

## 전산정보 관리 규정

### 제 1 장 총 칙

**제 1 조 (목적)** 이 규정은 호서대학교(이하 “본교”라 한다)의 전산정보를 이용하는 교내·외의 무단사용자에 의해 불법 유출, 파괴, 변경되는 것으로부터 안전하게 보호하며, 네트워크, 보안, 그룹웨어, 홈페이지, 정보시스템 및 데이터베이스 등을 포함한 정보운영환경과 응용 프로그램을 보다 안전하고 신뢰성 있게 운영해 본교 전산정보 이용자에게 원활한 서비스를 제공하고자 함을 그 목적으로 한다.

**제 2 조 (적용 대상 및 범위)** ① 적용 대상은 교내 전부서(부속기관 포함)로 한다.

② 본교의 전산정보자산 보호와 정보운영환경 및 응용프로그램의 운영과 제공에 관해는 별도 규정되는 경우를 제외하고는 이 규정에 따른다.

**제 3 조 (용어의 정의)** ① 전산자원이라 함은 호서대학교 내의 모든 전산관련 하드웨어와 소프트웨어를 말한다.

② 포탈시스템은 함은 호서대학교 종합정보서비스를 말한다. (개정 2024. 8. 26.)

③ 시스템 관리자라 함은 각 부서에 소속되어 시스템의 루트(root) 권한을 가지고 시스템을 운영관리하는 자를 말한다.

④ 데이터베이스 관리자라 함은 데이터베이스를 운영관리하는 자를 말한다.

⑤ 전산자료라 함은 전산장비에 의해 입력보관되어 있는 정보자료를 말하며, 백업미디어 등 저장 매체 등을 포함한다.

⑥ 보안 관리자라 함은 보안관련 시스템을 운영관리하는 자를 말한다.

⑦ 홈페이지 관리자라 함은 홈페이지 시스템을 운영관리하는 자를 말한다.

⑧ 그룹웨어 관리자라 함은 그룹웨어 시스템을 운영관리하는 자를 말한다.

⑨ 네트워크 관리자라 함은 네트워크 시스템을 운영관리하는 자를 말한다.

### 제 2 장 위 원 회

**제 4 조 (위원회)** 호서대학교의 체계적이고 효율적인 정보화 정책의 수립심의 및 관리를 위해 정보화위원회를 둔다.

**제 5 조 (구성 및 운영)** 정보화위원회의 구성 및 운영에 관한 사항은 별도의 규정으로 정한다.

### 제 3 장 보 안 관 리

**제 6 조 (기본 수칙)** ① 정보시스템 사용자는 개인별 사용자 계정 및 패스워드의 기밀을 유지해야 하며, 본래의 발급 목적으로만 사용해야 한다.

② 전산자원의 사용을 원하는 자는 허가 받은 정보시스템의 권한이 부여된 영역에 대해 본래의 목적으로만 사용할 수 있다.

③ 정보시스템 사용자는 정보시스템의 성능저하 및 보안상 위험을 초래할 수 있는 행위를 해서는 아니 된다.

④ 제3항의 규정에 언급된 행위를 한 자가 발견된 경우에는 소속 부서의 장 또는 전산정보원 정보보호팀(이하 ‘정보보호팀’이라 한다)에 이를 즉시 알려야 한다.(개정 2018. 2. 28, 2018. 12. 1, 2024. 8. 26.)

⑤ 정보자산과 연관된 저작권, 특허권 및 소프트웨어 라이선스의 사용 조건을 숙지하고

이를 준수해야 한다.

