	응용프로그램보안관리지침	규정번호	8-0-7
		제정일자	2013.03.01.
		개정일자	2020.03.01.
		개정번호 Ver.1	총페이지 11

제1장 총칙

제1조(목적)
이 지침은 동양미래대학교(이하 “본 대학”이라 한다)의 「보안규칙」,「정보보안규칙」,「개인정보보호규칙」에 의거 응용프로그램 개발, 유지보수 및 운영에 관한 사항을 규정함을 목적으로 한다.

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

제3조(용어정의)
이 지침에서 사용되는 용어 정의는 다음 각 호와 같다.

1. “중요 정보”라 함은 노출, 변경, 파괴되면 본 대학에 중대한 영향을 미칠 수 있는 정보로서, 행정정보, 개인정보(고유식별정보 등), 인사정보 및 사용자 인증정보 등을 말한다.
2. “접근통제”라 함은 응용프로그램의 기능 및 서비스 사용 등을 위한 사용자의 권한에 대한 제한을 말한다.
3. “로그”라 함은 시스템 사용에 관련된 전체의 기록, 즉, 프로그램 사용내역, 자료변경내역, 시작시간 및 종료시간 등의 기록을 말한다.
4. “접속기록”이라 함은 사용자 또는 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
5. “암호화”라 함은 정보의 비밀성을 보장하기 위하여 암호 알고리즘에 의하여 평문을 암호문으로 바꾸는 과정을 말한다.
6. “개발보안관리자“라 함은 본 대학의 정보시스템에서 서비스되고 있는 모든 응용프로그램에 관한 개발 및 운영 업무를 담당하는 자를 말한다.
7. “계정관리자”라 함은 서비스 사용자의 업무시스템별로 계정을 생성·폐기, 권한의 관리를 수행하는 자를 말한다.
8. “서버보안관리자“라 함은 본 대학의 정보시스템에서 서비스되고 있는 서버 장비의 운영·관리 업무를 담당하는 자를 말한다.
9. 기타 용어 정의는 「보안규칙」 및「정보보안규칙」,「개인정보보호규칙」등의 용어 정의에 따른다.

제2장 책임사항

제4조(개발보안관리자)

① 개발보안관리자는 이 지침에서 정한 사항을 이행하기 위한 권한과 책임이 있다.

② 개발보안관리자는 응용프로그램의 효율적 관리 또는 보안 강화를 위해 지침서 등을 개정 할 필요가 있는 경우에 정보보안담당관에게 개정을 건의할 수 있다.

제5조(프로그램개발자)

① 프로그램개발자는 개발보안관리자의 지시에 따라 보안에 관한 사항을 적절히 이행하여야 한다.

② 프로그램개발자는 교육과학기술부의「정보보안기본지침」을 준용하여 개발하여야 한다.

③ 프로그램개발자는 한국인터넷진흥원(KISA)의 “웹서버 구축 보안점검 안내서”와 “홈페이지 개발보안 안내서”, 행정안전부의 “행정기관 등 웹사이트 운영 가이드라인”과 “홈페이지 개인정보 노출방지 가이드라인”을 준용하여 개발하여야 한다.

제3장 응용프로그램 보안

제6조(응용프로그램 개발 보안)

① 개발보안관리자는 개발환경과 운영환경이 분리된 환경에서 개발되도록 관리하여야 한다. 다만, 개발환경이 운영환경에 영향을 주지 않는 방안이 강구되었을 때 동일한 하드웨어에 구축할 수 있다.

② 프로그램개발자는 새로운 응용프로그램을 개발하여 개발시스템을 통해 충분히 테스트한 후, 운영시스템에 적용하여야 한다.

③ 컴파일러, 편집기와 같은 개발에 필요한 도구(TOOL)는 가급적 운영 환경에 설치하지 않도록 한다.

④ 개발보안관리자는 개발에 적합한 언어를 선택할 때 개발언어 별로 알려진 보안취약점들을 프로그램개발자에게 숙지시켜야 한다. 특히, 소프트웨어 개발 시 행정안전부 “정보시스템 소프트웨어 개발·운영자를 위한 소프트웨어 개발보안가이드“에 따른 시큐어 코딩 가이드(Java, C, Android-JAVA) 및 국가정보원의 8대 보안취약점 등을 고려하여 개발하도록 하여야 한다.

