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

제1장 총 칙

제1조(목적)
이 지침은 동양미래대학교(이하 "본 대학"이라 한다)의「보안규칙」,「정보보안규칙」에 의거 네트워크시스템의 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. "내부 네트워크"라 함은 외부에서 직접 접근이 불가능한 네트워크 영역으로 내부IP체계에 따라 운영되는 네트워크 영역을 말한다.
2. "네트워크시스템"이라 함은 유·무선 네트워크 서비스 제공을 위해 사용되는 시스템을 말한다.
3. "네트워크보안관리자"라 함은 네트워크 관리 업무를 총괄하는 자를 말한다.
4. "DMZ영역"이라 함은 인터넷 구간과 내부망 구간 사이에 위치한 중간 지점으로 침입차단시스템 등으로 접근제한 등을 수행하지만 외부망에서 직접 접근이 가능한 영역을 말합니다.
5. 기타 용어 정의는「보안규칙」및「정보보안규칙」등의 용어 정의에 따른다.

제2장 책임사항

제4조(네트워크보안관리자)
네트워크보안관리자는 유·무선 네트워크시스템의 운용·유지보수 관리 및 보안 운용을 위하여 수행하여야 하는 업무는 다음 각 호와 같다.
1. 네트워크시스템 운용관리(정책, 라우팅, 서비스, 도입·변경·폐기, 유지보수 등) 업무
2. 유·무선 네트워크시스템의 주기적인 보안점검 수행 및 보고
3. 유·무선 네트워크시스템의 보안문제에 대한 신속한 해결 및·패치

제5조(네트워크사용자)
대학 내에서 내부 네트워크를 사용하는 모든 교직원 및 사용자를 말하며 준수하여야 하는 사항은 다음 각 호와 같다.

1. 네트워크시스템의 인가된 경로를 통해서만 네트워크 접속을 하여 사용한다.
2. 유·무선 네트워크시스템에 대한 접근이 불가능하거나 이상이 발견되면 즉시 네트워크보안관리자에게 통보하여야 한다.
3. 내부 네트워크에서 유·무선 네트워크 시스템 등 관련 인프라의 사용 시 변경 등이 필요한 경우에는 네트워크보안관리자와 사전 협의를 하여야 한다.
4. DMZ영역이나 내부 네트워크 영역에서 유·무선 네트워크시스템을 스캐닝하거나 스니핑 등의 불법적인 행위는 하지 않아야 한다.
5. 네트워크사용자는 교육 목적이 아닌 상업적인 용도로 사용하지 않아야 한다.

제3장 네트워크시스템 보안관리

제6조(네트워크시스템 도입 및 폐기)

① 네트워크보안관리자는 네트워크시스템 도입, 증설 등 네트워크 환경의 변화에 따라 네트워크시스템의 도입·증설·폐기의 요구가 있는지 모니터링하며, 요구가 적정하다고 판단되면 정보보안담당관에게 요청을 할 수 있다.
② 네트워크보안관리자는 네트워크시스템 도입·증설·폐기 시에 업무 중요도에 따라 정보자산 보안등급을 정하여 보안설정을 적용하며, 보안등급을 포함한「정보보안규칙」별지 제4호 서식 '정보자산목록(표)'를 작성하여 관리한다. 다만 정보자산 중 네트워크장비는 L3이상 및 백본 및 층간 스위치를 위주로 관리한다.
③ 주요 네트워크시스템 장비는 비인가자의 출입이 통제되는 곳에 설치한다.
④ 네트워크시스템을 폐기할 때에는 네트워크시스템에 저장된 설정 정보를 삭제한 후 폐기하여야 한다.
⑤ 네트워크보안관리자는 네트워크시스템 폐기 시 다음 각 호의 절차에 따라 수행한다.
1.「정보보안규칙」별지 제1호 서식 '전산장비 설치/폐기 요청서'를 작성한다.
2. 폐기되는 장비는「정보보안규칙」별지 제2호 서식 '데이터 삭제·폐기 확인서'를 작성한다.
3. 별지 제1호 서식 '네트워크시스템 이력 관리대장'을 포함하여 정보보안담당관의 승인을 득하여야 한다.
4. 폐기 후「정보보안규칙」별지 제4호 서식 '정보자산목록(표)'를 유지·관리하여야 한다.

