정보보안 관리규정

□ 2011. 10. 1 제정

제1장 총 칙

제1조(목적) 이 규정은 수원대학교(이하 '본교'라 한다) 정보자산이 불법 유출·파괴·변경되는 것으로부터 안전하게 보호하며, 네트워크 및 각종 정보시스템등 정보운영 환경과 응용프로그램을 보다 안전하고 신뢰성 있게 운영하여 본교 전산망 사용자에게 원활한 서비스를 제공하고자 함을 그 목적으로 한다.

제2조(적용 대상과 범위 및 의무와 책임)

①본교 시스템의 정보보안을 담당하는 부서는 정보전산원으로 하며 정보보안에 관한 업무를 진행하는 정보보안담당관은 정보전산원장으로 한다.

② 적용 대상은 교내 전산자원을 사용하는 모든 정보시스템 및 구성원으로 한다.

③ 본교의 정보자산 보호와 정보운영환경 및 응용프로그램의 운영과 제공에 관하여는 따로 규정되는 경우를 제외하고는 이 규정에 따른다.

④ 본교의 전산자원을 사용하는 모든 구성원은 정보보호에 대한 의무 및 정보보안·관리규정을 준수할 의무가 있으며, 본 규정을 준수하지 않아 발생한 사고의 책임은 원칙적으로 사용자 본인에게 있다

제3조(용어의 정의)

① "전산망"이라 함은 각종 정보시스템을 통신회선으로 연결하여 자료를 처리·보관하거나 전송하는 조직망을 말한다.

② "정보시스템"이라 함은 PC, 노트북 PC, PDA, 서버시스템, 네트워크시스템, 정보 보호시스템 등 정보통신에 이용되는 컴퓨터 기능을 보유한 모든 시스템을 말한다.

③ "시스템관리자"라 함은 각 부서에 소속되어 시스템의 루트(root) 권한을 가지고 시스템을 운영·관리하는 자를 말한다.

④ "데이터베이스관리자"라 함은 데이터베이스를 운영·관리하는 자를 말한다.

⑤ "전산자료"라 함은 전산장비에 의해 입력·보관되어 있는 정보자료를 말하며, 백업미디어 등 저장매체를 포함한다.

⑥ "정보보안" 또는 "정보보호"라 함은 정보통신 수단으로 수집·가공·저장·검색·송수신 되는 정보의 유출·위변조·훼손 등을 방지하거나 정보통신망을 보호하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위를 말한다.

⑦ "시스템실"이라 함은 서버·PC 등 전산장비와 스위치·교환기·라우터 등 통신 및 전송장비 등이 설치 운용되는 장소를 말하며, 전산자료 보관실 등을 말한다.

⑧ '개인정보'라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 등의 사항에 의하여 당해 개인을 식별 할 수 있는 정보(당해 정보만으로는 특정개인을 식별 할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다.

⑨ "침해사고"라 함은 해킹, 컴퓨터 바이러스, 악성코드, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등에 의하여 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행

위로 인하여 발생한 사태를 말한다.

제2장 위원회

제4조(구성)

① 체계적·효율적인 보안정책 수립·심의 및 관리를 위하여 정보보안심사위원회(이하 '위원회'라 한다)를 둔다.

② 위원회는 위원장을 포함하여 5인 내외의 위원으로 구성한다.

③ 위원은 정보전산원장 및 본부부서의 각 처·실장을 당연직으로 한다.

④ 위원장은 정보전산원장이 겸임한다.

⑤ 위원장을 포함한 각 위원의 임기는 보직재임기간으로 한다.

제5조(기능) 이 위원회는 제1조의 목적을 달성하기 위하여 다음 각 호의 사항을 심의·결정한다.

1. 정보보안정책 심의와 학내 정보보안의 총 관장
2. 정보보호 정책 및 총괄 계획 심의
3. 정보보안사고 처리의 책임을 심의·결정
4. 정보보안교육 및 정보보안준수 사항 감사
5. 기타 정보보안관련 제반업무의 총괄

제6조(실무협의회 구성과 역할)

① 위원회 산하에 부서 간 개인정보보호에 관한 업무협조를 위하여 '정보보안실무협의회'(이하 "협의회"라 한다)를 다음 각 호와 같이 둔다.

1. 협의회는 의장을 포함하여 10인 내외의 위원으로 구성한다.
2. 위원은 개인정보를 취급하는 관련 주요부서 업무담당자나 권한 위임자를 당연직으로 하고, 그 밖에 정보전산원장이 추천한 관련분야 약간 명을 위원으로포함 할 수 있다.
3. 의장은 정보전산원장이 겸임한다.
4. 의장을 포함한 각 위원의 임기는 보직재임기간 및 해당업무기간으로 한다.
5. 본교의 개인정보관리책임관은 따로 정하지 않는 한 의장이 겸임한다.

② 협의회는 각 부서의 담당자들이 업무를 수행하는데 있어 개인정보를 침해하는 일이 없도록 하기 위해 다음 각 호의 사항을 협의하여 결정된 사항을 정보보안심사위원회에 상정한다.

1. 각 부서 업무내역 중에 개인정보보호 시행세칙 작성
2. 시행세칙의 이행 및 관리감독
3. 기타 위 각 호에 부수되는 제반 사항

③ 위원회는 정보보안 규정의 준수여부를 연 1회 이상 자체 점검한다.

제3장 보 안

제7조(기본 수칙)

① 정보시스템 사용자는 개인별 사용자 계정 및 패스워드의 기밀을 유지해야 하며, 본래의 발급 목적으로만 사용하여야 한다. 패스워드는 영문자, 숫자, 특수문자를 혼용하여 8자리 이상으로 작성함을 원칙으로 한다.

② 교·직원 및 학생은 허가받은 정보시스템의 권한이 부여된 영역에 대하여 본래의

목적으로만 사용할 수 있다.

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

④ ③항의 규정에 언급된 행위를 한 자가 발견된 경우에는 소속부서의 장 또는 정보보안 담당부서에게 알려야 한다.

⑤ 정보자산과 연관된 저작권·특허권 및 소프트웨어 라이선스의 사용 조건을 숙지하고 이를 준수하여야 한다. 또한 교내에서는 구매증서가 있는 합법적인 소프트웨어만 사용 할 수 있다. 또한 불법적인 소프트웨어의 사용을 방지하기 위하여 각 부서의 장은 연간 1회 이상 부서내의 시스템을 점검한다.

⑥ 학내 전산망을 신설·변경 및 폐기하고자 하는 경우에는 정보보안담당부서의 사전 승인을 얻어야 한다.

⑦ 외부 전산망에서 학내 전산망으로의 접근은 학교에서 승인한 정보시스템을 제외하고는 원칙적으로 허용하지 아니 한다.

⑧ 모든 정보자산은 보안등급에 따라 분류·관리한다.

⑨ 본교는 주기적인 보안점검을 통해 학내 전산망 및 정보시스템의 안전성을 점검하고, 정보보안정책 및 규정의 준수 여부를 평가하며 학내 모든 사용자는 이에 적극 협조하여야 한다.

⑩ 업무와 관련해 습득한 정보자산을 본교의 허가 없이 외부에 유출해서는 아니 된다.

⑪ 교내 각종 민감 정보 및 주요 연구 자료의 교외이관 시 인터넷 메일과 같은 사적 E-Mail을 사용할 수 없다.

⑫ 정보보안 사고를 예방하기 위한 목적으로 학교의 승인을 득한 정보보안시스템 및 정보보안 활동은 즉시 시행 할 수 있다.

⑬ 휴대용 기기나 휴대용 저장매체는 각 부서장의 사전승인에 의하여 사용을 하고, 사용 후 폐기 및 재사용 여부를 반드시 승인 받는다.

제8조(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 정보자산을 보유한 부서의 장이 별도로 정한다.

③ 정보보안시스템은 국가정보원 CC인증을 받은 제품을 사용하며 업체로부터 CC인증 증명서를 제출 받는다.

④ 보안장비의 타 용도 사용을 금한다.

제9조(보안 점검)

① 정보보안담당부서는 교내 주요서버 및 각 연구실의 서버에 대해 필요시 수시 점검을 실시 할 수 있으며 다음 각 호의 단계를 따른다.

1. 보안점검 대상 및 분야를 해당 부서에 통보한다.
2. 해당 부서에서는 보안점검에 필요한 자료 및 제반 요청사항을 준비하여 보안점검에 대비 한다.
3. 보안점검을 실시한 후 그 결과를 위원회 위원장에게 보고한 후 해당 부서에 통보한다.
4. 해당 부서에서는 지적사항을 즉각 시정하고 그 결과를 위원회 위원장에게 보고한

다.

5. 정보보안담당부서는 필요시 각 부서의 보안점검 지적사항에 대한 시정 여부를 확인할 수 있다.

② 홈페이지 침해사고 및 개인정보노출사고 등을 예방 및 대처하기 위해 다음 각 호에 따라 정보보안 담당부서는 보안점검을 실시 또는 요구할 수 있다.

1. 보안점검 대상은 본교 모든 홈페이지로 한다.

2. 보안점검은 홈페이지를 구축 할 때와 점검사유가 발생할 때 실시한다.

3. 보안점검은 원칙적으로 정보보안담당부서에서 시행하나, 사전 협의된 경우 구축·관리 주최에서 자체적으로 보안점검을 진행하고, 그 점검결과를 정보보안담당부서에 통보할 수 있다.

4. 위 ①항에 따라 보안점검을 실시한다.

제10조(침해사고의 처리) 침해사고가 발생할 경우 정보보안전담팀은 다음 각 호의 단계에 따라 적절한 조치를 취하여야 한다.

1. 침입자의 침입예방을 위하여 침입 가능성이 있는 부분을 수시로 점검하여 불법침입자의 침입을 사전에 예방한다.

2. 시스템관리자는 자신의 시스템에 비정상적인 활동이나 징후가 보이면 무단 침입자의 유무를 즉각 점검해야 한다.

3. 침입자가 현재 시스템에 침투해 해킹을 하고 있을 경우 필요한 조치를 즉각 취하고 보고하여야 한다.

4. 침입자를 몰아냈거나 로그파일의 분석을 통해 침입한 흔적이 발견된 경우 즉시 보고하고, 보안진단 도구나 체크리스트를 이용하여 정보자료의 이상 유무를 점검하여야 한다.

제11조(보안 교육)

① 학내 의사결정자·사용자 및 시스템 관리자를 대상으로 연 1회 이상 정보보안 교육을 실시한다.

② 보안에 대한 인식을 제고하고 사용자와 시스템 관리자의 부주의나 고의에 의한 보안 사고를 최소화 한다.

③ 보안교육은 주제별, 대상별 필요에 따라 수시/정기교육을 실시 할 수 있다.

제4장 정보시스템 보안 지침

제12조(사용자 정의) 정보시스템을 사용할 수 있는 자는 다음 각 호와 같다.

1. 본교 교원·직원·재학생 및 졸업생

2. 연구소 및 부속기관의 장이 사용을 인정한 자

3. 단 외부용역업체의 시스템 설치 및 변경 시에는 내부담당자의 통제 하에 작업해야 하며, 내부정보시스템을 사용하는 경우 최소권한 부여 및 사용 후 권한회수를 원칙으로 한다.

제13조(적절성 확보) 학내 정보시스템 이용자는 정보시스템 사용에 있어 적절성을 유지하여야 한다. 다만, 다음 각 호에 해당하는 경우에는 부적절한 사용으로 간주하여 제재조치를 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 “root” 패스워드 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. 시스템관리자가 특별한 사유 없이 “root” 패스워드를 일반사용자와 공유한 경우
9. 허가된 보안등급 이상의 자료를 무단유출 하거나 읽고 쓰는 행위
10. 인터넷을 통해 자살 사이트나 음란 사이트 등 반사회적인 유해사이트에 접속·개설·열람하는 경우
11. 보안점검의 지적사항에 대해 즉각적인 시정을 취하지 않는 경우
12. 정보시스템을 이용한 개인정보 침해사고(불법유출, 훼손, 갈취, 불법열람 등)가 발생한 경우
13. PC 또는 개인서버의 관리 소홀로 해킹 경유지로 이용되거나 네트워크에 과다 트래픽을 일으켜서 타인의 업무에 방해가 되는 경우

제14조(사용자 제재)

① 제13조에 해당할 경우에는 사용자의 계정을 회수·삭제 또는 정보시스템의 사용을 제한·금지하며, 필요시 그에 따른 구체적 제재 사항은 위원회에서 심의·결정한다.

