정보보안 세부관리 지침

□ 제정 : 2011. 10. 01.
□ 개정 : 2013. 10. 01.
□ 개정 : 2016. 04. 01.
□ 개정 : 2017. 01. 01.

제1장 개요

제1조(목적) 이 지침은 수원대학교(이하 ‘학교’라 한다) 정보관리규정 제28조에 따라 학교 정보자산이 불법 유출 · 파괴 · 변경 되는 것으로부터 안전하게 보호하며, 네트워크 및 각종 정보시스템등 정보운영 환경과 응용프로그램을 보다 안전하고 신뢰성 있게 운영하여 본교 전산망 사용자에게 원활한 서비스를 제공하는데 필요한 세부사항을 정함을 그 목적으로 한다.

제2장 정보보안 기본 지침

제2조(정보보안담당관 책무)

① 교육부 정보보안기본지침 제2장, 제5조 “정보보안담당관 운영”에 의거하여 다음과 같은 기본활동을 부여한다.

1. 정보보안 정책 및 기본계획 수립 · 시행
2. 정보보안 관련 규정 · 지침 등 제 · 개정
3. 정보보안심사위원회에 정보보안 분야 안건 심의 주관
4. 정보보안 업무 지도 · 감독, 정보보안 감사 및 심사분석
5. 정보통신실, 정보통신망 및 정보자료 등의 보안관리
6. 정보보안 수준진단
7. 정보보안 사고 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. 주요정보통신기반시설 보호활동
13. 국가용 보안시스템 및 암호키의 운용・보안관리
14. 국가정보원장이 개발하거나 안전성을 검증한 암호모듈・정보보호시스템의 운용 및 보안관리
15. 정보통신망 보안대책의 수립 · 시행
16. 그 밖에 정보보안 관련 사항

제3조(시스템 보안책임)

① 학교에 필요한 일체의 정보시스템(PC · 서버 · 네트워크장비 등 포함)을 도입 · 사용할 경우, 사용자 · 시스템관리자 및 관리책임자를 지정 운용하여야 한다.

② 사용자는 개인PC 등 소관 정보시스템을 사용하거나 본인 계정으로 정보통신망에접속하는 것과 관련한 일체의 보안 및 관리 책임을 가진다.

③ 시스템관리자는 서버 · 네트워크 장비 등 부서 공통으로 사용하는 정보시스템의 운용과 관련한 보안책임을 가진다.

④ 제1항 내지 제3항과 관련하여 정보시스템을 실제 운용하는 부서의 과장 또는 처장이 정보시스템 '관리책임자'가 되며, 관리책임자는 정보시스템 관리대장을 수기 또는 전자적으로 운용 관리하여야 한다.

⑤ 관리책임자는 해당 부서의 정보시스템 관리대장에 정보시스템의 변경 최종 현황을 유지 및 관리하여야 한다.

⑥ 정보보안담당관은 제1항 내지 제5항에 명시된 정보시스템 운용과 관련한 보안 취약점을 발견하거나 보안대책 강구가 필요하다고 판단할 경우, 사용자 · 시스템관리자 및 관리책임자에게 시정을 요구할 수 있다.

제4조(정보보안 감사)

① 정보보안담당관은 연1회 이상 자체 정보보안 감사를 실시하여야 한다.

② 정보보안 담당관은 교육부 정보보안기본치짐 제2장, 제6조 "활동계획 수립 및 심사분석"에 따른 정보보안업무 세부추진계획 및 심사분석 결과 문건을 자체 보관한다.

③ 정보보안 담당관은 정보보안 감사의 효율적 수행을 위하여 교육부장관에게 감사 방향, 감사 중정사함, 감사관 지원 등 업무협조를 요청할 수 있다.

제3장 PC 및 바이러스 보안지침

제5조(CMOS 인증)

① 부팅 후 CMOS에서 패스워드를 설정함으로써 논리적인 접근통제가 이루어지도록 한다.

② CMOS 패스워드는 PC 사용자만이 알 수 있도록 설정한다.

③ 부팅시 Del키 혹은 F2키 등을 사용하여 CMOS 설정화면으로 들어간다. 각 시스템 마다 해당 키가 다르므로 초기 부팅화면에서 확인해 둔다.

④ CMOS 사용자 패스워드 설정 : 타인의 무단 이용에 의한 정보유출 및 데이터 파괴를 방지하기 위하여 CMOS 사용자 패스워드를 설정하여 부팅 초기에 패스워드 인증과정을 거치도록 한다.

⑤ CMOS 관리자 패스워드 설정 : 타인이 함부로 CMOS 설정에 들어가 CMOS 사용자 패스워드를 무단으로 변경시키는 것을 방지하기 위해 CMOS 관리자 패스워드를 설정해 둔다.

제6조(화면보호기)

① 모든 PC에 화면보호기를 설정하여 조작자가 잠시 자리를 비운 사이에 비인가자가 그 PC를 이용하여 작업하는 것을 방지하기 위하여 10분 이상 PC 작업 중단 시 비밀번호

가 적용된 화면보호 조치한다.

② 화면보호기는 적절한 패스워드로 보호되어야 하며, 화면보호기의 패스워드는 응용시스템용 패스워드와 다른 것을 사용하도록 한다.

③ 화면보호기는 윈도우에서 기본적으로 제공하는 것을 사용하도록 하며, 설치시 Ctrl+Alt+Del 키로 화면보호기가 없어지지 않도록 해당 파일에서 환경을 설정하도록 한다.

④ 시스템관리 목적상 제약이 발생되는 조건에서는 예외로 한다.

⑤ CD 자동실행으로 인하여 패스워드 입력 없이 화면보호기가 풀리게 되는 Win9x 취약점 이용을 방지하기 위해 CD 자동삽입 알림을 비활성화 시킨다.

제7조(사용자 패스워드)

① 사용자의 패스워드는 비밀로 유지하고 타인에게 노출하지 않도록 한다.

② 사용자가 관리자에게서 임시 패스워드를 부여 받은 경우 첫 번째 로그인시 패스워드를 변경해야 한다.

③ 패스워드를 별도의 문서에 적어 놓거나 보호되지 않은 형태로 PC에 저장해서는 아니된다.

④ 영문과 숫자를 혼용해 9자 이상의 패스워드를 사용한다.

⑤ 주민번호, 전화번호, 생일, 사전에 나오는 단어 등 임의 추측이 가능한 패스워드를 피하고 문장의 첫 글자 조합을 이용하는 등의 방법으로 패스워드를 만든다.

⑥ 소프트웨어 설치 후 공급자의 패스워드 기본값을 변경한다.

⑦ 패스워드가 타인에게 노출되었거나 노출이 우려될 경우 반드시 패스워드를 변경해야 한다.

제8조(공유)

① 업무상 필요한 경우를 제외하고는 공유를 하지 않으며, 부득이하게 공유를 사용할 경우 패스워드를 부여해야 한다.

② 공유는 전체 디스크를 대상으로 해서는 아니 되며, 최소한의 파일만 공유해야 한다.

③ 가능한 공유 이름 입력시 “$” 표시를 하여 네트워크 환경 상에 자신의 공유 폴더가 나타나지 못하게 한다.

제9조(PC데이터의 보관)

① PC는 일반 사용자의 접근이 가능하기 때문에 비밀 정보의 노출 위험이 존재하므로 가능한 비밀 정보를 보관하지 않으며, 삭제 시 복원할 수 없도록 휴지통 비우기 등의 조치를 취한다.

② 비밀 정보는 접근권한이 설정되어 있는 정보 서버에 저장되는 것을 원칙으로 한다.

③ 업무상 부득이하게 비밀 및 대외비 정보를 저장해야 하는 경우 패스워드 혹은 암호화 기법 등을 이용해 보안성을 확보한 후 저장하여 보관한다.

④ 주요 문서, 비밀 문서의 경우 MS-WORD 등의 워드프로세서에서 제공하는 문서 저장시 패스워드의 기능을 사용한다.

제10조(인터넷 사용)

① 웹 브라우저의 보안 수준을 점검한다.

1. 데이터를 전송하고 검색할 경우 보안 문제나 개인적인 프라이버시 침해 등을 미연에 방지하기 위해 보안 수준을 점검한다.
2. 웹 브라우저의 인터넷 영역의 보안 수준을 “보통” 혹은 “높음”으로 설정한다.(도구 | 인터넷 옵션 | 보안 항목에서 기본 수준 클릭 후 인터넷 선택)
3. 웹 브라우저의 로컬 인트라넷 영역의 보안 수준을 “낮음” 혹은 “보통”으로 설정한다.

② 웹 브라우저의 각종 보안 패치 및 서비스 팩을 설치한다.

1. 보안 담당자는 계속적으로 업데이트 되고 있는 IE(internet explorer) 관련 보안 패치 및 서비스 팩 중 사용자가 반드시 설치해야 할 필요가 있는 패치를 공지해야 한다.
2. 일반적으로 많이 쓰이고 있는 MS사의 IE 관련 보안 패치 및 서비스 팩은 http://www.microsoft.com/windows/ie/download/default.htm을 통해 다운이 가능하며, 중요 업데이트가 있을시 보안 담당자는 사용자에게 공지한다.
3. 사용자는 공지된 보안 패치 및 서비스 팩을 자발적으로 설치하여야 한다.

제11조(인터넷 접속)

① 다음의 사이트는 항시 접속이 금지된다.

1. 음란 사이트 : 음란사진, 동영상 등을 제공하는 사이트(뉴스그룹 포함)
2. 무단 복제 사이트 : 무단 복제된 프로그램이나 파일을 제공하는 사이트
3. 해킹 사이트 : 해킹과 관련된 정보를 담고 있는 사이트
4. 국가기관에서 접속 금지를 요청한 사이트
5. 기타 접속 금지의 필요성이 인정되는 사이트

② 사용자는 신뢰할 수 있는 웹 사이트를 방문한 경우를 제외하고는 자바와 Active-X 기능의 사용에 주의해야 한다.

③ 웹 브라우저가 제공하는 팝업 윈도우에 ‘Yes’ 로 하기 전에 그 내용을 상세히 파악함으로써 자바 스크립트, Active-X 공격 등에 노출될 수 있는 가능성을 줄여야 한다.

④ 악성 자료를 포함하는 사이트를 발견했을 경우, 해당 사이트의 URL을 반드시 보안 담당자에게 통보하여 해당 사이트의 접근을 침입차단시스템에서 제한하도록 한다.

제12조(바이러스 감염방지)

① 비인가된 소프트웨어 및 불법 소프트웨어 사용을 금지한다.

② 외부 네트워크나 매체로부터의 파일이나 소프트웨어를 다운로드 받을 경우 바이러스 백신프로그램을 적용한 후 사용한다.

③ 바이러스 백신프로그램이 PC 기동시 자동으로 실행되도록 하고, 바이러스 백신프로그램은 정기적으로 업데이트를 수행한다.

④ 중요한 업무 프로세스를 지원하는 시스템의 소프트웨어 및 데이터는 주기적으로 점검하여 허가되지 않은 파일이나 수정사항 등이 있는지 조사한다.

⑤ 전자우편 첨부파일에 대한 바이러스 감염여부를 점검한다.

⑥ 소프트웨어가 바이러스에 감염되는 것을 방지하기 위해 원본 소프트웨어는 쓰기방지가

되어 있어야 한다.

