전산 업무 보안 관리 규정

제 1 장 총 칙

제1조 (목적)

이 규정은 OOOO사의 전산 자료, 전산 기기, 통신 장비 등이 타인에게 유출 또는 점거시 자료 파괴와 혼란 및 불이익을 줄 수 있는 위해 상황으로부터 보호하기 위해 대외비 자료, 개인용 컴퓨터 보안, 통제 구역 등을 규정하여 보호함을 그 목적으로 한다.

제2조 (정의)

이 규정에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. 전산 자료라 함은 전산 기기로 출력되거나 저장된 유무형의 자료를 말한다.

2. 전산 기기라 함은 전산 자료를 읽을 수 있는 하드웨어와 이에 준하는 것을 말한다.

3. 대외비란 업무상 취급 인가자 외에 타인에게 노출해서는 안 될 자료를 말한다.

4. 통제 구역이란 전산 기기, 통신 장비, 전산 자료를 보호하기 위해 인가자 외에는 들어갈 수 없는 구역을 말한다.

5. 통신 장비란 통신을 하기 위해 설치된 기기들을 총칭한다.

6. 전자 우편, 전자 결재, 게시판이란 컴퓨터 통신망을 통해 문서를 수신, 발신 및 게시하는 등의 정보 전달 체계를 말한다.

7. 주 전산기란 전자계산소내 위치한 대용량 처리 능력의 컴퓨터를 말한다.

8. 개인용 컴퓨터(이하 '컴퓨터'라 한다)란 각 부서(과) 등에서 각각의 업무 처리에 이용되고 있는 기기를 말하며 입력 장치, 중앙 처리 장치, 출력 장치로 구성되어 있다.

9. 클라이언트란 주 전산기와 연결하여 각 부서(과)등에서 전산망을 통해 작업 하는 컴퓨터 및 작업자를 말한다.

10. 전산망이라 함은 각종 전산 장비를 통신 회선으로 연결하여 자료를 처리, 보관하거나 전송하는 조직망을 말한다.

제3조 (보안 관리 책임자의 지정 운영)

① 각 부서(과)는 전산 기기 및 자료에 대한 보안 관리 책임자(이하 '보안 책임자'라 한다)를 1명씩 두어 운영한다.

② 전자계산소는 시스템 보안 책임자 1명을 두어 운영한다

제 2 장 전산 자료 보안

제4조 (대외비 자료)

다음 각 호의 자료를 대외비 자료로 규정하며 유출을 금지한다.

1. 교직원의 인사, 급여와 관련된 자료와 이에 준하는 자료.

2. 학생의 학적 및 성적에 관한 자료와 이에 준하는 자료.

3. 입시 자료와 이에 준하는 자료.

4. 예산 및 결산에 관한 자료와 이에 준하는 자료.

제 3 장 컴퓨터 및 보조 기억 매체 보안

제5조 (컴퓨터 및 보조 기억 매체 보안)

① 각 부서(과)의 컴퓨터에는 관리 책임자(정, 부)를 두어 운영하여야 한다.

② 각 부서(과)의 보안 책임자는 컴퓨터에 비밀 번호(PASSWORD)를 부여해서 비 인가자의 무단 사용(복사, 열람, 파괴)방지 및 바이러스와 도난 등으로부터의 피해 방지 대책을 수립한다.

제 4 장 비밀 번호(PASSWORD) 부여

제6조 (비밀 번호(PASSWORD) 부여)

① 모든 전산 시스템에 사용하는 비밀 번호는 다음의 기준으로 부여해야 한다.

1. 비밀 번호는 전화번호, 생년월일, 주민등록번호, 사번, 이름 약자 등을 사용 해서는 안 되며 유추가 힘들도록 영문과 숫자, 특수 문자 등을 조합하여 6자 위상으로 부여한다.

2. 사용자 이름과 같지 않아야 하며 반드시 비밀 번호를 부여한다.

3. 비밀 번호는 변경시 현재의 비밀 번호와 달라야 하며 분기 1회 이상 주기 적으로 변경해야 한다.

4. 비밀 번호는 타인에게 유출되지 않도록 해야 한다.

제5장 전자 우편, 전자 결재, 게시판 보안

제7조 (전자 우편, 전자 결재, 게시판 보안)

전자 문서의 수신/발신 및 게시판의 게시 등은 익명으로 할 수 없으며 대외비, 친전, 인비 등 비밀 또는 보안이 필요한 문서는 전자 우편, 전자 결재, 게시판 등을 이용할 수 없다.

제 6 장 사용자 이름(ID) 보안

제8조 (사용자 이름(ID) 보안)

① 전산 시스템을 사용하는 모든 교직원은 고유의 사용자 이름과 비밀 번호를 보유해야 하며 타인의 사용자 이름과 비밀 번호를 공동으로 사용해서는 안된다.

② 시스템 보안 책임자는 모든 사용자의 사용자 이름과 비밀 번호를 관리해야 하며 비밀 번호 부여시 제 6조에 의거 부여한다.

제 7 장 전산망 보안

제9조 (전산망 보안)

시스템 관리 책임자는 자료의 유출, 변조, 파괴 등을 방지하기 위해 내부망과 외부망의 접속을 최소한으로 제한해야 하며 비 인가자의 전산망 침입 방지 대책을 수립해야 한다.

제 8 장 주 전산기 보안

제10조 (주 전산기 보안)

① 모든 주 전산기는 비 인가자의 출입이 통제된 통제구역 안에 설치하여 관리한다.

② 주 전산기의 비밀 번호는 제 6조에 의거 부여하며 유출하여서는 안 된다.

③ 시스템 보안 책임자는 제4조의 자료 열람 및 출력을 확인할 수 있는 대책을 수립해야 한다.

④ 시스템 보안 책임자는 주 전산기에 입력되어 있는 전산망 및 전산 자료 접근 기록을 월 1회 이상 출력하여 비 인가자에 의한 무단 열람 및 출력 사실 여부를 확인 점검하여야 한다.

제 9 장 클라이언트 보안

제11조 (클라이언트 보안)

① 전산망을 이용하여 작업을 할 경우 본인의 사용자 이름과 비밀 번호를 사용한다.

② 클라이언트는 일상 업무 외에 제4조에서 규정한 자료를 열람 또는 출력할 수 없다.

제 10 장 시 설 보 안

제12조 (시설 보안)

전자계산소를 운영하는 기관의 장은 교육부 보안 업무 규정 제30조(보호 구역) 및 동 시행규칙 제42조 제 5항(보호 구역)에서 정하는 바에 의거 전자계산소를 보호 구역으로 설정하고 다음 각 호에 정하는 보호 대책을 강구하여야 한다.

1. 방재 대책 및 외부로부터의 침입 방지 대책.

2. 항시 이용하는 출입문은 한 곳으로 하고 이중실 설치

3. 출입문 보안 장치 설치 및 주야간 감시 대책

4. 보조 기억 매체를 보관할 수 있는 철제 용기 비치

5. 보조 기억 매체에 대한 안전한 지출 계획 수립

6. 전자계산소 관리 책임자 및 자료, 장비별 취급자 지정

제 11 장 보 칙

제13조 전자계산소는 원활한 업무 수행과 전산 장비 보호를 위해 전산 보안 업무 지침을 둘 수 있다.

부 칙

제1조 (시행일) 이 규정은 0000년 0월 0일부터 시행한다.

제2조 (준용규정) 이 규정에 명시되지 않은 사항은 관련 법규 및 규정을 준용한다.