② 정보시스템 사용과 관련하여 학교에 해를 끼치거나 명예를 훼손시켰을 경우에는 다음 각 호의 제재 조치를 취할 수 있다.

1. ‘정보통신망 이용촉진 및 정보보호 등에 관한법률, 부정경쟁방지 및 영업비밀 보호에 관한법률’ 등 관련 법령에 의한 법적조치
2. 학칙 관련 규정에 따른 징계 조치
3. 정보시스템의 손해발생에 대한 손해배상 청구

제5장 네트워크 보안 지침

제15조(네트워크 관리)

① 캠퍼스통신망 관리자는 사용자가 본 규정을 위반하는 경우에 통신망 보호를 위해 설비를 단절, 사용금지 시킬 수 있으며 이에 따른 불이익 및 손해는 사용자에 있다.

② 랜 포트는 총장발령 전임 교직원에게는 1인 1개로 설치하되 정보전산원장이 필요하다고 인정하는 경우 추가 설치를 한다.

③ 운영부서의 관리자는 네트워크 신규설치 및 변경 시 정보보안담당자에게 변경정보를 통보해야 한다.

④ 네트워크 IP ADDRESS는 사용자가 임의로 변경할 수 없다.

⑤ 네트워크 장비의 패스워드는 제21조에 규정된 계정관리에 따른다.

⑥ 인터넷을 이용한 모든 외부로부터의 접근은 원칙적으로 금지한다. 단, 다음과 같은 적절한 사유와 승인절차를 거친 경우에 한해 허용 할 수도 있다.

1. 연구를 목적으로 원격접속이 필요한 경우
2. 정보시스템과 관련한 원격 업무지원이 필요한 경우

⑦ 정보시스템에 대한 원격접속을 허용할 경우 다음을 준수하여야 한다.

1. 원격접속 작업자는 보안서약서를 제출해야 한다.
2. 원격접속 작업자에게는 작업에 필요한 최소 권한만을 부여한다.
3. 원격접속 작업자는 해당 시스템관리자 또는 업무담당자의 관리·감독 하에서만

접근하게 한다.

4. 원격접속은 업무시간 범위에서만 허용한다.

5. DB서버와 같은 보안등급 최상위 정보시스템은 원격접속 대상에서 제외한다.

⑧ 일정횟수 접속실패 시 접속을 차단하고 관련 정보를 로그에 기록한다.

⑨ 보안상 취약한 무선 통신망의 신설 또는 증설은 억제한다.

제16조(네트워크의 보호)

① 정보보안담당부서는 본교에 유해하거나 불필요하다고 판단되는 웹사이트 접속을 통제 할 수 있다.

② 원격 사용자의 공중망 네트워크를 통한 접속은 인증 시스템 또는 방화벽 등의 보안 시스템에 의해 통제 할 수 있다.

③ 신뢰할 수 없는 정보시스템 및 서버로의 접속을 보호하기 위해 네트워크 정책을 설정하여 통제 할 수 있다.

④ 네트워크 보안 담당자는 의심스러운 활동에 대해서는 방화벽, 침입탐지시스템(IDS) 및 기타 보안 시스템의 로그를 분석하여 해당 내용을 확인하여야 하며 필요시 부서장에게 보고해야 한다.

⑤ 교내 네트워크 사용 시 적법한 사용자임을 인증 받아야 하며, 인증된 사용자의 유선·무선 통신 단말은 적정 무결성 수준 및 보안수준을 점검하여 본교 정보보안기대 수준에 미달 시 네트워크 사용을 제한 할 수 있다.

⑥ 무선통신 네트워크를 구축 시 무선중계기(AP)의 전파범위 조정, 사용자 인증, 패킷 암호화 등 보안대책을 적용하여 구축 한다.

제17조(네트워크 사용자 의무)

① 캠퍼스통신망을 이용하는 모든 정보 및 자원은 상업용으로 이용될 수 없다.

② 캠퍼스통신망 설비는 파손해서는 안 된다. 파손 시에는 사용자 부담으로 사고 발생 후 1개월 이내에 원상 복구시켜야 한다.

③ 사용자는 설비의 이동, 변경, 해체 시에는 반드시 정보전산원장의 승인을 받아야 한다.

④ 사용자는 캠퍼스통신망의 원활한 운영을 위하여 다음 각 호에 해당하는 행위를 하여서는 안 된다.

1. 캠퍼스통신망에 불법 접근 및 캠퍼스통신망에 피해를 입히는 행위
2. 캠퍼스통신망을 통해 외부 인터넷에 피해를 입히는 행위
3. 바이러스, 웜, 트로이 목마, 백도어 프로그램 등 각종 악성 코드의 감염으로 네트워크 속도 저하 및 다른 사용자에게 피해를 입히는 행위
4. 기타 통신망의 효율적인 운영에 방해되는 행위.

⑤ 캠퍼스통신망의 운영에 방해되는 사용자 또는 PC는 일정기간 통신망 사용을 제한할 수 있다.

제18조(본교 홈페이지 관리자 및 사용자 의무)

① 본교 홈페이지상의 자유게시판, 묻고답하기, 자료실 등에 적용한다.

② 답변을 요하는 게시물의 경우 관련 부서에서는 48시간 내에 성실하게 답변하여야 하며, 답변을 요하지 않는 게시물의 경우 답변을 하지 않는 것을 원칙으로 한다. ③항의 삭제 규정에 저촉되지 않는 게시물의 경우 무삭제를 원칙으로 한다.

③ 본교 홈페이지의 원활한 운영을 위하여 사용자는 다음 각 호에 해당하는 행위를 하여서는 안 되며, 관련된 게시물은 발견 즉시 통보 없이 삭제한다.

1. 각 게시판의 관리 운영 목적에 적합하지 않은 게시물
2. 게시판 운영 방해를 목적으로 한 의미 없는 게시물

3. 심한 욕설, 비속어, 사생활 침해, 명예훼손 등 민주적 기본 질서에 위배되는 게시물
4. 학내 질서를 어지럽히는 선전. 선동성 게시물
5. 음란, 저속, 선정, 성희롱 등 특정 성(性)을 비하하거나 성적 수치심을 조장하는 게시물
6. 특정 대학교나 학과를 비방하거나 우열을 비교하며 대학교간 서열화를 조장하는 게시물
7. 광고, 매매와 같은 상업적인 게시물
8. 타인의 신상정보를 도용하여 게재한 게시물
9. 삭제된 게시물에 대응하는 게시물

제6장 서버 보안 지침

제19조(운영 및 관리)

① 신규 임용된 교원과 직원의 계정 등록요구 시 시스템 관리자에게 사용목적・사용기간 및 연락처 등을 제출하도록 한다.
② 휴직자의 계정은 휴직기간동안 잠정 폐쇄를 원칙으로 한다.
③ 퇴직자는 사직원 제출 시 사용자 계정을 반납하도록 한다.
④ 시스템 관리자는 최소 월 단위로 사용자의 패스워드를 체크해 취약한 패스워드가 발견될 경우 당사자에게 통보하여 변경을 요구할 수 있다.
⑤ 취약한 패스워드를 사용한 계정에 대해서는 경고를 하되, 2회 이상의 경고를 받고도 변경하지 않을 경우에는 1개월 동안 계정을 폐쇄할 수 있다.
⑥ 시스템 개발 및 운영부서의 장은 응용프로그램 개발계획 단계에서 보안정책에 근거한 응용프로그램 개발을 지시하고, 이를 위반할 경우에는 개발을 중지시킬 수 있다.
⑦ 슈퍼유저의 권한은 정보보안업무 담당자/시스템 관리자로 제한하되 정기적으로 권한 사용내역을 부서장에게 보고토록 한다.
⑧ 장애복구나 점검을 위해 루트 권한을 위임할 경우에는 시스템 관리자 입회하에 작업을 실시하고, 작업종료 후 루트 계정과 패스워드를 변경한다.
⑨ 백업지침은 별도로 정하며, 반드시 지침에 따라 주기적인 백업을 실시한다.
⑩ 각 부서는 백업 미디어별로 적절한 사용연수를 정하여 노후된 백업미디어에 대해서는 사용하지 아니 한다.

제20조(보안관리)

① 전체 시스템에 대한 보안 관리는 정보보안전담팀에서 실시한다.
② 개별 서버에 대한 보안 관리는 각 서버의 관리자가 담당한다.

제21조(계정관리)

① 사용자 계정 분류는 그 사용목적에 따라 분류하고 그 기준은 따로 정한다.
② 사용자별 또는 그룹별로 접근권한을 부여한다.
③ 외부 사용자의 계정은 유효기간을 설정한다.
④ 특별한 사유 없이 1학기 이상 사용하지 않는 계정은 학기 시작 일주일 이내에 말소한다.
⑤ 패스워드가 없는 계정은 사용을 금지한다.
⑥ 일정회수 접속 실패시 사용을 금지한다.
⑦ 슈퍼유저는 Console 및 특정 단말에서만 접속을 허용한다.

⑧ 사용자 계정절차의 등록・변경 및 폐기는 다음을 따른다.

1. 사용자 계정은 사용자 등록이나 변경 또는 폐기 신청서를 작성한 후에 시스템 관리자에게 통보하되, 외부사용자는 반드시 사용기간 및 목적 등의 사유를 명확히 해야 한다.

2. 시스템관리자는 내용을 검토한 후에 사용자 계정을 등록이나 변경 또는 폐기하고 사용자에게 그 사실을 통보한다.

3. 사용자 계정을 등록하거나 변경 또는 폐기할 경우에 일반적인 사항은 월 단위로 부서장에게 사후 보고한다. 다만, 특별한 상황이 발생할 경우에 한하여 부서장의 허가를 받은 후에 작업을 실시한다.

제7장 전산자료 및 데이터베이스 보안 지침

제22조(자료의 관리)

① 데이터베이스 로그인 계정 관리기준은 데이터베이스 관리자(DBA)・응용프로그램 개발자 및 사용자에 따라 권한을 차등 부여하고, 패스워드는 암호화된 형태로 존재하도록 한다.

② 데이터베이스의 무결성 유지를 위해 데이터베이스의 수정은 적법한 인가자에 의해서만 이루어져야 하며, 물리적인 재해로부터의 보호를 위해 주기적으로 백업하여야 한다.

③ 데이터베이스에 대한 모든 접근은 감사기록을 유지하되, 일반사용자의 감사기록에 대한 접근은 제한해야 한다.

④ 데이터베이스 관리자(DBA)는 누가 어떤 필드, 레코드 수준에서 접근할 수 있는가를 정의해야 한다.

⑤ DBMS는 시스템과는 별도의 사용자 인증기능을 수행해야 한다.

⑥ 데이터베이스의 데이터는 응용프로그램을 통해서만 접근한다.

⑦ 별도지침에 의해 중요자료로 분류된 자료 및 데이터베이스는 데이터의 접근정보를 기록하여 주기적인 점검 및 분석을 실시한다.

제23조(자료의 보관)

① 별도지침에 의해 중요자료로 분류된 자료는 별도의 보호된 장소에 보관하고, 재해 및 비상시에 대비해 소산계획을 수립하여 운영한다.

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

제24조(자료의 파기)

① 별도지침에 의해 중요자료로 분류된 자료의 파기는 자료보관책임자의 입회하에 담당자가 파기를 실시하고, 자료관리 대장의 파기 확인란에 입회자는 파기확인을 한다.

② 자기테이프 등의 자기매체 자료의 파기는 컴퓨터를 이용하여 내용을 완전히 삭제하고, 자료접근이 불가능해 내용을 지울 수 없는 자기매체의 자료는 소각 또는 용해 등의 방법으로 파기한다.