⑦ 불법 소프트웨어의 사내 PC 설치를 금지한다.

⑧ 특별한 이유 없이 시스템 혹은 어플리케이션이 동작하지 않을 경우 사용하던 파일을 다른 PC에서 읽거나 실행해서는 아니 되며 즉각 보안 담당자에게 통지한다.

⑨ 시스템의 바이러스 감염 시 다음 각 호의 조치를 하여야 한다.

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

⑩ 9항의 조치가 완료된 후 감염 PC 등에 대하여 다음 각 호의 조치를 하여야 한다.

1. 최신 백신 등 악성코드 제거 프로그램을 사용하여 악성코드를 삭제한다.
2. 감염이 심각할 경우 포맷 프로그램을 사용하여 하드디스크를 포맷한다.
3. 악성코드 감염의 확산 및 재발을 방지하기 위하여 원인을 분석하고 예방조치를 수행한다.

⑪ 기타 세부적인 바이러스 대응절차는 제22조(바이러스 보안), 제23조(바이러스 보안 절차)에 의거한다.

⑫ 운영체제(OS) 및 응용프로그램(한컴오피스, MSOffice, Acrobat 등)의 최신 보안패치를 유지한다.

⑬ 정보보안담당관은 악성코드가 신종이거나 감염피해가 심각하다고 판단할 경우에는 관련사항을 교육부장관 및 국가정보원장에게 신속히 통보하여야 한다.

⑭ 정보보안담당관은 교육부장관이 해당기관에 악성코드 감염사실을 확인하여 조치를 권고할 경우, 즉시 이행하여야 한다.

제13조(불법 소프트웨어)

① 모든 사용자는 사용이 승인된 소프트웨어만을 사용해야 하며, 불법 소프트웨어를 사용한 경우 개인 및 회사가 모두 처벌 받을 수 있다

② 검증되지 않은 불법 소프트웨어의 사용은 바이러스나 백도어 등의 침투 경로가 될 수 있으며, 시스템 운영이 어려워지거나 파일에 대한 보존성이 위협받을 수 있다.

③ 다음 각 호의 1에 해당하는 불법 소프트웨어 사용을 금지한다.

1. 정품 소프트웨어를 별도의 라이센스 없이 무단복제
2. 온라인 통신망 및 인터넷을 통한 불법복제
3. 시리얼 넘버의 공유•도용•배포•전송 등의 행위
4. 기한이 지나거나 업무 목적에 의해 이용이 금지된 셰어웨어 사용
5. 업무 목적에 의해 이용이 금지된 프리웨어 사용

④ 불법 소프트웨어 삭제 방법은 다음과 같다.

1. 시작 | 설정 | 제어판 | 프로그램 추가/삭제 란에서 프로그램을 삭제하거나 해당 프로그램의 Uninstall 명령을 이용해 삭제한다.
2. 탐색기를 이용해 해당 프로그램이 설치된 디렉토리나 파일을 삭제한다.
3. 필요시 시스템운영자의 협조를 받아 윈도우 디렉토리상의 해당 프로그램과 연계된 dll 파일을 지우거나 레지스트리 편집에 의해 해당 레지스트리 정보를 삭제한다.

4. 휴지통 비우기를 실행한다.

제14조(백업 관리)

① 필요한 데이터는 디스크 또는 파일서버 등의 수단을 사용해서 백업을 하여 만일의 사태에 대비한다.

② 백업 내용이 들어있는 디스크 등 이동이 손쉬운 저장매체는 시건장치가 되어있는 장소에 보관한다.

③ 파일서버에 백업을 할 경우 접근권한을 확인하여 다른 사용자들로부터 내용이 보호받을 수 있도록 조치한다.

제15조(반・출입 관리)

① 사용자는 PC 등 단말기를 교체 · 반납 · 폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 관리책임자와 협의하여 하드디스크에 수록된 자료가 유출, 훼손되지 않도록 보안조치 하여야 한다.

② 관리책임자는 사용자가 PC 등을 기관 외부로 반출하거나 내부로 반입할 경우에 최신 백신 등을 활용하여 해킹프로그램 및 웜 · 바이러스 감염여부를 점검하여야 한다.

③ 개인소유의 PC 등 단말기를 무단 반입하여 사용하여서는 아니 된다. 다만, 부득이한 경우에는 관리책임자의 승인을 받아 사용할 수 있다.

제16조(전자정보 저장매체 불용처리)

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

② 자료의 삭제는 해당 정보가 복구될 수 없도록 해당기관 실정에 맞게 저장매체별, 자료별 차별화된 삭제방법을 적용하여야 한다.

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

제17조(서비스 팩 및 패치 설치)

① 시스템운영자 또는 보안 담당자가 제공하는 최신 서비스 팩 또는 패치를 설치한다.

② 서비스 팩이나 패치를 설치할 때는 반드시 제공업체에서 제시하는 주의사항을 명확히 이해한 후 설치한다.

③ 현재 시스템이 운영 중일 때에는 가능한 설치하지 않도록 하고 업무가 이루어지지 않는 시간에 설치한다.

제18조(사용자 PC 운영)

① PC를 설치하여 운영하고자 하는 때에는 PC의 용도에 따라 자료의 안정성을 고려하여 설치장소를 정하여야 한다.

② 비밀 자료, 중요 전산자료의 접근이 가능한 PC가 설치된 장소는 제한구역지정 등 필요한 조치를 취하여야 한다.

③ 모든 PC의 현황을 등록하도록 하며, 등록시에는 최소한 아래와 같은 내용들이 포함되

어 있어야 한다.

1. 담당자
2. Type, Model
3. 하드웨어/소프트웨어 구성
4. 응용시스템
5. 위치
6. 발급된 IP Address

④ PC가 설치된 부서의 장은 PC별로 취급자를 지정하여 운용한다.

⑤ PC 취급자는 실제 PC를 사용하는 사용자이다.

⑥ 보안관련 상 위험도가 큰 PC, 처리업무가 상당히 중요한 PC, 기밀데이터가 들어 있는 PC를 파악하여 주요 PC목록 및 대책 양식에 기입한다.

⑦ 주요 PC에 대해서는 보안관리자에게 신청하여 별도의 물리적 보안 및 논리적 보안(PC 보안 소프트웨어, PC지문인식 프로그램 등) 대책을 이행한다.

제19조(시스템 PC(콘솔)의 운영)

① 시스템 PC에 대하여 물리적 접근통제(잠금장치 설치, 접근통제가 되는 장소에 설치 등)를 적절히 실시하여야 한다.

② 시스템 PC에 대하여 다음 사항을 반영한 논리적 접근통제를 실시한다.

1. 사용자 확인
2. 자동 타임아웃(time-out) 또는 로그오프(log-off)
3. 이용 시간대 통제
4. PC 확인 및 인증
5. 특이사항 출력
6. 보안 로그
7. 비밀번호 및 중요 데이터 전송시 암호 알고리즘 사용
8. 시스템의 접근시도 제한횟수 초과시 자동 사용중지

제20조(응용프로그램 및 데이터처리 PC의 운영)

① PC에 개인정보관련 자료를 보관해서는 아니 되고, 부득이한 상황으로 보관할 경우 패스워드 등 주요 정보를 암호화하여 보관하여야 한다.

② 데이터 입력을 처리하는 온라인 PC에서는 인터넷에서 자료를 다운받지 못한다.

③ PC별로 사용가능 직원, 수행가능 거래 및 사용가능한 파일을 지정하는 원칙이 정의되어야 하며, 지정내역이 전산 기록되어야 한다.

제21조(보안 점검)

① PC 보안 담당자는 주기적으로 PC 보안 점검을 수행하고 그 결과를 PC보안 점검 결과서(양식 1)로 문서화하여 보안관리자에게 제출한다.

제22조(바이러스 보안)

① 바이러스로 인한 피해를 최소화하기 위해 사용자와 보안 담당자는 다음의 사항을 준수해야 한다.

1. 비인가된 소프트웨어 및 불법 소프트웨어 사용을 금지한다.
2. 외부 네트워크나 매체로부터 파일이나 소프트웨어를 다운로드 받을 경우 백신 프로그램을 적용한 후 사용한다.
3. 백신프로그램을 설치하고 정기적으로 업데이트를 수행한다.
4. 중요한 업무 프로세스를 지원하는 시스템의 소프트웨어 및 데이터는 주기적으로 점검하여 허가되지 않은 파일이나 수정사항 등이 있는지 조사한다.
5. 전자우편 첨부파일에 대한 바이러스 감염여부를 점검한다.
6. 소프트웨어가 바이러스에 감염되는 것을 방지하기 위해 원본 소프트웨어는 쓰기방지가 되어 있어야 한다.
7. 시스템의 바이러스 감염시 즉각 보안 담당자에게 통지한다.
8. 보안 담당자는 바이러스 공격에 의한 피해를 복구하기 위한 적절한 백업, 복구계획을 수립한다.
9. 악성 소프트웨어와 관련된 정보(잡지, 바이러스 백신업체 등)를 확인하는 절차를 수행한다.
10. 네트워크상의 파일 서버에 대한 관리책임을 명확히 하며, 주기적으로 점검하여 불법 소프트웨어 및 악성 소프트웨어(바이러스, 백도어 포함)에 대한 탐지를 수행한다.
11. 악성 소프트웨어에 대한 새로운 정보 및 보호 대책에 대해 사용자에게 주기적 혹은 수시로 공지를 수행 한다.

제23조(바이러스 보안 절차)

① 바이러스를 예방 및 제거하기 위하여 최신 버전의 백신프로그램을 배포해야 하며, 백신프로그램의 배포 및 설치는 다음의 사항 준수해야 한다.
1. 보안 담당자는 바이러스 관련 정보, 예방사항 및 점검에 관련된 사항을 사용자에게 공지하며, 공지결과를 바이러스 공지일지에 기록한다.
2. 사용자는 현재 사용 중인 컴퓨터가 바이러스에 감염되었는지 확인할 수 있도록 백신프로그램을 설치하고 주기적으로 업그레이드한다.

② 사용자는 바이러스를 예방 및 제거하기 위하여 백실프로그램의 실행 시 다음의 사항을 준수해야 한다.
1. 사용자는 USB 및 다운로드를 통해 외부에서 반입되는 파일은 사용전 반드시 바이러스의 감염여부를 검사하고 바이러스 발견시 이를 완전히 제거한 후 사용한다.
2. 사용자는 전자우편 첨부파일에 대한 바이러스 감염여부를 검사하고 바이러스 발견시 이를 완전히 제거한 후 사용한다.
3. 제3자에게 소프트웨어를 제공하기 전에 바이러스나 프로그램 오류 등이 있는지 검사하여야 한다.
4. 사용자는 주기적으로 백신프로그램을 실행한다.

③ 컴퓨터가 바이러스에 감염되었을 경우 정보보안관리자에게 즉시 알려야 한다.

④ 정보보안관리자는 바이러스 발견을 확인하고 적절한 조치를 취하며, 그 결과를 보안사고 및 대응결과서를 기록 및 정보보안담당관에게 보고해야 한다..

