 사항을 준수한다.
①사용자는 업무에 불필요 또는 불법 소프트웨어를 사용하지 않고, 정품 소프트웨어만을 사용한다.
②불확실하거나 출처가 명확하지 않은 파일, 신뢰할 수 없는 네트워크로부터 획득된 파일은 사용하기 전에 바이러스 검사를 한다.
③사용자는 월 1회 악의적인 바이러스, 불법 소프트웨어 등이 설치되어 있는지를 점검한다.

제9장 E-mail, 인터넷 보안관리

제58조(E-mail 사용의 제한) ①E-mail 사용자는 부서장의 허가를 받지 않은 정보 또는 외부에 공개할 수 없는 내부 정보를 외부에 발송하지 않는다.
②스팸메일 등 불법 메일 등을 송신하거나 타 직원의 E-mail 계정을 도용할 수 없다.
③정보시스템 자원의 낭비를 초래하는 스팸메일, 반복메일 등은 전송 및 배포를 금지한다.
④모든 E-mail 사용자는 제3자의 지적재산권, 저작권을 침해하는 내용, 명예훼손, 사기, 바이러스 유포 등의 불법적인 행위에 대한 내용을 E-mail에 포함하지 않는다.

⑤타인의 E-mail 내용 및 비밀번호를 중간에서 전자적으로 도청하지 않는다.
⑥E-mail이 암호화되지 않은 경우, E-mail 사용자들은 신용카드번호, 패스워드 등 개인의 중요한 정보를 E-mail 내용에 포함시켜 보내지 않아야 한다.
⑦내부정보를 외부로 송신하기 위해서는 사전에 그 타당성에 대해 해당 전결권자의 승인을 득해야 하며, 내용의 중요성에 따라 선택적으로 암호화하여 전송한다.
⑧직원은 외부의 네트워크 주소로 E-mail을 자동전달(Forwarding)해서는 안 된다.

제59조 (E-mail 이용 시 업무처리 절차) ①E-mail 계정의 신청/삭제는 계정신청, 삭제의 절차를 통해 처리한다.
②E-mail 관리 원칙
1.한 명의 직원 당 1개의 E-mail 계정 부여를 원칙으로 한다. 단, 업무 목적상 필요한경우 업무용 계정을 별도로 신청할 수 있다.
2.직원의 E-mail 주소 디렉토리는 공개적으로 접근하지 못하도록 조치한다.
③개인용 E-mail 사용 기준
1.E-mail에 첨부파일이 있을 경우 악성 프로그램 설치여부를 확인한다.
2.E-mail 패스워드는 분기별 1회 변경한다. E-mail 패스워드는 추측 가능하지 않도록 설정하고 타인에게 공개하지 않는다.
3.송신자, 메일제목, 첨부파일 등이 불확실한 경우 메일을 바로 삭제한다. 출처가 분명하지 않거나 메일내용과 상관없는 첨부파일이 있는 경우 악성 프로그램일 가능성이 높으므로 바로 삭제한다.
4.무분별한 사이트 가입을 지양하고 공개된 게시판 등에 개인정보 노출을 자제한다.
④업무용 E-mail 사용 기준
1.E-mail을 통한 업무자료 수발신은 내부 인트라넷시스템을 사용한다.
2.외부 사설메일(Naver,Daum, MSN 등)을 이용한 업무자료 송수신은 하지 않는다. 단, E-mail 시스템 장애 발생 시 예외로 할 수 있다.
3.E-mail로 발송한 자료를 규정상 정식 문서로 인정하지 않는 경우 정식문서가 아님을 나타내는 문구를 삽입하여 발송 한다.
4.본교외의 장소에서 웹 메일을 사용할 경우 접속에 관한 관리를 철저하게 한다.
⑤ 바이러스 점검
E-mail을 통해 유포되는 바이러스로부터 내부 정보자산을 보호하기 위하여 받은 E-mail에 대한 바이러스 검사를 수행한다.

제60조(E-mail 관리 및 보존) ①E-mail 자료의 보존 시 첨부파일을 포함하여 수발신된 모든 자료를 저장한다.
②스팸메일로 분류되어 스팸메일 차단시스템에 의해 차단된 메일의 경우, 스팸메일임이 확실하다고 판단되는 메일은 자동으로 삭제한다.

제61조(비정상적 메일(대량 스팸메일, 바이러스 첨부메일 등) 대응 절차) E-mail 시스템 관리자는 비정상적인 메일의 유입을 차단하기 위해 다음 각 항과 같은 절차에 따라 업무를 수행한다.

①대량의 스팸메일 혹은 바이러스가 첨부된 메일, 네트워크의 마비상태를 초래할 수 있는 메일 등에 대한 모니터링을 할 수 있다.
②대량의 스팸메일이나 비정상적인 메일의 유입이 탐지되는 경우, 해당 메일의 유입을 차단하고, 스팸메일 차단시스템에 차단정책을 추가한다.
③바이러스가 첨부되거나 네트워크의 마비를 불러올 수 있는 비정상적인 메일의 유입이 확인된 경우, 메일서버 등을 이용하여 E-mail 사용자에게 해당 메일의 열람을 금지하는 등의 대응방안을 공지한다.
④비정상적인 메일의 유입에 대해 '제16장 침해사고 대응'에 따라 조치한다.

제62조(인터넷 접속에 대한 보안) ①다음의 사이트는 접속을 금지한다.
1.유해 사이트
2. P2P 사이트
3.증권관련 사이트
4.기타 접속 금지의 필요성이 인정되는 사이트 등
②신뢰할 수 있는 웹 사이트를 방문한 경우를 제외하고는 자바와 Active-X 기능의 사용에 주의한다.
③웹 브라우저가 제공하는 팝업(Pop-up) 윈도우에 'Yes' 로 하기 전에 그 내용을 상세히 파악함으로써 자바 스크립트, Active-X 공격 등에 노출될 수 있는 가능성을 줄인다.
④악성 자료를 포함하는 사이트를 발견했을 경우, 해당 사이트의 URL을 정보보안담당관에게 통보하고, 정보보안담당관은 조사 후 유해사이트차단시스템 등의 보안시스템을 사용하여 해당 사이트의 접근을 차단한다.
⑤웹 사이트 회원으로 가입할 경우 본교 공식 메일주소를 사용하지 않아야 한다. 필요에 의해 메일주소를 등록할 경우 별도의 외부 메일계정을 사용한다
⑥정보보안담당관은 PC에서 음란・도박・증권 등 업무와 무관한 인터넷 사이트 접근을 차단 한다.

제10장 보조기억매체 관리

제63조(보조기억매체 등록 및 관리) ①정보보안담당관은 보조기억매체를 안전하게 관리하기 위하여 각 부서별 보조기억매체 관리책임자(이하 '관리책임자'라 한다)를 지정하여 운영하여야 하며, 각 부서의 부서정보보안담당관을 관리책임자로 지정한다.
②관리책임자는 보조기억매체를 일반용, 비밀용(대외비 포함) 및 공인인증서용으로 구분하여 '[별지 제10호 서식]보조기억매체 관리대장'에 등록한 후에 사용 한다.
③관리책임자는 사용자가 보조기억매체를 2항과 같이 등록된 경우에만 사용하고 업무목적 이외에 사적인 용도로 사용할 수 없도록 해야 한다. 다만, 공인인증서용에 한하여 등록 후 개인소지 및 사용을 허가할 수 있다.
④관리책임자는 분기1회 이상 보조기억매체의 수량 및 보관 상태를 점검하고 '[별지

제11호 서식]보조기억매체 점검대장'에 확인·서명하여야 한다.
⑤보조기억매체를 사용하는 부서에서 보조기억매체를 반출·반입할 경우'[별지 제8호 서식] 보조기억매체(전산장비 포함)반출·입 대장'에 기록해야 한다.
제64조(비밀용 보조기억매체 관리) ①관리책임자는 보조기억매체에 대외비 이상 비밀 자료를 보관하고자 하는 경우 다음 각 호와 같이 관리하여야 한다.
1.비밀관리기록부에 등재·관리하며 이중 캐비넷 또는 금고에 보관
2.비밀 작업 및 보관을 하는 경우 그 작업을 완료하거나 일시 중단할 때에는 PC에서 즉시 분리
3.비밀등급별로 각각 보조기억매체를 마련하여 하나의 보조기억매체에 등급이 다른 비밀 또는 대외비를 혼합하여 보관금지
②관리책임자는 보조기억매체를 파기 등 불용처리하거나 비밀용을 일반용 또는 다른 등급의 비밀용으로 전환하여 재사용할 경우 저장되어 있는 정보가 복구되지 못하도록 삭제 조치를 하여야 한다.

제11장 정보시스템 저장 매체 삭제

제65조(정보시스템 저장자료 삭제 책임) ①개인에게 지급된 PC, USB등의 정보시스템 및 저장매체에 저장된 업무자료 및 정보는 사용자 본인 책임하에 삭제하여야 한다.
②홈페이지 등 각 부서가 공통적으로 사용하는 정보시스템은 정보보안담당관 책임하에 저장자료를 삭제하여야 한다.
제66조(정보시스템 저장자료 삭제) 정보시스템 저장매체에 저장된 자료를 삭제할 경우는 다음과 같다.
1.정보시스템의 사용연한이 경과하여 폐기할 경우
2.정보시스템 무상 보증기간 중 저장매체 또는 저장매체를 포함한 정보시스템을 교체할 경우
3.정보시스템의 임대기간이 만료되어 반납할 경우
4.고장 수리를 위한 외부로 반출 할 경우
5.기타 PC, USB등 정보시스템 및 저장매체 사용자 변경 등으로 저장자료 삭제가 필요하다고 판단되는 경우

제12장 서버 보안

제67조(정보시스템 보안관리) ①정보보안담당관은 정보통신시스템(정보통신망 포함)의 효율적인 보안관리를 위하여 분임정보보안담당관을 두어 정보통신시스템별로 관리 운영하여야 한다.
②시스템관리자는 각종서버・PC・정보통신장비 등 정보통신시스템이 비인가 자에게 불필요한 서비스를 허용하지 않도록 보안기능을 설정하여야 한다.

③시스템관리자는 보안도구를 이용하여 년1회 이상 정보통신시스템의 보안취약성을 진단하여야 한다.
④시스템관리자는 주기적으로 불필요한 포트의 사용여부를 점검하여, 불필요한 포트 사용이 확인되는 즉시, 해당 포트를 삭제하는 등의 보안조치를 수행한다.
⑤중요정보를 취급하는 정보시스템은 관리자 권한으로 시스템에 접근하는 경우, 지정된 IP에서만 접근할 수 있도록 한다.

제68조(서버 시스템의 설치) ①서버시스템 설치 아래의 각호의 사항을 준수하여야 한다.
1.신규 시스템을 도입 시 시스템 보안설정, 서버백신, 장애관리 등의 도구를 설치해야 한다.
2.시스템관리자는 신규로 도입 설치되는 서버 시스템에 서버 취약점 점검도구를 설치하여 시스템 및 OS의 취약점 점검을 수행하며, 점검결과 발견된 취약점에 대해 발주부서에 통보하여 조치토록 한다.
3.시스템관리자는 신규 시스템 설치 및 변경 사항을 정보자산 관리목록에 갱신해야 한다.
②소프트웨어 설치 아래의 각호의 사항을 준수하여야 한다.
1.발주부서 담당자는 서버에 설치된 소프트웨어의 현황을 목록으로 만들어 관리하며 변경 시 현황을 수시로 업데이트 한다.
2.서버 시스템에 설치되는 소프트웨어는 정보보안담당관의 승인을 얻은 후 설치한다.
3.발주부서 담당자는 소프트웨어 설치작업 후 해당 서버의 소프트웨어 설치현황 목록에 추가한다.
4.업무통제나 시스템을 무력화 할 수 있는 유틸리티의 사용은 통제한다.
③소프트웨어 설치 시 아래의 각호의 사항은 제한하여야 한다.
1.서버에는 업무 목적 외의 불필요한 프로그램을 설치할 수 없다.
2.불법 소프트웨어는 설치할 수 없다.
3.원격관리 소프트웨어 등 서비스 관리 목적상 불가피하게 설치해야 할 필요성이 있을 때에는 자체 보안대책을 마련하여 정보보안담당관에게 승인을 얻는다.
④시스템관리자는 파일시스템을 구성할 때 시스템 데이터와 일반 데이터를 논리적 또는 물리적으로 분리하여 설치한다.

제69조(보안설정 적용) ①시스템관리자는 주기적인 패치 및 보안 설정을 적용한다.
②모든 서버는 로그인을 허용하기 전에 다음과 같은 보안권고문을 공지한다.
“부당한 방법으로 정보통신망 및 정보시스템에 접속하거나 정보를 삭제, 변경, 유출하는 자는 관련 법령에 따라 처벌을 받게 됩니다.”
③서버 로그인 시 OS버전, 서비스정보 등의 취약점 유추가 가능한 정보가 누출되지 않도록 설정한다.
④시스템의 보안 설정된 정보와 로그는 임의적으로 삭제되지 않도록 한다.