③ 소규모의 전산파지는 분쇄기를 이용하고 대규모의 파지는 보안담당자 입회하에 소각장에서 소각 시킨다

제8장 응용프로그램 보안 지침

제25조(응용프로그램 개발)

① 모든 응용프로그램은 접근하는 데이터의 정보등급에 따라 해당 응용프로그램의 보안등급을 설정한다.

② 응용프로그램의 계획서 및 설계서는 보안관리 규정에 근거하여 보안대책이 마련되어야 하며, 프로그램 개발 시에 이를 반영해야 한다.

③ 별도지침에 의해 중요자료로 분류된 응용프로그램은 정보보안을 위해 사용자계정 및 패스워드를 설정해야 한다.

④ 응용프로그램에서 사용하는 사용자계정·패스워드 및 기타 전산망 접근과 관계된 중요정보는 소스코드로부터 분리하여 1차 인식이 불가한 암호화된 형태로 존재해야 한다.

⑤ 별도지침에 의해 중요자료로 분류된 응용프로그램은 개발 시 시스템 사용에 대한 로그 정보를 관리함을 원칙으로 한다.

⑥ 패스워드 설계 및 구현

1. 패스워드는 문자/숫자를 조합하여 8자리 이상으로 한다.
2. 직전의 패스워드로는 변경이 허용되지 않아야 한다.
3. 계정의 패스워드 입력 제한의 횟수를 정의하고, 정의된 횟수 실패 시 자동적으로 연결이 해제 (disconnected) 되도록 한다.
4. 사용자 패스워드는 암호화하여 조회가 불가하도록 해야 한다.
5. 사용자 비밀번호는 화면 및 출력물에 노출되어서는 안 된다.

⑦ C/S, WEB 로그온 및 로그오프 설계 및 구현

(1) 로그인 후 일정시간 미사용 시 자동 로그오프를 적용하거나 화면 잠금 기능을 적용한다.

(2) 시스템 접속 시 최종사용시각을 표시한다.

(3) 일정기간 시스템 미사용 시 미 사용자의 로그인을 제한한다.

⑧ 인터넷/인트라넷 설계 및 구현

(1) 디렉터리 리스팅을 금한다.

(2) 인증이 필요한 경우임에도 인증과정 없이 중간페이지로 직접 접속하는 것을 금지한다.

(3) 사용자의 주요 정보는 암호화하여 전송한다.

⑨ 로깅/감사기능 설계 및 구현

(1) 시스템 개발 시 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 등을 시스템에 자동 기록되도록 하고 그 기록을 1년 이상 보관하여야 한다.

⑩ 응용프로그램 보안 확인 및 보고

응용프로그램 개발/유지보수 책임자는 응용프로그램 보안관련 설계 및 구현 사항에 대해서 각각 설계단계 종료 후 및 구현 종료 후 확인하며 확인결과를 응용프로그램 보안설계/구현표를 작성하여 IT보안 관리자에게 제출한다.

⑪ 응용프로그램의 외주 개발 시

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

1. 시스템 개발 시 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.

⑫ 개발 담당자 계정 부여 및 관리

1. 각 개발 담당자별로 사용자 계정을 부여하는 것을 원칙으로 한다.
2. 계정 공통 사용 시 그 상황 및 내역을 기록한다.

⑬ 개발 담당자 계정 부여 절차

담당자의 계정 부여 내역은 IT보안 관리자가 주기적으로 확인한다.

⑭ 개발 담당자 접근권한

1. 개발 담당자의 접근권한은 데이터 관리지침에 의해 현황을 정리한다.
2. 개발 담당자의 담당업무 변경, 전출, 퇴직 등의 사유 발생 시 기존에 허용했던 전산자원의 접근권한을 제한하도록 한다.
3. 중요하고 민감한 응용프로그램 및 라이브러리는 개발 보안담당자가 지정하고 보안 관리자가 확인하며, 이에 대한 내역을 기록하며 접근권한을 최소한으로 필요성이 있는 경우에만 부여한다.

⑮ 개발 담당자 접근통제

1. 개발 담당자는 다음의 구역에 원칙적으로 접근을 금하며 부득이한 경우 허가신청서를 작성한 후에 출입한다.
   - 컴퓨터실 출입 통제
   - 운영체제 관련 다큐멘테이션이 보관된 장소 출입 통제
2. 개발 담당자는 다음과 같은 사항에 논리적인 접근을 가능한 금하고 금하기 어려운 경우 허가를 득하며 로깅을 통해 접근내역을 기록한다.
   - 담당업무이외의 응용프로그램 및 다큐멘테이션 접근
   - 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 디렉터리 권한이 할당되어 타 개발 담당자 그룹에 접근하거나 OS의 파일들을 조작하지 않도록 한다.

⑯ 응용프로그램 및 데이터 처리 단말의 운영

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

⑰ 개발업무 보안점검

1. 개발 보안담당자는 주기적으로 개발업무와 관련된 보안점검을 실시하고 개발업무 보안점검 결과서에 기록한다.
2. 개발 보안담당자와 IT보안 관리자는 보안점검의 적정성을 확인한다.

제26조(응용프로그램 운영)

① 응용프로그램 운영자는 응용프로그램 사용자 계정에 대한패스워드 변경을 최소 6개월에 1회 이상 실시해야 한다.

② 응용프로그램 운영자는 시스템 사용에 대한 로그 정보를 주기적으로 분석하여 자료의 불법접근 및 변조에 대한 위험성을 사전에 방지해야 한다.

③ 응용프로그램의 버전관리는 소스프로그램과 실행프로그램의 버전이 일관성을 유지하도록 한다.

④ 개발된 응용프로그램의 복제는 시스템관리자의 사전양해와 입회하에 실시해야 한다.

⑤ 응용프로그램의 추가·삭제 또는 변경은 부서장의 허가를 받은 후에 시스템 관리자에 의해 실시되어야 한다.

⑥ 운영 중인 시스템에는 응용프로그램의 소스프로그램을 설치하지 않는 것을 원칙으로 한다.

⑦ 별도지침에 의해 중요자료로 분류된 응용프로그램은 가동 전 정보보호전담팀의 보안검증을 받아야 한다.

⑧ 계정 등록 및 관리

계정 등록을 원하는 사용자는 다음의 사항을 준수한다.

1. 사용자계정 등록은 사용자가 포탈시스템에서 본인사항을 확인 후 등록 요청에 의해 등록이 완료된다.
2. 사용자 삭제 또는 권한 변경 사유가 발생한 경우, 삭제 또는 변경 신청서를 작성하여 통보 하여야 한다.
3. 계정은 각 사용자별로 부여한다. 부서별 공동 사용자 계정은 생성이 금지된다.
4. 시스템 관리 담당자는 월간 단위로 사용자 등록 및 변경 현황을 유지 한다.
5. 사용자 계정의 재확인은 다음사항에 대하여 실시한다.
   - 퇴사여부, 업무 필요성 여부
   - 마지막 사용일자가 60일을 넘겼을 경우
6. 패스워드가 없거나 패스워드가 계정이름과 동일한 계정을 허용해서는 안 된다.
7. 하나의 로그인 아이디는 한번만 로그인 할 수 있다.

⑨ 계정 정지

1. 틀린 패스워드의 반복 시 계정을 정지시킨다.
2. IT보안 관리자에게 정지계정의 현황을 보고한다.

⑩ 정지된 계정의 재사용

다시 사용하는 사용자는 새로운 패스워드를 부여 받고, 최초로 로그인을 할 때, 즉시 패스워드를 변경하도록 해야 한다.

⑪ 계정의 폐쇄

1. 계정이 폐쇄 되는 사유가 발생 시에는 사유가 발생하는 즉시 삭제하도록 한다.
2. 계정의 폐쇄는 아래의 사유에 따른다.
   - 사용자가 퇴직하는 경우
   - 3개월 이상 미사용 계정

⑫ 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. IT보안 관리자는 응용프로그램 보안 설계대로 패스워드 기능이 작동하는지 확인한다.

4. 패스워드는 3개월마다 변경해야 한다.

제9장 PC 보안 지침

제27조(PC의 관리)

① PC 기동 시 CMOS에서 제공하는 패스워드를 설정한다.

② 화면 보호기를 작동시켜야 하며 패스워드를 설정한다.

③ 장시간 자리를 비울 때는 전원을 끈다.

④ 자신의 업무에 사용하는 응용 프로그램은 시스템 보안 관리 허락 없이 무단으로 타인에게 복사해 주어서는 아니 된다.

⑤ 휴대용 저장매체 사용 또는 데이터를 전송할 때에는 바이러스 검사를 한다.

⑥ 중요한 정보는 PC내에 보관하지 아니 하며, 별도의 저장매체에 담아 물리적인 보안이 철저한 위치에 보관한다.

제28조(바이러스 및 침해사고 예방조치)

① 정보보안담당부서는 컴퓨터 바이러스, 웜 발생으로 심각한 피해가 우려되는 경우 게시판이나 메일 등을 통해 경고 메시지 게시 등의 조치를 취한다.

② 교내 전산망을 통해 전산자원을 사용하는 모든 PC는 웜, 바이러스 감염 및 침해사고를 예방하기 위해 아래와 같이 조치해야하며, 정보보안 담당부서는 필요하다고 판단될 경우 이를 강제할 수 있다.

1. PMS 클라이언트를 의무적으로 설치하여 윈도우 업데이트를 항상 최신으로 유지.
2. 본교 정보보호담당부서에서 인증한 백신프로그램을 의무적으로 설치하고, 실시간 감시기능 및 자동 업데이트 설정.
3. 업무와 무관한 비인가 프로그램(P2P, 웹하드, 메신저 등) 설치 금지.
4. 불필요한 Active-X 등 보안에 취약한 프로그램 설치 금지.
5. 인가받지 않은 휴대용 저장매체(USB, 이동형 하드디스크, 메모리카드 등) 사용금지.
6. 업무상 불필요한 응용프로그램 설치 금지 및 공유폴더 삭제.
7. “내 PC 지키미” 등을 활용한 주기적인 사용자 PC 취약점 점검.
8. 출처 불분명한 이메일 수신 즉시 삭제.

③ 바이러스에 의한 데이터 손상에 대비해 정기적으로 데이터 백업을 실시한다.

④ 알려진 바이러스의 경우에는 해당 바이러스를 치료할 수 있는 진단 프로그램을 구비한다.

⑤ 무단, 불법 복사된 프로그램을 설치한 정보시스템은 교내 전산망 접속을 제한한다.

⑥ 바이러스의 감염이 확인될 경우 즉각 네트워크 접속을 단절 시킨 후 바이러스 백신 프로그램으로 바이러스를 치료한다.

⑦ 외부에서 온 저장매체, 인터넷에서 다운로드 받은 파일, 외부로부터 전송된 메일의 첨부파일 등은 실행 또는 열기 전에 반드시 바이러스 검사를 해야 한다.

제10장 시스템실 운영・관리 보안 지침

제29조(시스템실 시설기준)

① 출입구는 반드시 2중으로 설치하며 또한 입실자를 식별 및 로그인 가능한 출입보안장치(CCTV 등)를 설치하여 6개월간 내용을 보관한다.

② 자동 화재경보 설비를 설치하고, 할로겐 가스 등 소화 시 장비에 피해를 주지 않는 자동 소화 설비를 설치한다.

③ 정전에 대비하여 별도의 전원공급 시설을 둔다.

④ 온·습도를 적절히 유지할 수 있는 항온항습기를 설치한다.

제30조(시스템실 운영 및 관리)

① 시스템실의 운영을 담당하고 있는 부서장은 시스템실 사용 및 운영에 관한 절차 및 방법을 규정하고, 담당자들이 이를 숙지하도록 한다.

② 시스템실의 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 시스템실에는 출입자 명부를 비치하고 비인가자의 출입을 통제해야 한다.

⑤ 시스템실·자료보관실 및 통신실은 관리책임자를 지정하고 자료 또는 장비별로 취급자를 지정 운영해야 한다.