제4장 E-Mail 보안지침

제24조(E-Mail 사용원칙)

① 업무용 E-mail을 개인적인 용도로 사용해서는 아니 된다.
② 계약직원, 임시직원은 원칙적으로 본교 E-mail을 사용할 수 없으며, 예외의 경우 그 이유를 문서화 한다.
③ 비밀 또는 본교가 소유한 정보는 E-mail로 보내지면 아니 된다.
④ 교직원들을 위해 외부에서 접근 가능한 E-mail 주소는 하나만 제공한다.
⑤ 교직원의 E-mail 주소 디렉토리는 공개적인 접근이 가능해서는 아니 된다.
⑥ 고의로 E-mail을 오용하는 사용자를 발견하면 상응하는 징계조치를 취한다.
⑦ 사용자는 본인의 암호를 분기 1회 이상 주기적으로 변경해야 한다.
⑧ 사용자 암호는 9자리 이상의 특수문자+숫자+문자의 조합으로 입력해야 한다.
⑨ E-mail 메시지의 내용은 범죄 조사, 보안취약성 조사, 감사를 위한 경우를 제외하고 비밀로 간주한다.
⑩ 사용자는 상용 전자우편을 이용한 업무자료 송·수신을 금지하며 기관 전자우편으로 송·수신한 업무자료는 열람 등 활용 후 메일함에서 즉시 삭제하여야 한다.
⑪ 사용자는 메일에 포함된 첨부파일이 자동 실행되지 않도록 설정하고 첨부파일 다운로드 시 반드시 최신백신으로 악성코드 은닉여부를 검사하여야 한다.
⑫ 사용자는 출처가 불분명하거나 의심되는 제목의 전자우편은 열람을 금지하고 해킹메일로 의심되는 메일 수신시에는 즉시 해당기관의 정보보안담당관을 경유하여 교육부 사이버안전센터(cer1@ecsc.go.kr) 및 국가사이버안전센터(reply@ncsc.go.kr)에 신고하여야 한다.

제25조(암호화)

① 특별히 기밀성을 요하는 정보가 있을 경우 E-mail을 통해 전송되어야 한다면 본교에서 승인한 소프트웨어와 알고리즘을 사용하여 지정 수신인만 읽을 수 있도록 암호화 한다.
② 인터넷과 같은 개방된 네트워크를 통해 전송되는 비밀 정보는 암호화를 적용한다.

제5장 네트워크 보안지침

제26조(네트워크 보안)

① 네트워크 구성 및 보안과 관련된 정보(네트워크 노드, IP주소, 관리자 암호 등)에 관한 접근을 통제한다.
② 네트워크 데이터 덤프, 추적 및 다른 관련 진단 데이터 파일은 허가되지 않은 접근으로부터 보호되어야 한다.

제27조(IP 할당)

① IP 주소를 데이터베이스화 하여 일원적으로 관리한다.
② IP 주소의 변경은 관련 담당자들에게 통보한 후 실시한다.
③ 일반 사용자들은 PC의 IP 주소를 임의로 변경할 수 없다.
④ 내부망에는 공인 IP를 사용하며 사정에 따라 사설IP를 사용할 수 있다.

제28조(네트워크 진단/관리 도구)

① 네트워크 부하를 모니터링하고 분석하여 최적의 상태를 유지하기 위해 네트워크 진단/관리 도구를 사용한다.

② 네트워크 진단/관리 도구의 사용시 진단 포트가 열려 보안에 취약성이 발생할 수 있으므로 진단 포트에 대한 불법적인 접속 여부에 대해 주기적인 점검을 실시한다.

③ 네트워크 진단/관리 도구들은 네트워크 관리 담당자에 의해서만 사용되고 일반 사용자들에게는 사용이 허가되지 않는다.

제29조(네트워크 경로설정)

① 전산시스템 상의 중요한 정보에 접근이 허가된 단말기는 전용통신링크를 사용한다.

② 내부 사용자는 침입차단시스템 등 보안시스템의 경로를 우회하는 경로를 설정해서는 아니 된다. 원칙적으로 내부 사용자는 모뎀을 통하여 인터넷에 접속할 수 없으며, 부득이 한 경우 담당 부서장과 보안관리자의 승인을 득한 후 사용한다.

③ 네트워크 사용자는 부서 책임자로부터의 사전승인 없이 개인 소유의 컴퓨터, 주변장치 또는 소프트웨어를 조직내로 가져와서 네트워크에 연결해서는 아니 된다.

제30조(네트워크 사용)

① 인터넷을 통한 모든 접속을 로깅한다.

② 원격 사용자의 공중 네트워크를 통한 접속은 인증 또는 암호화되어야 한다.

③ 원격 전산시스템에 의한 접속은 인증되어야 한다.

④ 네트워크간의 접속은 보안 기능에 의하여 통제되어야 한다.

제31조(네트워크 장비 관리)

① 네트워크 장비 등 신규 전산장비 도입 시 생성되는 기본(default) 계정을 삭제 또는 변경하고 시스템 운영을 위한 관리자 계정을 별도로 생성한다.

② 네트워크 장비의 암호는 수시로 변경하고 담당자 외에는 결코 알려주어서는 아니 된다.

③ 네트워크 장비의 셋팅값은 수시로 백업하여 장애에 대비한다.

④ 네트워크 장비에 대한 원격접속은 원칙적으로 금지하되, 불가피할 경우 장비 관리용 목적으로 내부 특정 IP・MAC 주소에서의 접속은 허용한다.

⑤ 외부 네트워크와의 연결지점에 침입차단의 목적으로 방화벽, 침입탐지시스템 등 별도의 보안장비를 설치할 수 있다.

⑥ 펌웨어 무결성 및 소프트웨어・서버 운영체제 취약점과 최신 업데이트 여부를 주기적으로 확인하여 항상 최신 버전으로 유지 한다. 단, 불가피한 경우는 예외 한다.

제32조(보안장비의 물리적 보안)

① 네트워크 설비 또는 장비는 허가되지 않은 물리적 접근으로부터 보호하기 위하여 잠금장치가 되어 있는 장소에 설치를 한다.

② 통신망 및 관련 주요 장비는 무정전 시설 확보, 비상전원 확보, 공조장치, 환풍장치, 냉난방장치, 정전기 방지장치, 소화장비 등의 부대설비를 갖춘 곳에 설치한다.

③ 외부 사람이 네트워크 설비가 설치되어 있는 보호장소에서 작업을 할 경우 내부 관계

자가 동행하며 작업 일지에 기록한다.

④ 통신회선의 설치를 위한 협정 또는 작업은 부서 책임자의 승인 이후에 수행되어야 한다.

⑤ 허가되지 않은 장비의 접속을 탐지하기 위하여 정기적인 통신 케이블 점검을 실시한다.

⑥ 사용하지 않거나 불필요한 모든 통신 장비 및 네트워크 세그먼트는 물리적으로 네트워크상에서 접속을 차단한다.

⑦ 네트워크 장비의 설치, 이동, 폐쇄는 통신망 운영매뉴얼에 의거하여 수행한다.

제33조(논리적 접근통제)

① 허가된 자만이 허가된 네트워크에 접근하여 허가된 작업만 할 수 있도록 네트워크 접근권한 리스트를 보유한다.

② 필요시 네트워크에의 접근시간을 제한할 수 있다.

③ 네트워크 장비에 로그인시 반드시 사용자 인증을 수행한다. 이때 다음의 사항을 준수한다.

1. 패스워드 조합의 가능성을 최대로 하며 주기적으로 변경한다.
2. 5회 이상 정확하지 않은 패스워드의 시도가 있는 단말기는 자동으로 접속을 차단한다.
3. 관리자와 사용자 모드를 지원하는 경우 분리 운영한다.
4. 비활동 접속을 자동으로 차단한다.
5. 네트워크 소프트웨어는 비인가자의 접근을 막기 위하여 일정 시간동안 활동 없이 접속한 상태를 유지하는 사용자의 접속을 강제로 끊을 수 있어야 한다.
6. 허가된 사용자 또는 프로세스가 네트워크에서 부작용 없이 운영하고 있는 프로세스의 진행을 완료할 수 있도록 하기 위하여 자동 접속차단 전에, 사용자에게 재접속을 요구한다.
7. 기타 로그인, 계정 및 패스워드 지침은 해당 서버의 지침에 의거한다.

제34조(보안사고 대응)

① 보안사고 발생시 처리는 침해사고 대응지침에 준하여 시행한다.

제35조(로깅, 감사 및 보안점검)

① 네트워크 장비의 로깅과 감사는 서버의 로깅과 감사 지침에 준하여 시행한다.

② 해당 업무별 관리자는 주기적으로 네트워크 보안점검을 수행하고 그 결과를 별도로 기록하여 문서화한다.

③ 네트워크 관리 담당자는 라우터 등 중요 네트워크장비의 접속기록을 6개월 이상 유지하여야 하고 비인가자에 의한 접근 여부를 주기적으로 점검하고 정보보안담당관에게 관련결과를 보고하여야한다.

제36조(네트워크 구성, 변경 및 문서화 절차)

① 네트워크 관리 담당자는 네트워크 장비 설치에 대한 내용을 네트워크 시스템 목록에 기록하여 문서화한다.

② 장비의 특성별 상황에 맞추어 구성정보 변경과 구성정보 조회를 할 수 있는 사용자를

구분하여 설정한다.

③ 인가된 자만이 장비에 접속하여 구성을 변경해야 한다.

④ 네트워크 구성 및 보안과 관련된 정보(네트워크 노드, IP주소, 관리자 암호 등)에 관한 접근을 통제한다.

⑤ 네트워크 장비의 구성 및 IP할당 내역은 네트워크 관리 담당자가 관리한다.

제37조(네트워크 구성 변경)

① 네트워크 변경 작업 중 기관 신설 또는 이전 시에는 네트워크 관리 담당자가 작업의뢰서를 통하여 관리하며, 폐쇄시에는 네트워크 관리 담당자에게 반드시 보고한다.

② 장비의 불량으로 인한 교체시 네트워크 관리 담당자에게 통보되어야 하며, 장비설정이 가능한 경우 장비에 설정된 내역을 모두 삭제한 후 교체하여야 한다.

③ 단일 장비의 구성정보 오류에 대한 변경은 네트워크 관리 담당자의 직권으로 결정한다.

④ 네트워크의 주요 구성 변경시에는 네트워크 구성 변경 신청서를 통해 보안관리자에 보안성 검토를 요청한 후 승인이 이루어진 경우 변경을 수행한다.

제38조(문서화)

① 효과적인 네트워크 관리 및 통제를 위해 네트워크 구조, 물리적/논리적 토폴로지 및 노드, 통신 서비스 제공자 및 통신 사업자의 목록, 사용 네트워크 장비, IP에 대한 할당 내역 등에 대한 완전하고 정확한 기록이 작성되고 관리되어야 한다.

② 네트워크에 대한 관리 사항 및 네트워크 구성의 검토, 확인 사항이 주기적으로 기록되어야 한다.

③ 네트워크 장비에 대한 운영문서 및 장애시 대응 절차에 대한 문서가 유지·관리되어야 한다.

제39조(관리자 패스워드 보관절차)

① 네트워크 장비의 관리자 패스워드에 대한 기록은 네트워크 장비 관리자 계정 및 패스워드 현황대장에 기록하고 비밀문서로 취급하여 안전한 장소에 보관하며, 인가자 외에는 열람을 허가해서는 아니 된다. 분기별로 네트워크 관리 담당자는 변경된 관리자 패스워드를 밀봉하여 보안관리자에게 제출하고, 보안관리자는 내역을 기록한 후 안전한 곳에 보관한다.

