	보안감사지침	규정번호	8-0-10		
		제정일자	2013.03.01		
		개정일자			
		개정번호	Ver.0	총페이지	18

제1장 총 칙

제1조(목적)

이 지침은 동양미래대학교(이하 “본 대학”라 한다) 「보안규칙」에 따라 정보보안이 효과적으로 운영되고 있는지를 점검·평가하고, 보안감사 수행에 관한 사항을 규정함을 목적으로 한다.

제2조(적용범위)

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

제3조(용어정의)

이 규칙에서 사용되는 용어정의는 다음과 같다.

1. “비밀정보”란 내용이 누설될 경우 대학의 운영에 중요한 영향을 미칠 정보를 말한다.
2. “보호구역”이라 함은 중요한 부서 및 장소에 대한 외부인의 접근을 방지하기 위하여 출입의 안내가 요구되는 지역을 말한다.
3. “정보자산”이라 함은 데이터베이스, 데이터파일, 정보시스템 관련문서 등 정보시스템에 입력, 처리, 보관, 출력되어지는 모든 형태의 정보자료와 이의 관리를 위한 정보시스템 및 인적 자원을 총칭한다.

제2장 감사조직 및 역할

제4조(보안감사 조직)

① 보안감사를 실시하기 위해 총장이 임명하는 5인 이상의 보안감사팀을 구성하며, 팀장은 총장이 지명한다.

② 보안감사팀 구성에 대한 요구가 있을 시 각 부서(팀) 및 학부(과)에서는 해당 인원을 지원하여야 한다.

③ 보안감사팀원의 능력을 향상시키기 위해 필요한 경우 외부 기관으로부터 업무 지원 및 교육을 받을 수 있다.

제5조(역할)

① 보안감사팀은 정보보안 및 개인정보보호 관리활동의 적절성을 검토하기 위해 보안감사를 실시하며, 필요 시 수시감사를 실시 할 수 있다.

② 보안위반사항이 발생한 경우 보안감사팀은 관련 규칙에 따라 처벌을 의뢰할 수

있다.
③ 보안감사팀은 보안감사를 실시하고, 총장에게 그 결과를 보고하여야 한다.

제3장 보안감사
제1절 보안감사의 개요

제6조(보안감사의 정의)
보안감사는 정보보호 및 개인정보보호와 관련된 통제절차의 기록과 행동을 독립적으로 조사·관찰하고 관련 증거를 수집하여 분석함으로써 주요 정보자산의 무결성, 가용성 및 기밀성을 확인하고자 하는 일련의 정보 보안관리 활동을 말한다.

제7조(보안감사의 목적)
① 보안감사는 정보보호 관리활동을 모니터링 함으로써 궁극적으로 본 대학의 정보보안을 유지 향상시키는데 그 목적이 있다.
② 보안감사는 내부 및 외부의 잠재적 침입자에게 침입사실이 사후에 발견될 수 있는 가능성을 예고함으로써 사전에 예방효과를 극대화 하고자 함을 목적으로 한다.
③ 보안감사는 자체적인 보안관리 활동을 미리 진단하여 취약점을 제거하게 함으로써 보안사고에 적절히 대처할 수 있도록 한다.
④ 정보보호관리체계 및 개인정보관리체계 시스템에 적합하도록 실행상태 점검 후 보완을 통하여 조기에 정착시키는데 목적이 있다.

제8조(보안감사의 범위)
① 보안감사는 본 대학의 「보안규칙」및「정보보안규칙」,「개인정보보호규칙」등에 관계 지침들에서 규정한 사항을 확인하기 위한 모든 활동을 그 범위로 하며 정보자산, 정보자산 관리인력 및 일반사용자를 그 대상으로 한다.
② 보안감사는 다음 각 호의 부문을 포함한다.
1. 시스템 보안 감사
2. 네트워크, 응용프로그램(개발) 보안 감사
3. 서버, PC보안 감사
4. 물리적 보안 감사
5. 조직관리, 인적보안 감사
6. 데이터 보안 감사
7. 개인정보보호 감사
8. 기타 정보보호관리체계 및 개인정보관리체계 감사

제2절 보안감사 일반

제9조(보안감사의 계획)
최고보안담당관은 보안감사를 실시하기 위해 보안감사실시 범위와 시기 및 방법 등을 명시한 연간 보안감사계획서를 작성하여야 한다.

제10조(감사기간 및 대상)
① 정기 보안감사는 년 1회 실시함을 원칙으로 하고, 감사기간은 3일을 넘을 수 없다. 필요 시 수시감사를 실시 할 수 있다.
② 보안감사는 전 교직원을 대상으로 한다. 단, 업무특성상 전 교직원을 대상으로 감사할 수 없는 경우에는 샘플링으로 대상을 선발하여 실시한다.

