	서버보안관리지침	규정번호	8-0-6		
		제정일자	2013.03.01		
		개정일자			
		개정번호	Ver.0	총페이지	24

제1장 총칙
제1절 일반사항

제 1조(목적)
이 지침은 동양미래대학교(이하 "본 대학"이라 한다)의「보안규칙」,「정보보안규칙」,「개인정보보호규칙」에 의거 서버의 보안 관리에 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. "서버"라 함은 서버용 운영체제(윈도우, 리눅스 등)가 탑재되어 운영되는 하드웨어, 소프트웨어를 총칭한다.
2. "감사추적"이라 함은 서버 접근에서부터 종료 시까지 일련의 과정 간 서버에서 행한 모든 활동을 재생, 검토, 조사할 수 있는 서버 활동의 시간별 기록이다.
3. "서버보안관리자"라 함은 본 대학의 정보시스템에서 서비스되고 있는 서버 장비의 보안 운영 업무를 담당하는 자를 말한다.
4. "시스템관리자"라 함은 다중 사용자 컴퓨터 시스템과 통신 시스템의 사용에 대한 관리 책임이 있는 자를 말한다.
5. "해킹"이라 함은 컴퓨터바이러스, 스팸메일, 서비스방해공격(DoS : Deny of Service Attack) 등 전자적 수단에 의하여 정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 사이버공격 행위를 말한다
6. "DMZ 영역"이라 함은 인터넷 구간과 내부망 구간 사이에 위치한 중간 지점으로 침입차단 시스템 등으로 접근제한 등을 수행하지만 외부망에서 직접 접근이 가능한 네트워크 영역을 말합니다.
7. 기타 용어 정의는「보안규칙」및「정보보안규칙」,「개인정보보호규칙」등의 용어 정의에 따른다.

제2절 책임사항

제4조(서버보안관리자)
서버보안관리자는 서버의 운용·유지보수 관리 및 보안 운용을 위한 업무는 다음 각 호와 같다.
1. 서버 운영 관리(계정, 서비스, 도입/변경/폐기, 백업/복구, 관리)
2. 서버의 로깅 설정, 로그 점검
3. 보안문제에 대한 신속한 해결 및 패치
4. 보안사고 대응 및 지원
5. 서버 보안패치 적용 및 취약점 제거
6. 보안관련 문제 발견, 장비의 상태 및 로그관리, 장애발생 시 정보보안담당관에게 통보

제5조(사용자)
사용자는 서버에 접속할 수 있는 자와 서버 응용프로그램에 접속하여 업무를 수행하는 자로서 다음 각 호의 업무를 수행한다.
1. 서버에 접속하거나 서버의 응용프로그램에 접속하여 업무 수행 시 접근이 불가능하거나 이상이 발견되면 즉시 서버보안관리자에게 통보하여야 한다.
2. 모든 사용자는 서버 접근 시 인가된 경로를 통해 허용된 용도로만 사용하여야 한다.

제2장 서버의 관리
제1절 서버보안관리

제6조(서버 도입 시 보안성검토)
서버보안관리자는 서버 도입 시 기술적인 보안성 검토를 할 수 있으며, 검토하여야 하는 사항은 다음 각 호와 같다.
1. 기본 보안설정 이상의 보안 기능 제공 및 보장
2. 기밀성, 무결성 및 가용성 보장 확인

제7조(서버 도입 및 설치)
① 서버보안관리자는 서버를 설치할 경우 준수하여야 하는 사항은 다음 각 호와 같다.
1. 설치 또는 변경되는 하드웨어 목록을 유지 및 관리하기 위하여 별지 제1호 서식 '서버 구성·설정 관리대장'을 작성하여 보유 현황을 관리한다.
2. 서버는 물리적인 접근통제가 가능한 공간에 설치한다.
3. 정확한 기록을 위해 서버의 시각을 동기화시켜 로그를 관리하여야 한다.
② 서버에 소프트웨어를 설치할 경우에 준수하여야 하는 사항은 다음 각 호와 같다.
1. 서버에 설치된 소프트웨어의 현황을 작성하고 이를 관리한다.
2. 서버에는 본 대학 업무용 목적으로 사용되는 프로그램 이외의 불필요한 프로그램의 설치를 금지한다.
3. 서버를 침해할 수 있는 백도어, Trojan 등 악성코드가 포함된 소프트웨어의 설치를

금지한다.
③ 서버보안관리자는 신규 서버장비 도입·설치 시 「정보보안규칙」의 '서버보안 등 정보시스템 운용'을 준용하여야 하며, 서버 운영체제 별 한국과학기술정보연구원 과학기술사이버안전센터 '정보시스템 보안가이드' 등을 준용하여 보안설정을 적용한다.