제11장 개인정보 보호 지침

제31조(개인정보의 수집)

① 본교의 모든 부서는 직무와 관련이 없는 사상, 신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집할 수 없다.

② 직무상 필요한 개인정보를 수집하는 경우에도 꼭 필요한 최소한의 개인정보를 수집하며, 불필요한 개인정보를 요구하지 않는다.

③ 개인정보의 수집 시에는 다음 사항을 반드시 고지한다.

1. 개인정보 수집·이용 목적
2. 수집하려는 항목
3. 개인정보의 보유·이용 기간
4. 동의를 거부할 권리가 있다는 사실

제32조(개인정보의 보유 및 보존기한)

⑤ 직무와 관련된 소관업무를 수행하기 위하여 당해 부서 및 관리자는 제반 규정에 규정된 범위 안에서 최소한의 개인정보화일을 보유할 수 있다.

⑥ 부서에서 보유중인 개인정보화일의 보존기간을 관련 문서보관 규정에 따라 정하고 보유기간 만료시 규정에 따라 폐기한다.

제33조(개인정보의 이용 및 제공)

① 부서에서 보유중인 개인정보를 보유목적외의 용도로 이용하거나 타 부서에 임의로 제공할 수 없다. 단, 관련 법령 및 본교의 규정에 의한 경우에는 예외로 한다.

② 제1항에도 불구하고 다음 각 호의 1에 해당하는 경우에는 당해 개인정보화일의 보유목적외의 목적으로 개인정보를 이용하거나 다른 기관에 제공할 수 있다. 단, 다음 각 호의 1에 해당하는 경우일 때에도 정보주체 또는 제3자의 권리와 이익이 부당하게 침해할 우려가 있다고 인정될 때에는 제공치 않을 수 있다.

1. 정보주체의 동의가 있거나 정보주체에게 제공하는 경우
2. 다른 법률에서 정하는 소관업무를 수행하기 위하여 당해 처리정보를 이용할 상당한 이유가 있는 경우
3. 조약 기타 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하는 경우

4. 통계작성 및 학술연구 등의 목적을 위한 경우로써 특정개인을 식별할 수 없는 형태로 제공하는 경우

5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 동의를 할 수 없는 경우로서 정보주체외의 자에게 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우

6. 범죄의 수사와 공소의 제기 및 유지에 필요한 경우

7. 법원의 재판업무수행을 위하여 필요한 경우

8. 기타 대통령령이 정하는 특별한 사유가 있는 경우

③ 제2항의 규정에 의하여 개인정보를 정보주체외의 자에게 제공하는 때에는 수령한 자에 대하여 사용목적·사용방법 등 기타 필요한 제한을 하거나 개인정보의 안전성 확보를 위하여 필요한 조치를 강구하도록 요청 할 수 있다.

④ 정보주체의 권리와 이익을 보호하기 위하여 정보취급제한이 필요한 경우에는 개인정보의 처리를 당해 특정부서로 제한할 수 있다.

제34조(개인정보의 열람・정정・폐기)

① 정보주체는 본인에 관한 개인정보의 열람을 당해 정보 보유부서의 장에게 서면으로 청구할 수 있다.

② 부서의 장은 제1항에 의하여 열람청구를 받은 때에는 본교 제반 규정에 따른 특별한 사유가 없는 경우에는 15일 이내에 청구인으로 하여금 당해 개인정보를 열람할 수 있도록 하여야 한다.

③ 단, 입학에 관련한 정보는 어떠한 경우에도 열람청구를 할 수 없다.

④ 본인의 개인정보를 열람한 정보주체는 당해 부서장에게 서면으로 본인의 개인정보 정정을 요구할 수 있다.

⑤ 보유부서의 장은 정정청구를 받은 때에는 개인정보의 정정에 대하여 다른 규정이 있는 경우를 제외하고는 적절한 내부 심사를 통하여 필요한 조치를 취한 후 그 결과를 청구인에게 7일 이내에 통지하여야 한다.

⑥활용이 종료된 각종 개인정보 및 관련 출력자료는 즉시 파기해야 한다. 단, 문서관리 규정 등 관련 규정에 의하여 보존할 필요성이 있는 경우에는 그 규정에 따른다.

1. 문서화된 출력물은 외부로 유출되지 않도록 문서 세단기를 사용하여 파쇄 한다.

2. 디스켓, 테이프, CD, USB 등 정보보관용 미디어를 폐기할 때는 수록된 데이터를 삭제하고 복구할 수 없도록 미디어 본체를 파괴시킨다.

제35조(아동의 개인정보보호) 만14세 미만 아동의 개인정보를 보호하기 위하여 다음 사항을 준수해야 한다.

① 만14세 미만 아동의 개인정보 수집은 별도의 양식을 통해 이루어져야 하며 개인정보 수집 시 법정대리인의 동의를 구하여야 한다.

② 동의의 방법은 법정대리인의 성명과 주민등록번호 및 연락처 등을 입력하도록 하고, 수집된 아동의 법정대리인의 개인정보는 동의 여부를 확인하는 용도로만 사용하여야 한다.

③ 만14세 미만 아동의 법정대리인은 아동의 개인정보에 대한 열람, 수정 및 삭제를 요청할 수 있으며 이러한 요청에 지체 없이 필요한 조치를 취하여야 한다.

제36조(국외 이전 개인정보의 보호)

① 이용자의 개인정보를 국외로 이전하려면 이용자의 동의를 받아야 한다.

② 제1항에 따른 동의를 받으려면 미리 다음 각 호의 사항 모두를 이용자에게 고지하여야 한다.

1. 이전되는 개인정보 항목

2. 개인정보가 이전되는 국가, 이전일시 및 이전방법

3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭을 말한다)

4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간

제37조(개인정보 출력물 관리)

① 개인정보가 포함된 출력물에는 출력일시, 출력자등의 표시를 하여야 한다.

② 개인정보가 포함된 출력물의 위·변조 방지를 위한 기능이 있어야 한다.

제38조(정보화 기기폐기) 노후된 PC, 서버 등의 정보화기기를 폐기하거나 외부로 기증할 때에는 하드디스크 등에 저장된 개인정보 및 업무관련 자료를 기술적으로 복구할 수 없도록 완전히 삭제해야 한다.

제12장 기 타

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

제40조(준용) 기타 이 규정에 명시되지 아니한 사항은 본교의 관계 규정에 준한다.

부 칙

이 규정은 2011년 10월 1일부터 시행 한다.

정보보안 관리규정 시행세칙

□ 2011. 10. 1 제정

제1장 종합정보시스템 정보보안 지침

제1조(목적) 이 세칙은 정보보안·관리규정 제39조에 따라 종합정보시스템 정보보안에 관한 시행기준을 정함을 목적으로 한다.

제2조(종합정보시스템 사용목적) 종합정보시스템은 교내의 학적, 교무, 장학 및 행정을 지원하기 위한 기간시스템으로, 이 시스템을 사용하는 목적은 학생 및 교직원의 학사, 교무, 장학 및 행정 업무를 수행하는데 한한다.

제3조(사용자 범위) 사용자 범위는 다음 각 호와 같다.

1. 교내에 재직 중인 직원
2. 교외부서에서 재직 중인 직원으로 종합정보시스템을 사용하여 학사업무 및 행정업무를 수행하여야 할 경우는 업무주관부서의 동의를 얻어 사용권한을 부여받은 직원
3. 기타 행정업무 보조를 위해 행정부서에서 등록한 행정업무보조원 (근로/조교/공익요원 등)

제4조(사용 ID 발급 및 폐기 기준)

① 신규 임용자는 인사팀에서 임용발령 후 종합정보시스템에 신규임용자로 입력된 시점부터 교번이 부여되며, 부여된 교번은 퇴직 시까지 본인의 종합정보시스템 사용자 ID로 사용된다.

② 퇴직자는 인사팀에서 퇴직 처리된 직후 종합정보시스템에 퇴직자로 입력되어 종합정보시스템을 사용 할 수 없다.

③ 교외부서 사용자는 주기적으로 ID 사용 및 폐기 유무를 업무주관부서에 통보하며, 업무주관부서에서는 통보받은 내용을 확인하여 ID 재사용 여부를 결정하여 정보전산원에 통보한다.

④ 기타 행정업무보조원은 행정부서에서 직접 ID를 발급하고 종합정보시스템 사용기간을 입력하여 ID 사용/폐기 등을 관리한다.

제5조(사용권한 제한 및 권한부여 책임자)

① 종합정보시스템은 학사행정 분야, 일반 행정 분야, 연구행정 분야로 나누고 있으며 각 분야별 시스템 사용권한 통제 분류기준은 별표 1과 같다.

② 연구행정 분야의 시스템 사용권한 부여는 산학협력단에서 직접 부여 한다.

제6조(사용권한 요청 및 허가절차)

① 신규로 학사행정 분야, 일반 행정 분야, 연구행정 분야의 각 시스템 내의 프로그램을 사용하기 위해서는 해당 시스템 주관부서의 부서장에게 문서로써 사용 요청을 하여야 하며, 요청을 받은 주관부서의 부서장은 허가여부를 결정하여 정보전산원에 반드시 문서로써 통보하여야 하고, 정보전산원은 사용할 수 있도록 조치한다.

② 인사이동에 의한 시스템 사용권한 삭제 및 사용권한 변경요청 또한 주관부서의 부서장에게 문서로써 협조 요청을 하여 허가를 받아야 하며, 요청을 받은 주관부서의 부서장은 허가여부를 정보전산원에 반드시 문서로써 통보하여야 하고 정보전산원은 해당 시스템에 대한 권한을 조치한다.

③ 행정업무보조원이 학사행정 분야, 일반 행정 분야, 연구행정 분야의 각 시스템 내의 프로그램을 사용하기 위해서는 해당 시스템 주관부서의 부서장에게 문서로써 사용요청을 하여야 하며, 요청을 받은 주관부서의 부서장은 허가여부를 결정하여 정보전산원에 반드시 문서로써 통보하여야 하고, 정보전산원은 사용할 수 있도록 조치한다.

제7조(중요자료 변경 기록 보관)

① 정보시스템에서 발생되는 인사 사항, 학적 사항, 성적자료의 변경 LOG는 결재 후 5년간 보관한다.

② 행정부서 자료변동에 대한보고는 다음 각 호와 같이 실시한다.

1. 정보시스템에서 발생되는 자료 변경 LOG는 종합정보시스템에서 출력하여 부서장에게 결재후 5년간 보관 한다.
2. 결재 대상 중요자료는 인사사항, 학적사항, 성적사항으로 한정 한다.

③ 전산개발팀 내부보안 체계는 다음 각 호와 같이 정한다.

1. DBA (Data Base Administrator) 1명을 둔다.
2. DBA는 정보전산원장이 명하며, 매년 보안각서를 작성하도록 한다.
3. 발생되는 모든 LOG는 DBA만 접근 가능하도록 한다.

④ 전산개발팀장과 DBA는 1개월에 1번 Data Base 와 백업 받은 Tape를 비교하여 LOG 자료를 분석하며, 이를 정보전산원장에게 보고한다.

⑤ LOG 자료의 범위는 다음 각 호와 같다.