제3절 보안감사의 수행

제11조(감사증거의 수집)
①「보안규칙」,「개인정보보호규칙」및 보안관련 규칙·지침 등에 규정된 사항이 부정이나 오류없이 이행되었다는 것을 검증하기 위한 감사증거를 수집하여야 한다.
② 감사증거를 수집하기 위하여 질문, 관찰, 문서검증, 비교 대조, 실사 등의 방법 중에 선택하여 수행할 수 있다.

제12조(보안감사의 실시)
① 다음 각 호의 체크리스트를 기준으로 보안감사를 수행하여야 한다.
1. 별지 제1호 서식 '정보보안 현황 체크리스트'
2. 별지 제2호 서식 '개인정보보호 현황 체크리스트'
② 조직 전반에 적용되는 항목에 대해서는 샘플링 조사를 실시하여 서버 및 네트워크 등 정보시스템의 운영과 관련된 항목에 대해서는 전수조사 및 인터뷰를 병행한다.

제13조(감사결과의 보고)
① 보안감사 최종일에 보안감사팀장은 별지 제3-1호, 제3-2호 서식을 작성하여 최고보안담당관 및 분야별보안담당관에게 통지하고 총장에게 보고한다.
② 보안감사팀장은 감사결과 학사 운영에 중대한 영향을 미칠 수 있는 위반 사항이 발견된 경우 보안심사위원회에 심의를 요청할 수 있다.

제14조(보안감사의 사후조치)
① 감사결과 지적사항에 대해서는 조치한 후 피감사부서장은 별지 제4호 서식 '보안감사 시정조치 보고서'를 작성하여 최고보안담당관의 승인을 득한 후 감사팀장에게 제출하며, 감사팀장은 이를 확인하여 결과를 총장에게 보고한다.
② 별지 제4호 서식 '보안감사 시정조치 보고서'에는 감사 지적사항과 향후 조치 계획 또는 조치 결과 등이 함께 기술되도록 한다.
③ 보안감사의 일부를 외부전문가를 활용하여 시행한 경우 외부전문가에 의해 시행된 범위를 명시하고, 보안감사의 전부를 외부전문가를 활용하여 시행한 경우에는 외부 전문가의 보안감사 사후조치 보고서로 대치할 수 있다.
④ 보안감사 결과를 토대로 하여 보안상의 문제점을 개선하고 보안정책 등에 반영하여야 한다.

부 칙

(1) (**시행일**) 이 지침은 2013년 3월 1일부터 시행한다.

[별지 제1호 서식] 보안 현황 체크리스트

정보보안 현황 체크리스트

1. 보호(제한구역, 통제구역)구역 보안감사 점검항목

점검내용	상태	확인자
전산실의 물리적 보안을 위한 지침서 등이 마련되어 있고 적절히 활용되고 있는지 확인		
전원, 온도 등 전산실 내 환경의 조절은 정해진 기준치 내에서 잘 이루어지고 있는지 확인		
방재시설은 적정하며 잘 관리되고 있는지 확인		
물리적 접근보안을 위해 시건장치, CCTV 등 적절한 접근보안 장치가 설치되어 사용되고 있는지 확인		
전산실을 비롯한 각 부서의 네트워크 케이블이 안전하게 설치되어 관리되고 있는지 확인		
백업테이프 등 전산 보조기억매체 보관 및 입출 관리가 지침에 따라 행해지고 있는지 확인		
보조기억매체의 반 출입에 대하여 승인권자의 승인 등 적절한 절차를 통해 이루어지는지 확인		
상시 근무자 이외에 전산실에 출입하는 사람에 대한 출입관리기록이 지침에 의거 잘 이루어지고 있으며 관리자에 의해 정기적으로 검토가 이루어지고 있는지 확인		
전산실 출입 인가자 명부를 비치하여 관리하고 있는지 확인		
출입카드는 발행, 사용, 반납 및 폐기 등이 체계적으로 관리되고 있는지 확인		
문서가 보안등급에 적절하게 시건 장치가 된 문서함에 보관되고 있는지 확인		
비밀문건으로 정의된 정보자산의 입출 및 프린트 등이 적절히 통제되어 대학외부나 대학내부의 비인가자에게 유출되지 않도록 관리되고 있는지 확인		
이면지 사용 등에 의해 비밀정보가 비 인가자에게 유출되지 않도록 관리되고 있는지 확인		

2. 네트워크 정보보안감사 점검항목

점검내용	상태	확인자
장비의 도입 및 설치는 보안관리 절차에 따라서 이루어지고 있는지 확인		
장비의 데이터에 대하여 백업이 수행되고 있으며 필요 시 복구가능성을 확보하기 위해 정기적으로 복구테스트가 행해지고 있는지 확인		
장애가 발생하는 경우 발생 일시, 유형, 조치사항 등을 요약한 장애일지를 적시에 기록하고 있는지 확인		
계정은 지침에 따라 권한을 부여하고 있으며 패스워드는 안전하게 설정되고 있는지 확인		
장비에 대한 접근통제 및 불필요한 서비스 제공여부 확인		