제8조(서버 구성 및 변경관리)
① 서버보안관리자는 서버 운영 중 구성변경이 발생할 경우 별지 제1호 서식 '서버 구성·설정 관리대장'에 작성하여 현황목록을 유지하고 관리하여야 한다.
② 서버 구성 변경을 수행하여야 하는 경우는 일반변경과 긴급변경으로 구분하며, 변경절차는 다음 각 호와 같다.
1. 일반 변경의 절차는 다음 각 목과 같다.
가. 서버보안관리자는 서버의 변경 계획을 정보보안담당관에게 보고한다.
나. 서버 구성 변경 후 변경된 사항의 이상 유무를 검증한 후 설정을 적용한다.
다. 서버의 구성 변경이 완료된 후에는 별지 제1호 서식 '서버 구성·설정 관리대장'에 기록하여 목록을 유지하고, 관리하여야 한다.
2. 긴급 변경의 절차는 다음 각 목과 같다.
가. 서버보안관리자는 긴급하게 변경을 하여야 할 경우에는 정보보안담당관에게 보고를 생략하고 구성 변경을 수행할 수 있다.
나. 긴급 변경 수행 후 변경된 사항의 이상 유무를 검증한 후 설정을 적용하여야 하나 시간적인 여유가 없을 경우에는 검증을 생략할 수 있다.
다. 서버의 구성 변경이 완료된 후에는 별지 제1호 서식 '서버 구성·설정 관리대장'에 기록하여 목록을 유지하고, 관리하여야 한다.
③ 서버보안관리자는 서버의 하드웨어 및 소프트웨어의 가용성과 무결성 확보를 위해 주기적으로 예방점검을 한다.

제9조(서버 용량·성능관리)
① 서버의 사용량(CPU, 저장장치, 메모리 등)을 주기적으로 감시하여 서버성능목표, 성능관련 요구사항, 성능 측정대상 및 성능요구수준을 정의한다.
② 성능요구분석 결과를 바탕으로 다음 각 항목을 정의하여 성능계획을 수립한다.
1. 성능분석대상 별 성능요구수준
2. 성능분석대상 별 임계값
3. 성능 모니터링 및 정보수집 방법
③ 주기적인 성능분석을 위한 기초 데이터를 수집하여야 하며, 성능분석을 위한 기초데이터는 다음 각 항목을 고려하여 선정한다.

구분	용량·성능 보고 항목
서버	- CPU 사용평균 사용률 및 최대 사용률 - 메모리 사용률 - 디스크 사용률
데이터베이스	- 디스크 사용량
네트워크	- 네트워크 회선 평균 사용률 - 네트워크 회선 최대 사용률
디스크	- 디스크 사용률 - 디스크 응답속도 - I/O 건수
정보보안시스템	- CPU 사용률 - 메모리 사용률 - 디스크 사용률

④ 매월 사용량에 대해서 별지 제3호 서식 '성능용량분석 보고서'를 작성하여 정보보안담당관에게 보고하여야 한다.

1. 수집된 성능분석항목 정보
2. 누적된 성능정보 변화 추이
3. 임계치를 초과한 경우
4. 장애 및 성능저하로 인한 사용 지연사항

⑤ 성능개선이 필요하다고 판단되는 성능문제 징후는 다음 각 호와 같다.

1. H/W 리소스 부족 또는 성능 저하가 예측이 될 경우
2. 응용프로그램 리소스 사용이 과다한 경우
3. 응용프로그램의 응답속도가 느려지는 경우

⑥ 성능문제를 해결하기 위하여 성능개선 방안 수립 사항은 다음 각 호와 같다.

1. 용량 증설 및 성능 모니터링 기능 강화
2. 세부 성능분석 결과에 따른 시스템 성능 파라미터 조정
3. 응용프로그램 및 배치작업의 수행시간 조정 등

제10조 (서버 반출 및 폐기 시 보안조치)

① 서버의 교체·반납·수리를 위하여 외부로 반출 또는 폐기 시 저장장치를 분리하여 데이터가 복구되지 않도록 삭제하거나 디가우징 장비를 사용하여 보안조치를 강구한 후 반출·폐기하여야 하며,「정보보안규칙」의 별지 제2호 서식 '데이터 삭제·폐기 확인서'를 제출하여야 한다.

② 서버보안관리자는 공인 IP 주소가 부여되었던 중요 서버는 폐기 시 폐기 사실을 정보보안담당관에게 보고하여야 한다.

③ 홈페이지 등 각 부서(팀) 및 학부(과)가 공통적으로 사용하는 서버는 부서별보안담당관의 책임 하에 제1항에 따라 처리하여야 한다.

