| | 보안시스템관리지침 | 규정번호 | 8-0-5 | | |
|---|---|---|---|---|---|
| | | 제정일자 | 2013.03.01 | | |
| | | 개정일자 | | | |
| | | 개정번호 | Ver.0 | 총페이지 | 7 |

## 제 1장 총칙

**제 1조 (목적)**

이 지침은 동양미래대학교(이하 "본 대학"이라 한다)의 「보안규칙」,「정보보안규칙」내 보안시스템의 운영 관리에 관한 사항을 규정함을 목적으로 한다.

**제 2조 (적용범위)**

이 지침은 본 대학의 전 교직원 및 본 대학을 위해 종사하는 외부업체 직원 모두에게 적용된다.

**제 3조 (용어정의)**

이 지침에서 사용되는 용어의 정의는 다음 각 호와 같다.

1. "보안시스템" 이라 함은 정보의 수집, 가공, 저장, 검색, 송·수신 중에 나타나는 정보의 훼손, 변조, 유출 등을 방지하기 위한 기술적 수단으로써 방화벽, 침입차단시스템, 침입탐지시스템, VPN(가상사설망) 등이 이에 해당한다.
2. "원격근무"라 함은 정보통신망을 활용하여 업무의 전체 또는 일부를 소속기관 사무실 이외의 환경에서 수행하는 근무 형태로써 재택근무, 파견근무, 이동근무를 포함하는 개념을 말한다.
3. "침입차단시스템"라 함은 정보통신망간의 상호접속이나 데이터 전송을 안전하게 통제하기 위하여 신분확인, 접근통제, 무결성, 비밀성, 감사기록 및 추적, 보안관리 기능을 제공하는 소프트웨어 및 하드웨어를 말한다.
4. "침입탐지시스템"라 함은 외부 침입자가 시스템의 자원을 정당한 권한 없이 불법적으로 사용하는 시도 또는 내부 사용자가 자신의 권한을 오용, 남용하는 침입 시도를 탐지하고 대응하는 것을 목적으로 하는 소프트웨어나 하드웨어를 말한다.
5. "보안시스템관리자"라 함은 본 대학에 설치된 보안시스템을 운영하는 업무를 담당하는 자를 말한다.
6. 기타 용어정의는「보안규칙」및 「정보보안규칙」,「개인정보보호규칙」의 용어정의에 따른다.

## 제2장 책임사항

**제4조(보안시스템관리자)**

① 보안시스템관리자는 보안시스템의 운용·관리를 수행하며, 다음 각 호의 책임이 있

다.
1. 보안시스템 운용·관리 지침을 수립·변경·시행
2. 보안시스템 운용·관리(필터링 정책, 접근권한, 관리 등)
3. 보안문제에 대한 신속한 해결 및 패치
4. 주기적 보안점검 수행 및 보고

② 보안시스템을 보안관제 외주용역업체에 위탁 운영하는 경우 외주용역업체는 이 지침에 명시된 내용을 준수하여야 하며, 관련 내용을 협약서 또는 계약서에 명시하여야 한다.

③ 보안시스템관리자는 보안시스템 도입 후 환경에 맞는 설정 등 최적화 작업을 수행하여야 한다.

## 제3장 보안시스템

### 제5조(보안시스템 도입 계획)

① 침입차단시스템 및 침입탐지시스템 등의 보안시스템 도입 계획 시에는 조직의 성격, 정책, 네트워크 형태, 시스템의 성능 및 안정성, 사용자 편의성, 관리자의 기술·운용 수준 등의 다양한 요소들을 고려하여야 한다.

② 보안시스템관리자는 보안시스템 도입을 검토하는 경우 별지 제1호 서식 '보안성검토 신청서'를 작성하여 정보보안담당관에게 보안성 검토를 요청할 수 있다.