점검내용	상태	확인자
패치나 파라미터 변경은 관련절차에 따라서 이루어지고 있는지 확인		
취약점 점검은 정기적으로 이루어지고 있는지 확인		
네트워크의 변경 등의 경우에 네트워크보안관리 절차에 의거 적절한 승인절차를 거쳤는지 확인		
네트워크의 성능 및 부하 등이 실시간으로 관리되어 장애 등을 적시에 발견하여 조치를 취하고 있는지 확인		
네트워크 운영자의 콘솔이나 통신회선 등이 인가되지 않은 제3자에 의해 엑세스되지 않는지 확인		
통신회선 등의 장애에 대한 대책은 수립되어 있으며 적절히 운영되고 있는지 확인		
네트워크 주소의 발급, 회수 및 현황관리가 이루어지고 있는지 확인		
외부 및 내부의비 인가자에 의한 부정접속, 회선침입, 도청 및 파괴행위 등에 대한 적절한 대책 및 이의 시행여부를 확인		
대학교의 내부망에서 인터넷을 접속하는 경우 인가된 경로만을 사용하고 있는지 확인		
침입차단시스템, 침입탐지시스템 등 대학교의 정보보안을 위해 중요한 정보통신시스템의 운영현황을 파악하고 관리상태의 적정성을 확인		
건물 및 무선랜 장비 사용 장소에 대한 물리적인 접근제어		
보유한 무선랜카드 및 AP의 목록 작성/관리		
AP 설치 시 외부와 인접한 장소(벽, 창문 등) 회피		
AP 미사용 시 전원 차단		
AP 리셋 수행 시 설정된 보안 환경으로 복구하는 기능 확보		
기본으로 설정된 AP의 SSID 변경		
AP의 SSID 설정시 부서명, 학과명, 제품명 등의 사용 회피		
AP 보안인증의 종류가 WPA2이상으로 설정하는지 여부		
유선 네트워크와 무선 네트워크(AP 또는 Hub to APs) 구간에 침입차단 시스템 설치		
AP 간의 연결을 위해 허브 대신에 레이어 2 스위치 설치		
교환되는 정보의 중요도를 고려한 적절한 암호 메커니즘 사용		
주기적으로 소프트웨어 패치 및 업그레이드		
모든 AP에 보안강도가 강한 관리 패스워드(8자리이상) 사용		
향상된 보안 기능을 제공하는 802.11 제품 사용		

3. 정보시스템 보안감사 점검항목

점검내용	상태	확인자
시스템의 도입 및 설치, 소프트웨어 설치는 보안관리 절차에 따라서 이루어지고 있는지 확인		
컴퓨터 동작, 작업일정 및 작성 행위, 운용자, 작업제어 언어, 외부서비스, 테이프 및 디스크 등의 관리, 프로그램 라이브러리 관리 등이 보안체계에 맞게 운영되고 있는가를 확인		
정보처리시스템의 데이터와 프로그램에 대하여 백업이 수행되고 있으며 필요 시 복구가능성을 확보하기 위해 정기적으로 복구테스트가 행해지고 있는지 확인		
주요 데이터 및 프로그램 백업은 소산 보관하는지 확인		

점검내용	상태	확인자
시스템 장애가 발생하는 경우 발생 일시, 유형, 조치사항 등을 요약한 장애일지를 적시에 기록하고 있는지 확인		
사용자 계정은 지침에 따라 권한을 부여하고 있으며 패스워드는 안전하게 설정되고 있는지 확인		
시스템에 대한 접근통제 및 불필요한 서비스 제공여부 확인		
외부에 접속된 컴퓨터 시스템인 경우 데이터의 무결성 확보대책, 장애대책, 오류방지 대책의 수립 및 적절한 운영여부를 확인		
백신 프로그램을 설치하여 악의적 소프트웨어에 대응하고 있는지 확인		
패치나 시스템 파라미터 변경은 관련절차에 따라서 이루어지고 있는지 확인		
시스템의 정상적 운영에 대한 상시 모니터링이 이루어지고 있는지 확인		
취약점 점검은 정기적으로 이루어지고 있는지 확인		
시스템 운영 및 주요 정보에 대한 로그는 적절히 관리되고 있는지 확인		
공개용 웹 서버는 침입차단시스템의 DMZ영역에 설치하여 내부의 전산자원을 보호하고 있는지 확인		
홈페이지 게재내용은 비밀내용 중요자료가 공개되지 않도록 하고 있는지 확인		
공개용 웹 서버는 웹 서비스를 제외한 모든 서비스 및 시험·개발 도구 등의 사용을 엄격히 제한하고 있는지 확인		