1. [인사] - [교원기본자료출력] - 교원인사 LOG 내역
2. [인사] - [인사기본자료출력] - 직원인사 LOG 내역
3. [학적] - [학적기본출력] - 학적 LOG 내역
4. [학적] - [대학원기본출력] - 학적 LOG 내역
5. [성적] - [학부출력] - 성적 정정 LOG 내역
6. [성적] - [대학원출력] - 성적 정정 LOG 내역

(별표 1) 시스템 사용권한 부여 및 통제 기준

분야	시스템 명	주관 부서	시스템 권한부여 책임자
학사 행정	학적관리	학적・수업팀/대학원 학사팀	학적・수업팀장/대학원 학사팀장
	교과/수강관리	학적・수업팀/대학원 학사팀	학적・수업팀장/대학원 학사팀장
	성적/졸업관리	학적・수업팀/대학원 학사팀	학적・수업팀장/대학원 학사팀장
	장학관리	학생처 학생팀/대학원 학사팀	학적・수업팀장/대학원 학사팀장
	등록관리	총무처 경리팀/대학원 학사팀	경리팀장/대학원 학사팀장
	취업관리	취업정보처	취업정보처 팀장
	대학원입시	대학원 학사지원팀	대학원 학사팀장
일반 행정	인사관리	교무처 교무팀/총무처 인사팀	교무팀장/인사팀장
	급여관리	경리팀	경리팀장
	예산관리	기획실	기획실장
	회계관리	경리팀	경리팀장
연구 행정	구매/비품 시설관리	관리팀	관리팀장
	발전기금관리	기획실	기획실장
	병무관리	예비군연대	예비군연대장
	연구관리	산학협력단	산학협력단장

제2장 침해사고 대응 지침

제8조(목적) 이 세칙은 정보보안·관리규정 제39조에 따라 본교에서 발생하는 침해사고에 신속하게 대응하기 위한 준비와 대응절차를 기술하여 침해사고로부터의 피해를 최소화하고 후속 보안 대책을 세울 수 있도록 함을 그 목적으로 한다.

제9조(적용범위) 본 지침은 본교 IT부서 및 침해사고가 발생 가능한 자원의 관리자 그리고 이와 관련된 제 3자를 포함한다.

제10조(용어정의)

① 침해사고 : 해킹, 컴퓨터바이러스, 악성코드, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등에 의하여 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태를 말한다.

② 침해사고 대응팀 : 해킹 또는 바이러스 사고 발생에 따른 사고의 분석, 처리, 사후 복구, 사후 예방 조치 등을 주요 업무로 하는 보안팀을 말한다.

제11조(책임사항)

① IT 보안 관리자 : 침해사고대응 체계를 수립하고 관련 내용을 각 IT 직원에게 교육 및 훈련시키도록 한다.

② IT 담당자 : 침해사고와 관련된 내용을 숙지하고, 침해사고 발생 시 본 지침에 따라 대응 할 수 있도록 한다.

③ 일반 직원 : 침해사고와 관련된 내용을 숙지하고, 침해사고 발생 시 본 지침에 따라 IT 담당자 또는 보안 관리에게 보고해야 한다.

제12조(침해사고 대응팀 구축 및 운영) 본교에서 운영되는 전산망에 대한 침해사고 대응 활동을 지원하고 대외 침해사고대응 기관간의 사고대응체계를 구축하여 급증하는 인터넷 보안 사고에 대한 효율적인 대응을 제공한다.

① 침해사고 대응팀의 역할

1. 본교 내에서 발생한 침해사고의 분석, 처리, 후속조치 업무 및 지원 업무 수행
2. 대외 사고대응 기관과의 사고대응 협력
3. 침해사고 방지를 위한 교육, 기술개발 및 보급
4. 서비스 대상 : 본교의 전산 시스템을 대상으로 해킹/바이러스 사고 예방 및 대응 업무를 수행한다.

② 침해사고대응팀 구성

1. 인력 구성

▪ 체계적·효율적인 보안정책 수립·심의 및 관리를 위하여 정보전산원 산하에 침해 사고 대응팀(이하 '대응팀'이라 한다)을 둔다.

▪ 대응팀은 팀장, 연락 담당, 사고접수 담당, 침해사고 처리 담당, 취약성 분석/테스트 담당 등 5인 내외의 인원으로 구성하며, 정보전산원장 및 정보전산원의 구성원으로 한다.

2. 구성원의 역할

▪ 팀장 : 침해사고 대응팀의 실무 책임자로 침해사고대응 업무를 총괄하여 빠른 사고대응 업무가 가능하도록 한다. 본교 내에서는 타 부서 및 경영진과의 업무 조율 역할과 대외적으로는 국내 침해사고 대응팀과의 협력관계를 구축한다.

▪ 연락 담당 : 본교의 대내외 업무 조율을 위한 실무 대표자 역할을 한다. 주로 사고대응을 위한 대내외 협력 업무에 대한 연락업무를 수행한다.

▪ 사고접수 담당 : 해킹 및 바이러스 등의 침해사고 접수, 사고 할당, 사고 접수 자료에 대한 관리를 담당한다. 보안사고의 초기 접수에서 사고여부의 초기 판단 업무를 수행하고 이를 각 관련 담당자에게 이관하는 작업이다.

▪ 침해사고 처리 담당 : 해킹사고 발생 시, 해당 사고를 정확히 분석하고 대응할 수 있는 사고 분석 전문가 역할을 수행한다. 다음과 같은 업무를 수행한다.

- 사고노트 작성 배포
- 특정 중요 사안에 대한 기술문서 작성 배포
- 해킹사고 탐지 및 방지를 위한 프로그램 개발 참여

▪ 취약성 분석/테스트 담당 : 새로운 취약성에 대한 분석, 사이트에 대한 위협 여부 평가, 취약성 테스트 등 의 업무를 담당한다. 항상 새로운 취약성의 발표 자료를 검토하고 각 사이트에 적용 여부를 판단하여야 한다. 다음과 같은 업무를 수행한다.

- 보안권고문 작성 배포
- 기술 문서 작성 및 배포
- 보안 가이드라인 작성 및 배포

③ 비상 연락망 : 침해사고 대응팀 전원의 연락처, 비상 연락처를 비롯하여 사고대응과 관련된 타 부서 담당자도 비상 연락망에 포함 시키도록 한다.

④ 침해사고 대응 및 복구

1. 침해사고 신고 접수

▪ 전화 : (031)-220-2437

▪ 팩스 : (031)-220-2492

▪ E-mail : kcpark@suwon.ac.kr

2. 침해사고 신고 접수 : 침해사고 보고는 E-mail 보고를 기본으로 하고 관련 침해사고 신고 접수 지침 및 양식은 홈페이지에 등제한다. 사고가 보고될 경우, 다음과 같은 지침에 따라 사고를 처리하도록 한다.

▪ 침해사고 보고기관(사람)의 신분을 확인한다.

▪ 관련 담당자에게 사고접수 내용을 전달한다.

▪ 1주일 이내에 침해사고 신고기관에게 침해사고 접수확인 메일을 전송한다. 답장 메일 전송 시 침해사고 신고 접수 확인 및 할당된 사고번호를 메일의 Subject에 명시한다. 향후 연락 시 사고번호로 구분하여 정보를 교류한다.

3. 침해사고 접수 처리

▪ 침해사고 신고 접수 담당자는 침해사고 접수 후 24시간 이내에 담당자를 지정하여 침해사고 처리를 진행한다.

▪ 담당자는 침해사고 유형에 따라 우선순위를 부여하고 각 사고의 트래킹을 위해 사고번호를 부여한다. 만일, 침해사고로 처리하지 않아도 되는 잘못된 신고일 경우 신고자에게 해당 사실을 통지하고 사고를 종결한다.

▪ 담당자는 침해사고 사고보고 양식에 따라 보안 관리사고 개요를 보고하고 사고처리를 진행한다. 각 침해사고마다 침해사고 관리 목록에 기록하고 관리하도록 한다.

4. 사고 처리

▪ 초기분석 및 사고대응전략 수립 : 사고번호가 할당되면, 사고를 처리할 담당자를 지정하고 사고를 처리한다. 분석 담당자는 먼저 보고된 기본 자료를 검토하고 구체적인 처리 방향을 설정한다. 보고된 자료만으로도 해킹사고의 여부를 정확히 판단하기 힘든 경우에는 사고와 관련된 담당자와 연락을 취하고 추가적인 정보를

획득하거나 초기 분석을 한다.

▪ 대응방법 고려사항 : 공격자의 추적여부, 복구를 어떻게 할 것인가, 보안조치를 언제 할 것인가, 법적 대응 여부 판단 한다.

- 공격자 추적 : 공격자를 추적하기 위해서는 공격자 모니터링, 외부기관의 협력 등 많은 시간과 자원을 필요로 한다. 사고 범위, 피해 규모, 그리고 내부 자원의 역량에 따라서 추적 여부를 결정한다. 무엇보다 상대 기관과의 협의를 통해서 하도록 한다.
- 복구 : 해킹사고의 성격, 피해 범위에 따라 복구의 시기, 방법, 범위를 결정한다. 매우 중요한 사고이며 서비스가 계속 제공되어야 하는 경우 일차적인 초기분석을 통해 시스템을 먼저 복구하되 공격흔적이 훼손되지 않도록 주의한다. 그 외의 사고는 충분한 분석이 이루어진 후 복구한다.
- 법적 대응 : 사고의 경중에 따라서 또는 본교의 기본 방침에 따라서 법적인 대응을 할 것인지 고려한다. 만약 해킹사고로 인한 피해가 있다면 법적인 대응을 적극 고려해 볼 수 있다. 만약 법적 대응을 결정한 경우에는 최대한 피해시스템을 보존하도록 해야 한다.
- 피해시스템 통제 : 더 이상의 피해를 받지 않기 위해 외부로부터 시스템을 차단한다.
- 시스템의 처리 : 가능한 시스템을 직접 분석하지 않고 원본 상태로 보관한다. 긴급 시에는 서버를 이미지복사 한 후에 시스템 복구 작업을 하도록 한다.
- 위와 같이 처리한 다음 수사기관(경찰청 사이버테러 대응센터/검찰청 인터넷범죄 수사센터 등)에 신고하여 피해상담 및 복구, 법률적인 대응방안에 대해서 조력을 받도록 한다.

5. 피해 시스템 분석

▪ 사고가 발생한 원인 및 공격방법 : 공격자가 시스템에 어떻게 침입했는지에 대해서 분석한다. 주로 특정 어플리케이션의 취약성, 시스템의 잘못된 설정, 그리고 계정 도용 등을 이용하여 침입한다.

▪ 사고의 발생 시간 : 공격자가 언제 처음으로 시스템에 침입했는지 분석하고, 최초 침입 이후 재 침입이 언제 있었는지 등에 대해서 분석한다.

▪ 사고의 발생 범위: 보통 사이트 내에 하나의 시스템이 공격을 당했으면, 다른 시스템도 해킹을 당했을 경우가 많다. 따라서 사이내의 다른 모든 시스템, 그리고 피해시스템과 관련된 시스템에 대해서 피해여부를 확인해야 한다.

▪ 공격자 출처 : 공격자의 IP주소를 찾아내고, 해당 IP를 사용하는 기관 정보를 분석한다.

▪ 공격의 목적 : 공격자가 피해시스템에서 어떠한 활동을 했는지 분석함으로서 공격의 목적을 확인한다. 주로 정보유출, 단순한 침입, 공격시스템으로 사용 등의 목적이 있을 수 있다.

▪ 사고복구를 위한 긴급조치와 장기조치 방법: 사고를 분석하면서 긴급하게 취할 수 있는 예방 조치방법을 찾아보고 필요할 경우 예방조치를 취한다. 그리고 완전한 사고분석이 끝나면 향후 비슷한 유형의 사고를 예방하고 탐지할 수 있는 대책을 마련한다.

▪ 분석 시 유의 사항 : 분석 전에 해당 시스템의 보안 패치를 하고, 가능한 침입 흔적을 있는 그대로 보존, 백업, 각종 내용을 기록한다.

6. 사고대응 및 복구 : 사고대응 및 복구 단계에서는 취약성 제거, 피해시스템 복구, 관련자 통지, 보안대책 구현 등의 작업을 수행한다.

▪ 취약성 제거 : 공격에 이용된 취약성을 제거한다. 피해시스템뿐 아니라 피해시스템과 똑같은 종류의 시스템에 대해서 모두 분석하고 같은 취약성이 발견되면 이를 제거한다. 이러한 작업은 사고분석 결과를 보고서로 작성하여 기업 내의 관련된 담당자에게 배포함으로서 각 담당자가 직접 수정하도록 유도할 수 있다.

▪ 피해시스템 복구 : 취약성 제거를 한 다음, 정상적인 서비스가 이루어지도록 시스템을 복구한다. 만약 분석이 완벽하게 이루어지지 않았다고 판단된다면, 되도록 시스템을 다시 설치하는 것이 바람직하다.