제7조(유·무선 보안설정의 적용)

① 네트워크시스템은 관리자 계정외의 별도 계정 생성을 금지한다.
② 네트워크시스템은 각 모드별로 암호를 설정하여 필요 이상의 권한을 차단하여야 한다.
③ 유·무선 네트워크시스템을 설치한 후, IP별 접근제어 정책을 적용하여 네트워크사용자가 네트워크시스템에 접근할 수 없도록 보안 설정 및 SSID 설정을 적용한다.
④ 네트워크시스템의 SNMP(Simple Network Management Protocol)는 다음 각 호와 같이 설정하여야 한다.

1. 기본 Community 문자열(Public)을 사용하지 않음을 원칙으로 한다.
2. 읽기권한(Read Only)만을 허용한다. 필요시 정보보안담당관의 승인 후에 RW(Read Write) community를 한시적으로 설정하여 사용하고 SNMP 정보는 해당 부서에서만 볼 수 있도록 한다.

⑤ 네트워크시스템의 다음 각 호와 같이 불필요한 서비스는 Disable 한다.

1. Small-servers
2. echo
3. disable
4. daytime

⑥ 네트워크보안관리자는 무선랜을 사용하는 경우 무선 중계기(AP)와 관련하여 자체 보안대책 수립 시 다음 각 호의 사항을 포함하여야 한다.

1. 네트워크이름(SSID: Service Set IDentifier) 브로드캐스팅 중지
2. 추측이 어려운 복잡한 SSID 사용
3. WPA2이상의 암호체계를 사용하여 자료 암호화(국가정보원장이 승인한 암호논리 사용)
4. MAC 주소 및 IP 필터링 설정
5. RADIUS(Remote Authentication Dial-In User Service) 인증 사용
6. 기타 무선단말기·중계기(AP) 등 무선랜 구성요소 별 분실·탈취·훼손·오용 등에 대비한 관리적·물리적 보안대책

제8조(네트워크시스템 운영관리)

① 네트워크보안관리자는 네트워크시스템을 신규 설치·변경한 후 별지 제1호 서식 '네트워크시스템 이력 관리대장'을 작성하여 변경사항을 기록, 유지한다.

② 네트워크보안관리자는 네트워크시스템의 구성 정보 등의 변경은 다음 각 호에 따른다. 1. 네트워크시스템 변경을 위한 작업계획 수립 및 보고
2. 필요시 관련 업무 담당자에게 문서 발송
3. 작업수행 및 검증 테스트
4. 완료보고서 작성 및 보고

③ 네트워크시스템 구성 정보는 장애 등에 대비하기 위하여 백업을 하여야 한다.

④ 네트워크시스템 장애 시「서버보안관리지침」의 별지 제9호 서식 '장애결과보고서', 제10호 서식 '장애관리대장'을 작성하여야 한다.

제9조(네트워크시스템 성능관리)

① 네트워크보안관리자는 분기별로 네트워크시스템의 사용량에 대해서 검토하고, 특이사항이 있을 경우 정보보안담당관에게 보고한다.

② 네트워크시스템에 대한 최적의 용량 확보, 용량부족으로 인한 서비스 지연, 장애 등을 방지하기 위하여 수행하여야 하는 사항은 다음 각 호와 같다.

1. 네트워크시스템 자원에 대한 이용도 분석 및 응답시간 지연 시 원인분석
2. 네트워크시스템의 사용현황 파악 및 추이분석을 통한 네트워크시스템의 가용성 확보

제10조(네트워크시스템 주소관리)
① 모든 네트워크사용자는 자동으로 부여된 IP 주소를 사용한다. 다만, 고정 IP 주소가 필요한 경우는 정보보안담당관의 승인을 득하여야 한다.
② 네트워크보안관리자는 네트워크시스템에서 사용하는 IP 주소를 체계적으로 관리하여야 한다.
③ 네트워크보안관리자는 IP 주소 및 환경정보, 구성도 등은 외부로 유출되지 않도록 대외비로 관리한다.

