# 정 보 보 호 지 침

제정 2012. 7. 1

## 제1장 개 요

**제1조(목적)** 본 지침은 청강문화산업대학교 (이하 “본교”라 한다) 정보보호규정 제3장(정보자산 운영관리)에 의거하여 전자계산소와 기타 단위 부서의 시설 및 전산장비에 대한 물리적, 관리적 보안을 강화하는 것을 그 목적으로 한다.

**제2조(적용범위)** 본 지침은 본교 전자계산소와 기타 단위 부서의 전산시스템 운영자를 대상으로 한다.

**제3조(용어정의)**

1. 보안사고 : 보안정책에 위배되는 모든 사고를 말하며 보안 침해사고, 소프트웨어 이상 및 오류, 바이러스 등으로 인한 정보자산의 손상 등을 포함한다.
2. 침해사고 : 권한이 없는 사용자가 비합법적인 방법으로 시스템에 접근하여 시스템의 서비스를 지연시키거나 시스템을 파괴, 데이터를 변조, 삭제하는 등의 행위를 통칭한다.
3. 취약성 : 조직 내부 혹은 정보시스템을 사용하는 환경 등에 내재된 위협에 의해서 자산이나 조직의 업무 환경에 피해를 가할 수 있는 가능성을 제공하는 요소이다.
4. 전자문서 : 컴퓨터 등 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 정보를 말한다.
5. 전자기록물 : 정보처리능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 기록정보자료를 말한다.
6. 전자정보 : 각급기관이 업무와 관련하여 취급하는 전자문서 및 전자기록물을 말한다.
7. 사이버공격 : 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스방해 등 전자적 수단에 의하여 정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 공격 행위를 말한다.
8. 무결성 : 정보처리 과정 및 전송 도중에 정보가 불법적으로 변경되지 않고 일관성을 유지하는 것을 말한다.
9. 감사 : 전산시스템이 수립된 사용정책 및 보안정책에 준하여 안전하게 운용되고 있는지를 확인하기 위하여 전산시스템 내에 기록• 저장되어 있는 각종 사용자 행위에 대한 상세 내용을 조사•분석하는 것을 말한다.
10. 접근통제 : 인가된 사용자, 프로그램, 프로세스, 시스템 등의 주체만이 전산시스템의 자원에 접근할 수 있도록 제한하는 것을 말한다.
11. 데이터베이스 : 논리적으로 연관된 레코드나 파일의 모임으로 여러 개의 파일이나 응용 프로그램에 의해 저장되고 처리되던 자료들을 하나의 통합된 시스템으로 만들어서 이들 자료의 가치를 더욱 높이는 기능을 한다.

12. DBMS(database management system) : 데이터베이스를 구성하고 이를 응용하기 위하여 구성된 소프트웨어 시스템이다. 사용자나 응용프로그램이 데이터베이스를 쉽게 이용할 수 있도록 해 주며, 그 기능은 크게 구성 기능, 조작 기능, 그리고 제어 기능으로 나눌 수 있다.

13. 암호화 : 정보의 보안을 유지하기 위해 정보를 특정한 규칙에 따라 변형하여 저장함으로써 해독 방법을 모르는 사람은 그 정보의 내용을 알아볼 수 없도록 하는 것을 의미한다.

**제4조(정보보안담당관 운영)** ① 효율적·체계적인 정보보안 업무를 수행하기 위하여 정보보안 전문지식을 보유한 인력을 확보하고 관련 전담조직을 구성 운영하여야 한다.

② 대학은 정보보안 조직을 지휘하고 소속 및 산하기관에 대한 정보보안 업무를 총괄하기 위하여 전자계산소장을 '정보보안담당관(이하 담당관)'으로 임명한다.

③ 담당관은 보안담당자를 임명한다.

④ 담당관의 기본활동은 다음 각 호와 같다.