④ 부서별보안담당관은 별표 1 '서버시스템 저장매체·자료별 삭제방법'을 준용하여 저장매체·자료 삭제방법을 사전에 지정할 수 있다.

⑤ 서버에 저장된 자료의 삭제가 필요한 경우는 다음 각 호와 같다.

1. 서버의 사용연한이 경과하여 폐기 또는 양여 할 경우
2. 서버 무상 보증기간 중 저장매체 또는 저장매체를 포함한 서버를 교체할 경우

3. 서버의 임대기간이 만료되어 반납할 경우
4. 고장 수리를 위한 외부 반출 등 본 대학이 서버 저장매체를 보안통제 할 수 없는 환경으로 이동이 필요한 경우

제11조(원격접속 보안관리)
① 서버보안관리자는 원칙적으로 원격접속을 허용하지 않으며 다만 부득이한 경우 다음 각 호의 사항을 확인하고 정보보안담당관의 승인을 득한 경우는 허용할 수 있다.
1. 별지 제11호 서식 '원격접속 보안서약서'
2. 원격접속 시간의 최소화
3. 원격접속에 대한 인증기능 사용
② 원격접속 관리를 위하여 통제할 사항은 다음 각 호와 같다.
1. 원격접속이 필요한 경우 접근통제 기능을 적용하여 제한된 서비스만을 사용하도록 통제하여야 한다.
2. 원격접속 시는 사용자 인증, 패스워드 사용기준(자릿수, 변경주기, 사용기간 등) 및 사용기록 로깅 등의 보안기능을 적용하여야 한다.
3. 원격접속에 대한 무결성 및 비밀성 확보를 위해 암호화된 프로그램 또는 가상사설망(VPN)을 적용하여야 한다.
4. 인가하지 않은 사용자의 접근이 시도되고 있는지 주기적으로 점검(원격접속 주소, 시간 등)하여야 한다.

제2절 사용자 관리

제12조(사용자계정 관리)
① 사용자계정 등록(신규, 변경, 삭제)이 필요한 경우 정보보안담당관에게 제출하여야 하는 서류는 다음 각 호와 같다.
1. 원격작업 : 별지 제4호 서식 '사용자계정(신규, 변경, 삭제) 신청서' 및 별지 제11호 서식 '원격접속 보안서약서'
2. 학사행정 : 별지 제4호 서식 '사용자계정(신규, 변경, 삭제) 신청서' 및「인적보안관리지침」별지 제2호 서식 '보안서약서(외부인용)'
3. 사용자 계정 : 별지 제4호 서식 '사용자계정(신규, 변경, 삭제) 신청서'
② 계정관리자는 정보보안담당관의 승인을 득한 후 사용자 계정을 생성하고, 별지 제5호 서식 '서버 관리자계정 및 비밀번호 관리대장'을 관리하여야 한다.
③ 계정관리자는 사용자계정 생성은「응용프로그램보안관리지침」으로 따로 정한다.

제13조(관리자계정 비밀번호)
① 서버보안관리자는 관리자 계정 비밀번호에 대해서 별지 제5호 서식 '서버 관리자계정 및 비밀번호 관리대장'에 기록하여 대외비 문서로 취급하고 별도의 잠금장치가 있는 문서함에 보관하며 인가된 자 외에는 열람을 금지하여야 한다.
② 서버보안관리자는 관리자 계정 생성에 관한 사항은「응용프로그램보안관리지침」으로 따로 정한다.

제14조(사용자 권한관리)
① 서버보안관리자는 서버 접근 및 사용 권한 부여 시 고려하여야 하는 사항은 다음 각 호와 같다.
1. 유지보수, 장애처리 등의 업무적인 필요성에 의하여 제3자에게 접근권한을 부여하여야 하는 경우, 정보보안담당관의 승인을 득한 후 부여한다.
2. 서버의 정상적인 운용을 방해하거나, 다른 사용자의 사용을 저해하는 등의 행위가 발견되거나 의심이 될 때, 사용자의 권한을 제한 또는 취소할 수 있다.
② 서버보안관리자는 사용자의 퇴직·보직이동 시 권한 변경에 관한 사항은「응용프로그램보안관리지침」으로 따로 정한다.

제3절 접근통제

제15조(접근통제 적용원칙)
① 서버보안관리자는 운영·관리 중인 서버에는 업무 중요도에 따라 접근통제가 이루어지도록 한다.
② 서버보안관리자는 접근통제시스템을 우회하여 접근하지 않도록 하여야 한다.
③ 서버보안관리자는 서버가 정상적으로 동작하지 않는 경우 정상 동작 시까지 사용자의 접근을 제한할 수 있다.
④ 5회에 걸쳐 사용자인증 실패 시 서버 접속을 중지시키고 비인가자의 침입 여부를 점검하여야 한다.

