	PC보안관리지침	규정번호	8-0-8		
		제정일자	2013.03.01		
		개정일자			
		개정번호	Ver.0	총페이지	9

제1장 총칙

제1조(목적)
이 지침은「정보보안규칙」제37조에 의거 동양미래대학교(이하 '본 대학'이라 한다)의 PC보안 및 운용 방법에 관한 필요 사항을 규정함을 목적으로 한다.

제2조(적용범위)
이 지침은 본 대학의 전 교직원 및 본 대학을 위해 종사하는 외부인 모두에게 적용된다.

제3조(용어정의)
이 지침에서 사용되는 용어의 정의는 다음 각 호와 같다.
1. "상용 소프트웨어"란 합법적인 사용권을 얻은 후 PC에 설치하여 사용하는 소프트웨어들을 말한다.
2. "사용자"란 업무를 수행하기 위하여 PC를 이용하는 교직원을 말하며 외부인도 포함된다.
3. "패치"란 소프트웨어 회사가 프로그램 제공 후 사용자가 이용 시 발생하는 문제점을 보완하기 위하여 제공하는 프로그램을 말한다.
4. "휴대용 PC"란 노트북, 스마트폰 등 이동이나 휴대가 가능한 모든 PC를 말한다.
5. "개인정보유출방지 시스템"이라 함은 개인정보 유출 및 부정사용 방지를 목적으로 개인정보 열람이력을 생성하고 DB접근제어 등 다양한 사용 경로를 모두 감시, 기록하기 위하여 개인정보 열람이력을 생성하고, 부정사용에 대한 효과적인 감시와 부정사용자 적발을 위하여 개인정보 유출 위협에 보다 적극적으로 대처하기 위한 개인정보 부정사용 감시 시스템을 말한다.
6. 기타 용어 정의는「보안규칙」및「정보보안규칙」,「개인정보보호규칙」등에 따른다.

제4조(PC사용의 윤리)
① 본 대학에 설치된 PC는 개인적인 사업 목적이나 이익을 위하여 사용할 수 없으며, 본 대학 업무용으로만 사용하여야 한다.
② 본 대학의 PC 관련 자료를 무단을 변조하거나 훼손하지 않아야 한다.
③ 개인에게 제공된 ID와 패스워드는 절대 타인과 공유하지 않는다.
④ 타인의 ID와 패스워드를 알려고 하지 않으며, 이를 이용하여 허가 받지 않은 PC

에 임의로 접근하지 않아야 한다.
⑤ 타인의 패스워드를 무단 변경하여 업무 수행을 방해하지 않는다.
⑥ 업무상 취득한 본 대학의 정보 또는 제3자 소유의 PC관련 자료를 승인 없이 누설하지 않아야 한다.
⑦ 본 대학에서 비밀로 관리하는 정보자산은 부서별보안담당관의 승인 없이 외부로 유출하지 않아야 한다.
⑧ 저작권을 침해할 수 있는 자료를 본 대학 네트워크를 통하여 무단으로 배포하지 않는다.
⑨ PC사용자(이하 "사용자"라 한다)는 스팸메일, 불건전한 저속한 메일(자료) 등 미풍양속을 해치거나 물의를 야기할 수 있는 정보 또는 메일을 본 대학 네트워크를 통하여 유통시키지 않아야 하며, 유해사이트, P2P 등의 접속은 하지 않아야 한다.

제2장 역할과 책임

제5조(PC보안관리자)
① 부서별보안담당관은 PC보안관리자를 정하여 PC보안관리가 준수되도록 관리·감독하며 이에 필요한 보안대책을 수립·적용한다.
② PC보안관리자는 다음 각 호의 업무를 수행한다.
1. PC보안관리지침의 준수를 위한 해당 부서의 보안관리 업무
2. 주기적으로 바이러스 최신정보, 운영체제 취약점에 대한 패치 등 제공
3. 바이러스 및 불법 소프트웨어 점검
4. 기타 정보보안담당관이 PC보안 관리를 위해 필요하다고 인정하는 업무
③ PC보안관리자는 모든 사용자가 PC내의 정보보안 기능을 충분히 활용할 수 있도록 PC보안 교육프로그램을 마련하여야 하며, 주요 교육 내용은 다음 각 호와 같다.
1. PC 부팅 시 패스워드 지정 및 변경 방법
2. 부팅 시 백신프로그램 사용 방법
3. 화면보호기의 패스워드 사용으로 데이터 보호 방법
4. 공유 폴더나 파일에 대한 사용 방법
5. PC 유지보수 시에 데이터 보안 방법
6. 불법 소프트웨어 사용 시 문제점 인식
7. 바이러스 관련 정보의 주기적 홍보