▪ 관련자 통지 : 사고와 관련된 모든 사람에게 분석결과를 통지해 준다. 이 경우, 사고와의 관련성에 따라 주는 정보의 깊이가 달라져야 한다. 외부기관에 주는 정보는 사이트내의 세부 정보가 포함되지 않아야 하며, 상대방이 필요로 하는 정보만을 전달하도록 한다.

▪ 보고 및 피드백 : 사고분석 및 대응이 종료되면, 사고에 대한 보고서를 쓰도록 한다. 보고서에 들어가는 내용으로는 사고분석 및 대응 과정의 모든 내용과, 비슷한 유형의 사고를 방지하기 위한 보안시스템의 개선방향 등에 대해서 작성한다. 작성된 보고서는 조직 내의 책임자에게 보고되고 책임자의 결정에 따라 현재의 시스템 또는 네트워크에 그 결과가 피드백 되어야 한다.

관련 서식

(별지 1)

침해사고 비상 연락망

1. 침해사고대응팀 연락망

담당업무	담당자	연락처(E-mail, HP, office)
팀장		
사고분석		
헬프 데스크		
…	…	…

2. 관련 부서 연락망

부서명	담당자	담당업무	연락처(E-mail, HP, office)
시스템운영팀			
네트워크운영팀			
…			

3. 관련 업체 연락망

기관명	담당자	연락처(E-mail, HP, office)	URL
보안업체			
백신업체			
유지보수업체			
…			

4. 유관 공공기관 연락망

기관명	담당자	연락처(E-mail, HP, office)	URL
정보보호진흥원			
경창철			
검찰청			
…			

(별지 2)

침해사고 신고 양식

침해사고 신고번호	
신고기관 정보	
기관 이름	
신고자 이름	
전화번호	
E-mail	
피해 시스템 정보	
IP주소	
호스트 명	
운영체제	
추정 피해 시간	
시스템 운영 환경	
공격 시스템 정보(알 경우에 만 작성)	
IP 주소	
호스트 명	
사고에 대한 설명	
사고발견 경위, 피해현황 등	

사고발견 시간, 공격방법, 공격 흔적, 시스템 운영 환경, 공격출처, 피해상황, 취해진 작업 등에 대해서 아는 범위 내에서 작성

관련 기관(부서) 통지	
기관(부서)명	통지 내용

(별지 3)

침해사고 보고 양식

정보보호관리자

담 당	과 장	팀 장

침해사고 처리 담당자	침해사고 번호
	Ex) IN-040304-3212
신고기관 정보	
기관 이름	
신고자 이름	
전화번호	
E-mail	
피해 시스템 정보	
IP 주소	
호스트 명	
운영체제	
추정 피해 시간	
시스템 운영 환경	
공격 시스템 정보	
IP 주소	
호스트 명	
사고에 대한 설명(간단히 작성)	
사고발견 경위, 피해현황 등	

관련 기관(부서) 통지	
기관(부서)명	통지 내용

(별지 4)

침해사고 관리 목록

정보보호관리자

담 당	과 장	팀 장

접수번호	접수 날짜 (갱신 날짜)	침해사고 할당번호	상태	담당자	비고
Ex) 040304-123	2010-03-04		신고		
	2010-03-05	IN-040304-3212	접수		
	2010-03-06		처리		
	2010-03-10		완료		

(별지 5)

침해사고 처리 결과 보고서 양식

정보보호관리자

담 당	과 장	팀 장

* 주 : 하위 목차를 준수하여 자유양식으로 작성

1. 개 요
  1.1 피해시스템에 대한 상세한 정보
  1.2 분석일시 및 분석 환경
  1.3 특이사항

2. 초기분석 결과
 사고를 최초 탐지했을 때의 상태, 로그 기록과 초기분석 결과 등을 기록한다. 주로 탐지된 공격로그, 라이브 시스템 상에서 발견된 공격흔적에 해당한다.

3. 상세분석 결과
 공격자 활동에 대한 상세한 분석결과, 공격 프로그램 분석결과, 네트워크 모니터링 결과 등을 기술한다. 중요 결과만 정리해서 기술하고, 상세 분석 내용은 첨부로 작성한다.

4. 피해시스템 복구 및 대응방법
  사고분석 결과, 해당 사고를 탐지하는 방법, 피해시스템 복구 방법, 그리고 단기 대응방법, 장기 대응방법에 대해서 기술한다.

5. 의견
  사고를 분석한 담당자의 분석 의견을 적는다. 해당사고로부터 습득한 새로운 지식을 정리할 수도 있으며, 현재의 보안시스템에 대한 개선사항 등이 될 수 있다.

6. 참고 자료
  사고분석 과정에서 필요로 했던 참고자료를 정리한다.

제3장 정보시스템 긴급 재난복구

제13조(목적) 이 세칙은 본교 정보보안 관리규정 제39조에 따라 정보시스템 긴급재난복구에 관한 시행기준을 정함을 목적으로 한다.

제14조(적용범위) 적용범위는 다음 각 호와 같다.

1. 서버 시스템의 재난 복구
2. 네트워크 시스템의 재난 복구
3. 데이터, 어플리케이션의 재난 복구

제15조(서버 시스템 OS백업)

① 시스템의 OS 장애를 대비하기 위하여 시스템의 백업 기능을 이용 OS백업 이미지를 구성하여 원격지(중앙도서관)에 보관 한다.

② 시스템 OS백업은 다음 각 호에 따라 실시한다.

1. 백업 대상 : 정보서비스를 제공하는 서버로 데이터베이스 서버, 웹서버, WAS 서버, 계정서버 OS 및 설정파일을 백업한다. (대상 서버는 가감될 수 있다.)
2. 백업 주기 : 월 1회 실시한다.
3. 백업 방법 : Tape 장치를 사용한다.
4. 이동 방법 : 인편에 의한 OS 백업 이미지를 중앙도서관으로 이동한다.
5. 보관 방법 : 백업 Tape를 원격지(중앙도서관 내 전산장비 랙)에 이동 보관 한다.

제16조(서버 하드웨어 백업) 유지보수 계약을 통해 장애 발생 가능성이 있는 파트에 대한 예비 부품을 확보한다.

제17조(서버 시스템 OS 복구)

① 원격지(중앙도서관)에 사전 백업 보관된 OS이미지를 사용하여 복구한다.

② 시스템 OS 복구는 다음 각 호의 순으로 실시한다.

1. 백업 받아 두었던 OS 백업 이미지 Tape을 준비한다.
2. 백업 OS 이미지 tape을 시스템에 삽입하고 해당 tape을 이용하여 시스템을 부팅한다.
3. 부팅 후 시스템 복구 메뉴를 이용하여 OS 백업 이미지를 이용 OS를 복구한다.
4. 복구가 완료되면 시스템의 이상 유무를 확인 한 후 서비스를 구동한다.

제18조(서버 하드웨어 복구) 서버 시스템의 하드웨어 장애가 발생했을 경우 유지보수 계약업체는 대체 하드웨어를 조달하여 신속히 교체 복구한다.

제19조(네트워크 장비 소프트웨어 백업)

① 백업 대상은 백본 스위치, 주요 건물 스위치의 설정파일로 한다.

② 월 1회(정기백업), 설정 변경 시(수시백업) 실시한다.

③ 정보전산원 시스템실에 위치한 백업 파일서버에 보관한다.

제20조(네트워크장비 하드웨어 백업) 유지보수 계약을 통해 장애 발생 가능성이 있는 파트에 대한 예비 부품을 확보한다.

제21조(네트워크장비 소프트웨어 복구) 복구절차는 다음 각 호와 같다.

1. 백업 받아 두었던 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.

제22조(네트워크장비 하드웨어 복구) 네트워크 시스템의 하드웨어 장애가 발생했을 경우 유지보수 계약에 의거 계약업체의 대체 하드웨어를 조달하여 신속히 교체 복구한다.

제23조(네트워크장비 복구 우선순위) 재난에 의거 다수 지역에서 장애가 동시 발생했을 경우는 다음 각 호의 순에 의거하여 복구를 시행한다.

1. 백본 스위치
2. 주요 건물 스위치

제24조(백업서버를 이용한 데이터 백업)

① 각 주요 서버에 대해서 주별 백업 후 일별 증분백업을 한다.

② 중요 데이터, 어플리케이션은 백업서버를 이용하여 다음 각 호와 같이 일별 Online 백업을 실시한다.

1. 백업대상은 정보서비스를 제공하는 서버로 별표 2와 같으며, 대상은 가감될 수 있다.
2. 백업방법은 백업서버의 스케줄러 기능을 이용하여 각 대상 시스템에 Client를 탑재하여 일별 백업을 수행하며, 메인 DB서버의 경우 자체 백업프로그램을 이용한 백업도 병행한다.
3. 백업주기는 별표 3과 같다.

③ 백업한 백업데이터 복사본은 중앙도서관 백업 보조서버에 자동복사 하며 보관 주기는 6개월로 한다.

제25조(데이터 복구)

① 백업받은 OS를 복구하고 일별백업 한 데이터를 복구한다.

제26조(사용자 실수에 의한 데이터 손실복구)

① 일별백업 한 데이터로부터 복구한다.

(별표 2) 장비별 백업 내용

장비명	백업 내용
DNS	DNS 설정 내용
NS25-firewall	방화벽 설정 내용
KMS	KMS 설정 내용
AS/400	OS 및 학사행정 DB
Virobot	바이로봇 수집로그
NSM	방화벽 로그
SIMS	설정 및 로그
내PC지키미	설정 및 로그
PMS	설정 및 로그, DB
KRI 연계서버	설정 및 로그, DB
NMS	설정 및 로그, DB
PBL	설정 및 소스프로그램
www1	설정 및 로그, 사용자 계정, DB
백업서버	설정 및 DB
MAIL	설정 및 로그, DB
SPAM	설정 및 로그, DB
IPMENTOR	설정 및 로그, DB
회계서버	설정 및 로그, DB
swu	홈페이지 데이터
app	학사행정 Web 프로그래밍 데이터
L4 : 설정	L4 설정 내용
Foundry-2402	Foundry-2402 설정 내용

(별표 3) 서버별 백업주기

서버별 백업 시간은 매일 03시로 하되 데이터양이 많은 서버는 아래의 스케줄대로 한다.

요일	12:30	01:00	02:30	04:00	05:00	06:00	07:00
토	dns-full	swu-full	www1-full	pms-full	pbl-full	was-full	das-db
일	dns-full	swu-inc	www1-inc	pms-inc	pbl-inc	was-inc	das-db
월	dns-full	swu-inc	www1-inc	pms-inc	pbl-inc	was-inc	das-db
화	dns-full	swu-inc	www1-inc	pms-inc	pbl-inc	was-inc	das-db
수	dns-full	swu-inc	www1-inc	pms-inc	pbl-inc	was-inc	das-db
목	dns-full	swu-inc	www1-inc	pms-inc	pbl-inc	was-inc	das-db
금	dns-full	swu-inc	www1-inc	pms-inc	pbl-inc	was-inc	das-db

제4장 E-mail 보안 지침

제27조(목적) 이 세칙은 본교 정보보안 관리규정 제39조에 따라 E-mail 보안에 관한에 관한 시행기준을 정함을 목적으로 한다.

제28조(E-mail 계정 및 사용)

① E-mail 계정 신청 및 삭제

1. E-mail 계정은 본교 재적생, 교수, 직원에게만 제공한다.
2. E-mail 계정은 1인 1계정을 제공한다.
3. E-mail 계정은 졸업 및 퇴직 후 일정 기간 공지우 삭제를 원칙으로 한다.

② E-mail 사용 원칙

1. 업무용 E-mail을 개인적인 용도로 사용해서는 안 된다.
2. 비밀 또는 본교가 소유한 정보는 E-mail로 보내지면 안 된다.
3. 교직원의 E-mail 주소 디렉터리는 공개적인 접근이 가능해서는 안 된다.
4. 고의로 E-mail을 오용하는 사용자를 발견하면 상응하는 징계조치를 취한다.
5. 사용자는 본인의 암호를 3개월마다 변경해야 한다.
6. 사용자 암호는 8자리 이상의 특수문자 + 숫자 + 문자의 조합으로 입력해야 한다.