- ⑥ 학내 전산망을 신설, 변경 및 폐기하고자 하는 경우에는 정보보호팀의 사전승인을 얻어야 한다.(개정 2018. 2. 28, 2024. 8. 26.)
- ⑦ 외부 전산망에서 학내 전산망으로의 접근은 학교에서 승인한 정보시스템을 제외하고는 원칙적으로 허용하지 아니한다.
- ⑧ 모든 정보자산은 보안등급에 따라 분류 관리한다.
- ⑨ 본교는 주기적인 보안점검을 통해 학내 전산망 및 정보시스템의 안전성을 점검하고, 정보보안 정책 및 규정의 준수 여부를 평가한다. 다만, 학내 모든 사용자는 이에 적극 협조해야 한다.
- ⑩ 업무와 관련해 습득한 정보자산을 본교의 허가 없이 외부에 누출해서는 아니 된다.
- ⑪ 정보보안 사고의 책임은 원칙적으로 사용자 본인에게 있다.
- ⑫ 위 사항에 언급되지 않은 내용은 정보보안기본지침에 준한다. (개정 2024. 8. 26.)

**제 7 조 (보안등급 기준)** ① 보안등급의 분류기준은 다음의 각 호에 따라 정한다.

- 1. 정보의 중요도
- 2. 정보(시스템)의 절취 및 불법변경 시 손실 가치
- 3. 정보(시스템)의 파괴 시 복구비용
- 4. 정보의 사용권자
- ② 정보자산의 보안등급 및 사용자인가는 전항의 기준에 따라 별도로 정한다.

**제 8 조 (보안점검)** ① 각 기관에서 운영하는 시스템의 시스템관리자는 정보보호지침서에 의해 담당서버에 대해 년 1회 이상의 정기 점검과 필요시 수시 점검을 실시한다.

- ② 보안점검을 실시한 후 그 결과를 정보보안담당관에게 보고하고 지적된 사항에 대한 조치를 한다. (개정 2024. 8. 26.)

**제 9 조 (보안사고의 처리 및 조치)** 보안사고가 발생할 경우 정보보호팀은 다음 각 호의 단계에 따라 적절한 조치를 취해야 한다.(개정 2018. 2. 28, 2024. 8. 26.)

- 1. 침입자의 침입예방을 위해 침입 가능성이 있는 부분을 수시로 점검해 불법침입자의 침입을 사전에 예방한다.
- 2. 각 기관의 시스템관리자는 자신의 시스템에 비정상적인 활동이나 징후가 보이면 무단 침입자의 유무를 즉각 점검해야 한다.
- 3. 침입자가 시스템에 침투해 해킹을 하고 있을 경우 필요 조치를 즉각 취하고 정보보호팀에 보고해야 한다.(개정 2018. 2. 28, 2024. 8. 26.)
- 4. 침입자를 몰아냈거나 로그파일의 분석을 통해 침입한 흔적이 발견된 경우 즉시 보고하고, 보안 진단 도구나 체크리스트를 이용해 정보자료의 이상 유무를 점검해야 한다.
- 5. 침해사고 발생에 따른 보안사고의 처리 절차에 따라 자체적으로 복구를 수행하고, 자체적인 복구가 어려울 경우 교육부 및 관련기관에 사고 신고를 한다. (개정 2024. 8. 26.)
- 6. 인터넷 사고 중 해킹, 인터넷을 이용한 사기, 주민등록번호의 도용 등 침해 행위에 대해 침해 행위자에 대한 수사 등 법적인 처리를 고려하는 경우에는 경찰청 사이버테러대응센터에 신고해 지원을 받을 수 있다.
- 7. 공공기관의 개인정보보호에 관한 법률 및 정보통신법에 따른 법적 조치를 취한다.

**제 10 조 (보안 교육)** ① 학내 의사 결정자, 사용자 및 시스템 관리자를 대상으로 정보보안 교육을 실시한다.

- ② 보안에 대한 인식을 제고하고 사용자와 시스템 관리자의 부주의나 고의에 의한 보안사고를 최소화한다.
- ③ 보안교육은 년 1회의 정기교육과 필요에 따라 수시 교육을 실시한다.

## 제 4 장 그룹웨어 관리

**제11조 (이용자격)** ① 본교 교직원 및 기타 정보보안담당관이 필요하다고 인정한 경우 메일 계정을 사용할 수 있다.(개정 2015. 5. 1, 2018. 2. 28, 2018. 12. 12, 2024. 8. 26.)