제70조(시스템 접근 기록 관리) ①시스템 접속기록은 접속일시, 사용자 ID, 접속 IP

등이 포함되어야 한다.
②시스템 접근 및 사용에 대한 책임 추적성을 확보하기 위하여 시스템 가동 및 종료, 설정 변경, 중요파일 접근로그, 관리자 계정 명령어 사용내역 등의 로그를 기록한다.
③사고발생시 책임추적이 가능하도록 시스템 접근기록을 3개월 이상 보관하여야 한다.
④정보보안담당관의 사전 승인이 없는 한 모든 시스템 로그에 대해 비인가자가 접근할 수 없으며 시스템 로그를 비인가자가 열람하거나, 훼손하는 경우 심사위원회를 통해서 처벌하거나, 외부자의 경우 민.형사상 법적 조치를 취한다.
⑤시스템관리자는 정기적으로 시스템 접근기록을 검토하여 비인가자의 접속시도, 정보 위·변조 및 무단삭제 등의 의심스러운 활동이나, 침입흔적 발생시 정보보안담당관에게 보고하고 조치를 취해야 한다.
제71조(계정 및 패스워드 관리) ①시스템관리자는 사용자계정의 등록・변경・폐기시 정보보안담당관에게 그 결과를 보고하여야 한다.
②시스템관리자는 3개월 이상 미사용 계정, 사용자의 퇴직 또는 보직변경 등으로 사용하지 않는 사용자계정에 발생할 경우 이를 신속히 삭제하여야 한다.
③5회에 걸쳐 사용자인증 실패 시 정보통신시스템 접속을 중지시키고 비인가자 침입여부를 확인 점검하여야 한다.
④패스워드는 숫자와 문자, 하나 이상의 특수문자 등으로 8자리 이상으로 정하고 분기 1회 이상 주기적으로 변경 사용하여야 한다.
제72조(권한관리) ①서버 내 정보에 대한 접근 권한은 정보보안담당관이 검토 후 부여한다.
②시스템관리자는 개인의 계정으로 접속한 후에 관리자 권한을 획득한다.
③일반사용자는 다른 사용자의 홈디렉터리 혹은 시스템 관리에 관한 파일 혹은 디렉터리에는 접근할 수 없도록 제한한다.
④일반사용자가 서비스 중지 등을 일으킬 수 있는 시스템 명령어 혹은 컴파일러를 사용할 수 없도록 제한한다.
⑤일반사용자는 시스템관리자 및 정보보안담당관의 사전 승인 없이 운영체제의 접근통제를 우회할 수 있는 프로그램을 사용할 수 없도록 제한한다.
⑥관리자 권한 등의 중요 권한을 일반 사용자에게 생성해주지 않는다.
⑦슈퍼유저 계정을 이용한 FTP 접속권한을 해제한다.
⑧불필요한 RPC통신 권한을 해제한다.
제73조(접근통제관리) ①업무상 접속할 필요가 있는 사용자를 파악한 후 보안도구를 이용해 IP주소 기반의 접근제어를 한다.
②시스템관리자는 서버가 정상적으로 동작하지 않을 경우 정상적으로 동작될 때까지 사용자의 접근을 제한할 수 있다.
③시스템관리자는 비인가자의 불법적인 접근 및 서비스 중지 등을 예방하기 위해 업무적으로 불필요하거나, 침해의 위협이 있는 네트워크 서비스를 제공하지 않는다.

제74조(원격접근 보안관리) ①일반사용자가 서버에 접속할 경우 반드시 사용자 계정과 패스워드 또는 보다 강화된 인증방법을 적용하여 접근 가능하도록 한다.
②인증방법은 서버시스템이 제공하는 서비스 내용과 중요도에 따라 결정하며 다음과 같은 방법 등을 사용한다.
1.사용자 계정, 패스워드
2.음성, 지문, 홍채 등 신체적 특성을 이용한 인증
3.비밀번호 발생기, IC카드 등 소지형 인증
4.공개키 기반 인증 (PKI)
③인증 서버를 구축할 경우에는 인증 서버의 장애로 인한 서비스 중단 등이 발생하지 않도록 병렬구성을 원칙으로 한다.
④중요 서버에 접근 시에는 SSH(Secure Shell) 등의 암호화된 통신 프로토콜 사용을 원칙으로 한다.
⑤로그인 화면에서는 로그인 관련 정보만 표시한다. 조직이나 운영체제, 네트워크 환경, 내부적인 사항과 같은 정보는 로그인이 성공적으로 이루어진 후에 표시되도록 한다.
⑥일반사용자가 시스템에 로그인 실패 시 시스템 침해의 원인이 될 만한 정보를 일반사용자에게 보여주지 않도록 조치한다.
⑦연속적으로 5회 이상 패스워드를 잘못 입력할 경우 세션을 차단 후 분임정보보안담당관에게 해당 사실을 통지하고 비인가자의 침입여부를 확인 및 점검해야 한다.
⑧사용자가 서버 로그인에 성공하였을 경우 가장 최근에 성공적으로 접속한 시간, 날짜, 접속IP 등의 정보를 로그로 기록한다.
제75조(관리자 보안 이행사항) ①서버에 접속한 후 일정시간(20분 이하) 동안 어떤 입력도 일어나지 않으면 자동적으로 로그오프 시키거나 세션을 중단시키는 것을 원칙으로 한다. 단, 개발 업무나 서버 운영상 필요성이 인정되는 경우 예외로 할 수 있다.
②통제구역 이외의 장소에 설치된 서버는 시스템관리자 및 사용자가 5분 이상 자리를 비울 경우 패스워드가 설정된 화면보호기가 작동되도록 하거나 로그오프하여 비인가자가 접근할 수 없도록 한다.
제76조(외부망에 대한 접근보안관리) 시스템관리자 등 정보시스템관리자는 정보시스템을 외부에서의 네트워크를 통해 원격으로 접속하여 정비하는 것을 원칙적으로 금지하여야 한다. 다만, 부득이한 경우에는 아래의 각호에 해당하는 보안대책을 강구하고 정보보안담당관과 협의한 후 한시적으로 허용하여야 한다.
1.원격접속 수행자에게 임시 접근권한 부여
2.접근권한의 사용시간 명시, 시간경과 후 접근권한 삭제
3.원격정비 시스템의 IP사전 파악, 지정된 시스템에서만 수행
4.원격시스템과의 통신정보를 점검하여 실행코드에 악성코드 유입 방지
5.원격정비를 수행할 때 대상 정보시스템을 내부망과 분리
6.원격정비기록을 유지, 정비결과 서버관리자에게 보고

7. 원격 정비자가 네트워크를 통해 원격지 컴퓨터 파일을 자신의 컴퓨터 파일처럼 접근하여 작업할 수 있도록 하는 등 해킹에 취약한 방식으로 원격정비 금지

제77조(패치 및 변경 통제) 패치나 시스템 파라미터(IP, 사용자 계정, 권한설정, 환경설정값 등)를 변경할 시에는 그와 관련된 모든 사항(변경값, 변경사유, 승인자, 시행자, 일자, 해당 서버 등)에 대한 증적을 남긴다.

제78조(백신설치 및 운영) ①시스템관리자는 윈도우 시스템의 경우 최신버전의 백신을 설치하고 운영하여 컴퓨터바이러스 등에 의한 해킹 및 사이버테러에 대응해야 한다.

②출처, 유통경로 및 제작자가 명확하지 않은 응용프로그램은 바이러스 검색 프로그램으로 진단한 후 사용한다.

③바이러스 서버를 설치하여 외부에서 들어오는 메일 등에 대하여 사전 검색을 한다.

④정기적으로 일제점검이 가능하도록 특정일을 지정하여 점검을 실시한다.

⑤중요 실행파일은 읽기 전용으로 속성을 변경하여 관리한다.

⑥최신의 검색 프로그램을 활용하고 최신의 패치프로그램 배포 시 즉시 보정작업을 실시한다.

⑦바이러스 감염 시 피해를 최소화할 수 있도록 아래와 같이 조치한다.

1.감염사실을 부서정보보안담당관에게 신속히 신고

2.부서정보보안담당관은 정보보안담당관 신속히 보고

3.감염된 시스템 사용 중지

4.백신프로그램을 이용하여 바이러스 퇴치

5.원인분석 후 예방조치 권고사항의 수행

제79조(웹서버 등 공개서버 관리) ①외부인에게 공개할 목적으로 설치되는 웹서버 등 각종 공개서버는 내부망과 분리하여 운영하고 보안적합성이 검증된 침입차단시스템을 설치하는 등 보안대책을 강구하여야 한다.

②서버에 접근할 수 있는 사용자계정을 제한하며 불필요한 계정은 삭제하여야 한다.

③홈페이지 게재내용은 자체 해당팀장의 심의를 거쳐 비밀내용 등 비공개 자료가 포함되지 않도록 해야한다.

④공개서버는 업무서비스를 제외한 모든 서비스 및 시험·개발도구 등의 사용을 제한하도록 보안기능을 설정하여야 한다.

⑤공개서버의 보안취약성을 수시로 점검하고 자료의 위·변조, 훼손여부를 확인해야한다.

⑥보안사고에 대비하여 서버에 저장된 자료의 철저한 백업체계를 수립·시행하여야 한다.

⑦공개서버를 통해 개인정보가 유출, 위·변조되지 않도록 보안조치를 해야 한다.

제80조(취약점 점검) ①시스템관리자는 시스템 불법 접근 및 해킹 프로그램(백도어 및 스파이웨어 등)의 설치여부 점검 등 일상적인 보안활동을 수행한다.

②정보시스템에 대한 종합점검은 연 1회 이상 실시하고, 시스템의 변경, 외부 시스템

의 이관 및 신규 시스템도입 등 필요시 수시점검을 실시한다.
1.정보보안담당관은 종합점검 계획을 수립하여 시행한다.
2.분임정보보안담당관은 수시점검을 실시하고, 종합점검 및 수시점검 시 발견된 취약점에 대해 정보보안담당관에게 보고한다.
3.정보보안담당관은 단기 조치가 어려운 취약점에 대하여 그 사유를 기록, 관리한다.
4.취약점 조치를 위하여 관련 팀 및 업체의 협의가 필요할 경우에는 부서정보보안담당관 등 관련 소관 부서담당자 및 업체 직원을 소집하여 조치방안을 강구한다.
5.분임정보보안담당관은 취약점 점검대상, 기간, 주요 점검항목, 점검결과 및 조치 사항을 포함하는 '취약점 점검 결과보고서'를 작성하여 이력을 관리한다.
6.분임정보보안담당관은 외부시스템 이관 시 서버, 응용시스템 등 분야별 수시점검 결과 발견된 취약점에 대한 보완여부를 확인한다.

제81조(시스템 성능관리 및 유지보수) ①시스템관리자는 서버의 자원오용을 방지하기 위해 다음 지침을 주기적으로 점검관리하고 임계치를 초과할 경우 지속적으로 모니터링 해야 한다.
1.CPU사용률 임계치 : 80%~85% 이상일 경우 지속적인 모니터링
2.메모리 사용률 임계치 : 80%~85% 이상일 경우 지속적인 모니터링
3.디스크 사용률 임계치 : 70% ~ 75% 이상일 경우 지속적인 모니터링
②시스템관리자는 서버 자원의 모니터링결과를 통해 시스템 성능향상 계획을 도모한다.
1.분임정보보안담당관은 모니터링과 데이터의 분석을 통하여, 각 요소별 성능 상태변화를 주기적으로 확인한다.
2.성능기준 미흡 시 원인 및 대책을 정보보안담당관에게 보고하여 성능향상 작업을 추진할 수 있도록 한다.
3.현재의 상태를 바탕으로 환경여건의 변화를 고려하여 향후 작업의 부하정도를 예측하고 작업의 추이를 분석한다.

제82조(백업 관리) ①정보보안담당관은 정보화자료 백업 및 소산계획을 수립하고 백업을 실시한다.
②백업대상 선정 및 주기는 시스템별 중요도 및 자료 건수, 사용빈도, 사용시간 등을 검토하여 결정한다.
③백업에는 정기적인 백업, 비정기적인 백업을 포함하며, 비정기적인 백업은 시스템 변경작업, 소프트웨어 설치작업, 하드웨어 교체작업 등의 작업 전에 반드시 수행한다.
④백업수행 후에는 백업일자, 백업대상, 백업명, 백업용량 등을 포함하여 '시스템별 백업일지'를 작성 후 보관한다.
⑤백업시스템 도입 후 최초 적용 시 정기적인 항목들(보관기간, 방식, 데이터베이스 백업모드, 소산백업 여부)을 결정하여야 하며, 운영도중 변경사항이 발생하면 충분한 검토 및 승인을 통해 이를 반영하여야 한다. 그리고 백업데이터의 중요도에 따라 백업주기를 결정한다.

제83조(서버 시스템 백업매체 관리) ①백업매체는 비인가자가 접근할 수 없는 격리된 곳에 보관하여, 비인가자에 의한 백업정보의 유출이 일어나지 않도록 한다.
②백업매체가 재난 등으로 인해 원본과 동시에 손실되는 것을 방지하기 위해 원본과 물리적으로 떨어진 장소에 보관하도록 하며, 물리적인 접근통제 및 백업일자 목록을 유지 관리한다.
③백업매체의 폐기 시 정보보안담당관의 승인을 득한 후 소각 폐기한다.
④백업데이터를 관리하는 매체에 대한 반입, 반출은 반입 및 반출입자, 인적사항, 품명, 매체유형, 보관장소, 담당자 등이 포함된 '[별지 6호]반입·반출 관리대장'을 작성하여 관리한다.
제84조(복구관리) ①장애 발생 시 장애의 종류를 파악하여 문제가 발생한 부분이 서버운영에 별로 문제가 없을 경우 업무종료 후에 복구를 수행하고, 업무 중에 복구가 불가피하다고 판단되면 최소 시간에 복구를 할 수 있도록 복구의 종류를 파악하고, 즉시 복구를 수행한다.
②장애로 인하여 영향 받는 부서 및 업무를 파악하여 관련자에게 장애원인 및 복구 예정시간 등을 통보하여 복구로 인한 업무손실을 최소화 한다.
③발생한 장애에 대한 조치복구 결과를 '장애조치내역서'에 기록하여 관리한다.
④긴급사항 발생 시 선 조치 후 보고할 수도 있다.
제85조(용도변경) 시스템관리자는 해당 서버의 용도변경 시 서버에 저장되어 있는 자료가 삭제되었는지 확인하고 장비의 관리목록을 작성, 갱신 및 유지한다.
제86조(업무연속성) 시스템관리자는 장애 또는 재난에 대비하기 위해 업무연속성 계획을 수립하고 주기적으로 모의훈련을 통해 점검해야 한다.