제29조(E-mail 보안)

① E-mail 소프트웨어

1. 오직 인가된 E-mail 소프트웨어만 사용한다.
2. 익명 remailer 소프트웨어는 설치할 수 없다.

② 접근 제어

1. pop3는 학교 내에서만 접속하게 하고 외부에서는 접속을 거절하도록 한다.
2. E-mail 메시지의 내용은 범죄 조사, 보안취약성 조사, 감사를 위한 경우를 제외하고 비밀로 간주한다.

③ 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.

④ 바이러스 점검

받는 메시지의 경우 E-mail서버에서 첨부 파일에 대한 바이러스 검사를 실시한다.

⑤ 사고 대응

E-mail 관리자는 E-mail관련 보안문제나 외부 해킹공격 등의 발견 시 IT보안 관리자에게 즉시 알린다.

제5장 용역사업자 보안 지침

제30조(목적) 이 세칙은 본교 정보보안 관리규정 제39조에 따라 용역사업자 보안에 관한에 관한 시행기준을 정함을 목적으로 한다.

제31조(적용범위) 본 지침은 본교 정보전산원과 전산시스템을 자체로 도입 또는 및 정보화 관련 용역을 시행하고자 하는 단위 부서를 대상으로 한다.

제32조(보호구역 근무자 보안)

① 부서의 장은 정보전산원 등 보호구역에 신규로 근무하는 직원 또는 직원 외의 상시 근무자에 대해 다음 각 호의 보안조치를 수행해야 한다.

1. 보안의식 교육 및 별지 6호 서식에 의한 보안서약서 징구
2. 보호구역 출입 관리대장 및 수행 작업 로그 분석

② 부서의 장은 보호구역으로부터 전출 또는 퇴직자에 대해 다음 각 호의 보안조치를 수행해야 한다.

1. 전출 또는 퇴직자가 사용하던 PC에 저장되어 있는 비공개 자료 삭제
2. 전출 또는 퇴직자가 사용하던 사용자계정(ID)을 즉시 변경 또는 사용 중지

제33조(업무대행자 보안관리)

① 부서의 장은 정보시스템을 관리하기 위하여 일용직, 단순고용직, 자체직원 등을 업무대행자로 지정하여서는 아니 된다. 다만, 부득이한 경우에는 정보보안담당관의 승인하에 지정하되, 다음 각 호의 사항을 준수하여야 한다.

1. 정보시스템의 접속시간, 접속 및 이용 권한을 최소화
2. 유효기간이 설정된 임시 접속계정 부여
3. 인가되지 않은 정보시스템에 불법 접속하는지 여부를 주기적으로 확인 점검

② 부서의 장이 제1항에 의하여 특정 정보시스템에 대해 업무대행자를 지정한 경우에는 다음 각 호의 사항을 확인하는 등 보안조치를 수행하여야 하며, 그 사유가 소멸할 경우에는 즉시 해지하여야 한다.

1. 접속할 사용자, 사용자계정, 비밀번호
2. 접속주소, 접속시간, 접속사유(자료입력, 통계작성 등)
3. 접속 종료 후 사용자계정 및 비밀번호 회수 등 조치사항
4. 별지 6호 서식의 보안서약서 징구

제34조(용역사업 준비단계 보안)

① 부서의 장은 정보화·정보보호사업 및 보안감리·보안컨설팅 수행 등을 외부 용역으로 추진할 경우에 보안심사위원회 의 보안성 검토를 실시하여야 한다.

② 부서의 장은 제1항 관련 용역사업을 계약할 경우 계약서에 용역사업 참가직원의 보안준수 사항과 위반할 경우에 손해배상 책임 등을 명시하여야 한다.

③ 부서의 장은 용역업체가 사업의 일부 또는 전부에 대하여 하도급 계약을 체결하는 경우에 용역업체로 하여금 하도급 계약서에 본 사업계약 수준의 비밀유지 조항을 포함하도록 조치해야 한다.

④ 부서의 장은 필요한 경우에 업무위탁 또는 용역인력을 대상으로 신원조사를 실시하여야 한다. 이 경우신원조사 대상자에 대한 조사결과를 고지하거나 누설행위를 금지하며, 업무상 직접적인 관련이 없이 신원기록을 열람하지 않도록 하는 등 신원조사 정보의 보안이 유지되도록 하여야 한다.

제35조(용역사업 수행단계 보안)

① 부서의 장은 용역사업의 참여인력 및 용역회사 대표에 대하여 별지 6호 서식에 의한 보안서약서를 작성·제출토록 해야 한다.

② 부서의 장은 용역인력에 대해 비밀유지의 준수 의무 및 위반할 경우 처벌내용 등에 대한 보안교육을 실시해야 한다.

③ 부서의 장은 비밀관련 용역사업을 수행할 경우에 외부 참여인원에 대한 비밀취급인가 등 보안조치를 취해야 한다.

④ 부서의 장은 용역업체에게 자료를 제공하거나 용역수행 중 생산된 산출물에 대하여 다음 각 호에 따라 관리하여야 한다.

1. 비공개자료를 용역업체에게 열람하게 하거나 제공할 경우에 별지 7호 서식의 열람·제공자료 관리대장으로 작성하여 인계자와 인수자가 직접 서명한 후 인수·인계 실시
2. 산출물 등 사업 관련 자료는 인터넷 웹하드 등의 자료공유사이트 및 개인 메일함에 저장 금지, 대외비이상의 비밀은 전자우편으로 수·발신 금지
3. 용역업체에 제공한 비공개자료는 매일 퇴근할 때 반납 조치하며, 비밀문서를 제외한 일반 문서는 시건장치가 된 보관함에 보관
4. 산출물 중 비공개 자료는 비인가자 또는 대외에 제공 또는 열람 금지

⑤ 부서의 장은 용역사업을 수행하는 사무실과 장비에 대하여 다음 각 호에 따라 관리하여야 한다.

1. 시건장치가 구비되고 출입통제가 가능한 사무실 사용
2. 용역업체의 사무실과 인원·장비를 대상으로 정기적으로 보안점검 실시
3. 보호구역에서 용역사업자가 정보시스템이나 보조기억매체 등 정보자산을 반입 또는 반출하는 경우에 악성코드 감염 및 자료 무단반출 여부를 확인
4. 용역수행 PC에 허가받지 않은 USB 등 외부 저장매체 사용을 금지

⑥ 부서의 장은 용역업체가 업무를 위해 전산망을 이용하는 것이 필요하다고 판단되는 경우 전산망 접근을 허용하되 다음 각 호에 따라 관리를 해야 한다.

1. 사업별 또는 사용자별로 접속계정을 부여
2. 계정별로 정보시스템의 접근권한 부여, 계정에 대한 작업이력 확인
3. 용역인력의 접속계정에 대한 비밀번호를 기록·관리
4. 서버 및 네트워크 장비에 대한 접근기록을 확인·관리
5. 용역사업에 투입된 PC가 인터넷에 연결되는 것을 원칙적으로 금지하여야한다. 다만, 필요한 경우에는 전용단말기를 지정하거나 필요한 사이트에만 접속가능토록 통제하여야 한다.

⑦ 부서의 장은 용역업체 근무인력 중 대표 1인을 용역업체인력의 보안 관리자로 지정하여 용역사업자 자체적인 보안관리체계를 마련한다.

제36조(용역사업 종료단계 보안)

① 부서의 장은 최종 용역산출물 중 대외보안

이 요구되는 자료는 개발문서 관리 지침에 따라 등록하여 관리해야 한다.

② 부서의 장은 용역업체에 제공한 자료·장비·문서 및 중간·최종산출물 등 사업 관련 제반자료를 확인하여 전량 회수해야 하며, 노트북·보조기억매체 등에 의해 전자적으로 기록된 자료도 데이터 완전삭제 도구 등을 활용하여 복구가 불가능하도록 삭제 조치해야 한다.

③ 부서의 장은 제2항의 용역사업 관련자료 회수 및 삭제조치 후에 용역업체가 용역산출물의 복사본 등 용역사업 관련 자료를 보유하고 있지 않다는 용역업체 대표명의 별지 8호 서식의 보안확약서를 작성·제출토록 해야 한다.

④ 부서의 장은 필요한 경우 용역사업에 투입된 PC 등에 대하여 제2항 및 제3항의 용역사업 관련자료 회수 및 삭제조치에 대한 이행여부를 확인할 수 있다.

(별지 6)

보안 서약서

본인은 ____년 __월 __일부로 _____관련 용역사업(업무)을 수행함에 있어 다음사항을 준수할 것을 엄숙히 서약합니다.

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

2. 본인은 이 기밀을 누설함이 본교에 위해가 될 수 있음을 인식하여 업무수행중 지득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.

3. 본인이 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다.

4. 본인은 하도급업체를 통한 사업 수행 시 하도급업체로 인해 발생하는 위반사항에 대하여 모든 책임을 부담한다.

년 월 일

서 약 자 (업체)	업 체 명 : 직 위 : 성 명 : 주민등록번호 :	(서명)
서약집행자 (담당부서)	소 속 : 직 위 : 성 명 : 주민등록번호 :	(서명)

(별지 7)

열람.제공자료 관리대장

용역업체 관리책임자	기관 관리책임자

년(일련번호:) 사업명 : 사업주관 기업:

연번	자료명	인계 및 인수				자료반납	
		인계자	인수자	월일	장소	확인자	월일

(별지 8)

보안확약서

본인은 귀 기관과 계약한 _____사업의 수행을 완료함에 있어, 다음 각 호의 보안사항에 대한 준수 책임이 있음을 서약하며 이에 확약서를 제출합니다.

1. 본 업체(단체)는 업체(단체) 및 사업 참여자가 사업수행 중 지득한 모든 자료를 반납 및 파기하였으며, 지득한 정보에 대한 유출을 절대 금지하겠습니다.

2. 본 업체(단체)는 하도급업체에 대해 상기 항과 동일한 보안사항 준수 책임을 확인하고 보안확약서 징구하였으며, 하도급업체가 위의 보안사항을 위반할 경우에 주사업자로서 이에 동일한 법적책임을 지겠습니다.

3. 본 업체(단체)는 상기 보안사항을 위반할 경우에 귀 기관의 사업에 참여 제한 또는 기타 관련 법규에 따른 책임과 손해배상을 감수하겠습니다.

년 월 일

서약업체(단체) 대표
소 속 :
직 급 :
성 명 : (서명)

수원대학교총장 귀하

제6장 접근기록 관리 지침

제37조(목적) 이 세칙은 정보보안 관리규정 제39조에 따라 중요정보 접근기록의 작성 및 보관, 보존, 정보접근 및 허용 등의 관리와 기타 접근기록에 관한 사항에 관한 시행기준을 정함을 목적으로 한다.

제38조(구성) 이 지침에서의 접근기록의 구성은 별표 1과 같다.

제39조(적용범위) 접근기록의 관리에 관하여는 개인정보관리규정, 전기통신기본법, 전기통신사업법에서 정한 것을 제외하고는 이 지침이 정하는 바에 따른다.

제40조 (내용)

① 접근기록에는 접속자 ID, 접속자 IP, 호출 프로그램명, 실행 SQL문에 관한 모든 정보를 정확하게 기록해야 하며, 감사추적시스템은 기록된 내용, 생성된 결과 값 등에 대한 log file이 생성, 보존, 관리되어야 하며, 필요시 사용이력 확인이 가능하도록 구성되어야 한다.

② 접근기록에는 다음 각 호의 내용을 기록한다.

1. 접속자 ID
2. 수행프로그램명
3. 접속자 IP
4. 이벤트방법(조회, 수정, 삭제)
5. 대상 Table
6. 이벤트 발생시간
7. 실행 SQL

제41조(보관)

① 접근기록은 업무담당자의 책임성을 위하여 보관 유지한다.