제6조(PC사용자)
사용자는 자신의 PC에 대한 관리책임을 가지며, 이 지침에 따라 PC를 관리하고, 기술적인 정보보안 기능을 적용하여야 한다.
1. PC보안 교육프로그램 이수
2. PC의 비인가적 사용 방지
3. PC의 정보보안 기능 설정 및 활용
4. PC내 기밀정보 보호
5. 바이러스 감염 예방 및 검색

6. 소프트웨어 지적재산권 준수 등

제3장 PC 사용

제7조(PC사용 원칙)

① PC의 보안관리에 대한 1차적 책임은 사용자에게 있다.

② PC는 인가된 업무상의 목적을 위해서만 사용하여야 한다.

③ 교직원 및 외부인이 본인 소유의 PC를 교내로 반입하여 사용하는 경우 별지 제1호 서식 'PC사용 신청서'를 작성하여 승인을 득하여야 한다.

④ PC사용 시 자리를 비울 경우는 비밀번호가 설정된 화면보호기를 작동시키거나, 전원을 종료하여야 한다.

제8조(소프트웨어 설치제한)

① 소프트웨어는 업무상의 인가된 목적으로만 사용되어야 한다.

② 본 대학의 정보시스템을 침해하거나 우회할 수 있는 소프트웨어를 임의로 설치해서는 아니 된다.

③ 업무용 목적 이외의 프로그램(게임 등)을 설치하지 않아야 한다.

④ 상용 P2P·메신저, 웹하드 및 기타 인터넷 자료 공유 기능 등 정보유출 우려가 있는 보안에 취약한 프로그램은 사용하지 않아야 한다.

⑤ 모든 PC에는 적법한 절차에 따른 정품 소프트웨어만 설치되어야 하며, 사용권한이 없거나 임의로 복제된 불법 소프트웨어는 사용하지 않아야 하며, 사용 시 이에 대한 책임은 사용자 본인에게 있다.

⑥ 타인의 PC에 접근하거나, 정보를 수집할 수 있는 악의적인 프로그램 설치는 사용하지 않아야 한다.

제9조(사용자PC 비밀번호 설정)

① 사용자는 PC의 무단사용 방지를 위하여 분기마다 비밀번호 설정을 변경하여야 한다.

1. 1차 비밀번호(CMOS): 부팅(Booting) 시 PC확인용 비밀번호
2. 2차 운영체제 로그인 비밀번호
3. 화면보호기 비밀번호
4. 공유폴더 비밀번호

② 제1항에 대한 비밀번호 작성 규칙은 다음 각 목과 같다.

1. 최소 2종류 이상의 문자를 조합하여 최소 8자리 이상의 길이로 구성하되 문자의 종류는 다음 각 목과 같다.
   가. 영문 대문자(26개)
   나. 영문 소문자(26개)
   다. 숫자(0~9까지)
   라. 특수문자(32개)
2. 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 또는 3자리이상 연속

된 문자의 사용은 사용하지 않아야 한다.
3. 비밀번호는 유효기간을 설정하여야 한다.

제10조(화면보호기 설정)
① 모든 PC에는 화면보호기를 설정하여 사용자가 자리를 비운 사이에 비인가자가 해당 PC를 이용하는 것을 방지하여야 한다.
② 비인가자의 접근을 방지하기 위해서 사용자가 일정시간 (10분) 이상 입력이 없을 경우 비밀번호가 설정된 화면보호기가 자동으로 작동되도록 하여야 한다.
③ 화면보호기의 비밀번호 사용 및 설정 시 준수하여야 하는 세부사항은「응용프로그램보안관리지침」으로 따로 정한다.

제11조(공유폴더 관리)
① 공유폴더는 사용하지 않는 것을 원칙으로 하며, 업무상 목적에 의해 폴더를 공유할 경우 다음 각 호에 따른다.
1. 필요에 의해 파일 공유 기능을 사용 시에는 반드시 비밀번호를 설정하여야 하며, 비밀번호 사용 및 설정 시 준수하여야 하는 사항은 제9조를 적용한다.
2. 사용 완료 후에는 공유를 반드시 해제하여야 한다.
3. 파일 전달이 주된 목적일 경우에는 반드시 읽기 권한만을 주고 상대방이 쓰기를 할 경우에 있어서는 개별적으로 쓰기 권한을 설정하도록 한다.
4. 공유는 전체 데스크를 대상으로 해서는 아니 되며, 최소한의 파일만 공유하여야 한다.
5. PC에 운영체제를 설치한 후에는 디폴트 공유 폴더를 삭제하여야 한다.
6. 공동으로 사용되는 파일서버에 자료를 저장할 때는 반드시 바이러스 감염여부를 점검하여 치료 후 저장하여야 한다.