제13장 네트워크 보안

제87조(외부망 연동) ①다른 기관과의 정보통신망을 연결 사용하고자 할 경우에는 보안관리 책임한계를 설정하고 다음과 같은 보안대책을 수립·시행하여야 한다.
1.네트워크 취약성 점검
2.침입차단·탐지 시스템 설치 운용 등
②외부망과 접속하는 경우에는 전산자료 제공범위 및 이용자의 접근제한 등에 대해 정보보안책임관의 승인을 받아야 한다.
③외부망 연결에 따른 보안취약성 해소를 위하여 접속자료를 주기적으로 분석하고 보안도구를 이용하여 정보통신망의 취약성을 수시 점검하여야 한다.
④인터넷 등 상용망 및 타 기관과의 정보통신망 연동 시 불법침입(해킹)을 방지하고 효율적인 보안관리를 위하여 연결지점을 지정 운용함으로써 임의 접속을 차단하여야 한다.
제88조(네트워크 IP주소관리) ①내부 네트워크에서는 사설IP 주소를 사용하는 것을 원칙으로 하며 정보시스템 및 네트워크 장비에 한해서 공인IP주소를 부여할 수 있다.
②네트워크관리자는 내부통신망에서 사용하는 IP주소의 경우 사설 IP주소를 사용하여

체계적으로 관리하여야 하며, 내부 IP주소체계는 외부로 유출되지 않도록 하여야 한다.
③네트워크관리자는 IP현황을 최신으로 관리해야 한다.
④정보통신망 세부구성현황(IP 세부 할당 현황 포함)은 대외비 이상으로 지정하여 관리하여야 한다.

제89조(네트워크 장비 계정 및 권한 관리) ①네트워크 장비에는 관리자 계정 등 최소한의 계정만을 생성해야 한다.
②네트워크 장비 설치 시 기본적으로 생성되는 불필요한 계정을 삭제해야 하며 해당 계정이 필요한 경우 기본 패스워드를 변경하여 사용한다.
③네트워크 장비의 패스워드는 영문과 숫자를 조합하여 최소 8자 이상으로 설정하고 분기 1회 이상 주기적으로 변경해야 한다.

제90조(네트워크 장비 접근제어) ①네트워크관리자는 미사용 포트에 대한 비 인가자의 불법적인 접속을 방지하기 위하여, 네트워크 장비에 대한 물리적 접근통제를 수행하거나 미사용 포트는 사용 할 수 없도록 설정한다.
②네트워크 장비에 로그인시 적절한 경고 문구를 삽입 한다.
③필요치 않거나 사용되지 않는 정보통신망 서비스 기능은 제거 또는 중지한다.
④네트워크 관리자계정의 접속은 콘솔포트 및 특정 PC에서만 접근하도록 설정한다.
⑤네트워크 장비에 접근 시 사용자 인증을 수행하고, 다음의 사항을 준수한다. 단, 기능이 없는 장비는 제외한다.
1.5회 이상 정확하지 않은 패스워드의 시도가 있는 터미널은 자동으로 세션을 종료한다.
2.관리자와 사용자 모드를 지원하는 경우 분리 운영한다.
3.Idle Time은 10분 이내로 한다.

제91조 (네트워크 시스템 변경 통제) ①네트워크관리자는 패치나 시스템 파라미터(IP, 사용자 계정, 구성정보 데이터 등)를 변경할 시에는 정보보안담당관과 협의하여 변경에 따른 잠재적 영향 평가를 실시하고, 이에 따른 관련기록을 남겨야 한다.
②영향평가 실시 후 구성정보나 네트워크 시스템 변경이 적절하다고 판단되는 경우, 작업내용 및 영향평가 결과를 첨부하여 정보보안담당관의 승인을 받아야 한다.
③네트워크관리자는 네트워크 시스템 변경을 수행하기 전에 시스템의 현재 설정을 백업하여 이상 상황에 대비한다.

제92조(로그 및 백업관리) ①네트워크관리자는 모든 네트워크 시스템에 대해 시간을 동기화하여 로그 생성 시 정확한 시간이 기록되도록 한다.
②주요 네트워크 장비의 로그정보는 실시간으로 로그가 저장될 수 있도록 한다. 단. 기능을 제고하지 않는 장비는 제외한다.
③네트워크 로그는 분기1회 이상 백업을 수행하고, 1년 이상 보관하여야 한다.
④네트워크 로그파일 및 구성정보는 일반사용자 권한으로 수정 및 삭제할 수 없도록 설정한다.

⑤네트워크관리자는 네트워크 구성정보는 분기마다 백업하여 보관한다.

제93조(유지관리) ①라우터 및 스위치는 가용성 보장을 위해 유지보수를 해야 하며 최소 1개월마다 정기점검을 실시해야 한다.

②네트워크관리자는 라우터 및 스위치의 주요 패치정보를 수집하고 패치 시 안전성이 확보되는 시점에 패치 적용을 수행한다.

제94조(원격근무 보안관리) ①정보보안담당관은 정보통신망을 활용하여 본교 이외의 환경에서 재택·파견·이동 근무를 수행하는 인원을 지정하고 명단을 관리해야 한다.

②원격근무자에 대해서는 '[별지 제12호 서식] 원격근무 보안서약서'를 받는다.

③원격에서 내부시스템으로 접근하는 경우 인증서를 통한 사용자 인증을 수행한다.

④원격근무를 수행하는 인원에 대한 시스템 접근기록은 월1회 이상 주기적으로 확인한다.

제95조(무선랜 보안관리) ①본교 내의 모든 무선중계기(AP)는 정보지원팀에 설치 승인을 득한 후 설치 및 운영을 요구해야 한다.

②분임정보보안담당관은 비인가자의 무선랜 무단 사용, 비인가 AP설치 등에 대해서 분기1회 이상 점검을 수행해야 한다.

③무선랜 인증을 위해서 WPA2 이상을 적용하고, 설정된 키 값은 분기1회 이상 변경해야 한다.

④무선랜 사용에 있어서 다음과 같은 AP의 물리적 접근통제를 수행하도록 한다.

1.AP의 서비스 구역이 건물의 경계나 본교가 사용하는 건물내로 한정되도록 전파 출력을 조정하고, 외부 벽이나 창 쪽에서 먼 건물 안쪽에 설치한다.

2.AP는 물리적으로 외부인이 발견하거나 접근하기 어려운 곳에 설치한다.

⑤비인가자가 AP 보안기능의 설정을 변경하지 못하도록 출고시 AP 제조회사에서 설정한 AP 관리용 S/W의 ID, 패스워드를 변경하여 추측이 어렵게 설정한다.

제14장 어플리케이션 보안

제1절 설계 및 개발 단계

제96조(개발보안 일반) ① 정보보안담당관은 업무용 어플리케이션 및 홈페이지 등의 정보시스템을 개발하는 경우 보안대책을 수립하고 보안요구사항을 정의해야 한다.

②해당 프로젝트담당자는 정보시스템 개발 과정을 감독하고, 개발된 코드에 대한 점검과 테스트를 실시해야 한다.

③정보보안담당관은 안전한 코딩방법을 프로젝트 담당자에게 제시하여야 하며 프로젝트 담당자는 해당 기준에 따라 어플리케이션을 개발하도록 감독해야 한다.

④해당 프로젝트담당자는 모든 개발자에 대하여 사전에 보안서약서를 요구하고, 보안교육을 실시해야 한다.

제97조(개발 환경) ①개발공간은 비 인가자의 출입이 물리적으로 통제된 작업공간에

서 개발이 이루어져야 한다.
②개발서버가 위치한 네트워크는 인터넷과 분리되어야 하고, 네트워크에 연결된 경우에는 비 인가자의 접근으로부터 보호하기 위한 보안대책을 강구해야 한다.
③개발시스템과 운영시스템은 물리적 또는 논리적으로 분리되어야 한다.
④개발자의 PC는 컴퓨터 바이러스나 각종 보안 침해사고로부터 보호되어야 한다.
⑤개발자의 시스템 및 소스코드 접근은 공식적으로 허가된 경로만을 사용하여야 한다.
제98조(보안기능 요건 반영) ①본교 프로젝트담당자는 어플리케이션 설계 및 개발 시 '[별표 2] 어플리케이션 보안기능 요건'을 반영하여야 한다. 단, 업무적으로 반드시 필요하거나 정보보안담당관의 승인을 득한 경우에는 그 사유를 기록하고 보안기능 요건을 반영하지 않을 수 있다.
②본교 프로젝트담당자는 설계 및 개발 완료시 '[별표 2] 어플리케이션 보안기능요건' 반영 여부에 대해서 정보보안담당관에게 보고해야 한다.
③중요 정보의 전송 및 저장 시 국정원으로부터 승인을 얻은 암호화 기법을 사용하여 암호화해야 한다.
④다음과 같은 정보는 네트워크를 통해 전송될 수 없도록 해야한다. 단 불가피하게 전송을 필요로 할 경우 반드시 암호화된 상태로 전송해야 한다.
1.비밀번호, 주민등록번호 등 사용자와 관련된 민감한 정보
2.금융거래 정보 등 노출 시 사용자에게 피해를 줄 수 있는 정보
⑤암호화 Key의 접근은 인가된 사람으로만 제한하도록 하며 암호화 Key는 일정주기마다 변경하여야 한다.

제2절 테스트 단계

제99조(테스트 데이터 보호) ①테스트를 위하여 실 데이터를 이용하고자 할 경우에는 정보보안담당관의 승인을 받아야 한다.
②테스트 수행자는 사용자의 중요정보가 포함될 경우 제공받은 실 데이터를 적절한 과정 (익명화, 재생성, RENAME 등)을 통하여 테스트 데이터로 변환한 후 사용한다. 단, 실 데이터를 변환하지 않고 테스트를 할 경우에는 정보보안담당관의 승인을 받아야한다.
③실 데이터는 테스트 데이터와 분리되어야 하며, 테스트 데이터의 접근은 테스트 절차에 필요 최소인원으로 통제되어야 한다.
④테스트 수행자는 테스트 완료 후에는 즉시 테스트 데이터를 삭제해야 한다.
제100조(보안 점검) ①개발 완료 시 분임정보보안담당관은 해당 시스템에 대한 보안 취약점점검(시스템, 어플리케이션 점검)을 수행한다.
②보안점검 결과 나타난 취약점은 보완조치를 수행하고, 운영해야 한다.

제3절 운영 단계

제101조(사용자 계정 관리) ①어플리케이션 신규 계정에 대한 권한은 최소사용자 권한 만을 부여한다.
②공동으로 사용하는 ID를 부여하지 말아야 한다. 단, 업무상 필요시는 주관 부서장의 승인을 득해야 한다.
③계정(ID) 생성 시, 초기 Password는 추측 가능한 사번, ID 등으로 설정하지 말아야 한다.
④민감한 정보자산에 대한 사용자 접근 시, 날짜, 시간, 장소별 제한을 하는 등 강력한 접근통제 정책을 적용할 수 있어야 한다.
⑤불필요한 계정 및 권한에 대한 검토 및 삭제를 반기마다 1회씩 수행한다.
⑥전출 및 퇴직 등의 사유 발생 시, 어플리케이션 담당자는 사용자 ID를 신속히 삭제한다.
⑦사용자 퇴사 및 사용자 업무 등이 변경되어 계정의 삭제나 권한의 변경이 필요한 경우 인사발령사항을 기준으로 자동 계정삭제 및 권한변경을 원칙으로 한다. 단, 시스템이 인사시스템과 연동이 되어있지 않거나 업무상 주관부서의 검증이 필요한 경우에는 주관부서 담당자가 검증 후 최소 1개월 이내에 처리할 수 있다.
제102조(로그 및 소스 관리) ①사용자 ID, 사용시간, 사용 정보, 로그인 실패내역 등의 사용자 로그정보는 최소 6개월 이상 보관 되어야 한다.
②시스템상의 로그파일과 백업된 로그파일은 수정이 가능해서는 안 된다.
③컴퓨터 범죄나 오용이 발생했다고 의심될 때 조사를 위해 필요한 관련 정보를 즉시 안전하게 확보해야 한다.
④정보보안담당관의 사전승인 없이는 모든 어플리케이션 로그에 대해 비인가자가 접근할 수 없어야 한다.
⑤개발된 프로그램 소스는 실 운영시스템에 저장되어서는 안되며 실 운영시스템에는 실행 프로그램만을 저장하여야 한다.
⑥프로그램 소스를 실 운영시스템에서 컴파일 해야 할 경우에는 프로그램 생성 후 삭제하여야 한다.
⑦중요한 변경이 필요한 경우 정보보안담당관의 승인을 득한 후 문서화 된 양식을 통하여 변경 요청을 수행 하여야 한다.
⑧어플리케이션의 유지보수 및 변경 작업에 대해 정보보안담당관과 협의 후 수행하여야 한다.
⑨변경작업은 서비스 운영을 고려하여 업무이외의 시간에 변경 작업을 수행하여야 한다. 단, 긴급을 요하는 변경 작업의 경우 정보보안담당관의 승인을 득한 후 수행 할 수 있다.
⑩다음 사항과 같은 변경이 이루어지는 경우 보안성 영향분석 및 검토를 수행하여야 한다.
1.어플리케이션의 전면적인 수정

2.인증, 암호화 등 보안 기능의 변경이 수반되는 경우
3.새로운 위협, 취약성의 발견으로 정보시스템에 적용이 필요한 경우
⑪어플리케이션 변경에 관련된 사항은 문서화하여 관리하여야 한다. 문서화 내용에 다음의 사항을 포함하여야 한다.
1.변경 요청 전, 후의 내용
2.변경 방법
3.변경 일시
4.변경 수행 담당자

제 15 장 정보보안시스템 관리

제103조(선정 및 설치) ①정보보안시스템을 설치·운용하고자 하는 경우 아래와 같은 사항을 반영하여 선정하여야 한다.
1.정보보안시스템 평가인증 지침 및 공통평가기준에 의해 인증된 제품이나 국정원장이 그와 동등한 효력이 있다고 인정한 제품
2.소관업무 및 정보통신망 특성을 지원할 수 있는 제품
제104조(운용 및 보안관리) ①정보보안담당관은 정보보안시스템 운용 관리자로 '정보보안시스템 관리자'를 지정한다.
②정보보안시스템은 직접 연결된 단말기에서만 접속할 수 있도록 해야 한다. 단, 원격관리가 필요한 경우 지정된 단말기를 통해서 원격관리를 허용할 수 있다.
③침입차단시스템 등의 정보보안시스템 로그는 최소 3개월 이상 보관한다.
④정보보안시스템은 보안기능을 임의로 변경하거나 도입 목적이외의 용도로 운영하여서는 안 된다.
제105조(정보보안시스템 보안정책 등록, 변경, 삭제) ①정보보안시스템의 보안정책의 추가, 수정 등이 필요한 경우, 관련 업무담당자는 정보보안담당관에게 승인을 받아야 한다.
②정보보안시스템관리자는 정보보안담당관의 승인을 득한 후 정책 변경작업을 수행하고, 보안정책 변경 내역을 '[별지 제13호 서식]보안정책 변경 관리대장'에 기록한다.
③정보보안시스템 관리자는 보안정책을 분기 1회 이상 점검하여, 사용기간이 지난 보안정책이나 취약한 보안정책은 삭제한다.

