	암호 키 관리지침	규정번호	8-0-18		
		제정일자	2017.04.17		
		개정일자			
		개정번호	Ver.0	총페이지	7

제1장 총칙

제1조(목적)

본 지침은 「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」의 '개인정보의 보호', '정보통신망의 안전성 확보' 등 관계 법령의 규정을 토대로, 동양미래대학교(이하 '대학'이라고 함)의 중요 정보 자산에 대해 기밀성, 무결성, 인증 및 부인 방지 등을 보장하기 위한 암호화를 적용하는데 있어 필요한 사항들을 규정하는데 그 목적이 있다.

제2조(적용 범위)

대학의 중요 정보자산을 기밀/일반 데이터로 분류하고, 기밀 데이터로 분류된 모든 데이터들에 대해서 암호화를 적용한다.

제3조(용어 정의)

이 지침의 목적을 위해 다음의 용어 정의가 적용된다.

1. 암호화(Encryption) : 암호화 기법 및 프로그램을 사용하여 평문 정보를 알아볼 수 없는 정보로 변환하는 과정
2. 복호화(Decryption) : 암호화 기법 및 프로그램을 사용하여 암호화된 정보를 다시 평문 정보로 변환하는 과정
3. 암호화 키(Encryption Key) : 암호화 및 복호화를 수행하기 위해 암호화 기법 및 프로그램에서 사용하는 키
4. 암호화 패스워드(Encryption Password) : 기밀 데이터를 암호화 및 복호화하기 위해 사용하는 패스워드
5. 인증 패스워드(Authentication Password) : 시스템에 접근하기 위해 사용자 인증 시 사용하는 패스워드
6. 데이터베이스(Database) : 기업이나 조직체의 활동에 필요 불가결한 자원이 되는 대량의 정보를 수집, 관리하는 데이터 집합
7. 가상 사설 통신망(VPN, Virtual Private Network) : 공중망상에 사설망을 구축하여 마치 사설 구내망 또는 전용망 같이 이용하는 통신망
8. 보안 소켓 계층(SSL, Secure Sockets Layer) : 데이터를 송수신하는 두 컴퓨터 사이, 종단 간 즉 TCP/IP 계층과 애플리케이션 계층 사이에 위치하여 인증, 암호화, 무결성을 보장하는 업계 표준 프로토콜

제4조(책임 사항)

1. 정보보안담당관 : 대학의 전반적인 보안 계획을 수립 관리하는 자로 대학에서 1명을 선정하여, 암호화 기술 및 프로그램 등 암호와 관련된 모든 사항들에 대해서 최종 승인과 총괄적인 관리를 담당한다. 그리고 기술의 발달에 따라 암호화 기술 및 프로그램, 키의 기준을 검토하고 개정할 의무를 가진다.
2. 정보보안담당자 : 정보보안담당관의 업무수행을 보좌 및 업무 지원을 위해 보안 및 정보보안의 기술적인 실무를 수행하여야 하며, 암호화 기술 및 프로그램의 도입 또는 개발과 암호화 키 관리 등을 담당한다.
3. 사용자 : 암호화 기술 및 프로그램을 실제로 사용하는 자로 정보를 다루는 대학의 모든 직원이 이에 해당되며, 정보보안담당관이 승인한 암호화 기술 및 프로그램만을 사용해야 한다.

제2장 암호화 기술

제5조(암호화 기술 및 프로그램 선택 기준)

1. 암호화 기술 선택기준

① 암호화 기술은 다음의 사항들을 만족하는 암호화 기술 중에서 기밀 데이터의 보안성, 성 능, 호환성 및 목적 등을 고려하여 정보보안담당자가 선택 및 검토하고, 정보보안담당관이 최종 승인한다.

② 기밀성을 위한 암호 기술은 최소 128 비트 암호화키를 사용하는 시드 블록 암호 알고리즘(SEED) 이상 또는 이에 준하는 안전성이 입증된 대칭키 암호화 알고리즘을 이용한다.

③ 무결성 또는 전자 서명을 위한 암호 기술은 각각 최소 SHA-256과 RSA-2048 비트 이상 또는 이에 준하는 안전성이 입증된 해시 함수와 비 대칭키 암호화 알고리즘을 이용한다.

2. 암호화 프로그램의 선택 기준

암호화 프로그램은 다음의 사항들을 고려하여 정보보안담당자가 선택 및 검토하고, 정보보안담당관이 최종 승인한다.