제12조(바이러스 관리)
① 모든 PC(노트북 포함)에는 대학에서 제공하는 정품 백신프로그램을 설치하여야 하고 PC 운영체제 재설치 등의 작업 후에도 백신프로그램은 즉시 설치하여 항상 정상 작동하도록 하여야 한다.
② 중앙집중형 바이러스 방역시스템을 통해 모든 사용자 PC는 백신 업데이트가 신속하게 적용되도록 하고, '사이버 보안진단의 날' 등에 주기적으로 점검되도록 하여야 한다.
③ 백신프로그램은 항상 최신 버전으로 업데이트하여 사용하여야 한다.
④ 백신프로그램 설치 후 백신프로그램에서 제공하는 실시간 감시 기능 및 예약기능을 설정하여, 다운로드한 파일이나 첨부파일이 실행되기 전 바이러스 감염여부가 자동적으로 점검되도록 하여야 한다.
⑤ 바이러스 감염여부가 검증되지 않은 프로그램이나 파일을 메일 등으로 타인에게 전송하거나 게시해서는 아니 된다.
⑥ 첨부파일이 있는 전자메일의 송·수신시에는 첨부파일의 바이러스 검사를 실행 후 수신하여야 하며, 바이러스 예방을 위해 출처가 분명하지 않은 전자메일은 열지 않도

록 한다.
⑦ 시스템에 바이러스 등이 설치되거나 감염된 사실이 발견되었을 경우, 부서별보안담당관 또는 PC보안관리자가 조치하여야 하는 사항은 다음 각 호와 같다.
1. 바이러스 감염원인 규명 등을 위하여 파일 임의삭제 등 감염시스템 사용을 중지시키고 전산망과의 접속을 분리시킨다.
2. 최신 백신프로그램을 이용하여 바이러스를 제거한다.
3. 감염이 심각할 경우 포맷 프로그램을 사용하여 하드디스크를 포맷한다.
4. 바이러스 감염 확산방지를 위하여 정보보안담당관에게 관련 내용 및 보안조치 사항을 즉시 보고한다.
5. 바이러스 감염의 재발을 방지하기 위하여 원인 분석 및 예방조치를 수행한다.
⑧ 최고보안담당관은 바이러스 신종이 발견되거나 감염 피해가 심각하다고 판단되는 경우 관련 사항을 교육과학기술부장관 및 한국인터넷진흥원장 등 관계 기관에 신속히 통보하여야 한다.

제13조(PC 보안프로그램의 설치 및 유지)
① 교내의 모든 사용자가 PC보안 관리를 위해 설치하여야 하는 보안프로그램은 다음 각 호와 같다.
1. 바이러스 방역 에이전트 및 백신프로그램
2. 기타 정보보안담당관의 승인을 득한 프로그램
② 제1항에서 설치된 프로그램을 임의로 제거해서는 아니 된다.
③ 제1항의 설치 및 업데이트가 안 되는 경우는 부서별 PC보안관리자에게 문의하여야 한다.

제4장 PC 보안관리

제14조(PC보안관리)
① 모든 사용자는 PC 부팅이 불가능하거나 하드디스크 고장과 같은 비상시에 대비하여 다음 각 호의 사항을 준수하여야 한다.
1. 중요 자료를 정기적으로 백업하여야 한다.
2. 수리가 필요할 경우를 대비하여 제조사, 모델명, 구입처, 구입일, 하드웨어 구성 내역과 배포된 소프트웨어 목록을 작성하여 관리한다.
② PC에 설치 또는 부착된 하드웨어(CD Writer, LAN카드, 착탈식 디스크 등 주변장치 포함)를 임의적으로 설치·변경·제거해서는 아니 된다.
③ PC(노트북 포함) 등의 경우 부서별보안담당관에 의해 관리되어야 하며, 일정 기간 노트북을 사용하지 않을 경우 잠금장치가 있는 안전한 장소에 보관한다.
④ 컴퓨터 사용 시 “컴퓨터 이름”이 동일하게 중복하여 사용되지 않도록 하여야 하며, 해당 부서명과 개인별 사용자 이름을 조합하여 명명하여야 한다.
⑤ 외부에서의 원격접속은 원칙적으로 사용을 금지하며, 다만 부득이하게 원격접속 사용 시는 VPN을 통해서 사용하게 할 수 있다.