1. 정보보안 정책 및 기본계획 수립·시행
2. 정보보안 관련 규정·지침 등 제·개정
3. 정보보호위원회 정보보안 분야 안건 심의 주관
4. 정보보안 업무 지도·감독, 정보보안 감사 및 심사분석
5. 정보보안 관리실태 평가
6. 사이버위협정보 수집·분석 및 보안관제
7. 정보보안 예산 및 전문인력 확보
8. 정보보안 사고조사 결과 처리
9. 정보보안 교육 및 정보협력
10. 국가용 보안시스템 및 암호키의 운용·보안관리
11. 정보통신망 보안대책의 수립·시행
12. '사이버보안진단의 날' 계획 수립·시행
13. 그 밖에 정보보안 관련 사항

## 제2장 침해사고대응 지침

**제5조(침입자 발견 요령)** ① 보안담당자는 로그 점검 혹은 실시간 모니터링을 수행할 때 다음 사항에 주의하여 침입흔적을 확인한다.

(가) 같은 사용자 이름으로 두명 이상 동시 로그인이 되고 있는지 확인한다.

(나) 관리자 권한 외의 작업수행 시도가 있었는지 점검한다.

(다) 보안 관련 파일의 수정 및 수정 시도가 불법적으로 이루어졌는지 점검한다.

(라) 허가가 안된 파일, 서비스 및 기타 자원의 접근 시도를 확인한다.

(마) 네트워크 전송량을 증가시키는 비정상적인 작업이 있는지 점검한다.

(바) 일반 사용자의 홈 디렉토리에 시스템 파일이 존재하는지 확인한다.

(사) 한 사용자가 많은 외부 접속을 시도하고 있는지 점검한다.

(아) 외부의 불법적인 침입이 있는지의 여부를 점검한다.

② 침입의 흔적을 발견 시 그 원인이 IT운영 및 개발 담당 부서의 관리 담당자의 실수 때문인지 확인한다.

**제6조(침입자의 시스템 내 활동 시 처리 절차)** ① 보안담당자는 침입자가 시스템 내에서 활동하고 있는 것으로 판단될 때 정보보호총괄책임자(이하 담당관)에게 즉시 보고 한다.

② 담당관은 필요시 관련 국가기관(KISA 등)의 협조를 받기 위한 절차를 준비한다.

③ 침입자의 시스템 내 활동을 발견시 세부 처리 절차는 다음과 같다.

(가) 내부 단말기에서 침투한 경우 현재의 단말 위치를 확인한다.

(나) 침입자가 수행하고 있는 명령어를 파일로 저장하거나 기록한다.

(다) 침입자의 추적이 불가능 할 경우 침입자의 연결을 끊는다.

④ 보안담당자는 침입자의 시스템 내 활동에 대한 절차 적용 후 보안사고 및 대응결과를 문서로 작성하여 담당관에게 보고를 한다.

**제7조(침입흔적 발견 시 처리 절차)** ① 로그 파일의 분석 등을 통해 침입한 흔적이 발견된 경우 보안진단 도구나 체크리스트를 이용하여 다음과 같은 사항을 점검한다.

(가) 새로운 계정이 생성되어 있는지 확인한다.

(나) 패스워드 파일이 변경되었는지 확인한다.

(다) 주요 설정 및 실행 파일 등이 변경되었는지 확인한다.

(라) 특정 파일의 접근 모드가 변경되었는지 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 보안담당자는 보안사고 및 대응결과를 담당관에게 보고한다.

**제8조(침해사고에 대한 담당관의 처리 절차)** ① 침해사고 발생 시 담당관의 세부 처리 절차는 다음과 같다.

(가) 침해사고의 피해 상황을 파악한다.

(나) 침입자를 식별하기 위한 증거를 수집한다.

(다) 시스템의 복구를 지원한다.

(라) 문제점을 파악하여 대책을 제시한다.

(마) 필요시 교육과학기술부 및 관련 수사기관에 침해사고에 대한 수사를 의뢰 한다.

② 보안사고 및 대응결과서와 보안사고 발견 및 조치대장을 작성한다.