제 16 장 침해사고 대응

제106조(침해사고대응팀 구성) ①침해사고를 효과적으로 대응하기 위해서 침해사고대응팀을 구성하며, 침해사고대응팀은 침해사고 발생시, 한시적으로 운영한다.
②침해사고 발생시, 본교의 정보보안 조직은 침해사고대응팀으로 전환되어 운영되며,

각 부서의 부서정보보안담당관을 포함한다.
③침해사고대응팀의 총괄 책임자는 정보보안책임관으로 한다.
④침해사고대응팀의 실무 총괄자는 정보보안담당관으로 하며, 침해사고 대응 및 보고 업무를 총괄 수행한다.
⑤분임정보보안담당관은 분야별 담당업무 및 시스템에 대해 침해사고 현황 및 대응방안 등을 실무 총괄자에게 보고, 수시로 상황에 대처한다.
⑥분야별 시스템을 유지관리하고 있는 외부업체 주요 담당자는 분임정보보안담당관과 침해사고 대응책을 마련하여 시스템에 적용한다.
⑦침해사고대응 실무 총괄자는 침해사고대응팀 및 유관기관 등의 연락처를 '[별지 제14호 서식] 침해사고 비상연락망'에 기록하고 현행화해야 한다.
⑧침해사고대응팀은 년 1회 이상 자체 모의대응훈련을 실시하고, 그 결과를 기록관리 한다.

제107조(침해사고유형) 다음 각 호의 어느 하나에 해당하는 사항을 침해사고로 본다.
1.비인가자의 정보시스템 접근
2.정보자산의 유출(H/W, S/W, DATA 등)
3.비인가자에 의한 중요정보의 위·변조 및 삭제에 관한 사항
4.악성 프로그램(바이러스, 백도어 등) 유포
5.정보시스템에 대한 서비스 거부공격(DOS공격 등) 발생
6.네트워크 장비, 서버 및 PC 등에 대한 해킹 발생
7.어플리케이션에 대한 비인가 접근 발생
8.그 밖에 국가정보원의 정보보안사고 유형 [별표 3]에 해당하는 사항

제108조(침해사고 신고 및 접수) ①전 직원은 침해사고 등의 징후가 포착되거나 침해사고가 발생한 경우, 지체없이 부서정보보안담당관 또는 정보보안담당관에게 신고해야 한다.
②정보보안담당관은 상시 자체적인 모니터링을 수행 하면서 침해사고 등의 이상징후가 탐지되거나 발생되었을 경우, 즉시 정보보안책임관에게 보고한다.
③침해사고 발생 시 신고자는 가장 빠른 방법을 통해 신고해야 하며, 정보보안담당관은 '[별지 제15호 서식] 침해사고 발생보고서'에 기록하여 문서상으로 보관 관리해야 한다.

제109조 (침해사고의 보고) ①정보보안담당관은 접수된 신고 사항에 대해 기록하고, 시정 조치가 종료될 때까지 모든 기록을 유지, 관리하며 조치된 내역에 대해 '[별지 제16호 서식] 침해사고 처리결과서'를 작성하여 정보보안책임관에게 보고해야 한다.
②정보보안책임관은 사고내역 및 조치내역을 확인하고 총장에게 보고 한다.
③정보보안책임관은 홈페이지 변조, 침해사고로 인한 전산망 마비 또는 중요 정보자료, 개인정보 유출 등 중대사고 발생 시에는 그 사실을 관계기관(교육과학기술부, 행정안전부, 국정원 등)에 보고 한다.

제110조(침해사고 대응 및 조치) ①정보보안담당관은 정보통신망에 대하여 해킹, 웜·

바이러스 유포 등 사이버공격 시 피해실태를 파악하고 관련 로그자료 보존 및 필요시 해킹된 정보시스템과 전산망 분리, 공격IP 및 포트의 차단 등 초동 조치를 취한다.
②홈페이지 변조, 전산망 마비 또는 중요 정보자료, 개인정보 유출 등 중대사고 발생 시에는 초동조치 후 즉시 관계기관(교육과학기술부, 행정안전부, 국정원 등), 외부전문업체 등에 통보하여 지원을 받을 수 있다. 이 경우 해당 피해시스템은 사고원인 규명 시까지 증거보전을 의무화하고 임의 자료삭제 또는 포맷을 하여서는 아니 된다.
③정보보안담당관은 응급조치 후 정보보안 침해사고의 원인분석 및 증거확보를 위하여 해당침해사고 관련 로그 및 제반 증거 자료를 수집/확보 한다.

제111조(침해사고 복구 및 재발방지) ①정보보안담당관은 전자적 침해사고로 인하여 소관 정보통신기반시설이 파괴되거나 기능이 제대로 수행되지 아니하는 때에는 해당 시설이 정상적으로 가동될 수 있도록 필요한 복구조치를 신속히 취하여야 하며 관계 행정기관, 수사기관 및 외부 정보보안 전문업체에게 복구에 필요한 지원을 요청할 수 있다.
②정보보안담당관은 침해사고에 대한 복구가 완료된 경우, 유사사고 재발방지 대책을 수립하고, 대응·복구사항에 대한 교육 및 공지를 수행한다.

제17장 용역사업 보안관리

제112조(계약시 보안관리 등) ①정보화, 정보보안사업, 정보시스템 등을 외부 용역으로 외부업체와 계약할 경우에 계약서에 정보보안 준수 의무 및 위반할 경우에 손해배상 책임 등을 명시하여야 한다.
②계약서에 정보보안 준수 의무 및 위반에 대한 사항을 명시하는 경우 [별표 4]의 내용을 참조한다.

제113조(참여인원 보안관리) ①사업주관부서는 모든 참여인원에 대하여 각 개인의 친필서명이 들어간 보안서약서를 요구해야 한다.
②사업주관부서는 용역업체 자체 보안관리 및 직원 관리감독 강화를 독려하고 보안의 중요성 인식제고를 위해 업체대표 명의 '[별지 제17호 서식]정보보안 서약서(용역업체 대표자용)'을 제출 받아야 한다.
③사업주관부서 담당자는 사업시작 전 참여인원에 대한 보안준수 의무 등의 보안교육을 실시하고, 교육 참가에 대한 자필서명을 받는다.
④사업수행시 사업수행업체의 대표자(PM)를 정보보안책임관으로 지정·운영하며, 사업수행업체 대표자(PM)는 사업전반에 대한 인원·장비·자료·정보 등을 관리하며 보안사고 방지를 위한 자체 활동을 수행해야 한다.

제114조(자료에 대한 보안관리 등) ①전산망구성도, IP현황, 개인정보, 기타 용역업체에 제공하는 자료는 '[별지 제18호 서식] 자료관리대장'을 작성하여 인계자(본교 사업담당자)와 인수자(용역업체 사업수행대표)가 직접 서명한 후 인계·인수해야 한다.
②용역사업 관련자료 및 사업과정에서 생산된 모든 산출물은 본교의 파일서버에 저장

하거나 정보보안담당관이 지정한 PC에 저장/관리 한다.
③용역사업 관련 자료는 인터넷, 웹하드 등 인터넷 자료공유사이트 및 웹 메일 등의 외부메일함에 저장을 금지하고, 전자우편을 이용해 자료전송이 필요한 경우에는 본교 전자우편을 이용하여 첨부자료를 암호화한 후 수·발신한다.
④본교와 관련된 자료를 출력물로 제공한 경우에는 시건장치가 된 보관함에 보관하여야 한다.
⑤사업수행업체는 사업수행으로 생산되는 산출물 및 기록은 본교의 해당사업 주관부서장 또는 정보보안담당관이 인가하지 않은 비인가자에게 제공·대여·열람을 금지한다.

제115조(장비·사무실에 대한 보안관리) ①사업수행업체의 노트북, PC는 반입시 마다 최신의 바이러스 백신프로그램 설치와 바이러스 감염여부를 점검·확인해야 한다.
②반입된 노트북 PC는 사업 종료 시까지 반출을 금지한다. 다만 부득이하게 외부반출이 필요한 경우에는 최소한의 장비만 반출승인하고 자료유출에 대비한 보안조치(부팅·로그인 패스워드 설정, 자료 암호화 등)를 실시한 후 반출한다.
③USB 등의 보조기억매체 사용을 금지한다. 다만, 산출물작성 등 보조기억매체가 필요한 경우는 정보보안담당관의 승인하에 허가된 것만 사용한다.
④용역사업 수행장소는 시건장치와 출입통제가 가능한 공간을 사용해야 한다.

제116조(내·외부 정보망 접근에 대한 보안관리) ①용역사업 수행 시 정보시스템에 대한 사용자 계정(ID)이 필요한 경우, 외부인력에게 별도의 계정을 발급하고 접근권한을 부여 후 계정발급 및 접근권한 부여 기록을 별도로 관리 한다.
②외부인력에게 부여된 접속권한이 불필요한 경우 곧바로 권한을 해지하거나 계정을 삭제한다.
③프로그램 개발 용역사업 수행을 위한 작업은 사업수행업체의 자체 개발서버 또는 본교가 제공한 개발서버에서 수행함을 원칙으로 하며, 개발이 완료된 후 실 운영시스템에 설치시는 본교의 해당 시스템 담당자의 감독하에 작업한다.
④용역업체 전산망에서 P2P, 웹 하드 등 인터넷 자료공유사이트로의 접속을 차단한다.

제117조(사업완료시 보안관리 등) ①사업완료 후 생산되는 최종 산출물 중 대외보안이 요구되는 자료는 대외비로 작성·관리하고 불필요한 자료는 삭제 및 세단 후 폐기한다.
②용역업체에 제공한 제반자료, 장비, 서류와 중간・최종 산출물 등 용역과 관련된 제반자료는 전량 회수하고 업체에 복사본 등 별도보관을 금지한다. 단, 소스코드 등 향후 유지보수를 위해 필요하다고 판단되는 경우 정보보안책임관의 승인 후 용역업체에게 제공할 수 있다.
③사업완료시 용역업체의 노트북 PC 및 사용된 보조기억장치는 자료에 대하여 Format후 반출한다.
④노트북・보조기억매체 등 전자적으로 기록된 자료는 복구할 수 없도록 삭제해야 한다.

⑤사업완료시 용역사업 관련자료 회수 및 삭제조치 후 업체에게 복사본 등 용역사업 관련 자료를 보유하고 있지 않다는 대표 명의로 '[별지 제19호 서식] 보안자료 반납 및 파기 완료 확약서'를 요구한다.

제18장 백업 및 복구

제118조(백업일반) ①물리적 재난이나 정보통신설비의 오류 발생으로 긴급 상황이 발생할 경우, 즉각적으로 복구할 수 있도록 주기적으로 백업을 수행한다.
②정보의 중요성 및 데이터의 성격에 따라 백업주기, 백업방법, 보존기간 등을 포함하여 기록·관리해야 한다.
③시스템관리자는 '[별지 제20호 서식] 시스템 백업일지'을 수립하여, 정보보안담당관의 승인을 득한다.
④백업 데이터의 최소 보관기간은 3개월로 한다.
제119조(백업 대상 및 주기) ①백업대상은 데이터의 파손 시 복구의 필요성이 요구되는 본교의 주요 데이터이며 다음과 같은 정보들이 이에 해당한다.
1.OS및 유틸리티 프로그램
2.데이터베이스 파일 : 업무데이터 및 데이터베이스 구성파일
3.네트워크 장비 구성파일 및 로그파일
4.정보보안시스템 정책 및 로그파일
5.기타 필요로 하다고 생각되는 파일
②백업대상에 대한 백업 및 보관주기는 [별표 5]을 기준으로 정한다.
③백업 데이터는 원격지의 안전한 장소에 분산보관 하고, 그 기록을 관리 한다.
제120조(복구) ①데이터베이스 및 정보통신시스템 장애 시 백업된 자료를 사용하여 복구한다.
②장애 및 재해 발생 시 신속한 복구를 위해서 년1회 이상 복구 훈련을 수행한다.

제19장 정보보안 내부감사

제121조(내부감사) ①정보보안책임관, 정보보안담당관은 정보보안 전반에 대한 연간 내부감사 계획을 수립하여 실시한다.
②내부감사 수행 시 다음 각 호의 사항을 확인한다.
1.정보보안 관리규정의 업무 요구사항 부합 여부
2.적절한 위험평가 방법 적용 여부
3.잔여위험의 적절한 평가 및 수용가능 여부
4.기술적 통제장치의 적절한 운영 여부
5.이전 내부감사 수행 시 지적사항에 대한 적용계획의 이행 여부
③내부감사 시 아래 각호를 고려하여 감사를 실시해야 한다.