4. 보안시스템 보안감사 점검항목

점검내용	상태	확인자
보안시스템 관리를 위한 접속 이외의 접근경로를 차단하였는지 확인		
보안 시스템 관리자용 PC 이외의 IP로부터 접근이 차단되고 있는지 확인		
보안시스템의 장애 시 즉각 관리자에게 연락이 되는지 확인		
보안시스템 용도 이외의 S/W를 설치하지 않았는지 확인		
불필요하거나 현황에 맞지 않은 설정이 존재하지 않는지 확인		
발견된 침입 시도에 대한 통계를 모니터링 하는지 확인		
수집된 로그를 백업하고 일정기간 동안 관리 하는지 확인		
룰 변경은 정보보호시스템보안관리 절차에서 제시한 검토 및 승인 절차에 의해 변경되고 있는지 확인		

5. 데이터 보안감사 점검항목

점검내용	상태	확인자
정보시스템 내에 존재하는 데이터와 문서형태로 관리되는 데이터에 대한 보안등급에 따라 접근권한 설정이 부여되고 있는지 확인		
비밀 유지가 필요한 비밀정보에 대하여 암호화 등이 이루어지고 있는지 확인		
백업과 회복 절차가 적절히 수행되고 있는지 확인		
데이터베이스 운영시스템, 데이터사전, 유틸리티 소프트웨어, 운영체제 등의 시스템 소프트웨어에 대해 무결성이 유지되고 있으며 장		

점검내용	상태	확인자
애 시에 대책수립 등이 적절히 수행되고 있는지 확인		
학생이 원격교육용 시스템을 이용하고자 하여 시스템에 접속하는 경우 거래당사자의 진실성을 확인할 수 있는 기술적 요소를 포함하도록 설계, 운영되고 있는지 확인		
원격교육용 시스템의 접속 일시, 네트워크 주소, 등에 대하여 로깅이 되고 있는지의 여부와 정기적으로 백업하여 안전한 장소에 보관되는지 확인		
학생정보의 보호를 위해 학생 비밀번호 관리를 위한 보안대책이 준수되고 있는지 확인		

6. 응용시스템 보안감사 점검항목

점검내용	상태	확인자
아이디 및 패스워드 규칙에 따라 응용프로그램에 적용하고 있는지 확인		
응용프로그램 개발 시 계획단계에서 준수하여야 할 사항(보안요구사항 분석 및 명세화 등)이 적절히 준수되고 있는지에 대한 확인		
응용프로그램 개발 시 프로그래밍 단계에서 준수하여야 할 사항(보안을 고려한 프로그래밍 등)이 적절히 준수되고 있는지에 대한 확인		
응용프로그램 개발 시 테스트 단계에서 준수하여야 할 사항(데이터의 입출력 등)이 적절히 준수되고 있는지에 대한 확인		
테스트 수행 시 사용되는 데이터는 실 업무에 사용 중인 데이터를 변경하여 사용하는지의 여부를 확인		
개발된 응용프로그램이 적절한 통제절차에 의하여 운영환경으로 이전되고 있는지에 대한 확인		
프로그램 소스 라이브러리에 대한 엄격한 접근통제 유지를 확인		
프로그램 변경의 경우 변경절차의 따라 적절한 승인을 거친 후 운영환경에 이관되고 있는지 확인		
운영시스템에서의 직접적인 프로그램 변경 등 긴급한 상황하의 프로그램 변경이 사후의 승인을 득하였는지 등 적절한 통제절차에 의해 이루어 졌는지 확인		
인가된 응용소프트웨어 만을 사용하고 있는지에 대해 확인		
편집기와 같은 개발에 필요한 툴 등은 어플리케이션 운영 시스템에 설치되지 않았는지 확인		
중요 정보(개인정보, 인사정보 등)에 대한 접근이 성공한 사용자에 대한 기록은 보존되는지 확인		
사용자별 접근기록을 감사하고, 로그로 남겨진 변경 사항을 주기적으로 감사하여 불법으로 접근되거나, 변조된 내용이 없는지 확인		

7. PC 보안감사 점검항목

점검내용	상태	확인자
개인용 컴퓨터는 비인가자가 부팅을 하거나 접근하지 못하도록 부팅 시 패스워드의 설정사용, 화면보호기 패스워드의 설정사용, 공유폴더 사용제한, 개인용 컴퓨터의 패스워드 관리 등을 규정한 개인용 컴퓨터 보안관리 지침이 준수되고 있는지 실사 등을 통해 확인		