② 긴급 필요시(네트워크 관리 담당자의 부재시 등) 관련 부서장은 보안관리자에게 밀봉된 관리자 패스워드를 요청하고 보안관리자 또는 해당업무 담당 부서장의 승인을 득한 후 개봉하여 사용한다.

제40조(외부 접속)

① 외부로부터의 내부 네트워크 접속 요청시 보안 사항을 먼저 검토한다.

② 외부와의 연결은 신뢰할 수 있는 대상으로 제한한다.

③ TCP/IP를 통한 외부와의 연결은 반드시 침입차단시스템을 통하여 연결되어야 한다.

④ 공용망과의 연결은 보안에 최대한 중점을 두어 판단하도록 한다.

제41조(민감한 정보의 전송)

① 인터넷을 통한 비밀정보 전송시 암호화한다.

② 내부망에서도 민감한 정보의 보호가 필요할 경우 적절한 암호화 대책을 수립하여야 한다.

③ 암호화는 네트워크 장비상의 암호화를 구현하거나, 상황에 따라 적절한 프로그램상의 암호화를 고려한다.

④ 암호화 장비 및 툴을 도입할 경우 장비 및 알고리즘은 가능하면 국가나 관련 기관의 법적 및 규제적 요구를 만족시켜야 한다.

⑤ 암호화에 사용되는 키 값은 외부에 노출되지 않도록 철저히 관리한다.

제42조(외부 네트워크와의 연결시 사용)

① 교내에서 인터넷으로의 연결시는 모든 서비스를 허용함을 원칙으로 하나, 보안관리자가 판단하여 보안 관리상의 문제점이 노출될 경우 일부 서비스를 제한할 수 있다.

② 교외에서 인터넷을 통한 내부 네트워크로의 연결은 원칙적으로 금지한다. 필요시 SMTP, HTTP, FTP 서비스만을 이용할 수 있으나 서비스 이용시 보안관리자의 승인을 받아야 하며, 다음과 같은 사항을 준수해야 한다.

1. 외부 연결이 요구될시 네트워크 관리 담당자에게 필요 서비스를 네트워크 연결신청서를 통해 요청할 수 있으며, 네트워크 관리 담당자는 보안성 검토 후 허가 여부를 결정한다.
2. 그러나, Netbios 프로토콜(137, 138, 139번 포트) 및 r-command 등을 포함하여 보안관리자가 지정하는 서비스에 대하여는 불허된다.
3. 허가된 서비스는 한시적으로 허용되므로, 신청자는 서비스의 필요 기간이 지난 후에는 즉시 네트워크 관리 담당자에게 사용종료를 보고하여야 한다.

제6장 데이터베이스 보안지침

제43조(데이터베이스 인증)

① DB 보안 담당자는 계정 및 패스워드 관리에 대한 책임과 권한을 갖는다.

② DB에의 접근은 항상 인증을 통해서만 가능하도록 한다. 이를 위해 인증 모듈은 DB를 구동시키는 즉시 제공되어야 하며, 항상 활성화되어 있어야 한다.

③ DB의 접근 제한을 위해서는 Role을 통해 사용자 및 사용자그룹을 등록하여야 한다.

④ 각 사용자명은 비권한자의 사용을 방지하기 위해 패스워드와 연계되어 있어야 한다.

⑤ 각 DB에 연계된 사용자는 동일명의 스키마를 가져야 한다.

제44조(계정의 생성 및 폐기)

① DB를 사용하고자 하는 자는 DB 관리 담당자에게 사용자 정보 및 사용목적, 사용기간, 연락처 등이 포함된 DB사용자 계정 및 권한 신청서를 제출하고 DB 관리 담당자는 타당성 검토를 한 후 계정을 부여한다.

② 장기파견자, 휴직자는 업무에서 신속히 제거한다.

③ 퇴직자는 사직원 제출시 DB 관리 담당자의 계정반납 확인을 득해야 한다.
④ 디폴트 계정은 설치 후 업무에 사용되지 않는다면 삭제하도록 한다.

제45조(계정 운영)

① 계정 정보(이름, 연락처, 직위, 업무, DB에서의 작업과 권한)에 관한 사용자 관리대장이 존재하고 모든 사용자에 대해 작성되어야 한다.
② 패스워드가 없는 계정은 사용을 금한다.
③ 장애복구나 점검을 위해 DB 관리 담당자 권한 위임시 작업종료 후 주요 항목에 대해 DB보안 점검 결과서를 작성 후 점검 후 패스워드를 변경하도록 한다.
④ DB 관리 담당자 권한을 가지고 있던 사용자가 이직, 퇴직 등의 사유로 다른 곳으로 옮길 때에는 인수자는 즉시 변경하여 DB관리자 계정 및 패스워드 현황에서 기존 패스워드를 변경하도록 한다.

제46조(패스워드)

① 신규 사용자가 DB 사용에 대한 권한을 부여 받을 때 반드시 패스워드를 받도록 한다.
② 사용자 패스워드는 주기적으로 변경한다.
③ 모든 사용자는 패스워드 인증을 통해서만 DB에 접근할 수 있도록 한다.
④ 계정이름과 동일한 패스워드를 사용하거나 DB서버의 이름을 패스워드로 사용, 예정된 계정의 이름을 패스워드로 사용하는 경우 쉽게 계정에 대한 패스워드를 추측하여 서버에 접속할 수 있으므로 추측하기 쉬운 패스워드는 절대 사용하지 않는다.
⑤ DB의 디폴트 패스워드는 항상 추측하기 어려운 복잡한 패스워드로 변경하여 사용한다.
⑥ 정책을 통해 패스워드 관리에 대한 설정을 강화한다.

제47조(기타 인증 관리)

① 잘못된 로그인 횟수에 제한을 두어 제한된 수를 넘을 경우 자동적으로 연결을 해제한다.
② 일정 시간동안 작업이 없으면 자동으로 로그아웃 되도록 한다. 단, 업무상의 필요성이 있는 경우 예외를 둔다.

제48조(DB 접근제어)

① 사용자가 DB파일에 접근할 수 있는 수준은 보안관리 규정에 따른 정보보호 등급과 사용자의 접근 권한에 따라 DB 관리 담당자가 결정해야 한다.
② DB 관리 담당자는 사용자의 시스템 자원사용 수준을 결정해야 한다.
③ DB 관리 담당자는 테이블에 Insert, Update, Delete, Select의 행위별 권한, 필드 접근권한 등의 객체 권한을 조정해야 한다.
④ 사용자에게 DB 접근권한을 부여하는 경우, 적절한 Role을 생성하여 필요한 시스템 권한 및 객체 권한을 Role에 부여하고 사용자를 Role에 소속시킨다.
⑤ 시스템 권한은 DB 관리 담당자만이 가진다.
⑥ 시스템 권한 및 오브젝트 권한은 Public에게 부여하지 않는다.
⑦ 오브젝트 권한 부여시 DB 관리 담당자 또는 권한을 부여받은 사용자가 또 다른 사용자에게 권한을 부여해야 할 업무상의 필요가 있는 경우에만 권한을 부여한다.

⑧ View Table 생성시 View Table을 통해 조회할 수 없는 Row가 Insert되는 경우를 예방한다.
⑨ 저장 프로시저 및 툴을 사용하여 설정된 접근권한을 체크하고 수정한다.

제49조(접근제어 설정 갱신 절차)

① 접근 제어에 대한 설정은 DB 관리 책임자의 허가를 득하고서만 변경될 수 있도록 한다.
② 접근제어에 대한 설정은 환경의 변화 등을 반영하여 주기적으로 갱신한다.

제50조(접근제어 메커니즘)

① DB의 중요성과 특성에 맞는 접근제어 메커니즘(강제적 접근제어/재량적 접근제어)을 택하여 적용한다.
② 메커니즘에 맞는 구체적인 접근제어 절차를 마련한다.
③ 주체와 객체의 권한, 접근시도 장소 및 시간 등에 따른 접근제어를 실시한다.
④ 필요한 경우 관리툴을 이용하여 접근권한을 설정/통제한다.
⑤ 사용하지 않는 계정에 대해서는 주기적으로 검사하고 권한을 적절히 제한하도록 한다.
⑥ 사용자와 업무에 관한 권한 정보는 문서화되어 관리되며, 항상 최신의 상황을 반영하도록 갱신되도록 한다.

제51조(암호화)

① 기밀성이 요구되는 DB 시스템 내의 중요 필드에 대해 암호화되어 있어야 한다.
② 암호화를 지원할 수 있는 암호화 기술이 DB 시스템에 도입되어야 한다.
③ DB로 기밀성이 요구되는 데이터를 전송할 때에는 암호화되어야 한다.
④ DB로의 암호화 전송을 지원할 수 있는 전송 시스템이 도입되어야 한다.

제52조(DBMS 요구기능)

① 개별 사용자의 접근권한 통제 및 데이터 요소별로 데이터를 보호할 수 있는 자체보안 알고리즘을 갖추고 있어야 한다.
② 프로그램, 유틸리티, 명령어 등의 데이터에 대한 접근을 통제해야 한다.
③ DB 감시기능이 가동 중인지 아닌지를 조사해야 한다.
④ 특정 스키마 객체나 특정한 운영만을 사용자에게 허락해야 한다.
⑤ 각 스키마 객체를 감시해야 한다.
⑥ DB내의 장애나 데이터의 불일치를 검색하고 해결할 수 있는 기능을 갖추어야 한다.
⑦ 로그 기능이 있어야 한다.

제53조(로깅 및 감사)

① 사용자의 로그인 시간 및 로그인 지속시간이 적절한 범위 내에서 로깅 되어야 한다.
② DB에 연결된 사용자의 수가 적절한 범위 내에서 로깅 되어야 한다.
③ 접속에 실패한 접근 시도가 로깅 되어야 한다.
④ DB 내의 deadlock이 로깅 되어야 한다.
⑤ 모든 사용자의 I/O 통계가 적절한 범위 내에서 로깅 되어야 한다.

⑥ System Table에의 접근이 로깅 되어야 한다.
⑦ 새로운 DB 객체의 생성이 로깅 되어야 한다.
⑧ 데이터 조작이 적절한 범위 내에서 로깅 되어야 한다.
⑨ 기록된 로그파일교직원은 DB 보안 담당자에 의해서 정기적으로 점검되어야 한다.
⑩ 점검이 이루어진 로그파일은 정기적으로 삭제되어야 한다.
⑪ 로그파일의 분석을 위하여 관리자가 부가적인 도구를 설치 사용할 수 있다.
⑫ 로그/감사에 대한 엄격한 접근제어를 실시한다.
⑬ 중요 DB의 경우 DB 관리 담당자와 DB 보안 관리자의 권한을 분리한다.
⑭ 로그파일의 조작 및 읽기 권한은 DB 보안 관리자에게만 있어야 한다.
⑮ 로그파일의 무결성을 보장하기 위하여 로그파일 자체에 대한 모니터링을 주기적으로 실시한다.