제16조(외부인 접근통제 기준)
① 서버보안관리자는 업무적인 필요성에 의하여 외부인에게 계정을 부여하는 경우, 별지 제4호 서식 '사용자계정(신규, 변경, 삭제) 신청서' 및「인적보안관리지침」별지 제2호 서식 '보안서약서(외부인용)'를 제출받아 정보보안담당관의 승인을 득한 후에 부여한다.
② 서버보안관리자는 외부인의 출입현황을 관리하고, 입회·감독 하에 작업을 수행하도록 하여야 한다.
③ 기타 외부인에 대한 세부적인 보안 준수 사항은「인적보안관리지침」과「보안시스템관리지침」에 따른다.

제17조 (로그인 세션의 보호)
① 서버보안관리자는 서버에 접속한 후 사용자나 다른 서버로부터 일정시간(10분) 이상 입력이 없는 경우 자동적으로 로그오프 시키거나 해당 세션을 중단시켜야 한다.
② 일정시간(10분) 이상 사용자가 자리를 비울 경우 비인가자가 자료를 보거나 변경하지 못하도록 비밀번호가 설정된 화면보호기 기능을 설정해야 한다.
③ 사용자는 하나의 사용자계정(ID)으로 여러 터미널(장소)에서 동시에 온라인 세션을 연결해서는 아니 된다. 다만, 업무적으로 불가피할 경우에는 예외로 할 수 있다.

제18조(접근통제의 강화)

① 서버보안관리자는 접근통제 기능의 강화를 위해 필요한 경우, IP 주소와 서비스포트 기반의 접근통제 기능을 사용할 수 있다.

② 서버보안관리자는 접근통제를 강화하기 위하여 서버보안 툴을 구축하여 운영할 수 있다.

제4절 침입탐지 및 대응

제19조(로그기록)

① 서버보안관리자는 운영 서버에 대한 모든 계정(ID)의 로그인 및 사용내역을 로그파일에 기록해야 하며, 필요시 그 내용을 정보보안담당관에게 보고하여야 한다.

② 서버접근 및 사용에 대한 책임추적성을 확보하기 위하여 다음 각 호의 사항을 로그로 남기고 일단위로 확인하여야 한다.

1. 서버 운영상의 이상 내역 로그
2. 원격 서비스를 통한 접근로그(접근시간, 접근IP 주소, 접근 터미널 등을 포함)
3. 원격 서비스를 통한 접근 실패 로그
4. 비밀번호 변경 등과 같은 중요 서버 명령의 수행 로그
5. 부여된 권한 허용 수준 이상의 정보를 얻으려는 시도에 관한 로그

③ 로그를 기록하는 경우는 다음 각 호의 사항을 준수하여야 한다.

1. 로그의 정확한 기록을 위해 네트워크에 연결된 모든 서버의 내부 시각을 동기화시키도록 한다.
2. 서버보안관리자는 정보보안담당관과 협의 하에 서버의 성능 및 디스크 용량 등을 고려하여 로그를 남길 대상을 선정한다.
3. 중요서버의 로그파일들은 별도의 로그서버를 지정하여 통합 저장하여 운영할 수 있으며, 로그에 대한 정기적인 백업을 실시하고 변조되지 않도록 관리하여야 한다.
4. 서버보안관리자는 서버 접속 내역을 기록한 로그에 대해 정보보안담당관의 공식적인 요청이나 법률에 의한 협조 요청에 의하지 않고는 타인에게 공개할 수 없다.
5. 정보보안 관련 이벤트가 기록되어 있는 로그는 6개월 이상 보관하도록 하여야 한다.

제20조(로그확인 및 분석)

서버보안관리자는 보안사고 예방 활동을 위하여 로그점검 이상 시 별지 제6호 서식 '로그점검 관리대장' 양식에 따라 다음 각 호의 보안사항을 분기별 1회 이상 점검하고 보고하여야 한다.

1. 시스템 로그
2. 작업 로그
3. 접속 로그
4. 보안과 관련되는 Task 수행에 대한 실패

제21조(서버 취약성 관리)

① 서버보안관리자는 정보보안 도구를 설치 및 운영 시 다음 각 호의 사항을 준수하여야 한다.
1. 서버보안관리자는 비인가자의 불법적인 침입으로부터 서버를 보호하기 위하여 정보보안 도구를 설치하여 서버의 보안 상태를 주기적으로 검사하여야 한다.
2. 정보보안 도구 사용 및 이를 통한 분석 결과는 외부로 유출되지 않도록 엄격히 통제되어야 한다.
② 사용자들이 서버에 접속해서 서버의 보안 취약성이나 결함을 탐지하는 모든 행위는 제한되어야 한다.
③ 서버보안관리자는 바이러스, 백도어, 트로이목마 등의 악성 프로그램 탐지 및 불필요한 서비스 차단을 위하여 정기적 또는 필요시 해당 서버의 보안 취약성을 점검하여야 하며, 자동화 스캐닝 도구를 사용할 수 있다.
④ 서버보안관리자는 서버의 보안성 강화를 위하여 서버보안 솔루션을 도입, 구축하여 운영할 수 있다.