⑤ 개발보안관리자는 개발하고자 하는 응용프로그램의 보안요구사항이 구현되도록 하기 위한 사항은 다음 각 호와 같다.

1. 프로그램개발자는 업무와 관련하여 사용자 인증방법, 암호화 방법 등 정보보호 요건을 개발보안관리자와 협의하여 정의하여야 한다.
2. 프로그램개발자는 요건 정의 및 분석 시 기존 시스템과의 연동성, 보안 위협요인 등을 고려하여 응용프로그램 개발에 반영하여야 한다.

제7조(응용프로그램 개발 보안 통제)

① 개발보안관리자는 외부업체를 이용한 소프트웨어 개발 시 위험요소를 파악하고 보안통제를 시행하여야 한다.
② 개발보안관리자는 응용프로그램 개발 시 응용프로그램 자체 기능에 위협을 줄 수 있는 악성코드 삽입을 통제하기 위해 다음 각 호의 사항을 준수하여야 한다.
1. 프로그램개발자를 위한 보안교육 실시
2. 외주업체를 통한 응용프로그램 개발 시 운영시스템에 적용 전 사업책임자가 서명한 소스확인서 징구
3. 외주를 통한 개발 용역 시「인적보안관리지침」별지 제2호 서식 '보안서약서(외부인용)' 징구
4. 개발용 PC에 백신프로그램을 설치하여 보안업데이트를 최신으로 유지

제4장 분석 및 설계 단계

제8조(사용자 인증 설계)
사용자 인증 기능 설계 시 다음 각 호의 사항을 준수하여야 한다.
1. 인증을 수행하는 기능은 별도의 서브프로그램(모듈)화 해서 다른 부분과 독립적으로 구성하여 보안성을 강화하고, 차후 인증 수단을 변경할 경우 작업이 용이하도록 설계하여야 한다.
2. 인증시스템을 별도로 사용하는 경우, 인증시스템을 거치지 않고 응용 프로그램으로 직접 접속할 수 없도록 하여야 한다.
3. 정보통신망을 통해 사용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버 구성은 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하도록 하여야 한다.
4. 사용자 인증 없이 데이터의 접근 및 처리가 가능한 시스템 명령어를 사용하여 응용프로그램을 개발해서는 아니 된다.
5. 비밀번호의 자동 저장기능을 제공하지 않아야 하며, 사용자가 비밀번호를 입력하지 않으면 자동으로 로그인 되지 않도록 하여야 한다.

제9조(사용자ID 설계)
① 사용자ID 관리 기능 설계 시 다음 각 호의 사항을 준수하여야 한다.
1. 사용자ID는 사용자 신분과 관련된 정보(직무, 직책 등)를 포함하고 있지 않아야 하며, 사용자를 식별할 수 있도록 사용자마다 유일하게 부여되어야 한다.
2. 제품 공급 시 기본적으로 제공 받은 사용자ID 중 업무적으로 불필요한 ID는 삭제 또는 즉시 변경하여야 한다.
3. 공동ID는 부여하지 않는 것을 원칙으로 한다. 다만, 공동의 업무에 해당하는 경우에는 정보보안담당관의 승인을 득하고 관리자를 지정하여 특별 관리하여야 한다.
4. 퇴직한 사용자ID는 다른 사용자에게 재부여하여 사용하지 않도록 하여야 한다.
5. 퇴직자나 사용 목적이 만료된 사용자ID는 즉시 접근권한을 변경하여야 하며, 주기적으로 검토하여야 한다.
② 사용자ID 작성규칙을 수립하고, 이를 적용·운용하여야 하는 사항은 다음 각 호와 같다.