③ 보안사고 기록은 비밀로 분류하고 1년 이상 보관한다.

④ 교육 및 홍보를 강화하고 동일 문제가 재발하지 않도록 한다.

**제9조(보안취약성 발견 및 대응)** ① 보안담당자는 주기적으로 시스템을 모니터링하여 시스템이나 소프트웨어의 보안취약성을 파악한다.

② 보안담당자는 보안취약성 발견시 다음과 같이 대응한다.

(가) 화면상의 메시지들 또는 로그 결과들에 대하여 기록한다.

(나) 컴퓨터를 고립시키고 작업을 중지한다.

(라) 담당관의 허가가 이루어지기 전까지는 의심스런 소프트웨어를 제거 하지 않는다.

(마) 보안사고 및 대응결과서를 작성한 뒤 담당관에게 즉시 보고한다.

③ 담당관은 처리 결과를 보안사고 및 대응결과와 보안사고 발견 및 조치로 나누어서 별도로 문서화한다.

## 제3장 네트워크 보안지침

**제10조(네트워크 보안)** ① 네트워크 구성 시 보안과 관련된 정보 ( 네트워크 노드, IP주소, 관리자 암호 등)에 관한 접근을 통제한다.

② 일반 사용자들은 PC의 IP 주소를 임의로 변경할 수 없다.

③ 내부망에는 공인 IP를 사용하며 사정에 따라 사설IP를 사용 할 수 있다.

④ 타 네트워크 연결 시 IP 인증 외에 사용자 인증을 사용하도록 한다.

⑤ 인터넷을 통한 모든 접속을 로깅한다.

⑥ 원격 사용자의 공중 네트워크를 통한 접속은 인증 또는 암호화되어야 한다.

⑦ 원격 전산 시스템에 의한 접속은 인증되어야 한다.

⑧ 네트워크간의 접속은 보안 기능에 의하여 통제되어야 한다.

⑨ 보안사고 발생 시 처리는 침해사고대응 지침에 준하여 시행한다.

⑩ 해당 업무별 관리자는 주기적으로 네트워크 보안점검을 수행하고 그 결과를 별도로 기록하여 문서화한다.

**제11조(네트워크 진단 /경로설정)** ① 네트워크 포트가 열려 보안에 취약성이 발생할 수 있으므로 진단 포트에 대한 불법적인 접속 여부에 대해 주기적인 점검을 실시한다.

② 네트워크 진단/관리 도구들은 네트워크 관리 담당자에 의해서만 사용되고 일반 사용자들에게는 사용이 허가되지 않는다.

③ 전산시스템상 접근이 허가된 단말기 외에 전용통신링크를 사용 할 수 없다.

④ 네트워크 사용자는 부서 책임자로부터의 사전승인 없이 개인 소유의 컴퓨터, 주변장치 또는 소프트웨어를 별도로 네트워크에 연결해서는 안된다.

**제12조(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 관계자가 동행을 수행하며 작업 일지에 기록한다.

④ 인터넷 설치를 위한 협정 또는 작업은 담당관의 승인 이후에 수행되어야 한다.

⑤ 사용하지 않는 통신 장비 및 네트워크 세그먼트는 물리적으로 접속을 차단한다.

⑥ 네트워크 변경, 신설, 이전 시에는 네트워크 관리자가 작업의뢰서를 통하여 관리하며, 폐쇄 시는 네트워크 관리자에게 반드시 보고한다.

⑦ 장비의 불량으로 인한 교체 시 네트워크 관리 담당자에게 통보되어야 하며, 장비설정이 가능한 경우 장비에 설정된 내역을 모두 삭제한 후 교체하여야 한다.

⑧ 단일 장비의 구성 정보 오류에 대한 변경은 네트워크 관리 담당자의 직권으로 결정한다.

**제13조(보안장비의 논리적 보안)** 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.

(가) 패스워드 조합의 가능성을 최대로 하며 주기적으로 변경한다.