② 접근기록은 컴퓨터 서버에 저장하며 백업공간을 두어 접근기록 원본이 훼손된 경우 복구할 수 있도록 한다. 백업공간으로의 사본 저장은 정기적으로 정보부서에서 시행한다.

③ 접근기록의 불법적인 접근 및 이용 방지를 위하여 정보부서 및 감사부서 직원 및 정보부서장이 권한을 인정하는 대학 구성원만이 전자적 접근기록에 접근할 수 있다.

제42조(관리,보존)

① 정보부서장은 접근기록 관리담당자를 지정하여 자료처리 등이 로그파일에 기록·유지되도록 하여야 한다.

② 접근기록 관리담당자는 접근기록을 수시로 점검하여야 하고, 중대한 사고가 발생 할 경우에는 정보부서의 장에게 보고한 후 응급복구 등의 조치를 하여야 한다.

③ 접근기록파일에 기록된 사용자는 자료변환의 모든 책임을 진다.

④ 로그별 보존기간 및 작업주기에 따라 접근기록을 보존 한다.

⑤ 접근기록은 특별한 지침이 있는 경우를 제외하고 5년간 보존 한다.

제43조(이용) 허가를 받은 사람 이외에는 출력, 조회기능 권한이 없으며 분쟁이 있는 경우는 정보부서에 요구하여 담당자에게 출력하여 이용 할 수 있게 한다.

① 접근기록은 법원의 지시이외에는 교외 반출을 할 수 없다.

② 접근기록의 출력은 다음의 경우에만 가능 한다.

1. 중요자료의 변동에 따른 책임추적이 필요시
2. 개인정보 조회에 대한 분석 필요시

3. 관련 부서장의 결재를 득한 후 정보부서장의 허가를 받은 경우

제44조(열람)

① 접근기록의 열람은 책임추적 등의 목적으로 열람(검색, 조회)할 수 있으며, 보안담당자, 감사부서 담당자를 제외한 기타 부서원은 접근기록 요청.열람신청서(별지 9호)를 작성하여 정보부서장의 승인을 받아야 한다.

② 접근기록 열람은 지정된 장소(정보부서)에서만 허용 한다.

③ 접근기록정보 이용은 목적 용도이외에는 사용하여서는 아니 되며, 개인정보보호법을 준수하여야 한다.

④ 접근기록은 다음 각 호의 경우를 제외하고는 관계직원이 아닌 일반인에게 열람하게 할 수 없다.

1. 법령에 의하여 권한이 부여된 관계 공무원의 열람 요구가 있을 때에는 그 권한의 증표를 확인하고 열람하게 한다.

2. 기타 정부 기관에서 업무 수행상 열람 요구가 있을 때에는 열람하게 한다. 단, 범죄수사와 같이 본인의 승낙을 얻을 수 없을 경우에는 전항과 같이 처리한다.

제45조(이용권한) 접근기록의 작성, 조회 및 검색권리를 의미하며 다음 각 호와 같이 구분된다.

① 정보부서는 접근기록에 대하여 조회, 검색의 권한을 갖는다.

② 전산개발담당은 중요정보의 문제 발생 및 프로그램 개발, 유지보수를 위하여 접근관리할 수 있다.

제46조(보안) 누구든지 정당한 사유 없이 접근기록에 저장된 정보를 탐지하거나 누출, 변조 또는 훼손하여서는 아니 되며 이러한 정보를 보호하기 위한 것으로 불법적인 유출이나 수정, 파괴를 막기 위하여 기술적이고 행정적인 절차와 조치를 취하여야 한다.

(별지 9호)

접근기록 요청.열람 신청서

<table>
<tr><td colspan="8">본인은 접근기록업무 관리지침 제43조 (접근기록 정보의 이용) 및 제 44조
(접근기록정보의 열람)에 의하여 아래와 같이 신청합니다.</td></tr>
<tr><td rowspan="3">신청내용</td><td>No</td><td colspan="3">프로그램명</td><td>이벤트
(수정,삭제,조회,출력)</td><td colspan="2">해당사항선택</td></tr>
<tr><td>1</td><td colspan="3"></td><td></td><td colspan="2">열람, 신청</td></tr>
<tr><td>2</td><td colspan="3"></td><td></td><td colspan="2">열람, 신청</td></tr>
<tr><td>사유</td><td colspan="7"></td></tr>
<tr><td rowspan="4">신청인</td><td>구분</td><td>소속</td><td>직위</td><td>성명</td><td>서명</td><td colspan="2" rowspan="3">* 비고</td></tr>
<tr><td>신청자</td><td></td><td></td><td></td><td></td></tr>
<tr><td>부서장</td><td></td><td></td><td></td><td></td></tr>
<tr><td>기간</td><td colspan="4">년 월 일~ 년 월 일</td><td>접수일시</td><td>년 월 일</td></tr>
<tr><td colspan="5" rowspan="3">확인자
소 속 : 직위 :
성 명 : (인)</td><td>접수자</td><td>(인)</td></tr>
<tr><td>조치일자</td><td>년 월 일</td></tr>
<tr><td>조치자</td><td>(인)</td></tr>
</table>

제7장 포털시스템 정보보안 시행세칙

제47조 (목적) 이 세칙은 포털시스템 정보보안에 관한 시행기준을 정함을 목적으로 한다.

제48조 (포털시스템 사용목적) 포털 시스템은 가상강좌, 그룹웨어, 통합정보시스템, 웹메일, 과제관리, 혁신관리, 성과관리, 지식관리, 고객관리, 도서정보시스템 등을 통합한 정보시스템이며, 이를 기반으로 한 학생/교직원별 맞춤 정보서비스를 제공한다.

제49조 (사용자 범위) 사용자 범위는 다음 각 호와 같다.

① 재직 중인 교직원

② 학부, 대학원 학생(졸업생, 휴학생 포함)

③ 강의를 맡은 당해 학기 외래강사, 겸임교수 등

④ 교외부서(부속기관, 연구소 등 이하 기타사용자)에서 포털 시스템을 사용하여 업무를 수행하여야 할 경우에 업무주관부서의 승인을 얻어 사용권한을 부여받은 직원

제50조 (사용 ID 발급 및 폐기 기준)

① 신규 임용자는 임용발령 후 종합정보시스템에 신규임용자로 입력된 시점부터 교번이 부여되며, 부여된 교번을 본인의 포털 시스템 사용자 ID로 사용한다.

② 신입생은 입학 후 종합정보시스템에 학적이 입력된 시점부터 학번이 부여되며, 부여된 학번을 본인의 포털 시스템 사용자 ID로 사용한다.

③ 신규로 강의를 맡은 해당 학기 강사로 종합정보시스템에 입력된 시점부터 교번이 부여되며, 부여된 교번을 본인의 포털 시스템 사용자 ID로 사용한다.

④ 명예퇴직자, 정년퇴직자, 졸업생, 휴학생은 재직 또는 재학 중에 개설한 사용자ID를 계속하여 사용할 수 있다. 다만, 중도 퇴직의 경우에는 변동사항이 발생한 시점에서 사용자 ID는 폐기되며 포털 시스템을 사용할 수 없다.

⑤ 외래강사는 강의를 맡은 당해 학기에 사용 권한이 부여되며, 강의를 맡지 않는 학기에는 사용자 ID는 폐기되며 포털 시스템을 사용할 수 없다.

⑥ 기타사용자는 원칙적으로 포탈 시스템에 접속 할 수 없다.

다만, 개인 ID를 발급한 경우에는 주기적으로 개인 ID 사용 및 폐기 유무를 업무주관부서에 통보하며, 업무주관부서에서는 통보받은 내용을 확인하여 ID재사용 여부를 결정하여 정보전산원에 통보한다.

제51조 (사용권한)

① 사용자 그룹별 사용권한은 업무주관부서의 승인을 얻어 부여한다.

② 휴직은 재직에 준하는 사용권한을 가진다.

제52조 (사용권한 요청 및 허가절차)

① 신규로 ID를 사용하고자 할 경우에는 정보전산원에 반드시 통보하여야 하고, 정보전산원은 사용할 수 있도록 이를 조치한다. 다만 ID 발급대상자 중에서 전자결재를 사용하여야 하는 경우에는 총무과에서 이를 심의하여 제한적으로 직원 ID를 발급한다.

② 인사이동, 학적변동, 중도퇴직 등에 의한 시스템 및 문서에 대한 사용권한 변경은 종합정보시스템에 변동사항이 입력되면 정보전산원은 해당 시스템 및 문서에 대한 권한을 7일 이내에 일괄 조치한다.

제53조 (사용권한에 대한 감사)

① 포털 시스템 내의 자료들이 사용권한을 갖지 않은 자에 의해 변조, 파괴, 분실될 경우 확인이 가능하도록 각 컴포넌트 별로 접속과 관련된 Log File(접속일시, 접속IP등)을 남기도록 한다.

② 위 감사 대상에 대하여는 기록이 자동적으로 시스템에 남도록 하며, 최소 6개월간의

기록을 유지토록 한다.

제8장 CCTV 관리운영 지침

제54조(목적) 이 세칙은 본교 정보보안 관리규정 제39조에 따라 CCTV 관리운영에 관한에 관한 시행기준을 정함을 목적으로 한다.

제55조(정의) 이 규정에서 사용하는 용어의 정의는 다음과 같다.

① “CCTV"라 함은 일정한 공간에 설치된 촬영기기로 수집한 화상정보를 폐쇄적인 유·무선 전송로를 통하여 전송함으로써 특정인만이 수신할 수 있는 통신장비 일체로서 폐쇄회로 모니터를 말한다.

② “화상정보”라 함은 CCTV로 촬영된 영상에 의하여 당해 개인의 동일성 여부를 확인할 수 있는 정보를 말한다.

③ “정보주체”라 함은 화상정보에 의하여 식별되는 사람으로서, 당해 화상정보의 주체가 되는 자연인을 말한다.

제56조(설치·운영책임자 지정) 수원대학교 내의 CCTV 설치 및 관리의 총책임자는 총무처장으로하며 운영 책임자는 환경관리과장으로 한다.

제57조(카메라 설치현황) 수원대학교내에 설치된 CCTV현황은 아래와 같은 양식으로 작성하여 홈페이지에 게시하고, 변경사항이 있을 경우 즉시 해당 내용을 수정토록 한다.

관리부서	카메라 설치 현황		설치 목적	운영시간	화상정보 관리	비고
	설치위치	수량				

제58조(안내판 부착) 안내판은 정보주체가 알아보기 쉽도록 설치된 각 실 또는 건물 입구에 부착한다.

(별지 11호 서식 참조)

제59조(정보주체의 권리행사) 정보주체는 화상정보의 존재확인 및 열람·삭제를 할 수 있다.

제60조(촬영시간) 촬영시간은 연중 00:00~24:00까지로 성능을 최대한 이용하여 촬영을 원칙으로 한다.

제61조(화상정보의 보유) 수원대학교에 설치된 CCTV는 특별한 경우를 제외하고는 화상정보를 보유하지 않는다.

제62조(화상정보의 보관) 녹화된 화상정보는 일정기간 하드디스크에 저장한다.

제63조(화상정보의 열람) 화상정보의 열람을 원할 경우 화상정보열람신청서(별지 10호)를 작성하여 총무처로 제출한 후, 결재권자의 승인을 득한 후 열람할 수 있다.

이 시행세칙은 2011년 10월 1일부터 시행 한다.

(별지 10호)

CCTV 화상정보 열람 신청서

신청자 인적사항	
소속 및 성명	
주소	
연락처	
열람 신청 내용	
열람 신청 내용	
CCTV설치장소	
열람희망 시간대	
열람목적	

20 . . .

신청인 : (서명)

접수자 : (서명)

총무처장 귀하

(별지 11호)

안내판 부착 서식

1. 출입구 안내판

CCTV 설치안내	
설치목적	시설물 보호, 화재, 도난, 범죄 예방
설치장소	00 건물
촬영시간	24시간 연속촬영 녹화
촬영범위	1층, 2층 출입구 등 구체적으로
관리책임자	환경관리과장
연 락 처	☎ 031) 220-2248

수원대학교