제5절 백업 및 패치관리

제22조(백업관리)
① 서버보안관리자는 서버 장애 시 신속한 업무 복구를 위해 필요한 내용을 백업 대상으로 선정하여야 한다.
② 서버보안관리자는 서버의 장애나 저장매체의 불량으로부터 중요 정보와 소프트웨어를 보호하기 위해 일별, 주별, 월별 백업주기를 설정하고 백업내용은 3개월 이상 보관하여야 한다.
③ 백업은 정보통신실의 완전 소실인 경우에도 복구 가능한 수준으로 이루어져야 하며, 소산은 6개월마다 실시할 수 있다.
④ 서버보안관리자는 백업매체를 원본과 물리적으로 떨어진 장소에 보관하여 재해 등으로부터 원본 손실을 방지하도록 물리적인 접근통제 및 백업 일자 목록을 별지 제7호 서식 '백업매체 관리대장'에 기록하여 유지·관리하여야 한다.
⑤ 서버보안관리자는 백업을 위한 DR(Disaster Recovery) 구성 및 서버(별) 이중화 구성 여부 등을 검토하여 적용할 수 있다.

제23조(백신설치 및 운영)
① 서버보안관리자는 서버에서 바이러스를 진단 및 치료할 수 있는 백신 프로그램을 설치하여 운영하여야 한다.
② 서버보안관리자는 정상 업무 시간 종료 이후, 백신 프로그램을 이용하여 정기적인 검사를 실시하고 필요시 비정기 검사를 실시한다.
③ 서버보안관리자는 정상 업무 이외의 시간을 이용하여 정기적인 업데이트(주 1회 이상)를 수행하며, 필요시 긴급 업데이트를 수행한다.
④ 서버보안관리자는 신종 바이러스 발견 시 정보보안담당관에게 보고하고 필요 시 백신 프로그램 전문 업체에 신고하여 신속하게 조치하여야 한다.

제24조(패치관리)

① 서버보안관리자는 서버의 패치관리를 위하여 수행하는 업무는 다음 각 호와 같다.

1. 새로운 취약성에 대한 보안패치 정보를 수집하고 해당 패치의 안정성이 확보되는 시점에 패치 적용을 수행한다. 이때, 패치정보는 OS 패치 및 보안 패치를 포함한다.
2. 패치대상 서버, 소프트웨어별로 보안패치 방법 및 절차를 정리하여 패치 적용 정보를 기록할 수 있다.
3. 제공된 패치의 영향도 평가 및 백업 등 원상복구 대책 수립 후 패치를 적용한다.
4. 패치 적용 후 서버가 정상적으로 서비스를 제공하고 있는지에 대해 테스트를 수행하고 장애 발생 시 원상복구를 한다.
5. 테스트 장비가 존재하는 경우 테스트 장비에 우선 패치를 적용한 후 이상 유무를 확인하여 운영 장비에 적용한다.
6. 보안 패치 적용 후 별지 제8호 서식 '서버패치 관리대장'에 기록하여 보관한다.

제6절 장애관리

제25조(장애범위 및 유형 분류)

① 발생원인 관점의 장애 분류 기준은 다음과 같다.

<table>
<tr><th>통제</th><th colspan="3">재해 및 장애</th><th>재해 및 장애의 요인</th><th>장애 대응방안</th></tr>
<tr><td rowspan="2">통제
불가능
요인</td><td colspan="3">자연 재해</td><td>- 화재(전산실, 사무실)
- 지진 및 지반침하
- 장마 및 폭우 등의 수재, 태풍 등</td><td>재해복구센터 구축을 통한
장비 및 프로그램의 이중화,
데이터 백업 및 소산 철저</td></tr>
<tr><td colspan="3">인적 재해</td><td>- 시민폭동
- 폭탄테러 등</td><td rowspan="3">백업 또는 대체요원 확보</td></tr>
<tr><td rowspan="3">통제
가능
요인</td><td colspan="2">인적 장애</td><td rowspan="2">운영장애</td><td>- 시스템운영 실수
- 단말기 및 디스크 등의 파괴
- 해커의 침입
- 컴퓨터 바이러스의 피해
- 자료 유출 등</td></tr>
<tr><td rowspan="2">기술적
장애</td><td>시스템
장애</td><td>- 운영체제 결함
- 응용프로그램의 결함
- 통신 프로토콜의 결함
- 통신 소프트웨어의 결함
- 하드웨어의 손상 등</td><td rowspan="2">전산기기 이중화 및 프로그램
변경통제 강화,
재해복구(DR)센터 구축을
통한 기기 및 프로그램의
이중화, 통신망 이중화,
전력공급 중단에 대비한
무정전설비(UPS) 및 발전설비
구축</td></tr>
<tr><td>기반구조
장애</td><td>- 정전사고, 단수, 설비 장애
- 건물의 손상 등</td></tr>
</table>