1. ID는 5자리 이상 20자리 이하 길이로 구성하되 문자의 종류는 다음 각 목과 같다. <개정 2020.03.01.>
 가. 영문 소문자(a~z까지 26개) <개정 2020.03.01.>
 나. 숫자(0~9까지 10개)
 다. 첫째 자리는 반드시 영문자만 허용 <개정 2020.03.01.>
 라. ID는 영문자만으로도 가능 <신설 2020.03.01.>
2. ID로 사용할 수 없는 경우는 다음 각 목과 같다. <개정 2020.03.01.>
 가. 생년월일 <신설 2020.03.01.>
 나. 학번, 교번 <신설 2020.03.01.>

제10조(비밀번호 설계)

① 개인정보취급자를 대상으로 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 하는 사항은 다음 각 호와 같다.
1. 2종류 이상의 문자를 조합하여 최소 10자리 이상 또는 3종류 이상의 문자를 조합하여 최소 8자리 이상의 길이로 구성하되 문자의 종류는 다음 각 목과 같다.
 가. 영문 대문자(A~Z까지 26개)
 나. 영문 소문자(a~z까지 26개)
 다. 숫자(0~9까지 10개)
 라. 특수문자(~ · ! @ # $ % ^ & * ( ) _ - + = { } [ ] ¦ \ ; : ‘ “ < > , . ? / 32개)
2. 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않아야 한다.
3. 비밀번호에 유효기간을 설정하여야 한다.
② 사용자의 비밀번호 설정 시 일정 수준 이하의 비밀번호는 설정되지 않도록 시스템을 구성하여야 한다.
③ 응용프로그램 개발 시 서비스 및 업무시스템을 대상으로 비밀번호를 적용하는 경우 비밀번호의 신뢰성을 보장하기 위하여 다음 각 호의 사항을 준수하여야 한다.
1. 비밀번호가 없거나 사용자 계정과 동일한 비밀번호를 허용하지 않도록 설계한다.
2. 비밀번호는 제1항제1호의 비밀번호 작성규칙을 사용하여 적용하여야 한다.
3. 초기 비밀번호는 사용자가 최초 회원가입 시에 정하도록 설계한다.
4. 입력된 비밀번호는 별표(*) 등으로 마스킹 처리되도록 설계하고 단말기의 화면에서 읽을 수 없도록 설계하여야 한다.
5. 비밀번호는 3개월마다 사용자가 변경하도록 설계하여야 한다. <개정 2020.03.01.>
6. 비밀번호 변경시 변경 전 비밀번호를 재사용하지 못하도록 설계하여야 한다. <개정 2020.03.01.>
7. 비밀번호를 입력하지 않아도 자동으로 로그인되는 것을 방지하기 위해 비밀번호의 자동 저장기능은 제공하지 않아야 한다.
8. 모든 비밀번호는「개인정보보호법」에 따른 안전한 암호화 알고리즘을 사용하여 단방향 암호화를 적용하여 저장하도록 설계하여야 한다.
④ 모든 비밀번호 작성 규칙은 이 지침에 따르는 것을 원칙으로 하며, 원칙의 적용이 어려운 경우에는 정보보안담당관의 승인을 득한 후 예외로 처리 할 수 있다. <개정

2020.03.01.>

제11조(접근통제 기능 설계)

접근통제 기능 설계 시 다음 각 호의 사항을 준수하여야 한다.

1. 동일한 계정을 이용한 이중 로그인(동시 접속 로그인)을 제한하도록 설계한다. 다만, 이중 로그인이 반드시 필요한 경우에는 정보보안담당관의 승인을 득한 후 사용할 수 있다.
2. 일정시간동안 사용하지 않을 경우 자동 로그아웃 되도록 설계한다. <개정 2020.03.01.>
3. 비인가자로 인한 ID 도용을 탐지할 수 있도록 로그인 시에는 최종 접속 일시 및 접속IP 등이 저장되도록 설계하여야 한다.
4. 일반사용자가 응용프로그램을 통하지 않고 직접적으로 DB 및 중요 정보를 가진 파일에 접근할 수 없도록 설계한다.
5. 5회 이상 로그인 실패 시 해당 계정을 잠금처리(Locking)하고, 일정시간 이후 해제될 수 있도록 설계한다.