(나) 3회 이상 틀린 패스워드의 시도가 있는 터미널은 자동으로 접속을 차단한다.

(다) 네트워크 소프트웨어는 비인가자의 접근을 막기 위하여 일정한 시간동안 활동 없이 접속한 상태를 유지하는 사용자의 접속을 강제로 끊을 수 있어야 한다.

(라) 기타 로그인, 계정 및 패스워드 지침은 해당 서버의 지침에 의거한다.

④ 네트워크 관리 담당자는 네트워크 장비 설치에 대한 내용을 네트워크 시스템 목록에 기록하여 문서화한다.

⑤ 장비의 특성별 상황에 맞추어 구성 정보 변경과 구성 정보 조회를 할 수 있는 사용자를 구분하여 설정한다.

⑥ 인가된 자만이 장비에 접속하여 구성을 변경해야 한다.

⑦ 네트워크 구성 및 보안과 관련된 정보 ( 네트워크 노드, IP주소, 관리자 암호 등 )에 관한접근을 통제한다.

⑧ 네트워크 장비의 구성 및 IP 할당 내역은 네트워크 관리 담당자가 관리한다.

**제14조(인터넷망의 외부접속)** ① 외부로부터의 내부 네트워크 접속 요청 시 보안 사항을 먼저 검토한다.

② 외부와의 연결은 신뢰할 수 있는 대상으로 한정한다.

③ 인터넷 연결은 보안에 최대한 중점을 두어 판단하도록 한다.
④ 인터넷을 통한 비밀정보 전송시 암호화한다.
⑤ 내부망 포함 민감한 정보는 반드시 암호화 대책을 수립하여야 한다.
⑥ 암호화에 사용되는 키 값은 외부에 노출되지 않도록 철저히 관리한다.
⑦ 교내에서 인터넷으로의 연결시는 모든 서비스를 허용함을 원칙으로 하나, 보안 관리상의 문제점이 노출될 경우 일부 서비스를 제한할 수 있다.
⑧ 교외에서 인터넷을 통한 내부 네트워크로의 연결은 원칙적으로 금지한다. 필요시 보안 관리자의 승인을 받아야 한다.
⑨ 서비스가 요구될시 네트워크 관리 담당자에게 필요 서비스를 네트워크 연결신청서를 통해 요청할 수 있으며, 네트워크 관리 담당자는 보안성 검토 후 허가 여부를 결정한다.
⑩ 허가된 서비스는 한시적으로 허용되므로, 신청자는 서비스의 필요 기간이 지난 후에는 즉시 네트워크 관리 담당자에게 사용종료를 보고하여야 한다.
⑪ 침입차단 시스템을 적용할 경우 구체적인 절차는 해당 절차서를 따른다.

## 제4장 PC 및 바이러스보안 지침

**제15조(PC보안)** ① 부팅 후 CMOS에서 패스워드를 설정함으로써 논리적인 접근통제가 이루어지도록 한다.
② 모든 PC에 화면보호기 패스워드를 설치하여 조작자가 잠시 자리를 비운 사이에 비인가자가 그 PC을 이용하여 작업하는 것을 방지한다.
③ 영문과 숫자를 혼용해 8자 이상의 패스워드를 사용한다.
④ 주민번호, 전화번호, 생일, 사전에 나오는 단어 등 임의 추측이 가능한 패스워드를 피한다.
⑤ 업무상 필요한 경우를 제외하고는 공유를 하지 않으며 부득이 하게 공유를 사용할 경우 패스워드를 부여해야 한다. 단 공유는 최소한의 파일만 공유해야 한다.
⑥ PC는 일반 사용자의 접근이 가능하기 때문에 비밀 정보의 노출 위험이 존재하므로 가능한 비밀 정보를 보관하지 않는다.
⑦ PC에서 데이터를 전송과 검색을 할 경우 보안 문제나 개인적인 프라이버시 침해 등을 미연에 방지하기 위해 보안 수준을 점검하며, 웹 브라우저의 인터넷 보안 수준을 "보통" 혹은 "높음"으로 설정한다.
⑧ 웹 브라우저의 각종 보안 패치 및 서비스 팩을 설치한다.