### 제6조(보안시스템 설치)

① 보안시스템은 무정전 전원공급 장치(UPS), 과전압 보호장치, 에어컨, 화재경보기 등의 장치에 의해 적절한 운영환경이 보장된 곳에 위치하도록 한다.

② 보안시스템 설치작업은 설치, 운영 및 관리를 담당하는 인가된 사람으로 제한하여야 한다.

③ 보안시스템 설치 작업 시 다음 각 호의 사항을 확인하여야 한다.
1. 시스템 사양(CPU, 메모리, 하드디스크 등)은 충분한지 점검한다.
2. 시스템 운영체제 버전을 확인한다.
3. 설치될 OS의 취약성, 최신패치의 여부 등을 점검한다.

④ 보안시스템관리자는 보안시스템 설치 시 업무 중요도에 따른 보안등급을 설정하고설치 완료 후 정보자산의 위험평가 후「정보보안규칙」별지 제4호 서식 '정보자산목록(표)'에 추가하여 관리하여야 한다.

### 제7조(보안시스템 운용 및 보안관리)

① 보안시스템관리자는 보안시스템 운용 및 관리를 위해 교육을 이수하여야 하는 사항은 다음 각 호와 같다.
1. 최근 정보보안 동향
2. 운용관리 직무기술
3. 시스템 취약점 분석 및 보안진단 방법
4. 침해사고 발생 시 긴급조치 등

② 보안시스템에서 상용 P2P·메신저, 웹하드 및 기타 업무에 불필요한 서비스 사용을 금지하고 관련 서비스 포트를 차단하도록 하여야 한다.
③ 주기적으로 다음 각 호의 사항을 점검하여 매월 월간점검보고서를 작성하여 정보보안담당관에게 보고하여야 한다.
④ 보안시스템관리자는 보안시스템의 로그를 상시 모니터링하여야 하며, 로그점검 결과를「서버보안관리지침」별지 제6호 서식 '로그점검 관리대장' 을 작성하여 정보보안담당관에게 보고하여야 한다.
⑤ 보안시스템의 중요 설정 내용은 백업하여야 하며, 로그는 6개월 이상 보관 및 별도의 방법으로 보관, 관리한다.

**제8조(변경 및 업그레이드)**
① 보안시스템관리자는 보안시스템의 업그레이드가 필요한 지의 여부를 확인하기 위해 분기별 1회 이상 검토하여야 한다.
② 새로운 보안기술의 적용과 보안시스템의 버그에 대한 주기적 검토로 보안시스템을 안정적으로 운영하고, 외부 네트워크에서의 새로운 침입에 대비할 수 있도록 하여야 한다.
③ 보안시스템 소프트웨어에 변경이 필요한 경우 보안시스템관리자는 정보보안담당관에게 보고하고 변경작업을 수행한다.
④ 모든 보안시스템의 업그레이드 파일, 자료들은 신뢰할 수 있는 공급업체 및 외주업체로부터 제공 받아야 한다.
⑤ 업그레이드 후에는 보안시스템이 정상 동작하는 지 여부를 검증하고 운영에 들어가야 한다.

**제9조(보안시스템 접근통제)**
① 보안시스템 관리는 원칙적으로 콘솔에서 직접 작업을 하여야 한다. 다만, 부득이한 경우에는 보안시스템 관리자에게 사용자 계정을 발급받아 대학에서 지정하는 접근통제시스템을 통하여 접속하여야 한다.
② 보안시스템을 원격접속 하고자 할 경우 준수하여야 하는 사항은 다음 각 호와 같다.
1. 원격접속관리 시간(작업시간)을 최소화한다.
2.「서버보안관리지침」제4호 서식 '사용자계정(신규, 변경, 삭제) 신청서' 제출한다.
3. 원격접속관리자의 접속비밀번호 임시 부여 및 전송내역 암호화 등 보안대책을 적용한다.
4. 원격접속관리가 가능한 IP대역 설정 및 인가되지 않은 곳에서 원격접속관리가 수행되는지 주기적으로 확인 및 점검한다.
③ 보안시스템의 계정과 비밀번호는 별지 제2호 서식 '보안시스템 계정 및 비밀번호 관리대장'을 작성한다.
④ 원격접속과 관련된 보안사항은 「서버보안관리지침」으로 따로 정한다.