제15조(휴대용 PC관리)

휴대용 PC(노트북 등)는 도난당하기 쉽고 비인가자의 접근이 용이하기 때문에 분실 및 정보 유출 위험을 최소화하기 위해 준수하여야 하는 사항은 다음 각 호와 같다.

1. 휴대용 PC(노트북 등)는 부서별보안담당관에 의해 관리되어야 한다.
2. 반입 또는 반출시 최신 백신프로그램을 이용하여 웜·바이러스 감염여부를 점검하여야 한다.
3. 사용자 출장이나 장시간 이석 시 휴대용 PC(노트북 등)를 책상위에 방치해서는 아니 되며, 잠금장치가 있는 서랍이나 캐비닛에 보관하도록 한다.
4. 업무용으로 외부에 반출한 휴대용 PC(노트북 등)는 공공장소에 방치하지 않도록 하며 장시간 이석 시에는 휴대하도록 한다.
5. 비밀번호 설정 규칙을 준수하여 도난 및 분실에 대비하여야 한다.
6. 휴대용 PC(노트북 등) 내에 저장된 비밀, 대외비 문서는 암호화를 반드시 적용하여야 하며, 필요 시 백업을 통하여 휴대용 PC(노트북 등)외 다른 장소에 보관하고 있어야 한다.
7. 휴대용 PC의 사용 시 업무 목적이 종료되었을 경우에는 PC 내부에 저장된 문서를 백업한 후 삭제하여야 한다.

제16조(인터넷 사용 및 전자메일 보안)

① 중요 자료를 저장 및 관리하는 파일서버는 인터넷 접속이 되어서는 아니 된다.

② 인터넷 상의 특정 사이트에 대해서는 정상적인 업무 활동을 위해 접속을 금할 수 있으며, 금지 대상 사이트의 유형은 다음 각 호와 같다.

1. 불건전 음란 정보를 포함하는 사이트
2. 사이버 주식, 게임, 도박, 음란사이트
3. 기타 접속 시 정보유출이 우려되는 사이트

③ 사용자는 인터넷상에서 다운로드 되는 모든 소프트웨어와 파일들은 사용 전에 바이러스 감염여부를 백신프로그램으로 점검하여야 한다.

④ 상용 P2P·메신저, 웹하드 및 기타 인터넷상에 정보 공유·저장 기능을 이용한 정보 송수신을 금지한다. 다만, 내부업무용 웹하드, 메신저를 이용하는 경우는 허용 가능하며 비밀 등 중요 자료의 저장·공유는 별도의 보안조치를 강구하여야 한다.

⑤ 본 대학의 전자메일은 업무적인 목적을 위해서만 사용되어야 하며 불법적인 용도나 불순한 목적으로 사용하지 않아야 한다.

⑥ 공식적인 메일의 송·수신 시 본 대학에서 제공하는 메일시스템 외의 사용과 타인의 전자메일 계정 사용은 금지한다.

제17조(스팸메일 보안)

① 업무적인 목적을 제외하고 외부의 웹 사이트 회원으로 가입할 경우 본 대학의 공식 메일은 사용하지 않아야 한다. 다만, 필요에 의해 메일주소를 등록할 경우 별도의 외부 메일계정을 사용한다.

② 스팸메일은 읽거나 회신하지 않고 즉시 삭제하거나 스팸메일 수신 거부로 설정한다.

제18조(PC 내부 자료의 보안관리)

① 모든 PC에는 업무상 비밀, 대외비(개인정보 포함) 및 비공개 문서가 포함된 중요정보를 보관하지 않는다. 부득이한 경우 암호화(문서 비밀번호 설정 포함) 등을 이용하여 보안성을 확보한 후 저장하여야 한다.

② PC내에 저장된 모든 문서(진행 중인 문서포함)는 본 대학의「보안규칙」,「정보보안규칙」및「개인정보보호규칙」등에 따른다.

③ PC 저장장치에는 불건전한 자료 혹은 본 대학에 손해를 줄 수 있는 자료는 보관하지 않아야 한다.