② 사용자그룹은 교원그룹, 직원그룹, 조교그룹, 기타그룹으로 분류한다.

③ 사용자별 이용자격을 지정하여 무자격자의 열람으로 인한 피해가 없도록 하기 위해 사용자별 이용자격을 제한할 수 있다.

**제12조 (사용자 의무)** ① 메일 사용자는 다음의 사용자 의무를 준수해야 한다.

1. 계정 소유자는 개인 데이터와 그 계정으로 인해 발생한 모든 행위나 결과에 대해 책임 진다.

2. 계정 소유자는 본인 암호에 대한 비밀을 유지해야 한다.

3. 사용자는 시스템 보안에 문제가 발견되면 즉시 메일 계정 관리자에게 연락해야 한다.

4. 계정은 대여 및 판매를 할 수 없다.

② 기타 소속 부서장의 확인을 받아 정보보안담당관이 필요하다고 인정한 경우 사용 기간은 계약기간 및 신청기간으로 한다.(개정 2015. 5. 1, 2018. 2. 28, 2024. 8. 26.)

**제13조 (계정 부여)** ① 메일 계정은 1인 1계정을 원칙으로 한다.

② 기타 등록을 원하는 경우에는 메일 계정 신청서를 작성해 전산운영팀 담당자에게 직접 신청해야 한다.(개정 2018. 2. 28, 2024. 8. 26.)

**제14조 (계정 변경 및 삭제/비밀번호의 변경)** ① 계정의 변경은 전산운영팀 담당자에게 계정 변경신청서를 제출해 기존 계정삭제 후 변경할 수 있다.(개정 2018. 2. 28, 2024. 8. 26.)

② 계정의 이용자격을 상실(퇴직, 강의기간 만료 등)한 경우에는 한 달간의 유예기간 후 자동 삭제한다.

③ 비밀번호는 사용자의 책임 하에 임의로 변경할 수 있으며 주기적인 변경을 권장한다.

**제15조 (계정 용량)** ① 메일 및 정보통신시스템 이용자 계정의 기본용량은 시스템 운영상황에 따라 할당한다. (개정 2024. 8. 26.)

② 시스템 증설에 따라 변경, 보완될 수 있으며 이후의 변경된 내용은 그룹웨어게시판에 공지한다.

**제16조 (게시판 이용)** 게시판의 게시물 이용에 관한 사항은 정보화 및 정보보안 실무위원회에서 정한다. (개정 2024. 8. 26.)

## 제 5 장 종합정보서비스(포탈시스템) 관리

**제17조 (적절성 확보)** 학내 정보시스템 이용자는 정보시스템 사용에 있어 적절성을 유지해야 한다. 다만, 다음 각 호에 해당하는 경우에는 부적절한 사용으로 간주해 제재 조치를 취할 수 있다.

1. 타 사용자의 계정 및 패스워드를 허가 없이 사용한 경우

2. 타 사용자의 정당한 사용을 방해한 경우

3. 타 사용자의 자료를 허가 없이 유출하거나 읽고 쓰는 행위

4. 일반사용자가 관리자 또는 타 사용자의 패스워드를 획득하고자 해킹하는 행위

5. 내부의 중요 전산정보를 불법으로 외부에 유출한 경우

6. 외부의 불법사용자에게 계정 및 패스워드를 제공한 경우

7. 사용자 계정 및 패스워드를 상호 공유하는 행위

8. 허가된 보안등급 이상의 자료를 무단유출 하거나 읽고 쓰는 행위

9. 보안점검의 지적사항에 대해 즉각적인 시정을 취하지 않는 경우

**제18조 (사용자 제재)** ① 제 17 조에 규정된 사항에 해당할 경우에는 사용자의 계정을 회수·삭제해 정보시스템의 사용을 제한 또는 금지하며, 그에 따른 구체적 제재 사항은 정보화 위원회에서 심의한다.

② 정보시스템의 불법사용으로 학교에 해를 끼치거나 명예를 훼손시켰을 경우에는 다음 각 호의 제재 조치를 취할 수 있다.