개인소유의 컴퓨터는 적절한 승인절차 없이 중요정보가 처리, 보관되는 기관 내부로 반입하여 사용할 수 없도록 적절한 통제절차가 수립되어 시행되는지 확인		
개인용 컴퓨터에 보관되어 있는 정보일지라도 비밀정보를 저장하고 있는 경우 패스워드의 설정, 암호화 등을 통해 비 인가자에 의한 정보의 유출을 방지하기 위한 적절한 대책이 강구되어 있는지 확인		
개인용 컴퓨터에 대하여 불법 소프트웨어의 사용 금지 및 사내 표준 운영체제와 소프트웨어를 사용하도록 하는 지침이 잘 준수되고 있는지 확인		
노트북 등 특히 분실의 염려가 있는 경우 별도의 도난방지 장치를 설치하여 사용하는지 확인		
노트북 컴퓨터를 내부에서 전산망에 연결하여 사용하는 경우에도 개인용 컴퓨터 및 단말기에 적용되는 수준의 보안이 동일하게 적용되고 있는지 확인		
개인용 컴퓨터에 바이러스의 유입을 방지하기 위한 바이러스 방역 지침이 잘 준수되고 있는지 확인		
업무 연락, 사내게시판, 메일 등을 통해 개인용 컴퓨터 보안 및 바이러스 방역을 위한 홍보가 지속적으로 행해지는지 확인		

[별지 제2호 서식] 개인정보보호 현황 체크리스트

개인정보보호 현황 체크리스트

1. 대학 개인정보관리체계 점검항목

점검내용	상태	확인자
내부관리계획에 개인정보보호 조직구성 및 운영 등의 세부 사항이 명시되어 있는가?		
정보주체의 개인정보를 보호하고 개인정보와 관련한 정보주체의 고충을 처리하기 위하여 개인정보 보호책임자(CPO)가 지정되었는가?		
개인정보보호책임자(CPO)의 자격 요건을 정하여 이에 적합한 자를 지정하고 있는가?		
개인정보보호책임자(CPO)의 개인정보보호에 관한 역할 및 책임이 정의되었는가?		
개인정보취급자의 개인정보보호에 관한 역할과 책임 및 권한이 정의되었는가?		
교육·훈련의 대상은 개인정보 보호책임자(CPO), 개인정보 취급자 및 개인정보취급부서 책임자 및 관리 담당자 등을 포함하고 있는가?		
조직이 보유한 개인정보를 공유, 제공 받거나 접근 권한을 부여받은 외부 직원에 대한 교육훈련을 제공 하는가?		
교육내용은 개인정보보호 관련 법률 및 제도, 사내 규정, 관리적 기술적 조치사항 및 이를 수행하기 위한 방법 등 개인정보취급자가 필수적으로 알아야 하는 사항을 포함하는가?		
개인정보보호 교육 시 교육대상자의 직위 및 담당하는 업무의 특성에 따라 교육 내용을 차별화하여 적합한 교육을 실시하고 있는가?		
교육 및 훈련이 계획에 따라 년2회 이상 시행되고, 이에 대한 기록을 유지 하는가?		
업무상 개인정보를 취급해야 하는 사람들을 최소한으로 제한하고 있는가?		
인사규정 또는 채용계약서 등에 개인정보취급자가 직무상 취득한 개인정보를 훼손·침해 또는 누설하는 경우 관계법령상의 책임 및 처벌규정에 대해 명시하고 있는가?		
개인정보취급자의 퇴직 및 직무변동 시, 인사부서와 개인정보 관련부서 간에 상호 공지가 이루어지는가?		
내부직원(정규직/계약직/임시직)의 개인정보 취급 업무 시작 시 개인정보보호에 관한 책임 및 의무를 고지한 개인정보보호 서약서를 징구하는가?		
제3자 등 외부 인원에게 개인정보처리시스템 접근권한을 부여하는 경우 개인정보보호에 관련된 사항이 계약서에 포함되어 있으며, 개인정보를 취급하는 인원에 대해서는 개인정보보호 서약서를 받는가?		
개인정보 사고 보고 시 법률이나 규정 등에 의해 관련 기관에 보고해야 할 경우 보고되고 있는가?		
개인정보사고가 종결된 후 개인정보사고의 원인을 분석하고 있는		

점검내용	상태	확인자
가?		