① 사용 목적
② 시스템의 적합성 여부 및 암호화 키 관리 방안
③ 시스템 구성도 및 동작 프로토콜
④ 시스템 구성 요소별 기능 및 제원
⑤ 보안 서비스 요구 사항

제6조(암호화 기술 및 프로그램 적용 대상)

암호화 기술 및 프로그램 적용 대상은 크게 데이터의 저장, 데이터의 접근 제어, 네트워크를 통한 데이터의 송수신으로 분류한다.

1. 데이터의 저장

구 분	적용 대상
개인 PC/노트북	내부 또는 외부에서 개인이 사용하는 PC/노트북에 저장하는 내부보안 문서 등의 기밀 데이터
데이터베이스	내부 서버에 저장하는 고객정보, 보안 시스템 정책, 네트워크 구성도 등의 기밀 데이터
이동식 저장매체	분실 위험이 있는 이동 가능한 디스크, USB 메모리 등의 저장매체에 저장하는 기밀 데이터
기타	그 외 컴퓨팅 디바이스와 저장매체들에 저장하는 기밀 데이터

2. 데이터의 접근 통제

구 분	적용 대상
개인 PC/노트북	개인 사용자 기반의 컴퓨터 시스템에 대한 사용자 인증
서버	데이터베이스와 같은 공용 자원을 다수의 사용자가 이용할 수 있도록 서비스를 제공하는 컴퓨터 시스템에 대한 사용자 인증
이동식 저장매체	전산화된 정보를 저장하는 장치로서 이동 가능한 디스크, USB 메모리 등의 저장매체에 대한 사용자 인증
외부에서 내부 시스템 접근	내부 직원들이 회사 외부에서 내부 시스템으로 접근하는 경우 사용자 인증
기타	그 외 인가된 사용자만이 기밀 데이터에 접근 가능하도록 인증이 필요한 대상들에 대한 사용자 인증

3. 네트워크를 통한 데이터의 송수신

구 분	적용 대상
메일	메일을 사용하여 내부 또는 외부와 송수신하는 기밀 데이터
메신저	메신저를 사용하여 내부 또는 외부와 중요한 내용의 대화 및 송수신하는 기밀 데이터
서버와 클라이언트	내부 서버와 외부 클라이언트 사이에 송수신하는 로그인 정보(패스워드)와 같은 기밀 데이터
기타	그 외 네트워크에서 송수신하는 기밀 데이터

제7조(적용 대상에 따른 암호화 기술 및 프로그램)

제6조(암호화 기술 및 프로그램 적용 대상)에서 분류한 적용 대상들은 다음과 같은 암호화 기술 및 프로그램을 사용해야 한다.

1. 데이터의 저장

① 개인 PC/노트북은 개인용 또는 기업용 파일 암호화 프로그램을 사용하며, 파일 암호화 프로그램을 사용하지 않는다면, 파일과 폴더는 운영체제 및 압축 프로그램에서 제공하는 암호화 기능을 사용한다. 문서 파일은 문서 프로그램에서 기본적으로 제공하는 암

호화 기능이나 PDF 생성 시 제공하는 보안 기능을 사용한다.
② 데이터베이스는 데이터베이스 암호화 전용 프로그램이나 데이터베이스 관리시스템을 사용해야 하며, 다양한 기능을 제공하는 데이터베이스 암호화 전용 프로그램을 사용한다.
③ 이동식 저장 매체에서 암호화 기능을 제공하는 보안 USB 등의 저장 매체들은 반드시 인증 패스워드를 설정하여 보안 기능을 사용하고, 풀 디스크 암호화 프로그램을 사용한다. 보안기능이 없거나 풀 디스크 암호화 프로그램을 사용하지 않는 경우에는 매체에 기밀 데이터를 저장할 때, 각 파일을 암호화한 후에 저장한다.
④ 기타 그 외 컴퓨팅 디바이스와 저장 매체들은 각각에 알맞은 암호화 기술 및 프로그램을 사용한다.