제26조(장애탐지)

① 서버보안관리자는 장애상황을 상시 모니터링 하여야 한다.

1. 타 부서에 의한 장애신고
2. 시스템 콘솔 메시지 및 시스템 관리도구 화면의 장애 메시지
3. 네트워크 트래픽 지연

② 장애가 탐지되면 업무별 관리자는 다음과 같이 장애등급을 분류한다.

구분	장애 분류 기준
중대 장애	- 중요한 업무기능을 수행하는 다수 사용자의 업무중단 및 지장을 초래하는 장애 - 데이터의 손실이나 손상으로 인한 업무 중단
일반 장애	- 시스템의 기능 저하가 발생하여 일부 업무수행 속도에 지장을 초래하는 장애 - 비 핵심 업무기능을 수행하는 다수 사용자의 업무중단 및 지장을 초래하는 장애

제27조(장애처리 및 복구)

① 서버보안관리자는 다음 각 호의 사항을 분석하여 장애의 원인을 분석한다.

1. 서버, 정보보안시스템

가. 시스템 콘솔 메시지

나. 응용프로그램 에러메시지(응용프로그램에서 생성된 메시지)

다. 응용프로그램 로그

라. 시스템 관리도구 메시지

마. 시스템 로그(시스템 생성 로그)

바. 포트 및 F/W, IDS 등 정보보안시스템의 정책 확인

사. 각 시스템 관련 H/W 장애

2. 데이터베이스

가. 데이터베이스 프로세스 확인

나. 데이터베이스 로그 확인

다. 데이터베이스 서버의 이상 유무 확인

라. 데이터베이스 저장 공간 확인

② 장애발생 시 서버보안관리자는 별지 제9호 서식 '장애결과보고서'를 작성하여 정보보안담당관에게 보고한 후 장애원인을 파악하여 조치를 강구하여야 한다.

③ 장애원인이 명확하지 않거나 원인 규명에 시간이 소요된다고 판단되는 경우는 정보보안담당관에게 보고한 후, 긴급조치를 취하여 장애를 최소화하고, 사후에 상세 원인 분석 및 제9호 서식 '장애결과보고서'를 작성하여야 한다.

③ 다음 각 호의 경우에는 원인규명을 생략할 수 있다.

1. 원인 규명에 소요되는 비용이 긴급조치 비용보다 과다할 경우

2. 제조업체, 공급업체 또는 유지보수업체의 기술자가 분석하여도 그 원인을 알 수 없는 경우

3. 하드웨어, 소프트웨어 및 네트워크 등 다양한 요소가 복합적으로 작용하여 그 원인을 정확히 알기가 어려운 경우

4. 원인 규명을 위한 증거를 확보하기가 어려운 경우

5. 기타 원인 규명이 곤란하거나 불가능한 경우

④ 서버보안관리자는 장애 발생 시 정보보안담당관에게 보고한다.

⑤ 장애처리 및 복구를 수행 시 절차는 다음 각 호와 같다.
1. 중대 장애의 복구는 타 업무에 우선하여 조치
2. 과거의 장애조치 기록 등과 유사한 장애의 경우는 해당 절차에 따라 장애 복구
3. 자체 기술력으로 조치·수리 불가능 시에는 유지보수업체 기술담당자에게 연락
4. 장애발생에 대한 분석 및 조치사항 등을 별지 제10호 서식 '장애관리대장'에 작성하여 유지·관리

부 칙

(1) (시행일) 이 지침은 2013년 3월 1일부터 시행한다.
(2) (예외적용) 다음 각 항목에 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

[별표 1] 서버시스템 저장매체·자료별 삭제방법

서버시스템 저장매체 ·자료별 삭제방법

저장자료 / 저장매체	공개 자료	민감 자료 (개인정보 등)	비밀 자료 (대외비 포함)
플로피디스크	㉮	㉮	㉮
광디스크 (CD·DVD 등)	㉮	㉮	㉮
자기 테이프	㉮·㉯중 택일	㉮·㉯중 택일	㉮
반도체메모리 (EEPROM 등)	㉮·㉰중 택일	㉮·㉰중 택일	㉮·㉰중 택일
	완전포맷이 되지 않는 저장매체는 ㉮ 방법 사용		
하드디스크	㉱	㉮·㉯·㉰중 택일	㉮·㉯중 택일