**제10조(보안시스템 보안정책 관리)**

① 보안시스템관리자는 보안시스템에 보안정책의 추가 수정이 발생한 경우 별지 제3호 서식 '보안시스템 보안정책 관리대장'에 기록하고 정보보안담당관에게 보고하여야 한다.
② 보안시스템관리자는 해당 서비스가 불필요해진 경우 보안정책을 삭제하여야 한다.
③ 보안정책은 분기별 1회 이상 점검하여야 한다.

## 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. 기술 환경의 변화로 적용이 불가능할 경우
2. 기술적, 관리적 필요에 따라 지침의 적용을 보류할 긴급한 사유가 있을 경우
3. 기타 재해 등 불가항력적인 상황일 경우

[별지 제1호 서식] 보안성검토 신청서

# 보안성검토 신청서

## □ 사업 개요

| 구 분 | 사 업 내 용 |
|---|---|
| 사 업 명 | |
| 사업기간 | |
| 사업부서 및 담당 | |

## □ 보안성검토 요청 내역

| 구 분 | | 보안성 검토 내역 |
|---|---|---|
| 사업 추진 관련 | 시스템 | □신규 구축 □기존 시스템 활용 |
| | 네트워크 | □네트워크 구성 변경(증설, 축소 등) □기존 네트워크 활용 |
| | 업무 연관 조직 | |
| 보안대책 주요 사항 (관리적, 물리적, 기술적, 기타) | | |
| 보안성 검토 방법 | | □ 보안심사위원회 검토 □ 정보보안위원회 검토<br>□ 자체 보안성 검토 |
| 기타 관계 자료 | | □ 사업 목적 및 추진계획<br>□ 사업계획서(신규 사업에만 적용)<br>□ 기술제안요구서 (RFP)<br>□ 정보통신망 구성도<br>□ 기타 (보안대책 강구사항) |

| 결 재 | |
|---|---|
| 직위 | 서명 |
| | |
| | |
| | |
| | |

[별지 제2호 서식] 보안시스템 계정 및 비밀번호 관리대장

# 보안시스템 계정 및 비밀번호 관리대장

작성일: 작성자:

| No | 제조사 | 장비 모델명 | 장비 구분 | OS 구분 | 사용 목적 (용 도) | 접속방법 | 설치위치 | ID | Password | 관리자 | 장비보안 인증등급 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | | | | |
| 2 | | | | | | | | | | | |
| 3 | | | | | | | | | | | |
| 4 | | | | | | | | | | | |
| 5 | | | | | | | | | | | |
| 6 | | | | | | | | | | | |
| 7 | | | | | | | | | | | |
| 8 | | | | | | | | | | | |
| 9 | | | | | | | | | | | |
| 10 | | | | | | | | | | | |

[별지 제3호 서식] 보안시스템 보안정책 관리대장

# 보안시스템 보안정책 관리대장

작성일: 작성자:

| 순번 | 장비명 | 설치위치 | 출발지 IP | 도착지 IP | 서비스 Port | Action | 정책요청일시 | 정책사용기간 | 정책 요청자 | 정책내용(상세) |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | | | |
| 2 | | | | | | | | | | |
| 3 | | | | | | | | | | |
| 4 | | | | | | | | | | |
| 5 | | | | | | | | | | |
| 6 | | | | | | | | | | |
| 7 | | | | | | | | | | |
| 8 | | | | | | | | | | |
| 9 | | | | | | | | | | |
| 10 | | | | | | | | | | |
| 11 | | | | | | | | | | |
| 12 | | | | | | | | | | |
| 13 | | | | | | | | | | |