2. 개인정보 기술적 보호 점검항목

점검내용	상태	확인자
개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 최소한의 인원에게 부여하고 있는가?		
개인정보취급자의 업무 내용에 따라 접근 권한을 제한하고 있는가?		
개인정보처리시스템의 접근권한 부여 현황, 변경 또는 말소 내역 등을 기록하고 최소 3년 이상 보관하는가?		
다음 사항을 포함하는 사용자 패스워드 관리 절차가 존재하고, 이에 따라 이행되고 있는가? -안전한 패스워드 사용 기준 -초기 패스워드 할당후의 변경 -패스워드의 암호화 -패스워드의 재발급 등		
전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 개인정보처리시스템의 접근권한을 지체없이 변경 또는 말소하는가?		
개인정보처리시스템 및 패스워드 관리지침을 제공하고 있는가?		
암호정책은 법적 요건을 만족하고 있는가?		
암호정책에 따라 암호화가 필요한 경우, 적절한 알고리즘과 키 길이를 결정하여 사용하고 있는가?		
개인정보취급자가 사용자의 개인정보를 개인용컴퓨터 (PC)에 저장할 때 암호화하여 저장하고 있는가?		
취급중인 개인정보가 권한 없는 자에게 공개되지 않도록 개인정보취급자의 PC 및 개인정보처리시스템의 네트워크 설정에 대한 정책이 수립되어 있는가? -인터넷 연결 시 네트워크 구성 정책 -이메일, 인터넷사이트의 접속, 메신저, P2P 등을 통한 파일전송 제한 -공유설정 제한		
개인정보처리시스템은 침입차단시스템에 의해 보호되는가?		
침입차단시스템을 우회한 인터넷접속을 금지하고 있는가?		
침입을 확인하기 위해 침입차단시스템의 로그가 수집되고, 정기적으로 점검되는가?		
개인정보처리시스템 접속 시 외부 망에서의 직접 접속은 차단되고, 가상사설망(VPN) 등을 통해 접근하도록 통제되는가?		
침입기록의 자동기록, 비인가자 접속 시 자동차단, 자동 경보 기능 및 분석정보 제공 기능을 보유하고 있는 침입탐지시스템을 설치하여 운용하고 있는가?		
네트워크를 통해서 시스템을 운영하는 경우 시스템 관리는 특정 터미널을 통해서만 수행할 수 있도록 제한되는가?		
원칙적으로 인터넷 등 외부 망을 통해 내부 시스템을 관리하는 것을 금지하고 있으며, 부득이 하게 이를 허용할 경우 강력한 사용자 인증, 암호 및 접근통제 기능을 설정하는가?		

점검내용	상태	확인자
허가되지 않거나 불분명한 소스, 네트워크 등으로 부터의 다운로드를 금지하고, 부득이 하게 다운로드 받을 경우 다운로드 받은 소프트웨어는 바이러스 검사를 하는가?		
전자우편의 첨부파일에 대해 전자우편서버 등에서 바이러스 검사를 수행하는가?		
주기적으로 바이러스 스캐닝이 이루어지고 있는가?		
바이러스 프로그램은 최신버전으로 업데이트 되는가?		
바이러스 감염이 발견되었을 경우에 바이러스 확산 및 피해 최소화를 위한 절차가 있는가?		
원격작업을 통해 내부시스템 접근 시, 접근통제, 암호화 대책이 수립되어 있는가?(ID/Password 외 추가인증, VPN 등)		
공개 서버는 내부 망과 분리하여 설치되며, 침입차단 시스템 등에 의해 보호되는 네트워크 보호 대책이 수립되고 운영되고 있는가?		
공개 서버 내에 보호되어야 할 주요 개인정보를 정의하며, 주요 개인정보 전송 시 비밀성과 무결성을 보장하는 보안서버 구축 등의 조치를 적용하고 있는가?		
개인정보처리시스템에서 개인정보의 인쇄물 출력 시 용도에 따른 출력 항목을 최소화하는가?		
개인정보처리시스템의 화면에서 개인정보를 출력할 때 메뉴 별로 업무 내용 및 개인정보취급자의 권한에 따라 필요한 최소한의 정보만을 표시하는가?		
개인정보취급자가 테이프, 디스크, 출력물, 이동식 저장 장치 등에 복사할 경우 필요한 사항을 기록하는가?		
개인정보를 출력하거나 이동 가능한 저장매체에 복사할 경우 사전에 개인정보 보호책임자(CPO)의 승인을 받는가?		
출력물, 복사물에는 조직의 명칭 및 기록된 출력, 복사물의 일련번호를 표시하는가?		
출력물, 복사물로부터 다시 출력 또는 복사하는 경우에도 조직의 명칭 및 새로운 일련번호를 표시하며 이에 대한 로그가 기록되는가?		
개인정보의 출력, 복사에 대한 승인 시 승인받고자 하는 개인정보취급자에게 불법 유출 시 법적 책임을 지게 됨을 주지시키는가?		
개인정보의 조회, 출력 시 개인정보를 마스킹(* 등)하여 표시제한을 수행하는가?		
개인정보 취급공간과 개인정보처리, 저장시설 및 장비를 보호하기 위한 보호구역을 정의하였는가?		
개인정보장비의 폐기 시에는 저장매체를 물리적으로 파기하거나, 저장된 정보가 완전히 삭제되어 복구가 불가능한지 확인하고 있는가?		
개인정보 취급자 등의 의무자 외 위탁업체 및 제3자의 개인정보처리시스템에 대한 접속 일시 및 내역 등 접속기록을 최소 6개월 이상 저장하는가?		
개인정보처리시스템 접속 기록을 월1회 이상 정기적으로 확인 및 감독 하는가?		
개인정보처리시스템의 접속기록이 위·변조되지 않도록 별도 저장장치에 백업 보관하는가?		
개인정보보호 감사에 대한 정책 및 공식적인 계획이 수립되어 있		

점검내용	상태	확인자
고 계획에는 다음과 같은 사항을 포함하는가? -대상, 범위, 주기, 방법, 절차, 감사자, 감사도구		
개인정보보호감사는 정기적으로 수행되는가?		
감사결과에 따른 지적사항이 이행되도록 사후관리가 수행되는가?		