1.업무 프로세스의 중단위험을 최소화 시킬 수 있도록 운영시스템에 대한 감사 필요 요건과 활동을 신중하게 계획한다.
2.감사자는 내부감사 수행 중 중대한 업무상 부정, 고의적 정보시스템 위해 행위 등의 사고를 발견한 경우 지체 없이 정보보안담당관에게 보고한다.
④정보보안책임관은 내부감사 결과 발견된 취약점 및 부적합 사항에 대해 각 해당 팀·처에게 적절한 조치를 취하도록 권고하며, 이의 이행을 모니터링 한다.
⑤정보보안책임관은 제1항의 규정을 준용하여 당해 본교 각 팀, 처에 대하여 내부감사를 실시하고 그 결과를 총장에게 보고하고, 필요 시 관련 팀에 통보한다.

제122조(내부감사 수행 조직 및 범위) ①내부감사는 정보보안책임관이 주관하여 실시하며, 감사반은 정보보안담당관 주관으로 분임정보보호담당관으로 편성한다.
② 내부심사의 범위는 아래 각호와 같으며, 각 분야에 대한 점검항목은 '[별지 39호] 정보보안 내부심사 점검항목'을 기준으로 한다.
1.관리적 보안관리
2.물리적 보안관리
3.네트워크 보안관리
4.서버시스템 보안관리
5.보안시스템 보안관리
6.응용시스템 보안관리
7.PC 보안관리

제123조(내부감사 계획) ①정보보안책임관, 정보보안담당관은 연간 내부감사 계획을 수립하여 실시한다. 연간 내부감사 계획에는 목적, 대상, 방법 및 실시 시기 등을 명시한다.
②내부감사는 연간 1회 이상 정보보호관리체계(ISMS)의 전 부문이 포함되도록 계획한다.
③년간 내부감사 계획에 의한 심사 또는 특별감사를 실시할 때에는 세부 감사수행 계획을 수립하여 실시한다.
④내부감사의 감사자는 감사 절차의 객관성 및 공정성을 보장한다.

제124조(특별 내부심사 실시) ①정보보안책임관은 보안사고의 우려가 있거나 침해사고가 발생한 경우 특별감사를 실시할 수 있다.
②특별감사의 경우에도 감사 진행 및 결과보고의 절차는 정기감사와 동일하게 진행함을 원칙으로 한다. 단, 특별한 목적을 가지고 수행하는 내부감사는 해당 목적에 적합하도록 변경하여 실시할 수 있다.

제125조(내부감사 증적의 확보) ①감사대상 영역에 대한 보안감사 증적(Audit Trails)을 확보하고, 증거자료의 무결성이 보장되도록 조치한다.
②서버, 네트워크시스템, 응용시스템, 데이터베이스 등에 대하여 내부감사에 필요한 시스템 로그의 종류와 보존기간을 해당 지침 및 매뉴얼에 명시하여, 심사 시에 충분한 증거로서 활용한다.

제126조(내부감사 결과에 따른 시정 및 검증) ①정보보안책임관은 내부감사에서 지적된 사항을 해당 팀·처의 장에게 통보하여 시정조치계획을 수립하게 한다.
②각 팀장은 지적사항에 대해 원인분석, 재발방지 대책, 상세 이행계획 등이 포함된 시정 조치 계획을 수립하여 이행한다.
③정보보안담당관은 시정조치계획의 수립 및 이행여부를 주기적으로 점검하고 사후관리하며, 내부감사자는 이행 완료여부를 검증한다.
제127조(내부심사에 대한 인식 확산) ①정보보안책임관은 피 감사과에 내부감사의 의의, 실시방법 등에 대한 정보를 제공하여 보안의 중요성 및 내부감사의 필요성에 대하여 공감하도록 한다.
②내부감사가 실시되고 있다는 것을 관련 직원들에게 공지하여 보안사고를 예방하도록 한다.
③정보보호 관련 규정의 위반 및 보안침해에 따른 징계사항을 교육함으로써 직원들의 규정준수를 유도한다.

제20장 개인정보보안

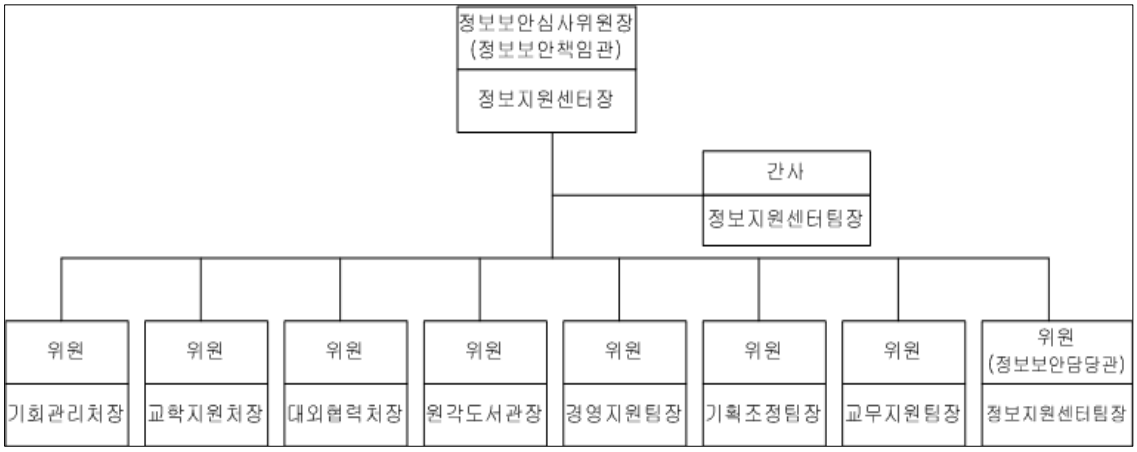
제128조(개인정보보안) ①모든 직원은 업무 목적으로 개인정보를 수집, 이용, 저장하는 경우 개인정보가 유출되지 않도록 유의해야 한다.
②모든 직원은 업무용도외 개인정보를 사용하지 않아야 하며, 업무상 알게 된 개인정보를 침해 또는 누설하여서는 안된다.
③개인정보보안과 관련된 세부사항은 '개인정보보호 지침'을 따른다.
④CCTV와 관련된 세부사항은 'CCTV 설치·운영 지침'을 따른다.

부 칙

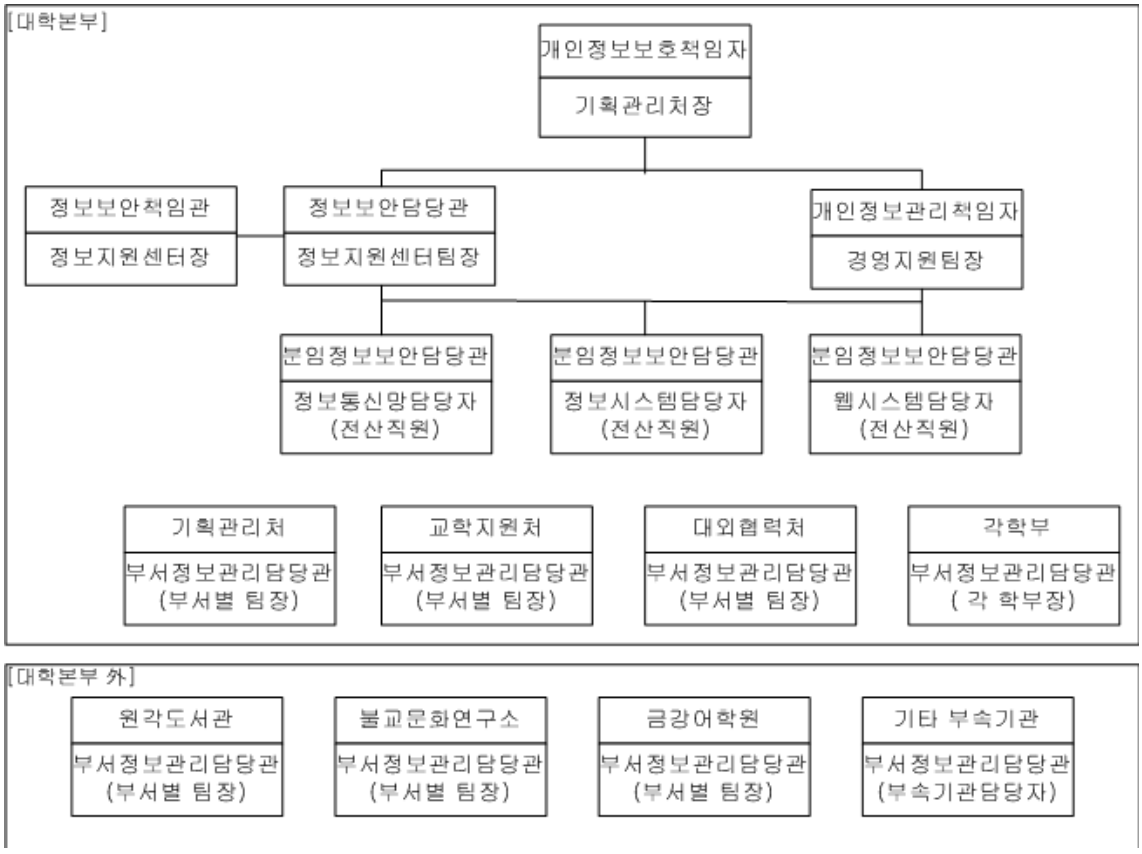
(시행일) 이 규정은 2012년 6월 1일부터 시행한다.

[별표 1]

정보보안심사위원회 구성



정보보안조직 구성



[별표 2]

어플리케이션 보안기능 요건

구분	보안기능 요건	비고
인증 기능	① 인증시스템을 별도로 사용하는 경우, 인증시스템을 거치지 않고 응용 프로그램으로 직접 접속할 수 없도록 함.	
	②사용자가 메인 메뉴를 경유하지 않고 서브메뉴를 직접 접속 시에도 인증과 정을 반드시 거치도록 해야 함.	
	③사용자 인증 없이 데이터의 접근 및 처리가 가능한 시스템 명령어를 사용하여 프로그램을 개발해서는 안됨.	
	④ 패스워드의 자동 저장 기능을 제공하지 않음으로써, 사용자가 패스워드를 입력하지 않으면 자동적으로 로그인 되지 않도록 함.	
패스워드	① 패스워드가 없거나 사용자 계정과 동일한 패스워드를 허용하지 않도록 함.	
	② 패스워드는 문자, 숫자, 특수문자로 이루어진 최소길이 8자 이상으로 함.	
	③ 입력된 패스워드는 별표(*) 처리되거나 음영 처리 되도록 설계하여 단말기 화면에서 읽을 수 없도록 함.	
	④ 패스워드는 패스워드 정책에 따라 주기적으로 강제 변경되도록 함.	
	⑤ 보안이 중요한 어플리케이션은 변경 직전에 사용했던 패스워드를 재사용 하지 못하도록 한다.	
	⑥ 패스워드를 입력하지 않아도 자동으로 로그인되는 것을 방지하기 위해 패스워드의 자동 저장 기능을 제공하지 않음.	
접근통제	① 동일한 계정을 이용한 이중 로그인(동시 로그인)을 제한하도록 함	
	② 개인정보, 비공개정보를 처리하는 주요 업무용시스템은 로그인 실패횟수(3회 권장)를 제한 함.	
	③ 개인정보, 비공개정보를 처리하는 주요 업무용시스템은 로그인 성공 후, ‘사용시 주의사항’등을 팝업창으로 표시함.	
	④ 사용자 로그인 성공후에는 이전 접속 일시, 접속IP 등 접속정보를 표시함.	
	⑤ 일정시간(1시간 이하) 동안 어떤 입력도 일어나지 않으면 자동적으로 로그오프 시키거나 세션을 중단시킴. 단, 사용자와 협의 하에 해당 시간을 조정할 수 있음.	
	⑥ 사용자 로그인 성공후에는 이전 접속 일시, 접속IP 등 접속정보를 표시함.	
	⑦ 일반사용자가 어플리케이션을 통하지 않고 직접적으로 DB 및 중요정보를 가진 파일에 접근할 수 없도록 함.	
	⑧ 접근권한 별로 접근 가능한 정보를 제한하여 부여된 권한 이외의 정보에는 접근이 불가능하거나 화면에 보이지 않도록 함.	
	⑨ 사용자 계정, 부서, 사용자 그룹에 따라 사용권한을 설정할 수 있도록 함.	
로그	① 모든 사용자의 사용자 접속 로그(사용자 계정, IP, 일시,로그인 및 로그아웃시간)를 기록하도록 함.	
	②모든 사용자의 로그인 실패 내역을 로그파일에 기록하도록 해야 함. 1. 로그인 연속 실패 로그 (실패한 사용자 계정, IP,일시, 시간) 2. 로그인 실패 로그 (실패한 사용자 계정, IP,실패 횟수,일시, 시간)	
	③ 특정사용자(관리자, 특수권한 소유 사용자 등)의 사용 내역은 일반사용자 보다 상세하게 관리되도록 로깅 기능을 설계해야 함.	
	④ 모든 사용자의 권한 설정 및 변경 내역은 기록 되도록 설계되어야 함.	

암호화	① 주요 정보(개인정보, 고객정보, 인증정보(ID/패스워드) 등)는 안전한 암호 알고리즘(DES, 3DES, SEED, SSL 등) 및 충분한 키길이(대칭키128bit, 비대칭키 2048bit 이상)을 가진 암호 모듈로 암호화하여 저장 및 전송한다.	
정보유출 방지	① 권한이 없는 사용자가 고객정보 등 중요정보에 접근 할 수 없도록 해야 하며. 권한이 있는 경우에도 업무성격에 맞는 정보만 표시 될 수 있도록 함.	
	② 어플리케이션에서 리스트 형식의 상세 고객정보(주민등록번호, 패스워드, 전화번호 등)를 화면에 출력할 때에는 정보의 일부가 음영 또는 별표(*)처리 되도록 함.	
	③ 어플리케이션에서 웹 소스 보기등을 통해 사용자의 인증 정보가 노출되지 않도록 함.	
	④ 업무적 필요에 의해서, 어플리케이션에서 중요 정보를 PC로 다운로드하는 경우 사용자계정, IP, 다운로드한 파일이름, 일시등의 로그를 남겨야 함.	