제7장 응용프로그램 보안지침

제54조(패스워드 설계 및 구현)

① 패스워드는 문자와 숫자를 조합하여 9자리 이상으로 한다.
② 직전의 패스워드로는 변경이 허용되지 않아야 한다.
③ 계정의 패스워드 입력제한의 횟수를 정의하고, 정의된 횟수 실패시 자동적으로 연결이 해제되도록 한다.
④ 사용자 패스워드는 암호화하여 조회가 불가하도록 해야 한다.
⑤ 사용자 비밀번호는 화면 및 출력물에 노출되어서는 아니 된다.

제55조(C/S, WEB 로그온 및 로그오프 설계 및 구현)

① 로그인 후 일정시간 미사용시 자동 로그오프를 적용하거나 화면잠금 기능을 적용한다.
② 시스템 접속시 최종사용시각을 표시한다.
③ 일정기간 시스템 미사용시 미사용자의 로그인을 제한한다.

제56조(인터넷/인트라넷 설계 및 구현)

① 디렉토리 리스팅을 금한다.
② 인증이 필요한 경우임에도 인증과정 없이 중간페이지로 직접 접속하는 것을 금지한다.
③ 사용자의 주요 정보는 암호화하여 전송한다.

제57조(로깅/감사기능 설계 및 구현)

① 시스템 개발시 감사업무 수행에 필요한 자료를 생성하도록 감사기능을 설계한다.
② 관리자 활동내역에 대해서 로그할 수 있는 감사기능을 설계한다.
③ 단말기를 통해 구성원의 기본정보를 조회, 수정하는 경우에는 조회자, 조회일시, 변경 또는 조회내용, 접속방법, 접속 IP 등을 시스템에 자동 기록되도록 하고 그 기록을 6개월 이상 보관하여야 한다.

제58조(응용프로그램 보안 확인 및 보고)

① 응용프로그램 개발/유지보수 책임자는 응용프로그램 보안관련 설계 및 구현사항에 대해서 각각 설계단계 종료 후 및 구현 종료 후 확인하며, 확인결과를 응용프로그램 보안설계/구현표로 작성하여 보안관리자에게 제출한다.

제59조(응용프로그램의 외주 개발시)

① 응용프로그램을 외주 개발로 수행하여 공급받을 경우 공급자로부터 아래 항목을 포함한 개발 소프트웨어 무결성 증명서를 받아 두어야 한다.

1. 시스템 개발시 감사업무 수행에 필요한 자료를 생성하도록 감사기능을 설계한다.
2. 개발된 소프트웨어의 기능이 문서화 내용과 차이가 없어야 한다.
3. 정보보호를 위협하는 은폐구조가 없어야 한다.
4. 실행 중 보안/통제 설계의 오류나 설계된 보안구조를 회피하거나 변경시키는 코드가 없어야 한다.

제60조(응용프로그램 사용자 계정 및 패스워드 관리)

① 계정 등록을 원하는 사용자는 다음의 사항을 준수한다.

② 사용자계정 등록은 사용자가 정보시스템에서 본인사항을 확인 후 등록 요청에 의해 등록이 완료된다.

③ 사용자 삭제 또는 권한 변경 사유가 발생한 경우 삭제 또는 변경 신청서를 작성하여 통보하여야 한다.

④ 계정은 각 사용자별로 부여한다. 부서별 공동사용자 계정은 생성이 금지된다.

⑤ 시스템 관리 담당자는 월간 단위로 사용자 등록 및 변경 현황을 유지한다.

⑥ 사용자 계정의 재확인은 다음 사항에 대하여 실시한다.

1. 퇴사 여부, 업무 필요성 여부
2. 마지막 사용일자가 60일을 넘겼을 경우

⑦ 패스워드가 없거나 사용자 계정이름과 동일한 계정을 허용해서는 아니 된다.

⑧ 하나의 로그인 아이디는 한번만 로그인 할 수 있다.

제61조(계정 정지)

① 틀린 패스워드의 반복시 계정을 정지시킨다.

② 보안관리자에게 정지계정의 현황을 보고한다.

제62조(계정의 폐쇄)

① 계정이 폐쇄되는 사유가 발생시에는 사유가 발생하는 즉시 삭제하도록 한다.

② 계정의 폐쇄는 아래의 사유에 따른다.

1. 사용자가 퇴직하는 경우
2. 3개월 이상 미사용 계정

제63조(패스워드 관리)

① 신규 사용자에게 시스템 사용에 대한 권한을 부여할 때에는 반드시 패스워드를 받도록 해야 한다.

② 모든 사용자는 패스워드 인증을 통해서만 시스템을 사용할 수 있게 하여야 한다.
③ 보안관리자는 응용프로그램 보안 설계대로 패스워드 기능이 작동하는지 확인한다.
④ 패스워드는 분기 1회 이상 주기적으로 변경되어져야 한다.

제64조(개발업무 계정 및 권한 부여/관리)

① 각 개발 담당자별로 사용자 계정을 부여하는 것을 원칙으로 한다.
② 계정공동 사용시 그 상황 및 활동내역을 기록한다.
③ 담당자의 계정 부여 내역은 보안관리자가 주기적으로 확인한다.
④ 개발 담당자의 접근권한은 데이터 관리지침에 의해 현황을 정리한다.
⑤ 개발 담당자의 담당업무 변경, 전출, 퇴직 등의 사유 발생시 기존에 허용했던 전산자원의 접근권한을 제한하도록 한다.
⑥ 중요하고 민감한 응용프로그램 및 라이브러리는 개발 보안담당자가 지정하고 보안관리자가 확인하며, 이에 대한 내역을 기록하며 접근권한을 최소한으로 필요성이 있는 경우에만 부여한다.

제65조(개발 담당자 접근통제)

① 개발 담당자는 다음의 구역에 원칙적으로 접근을 금하며 부득이한 경우 허가신청서를 작성한 후에 출입한다.
1. 컴퓨터실 출입 통제
2. 운영체제 관련 도큐멘테이션이 보관된 장소 출입 통제

② 개발 담당자는 다음과 같은 사항에 논리적인 접근을 가능한 금하고 금하기 어려운 경우 허가를 득하며 로깅을 통해 접근내역을 기록한다.
1. 담당업무 이외의 응용프로그램 및 도큐멘테이션 접근
2. 시스템 운영과 관련된 유틸리티 응용프로그램, 시스템 운영 용도의 응용프로그램과 라이브러리 접근

③ 개발 담당자 그룹별로 할당 라이브러리를 지정하여 할당된 라이브러리만 접근 하고 그 외의 라이브러리는 접근을 금지하거나 조회만 가능하도록 한다. 타 라이브러리의 접근이 필요할 경우 해당 라이브러리 책임자에게 접근권한 요청서를 제출하여 접근사유의 승인을 득한 후 접근을 수행한다.
④ 개발 담당자 그룹별로 디렉토리 권한이 할당되어 타 개발 담당자 그룹에 접근하거나 OS의 파일들을 조작하지 않도록 한다.

제66조(응용프로그램 및 데이터 처리 단말의 운영)

① 단말기에 업무 및 이용자관련 자료를 보관해서는 아니 되고, 부득이한 상황으로 보관할 경우 비밀번호 등 주요 정보를 암호화하여 보관하여야 한다.

제67조(개발업무 보안점검)

① 개발 보안 담당자는 주기적으로 개발업무와 관련된 보안점검을 실시하고 개발업무 보안점검 결과서에 기록한다.

② 개발 보안 담당자와 보안관리자는 보안점검의 적정성을 확인한다.
③ 외부인력에 대한 세부지침은 “외부용역 보안지침”에서 정한 바에 따른다.

제68조(개발환경)

① 독립된 개발시설을 확보하고 비인가자의 접근을 통제한다.
② 개발시스템과 운영시스템은 물리적으로 분리한다.

제69조(시스템 개발보안)

① 시스템 개발보안에 대한 세부지침음 “시스템 개발보안 지침”에서 정한 바를 따른다.

제70조(웹서버 설치)

① 웹서버의 설치 및 운영 시에는 책임자의 승인을 받아야 한다.
② 웹서비스가 제공되는 호스트에는 적절한 조치 없이 대외비 이상의 정보가 있으면 아니 된다.
③ 웹서버에서 실행되는 프로그램의 목록을 문서화하여 관리해야 한다.
④ 웹서버에서 외부에 제공되는 정보의 목록을 문서화하여 관리해야 한다.
⑤ 웹서버의 정보 제공자의 목록을 문서화하여 관리해야 한다.
⑥ 웹서버의 CGI 프로그램의 목록을 문서화하여 관리해야 한다.
⑦ 일반 사용자들은 웹서버를 설치하거나 작동할 수 없다.
⑧ 일반 사용자가 웹서버에 CGI 등 스크립트를 설치할 수 없도록 한다.
⑨ 웹 서버용 소프트웨어와 OS는 현재 사용하고 있는 버전에서 제공자가 권고한 패치를 설치해야 한다.
⑩ 분기마다 웹서버를 점검하여 문제점의 발견시 관련 패치를 설치해야 한다.
⑪ PC 등에 있는 웹서버 소프트웨어와 웹문서 저작도구는 담당자에 의해 별도로 관리되어야 한다.
⑫ 웹서버에는 HTTP를 제외한 다른 네트워크 서비스(SMTP, FTP 등)는 사용하지 말아야 한다.
⑬ 로그인이나 개인정보가 있는 경우는 보안서버로 구축해야 한다.
⑭ 서버 관리자는 외부인에게 공개할 목적으로 설치되는 웹서버 등 공개서버를 내부망과 분리된 영역교직원에 설치 · 운용하여야 한다.
⑮ 각급기관의 장은 비인가자의 서버 저장자료 절취, 위 · 변조 및 분산서비스거부교직원 공격 등에 대비하기 위하여 국가정보원장이 안전성을 검증한 침입차단 · 탐지 시스템 및 DDoS 대응시스템을 설치하는 등 보안대책을 강구하여야 한다.

제71조(웹서버 계정관리)

① 가능하면 사용자 계정을 만들지 않는다.
② 시스템 관리 담당자는 지속적으로 사용자 계정을 검토하여 불필요한 직원의 접속을 가능한 줄이도록 노력하며, 서버에 로그인 할 수 있는 인원수를 최소화한다.
③ 반드시 필요로 하는 사용자 이외에는 슈퍼 사용자의 권한을 가질 수 없도록 제한하며, 권한 대상자는 별도로 관리한다.

제72조(웹서버 구성)

① 특정한 웹 관리자 계정을 만든다.
② HTML문서에 접근하는 모든 사용자를 위한 특정 그룹을 만든다.
③ 사용자 및 관리자 계정 관리는 각 서버의 계정 관리 지침을 따른다.
④ 필요한 최소한의 서비스만 제공한다.
⑤ 필요하지 않은 쉘과 인터프리터는 설치하지 않는다.
⑥ CGI 디렉토리에는 쉘과 인터프리터를 설치하지 않는다.
⑦ 디렉토리 및 파일에 다음과 같이 권한을 설정하며, 매 분기마다 검사한다.