3. 개인정보 수집 점검항목

점검내용	상태	확인자
서비스 제공을 위해 필요한 최소한의 정보만을 수집하고 있으며, 이 외의 개인정보를 제공하지 않는다는 이유로 해당 서비스의 제공을 거부하지 않고 있는가?		
서비스 제공을 위해 필요한 최소한의 정보 이외의 정보를 수집할 경우, 정보주체가 선택 제공할 수 있도록 하고 있는가?		
개인정보 수집 시 아이핀 등 주민등록번호를 대체하는 수단을 제공 하는가?		
중요한 개인정보를 수집하는 경우, 법적 근거가 있거나, 정보주체의 동의를 받는가?		
수집하는 개인정보에 대하여 정보주체에게 알리고 동의를 받는가?		
개인정보 수집 시 정보주체가 쉽고 명확하게 이해할 수 있는 방법으로 사용자의 동의를 받고 있는가?		
동의를 얻어야 할 내용을 정보주체가 명확히 인지하고 확인할 수 있도록 표시하는가?		
만14세 미만 아동의 개인정보를 수집하는 경우 법정 대리인에게 필요한 사항에 대하여 고지하는가?		
만14세 미만 아동의 개인정보를 수집하는 경우 법정 대리인의 동의를 받고 있는가?		
만14세 미만 아동의 동의를 얻을 경우 아동이 쉽게 이해할 수 있는 평이한 표현으로 고지하는가?		
개인정보취급방침이 법적 요구사항 및 운영에 필요한 사항을 포함하여 정의되었는가?		
개인정보취급방침을 사용자가 언제든지 쉽게 확인할 수 있도록 적절한 방법으로 공개하였는가?		
개인정보취급방침을 변경하는 경우에는 그 이유 및 변경 내용을 지정된 방법에 따라 지체 없이 공지하고, 사용자가 언제든지 변경된 사항을 쉽게 알아 볼 수 있도록 조치하는가?		

4 개인정보 이용·제공 점검항목

점검내용	상태	확인자
정보주체 및 정보주체의 법정대리인으로부터 수집한 개인정보를 동의한 범위를 벗어나 이용하지 않는가?		
개인정보 수집 시 고지하거나 이용약관에 명시한 목적 범위를 벗어난 개인정보의 이용 또는 제3자 제공이 발생할 경우, 정보주체로부터 추가적인 동의를 받는 절차와 방법이 마련되어 있는가?		
정보주체로부터의 개인정보에 관한 의견과 불만을 접수하고 처리하는 상담창구를 운영하고 있는가?		
정보주체 및 정보주체의 법정 대리인으로부터 정보주체 자신의		

점검내용	상태	확인자
개인정보에 대한 열람 또는 이용 및 제공내역을 요구할 수 있는 방법 또는 절차를 제공하는가?		
정보주체 및 정보주체의 법정 대리인으로부터 정보주체 자신의 개인정보 열람, 개인정보의 이용 및 제공 내역, 또는 정정에 대한 요구가 있는 경우 지체없이 필요한 조치를 취하는가?		
정보주체 및 정보주체의 법정 대리인이 정보주체 자신의 개인정보에 오류가 있는 경우 정정을 요구할 수 있는 방법 및 절차를 제공하는가?		
정보주체의 열람, 이용, 정정 및 제공내역 요청을 받은 경우 본인 여부를 확인하는 절차가 있는가?		
정보주체 및 정보주체의 법정대리인은 정보주체 개인정보에 대한 오류 정정을 요구할 경우 오류를 정정할 때까지 해당 사용자의 개인정보 이용 및 제공을 중단하고 있는가?		
외부위탁 또는 제3자에게 제공한 개인정보가 있을 경우 이에 대해서도 정정 및 동의철회에 대한 조치를 취하고 결과를 확인하는가?		
정보주체 및 법정대리인이 언제든지 개인정보 사용에 대한 동의를 철회할 수 있는 방법 및 절차가 있는가?		
정보주체 및 정보주체의 법정대리인이 정보주체의 개인정보 수집·이용·제공 등의 동의철회를 요청할 경우 지체없이 수집된 개인정보를 파기하는 등 필요한 조치를 취하는가?		
정보주체가 동의의 철회, 개인정보의 열람·제공 또는 오류의 정정을 요구하는 방법은 개인정보의 수집 방법보다 쉬운가?		
정보주체가 개인정보 수집·이용·제공 등의 동의철회 또는 개인정보의 열람·제공, 오류의 정정 등을 요구할 경우 지연 또는 거절 시 타당한 사유에 근거하고 있는가?		
제3자에게 정보주체의 개인정보 처리 업무를 위탁하는 경우 관련 사항을 정보주체에게 알리는가?		
개인정보 취급위탁에 대한 동의 획득 시, 개인정보 수집 시와 동일한 방법으로 동의를 받는가?		
개인정보 취급 위탁 시 수탁업체 변동 또는 위탁업무 범위 및 계약상의 변동사항이 발생할 경우 정보주체로부터 별도의 동의절차를 거치고 있는가?		
업무위탁 시는 개인정보 취급 목적을 미리 정하고, 수탁사가 취급 목적을 벗어나서 정보주체의 개인정보를 취급하지 않도록 관리하는가?		
수탁사가 개인정보취급 시 법규정을 위반하였을 경우 처리 및 배상에 관한 절차가 있는가?		
수탁자로부터 개인정보보호와 관리 상황을 주기적으로 보고 받고, 정기 또는 수시점검을 통해 관리감독하고 있는가?		
외부위탁 계약 시 개인정보보호와 관련한 법적 요건 및 조직의 개인정보보호 정책을 만족하기 위한 요구사항을 계약서상에 명시하였는가?		
정보주체의 개인정보를 제3자에게 제공하는 경우 다음 각 호의 사항에 대하여 정보주체에게 알리고 동의를 얻는가? 1.개인정보를 제공 받는 자 2.개인정보를 제공 받는 자의 개인정보 이용 목적		