[별표 3]

국정원 정보보안사고 유형

조	내용	항	세 부 내 용
1	정보시스템 및 정보통신실	1	정보시스템 및 정보통신실 파괴
		2	정보통신망에 대한 해킹・악성코드의 유포
		3	비밀이 저장된 보조기억매체 분실
		4	악성 바이러스 유포 또는 비밀번호 파일 유출
2	전산자료	1	컴퓨터·전자기록 손상 및 파괴
		2	저장자료의 유출·파괴·변조
3	정보보안시스템	1	침입차단시스템 보안기능 변경사용
		2	침입차단시스템 분실·피탈

[별표 4]

용역사업 계약시 정보보안 준수 및 의무 사항

1.정보자산의 기밀성, 무결성, 가용성보장

가. 본교 정보자산을 허가 없이 외부 또는 제3자에 공개 및 유출하지 말아야 하며, 특히 업무수행 시 취득한 정보를 다른 협력회사 등에 유출되지 않도록 주의한다.

나. 본교 정보자산을 무단으로 변경하지 말아야 하며, 정확하고 완전한 상태로 유지한다.

2.보안관련법적조항 및 보안규정, 지침준수책임

가.개인정보보호법 등의 법적인 요구사항을 준수한다.

나.정보보안 관련 법률에서 금지하고 있는 본교 시스템 및 정보통신망에 대한 해킹 및 침해 행위를 금한다.

다.본교 정보보안관련규정을 숙지하여 위반사항이 발생하지 않도록 준수한다.

라.본교 지적재산에 대한 보호 의무를 성실히 준수한다.

3.계약완료시 정보자산 반환 및 폐기 의무

가.사업수행을 위해 이용한 모든 본교 정보자산은 해당 사업종료 시 반드시 본교에 귀속되어야 한다.

나.계약완료 시 정보자산의 반환 및 폐기는 해당 사업의 본교 책임자에 의해 확인되어야 한다.

4.바이러스 확산 방지

가. 본교 교내로 반입되는 모든 장비에는 반드시 백신이 설치되어 있어야 하며, 바이러스 검역 과정을 거친 후 본교 네트워크에 연결할 수 있다.

나.수시로 반·출입되는 장비에 대한 관리 책임은 협력회사 측에 있으며, 백신의 정상 작동 여부와 바이러스 엔진의 업데이트 여부를 반드시 확인한다.

다.본교 교내망에 연결된 상태로 E-mail을 이용하거나 인터넷을 통한 자료를 다운로드 받는 경우 반드시 바이러스 점검을 수행한다.

5.보안위반사항 발생 시책임

보안요구사항 및 계약서상에 명시된 준수사항 불이행으로 인해 본교에 피해가 발생한 경우 보상 책임은 용역회사측에 있으며, 현재사업 및 향후 계약에 불이익이 발생할 수 있다

6.보안사고보고 및 조사 동의

용역업체 참여 직원은 본교에서 사업수행 중 보안사고 발견 시 신속히 해당사항을 본교에 보고하여 지속적인 업무 활동이 보장될 수 있도록 협조한다.

7.보안감사수용

가.용역업체 참여 직원은 본교 정보보안관리규정 준수 현황 감독을 위해 본교는 정기적으로 보안감사를 실시할 수 있는 권한이 있으며,용역회사는 이에 적극적으로 협조한다.

나. 본교의 핵심 정보시스템 또는 기밀 정보를 다루는 업무를 수행하는 협력회사 직원에 대해서 E-mail 모니터링 등의 물리적, 논리적 모니터링을 실시할 수 있다.

8.기타사항

가.본교 출입 시 반드시 허가된 지역만 출입한다.

나.사업 수행을 위해 본교 내부 시스템에 대한 사용권한을 부여 받은 경우 용역회사직원은 부여받은 계정 및 패스워드가 노출되지 않도록 각별히 주의한다.

[별표 5]

백업대상, 주기 및 보관주기

백업대상	백업주기	보관주기
OS, DBMS, 기타 시스템 S/W	월간	3개월
핵심업무 및 중요업무 데이터(민원고객 관련 데이타)	일일, 주간, 월간	6개월
일반업무 데이터(본교 내부업무 처리 관련 데이터)	주간, 월간	3개월
정보보안관련 데이터(방화벽 정책, 로그 파일)	일일, 주간, 월간	3개월
네트워크 관련 데이터(라우터, 스위치 구성파일)	환경설정 변경이전, 분기	3개월

【별지 제1호 서식】

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

도출내용	조치내역	담당부서

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

【별지 제2호 서식】

정보보안업무 심사분석

1. 총평

2. 주요성과 및 추진사항

3. 세부 사업별 실적 분석

추진계획	추진실적	문제점	개선대책

※ 추진실적은 목표량과 대비하여 성과 달성도를 계량화

4. 부진(미전)사업

부진사업	원인 및 이유	익년도 추진계획

5. 애로 및 건의 사항

6. 첨부(정보통신망 및 정보보안시스템 운용현황 등)

【별지 제3호 서식】

정보자산목록

담당자	부서정보보안 담당관	정보보안 담당관	정보보안 책임관

부서명 :

자산분류	시스템	네트워크	어플리케이션	정보보안시스템	프로그램	물리적 설비	기타

기본사항								추가사항				자산중요성 평가			
NO	자산명	목적/내용	IP	수량	자산위치	담당자	책임자	제조업체	모델명	O.S	설치 S/W	기밀성	가용성	무결성	등급분류

【별지 제4호 서식】

정보보안 서약서(교직원용)

본인은 본교 (이하 “본교”라 함)에 근무함에 있어서 다음 각 호의 정보보안사항을 충분히 숙지하고, 성실히 준수할 것을 서약합니다.

1. 본인은 본교의 정보보안 규정을 준수하여, 보안 사고가 발생되지 않도록 예방 및 주의에 최선을 다할 것입니다.
2. 본인은 본교에서 근무하는 동안 취득한 본교의 정보, 개인정보, 지적 재산권들을 엄격히 보호할 것이며, 이를 개인적인 용도나 제 3자를 위한 정보로 이용하지 않고 맡은 바 업무수행을 위해서만 사용할 것입니다. 또한, 이러한 정보를 타인에게 누설하지 않을 것입니다.
3. 본인은 본교의 정보자산(문서서류, 전자파일, 저장매체, 전산망, 전산장비 등)을 무단 변조, 훼손, 분실 등으로부터 안전하게 사용하고 관리할 것이며, 불법적인 목적으로 사용하지 않을 것입니다.
4. 본인은 본교의 업무 수행 과정 중 사용하는 PC에 승인 받은 정품 소프트웨어만을 사용할 것이며, 불법 소프트웨어 사용으로 인한 모든 책임은 본인에게 있음에 동의합니다.
5. 본인은 본교에서 퇴직하는 경우, 재직 시에 취득한 본교 소유의 모든 정보 자산을 반드시 반납할 것이며, 이후에도 개인적으로 이용하지 않을 것입니다.

본인은 상기 사항을 숙지하고 이를 성실히 준수할 것을 동의하며, 본 서약서의 준수사항을 위반한 경우에는 관련 법령에 의한 일체의 민·형사상의 책임 이외에도, 본교에 끼친 손해에 대해지체 없이 변상·복구 할 것을 서약합니다.

20 년 월 일

서약자 소속 :

직위 성명 (인)

서약자 집행자 소속 :

직급 직위 성명 (인)

【별지 제5호 서식】

기계실 출입관리대장

일자	출입자			출입목적	비고	출입시간		확인	정보보안 담당관
	소속	성명	연락처			입실	퇴실		

【별지 제6호 서식】

반입·반출 관리대장

번호	반입. 반출명	반입. 반출처	반입.반출		반입.반출자		반입. 반출 사유	반입. 반출 일자	확인
			반입	반출	소속	이름			

【별지 제7호 서식】

PC관리대장

연번	소속	취급자 (성명)	관리번호	종류 (PC, 노트북)	비밀번호 (부팅, 사용자, 인증용, 자료용)	등록 일자	해제 일자

※ 부서별 PC 및 노트북 현황을 기록한다.

※ PC등의 비밀번호를 기재하지 아니할 수 있다.

【별지 제8호 서식】

보조기억매체(전산장비 포함) 반출·입 대장

부서 :　　부서정보보안담당관 :

장비명	관리번호 (시리얼번호)	사용자	용도	반출입 기간			
				반출(시작)	확인	반입(종료)	확인

【별지 제9호 서식】

정보보안 서약서(외부자용)

본인은 _____년____월____일부로 금강대학교 _____관련 용역사업(업무)을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

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

2. 본인은 비밀, 행정문서, 중요정보, 개인정보 등 비공개자료의 열람·취급 후 금강대 규정을 준수하겠습니다.

2. 본인은 업무취급 시 취득한 사실에 대하여는 대인관계에 있어서나 장소여하를 막론하고 누설 및 공개하지 않을 것을 서약한다.

3. 본인이 이 기밀을 누설하거나 관계규정을 위반한 때는 관련법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다,

4. 본인은 하도급 업체를 총한 사업수행 시 하도급 업체로 인해 발생하는 위반사항에 대하여 모든 책임을 부담한다.

20 년 월 일

서 약 자 소 속 :
직 급 :
성 명 : (서명)

서약집행자 소 속 :
직 급 :
성 명 : (서명)

【별지 제10호 서식】

보조기억매체 관리대장(일반용)

부서 :　　부서정보보안담당관 :

연번	관리번호(S/N)	매체형태	등록일자	취급자(성명)	불용처리일자	불용처리방법(재사용용도)	비고(사유)

보조기억매체 관리대장(비밀용)

부서:　　부서정보보안담당관 :

연번	관리번호(S/N)	매체형태	등록일자	취급자(성명)	불용처리일자	불용처리방법(재사용용도)	비고(사유)

보조기억매체 관리대장(공인인증서용)

부서 :　　부서정보보안담당관 :

연번	관리번호(S/N)	매체형태	등록일자	취급자(성명)	용도	해지일자	해지사유

【별지 제11호 서식】

보조기억매체 점검대장

부서 :　　부서정보보안담당관 :

점검일시	현 보유수량					이상 유무	점검관		비고 (서명)
	II급	III급	대외비	일반	인증		성명	서명	

【별지 제12호 서식】

원격근무 보안서약서

본인은 년 월 일부로 원격근무를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 나는 부여받은 인증 관련 정보 및 매체를 타인에게 유출하지 아니한다.

2. 나는 원격근무 중 작성·저장·열람·출력한 문서는 업무 목적에만 활용하고 타인에게 유출하지 아니한다.

3. 나는 원격근무용 소프트웨어 및 전산장비를 업무목적에만 활용하며 바이러스 백신 프로그램 및 기타 보안 프로그램을 설치하여 최신 상태로 유지한다.

4. 나는 여타 보안사항들을 성실히 준수하며 위반 시 관련규정에 따라 처벌도 감수한다.

20 년 월 일

서 약 자 소 속 :
직 급 :
성 명 : (서명)

서약집행자 소 속 :
직 급 :
성 명 : (서명)

【별지 제13호 서식】

정보보안정책 변경관리대장

구분	변경일자	변경 전	변경 후	사유	비고
추가					
수정					
삭제					

【별지 제14호 서식】

침해사고 비상연락망

1. 침해사고대응팀 연락망

담당업무	담당자	집전화번호	휴대전화번호	E-mail
침해사고대응팀장				

2. 팀별 보안책임자, 담당자 연락망

팀명	담당자업무	담당자	연락처(E-mail, HP, office)

3. 관련 업체 연락망

기관명	담당자	연락처(HP, office, e-mail)	비고
침입차단시스템			

4. 유관 공공기관 연락망

기관명	담당자	연락처 (E-mail, Mobile, Office)	URL
국가사이버안전센터		02-3432-0462	http://www.ncsc.go.kr
한국정보보안진흥원 (인터넷침해사고대응센터)		02-118	http://www.kisa.or.kr http://www.krcert.or.kr
경찰청 사이버테러 대응센터			http://www.ctrc.go.kr

【별지 제15호 서식】

침해사고 발생보고서

결재	분임정보보안담당관	정보보안담당관	정보보안책임관

발견일자		발견자	
침해사고 개요			
1) 발견시스템 : 2) 현상 : 3) 파급 영향 : 4) 협조요구 항목 5) 기타 :			
긴급성 여부			

긴급조치일자		긴급조치담당자	
긴급조치내용 요약			

【별지 제16호 서식】

침해사고 처리 결과서

결재	분임정보보안담당관	정보보안담당관	정보보안책임관

작성 일자		작성 부서		작성자	
문제발생 일시					
대상시스템					
문제내용					
문제 원인					

조치시간		조 치 자	
사고원인		피해 범위	
조치내용 및 결과			
향후 대책			

【별지 제17호 서식】

정보보안 서약서(용역업체 대표자)

_____(주) 대표이사 _____은 20 . . 부터 사업 종료시까지 수행하는 「(사업명) 」의 주관사업자로서 참여함에 있어 사업수행 기간 중 취득한 사항에 대해 비밀을 엄수하고 법인 또는 개인의 영리를 목적으로 이용하지 않으며, 이를 위반하여 발생되는 보안상의 책임과 관련법령에 의한 조치를 따를 것을 각호와 같이 서약합니다.

1. 당사는 금강대학교에서 업무를 수행함에 있어 알게 된 내부정보, 개인정보, 기타 모든 업무에 관련된 정보를 제3자에게 제공하거나, 공개 또는 누설하지 않을 것이며, 금강대학교의 사전 동의 없이 무단 사용하지 않겠습니다.

2. 당사는 금강대학교로부터 업무수행을 위하여 명시적으로 접근을 허가 받은 시설과 정보만을 이용하겠습니다.

3. 당사는 금강대학교의 사전 동의 없이는 내부정보 및 기타 개인정보와 관련된 모든 문서나 자료 및 결과물 등을 어떠한 형태로도 외부로 반출하지 않겠습니다.