**제16조(인터넷 접속)** ① 무단 복제, 해킹, 음란, 국가기관에서 접속 금지를 요청한 사이트는 항시 접속이 금지된다.
② 악성 자료를 포함하는 사이트를 발견했을 경우, 해당 사이트의 URL을 반드시 보안 담당자에게

통보하여 해당 사이트의 접근을 침입차단시스템에서 제한하도록 한다.

③ 비 인가된 소프트웨어 및 불법 소프트웨어 사용을 금지한다.

④ 인터넷을 통해 파일이나 소프트웨어를 다운로드 받을 경우 바이러스 백신 프로그램을 적용한 후 사용한다.

⑤ 바이러스 백신 프로그램이 PC 기동 시 자동으로 실행되도록 하고, 바이러스 백신 프로그램은 정기적으로 업데이트를 수행한다.

**제17조(바이러스 관리)** ① 비 인가된 소프트웨어 및 불법 소프트웨어 사용을 금지한다.

② 외부 네트워크나 매체로부터 파일이나 소프트웨어를 다운로드 받을 경우 백신 프로그램을 적용한 후 사용한다.

③ 전자우편 첨부 파일에 대한 바이러스 감염 여부를 점검한다.

④ 시스템의 바이러스 감염 시 즉각 보안담당자에게 통지한다.

⑤ 네트워크상의 파일 서버에 대한 관리책임을 명확히 하며, 주기적으로 점검하여 불법 소프트웨어 및 악성 소프트웨어 (바이러스, 백도어 포함) 에 대한 탐지를 수행 한다.

⑥ 보안담당자는 바이러스를 예방 및 제거할 수 있는 최신 백신 프로그램을 배포한다.

⑦ 사용자는 USB 및 다운로드를 통해 외부에서 반입되는 파일은 사용 전 반드시 바이러스의 감염 여부를 검사하고 바이러스 발견 시 이를 완전히 제거 후 사용한다.

⑧사용자는 제3자에게 소프트웨어를 제공하기 전에 바이러스나 프로그램 오류 등이 있는지 검사하여야 한다.

⑨보안관리자는 바이러스 발견을 확인하고 적절한 조치를 취하며 그 결과를 보안사고 및 대응 결과서 및 바이러스 발견 및 조치대장에 기록한다.

**제18조(불법소프트웨어)** ① 모든 사용자는 반드시 사용이 승인된 소프트웨어만을 사용해야 하며 불법 소프트웨어를 사용한 경우 개인이 처벌을 받을 수 있다.

② 다음과 같은 불법 소프트웨어 사용을 금지한다.

(가) 정품 소프트웨어를 별도의 라이센스 없이 무단 복제

(나) 온라인 통신망 및 인터넷을 통한 불법 복제

(다) 시리얼 넘버의 공유 • 도용 • %배포 • 전송 등의 행위

(라) 기한이 지나거나 업무 목적에 의해 이용이 금지된 셰어웨어 사용

(마) 업무 목적에 의해 이용이 금지된 프리웨어 사용

## 제5장 E-Mail 보안지침

**제19조(E-mail 사용 보안지침 및 절차)** ① 퇴직 또는 의원면직 시 E-mail 계정을 곧바로 삭제한다.

②업무용 E-mail을 개인적인 용도로 사용해서는 안된다.

③ 외부직원, 임시 직원은 원칙적으로 본교 E-mail을 사용할 수 없으며, 예외의 경우 그 이유를 문서화한다.

④ 비밀 또는 본교가 소유한 정보는 E-mail로 보내지면 안된다.

⑤ 사용자는 본인의 암호를 3개월마다 변경해야 하며, 사용자 암호는 8자리 이상의 특수문자 + 숫자 + 문자의 조합으로 입력해야 한다.