제12조(접근권한 관리 기능 설계)

접근권한 관리 기능 설계 시 다음 각 호의 사항을 준수하여야 한다.

1. 접근 권한별로 접근 가능한 정보를 제한하여 부여된 권한 이외의 정보에는 접근이 불가능하거나 화면에 보이지 않도록 설계한다.
2. 사용자 계정은 사용자 그룹 또는 사용자 계정 별로 접근권한을 설정할 수 있도록 설계하여야 한다.
3. 계정관리자는 접근권한 설정을 변경하기 용이하도록 권한 관리 기능을 설계하여야 하고 계정관리자는 정보보안담당자의 승인을 득한 후 권한부여를 하여야 한다.
4. 모든 권한 설정 및 변경 내역은 기록이 남도록 설계하여야 하며, 별도의 로그관리시스템에 3년 이상 보관하여야 한다.
5. 모든 정보시스템은 별지 제1호 서식 '정보시스템 신분별 접근권한 관리대장'에 따라 신분별 권한이 적용되도록 설계하여야 한다. <신설 2020.03.01.>

제13조(로그설계)

① 로그 설계 시 책임추적성 확보를 위해 모든 응용프로그램은 다음 각 호에 따라 접속기록이 저장되도록 설계하여야 한다.

1. 모든 사용자의 응용프로그램 접속기록 로그는 2년 이상 보관·관리되도록 설계하여야 한다. <개정 2020.03.01.>
2. 모든 사용자의 로그인 실패 내역은 다음 각 목의 정보가 로그파일에 기록되도록 설계하여야 한다.

가. 로그인 연속 실패 로그(실패한 사용자 계정, 실패 횟수, IP, 일시, 시간)

3. 접속기록 로그는 접속계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무, 처리 정보주체 건수를 포함 하여야 한다. <개정 2020.03.01.>

가. <삭제 2020.03.01.>

4. 사용자의 개인정보를 다운로드하여 저장 시에는 '개인정보의 안전성 확보조치 기

준’의 내부관리계획을 따른다. <개정 2020.03.01.>
가. <삭제 2020.03.01.>
5. 중요 개인정보를 취급하는 응용프로그램은 자세한 로그를 남길 수 있도록 설계한다.
② 저장된 접속기록은 서비스 제공 시 위·변조되지 않도록 관리하여야 한다.

제14조(암호화)
응용프로그램 개발 시 중요 정보(개인정보, 민감정보, 비밀번호 등)는 기밀성 유지를 위한 보안대책을 마련하여 다음 각 호의 사항을 적용하여야 한다.
1. 개인정보처리시스템은 안전한 암호 알고리즘(SEED, SSL, SHA-256 등)을 사용하여 저장하여야 한다.
2. 개인정보처리시스템은 충분한 키 길이(최소한 대칭키128bit이상, 비대칭키 2048bit 이상, 해쉬함수 128bit이상)를 가진 암호 알고리즘으로 사용하여야 한다.

제15조(중요 정보노출 방지)
① 개인정보를 비롯한 중요 정보가 사용자에게 노출되지 않도록 응용프로그램 설계 시 다음 각 호의 사항을 준수하여야 한다.
1. 권한이 없는 사용자가 학생 및 교직원 정보 등 중요 정보에 접근 할 수 없도록 설계하여야 하며, 권한이 있는 경우에도 업무성격에 맞는 정보만 표시 될 수 있도록 설계한다.
2. 응용프로그램에서 사용자의 정보가 노출되지 않도록 암호화하여 처리하고 응용프로그램 화면에서는 소스 보기 기능 차단 등을 통해 사용자의 인증 정보가 노출되지 않도록 설계하여야 한다.
② 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보 보호를 위하여 적절한 표시 제한 조치를 취하여야 한다. <개정 2020.03.01.>
1. <삭제 2020.03.01.>
2. <삭제 2020.03.01.>
3. <삭제 2020.03.01.>
4. <삭제 2020.03.01.>
5. <삭제 2020.03.01.>

제5장 개발단계

제16조(개발환경)
개발환경 보안은 다음 각 호에 따른다.
1. 비 인가자의 출입이 물리적으로 통제된 작업공간에서 개발이 이루어져야 한다.
2. 비 인가자의 접근으로부터 보호하기 위한 보안대책을 강구하여야 한다.
3. 프로그램개발자의 응용프로그램 및 소스코드 접근은 공식화된 경로만을 사용하여야 한다.
4. 프로그램개발자 PC는 컴퓨터 바이러스나 각종 보안 사고로부터 보호되어야 한다.