제11조(네트워크시스템 접근통제)
① 네트워크보안관리자는 별지 제2호 서식 '네트워크시스템 계정 및 비밀번호 관리대장'을유지하고 주기적으로 계정, 비밀번호 및 권한에 대한 현황을 점검하여야 한다.
② 네트워크보안관리자는 최소한의 계정만을 생성하여 제한된 사용자만이 사용하도록 하여야 한다.
③ 네트워크시스템에 설치 시 기본적으로 생성되는 불필요한 계정을 삭제하고, 해당 계정이 필요한 경우 비밀번호를 변경하여 사용하여야 한다. 다만, 해당 기능이 없는 장비인 경우는 제외한다.
④ 네트워크시스템의 관리자 계정 접속은 콘솔포트 및 특정 PC에서만 접근 가능하도록 설정한다. 다만, 해당 네트워크시스템에 접속 제한 기능이 없는 경우는 별도의 보안대책을 강구한다.
⑤ 네트워크시스템의 비밀번호 및 인증에 관한 사항은「응용프로그램보안관리지침」으로 따로 정한다.

제12조(네트워크시스템 보안관리)
네트워크보안관리자는 네트워크시스템 운용을 위하여 적용할 보안조치 사항은 다음 각 호와 같다.
1. 네트워크시스템에 대한 원격접속은 원칙적으로 금지하며, 불가피한 경우 장비 관리용 목적으로 내부 특정 IP·MAC 주소에서의 접속은 허용
2. 물리적으로 안전한 장소에 설치하여 비인가자의 무단 접근통제
3. 최초 설치 시 보안취약점을 점검하여 제거하고 주기적으로 보안패치 실시
4. 불필요한 서비스 포트 제거

제4장 네트워크시스템 설정관리

제13조(네트워크시스템 장비식별 및 운영)
① 네트워크보안관리자는 모든 네트워크시스템 장비의 위치와 기능을 파악하여야 한다.
② 네트워크보안관리자는 모든 장비에 대한 자산관리가 가능하도록「정보보안규칙」별지 제4호 서식 '정보자산목록(표)'를 작성, 유지하여야 한다.
③ 네트워크시스템은 도입 후 기본으로 제공되는 초기 값을 변경하여야 하며, 시스템

의 설치 목적 기능을 제외한 모든 기능을 해제(불필요한 서비스 및 포트 제거)하여야 한다. 다만, 필요시 정보보안담당관의 승인을 득한 후 적용한다.
④ 모든 통신 케이블 배선은 도청이나 손상으로부터 보호받을 수 있도록 전용 관로를 설치한다.

제14조(장비 운영 시 사전 협의)
① 부서별보안담당관은 유·무선 네트워크 장비(공유기, 무선AP 등)의 추가 설치 및 실습실 네트워크 구성 변경 등이 필요한 경우에는 정보보안담당관과 사전 협의를 하여야 한다.
② 부서별보안담당관은 연구실, 실습실 등에서 IP 주소가 추가로 필요한 경우에는 정보보안담당관과 사전 협의를 하여야 하며, 사전 협의 대상은 다음 각 호와 같다.
1. 독자적으로 IP 주소, 도메인 사용이 필요한 경우
2. 대량으로 IP 주소 할당이 필요한 경우(NAT: Network Address Translation 사용 등)
3. 많은 트래픽 발생이 예상되는 경우
4. 서비스의 추가 또는 변경 등이 필요한 경우
③ 정보보안담당관은 사전 협의 없이 교내 네트워크 서비스에 영향을 주는 경우 네트워크 사용을 제한할 수 있다.

제15조(백업관리)
① 네트워크보안관리자는 네트워크시스템 장애 시 신속한 업무 복구를 위해 네트워크시스템 구성정보 등 필요한 내용은 백업하고「서버보안관리지침」별지 제7호 서식 '백업매체 관리대장'을 작성하여 관리한다.
② 네트워크보안관리자는 비밀번호 파일이나 네트워크시스템 설정 파일과 같은 중요한 정보는 변경 시 마다 백업한다.