㉮ : 완전파괴(소각·파쇄·용해)

* 비밀이 저장된 플로피디스켓·광디스크 파쇄시에는 파쇄조각의 크기가 0.25mm 이하가 되도록 조치

㉯ : 전용 消磁장비 이용 저장자료 삭제

* 소자장비는 반드시 저장매체의 磁氣力보다 큰 磁氣力 보유

㉰ : 완전포맷 3회 수행

* 저장매체 전체를 '난수'·'0'·'1'로 각각 중복 저장하는 방식으로 삭제

㉱ : 완전포맷 1회 수행

* 저장매체 전체를 '난수'로 중복 저장하는 방식으로 삭제

[별지 제1호 서식] 서버 구성·설정 관리대장

구성 관리 대장(소프트웨어)

정보자원번호		호스트명	
제조사		모델명	
용도		설치일자	
Certification		OS	
CPU		메모리	
Serial No.		S/W무상 보증기간	
납품 업체		구분	☐ Database ☐ WAS ☐ Tool ☐ Application
Application 정보	License No.:	백업Agent	☐설치 ☐미설치
	Version :	Secure OS	☐설치 ☐미설치
	기타		
설치Path (엔진,데이터,로그파일, 설정파일 등)			
구성요소1			
구성요소2			
유지보수	☐ 계약 ☐ 미계약 / 계약기간 / 계약업체명		
	영업대표 : (H.P.:), 기술지원: (H.P.:)		
변경이력			
장애이력			
특기사항			

처리 부서 결재	
직위	서명

구성 관리 대장(하드웨어)

정보자원번호		호스트명	
제조사		모델명	
용도		설치일자	
Certification		OS	
CPU		메모리	
Serial No.		무상보증 기간	
납품 업체		구분	□ 서버 □ 스토리지 □ 네트워크 □ 기타
IP 주소	License No.:	백업Agent	□설치 □미설치
	Version :	Secure OS	□설치 □미설치
	기타		
Mount 정보		Application (Database) 설치 내역	
NIC		KVM	□사용 □미사용
Disk(내장)		기타 구성요소	
Disk(외장)			
유지보수	□ 계약 □ 미계약	계약기간	계약 업체명
변경이력			
장애이력			
특기사항			

처리 부서 결재	
직위	서명

[별지 제2호 서식] 변경관리대장

변경 관리대장

순번	변경이력번호	변경요청자	모델명	호스트명	변경수행자	변경수행기간	변경 내용(변경결과보고서)	확인자	비고
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									

[별지 제3호 서식] 성능용량분석 관리대장

성능용량분석 관리대장

순번	시스템명	CPU		메모리		디스크	임계치 초과여부	점검일자	점검자	비고
		평균사용률	최대사용률	평균사용률	최대사용률	사용가능한 용량				
1										
2										
3										
4										
5										
6										
7										
8										
9										

처리 부서 결재	
직위	서명

[별지 제4호 서식] 사용자 계정(신규, 변경, 삭제) 신청서

사용자 계정(신규, 변경, 삭제) 신청서

신청 부서(회사)		**신청자 성명**	
신청일		**완료요청일**	
전화번호(휴대폰)		**이메일 주소**	
신청 구분	□ 신규 □ 변경 □ 삭제	**신청 사유**	
신청 ID	*6자~14자, 숫자, 문자 포함*	**비밀번호**	*비밀번호 작성규칙*
사용 기간	20 년 월 일 ~ 20 년 월 일		

세부 사항		
서비스 구분	□ 학사행정시스템 □ 원격작업 □메일 □ O/S □기타( )	
학사행정시스템 업무 그룹	*학사행정시스템에서 사용할 메뉴를 적어 주세요.* *예)입시시스템>원서입력>원서대조 외 다수*	
원격 작업	출발 IP 주소	
	서버 IP 주소	
메일	*요청사항을 상세하게 적어 주세요.*	
O/S 및 기타		
첨부 서류	*보안서약서, 원격접속서약서(서명 포함 문서를 스캔 후 첨부하여 주시기 바랍니다.*	

위 계정신청자는 원활한 업무 수행을 위하여 위와 같이 계정을 신청하오니 재가하여 주시기 바랍니다.