제17조(응용프로그램 계정관리)

① 프로그램개발자는 응용프로그램 개발서버 접근을 위한 계정이 필요한 경우「서버보안관리 지침」별지 제4호 서식 '사용자계정(신규, 변경, 삭제) 신청서'를 작성하여 계정관리자에게 요청하여야 한다.

② 계정관리자는 요청서를 검토한 후, 프로그램개발자에게 별도 계정을 부여하여야 한다.

③ 프로그램개발자는 개발 종료 후, 개발서버에 접근했던 계정에 대해서「서버보안관리 지침」제4호 서식 '사용자계정(신규, 변경, 삭제) 신청서'를 작성하여 계정관리자에게 계정 삭제를 요청하여야 한다.

제18조(개발도구 및 소프트웨어 사용)

프로그램개발자는 특별한 사유가 없는 한 자체 응용프로그램 개발 시 신뢰할 수 있는 개발도구나 기술을 사용하여야 하며, 정상적으로 구매 또는 사용권한을 획득하지 않은 소프트웨어는 사용하지 않아야 한다.

제19조(개발정보에 대한 접근통제)

① 개발정보는 개인을 식별할 수 있는 프로그램개발자의 개별 계정을 통해 접속하고, 개발보안관리자로부터 접근 권한을 부여 받아야 한다.

제20조(테스트 데이터 사용)

테스트 데이터가 필요한 경우 프로그램개발자는 별지 제2호 서식 '테스트 데이터 (삭제, 이관) 신청서'를 제출하고, 개발보안관리자는 운영 데이터를 가공하여 승인을 득한 후 제공하여야 한다.

제21조(변경관리 및 테스트)

① 개발보안관리자는 소스프로그램의 변경이력을 관리하여야 한다. <개정 2020.03.01.>

② 프로그램개발자는 응용프로그램의 변경이 발생하는 경우에는 개발보안관리자와 협의하여 변경하여야 한다.

③ 프로그램 변경은 사용자의 요청에 의해 변경관리가 이루어지며, 개발보안관리자의 승인을 득한 후에 적용하고 테스트를 수행하여야 한다.

④ 개발보안관리자는 테스트를 수행할 때에는 다음 각 호에 따른다.

1. 개발보안관리자는 운영 데이터의 노출을 방지하기 위해 임의의 테스트 데이터를 생성하여 활용하거나 운영 데이터를 변조하여 테스트에 사용한다.
2. 테스트 환경은 이관 대상 운영 환경과 동일한 상태로 구성하여 테스트의 신뢰성을 보장하여야 한다.
3. 개발보안관리자는 요구사항에 각 구성 요소를 시험할 수 있도록 테스트 계획서 및 테스트 시나리오 작성을 요청하여야 한다.
4. 개발보안관리자는 수립된 테스트 계획에 따라 테스트 수행 후 예상 결과와 실제 테스트 결과를 검토하여 상이한 경우 개발자에게 보완을 요구하여 테스트 수행을 재진행하여야 한다.
5. 테스트가 완료된 응용프로그램은 개발보안관리자가 운영 환경으로 이관하며, 정보보안

담당관에게 보고할 수 있다.

제6장 운영환경 및 이관 단계

제22조(운영환경 이관)

① 운영 환경 이관 전 공식화된 접근권한을 제외한 모든 접근경로와 불필요한 권한 설정은 제거하여야 한다.
② 이관 작업 시 개발 완료된 응용프로그램에 대한 일체의 변경을 금한다.
③ 운영환경 이관 시 운영 프로그램 소스, 라이브러리, 컴파일 된 이진 파일의 변경에 대한 이력을 관리하여야 한다.
④ 테스트 중이거나 개발 중인 프로그램은 운영환경 이관을 금지한다.