제19조(유지보수 보안)

① PC 유지보수는 인가된 직원에 의해서만 수행되어야 하며, 유지보수 업체 직원에 의해 수행될 경우 사용자 또는 내부직원의 참석 하에 유지보수가 이루어지는 것을 원칙으로 한다.

② PC 유지보수를 위하여 외부로 반출이 필요한 경우는 보안조치를 적용하여 해당 부서의 PC보안관리자에게 승인을 득하여야 한다.

③ 제2항에 따른 사용자는 PC에 하드디스크가 포함된 경우는 분리하거나, 중요한 정보가 저장된 경우는 데이터가 복구되지 않도록 삭제 프로그램을 이용하여 삭제한 후 반출하여야 하며「정보보안규칙」별지 제2호 서식 '데이터 삭제·폐기 확인서'를 제출하여야 한다.

제20조(보안사고 보고 및 대응)

① PC관련 보안사고 발생 시 사용자는 부서별보안담당관에게 보고하여야 하며, 관련 기록을 보존하여야 한다.

② PC관련 보안사고 발생 시 세부적인 대응절차는「보안사고대응관리지침」으로 따로 정한다.

제5장 소프트웨어 사용 및 PC 보안점검

제21조(불법 복제·사용의 정의)

저작권법 및 관계 법령에서 정하는 불법복제 정의에 따르며, 불법복제 범위는 다음 각 호와 같다.

1. 저작권자의 허락을 받지 않은 소프트웨어를 PC의 하드디스크, CD-ROM 등 저장매체에 복사하거나 설치하는 경우
2. 저작권자의 허락 없이 소프트웨어를 통신망에 올리거나 유선 혹은 무선으로 전송하는 행위 일체
3. 정품 프로그램의 소지 및 사용권을 계약 만료 등으로 상실한 상태에서 복제물을 보유하거나 사용하는 경우
4. 구 버전을 보유하여 사용 중에 불법복제 된 신 버전으로 업그레이드하여 사용하는 경우

5. 본 대학에서 정식으로 인가하지 않은 소프트웨어를 PC에 무단으로 설치하여 사용하는 경우
6. 타인의 PC에 저장된 매체를 불법으로 복사하여 사용하는 경우

제22조(사용자 PC보안점검)
① 사용자는 이 지침의 준수여부 확인을 위한 보안점검 및 감사업무에 적극 협조하여야 한다.
② 부서별 PC보안관리자는 해당 부서의 PC를 이용하는 교직원 및 외부인에 대해 소프트웨어 불법 복제를 포함하여 이 지침의 준용여부를 정기적으로 점검 할 수 있으며, 점검결과는 부서별보안담당관에게 보고한다.
③ 부서별 PC보안관리자는 PC보안의 중요성을 인식시키고 경각심을 제고시키기 위하여 제2항에 따른 결과를 토대로 PC보안 교육을 실시하여야 한다.
④ 소프트웨어를 불법 복제 사용으로 외부기관 단속 적발 시 1차적인 책임은 해당 사용자 본인에게 있다.
⑤ 개인정보취급책임자는 중앙집중형 개인정보유출방지 시스템을 통해 모든 개인정보취급자 PC에 대하여 개인정보를 보유하고 있는지 여부를 '사이버 보안진단의 날' 등에 정기적으로 점검하고, 이에 대한 결과를 개인정보보호책임자(CPO)에게 보고하여야 한다.

부 칙

(1) (시행일) 이 지침은 2013년 3월 1일부터 시행한다.
(2) (기타 지침과의 관계) 이 지침에서 명시되지 않았거나 명확하지 않는 사항은「개인정보보호법」,「저작권법」등 관계 법령과 본 대학의「보안규칙」및 관계 지침을 준용한다.

[별지 제1호 서식] PC사용 신청서

접수번호		신청 구분	□ 신규요청 □ 변경요청

소속/부서명		성 명	(서명)
직 위		연락처	
E-mail 주소			

PC 사양			
제조사/모델명			
CPU		메모리(RAM)	
HDD용량		USB 포트	개
O/S 종류		CD-RW	개
LAN카드 MAC주소			

업무 용도	
처리 일자	
PC보안점검 여부	

위와 같이 PC사용을 신청하오니 재가하여 주시기 바랍니다.

▸첨부: PC 보안점검 사항 (내PC지킴이 실행 후 취약점 점검결과 확인)

처리 부서 결재	
직위	서명