1. “정보통신망 이용촉진 등에 관한 법률”에 의한 법적 조치
2. 정보시스템의 손해발생에 대한 손해배상 청구

**제19조 (비밀번호 관리원칙)** ① 포탈시스템에 처음 등록된 사용자의 최초 비밀번호는 생년월일 6자리로 설정되어 있으며, 사용자는 로그인 후 비밀번호를 즉시 변경해 사용토록 한다. (개정 2024. 8. 26.)

② 비밀번호를 잊어버렸을 경우에는 본인인증을 통해 초기화하여야 한다. (개정 2018. 2. 28, 2024. 8. 26.)

**제20조 (운영프로그램 관리)** ① 중요자료로 분류된 프로그램은 정보보안을 위해 사용자 계정 및 비밀번호를 설정한다.

- ② 사용자 계정 및 비밀번호는 1차 인식이 불가능한 암호화된 형태로 존재해야 한다.
- ③ 사용자 로그인 정보를 관리한다.
- ④ 소스프로그램은 종합행정서버와 별도의 백업 서버에 보관한다.

**제21조 (응용프로그램 개발)** ① 응용프로그램을 개발하거나 수정하고자 할 경우에는 다음의 각호에 의한다.

1. 실무부서가 전산운영팀에 새로운 행정용 프로그램의 개발을 요청할 경우 전산운영팀과 6개월 전에 협의해야 하며, 이미 개발한 프로그램을 수정할 경우에는 2개월 전에 협의해야 한다. (개정 2018. 2. 28, 2024. 8. 26.)
2. 전문성이 있는 업무개발 시 전산운영팀은 주무부서의 인원지원을 요청할 수 있다. (개정 2018. 2. 28, 2024. 8. 26.)
3. 개발대상업무의 규모, 소요기간, 인원 등의 부족으로 인해 전산운영팀에서 자체개발이 불가능할 경우 개발업무의 일부 또는 전부를 외부 용역으로 개발할 수 있다. (개정 2018. 2. 28, 2024. 8. 26.)
- ② 응용프로그램 개발기간에는 다음 각호의 사항을 준수해야 한다.

1. 모든 응용프로그램은 접근하는 데이터의 정보등급에 따라 해당 응용프로그램의 보안등급을 설정한다.
2. 응용프로그램의 계획서 및 설계서는 보안관리규정에 근거해 보안대책이 마련되어야 하며, 프로그램 개발 시에 이를 반영해야 한다.
3. 별도지침에 의해 중요자료로 분류된 응용프로그램은 정보보안을 위해 사용자 계정 및 패스워드를 설정해야 한다.
4. 응용프로그램에서 사용하는 사용자계정, 패스워드 및 기타 전산망 접근과 관계된 중요 정보는 소스코드로부터 분리해 1차 인식이 불가능한 암호화된 형태로 존재해야 한다.
5. 별도지침에 의해 중요자료로 분류된 응용프로그램은 개발 시 시스템 사용에 대한 로그 정보를 관리함을 원칙으로 한다.

**제22조 (응용프로그램 운영)** ① 응용프로그램 운영자는 응용프로그램 사용자 계정에 대한 패스워드 변경을 최소 6개월에 1회 이상 실시해야 한다.

- ② 응용프로그램 운영자는 시스템 사용에 대한 로그 정보를 주기적으로 분석해 자료의 불법접근 및 변조에 대한 위험성을 사전에 방지해야 한다.
- ③ 응용프로그램의 추가, 삭제, 변경은 부서장의 허가를 받은 후에 시스템 관리자에 의해 실시되어야 한다.
- ④ 운영중인 시스템에는 응용프로그램의 소스프로그램을 설치하지 않는 것을 원칙으로 한

다.