2. 데이터의 접근 통제
① 개인 PC/노트북은 부팅 시 CMOS와 운영체제에서 제공하는 로그인 인증 패스워드를 설정하여 사용한다. 또한, 화면보호기를 설정하여 일정시간 자리를 비울 경우 화면 보호기가 자동 실행되도록 하고 재로그인 시 패스워드가 필요하도록 한다. 공용 PC/노트북인 경우 사용자의 수만큼 계정을 생성하고, 각각 다른 인증 패스워드를 사용 한다.
② 서버는 부팅 시 CMOS와 운영체제에서 제공하는 로그인 인증 패스워드를 설정하여 사용한다. 또한, 화면보호기를 설정하여 일정 시간 자리를 비울 경우 화면보호 기가 자동 실행되도록 하고 재로그인 시 패스워드가 필요하도록 한다. 서버 관리자가 여러 명인 경우 관리자의 수만큼 계정을 생성하고, 각각 다른 인증 패스워드를 사용한다. 인증 패스워드를 주기적으로 변경하고, 인증 패스워드가 지정되지 않은 계정이나, 불필요한 계정들은 제거한다.
③ 사용자 식별/인증기능 및 암호화 기능을 제공하는 보안 USB 등의 저장 매체들은 반드시 인증 패스워드를 설정하여 보안 기능을 사용해야 하고, 그렇지 않은 저장 매체들은 기밀 데이터 파일을 저장할 때, 각 파일을 암호화한 후에 저장한다.
④ 외부에서 내부 시스템 접근은 인가된 사용자라 할지라도 공개키 기반 구조(PKI, Public Key Infrastructure) 기반의 강화된 인증 방법을 사용하고, 가상 사설 통신망(VPN) 등의 추가적인 보안 시스템을 통해 접근을 통제한다.
⑤ 기타 그 외 인가된 사용자만이 기밀 데이터에 접근 가능하도록 인증이 필요한 대상들은 각각에 알맞은 암호화 기술 및 프로그램을 사용한다.

3. 네트워크를 통한 데이터의 송수신
① 메일의 경우 OpenPGP(Open Pretty Good Privacy), S/MIME(Security services for Multipurpose Internet Mail Extension) 등의 이메일 보안 프로토콜을 사용하거나 메일 암호화 프로그램을 사용한다. 추가적인 프로그램을 사용하지 않는다면, 사용자가 사용 하고 있는 메일 클라이언트 소프트웨어에서 제공하는 메일 암호화 기능을 사용한다.
② 메신저는 소프트웨어에서 기본적으로 제공하는 대화 암호화 기능 및 파일 암호화 전송 기능을 사용하거나, 메신저 암호화 프로그램을 사용하여 대화하고 기밀 데이터를 송수신 한다. 이러한 기능을 제공하지 않는다면, 메신저를 통한 중요한 내용의 대화는 삼가고, 기밀 데이터 전송 시 파일을 사전에 암호화하여 전송한다.
③ 서버와 클라이언트는 보안 소켓 계층(SSL) 및 전송 계층 보안(TLS) 프로토콜 등과 같

은 통신 암호 기술이나 관련 프로그램을 이용해야 하며, ID/패스워드, 계좌번호 및 신용카드 번호, 그 외 개인 정보 등을 암호화하여 송수신 한다.
④ 기타 그 외 네트워크에서 기밀 데이터를 송수신하는 경우 각각에 알맞은 암호화 기술 및 프로그램을 사용한다.

제8조(암호화 기술 및 프로그램 운용)
암호화 기술 및 프로그램은 정보보안담당관의 승인을 얻어 본 지침에서 명시하고 있는 국내외 표준 암호화 기술 및 이를 이용한(또는 탑재한) 프로그램만을 사용해야 한다. 부득이한 경우 본 지침에서 정하지 않은 암호화 기술 및 프로그램을 사용하기 위해서는 반드시 정보보안담당자의 검토와 정보보안담당관의 승인을 얻어야 한다. 정보보안담당관은 사용 중인 암호화 기술 및 프로그램에 대해서 3개월 주기로 적용 현황, 신뢰수준의 적절성 등을 포함한 보안 감사를 실시한다.

제3장 암호 키 관리

제9조(키 관리)
키 관리는 암호화 키와 패스워드의 선택, 관리, 복구 항목으로 분류하여 규정하고, 정보보안담당관은 사용 중인 암호화 키 및 패스워드에 대해서 3개월 주기로 관리 현황, 암호화 키 및 패스워드 길이의 적절성 등을 포함한 보안감사를 실시한다.