1. 웹 관리자만이 서버의 Root 디렉토리에 Write 권한을 갖는다.
2. CGI 프로그램 디렉토리와 CGI 프로그램은 readable, executable 되어야 하나 Write 권한이 설정되면 아니 된다.
3. Document Root와 서브 디렉토리는 사용자를 위한 1항의 웹 관리자계정과 2항에서 만들어진 그룹에 의해 소유되며, 외부에 대해 read 권한을 주어야 하지만 write 권한이 주어지면 아니 된다.
4. 다음과 같이 사용권한을 설정한다.
   - Ever root directory : log 및 configuration 파일이 저장되는 디렉토리
   - Document root directory : HTML 문서가 저장되는 디렉토리

```
[ server root directory 설정 ]
drwxr-xr-x     5 www     www    1024 Aug 8 00:01 cgi-bin/
drwxr-x---     2 www     www    1024 Jun 11 17:21 conf/
-rwx------     1 www     www    109674 May 8 23:58 httpd
drwxrwxr-x     2 www     www    1024 Aug 8 00:01 htdocs/
drwxrwxr-x     2 www     www    1024 Jun 3 21:15 icons/
drwxr-x---     2 www     www    1024 May 4 22:23 logs/

[ document root directory 설정]
drwxrwxr-x     3 www     www    1024 Jul 1 03:54 contents
drwxrwxr-x    10 www     www    1024 Aug 23 19:32 examples
-rw-rw-r--     1 www     www    1488 Jun 13 23:30 index.html
-rw-rw-r--     1 lstein  www    39294 Jun 11 23:00 resource_guide.html
(   : www - 웹 관리자 계정, www - HTML 문서 접근하는 모든 사용자를 위한 그룹 )
```

⑧ 웹 서버가 다음과 같은 특징을 제공하는 경우, 사용을 제한한다. 사용시 충분히 보안에 유의해야 한다.

1. Automatic Directory Listings
2. Symbolic Link Following
3. Server Side Includes
4. User-maintained Directories

⑨ 웹 데몬의 차일드 프로세스가 Root의 권한을 가지고 수행되지 않도록 한다.
⑩ FTP가 upload를 허용하면, 웹과 디렉토리를 공유하지 않는다.
⑪ chroot를 사용하여 웹의 디렉토리를 분리시켜야 한다.
⑫ 한 달마다 HTML 문서의 내용을 확인해야 한다.
⑬ .htaccess, .htpasswd, .htgroup 등을 사용하여 주요 디렉토리에 사용자 인증 기능을 추가하여 운영한다. 추가적으로 강화된 인증 기법을 사용할 수도 있다.
⑭ ID 및 비밀번호를 통하여 로그인시에는 SSL 통신을 통하여 접속하여야 한다.

제73조(웹서버 백업)

① 사용자는 업무상 중요한 데이터를 변경주기에 따라 수시로 백업하여야 한다.
② 홈페이지 관리담당자는 보안 침해사고를 대비해 정기적으로 시스템을 백업하여야 한다.

제8장 서버 보안지침

제74조(서버 보안)

① 서버관리자는 서버를 도입・운용할 경우, 정보보안담당관과 협의하여 해킹에 의한 자료절취, 위・변조 등에 대비한 보안대책을 수립・시행하여야 한다.
② 서버 관리자는 서버 내 저장자료에 대해 업무별・자료별 중요도에 따라 사용자의 접근권한을 차등 부여하여야 한다.
③ 서버 관리자는 사용자별 자료의 접근범위를 서버에 등록하여 인가여부를 식별토록 하고 인가된 범위 이외의 자료접근을 통제하여야 한다.
④ 서버 관리자는 서버의 운용에 필요한 서비스 포트 외에 불필요한 서비스 포트를 제거하며 관리용 서비스와 사용자용 서비스를 분리 운용하여야 한다.
⑤ 서버 관리자는 서버의 관리용서비스 접속 시 특정 IP와 MAC 주소가 부여된 관리용 단말을 지정 운용하여야 한다.
⑥ 서버 관리자는 서버 설정 정보 및 서버에 저장된 자료에 대해서는 정기적으로 백업을 실시하여 복구 및 침해행위에 대비하여야 한다.
⑦ 서버 관리자는 데이터베이스에 대하여 사용자의 직접적인 접속을 차단하고 개인정보 등 중요정보를 암호화하는 등 데이터베이스별 보안조치를 실시하여야 한다.
⑧ 정보보안담당관은 제1항 내지 제7항에서 수립한 보안대책의 적절성을 수시 확인하되, 연1회 이상 보안도구를 이용하여 서버 설정 정보 및 저장자료의 절취, 위・변조 가능성 등 보안취약점을 점검하여야 한다.
⑨ 서버에 등록된 비밀번호는 암호화하여 저장하여야 한다.

제75조(웹서버 등 공개서버 보안)

① 서버관리자는 외부인에게 공개할 목적으로 설치되는 웹서버 등 공개서버를 내부망과 분리된 영역(DMZ)에 설치・운용하여야 한다.
② 정보시스템을 운영하는 소속기관의 장은 비인가자의 서버 저장자료 절취, 위・변조 및 분산서비스 거부교직원 공격 등에 대비하기 위하여 침입차단・탐지시스템 및 DDos 대응시스템을 설치하는 등 보안대책을 강구하여야 한다.
③ 서버관리자는 비인가자의 공개서버 내에 비공대 정보에 대한 무단 접근을 방지하기 위

하여 서버에 접근 사용자를 제한하고 불필요한 계정을 삭제한다.

④ 공개서버의 서비스에 필요한 프로그램을 개발하고 시험하기 위해 사용된 도구(컴파일러 등)는 개발 완료 후 삭제를 원칙으로 한다.

제76조(홈페이지 게시자료 보안)

① 개인정보를 포함한 중요 업무자료가 홈페이지에 무단 게시되지 않도록 홈페이지 게시자료의 범위·방법등을 명시한 자체 홈페이지 정보공개 보안지침을 수립·시행하여야 한다.

② 사용자는 개인정보, 비공개 공문서 및 민감 자료가 포함된 문서를 홈페이지에 공개하여서는 아니된다.

③ 홈페이지에 정보를 게시하고자 하는 부서의 장은 정보보안담당관과 협의하여 사전에 보안심사위원회의 심사를 거쳐 비밀 등 비공개 자료가 게시되지 않도록 하여야 한다. 다만, 기존에 게시한 내용 중 단순하게 수치를 변경하거나 경미한 사항은 그러하지 아니할 수 있다.

④ 사용자는 인터넷 블로그·카페·게시판·개인 홈페이지 또는 소셜네트워크 서비스 등 일반에 공개된 전산망에 업무관련 자료를 무단 게재하여서는 아니 된다.

⑤ 정보보안담당관은 소속기관의 홈페이지 등에 비공개 내용이 게시되었는지 여부를 주기적으로 확인하고 개인정보를 포함한 중요정보가 홈페이지에 공개되지 않도록 보안교육을 주기적으로 실시하여야 한다.

⑥ 각급기관의 장은 홈페이지에 중요정보가 공개된 것을 인지할 경우 이를 즉시 차단하는 등의 보안조치를 강구 시행하여야 한다.

제77조(클라우드시스템 보안관리)

① 클라우드 컴퓨팅시스템을 구축 할 경우 '국가·공공기관 클라우드 컴퓨팅 보안가이드라인'을 준용한 보안대책을 강구하여야 한다.

② 상용 클라우드 컴퓨팅 시스템을 활용하고자 할 경우에는 보안성 검토를 자체적으로 실시하여야 한다.

제9장 백업 및 복구 처리지침

제78조(서버 시스템의 재난 복구)

① 시스템의 OS 장애를 대비하기 위하여 시스템의 백업기능을 이용하여 OS백업 이미지를 구성하여 원격지(타 전산실)에 보관한다.

② 시스템 OS 백업은 다음 각 호에 따라 실시한다.

1. 백업 대상 : 정보서비스를 제공하는 서버 시스템의 OS 및 설정파일을 백업 한다.(대상 서버는 가감될 수 있다.)
2. 백업 주기 : 자동백업 관리시스템의 스케줄에 등록하여 실시한다.
3. 백업 방법 : 자동백업 관리시스템과 카트리지 DAT Tape을 사용한다.
4. 이동 방법 : 인편에 의한 OS백업 이미지를 안정한 보관장소까지 이동한다.
5. 보관 방법 : 백업 Tape를 원격지에 이동 보관한다.

③ 유지보수 계약을 통해 장애발생 가능성이 있는 파트에 대한 예비부품을 확보한다.
④ 원격지(타 전산실)에 사전 백업 보관된 OS이미지를 사용하여 복구한다.
⑤ 시스템 OS 복구는 다음 순서에 따라 실시한다.
1. 백업 받아 두었던 OS백업 이미지 Tape을 준비한다.
2. 백업 OS 이미지 tape을 시스템에 삽입하고 해당 tape을 이용하여 시스템을 부팅한다.
3. 부팅 후 시스템 복구 메뉴를 이용하여 OS백업 이미지를 이용하여 OS를 복구한다.
4. 복구가 완료되면 시스템의 이상 유무를 확인한 후 서비스를 구동한다.
⑥ 서버 시스템의 하드웨어 장애가 발생했을 경우 유지보수 계약업체는 대체 하드웨어를 조달하여 신속히 교체 복구한다.

제79조(네트워크 시스템의 재난 복구)

① 소프트웨어 백업 대상은 인터넷 관문 라우터, 백본 L3 스위치, 각 건물의 주요 L3 스위치의 펌웨어(IOS, AOS)와 설정파일로 한다.
② 월 1회(정기백업), 설정 변경시(수시백업) 실시하며, 자동백업 시스템를 이용하여 백업한다.
③ 전산실에 위치한 백업 파일서버에 보관한다.
④ 하드웨어 백업은 유지보수 계약을 통해 장애발생 가능성이 있는 파트에 대한 예비부품을 확보한다.
⑤ 소프트웨어 복구는 백업 파일서버에 백업된 이미지를 사용하여 복구하며, 복구절차는 다음과 같다.
1. 백업 받아 두었던 펌웨어(IOS, AOS)와 설정파일을 준비한다.
2. 펌웨어를 시스템에 적용하고 재부팅한다.
3. 부팅 후 백업된 설정파일을 적용하여 시스템의 설정을 복구한다.
4. 복구가 완료되면 시스템의 이상 유무를 확인 및 통신 상태를 점검한다.
⑥ 복구 우선순위는 재난에 의거 다수 지역에서 장애가 동시 발생했을 경우는 다음 순서에 따라 복구를 시행한다.
1. 인터넷 관문
2. 백본 L3스위치
3. 주요 건물 L3/L2 스위치

제80조(데이터, 어플리케이션의 재난 복구)

① 백업솔루션을 이용한 백업을 수행 시 각 주요 서버에 대해서 일별 Online백업, 월별 소산백업을 진행하며, 중요 데이터, 어플리케이션은 백업솔루션을 이용하여 다음과 같이 일별 Online 백업을 실시한다.
1. 백업대상은 정보서비스를 제공하는 서버로 별도로 정하며, 대상은 가감될 수 있다.
2. 백업방법은 백업솔루션의 스케줄러 기능을 이용하여 각 대상 시스템에 Client 스케줄러를 탑재하여 일별 백업을 수행하며, Crontab을 이용하여 주기적으로 백업 명령을 자동으로 수행한다.
3. 백업주기는 별도로 정한다.
② 월 1회 주기로 백업시스템을 이용하여 백업된 데이터들에 대해서 다음과 같이 소산 백

업을 실시한다.