⑤ 별도지침에 의해 중요자료로 분류된 응용프로그램은 가동 전 정보보호팀의 보안검증을 받아야 한다.(개정 2018. 2. 28, 2024. 8. 26.)

## 제 6 장 유·무선 네트워크 관리

**제23조 (사용방법)** ① 호서대학교 네트워크를 사용하기 위해서는 정보보호팀으로부터 IP 주소 및 무선 ID를 발급 받아야 한다. (개정 2009. 12. 8, 2018. 2. 28, 2024. 8. 26.)

② 정보보호팀의 승인 없이 IP를 변경한 경우 이를 불법사용자로 간주해 네트워크 사용을 제한한다.(개정 2018. 2. 28, 2024. 8. 26.)

**제24조 (LAN 설치)** ① 신규설치를 요구할 경우에는 캠퍼스 전산망 설치 신청서를 첨부, 이전 설치를 요구할 경우에는 캠퍼스 전산망 설치 신청서를 첨부해 공문으로 정보보호팀에 제출한다. 단, PC 실습실 및 실험실은 구성도를 제출해야 한다.(개정 2018. 2. 28, 2024. 8. 26.)

② 행정부서 및 PC 실습실, 실험실을 제외한 모든 장소에는 1실 1포트 설치를 원칙으로 하며, 1실 2포트 이상이 필요한 경우 자체적으로 공유기를 설치할 수 있으며 공유기의 장애에 대한 처리를 요구할 수 없다.(개정 2018. 2. 28, 2024. 8. 26.)

③ 신규 및 추가 설치 신청은 수시로 접수하며 학기 시작 후 설치를 원칙으로 한다. 단, 긴급을 요하는 경우에는 이를 정보보호팀과 협의 후 처리한다.(개정 2018. 2. 28, 2024. 8. 26.)

④ IP 주소 및 무선 ID의 사용료

1. 교직원, 학생은 IP 주소 및 무선 ID를 무료로 사용할 수 있다.

2. 단, 교직원, 학생 외에 교내전산망을 사용하고자 하는 외부업체 또는 개인은 정보보호팀의 허가를 받아야 하며 지속적으로 교내전산망을 사용할 경우에는 교내 인터넷망 관리 규정에 따라 해당 IP와 무선ID의 사용료를 납부해야 한다. (신설 2009. 12. 8, 개정 2018. 2. 28, 2024. 8. 26.)

**제25조 (장애 접수)** ① 네트워크 사용 중에 문제가 발생할 경우에는 장애 내용을 신고해야 한다.

② 네트워크 장애 신고 방법은 전화 또는 장애처리 요청서에 의한다.

**제26조 (IP 주소 할당)** ① IP 주소 할당은 다음과 같다.

1. 교내에 설치된 PC에 한해 부여하고 IP 주소 여유분에 따라 신축적으로 부여하는 것을 원칙으로 한다.

2. 실험실 및 PC 실습실은 사용목적 및 요구 수량에 따라 IP 주소를 할당할 수 있다.

3. IP 주소는 소유가 아닌 대여로 사용되며 할당받은 IP 주소를 타 기관 또는 개인에게 위임하거나 판매할 수 없다.

② IP 주소 할당은 지속적으로 변경, 보완될 수 있으며 이후의 변경된 내용은 전화 또는 E-Mail로 통보한다.

**제27조 (IP 주소 신청)** IP 주소 및 무선 ID의 신청, 변경, 반납은 다음 각 호와 같다. (개정 2009. 12. 8)

1. IP 주소의 경우에는 IP 주소 신청서를 첨부해 공문으로 정보보호팀에 제출해야 한다. (개정 2018. 2. 28, 2024. 8. 26.)

2. 무선 ID의 경우에는 공지된 해당 웹서버에서 온라인으로 신청을 한다.