제10조(암호화 키 및 패스워드 선택 기준)
① 암호화 키의 길이는 전수 조사 공격(가능한 모든 경우의 수를 시행하여 키를 찾아내는 공 격)에 의한 피해를 막기 위해 대칭키 암호 알고리즘의 암호화 키는 128 비트 이상, 비 대칭 키 암호 알고리즘의 암호화 키는 2048비트 이상이어야 한다.
② 패스워드의 길이 및 문자 구성에서 패스워드는 3가지 종류(대문자, 소문자, 특수문자, 숫자 등) 이상의 문자 구성으로 8 자리 이상의 길이 또는 2가지 종류 이상의 문자 구성으로 10 자리 이상의 길이여야 한다. 또한, 다음과 같은 기준을 따라야 한다.
- 한글, 영어 등의 사전적 단어를 포함하지 않는다.
- 널리 알려진 단어를 포함하지 말고 예측이 어렵도록 만든다.
- 사용자 ID와 연관성이 있는 단어 구성을 포함하지 않는다.
- 제3자가 쉽게 알 수 있는 개인정보를 포함하지 않는다.
- 해당 시스템에서 이전에 사용하지 않은 새로운 문자 구성을 사용한다.
- 이전의 문자 구성과 연관된 문자 구성을 사용하지 않는다.

제11조(암호화 키 및 패스워드 관리)
1. 암호화 키
① 암호화 키 생성 : 기밀 데이터를 암호화할 경우 정보보안담당자의 승인을 받아 생성하고 ‘암호화 키 관리 대장’에 기록한다.
② 암호화 키 사용 : 접근이 인가되지 않은 사용자는 암호화 키를 사용할 수 없도록 강력하게 접근을 통 제해야 하며, 접근이 인가된 사용자 외에게는 암호화 키가 노출되지

않도록 철저하게 관리해야 한다. 또한, 암호화 키는 노출 위협을 최소화하기 위해 1년마다 변경해야한다. 그 외에도 암호화 키의 생성·사용 및 폐기 기록을 관리하는 '암호화 키 관리 대장'에 대한 접근은 정보보안담당자가 관리하며, 내화 금고 등에 보관하는 등 암호화 키를 관리하는 수준의 강력한 접근 통제가 필요하다.
③ 암호화 키 폐기 : 암호화 키는 사용 용도가 종료되거나 사용 주기가 만료된 경우 폐기한다. 암호화 키는 정보보안담당자가 폐기하고 '암호화 키 관리 대장'에 기록한다.

2. 패스워드
① 패스워드 생성 : 개인 패스워드는 사용자가 직접 생성하고 그룹 패스워드는 그룹의 장이 생성하여 구성원들에게 안전한 방법을 통해 전달한다.
② 패스워드 사용 : 패스워드는 제3자에게 노출되지 않도록 해야 하며, 자신의 패스워드와 관련된 정보 및 힌트를 제공하지 않아야 한다. 패스워드 변경 주기는 3개월이다. 시스템 및 소프트웨어의 기본 제공 패스워드는 설치 시 즉시 변경해야 한다.
③ 패스워드 폐기 : 패스워드는 사용 용도가 종료되거나 사용 주기가 만료된 경우 폐기한다. 인증 패스워드는 시스템 담당자가 사용자 계정의 삭제와 함께 폐기하고, 암호화 패스워드는 사용 자가 직접 폐기한다.

제12조(암호화 키 복구)
암호화 키의 복구는 암호화 키 소유자의 퇴사 등의 사유로 암호화 키를 알 수 없을 경우 정보보안담당관의 승인을 받아 '암호화 키 복구 대장'에 기록하고, '암호화 키 관리 대장'에서 암호화 키를 복구한다. '암호화 키 복구 대장'에 대한 접근은 정보보안담당자가 관리하며, 내화금고 등에 보관하는 등 암호화 키 수준의 강력한 접근 통제가 필요하다.

제4장 문서 및 기록

제13조(예외 규정)
본 지침에서 명시한 내용일지라도 다음에 해당하는 경우에는 정보보안담당관의 승인을 받아 예외 취급할 수 있다.
- 기술 환경의 변화로 적용이 불가능할 경우
- 기술적, 관리적 필요에 따라 암호 정책의 적용을 보류할 긴급한 사유가 있을 경우
- 기타 재해 등 불가항력적인 상황일 경우

제14조(경과 조치)
특별한 사유에 의하여 본 지침을 따르지 못하는 경우 시행일로부터 1년 이내에 개선 방안을 강구한다.

제15조(관련 서식)
- [관련서식 1] 암호화 키 관리 대장

부 칙

(1) **(시행일)** 이 규칙은 2017년 4월 17일부터 시행한다.