1. 백업 대상은 백업장비에 보관 중인 모든 백업 데이터로 한다.
2. 백업 방법은 백업시스템의 백업 데이터 복사기능을 이용하여 소산용 백업 미디어에 백업 데이터를 복사한다.
3. 소산 방법은 백업 장비에서 백업데이터 복사본을 배출하여 소산한다.

③ 산 백업한 백업데이터 복사본은 인편으로 안전한 장소로 이동 보관하며 다음과 같이 처리한다.

1. 이동 방법은 인편을 이용한 미디어 이동을 한다.
2. 보관 방법은 본교의 안전한 장소에 보관한다.
3. 보관 주기는 6개월로 한다.

④ 사용자 실수에 의한 데이터 손실 복구는 백업솔루션에 의해 백업된 데이터를 사용하여 다음과 같이 복구를 실시한다.

1. 주기적인 백업을 수행한 백업본을 이용한 데이터 복구를 수행한다.
2. 데이터가 소실된 대상 서버에서 복구 명령교직원 또는 GUI 매니저를 이용하여 손실된 데이터(파일 또는 파일 시스템)를 복구한다.
3. 복구된 데이터에 대한 정합성 및 활용성 테스트를 진행한다.

⑤ 재난에 의한 데이터 손실 복구는 백업솔루션의 백업데이터를 사용하여 복구한다.

⑥ 유지보수 계약업체를 통해 파손된 하드웨어의 대체 하드웨어를 신속하게 준비한다.

⑦ 시스템 OS 복구는 서버 시스템의 재난 복구계획을 참고한다.

⑧ 데이터, 어플리케이션의 복구는 준비된 시스템에 백업솔루션을 사용하여 백업데이터를 다음 순서에 따라 복구한다.

1. 소산된 백업 미디어를 준비한다.
2. 백업솔루션을 사용하여 백업시스템을 구성한다.
3. 백업시스템을 이용하여 소산된 백업 미디어에서 데이터를 복구한다.

⑨ 데이터 복구 완료시 해당 시스템에 대한 어플리케이션 서비스를 재개한다.

제10장 정보시스템 유지보수

제81조(정보시스템 유지보수)

① 정보시스템 유지보수 절차・주기・문서화 수립시 고려사항은 아래의 각 호와 같다.

1. 유지보수 인력에 대한 보안서약서 집행, 보안교육 등을 포함한 유지보수 인가 절차를 마련하고 인가된 유지보수 인력만 유지보수에 참여한다.
2. 결함이 의심되거나 발생한 결함, 예방 및 유지보수에 대한 기록을 보관한다.
3. 유지보수를 위해 원래 설치장소 외 다른 장소로 정보시스템을 이동할 경우, 통제수단을 강구한다.
4. 정보시스템 유지보수 시에는 일시, 담당자 인적사항, 출입 통제조치, 정비내용등을 기록・유지하여야 한다.

② 시스템관리자는 자체 유지보수 절차에 따라 정기적으로 정보시스템 정비를 실시하고

관련 기록을 보관하여야 한다.

③ 시스템관리자는 정보시스템의 변경이 발생할 경우, 정보보안담당관과 협조하여 정보시스템의 설계・코딩・테스트・구현과정에서의 보안대책을 강구하며 정보보안담당관은 관련 적절성을 주기적으로 확인하여야 한다.

④ 정보보안담당관은 시스템관리자 등이 유지보수와 관련된 장비・도구 등을 반출입할 경우, 악성코드 감염여부, 자료 무단반출 여부를 확인하는 등 보안조치 하여야 한다.

⑤ 시스템관리자는 외부에서 원격으로 정보시스템을 유지보수 하는 것을 원칙적으로 금지하여야 하며 부득이한 경우에는 정보보안담당관과 협의하여 자체 보안대책을 강구한 후 한시적으로 허용할 수 있다.

제11장 침해사고 대응지침

제82조(침입자 발견 요령)

① 보안 담당자는 로그 점검 혹은 실시간 모니터링을 수행할 때 다음 사항에 주의하여 침입흔적을 확인한다.

1. 같은 사용자 이름으로 두 명 이상 동시 로그인이 되고 있는지 확인한다.
2. 정규 시간 외의 시스템 사용자를 확인한다.
3. 관리자 권한 외의 작업수행 시도가 있었는지 점검한다.
4. 보안 관련 파일의 수정 및 수정시도가 불법적으로 이루어졌는지 점검한다.
5. 허가가 되지 않은 파일, 서비스 및 기타 자원의 접근 시도를 확인한다.
6. 일반 사용자의 홈 디렉토리에 시스템 파일이 존재하는지 확인한다.
7. 계정 관련 시스템 파일에 관리자 이외의 접근 시도가 있었는지 점검한다.
8. 네트워크 전송량을 증가시키는 비정상적인 프로그램 실행 작업이 있는지 점검한다.
9. 한 사용자가 많은 외부 접속을 시도하고 있는지 점검한다.
10. 허가된 모뎀 사용자가 아닌데 모뎀으로 로그인을 하려는 시도 및 접속을 점검한다.
11. 시스템의 비정상적인 동작이 있다면 외부의 불법적인 침입이 있는지의 여부를 점검한다.

② 침입 흔적을 발견시 그 원인이 IT운영 및 개발담당 부서의 관리 담당자나 프로그래머의 실수 때문인지 확인한다.

제83조(침입자의 시스템내 활동시 처리 절차)

① 보안 담당자는 침입자가 시스템 내에서 활동하고 있는 것으로 판단될 때 보안관리자에게 즉시 보고를 한다.

② 보안관리자는 필요시 관련 국가기관(KISA, CERT)의 협조를 받기 위한 절차를 준비한다. 이때, 협조 의뢰의 최종 결정은 IT담당부서장이 한다.

③ 침입자의 시스템내 활동 발견시 세부 처리 절차는 다음과 같다.

1. 내부 단말기에서 침투한 경우 현재의 단말 위치를 확인한다.
2. 현재 침입자가 시스템 내에 있다면 가능한 도구나 명령어를 이용하여 침입자에 관련된 정보를 수집한다.

3. 침입자가 수행하고 있는 명령어를 파일로 저장하거나 기록한다.
4. 침입자가 중요한 데이터에 접근을 할 경우 또는 침입자를 추적할 자신이 없을 경우 침입자의 연결을 끊는다.

④ 보안 담당자는 침입자의 시스템 내 활동에 대한 절차 적용 후 보안사고 및 대응결과를 문서로 작성하여 보안관리자에게 보고를 한다.

제84조(침입흔적 발견시 처리 절차)

① 로그 파일의 분석 등을 통해 침입한 흔적이 발견된 경우 보안진단 도구나 체크리스트를 이용하여 다음과 같은 사항을 점검한다.
1. 새로운 계정이 생성되어 있는지 확인한다.
2. 패스워드 파일이 변경되었는지 확인한다.
3. 주요 설정 및 실행 파일 등이 변경되었는지 확인한다.
4. 특정 파일의 접근 모드가 변경되었는지 확인한다.
5. 시스템 유틸리티가 변경 및 수정되었는지 확인한다.

② 데이터의 변조나 불법 접근의 흔적이 있을 경우 해당 서비스를 중지시킨다.

③ 침입자를 식별하기 위한 증거 수집을 한다.

④ 백업 등을 이용하여 복구한다.

⑤ 보안 담당자는 침입자의 시스템 내 활동에 대한 절차 적용 후 보안사고 및 대응결과서를 작성하여 보안관리자에게 보고를 한다.

제85조(침입사고 발생 시 보안관리자의 처리 절차)

① 침해사고 발생시 보안관리자의 세부 처리 절차는 다음과 같다.
1. 침해사고의 피해 상황을 파악한다.
2. 침입자를 식별하기 위한 증거를 수집한다.
3. 시스템의 복구를 지원한다.
4. 문제점을 파악하여 대책을 제시한다.
5. 필요시 교육과학기술부 및 보안관련 수사기관에 침해사고에 대한 수사를 의뢰한다.

② 보안사고 및 대응결과서(양식 2) 및 보안사고 발견 및 조치 대장(양식 3)을 작성한다.

③ 보안사고 기록은 비밀로 분류하고 1년 이상 보관한다.

④ 교육 및 홍보를 강화하고 동일 문제가 재발하지 않도록 한다.

제86조(보안취약성 발견 대응)

① 보안 담당자는 보안취약성 발견시 다음과 같이 대응한다.
1. 화면상의 메시지들 또는 로그 결과들에 대하여 기록한다.
2. 컴퓨터를 고립시키고 작업을 중지한다.
3. 보안관리자와 취약성에 대해 점검한다.
4. 보안관리자의 허가가 이루어지기 전까지는 의심스런 소프트웨어를 제거하지 않는다.
5. 보안사고 및 대응결과서(양식 2)를 작성한 뒤 보안관리자에게 즉시 보고한다.

② 보안관리자는 처리 결과를 보안사고 및 대응결과와 보안사고 발견 및 조치로 나누어서 별도로 문서화한다

제12장 위탁업체 보안지침

제87조(외주용역 보안지침)

① 시스템 개발사업 담당자는 외부용역 업체와 계약하여 정보시스템을 개발하고자하는 경우에는 다음 각 호의 사항을 고려하여 보안대책을 수립하고 정보보안담당관의 승인을 득하여야 한다.

1. 외부인력 대상 신원확인, 보안서약서 징구, 보안교육 및 점검
2. 외부인력의 보안준수 사항 확인 및 위반 시 배상책임의 계약서 명시
3. 용역기간 중 참여인력 임의교체 금지
4. 외부인력의 정보시스템 접근권한 및 제공자료 보안대책
5. 외부인력에 의한 장비 반입·반출 및 자료 무단반출 여부 확인
6. 정보통신망도, IP현황 등 용역업체에 제공할 자료는 자료 인계인수대장을 비치, 보안조치 후 인계·인수하고 무단 복사 및 외부반출 금지
7. 사업 종료 시 외부업체의 노트북·휴대용 저장매체 등을 통해 비공개 자료가 유출되는 것을 방지하기 위해 복구가 불가능하도록 완전삭제
8. 용역업체로부터 용역 결과물을 전량 회수하고 비인가자에게 제공·열람 금지
9. 용역업체의 노트북 등 관련 장비를 반입·반출시마다 악성코드 감염여부, 자료 무단반출 여부를 확인
10. 용역업체에서 사용하는 PC는 인터넷 연결을 금지. 단, 사업수행 상 연결이 필요한 경우에는 발주기관의 보안통제 하에 제한적 이용 가능
11. 원격작업은 원칙적으로 금지하나, 부득이한 경우 IP·사용서비스·접근계정 제한, 암호화 통신 등 필요한 보안대책 마련 후 한시적으로 허용하여야 하며, 반드시 정보보안담당관의 승인 후 수행함
12. 그 밖의 보안관리가 필요하다고 판단되는 사항이나 교육부장관이 보안조치를 권고하는 사항

② 용역사업 추진 시 과업지시서 · 입찰공고 · 계약서에 다음의 누출금지 대상정보를 명시해야하며 해당정보 누출 시 입찰 참가자격 제한을 위한 부정당업자로 등록하여야 한다.