**제28조 (IP 주소 회수 및 반납)** ① 다음 각 호의 1에 해당할 경우에는 IP 주소를 회수 할 수 있다.

1. 정해진 절차에 따라 IP 주소를 반납하는 경우
  2. IP 주소 신청서나 증빙서류의 내용을 허위로 작성한 경우
  3. IP 주소를 무단 사용하는 경우, 기존 부여된 IP 주소를 회수 할 수 있다.
- ② IP 주소를 반납 할 경우에는 IP 주소 신청서를 첨부해 공문으로 정보보호팀에 제출해야 한다.(개정 2018. 2. 28, 2024. 8. 26.)

**제29조 (도메인 네임의 등록)** ① 도메인 네임 등록 원칙은 다음과 같다.

1. 도메인 신청은 사전 문서 접수 후 처리를 원칙으로 한다.
  2. 도메인 네임은 소유권이 아니라 인터넷을 이용하기 위한 이용권으로 간주한다.
  3. 전세계 인터넷주소 관련 권고문서(RFC-2181, RFC-2182)를 준수해야 한다.
  4. 도메인 이름은 호서대학교 교내 네트워크에 연결 확인 후 인터넷 연결과 도메인 네임 서비스가 가능한 상태에서 인터넷 서비스 이용(web, ftp, mail 등)을 목적으로 신청한다.
- ② 도메인 네임을 등록, 변경, 반납 하고자할 경우에는 도메인 네임 등록 신청서를 작성해 부서장의 결재를 득한 후 정보보호팀에 제출해야 한다.(개정 2018. 2. 28, 2024. 8. 26.)
- ③ 도메인 네임 등록 결과는 전화 또는 메일로 통보한다.

**제30조 (도메인 네임의 회수)** ① 다음 각 호의 1에 해당할 경우에는 도메인 네임을 회수할 수 있다.

1. 공문에 의해 도메인 네임을 반납하는 경우
  2. 도메인 네임 등록 신청서를 허위로 작성한 경우
  3. 도메인 네임과 관련해 변경내용을 통보하지 않은 경우
- ② 도메인 네임의 회수는 이용자에게 사전에 통보하고 3일 이내에 해당 도메인 네임을 자동 삭제하는 것을 원칙으로 하나 이용자 확인이 안 될 경우 바로 삭제한다.

## 제 7 장 전산자료 및 데이터베이스 관리

**제31조 (자료의 관리)** ① 데이터베이스 로그인 계정 관리기준은 DBMS관리자(DBA), 응용프로그램 개발자 및 사용자에 따라 권한을 차등 부여하고, 패스워드는 암호화된 형태로 존재하도록 한다.

- ② 데이터베이스의 무결성 유지를 위해 데이터베이스의 수정은 적법한 인가자에 의해서만 이루어 져야 하며, 물리적인 재해로부터의 보호를 위해 주기적으로 백업해야 한다.
- ③ 데이터베이스에 대한 모든 접근은 감사기록을 유지하되, 일반사용자의 감사기록에 대한 접근은 제한되어야 한다.
- ④ 데이터베이스 관리자(DBA)는 누가 어떤 필드, 레코드 수준에서 접근할 수 있는가를 정의해야 한다.
- ⑤ DBMS는 시스템과는 별도의 사용자 인증 기능을 수행해야 한다.
- ⑥ 데이터베이스의 데이터는 응용프로그램을 통해서만 접근한다.
- ⑦ 별도지침에 의해 중요자료로 분류된 자료 및 데이터베이스는 데이터의 접근 정보를 기록해 주기적인 점검 및 분석을 실시한다.

**제32조 (자료의 보관)** ① 별도지침에 의해 중요자료로 분류된 자료는 별도의 보호된 장소에 보관하고, 재해 및 비상시를 대비한 계획을 수립해 운영한다.

- ② 별도지침에 의해 중요자료로 분류된 자료의 이용 및 변경은 부서장의 허가과 관리책임자의 입회하에 이용 및 변경할 수 있다.