4. 당사는 업무가 종결되거나 금강대학교의 요청이 있는 경우, 교대학교가 제공한 모든 자료와 자산을 즉시 반납하겠습니다.

5. 당사는 업무수행의 결과 산출된 모든 결과물(보고서, 도면, 컴퓨터 프로그램, 장치 등)에 대한 제반 권리가 금강대학교에 귀속됨을 인정하고, 금강대학교 이에 대한 권리를 행사하는데 협조하겠습니다.

6. 만일 본 서약 사항을 위반하였을 경우에 당사는 법령이 정한 바에 따라 민·형사상의 모든 책임을 부담하겠으며, 본 서약 위반 행위로 인하여 금강대학교에 발생한 모든 손해를 배상하겠습니다.

20 년 월 일

용역업체명: _____ 대 표 자 : _____(인)

금 강 대 학 교 총 장 귀 하

【별지 제18호 서식】

열람·제공자료 관리대장

사 업 명 :
사업주관기업 :

용역업체 관리담당자	용역업체 관리책임자

연번	자료명	인계 및 인수				자료 반납	
		인계자	인수자	월일	장소	확인자	월일

【별지 제19호 서식】

보안자료 반납 및 파기 완료 확약서

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

1. 본 업체는 업체 및 사업 참여자가 사업수행 중 지득한 모든 자료를 반납 및 파기하였으며, 지득한 정보에 대한 유출을 절대금지 하겠습니다.

2. 본 업체 직원의 과실은 곧 당사의 과실이며 이로 인해 발생하는 금강대학교의 손해에 대해서는 당사에서 책임지겠습니다.

3. 본 업체는 보안사항을 위반했을 경우에 민·형사상 및 보안상의 책임과 관계법규에 의한 조치에 따를 것을 서약하오며 이에 확약서를 제출합니다.

20　　년　　월　　일

업체 (단체) 명 :
주　　소 :
사업자등록번호 :
성　　명 :　　(서명)

금 강 대 학 교 총 장 귀 하

【별지 제20호 서식】

시스템 백업일지

분임정보 보안담담관	정보보안 담당관	정보보안 책임관

장비명	백업대상	백업방법	백업 주기	최소보관 기간	운영 담당자

【별지 제21호 서식】

내부감사 점검항목

1. 정보보안 관리규정

구분	점검항목
지침/매뉴얼 관리	주기적으로 정보보안 관리규정 및 지침을 검토하여 변경사항 발생시 개정하였는가?
	정보보안 관리 규정 및 지침 개정 시 관련담당자들에게 개정 내용을 전달하였는가?
정보보안 업무 계획	보안업무 세부추진 계획을 수립하였는가?
보안 심의	보안심사 위원회에 심의를 요구한 경우 관련 문서들을 보관하고 있으며, 심의 결정사항을 이행하고 있는가?
운영검토	정보보안 관리체계 운영검토를 실시하였는가?

2. 정보보안 관리체계 내부심사 매뉴얼

구분	점검항목
계획 및 이행	연간 내부심사 계획을 수립하고 이행하였는가?
결과 보고 및 시정	이전 내부심사 지적사항을 이행하였는가?
	내부심사 결과를 정보보안담당관에게 보고하였는가?
	내부심사 결과 지적된 사항에 대한 시정조치계획을 수립하였는가?
	시정조치계획에 따라 이행하였는가?

3. 침해사고 대응 매뉴얼

구분	점검항목
침해사고 대응	침해사고 발생시 발견자는 침해사고 신고서를 작성하여 신고하였는가?
	침해사고 대응을 위해 지식정보보호 전문업체에 기술지원을 요청했을 경우, 보안서약서를 청구하였는가?
	발생된 침해사고에 대한 사고 분석을 실시하였는가?
	중대한 침해사고가 발생되었을 경우, 침해사고 대응센터를 운영하였는가?
사후 관리	동일한 침해사고가 발생되지 않도록 교육 및 감시 활동 등의 사후관리를 수행하였는가?

4. 정보자산 및 위험관리 매뉴얼

구분	점검항목
자산 관리	정보자산의 변경사항이 발생한 경우 정보자산관리 목록을 갱신하였는가?
	응용시스템 및 서버를 대상으로 연1회 자산 중요도 평가를 수행하였는가?
	등록된 정보자산에 대하여 라벨을 부착하였는가?
위험분석	연1회 위험분석을 실시하였는가?
	각 팀장은 위험분석 결과를 바탕으로 하여 수용 가능한 위험의 수준(DoA)을 정하고 관리대상 위험을 식별하였는가?
	정보보호대책 명세서 및 단계별 위험관리 방안을 작성하였는가?
	정보보호 적용성 보고서를 작성하여 관리하고 있는가?

5. 외주 보안관리 매뉴얼

구분	점검항목
일반사항	제3자 및 외부위탁 계약 시 계약서 등에 보안 요구사항을 반영하여 체결하였는가?
	참여인원의 친필서명이 들어간 보안서약서를 징구하였는가?
내부자료 보안	제공된 내부자료에 대해 자료관리대장을 작성하여 관리하고 있는가?
	업무 수행을 위해 제공하는 내부 자료를 안전하게 보관하고 있는가?
장비 보안관리	참여인원의 PC 반입 시 바이러스 백신 프로그램 설치 및 바이러스 감염 여부를 확인하였는가?
	반입된 PC는 업무 종료 시까지 반출되지 않도록 통제하고 있는가?
내외부망 접근에 대한 보안관리	사용자 계정은 하나의 그룹으로 등록하고 사용자 계정별로 정보시스템에 접근권한을 부여하였는가?
	사용자 계정별로 부여된 권한은 불필요 시 곧바로 권한을 해지하거나 계정을 폐기하였는가?

6. 정보보안 교육훈련 매뉴얼

구분	점검항목
계획 수립	연간 정보보안 교육계획을 수립하였는가?
기본교육 실시	각 팀장은 팀원들을 대상으로 분기별 1회 이상 정보보안 기본교육을 실시하고 있는가?
	각 팀장은 신규직원에 대해 발령 후 1개월 이내에 정보보안 기본교육을 실시하는가?
	외주업체 인원에 대해서 용역 실시단계에서 필요한 정보보안 기본교육을 실시하는가?
전문교육 실시	정보보안 전문교육을 실시하였는가?

7. PC/LAN사용자 보안 매뉴얼

구분	점검항목
PC 관리	개인소유 등 인가 받지 않은 PC가 반입되어 있는가?
	반출된 PC(노트북)에 대해 중요자료를 백업 후 제거하여 반출하며, '전산장비 반출입대장'에 관련 내용을 기록하였는가?
	파일 및 디렉토리 공유설정을 금지하였는가? 부득이 공유설정 시 암호설정 후 사용하고 있는가?
	PC 부팅 시 CMOS 패스워드를 설정하고 있는가?
	PC 로그인 및 화면보호기에 암호를 설정하고 있으며, 화면보호기 대기시간은 10분 이하로 설정되어 있는가?
	백신 프로그램이 설치되어 있으며, 최신버전으로 유지하고 있는가?
	최신 윈도우 보안 패치를 설치하였는가?
	PC내에 비밀문서가 저장되어 있는가?
	PC에 불법 소프트웨어가 설치되어 있는가?
	사용자는 월1회 바이러스, 불법 소프트웨어 설치 유무를 점검하고 있는가?
LAN 사용 통제	외부 사용자가 LAN 사용 시 'LAN 사용신청서'와 'LAN 사용 보안 서약서'를 작성하여 분임보안담당관에게 제출하였는가?
데이터 백업	필요한 데이터는 적절하게 백업하고 있는가?
	데이터 백업매체는 시건 장치가 되어 있는 장소에 보관하고 있는가?

8. 응용시스템 보안관리 매뉴얼

구분	점검항목
개발 및 운영의 분리	개발 및 테스트 시스템과 운영시스템은 분리되어 있는가?
	개발에 필요한 도구가 운영환경에 설치되어 있는가?
요구사항 분석	시스템의 도입 미치 개발 발주 시 중요도에 따라 보안기능 요구사항을 검토 후 반영하였는가?
	보안기능을 반영하여 요구사항을 분석하고, 설계하고 있는가?
보안 기능의 설계	응용시스템 관리자 모듈과 사용자 모듈을 분리하고 별도의 관리자 인증을 수행하고 있는가?
	응용시스템 관리자 모듈의 사용자 계정 및 비밀번호 입력이 3회에 걸쳐 일치하지 않을 때 해당 접속을 중지시키고 비인가자 침입 여부를 확인할 수 있도록 설계되어 있는가?
	패스워드 생성기준은 숫자와 문자 등으로 8자리 이상으로 정하고 주기적으로 변경하도록 설계되어 있는가?
	모든 입력 데이터에 대하여 유효성 점검을 수행하도록 설계되어있는가?

	화면상에 패스워드와 같은 민감한 데이터가 평문으로 보이지 않도록 되어 있는가?
	비밀성을 요하는 데이터는 암호화하여 저장하고 있는가?
	중요한 응용시스템의 경우 관리자와 사용자의 중요한 활동에 대한 감사 로그를 생성하고 있는가?
응용시스템의 테스트	응용시스템 테스트 시 임의의 테스트 데이터를 생성하여 활용하거나 운영 데이터를 가공하여 사용하며, 실제 운영 데이터의 사용을 금하고 있는가?
	입력데이터의 유효성 점검을 실시하고 있는가?
응용시스템의 설치	응용시스템의 설치 시 테스트 시나리오를 작성하여 승인을 득하였는가?
응용시스템의 변경관리	응용시스템의 변경사항이 발생한 경우 변경 요청서를 작성하여 응용시스템 관리 팀장에게 변경을 요청하였는가?
	변경 요청의 타당성 검토 후 변경하고 관련 내용을 기록하고 있는가?
	긴급한 상황 하에서 승인절차를 생략하고 응용시스템을 변경한 경우 사후 승인을 득하였는가?
소스 관리	프로그램 소스는 운영중인 시스템에 저장하여 관리하는 것을 금하고 있는가?
	프로그램 소스 접근을 통제하고 접근기록을 남기고 있는가?
	개발 중이거나 유지보수 중인 프로그램은 운영중인 프로그램의 소스와 분리하여 관리하고 있는가?
계정 및 권한관리	사용자 계정의 등록(신규, 추가, 변경, 삭제 등) 사유가 발생할 경우 양식을 이용하여 신청하고 있는가?
	사용자 계정에 대해 사용자 ID 관리 대장에 기록하고 있는가?
	분기별로 사용자 계정에 대해 재확인을 실시하여 삭제, 중지, 등록 등 필요한 조치를 취하고 있는가?
	퇴직자 및 전출자의 계정을 적시에 삭제하고 있는가?
	응용시스템 사용자들의 권한관리를 실시(정기적 권한의 적절성 검토)하고 있는가?
	응용시스템 접속 한 후 일정시간 동안 어떤 입력도 일어나지 않을 경우 자동적으로 세션을 중단시키도록 해당 시스템을 설정하고 있는가?
백업	소스 파일을 변경 시마다 백업하여 안전한 장소에 보관하고 있는가?
모니터링	응용시스템이 처리하는 중요정보에 대한 접근 기록을 3개월 이상 보관하고 있는가?
취약점 점검	외부 응용시스템의 이관 시에 수시 취약점 점검을 실시하고 있는가?
	종합점검 및 수시점검 시 발견된 취약점에 대하여 보완계획을 수립하고 이행하였는가?

9. 서버 보안관리 매뉴얼

구분	점검항목
신규 도입	서버 신규 도입 시 보안성 검토를 요청하고, 결과에 따라 조치하였는가?
	신규로 도입 설치되는 서버시스템에 취약점 점검을 실시하고, 발견된 취약점을 조치토록 하였는가?
	취약점 조치 권고안에 따라 조치가 불가하거나 불가피하게 적용되어야 할 사항에 대해 보안규정 예외적용신청서를 작성하였는가?
소프트웨어의 설치	서버에 설치된 소프트웨어의 현황을 관리하고 있는가?
	업무 목적 외 또는 불법 소프트웨어는 설치되지 않았는가?
	원격관리 소프트웨어 설치에 대한 보안대책을 수립하고 승인을 받았는가?
보안설정	서버에 주기적으로 보안 패치 및 보안설정을 적용하고 있는가?
	모든 서버는 로그인을 허용하기 전에 보안권고문을 공지하고 있는가?
계정 생성 및 관리	사용자 계정의 등록(신규, 추가, 변경, 삭제 등) 사유가 발생할 경우 양식을 이용하여 신청하고 있는가?
	사용자 계정 생성 절차 및 규정을 따르고 있는가?
	서버 사용자 계정에 대해 사용자 ID 관리 대장에 기록하고 있는가?
	기 사용된 계정은 최소 1년 동안 다른 사용자에게 재부여하지 않는가?
	디폴트 계정은 삭제하였는가? 예외로 사용 시 패스워드를 변경하였는가?
	60일 이상 사용자 계정이 사용되지 않을 경우 일시 중지시키며, 일시 중지된 후부터 60일간 사용요청이 없는 경우 계정을 삭제하고 있는가?
	분기별로 사용자 계정에 대해 재확인을 실시하여 삭제, 중지, 등록 등 필요한 조치를 취하고 있는가?
	퇴직자 및 전출자의 계정을 적시에 삭제하고 있는가?
패스워드 생성 및 관리	패스워드 길이는 최소 8자 이상인가?
	접근시도 패스워드가 3회 이상 일치하지 않을 경우 접속이 거부되고 있는가?
	사용자가 패스워드를 사용할 수 있는 최대기간(1회/1월) 및 사용해야 하는 최소기간(1일)을 설정하고 있는가?
	사용자가 과거에 사용했던 패스워드를 최소 6개월 이내에 사용하지 못하도록 하고 있는가?
	패스워드는 암호화되어 저장되며, 화면에 읽을 수 있는 형태로 표시되지 않고 있는가?
	서버관리자에 의해 부여된 초기 패스워드는 사용자가 처음 접속 시 자신의 패스워드로 변경하도록 강제화하고 있는가?