⑥ E-mail서버에서 첨부 파일에 대한 바이러스 검사를 실시한다.

## 제6장 데이터베이스 보안지침

**제20조(DB 계정관리)** ① DB 보안담당자는 계정 및 패스워드 관리에 대한 책임과 권한을 갖는다.

② 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.

③ 퇴직자, 장기 파견자, 휴직자는 업무에서 신속히 제거한다.

④ 계정 정보 (이름, 연락처, 직위, 업무, DB에서의 작업과 권한 ) 에 관한 사용자 관리대장이 존재하고 모든 사용자에 대해 작성되어야 한다.

⑤ 장애복구나 점검을 위해 DB 관리 담당자 권한 위임 시 작업종료 후 주요 항목에 대해 DB보안 점검 결과서를 작성 후 점검 후 패스워드를 변경하도록 한다.

⑥ DB 관리 담당자 권한을 가지고 있던 사용자가 이/퇴직 등의 사유로 다른 곳을 옮길 때에는 인수자는 즉시 변경하여 DB관리자 계정 및 패스워드 현황에서 기존 패스워드를 변경하도록 한다

⑦ 계정이름과 동일한 패스워드를 사용하거나 DB서버의 이름을 패스워드로 사용, 예정된 계정의 이름을 패스워드로 사용하는 경우 쉽게 계정에 대한 패스워드를 추측하여 서버에 접속 할 수 있으므로 추측하기 쉬운 패스워드는 절대 사용하지 않는다.

⑧ 사용자가 DB 파일에 접근할 수 있는 수준은 보안관리 규정에 따른 정보보호 등급과 사용자의 접근 권한에 따라 DB 관리 담당자가 결정해야 한다.

**제21조(DB 암호화/감사)** ① 기밀성이 요구되는 DB 시스템 내의 중요 필드에 대해 암호화되어 있어야 한다.

② 암호화를 지원할 수 있는 암호화 기술이 DB 시스템에 도입되어야 한다.

③ 개별 사용자의 접근권한 통제 및 데이터 요소별로 데이터를 보호할 수 있는 자체보안 알고리즘을 갖추고 있어야 한다.

④ 기록된 로그파일 ( 감사증적 ) 은 DB 보안담당자에 의해서 정기적으로 점검되어야 한다.

⑤ 로그/감사에 대한 엄격한 접근제어를 실시한다.

⑥ 중요 DB의 경우 DB 관리 담당자와 DB 보안관리자의 권한을 분리한다.

⑦ 로그파일의 무결성을 보장하기 위하여 로그파일 자체에 대한 모니터링을 주기적으로 실시한다.

## 제7장 응용프로그램 보호지침

**제22조(응용프로그램 패스워드 관리)** ① 패스워드는 문자/숫자를 조합하여 8자리 이상으로 한다.

②계정의 패스워드 입력 제한의 횟수를 정의하고, 정의된 횟수 실패 시 자동적으로 연결이 해제 ( disconnected ) 되도록 한다.

③ 사용자 패스워드는 암호화하여 조회가 불가하도록 해야 한다.

④ 사용자 비밀번호는 화면 및 출력물에 노출되어서는 안된다.

⑤ 패스워드가 없거나 패스워드가 계정이름과 동일한 계정을 허용해서는 안된다.

⑥ 모든 사용자는 패스워드 인증을 통해서만 시스템을 사용할 수 있게 하여야 한다.

⑦ 패스워드는 3개월마다 변경되어 져야 한다.

**제23조(응용프로그램 외주 개발)** ① 응용프로그램을 외주 개발로 수행하여 공급받을 경우 공급자로부터 아래항목을 포함한 개발 소프트웨어 무결성 증명서를 받아 두어야 한다.

(가) 시스템 개발시 감사업무 수행에 필요한 자료를 생성하도록 감사기능을 설계한다.

(나) 개발된 소프트웨어의 기능이 문서화 내용과 차이가 없어야 한다.