**제33조 (자료의 파기)** ① 별도지침에 의해 중요자료로 분류된 자료의 파기는 자료 보관책임자의 입회하에 담당자가 파기를 실시하고, 자료관리 대장의 파기 확인란에 입회자는 파기 확인을 한다.

- ② 자기테이프 등의 자기매체 자료의 파기는 컴퓨터를 이용해 내용을 완전히 삭제하고, 자료접근이 불가능해 내용을 지울 수 없는 자기매체의 자료는 소각 또는 용해 등의 방법으로 파기한다.
- ③ 소규모의 전산파지는 분쇄기를 이용하고, 대규모의 파지는 소각장에서 소각시키거나 분쇄업체를 통해 분쇄확인서를 발부 받아 부서장의 결재를 받는다.

## 제 8 장 PC 관 리

- 제34조 (PC의 관리)** ① PC 기동 시 OS 및 화면보호기에서 제공하는 패스워드를 설정한다.
- ② OS 및 바이러스 백신 프로그램의 최신 보안 패치를 유지해야 한다.
  - ③ 장시간 자리를 비울 때는 전원을 끈다.
  - ④ 자신의 업무에 사용하는 응용 프로그램은 시스템 보안관리자의 허락 없이 무단으로 타인에게 복사해 주어서는 아니 된다.
  - ⑤ 휴대용저장장치 등을 사용할 때 또는 데이터를 전송할 때에는 바이러스 검사를 한다.  
(개정 2024. 8. 26.)
  - ⑥ 중요한 정보는 PC내에 보관하지 아니 하며, 별도의 휴대용저장장치에 담아 물리적인 보안이 철저한 위치에 보관한다. (개정 2024. 8. 26.)
- 제35조 (바이러스 예방 및 조치)** ① 정보보호팀은 컴퓨터 바이러스 발생이 우려되는 날짜에는 미리 게시판이나 메일 등을 통해 경고 메시지 게시 등의 조치를 취한다.(개정 2018. 2. 28, 2024. 8. 26.)
- ② 윈도우 부팅 시 바이러스 체크기능을 설정해 부팅 시 바이러스를 진단할 수 있도록 한다.
  - ③ 바이러스에 의한 데이터 손상에 대비해 정기적으로 데이터 백업을 실시한다.
  - ④ 알려진 바이러스의 경우에는 해당 바이러스를 치료할 수 있는 진단 프로그램을 구비한다.
  - ⑤ OS 및 바이러스 백신 프로그램의 최신 패치가 유지되지 않을 경우 전산자원서비스를 강제적으로 중단할 수 있다.

## 제 9 장 시스템실 운영 관리

- 제36조 (시스템실 시설기준)** ① 출입구에 입실자의 식별 및 로깅 가능한 출입보안장치를 설치한다.
- ② 자동 화재경보 설비를 설치하고, 할로젠 가스 등 소화 시 장비에 피해를 주지 않는 자동 소화 설비를 설치한다.
  - ③ 정전에 대비해 별도의 전원공급 시설을 둔다.
  - ④ 온습도를 적절히 유지할 수 있는 항온항습기를 설치한다.
- 제37조 (시스템실 관리)** ① 시스템실의 운영을 담당하고 있는 정보보안담당관은 시스템실 사용 및 운영에 관한 절차 및 방법을 규정하고, 담당자들이 이를 숙지하도록 한다.(개정 2015. 5. 1, 2018. 2. 28, 2024. 8. 26.)
- ② 시스템실의 관리자는 운영일지 및 장애일지를 작성해야 한다.
  - ③ 시스템 관리자는 주기적으로 로그화일을 분석해야 하며, 시스템에 이상이 발견되었을 경우에는 보안사고 처리지침에 따라 즉시 조치를 취하고 이를 정보보호팀 및 부서장에게 보고해야 한다.(개정 2018. 2. 28, 2024. 8. 26.)
  - ④ 시스템실에는 출입자 명부를 비치하고 비인가자의 출입을 통제해야 한다.

⑤ 시스템실, 자료보관실 등은 관리책임자를 지정하고 자료 또는 장비별로 취급자를 지정 운영해야 한다.