신청 부서 결재	
직위	**서명**

처리 부서 결재	
직위	**서명**

[별지 제5호 서식] 서버 관리자계정 및 비밀번호 관리대장

서버 관리자 계정 및 비밀번호 관리대장

작성일: 작성자:

No	제조사	장비 모델명	장비 구분	서버명	상태	IP 주소	CPU모델/수량	Core 수	메모리	OS구분	사용 목적 (용 도)	ID	Password	시스템관리자
1														
2														
3														
4														
5														
6														
7														
8														
9														
10														

[별지 제6호 서식] 로그점검 관리대장

로그점검 관리대장

확인일자	년 월 일	점검대상	□ N/W □ 서버 □보안시스템 □ 기타	확인자	
특이사항					

점 검 세 부 내 용										
순번	장비명	자산번호	점검항목(O, X)				이상내용	조치/확인결과 (별첨여부)	점검일자	점검자
			시스템 로그	보안 로그	접속 로그	작업 로그				
1										
2										
3										
4										
5										
6										

처리 부서 결재	
직위	서명

[별지 제7호 서식] 백업매체 관리대장

백업매체 관리대장

순번	매체 번호 (YYYY-MM-01)	매체 형태	백업대상 서버	백업 도구	보관 주기	백업일자	만료일자	관리자	비고
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									

[별지 제8호 서식] 서버패치 관리대장

서버패치 관리대장

순번	서버명	장비모델명	OS구분	패치명	Patch ID	용도	패치일자	작성일자	관리자	비고
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

[별지 제9호 서식] 장애결과보고서

장애결과보고서

장애발생번호		장비 모델명		장비구분	
장애 제목					
내용 현상					
장애 원인					
영향 범위					
발생 일시		해결일시		장애시간	시간
장애 유형	□ 인적장애 □ 시스템 장애 □ 기반구조 장애 □ 재해 장애 □ 기타				
장애 등급	□ 낮음 □ 중간 □ 높음 □ 매우 높음			작성자	

장애 구분	조치 내용 및 경과
□ S/W장애 □ H/W장애 □ 기 타	
특이 사항	

향후 이행 대책	완료일	이행담당자

※장애등급 (낮음: 개인, 중간: 특정 사용자 집단, 높음: 특정 부서, 매우 높음: 전체조직)

처리 부서 결재	
직위	서명

[별지 제10호 서식] 장애관리대장

장애관리대장

번호	장애발생 번호	장애 확인일시	장애내용	조치내용 (장애결과보고서)	장애 조치일자	RTO (복구시간)	조치자	확인자	장애 유형
1									□ 인적장애 □ 시스템장애 □ 기반구조 장애 □ 재해 장애 □ 기타
2									□ 인적장애 □ 시스템장애 □ 기반구조 장애 □ 재해 장애 □ 기타
3									□ 인적장애 □ 시스템장애 □ 기반구조 장애 □ 재해 장애 □ 기타
4									□ 인적장애 □ 시스템장애 □ 기반구조 장애 □ 재해 장애 □ 기타
5									□ 인적장애 □ 시스템장애 □ 기반구조 장애 □ 재해 장애 □ 기타
6									□ 인적장애 □ 시스템장애 □ 기반구조 장애 □ 재해 장애 □ 기타
7									□ 인적장애 □ 시스템장애 □ 기반구조 장애 □ 재해 장애 □ 기타

[별지 제11호 서식] 원격접속 보안서약서

원격접속 보안서약서

성 명	
생년월일	
소 속	

본인은 동양미래대학교(이하 “대학”이라 한다)에 년 월 일부로 원격 접속을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 대학의 제한구역 및 통제구역에 무단으로 출입하지 않는다.
2. 대학의 자산을 불법으로 유출, 변조하거나 훼손하지 않는다.
3. 대학의 자산을 개인적인 목적이나 이익을 위하여 사용하지 않으며, 허가된 용도로만 사용한다.
4. 허용되지 않은 정보자산에 접근을 시도하거나 정보보안 기능을 우회하는 시도를 하지 않는다.
5. 업무상 취득한 대학 또는 제3자 소유의 정보를 대학의 승인 없이 누설하지 않는다.
6. 대학의 통신망을 이용하여 외부인 접근이 금지된 타 대학이나 기관의 통신망 또는 시스템에 임의로 접속을 시도하지 않는다.
7. 대학의 자산(정보 포함)을 사용 후에는 즉시 대학에 전부 반환한다.
8. 기타 대학의 정보보안 관련 규정을 준수한다.

본인은 위의 사항을 숙지하여 이를 성실히 준수할 것이며 만일 이를 위반하였을 경우 민·형사상의 책임을 감수함은 물론 대학에 끼친 손해에 대해 지체 없이 변상·복구할 것을 서약합니다.

	년 월 일
서약자	(인)

동양미래대학교 정보보안담당관 귀하