제23조(운영환경 응용프로그램 관리)

① 개발보안관리자는 서버보안관리자와 협의하여 프로그램 소스코드에 대한 접근을 엄격하게 통제하여야 한다.
1. 프로그램 소스 코드에 대한 사용자 접근을 통제하여야 한다.
2. 프로그램 소스 코드에 대한 모든 접근기록을 남겨야 한다.
3. 프로그램 소스 코드에 대한 복사 및 유지보수는 엄격한 접근 계정관리 등의 통제가 이루어져야 한다.
4. 프로그램 소스 코드에 보안 위협 코드의 삽입을 금지하여야 한다.
② 컴파일러, 편집기와 같은 개발에 필요한 도구(TOOL)는 운영시스템 서버로의 접근을 엄격히 통제하여야 한다.

제7장 응용프로그램 접근권한

제24조(응용프로그램 접근통제)

① 개발보안관리자는 응용프로그램 접근통제는 다음 각 호에 따른다.
1. 사용자의 신분에 따라서 그룹별 접근통제
2. 시스템의 메뉴(대분류~소분류)에 따라서 사용자별 접근권한 부여
② 사용자는 응용프로그램 개발서버 접근을 위한 계정이 필요한 경우「서버보안관리 지침」별지 제4호 서식 ‘사용자계정(신규, 변경, 삭제) 신청서’를 작성하여 계정관리자에게 요청하여야 한다.
③ 계정관리자는 요청서를 검토한 후, 업무수행에 필요한 최소한의 범위 내에서 사용자에게 별도 계정을 부여하여야 한다.
④ 사용자는 퇴직·보직이동 시 운영서버에 접근했던 계정에 대해서「서버보안관리지침」제4호 서식 ‘사용자계정(신규, 변경, 삭제) 신청서’를 작성하여 계정관리자에게 계정 삭제를 요청하여야 한다.

제25조(접근권한 부여 방법)

① 신분에 따른 접근통제는 사용자의 편의성을 고려하고, 접근권한 설정은 메뉴별로 정

보보안담당관의 승인 후 부여한다.
② 화면메뉴 접근통제는 업무 효율성을 고려하고, 접근권한 설정은 메뉴별로 부서별보안담당관의 요청에 따라 부여한다.

부 칙

(1) (시행일) 이 지침은 2013년 3월 1일부터 시행한다.
(2) (예외적용) 다음 각 호에 해당하는 경우에는 이 지침에서 규정한 내용일지라도 정보보안담당관의 승인을 받아 예외 취급할 수 있다.
1. 운영환경에서 직접 소스코드를 수정하여야 하는 긴급한 경우
2. 기술적, 관리적 필요에 따라 지침의 적용을 보류할 긴급한 사유가 있는 경우

부 칙

(1) (시행일) 이 지침은 2020년 3월 1일부터 시행한다.

[별지 제1호 서식] 정보시스템 신분별 접근권한 관리대장

정보시스템 신분별 접근권한 관리대장

No	시스템명	전임교원						비전임			직원							학생				퇴직자
		일반	실습	강의	산학협력중점	산업체경력	실습전담	겸임	초빙	강사	일반직	기술직	교육행정직	계약직(학부)	계약직(부서)	산학협력단직원	촉탁직	재학생	휴학생	졸업생	제적생	
1																						
2																						
3																						
4																						
5																						
6																						
7																						
8																						
9																						
10																						
11																						
12																						

[별지 제2호 서식] 테스트 데이터 (삭제, 이관) 신청서

테스트 데이터 (삭제, 이관) 신청서

신청 구분		□ 삭제 □ 이관	소속/성명	
신 청 일			완료 요청일	
전화번호 (휴대폰)			이메일 주소	
신청 정보	신청 데이터			
	신청 사유			
승인 정보	사용 기간	20 . . . ~ 20 . . .		
	승인 데이터			
	승인 조건			
	비 고			

「응용프로그램보안관리지침」에 따라 위와 같이 신청하오니 재가하여 주시기 바랍니다.

처리 부서 결재	
직위	서명