## 제 10 장 기 타

**제38조 (교육 및 지원)** ① 다음과 같이 교직원 및 학생들의 컴퓨터 이용과 관련한 교육 및 지원을 한다.

1. 교직원들에게 종합정보시스템 사용과 컴퓨터 일반 이용과 관련한 사용자 교육을 실시한다.
2. 학생들의 컴퓨터이용능력 향상을 위한 교육을 정규교과 또는 특별과정을 통해 실시할 수 있도록 지원한다.

② 지역사회인의 컴퓨터 이용을 위한 교육을 지원할 수 있다.

**제39조 (시행세칙)** 이 규정의 운용에 필요한 세부사항은 시행세칙으로 따로 정할 수 있다.

**제40조 (준용)** 기타 이 규정에 명시되지 아니한 사항은 본교의 관계 규정 및 상위법(정보통신부, 국가정보원, 한국전산원)의 관련 항목을 적용한다.

### 부 칙

- (1) (시행일) 이 규정은 2007년 9월 11일부터 시행한다.
- (2) (경과조치) 이 규정시행과 동시에 정보관리처 규정은 폐지한다.

### 부 칙

- (1) (시행일) 이 규정은 2009년 12월 8일부터 시행한다.

### 부 칙

- (1) (경과조치) 직제 및 사무분장 규정 개정(2010.9.15 시행)에 따라 정보관리처 전산운영팀을 전산정보원 전산운영팀으로 정보관리처장을 전산정보원장으로 일괄 변경한다.

### 부 칙

- (1) (경과조치) 직제 및 사무분장 규정 개정(2012.10.23 시행)에 따라 전산정보원 전산운영팀을 경영평가실 경영정보팀으로 전산정보원장을 경영평가실장으로 일괄 변경한다.

### 부 칙

- (1) (시행일) 이 규정은 2015년 5월 1일부터 시행한다.

### 부 칙(2018. 2. 28)

- (1) (조직개편에 따른 개정) 조직개편에 따라 '경영평가실', '기획처'를 '대외협력실'로 '경영정보팀'을 '전산팀'으로 한다.

### 부 칙(2018. 12. 12)

- (1) (조직개편에 따른 개정) 조직개편에 따라 '대외협력실'를 '기획처'로 한다.

### 부 칙(2024. 8. 26)

이 규정은 공포일로 부터 시행한다.



(별지서식 1)

◇ 메일계정 신청서 ◇

소속		
직위		
성명	한글	
	영문	
전화번호		
교번		
ID		(영문소문자이용, 첫글자영문, 숫자사용가능, 8자 이내 )
Password		(영문/숫자 조합 6자 이상)
ID 사용목적		

200 . . . . .

소 속 :                      대학                      학부(과)

신청인 :                      (인)

(별지서식 2)

◇ 전산망 신청서 ◇

사 용 자 정 보		
소속	학부(과)                      연구실(실험실)	
설치 장소 (건물명/호실/호실명)		
연락처	office	
	H.P	
신 청 정 보		
IP Address	수량	
	현재 보유 IP Address 예) 10.10.10.1	
랜 포트 (1실에 1Port 원칙)		
랜선 (길이포함)		
기타 신청사항		

20 . . .

신청자 :

(인)

(별지서식 3)

## ◇ 도메인네임(방화벽) 등록 신청서 ◇

구 분			대학	학부(과)	연구실(실험실)
용 도					
OS 종류					
설치 프로그램					
사용 PORT(방화벽등록)					
도메인이름	신청 ( )		IP Address (예 : 10.10.10.1)	도메인 이름 (예 : bbb.hoseo.ac.kr)	
	반납 ( )				
	변경( )	기존			
		변경			
설치장소 (건물명/호실/호실명)					
관리자			소속 :	직책 :	이름 :
관리자 연락처			office :	Email :	
			H.P :		
서비스			(※ 서비스 open에 따른 모든 행위나 결과에 책임짐)		

20 . . .

소 속 : 대학 학부(과)

신청인 : (인)