1. 학교 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
6. 보안시스템 및 정보보호시스템 도입 현황
7. 침입차단시스템 · 방지시스템교직원 등 정보보호제품 및 라우터 · 스위치 등 네트워크 장비 설정 정보
8. 비공개 대상 정보로 분류된 기관의 내부문서
9. 교직원 및 학생 개인정보
10. 그 밖에 학교의 장이 공개가 불가하다고 판단한 자료

③ 정보보안담당관은 비밀 및 중요 외주 용역사업을 수행할 경우, 외부인원에 대한 신원조사·비밀취급인가, 보안교육 및 외부유출 방지 등 보안조치를 수행하여야 한다.

④ 사업 관리책임자는 제1항부터 제3항까지 규정한 보안대책의 시행과 관련한 이행실태를 주기적으로 점검하고 미비점 발견 시 사업담당자로 하여금 보완토록 조치하여야 한다.

제88조(정보시스템 위탁운영 보안관리)

① 정보시스템에 대한 외부업체의 위탁 운영을 최소화하되, 위탁 운영과 관련한 관리적·물리적·기술적 보안대책을 수립하여 시행하여야 한다.

② 정보시스템의 위학 운영은 여타 기관 또는 업체 직원이 당해 기관에 상주하여 수행하는 것을 원칙으로 한다. 다만, 해당기관에 위탁업무 수행 직원의 상주가 불가한 타당한 사유가 있을 경우, 그러하지 아니할 수 있다.

③ 정보시스템 위탁운영과 관련하여 동 조문에 명시되지 않은 사항에 대하서는 “외주용역 보안지침”을 준용한다.

제13장 휴대용저장매체 보안지침

제89조(휴대용저장매체 보안지침)

① 휴대용 저장매체 관리책임자는 휴대용 저장매체를 사용하여 중요 업무자료를 보관할 필요가 있을 때에는 위변조, 훼손, 분실 등에 대비한 보안대책을 강구하여 정보보안담당관의 승인을 받아야 한다.

② 휴대용 저장매체 관리책임자는 휴대용 저장매체를 비밀용, 일반용으로 구분하고 주기적으로 수량 및 보관 상태를 점검하며 반출·입을 통제하여야 한다.

③ 휴대용 저장매체 관리책임자는 USB 관리시스템을 도입할 경우 국가정보원장이 안정성을 확인한 제품을 도입하여야 한다.

④ 휴대용 저장매체 관리책임자는 사용자가 USB 메모리를 PC 등에 연결 시 자동 실행되지 않도록 하고 최신 백신으로 악성코드 감염여부를 자동 검사하도록 보안 설정한다.

⑤ 비밀자료가 저장된 휴대용 저장매체는 매체별로 비밀등급 및 관리번호를 부여하고 비밀관리기록부에 등재 관리하여야 한다. 이 경우에는 매체 전면에 비밀등급 및 관리번호가 표시되도록 하여야 한다. 다만, 휴대용 저장매체가 국가용 보안시스템에 해당될 경우에는 해당 보안시스템의 운용·관리체계에 따라 관리하여야 한다.

⑥ 휴대용 저장매체를 파기 등 불용처리 하거나 비밀용을 일반용 또는 다른 등급의 비밀용으로 전환하여 사용할 경우 저장되어 있는 정보의 복구가 불가능하도록 보안조치를 하여야 한다.

⑦ 정보보안담당관은 사용자의 휴대용 저장매체 무단 반출 및 미등록 휴대용 저장매체 사용 여부 등 보안관리 실태를 주기적으로 점검하여야 한다.

제14장 전산실 운영·관리 보안지침

제90조(전산실 시설기준)

① 통신장비, 정보시스템이 설치되어 있는 전산실은 보호구역으로 설정 관리한다.
② 출입구는 반드시 2중으로 설치하며 또한 입실자를 식별 가능한 출입보안장치를 설치하여 6개월간 내용을 보관한다.
③ 자동 화재경보 설비를 설치하고, 할로겐 가스등 소화 시 장비에 피해를 주지 않는 자동 소화설비를 설치한다.
④ 정전에 대비하여 별도의 전원공급 시설을 둔다.
⑤ 온·습도를 적절히 유지할 수 있는 항온항습기를 설치한다.

제91조(전산실 운영 및 관리)

① 전산실의 운영을 담당하고 있는 부서장은 시스템실 사용 및 운영에 관한 절차 및 방법을 규정하고, 담당자들이 이를 숙지하도록 한다.
② 전산실의 운영자는 운영일지 및 장애일지를 작성해야 한다.
③ 시스템 운영자는 주기적으로 로그 파일을 분석해야 하며, 시스템에 이상이 발견 되었을 경우에는 보안사고 처리 지침에 따라 즉시 조치를 취하고 이를 정보보안전담팀 및 부서장에게 보고해야 한다.
④ 전산실에는 출입자 명부를 비치하고 비인가자의 출입을 통제해야 한다.
⑤ 휴대용 전자매체를 보관할 수 있는 용기를 비치한다.
⑥ 전산실의 불법 촬영 방지를 위하여 카메라, 휴대전화의 반입을 금지하며, 반입 필요 시 관리자책임자의 승인을 득한다.
⑦ 전산실의 관리책임자를 지정하고 자료 또는 장비별로 취급자를 지정 운영해야 한다.

제15장 정보통신망 자료 보안지침

제92조(정보통신망 관련 형황 자료)

① 다음 각 호에 해당하는 정보통신망 관련 현황·자료 관리에 유 의하여야 한다.
1. 정보시스템 운용 현황
2. 정보통신망 구성 현황
3. IP 할당현황
4. 주요 정보화 사업 추진현황

제93조(정보통신망 대외비 자료)

① 다음 각 호의 자료를 대외비로 분류하여 관리하여야 한다.
1. 정보통신망 세부 구성현황 (IP 세부 할당현황 초함)
2. 보안시스템 운용 현황
3. 보안취약점 분석·평가 결과물
4. 그 밖에 보호할 필요가 있는 정보통신말 관련 자료

제16장 접근기록 관리

제94조(접근기록 관리)

① 시스템관리자는 정보시스템의 효율적인 통제·관리, 사고 발생 시 추적 등을 위하여 이용자의 정보시스템 접근기록을 유지 관리하여야 한다.

② 접근기록에는 다음 각 호의 내용이 포함되어야 한다.

1. 접속자, 정보시스템·응용프로램 등 접속 대상
2. 로그 온·오프, 파일 열람·출력 등 작업 종류, 작업 시간
3. 접속 성공·실패 등 작업 결과
4. 전자우편 사용 등 외부발송 정보 등

③ 시스템관리자는 접근기록을 분석한 결과, 비안가자의 접속 시도, 정보 위·변조 및 무단 삭제 등의 의심스러운 활동이나 위반 혐의가 발생한 사실을 발견한 경우 정보보안담당관에게 즉시 보고하여야 한다.

④ 접근기록은 정보보안 사고발생 시 확인 등을 위하여 6개월 이상 보관하여야 한다.

제17장 정보보호시스템 도입관리

제95조(정보보호시스템의 도입 등)

① 정보 및 정보통신망 등을 보호하기 위해 정보보호시스템, 네트워크 장비 등 보안기능이 있는 정보통신제품을 도입 시 보안접합성 검증을 해야한다. 단, 시스템 단순 교체 등 사안이 경미하다고 판단하는 경우에는 보안접합성 검증을 생략할 수 있다.

② 정보보호시스템에 중요자료 저장·소통을 위한 암호기능이 포함될 경우 아래와 같은 알고리즘 및 보호함수가 포함된 검증필 암호모듈을 탑재하여야 하며 구체적인 사항은 국가정보원장이 별도로 정한다.

제18장 무선랜 보안관리

제96조(무선랜 보안 관리)

① 무선랜(와이파이 등)을 사용하여 업무자료를 소통하고자 할 경우 자체 보안대책을 수립하여야 한다.

② 시스템관리자는 제1항의 보안대책 수립 시, 다음 사항을 포함하여야 한다.

1. WPA2 이상(256비트 이상)의 암호체계를 사용하여 소통자료 암호화(국가정보 원장이 승인한 암호논리 사용)
2. MAC 주소 및 IP 주소 필터링 설정
3. RADIUS(Remote Authentication Dial-In User Service) 인증 사용
4. 무선망을 통한 업무망 정보시스템 접근을 정보보호시스템 등으로 차단하는 보안 대책
5. 무선단말기·중계기(AP) 등 무선랜 구성요소별 분실·탈취·훼손·오용 등에 대비한 관리적·물리적 보안대책
6. 그 밖에 학교의 장이 정하는 무선랜 보안 대책 강구

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

제97조(무선인터넷 보안관리)

① 무선인터넷(WiBro, HSDPA 등) 시스템을 구축하여 업무자료를 소통하고자 할 경우 자체 보안대책을 수립하여 관련 사업 계획단계(사업 공고 전)에서 보안성검토를 자체적으로 실시한다.

② 시스템관리자는 업무용PC에서 무선인터넷 접속장치(USB형 등)가 작동되지 않도록 관련 프로그램 설치 금지 등 기술적 보안대책을 강구하여야 한다.

③ 사용자는 개인 휴대폰을 제외한 무선인터넷 단말기의 사무실 무단 반입·사용을 금지하여야 한다.

제98조(스마트폰 등 모바일 행정업무 보안관리)

① 스마트폰 등을 활용하여 내부행정업무와 현장행정업무 및 대민서비스업무 등 모바일 업무환경을 구축할 경우 보안대책을 수립·시행하여야 한다.

제19장 원격근무 보안관리

제99조(원격근무 보안관리)

① 재택 · 파견 · 이동근무 등 원격 근무를 지원하기 위한 정보시스템을 도입 · 운영할 경우 기술적 · 관리적 · 물리적 보안대책을 수립하여야 한다.

② 원격근무 가능 업무 및 공개·비공개 업무 선정기준을 수립하되 대외비 이상 비밀자료를 취급하는 업무는 원격근무 대상에서 원칙적으로 제외하되 반드시 수행해야 하는 경우 보안대책 강구 후 교육부장관과 협의하여 수행여부를 결정한다.

③ 모든 원격근무자에게 원격근무 보안서약서를 징구하고 원격 근무자의 업무변경 · 인사이동 · 퇴직 등 상황 발생 시 정보시스템 접근권한 재설정 등 관련 절차를 수립하여야 한다.

④ 원격근무자는 원격근무 시 해킹에 의한 업무자료 유출을 방지하기 위하여 작업수행 전 백신으로 원격근무용 PC 점검·업무자료 저장금지 등 보안조치를 수행하여야 한다.

⑤ 원격근무자는 정보시스템 고장 시 정보유출 방지 등 보안대책을 강구한 후 정보보안담당관과 협의하여 정비·반납 등 조치를 취하여야 한다.

⑥ 비공개 원격업무인 경우에는 국가용 보안시스템을 사용하여 소통자료를 암호화하고 행정전자서명체계를 이용하여 인증하며 인증강화를 위해 일회용 비밀번호·생체인증 등 보안기술을 사용하여야 한다.

⑦ 정보보안담당관은 주기적인 보안점검을 실시하여 원격근무 보안대책의 이행여부를 확인하여야 한다.

부 칙

이 규정은 2011년 10월 1일부터 시행 한다.

이 규정은 2013년 10월 1일부터 시행 한다.

이 규정은 2016년 4월 1일부터 시행 한다.

이 규정은 2017년 1월 1일부터 시행 한다.