(다) 정보보호를 위협하는 은폐구조가 없어야 한다.

(라) 실행 중 보안/통제 설계의 오류나 설계된 보안구조를 회피하거나 변경시키는 코드가 없어야 한다.

**제24조(개발업무 보안지침)** ① 각 개발 담당자별로 계정을 부여하는 것을 원칙으로 한다.

② 개발 담당자의 접근권한은 데이터 관리지침에 의해 현황을 정리한다.

③ 개발 담당자의 담당업무 변경, 전출, 퇴직 등의 사유 발생시 기존에 허용했던 전산자원의 접근권한을 제한하도록 한다.

④ 단말기에 업무 및 이용자관련 자료를 보관해서는 안되고, 부득이한 상황으로 보관할 경우 비밀번호 등 주요 정보를 암호화하여 보관하여야 한다.

⑤ 개발 보안담당자는 주기적으로 개발업무와 관련된 보안점검을 실시하고 개발업무 보안점검 결과서에 기록한다.

## 제8장 백업 및 복구 지침

**제25조(백업주기)** ① 시스템 OS백업은 다음 각 호에 따라 실시한다.

가. 백업 대상 : 정보서비스를 제공하는 서버 시스템의 OS 및 설정파일을 백업한다.

(대상 서버는 가감될 수 있다.)

나. 백업 주기 : 자동 백업 관리 시스템의 스케쥴에 등록하여 실시한다.

다. 백업 방법 : 자동 백업 관리 시스템과 카트리지 DAT Tape을 사용한다.

라. 이동 방법 : 인편에 의한 OS 백업 이미지를 안정한 보관장소 까지 이동한다.

마. 보관 방법 : 백업 Tape를 원격지에 이동 보관 한다.

**제26조(백업솔루션을 이용한 백업)** ① 각 주요 서버에 대해서 일별 Online백업, 월별 소산백업을 진행한다.

② 중요 데이터, 어플리케이션은 백업솔루션을 이용하여 일별 Online 백업을 실시하며, 백업주기는 별도로 정한다.

③ 주 1회 주기로 백업시스템을 이용하여 백업된 데이터들에 대해서 다음과 같이 소산 백업을 실시한다.

가. 백업 대상은 백업장비에 보관 중인 모든 백업 데이터로 한다.

나. 백업 방법은 백업시스템의 백업 데이터 복사 기능을 이용하여 소산용 백업 미디어에 백업 데이터 복사한다.

다. 소산 방법은 백업 장비에서 백업데이터 복사본을 배출하여 소산한다.

④소산 백업한 백업데이터 복사본은 인편으로 안전한 장소로 이동 보관하며 다음과 같이 처리한다.

가. 이동 방법은 인편을 이용한 미디어 이동을 한다.

나. 보관 방법은 본교의 안전한 장소에 보관한다.

다. 보관 주기는 6개월로 한다.

**제27조(데이터 복구)** ① 주기적인 백업을 수행한 백업 본을 이용한 데이터 복구를 수행한다.

② 복구된 데이터에 대한 정합성 및 활용성 테스트를 진행한다.

③ 시스템 하드웨어와 데이터의 완전 파손 시 백업솔루션에 의해 백업된 데이터를 사용하여 다음의 순서로 복구를 진행한다.

가. 유지보수 계약업체를 통해 파손된 하드웨어의 대체 하드웨어를 신속하게 준비한다.

나. 시스템 OS 복구는 서버 시스템의 재난 복구계획을 참고한다.

다. 데이터, 어플리케이션의 복구는 준비된 시스템에 백업솔루션을 사용하여 백업데이터를 다음순서로 복구한다.

1) 소산된 백업 미디어를 준비한다.

2) 백업솔루션 을 사용하여 백업시스템을 구성한다.

3) 백업시스템을 이용하여 소산된 백업 미디어에서 데이터를 복구 한다.

## 부 칙

1. 이 지침은 2012년 7월 1일 시행한다.