권한 관리	사용자 접근권한 신청 및 검토 절차를 준수하였는가?
	일반사용자의 타 사용자 디렉토리 등에 대한 접근권한 제한을 하였는가?
	일반사용자에게 관리자 권한을 부여하지 않았는가?
접근통제	중요 서버 접근 시 SSH 등 암호화된 통신 프로토콜을 사용하는가?
	로그인 화면에서는 로그인 관련 정보외의 정보를 보여주지는 않은가?
	로그인 실패 시 시스템 침해의 원인이 될 정보를 보여주지는 않은가?
	로그인 성공 시 최근 접속 시간, 날짜, 터미널 등의 정보를 보여주는가?
	서버에 접속한 후 사용자나 다른 시스템으로부터 일정시간 동안 어떤 입력도 일어나지 않으면 자동적으로 로그오프 시키거나 세션을 중단시키고 있는가?
	통제구역 이외의 장소에 설치된 서버에 화면보호기가 설정되어 있는가?
	시스템 관리자들이 원격접속을 수행하고 있는가? 원격접속시 안전한 방법으로 로그인 및 통신하고 있는가?
	업무상 불필요한 서비스는 제거하였는가?
패치/시스템 파라미터 관리	패치나 시스템 파라미터를 변경할 때 그와 관련된 모든 사항에 대한 기록을 남기고 있는가?
백신 설치 및 운영	윈도우 서버의 경우 바이러스 백신이 설치되고, 최신 업데이트가 되어있는가?
	바이러스 감염 시 담당자에게 신고 등의 절차를 준수하는가?
무결성 점검	시스템 무결성을 검증하는 틀을 이용하여 정기적으로 시스템에 대한 무결성을 검하고 있는가?
인터넷 서버 운영	웹서버와 메일서버는 분리해서 운영하고 있는가?
취약점 점검	년1회 이상 취약점에 대한 종합점검과 수시점검을 실시하고 있는가?
	점검 결과 발견된 취약점에 대한 보완계획을 수립하여 이행하는가?
	단기 조치가 어려운 취약점에 대하여 사유를 기록, 관리하는가?
로그관리	침해사고 발생시 추적성을 확보하기 위해 로그를 남기고 있는가?
	모든 서버들의 내부시각이 일치하는가?
	시스템 접속 로그는 최소 3개월 이상 보관하고 있는가?
백업 및 매체 관리	백업계획에 따라 백업을 수행하고 있는가?
	백업 매체는 비인가자가 접근할 수 없도록 격리되어 보관하는가?
	백업매체의 폐기 시 승인을 얻고 소각하는가?
운영 및 폐기	데이터센터 SOP에 따라 성능/용량/장애/변경관리가 이루어지고 있는가?
	철수 또는 폐기 시 자료가 유출되지 않도록 보안대책을 강구하였는가?

10. 데이터베이스 보안관리 매뉴얼

구분	점검항목
보안설정의 적용	OS상의 사용자 계정 및 파일시스템의 접근제어를 설정하였는가?
	불필요한 디폴트 계정은 삭제하였는가? 필요 시 패스워드를 변경하였는가?
	DBMS에 대한 취약점 제거 및 패치를 수행하였는가?
계정관리	서비스 제공을 위한 ID 이외에 ID를 공동으로 사용하지 않고 있는가?
	ID 신청 시 ' 사용자 ID 등록/삭제/권한변경 요청서'를 작성하여 신청하고 있는가?
패스워드 관리	패스워드 길이는 최소 8자 이상인가?
	접근시도 패스워드가 3회 이상 일치하지 않을 경우 접속이 거부되고 있는가?
	사용자가 패스워드를 사용할 수 있는 최대기간(1회/1월) 및 사용해야 하는 최소기간(1일)을 설정하고 있는가?
	사용자가 과거에 사용했던 패스워드를 최소 6개월 이내에 사용하지 못하도록 하고 있는가?
	패스워드는 암호화되어 저장되며, 화면에 읽을 수 있는 형태로 표시되지 않고 있는가?
	서버관리자에 의해 부여된 초기 패스워드는 사용자가 처음 접속 시 자신의 패스워드로 변경하도록 강제화하고 있는가?
	서비스 특성상 취약한 패스워드를 사용할 경우 보안규정 예외적용 신청서를 작성하여 서버시스템 운영팀장에게 제출하고 있는가?
사용자 ID의 등록 및 삭제	신규 ID 등록 시 요청서의 접수, 검토 등의 절차를 준수하는가?
	사용자 ID의 등록 삭제 시 'DBMS 사용자 현황'을 작성하여 관리하는가?
접근권한	DB 사용자를 데이터 갱신이 가능한 사용자와 조회만 가능한 사용자로 구분하여 운용하고 있는가?
	DB 설계자와 DB 관리자의 임무가 분리되어 있는가?
접근통제	DBMS 설치 소프트웨어 라이브러리 또는 DB 운영체제 파일의 변경은 DB 관리자만이 가지고 있는가?
	DBMS가 제공하고 있는 유틸리티 프로그램의 사용권한은 DB 관리자로 제한하고 있는가?
	데이터베이스 업무팀의 장은 데이터베이스 갱신 유틸리티(isqldbaccess, sqlplus 등)의 사용을 작업의뢰서에 의해서만 허락하며 작업 내역을 일일 관리하고 있는가?
	사용자에게 부여된 권한을 주기적을 재평가 하고 있는가?
	DB에 대한 추가 접근권한이 필요한 자는 '사용자 ID 생성/권한변경/삭제 요청서'를 작성하여 의뢰하고 있는가?

백업 및 복구	주기적으로 백업 및 소산하고 있는가?
	DB 장애 발생시 DBMS 장애 내역 보고서를 작성하여 보고하고 있는가?
	DBMS 복구 테스트를 주기적으로 실시하고 있는가?
로그관리	DB 보안관련 사항에 대한 로그를 저장하고 있는가?
운영관리	DB 운영과 관련하여 DB 월별 현황, 장애보고서, 유지보수 업체 작업일지, DBA 지원 비상연락망 등을 작성하고 있는가?

11. 네트워크 보안관리 매뉴얼

구분	점검항목
도입	네트워크 시스템 신규 도입 시 필요할 경우 성능 시험을 실시하고 있는가?
운영절차	네트워크 시스템은 보호구역에 설치되어 있는가?
	IP별 접근제어 정책을 구성하여 일반 사용자가 시스템에 접근할 수 없도록 보안 설정을 적용하고 있는가?
	시스템 로그인을 허용하기 전에 보안 권고문을 공지하고 있는가?
	네트워크 계정 등록, 변경, 삭제 시 '사용자 계정 생성/권한변경/삭제 요청서'를 작성하여 신청하고 있는가?
	네트워크 시스템간의 시간을 동기화 하고 있으며, 주기적으로 이를 점검하고 있는가?
접근통제	로그인 전에 불법사용에 대한 경고 메시지를 제시하고 있는가?
	사용자에게 부여된 권한을 월1회 이상 재확인하여 조치하고 있는가?
	연속적으로 3회 이상 패스워드를 잘못 입력할 경우 세션을 차단시키고 있는가?
	시스템 관리자들이 원격접속을 수행하고 있는가? 원격접속시 안전한 방법으로 로그인 및 통신하고 있는가?
무결성 점검	월 1회 이상 구성정보(Configuration)을 검토하며, 네트워크 시스템 구성정보에 대한 백업을 실시한 후 시스템에 대한 무결성을 검토하고 있는가?
패치 및 구성 정보 변경 통제	패치나 시스템 파라미터를 변경할 경우 관련 기록을 남기고 있는가?
	구성정보나 네트워크 시스템을 변경할 경우 '네트워크 시스템 환경설정 변경 보고서'를 작성하여 팀장 승인 하에 작업을 수행하는가?
	네트워크 시스템 로그 정보를 정기적인 시스템 백업 시 함께 백업하고 1년 이상 보존하고 있는가?
취약점 점검	년 1회 이상 정기적으로 취약점 점검을 실시하고, 조치사항을 이행하고 있는가?
시스템 성능 관리	시스템 성능 네트워크 시스템에 대한 성능을 주기적으로 검토하여 보고서를 작성하고 있는가?
백업 및 매체 관리	네트워크 시스템 구성정보에 대한 백업을 실시하고 있는가?
장애관리	장애 발생시 장애 내역 보고서를 작성하여 팀장에게 보고하고 있는가?

12. 정보보안시스템 운영 매뉴얼

구분	점검항목
접근통제	정보보안시스템은 콘솔에서 직접 작업을 하며, 모뎀을 연결해서 직접 접속하거나 인터넷 등 외부에서 원격 접속하는 것을 금지하고 있는가?
	원격관리가 필요한 경우 팀장의 승인을 받아 분임정보보안담당관에 통보하였는가?
	정보보안시스템 고유의 서비스와 자체 보안을 강화하기 위한 응용프로그램만 운영하고 있는가?
	업무상 사용자 계정 등록이 필요한 경우 '정보보안시스템 사용자 계정 등록/변경/재발급/삭제 요청서'를 작성하여 사용자를 등록하고 있는가?
보안정책	룰셋을 등록, 변경할 필요가 있는 경우 '정보보안시스템 Rule 등록(변경/삭제) 요청서'를 작성하여 적용하고 있는가?
	분기별 1회 이상 정보보안시스템 보안정책을 점검하여 사용하고 있지 않거나 사용기간이 경과된 룰셋을 삭제하고 있는가?
	패킷필터링 관리대장, 서비스 관리대장, 침입차단시스템 점검관리 대장, 상세 연결내용을 포함한 구성도, 침입차단시스템 제품 및 버전, 운영체제명 및 버전 등을 문서화하여 보관하고 있는가?
로그 및 백업	정보보안시스템의 로그를 매월 분석하여 그 결과를 보관하고 있는가?
	구성정보는 HDD 등에 매주 1회 이상 백업하며 2주 이상 보관하고 있는가?
	로그의 복사본을 별도의 장소에 보관하고 있는가?
	로그는 테이프 등에 매일 1회 이상 백업하여 3개월 이상 보관하고 있는가?
	백업매체는 안전한 방법으로 폐기되고 있는가?
점검	분기별로 1회 이상 정보보안시스템을 점검하고 있는가?
	시스템 무결성 파일을 정기적으로 점검하여 변경, 교체, 삭제된 파일의 리스트를 작성하여 관리하고 있는가?
	로그분석이 제대로 수행되고 있는지 월1회 이상 감사하고 있는가?

13. 웹메일 운영 매뉴얼

구분	점검항목
웹 메일 보안	내부 정보를 외부로 송신하기 위해서는 사전에 그 타당성에 대해 해당 전결권자의 승인을 득하며 선택적으로 암호화하여 전송하고 있는가?
	e-mail 계정 신청/삭제는 e-mail 시스템 관리자에게 요청하고 있는가?
	한명의 직원이 1개의 e-mail 계정을 가지고 있는가?
	e-mail 패스워드를 주기적으로 변경하고 있는가?
	e-mail을 통한 업무자료 수발신은 내부 전자문서시스템을 사용하고 있는가?
	비정상적인 메일(대량의 스팸메일, 바이러스 첨부메일 등)을 대응하기 위해 모니터링을 하며 차단하고 있는가?
	e-mail 사용과 관련한 보안사고 인지 시 침해사고대응매뉴얼에 따라 대응하며, 관련 내용을 E-Mail 보안사고 및 대응 결과서에 기록하고 있는가?

14. 물리적 보안관리 매뉴얼

구분	점검항목
보호구역 설정	보호구역을 적절히 설정 하였는가?
전산장비실 관리	출입문 상단 중앙에 통제구역의 표찰을 부착하고 있는가?
	전산장비실에 상주하는 외부인력은 신원조회를 실시하여 근무적격 여부를 판단하고 있는가?
	전산장비실 창문은 개폐 및 분리가 않되고 있는가?
	감시 카메라 및 출입통제장치를 설치하고 있는가?
출입통제	보호구역 출입자 명부를 비치하여 출입 시마다 기록을 유지하는가?
	반출입되는 모든 가방, 서류, 기타휴대폰 정보시스템 등은 필요 시 검색할 수 있으며, 사진기, 녹음기, 비디오 장비는 반입을 불허하고 있는가?
	출입문을 항상 닫아놓고, 비인가자의 출입을 금지 하는가?
방재시스템 관리	방재시스템은 적정하며 잘 관리되고 있는가?
장비관리	대용량 착탈식 디스크, CD-ROM Writer 등과 같은 휴대용 정보시스템의 사용을 제한하고 있는가?
	장비 폐기 전에 저장매체로부터 중요한 데이터 라이센스가 있는 소프트웨어가 제거되었는지 확인하고 있는가?
자료 보안	문서는 안전하게 파지 또는 소각하고 있는가?
	주요 서류 및 이동형 저장매체를 사용하지 않을 경우 시건 장치가 있는 캐비닛이나 창고에 보관하고 있는가? (비품 등과 함께 보관되어 있는가?)
사무실 보안	사무실 정리 정돈을 적절히 수행하고 있는가?

15. 기타

구분	점검항목
업무연속성 계획의 시험 및 유지관리	업무연속성계획서(재난복구대책 등)가 수립되어 있으며, 현 상황에 맞게 지속적으로 업데이트 되고 있는가?
	재해 대응을 위해 주기적으로 모의훈련을 실시하고 있는가?
	재해 대응을 위해 업무연속성관리 조직이 구성되어 있고, 각 담당자들이 자신의 역할을 충분히 인지하고 있는가?
	해당 담당자나 직원들에게 업무연속성(BCP)에 대한 교육이 적절히 이루어지고 있는가?
준거성	홈페이지에서 제공하는 개인정보보호 방침 내에 개인정보보호 관리책임자가 실제 담당자와 일치하는가?
	정보보안관련 법을 포함한 법적, 계약적 요구사항을 식별하여 대응할 수 있도록 방안을 수립하는 담당자가 지정되어 있는가?