제5장 보안패치 및 로그관리

제16조(보안패치)
① 새로운 취약성에 대한 보안패치가 발표되면 해당 네트워크시스템의 보안사고 예방을 위한 보안조치 사항은 다음 각 호와 같다.
1. 보안패치 정보를 주기적으로 확인하여 적용한다.
2. 주요 보안패치에 대해서는 적용일 등 패치정보를 별지 제3호 서식 '네트워크시스템 보안패치 관리대장'을 작성하여 관리한다.
② 패치적용 대상 네트워크시스템 별로 보안패치 방법 및 절차는 다음 각 호와 같다.
1. 네트워크시스템 성능 및 환경의 문제로 패치를 못하는 경우에는 해당 사유와 이를 보완하기 위해 적용한 대체수단이나 방법을 기록한다.
2. 패치는 업무시간 종료 이후에 적용함을 원칙으로 한다.
3. 테스트 장비가 존재할 경우에는 테스트 장비에서 먼저 패치를 적용하여 이상 여부를 확인한 후 운영 장비에 적용한다.

4. 다수의 장비에 동시 적용하는 경우 1개의 장비에 먼저 패치를 적용하여 안정성을 확인한 후 나머지 장비에 확대 적용한다.
5. 네트워크시스템의 보안패치 적용은 일정을 수립하여 패치를 적용한다.
6. 패치 적용 후 네트워크시스템이 정상작동 되는지에 대해 테스트를 수행하고, 장애 발생 시 원상 복구한다.

제17조(로그관리)
네트워크보안관리자가 로그 데이터를 관리하여야 하는 사항은 다음 각 호와 같다.
1. 로그데이터는 접속의 성공여부와 무관하게 기록을 유지하여야 한다.
2. 네트워크시스템에 특이사항 발생 시 로그점검 결과를「서버보안관리지침」별지 제6호 서식 '로그점검 관리대장' 을 작성하여 정보보안담당관에게 보고하여야 한다.
3. 자동 수록된 자료는 보안사고 발생 시 확인 등을 위하여 중요 설정내용은 백업하여야 하며, 이벤트가 기록되어 있는 시스템 로그는 6개월 이상 보관하여야 하며 임의로 변경되지 않도록 별도의 방법으로 보관, 관리한다.

제18조(유지관리)
① 네트워크보안관리자는 유·무선 네트워크시스템의 가용성을 보장하기 위해 유지보수 업체에 예방점검을 요청하여 정기점검을 실시하여야 한다.
② 네트워크보안관리자는 네트워크시스템의 안정적인 운용을 위해 최신 운영체제 중 가장 안전한 버전을 사용하여야 하며, 새로운 운영체제 적용 시에는 모든 보안취약점을 제거하여야 한다.
③ 유지보수 수행 과정에서 네트워크시스템 정보가 유지보수 인력에 의해 유출되지 않도록 조치하여야 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] 네트워크시스템 이력 관리대장

네트워크시스템 이력 관리대장

순번	장비 모델명	장비구분	장비번호(S/N)	사용목적 (용도)	작 업 내 용	설치위치/건물명	작업일자	비 고
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								

[별지 제2호 서식] 네트워크시스템 계정 및 비밀번호 관리대장

네트워크시스템 계정 및 비밀번호 관리대장

작성일: 작성자:

No	장비 모델명	장비 구분	설치위치/빌딩	S/N	사용목적 (용 도)	관리자ID	관리자 PWD	Guest ID	Guest PWD	Enable PWD	IP주소	게이트웨이	Stack	Version
1														
2														
3														
4														
5														
6														
7														
8														
9														
10														

[별지 제3호 서식] 네트워크시스템 보안패치 관리대장

네트워크시스템 보안패치 관리대장

NO	장비명	장비모델명	OS버전 구분	패치명	Patch ID	용도	패치일	시스템관리자	작성일	비고
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

처리 부서 결재	
직위	서명