점검내용	상태	확인자
3.제공하는 개인정보의 항목 4.개인정보를 제공 받는 자의 개인정보 보유 및 이용기간		
개인정보의 제3자 제공과 관련하여 사전에 정보주체에게 고지한 사항 중 변경이 발생한 경우 사용자에게 알리고 동의를 얻는가?		
개인정보를 제공받은 경우 제공받은 목적 외의 용도로 이용하지 않는가?		
제공받은 개인정보를 또 다른 제3자에게 제공할 경우, 법률에 근거한 사항이거나 정보주체의 동의를 받고 있는가?		
법규정 혹은 정보주체의 동의에 따라 개인정보를 제공할 경우 사안 별 적법성을 확인하고 승인 및 기록을 남기는 등의 절차가 있는가?		
제3자에 개인정보를 제공 시, 제공 후에도 보안요구사항이 준수될 수 있도록 이와 관련된 항목을 계약서 상에 명시하고 있는가?		
영업의 양도, 합병 등으로 개인정보를 이전할 경우 필요한 사항을 사용자에게 미리 통지하는가?		
영업의 양도, 합병 등으로 개인정보를 이전하려는 경우 전자우편, 서면, 팩스, 전화 또는 이와 유사한 방법으로 통지하는가?		
양도자가 이전한 사실을 통지하지 않고 영업의 양도, 합병 등으로 개인정보를 이전받았다면, 지체없이 그 사실을 사용자에게 통지하였는가?		
영업의 양도, 합병 등으로 개인정보를 이전받은 경우 양도자가 정보주체의 개인정보를 이용하거나 제공할 수 있는 당초의 목적 범위 안에서만 개인정보를 이용하거나 제공하는가?		
영업의 양도, 합병 등으로 개인정보를 이전받아 양도자가 정보주체의 개인정보를 이용하거나 제공할 수 있는 당초의 목적 범위 외로 개인정보를 이용하거나 제공하고자 하는 경우, 별도로 정보주체의 동의를 얻는가?		
개인정보의 해외 이전 시 국내법 및 해당 국가의 법을 만족하는 공식적인 계약을 체결하였는가?		
개인정보의 해외 이전 시 이전 목적을 사전에 사용자에게 고지하고 동의를 얻었는가?		
해외 이전된 개인정보에 대하여 기술적, 관리적 보호조치를 취하고 있는가?		

5. 개인정보 파기 점검항목

점검내용	상태	확인자
수집된 개인정보는 정확하고 최신의 상태로 유지되는가?		
개인정보의 수집 및 이용목적이 달성된 경우 지체없이 개인정보를 파기하는가?		
사업을 폐지하는 경우 지체없이 개인정보를 파기하는가?		
개인정보를 파기하여야 하는 경우, 위탁 또는 제3자에게 제공한 개인정보도 함께 지체없이 파기하는가?		
저장 매체에 저장된 개인정보 파기 시 복구할 수 없는 방법으로 파기하였는가?		
개인정보가 기재된 종이문서의 경우 쇄절, 소각 등을 통해 파기하였는가?		

[별지 제3-1호 서식] 보안감사 결과 보고서

보 안 감 사 결 과 보 고 서

작성일자: 20 년 월 일

감 사 구 분	☐ 정 기 감 사 ☐ 수 시 감 사		
감 사 부 서			
감사목적/요건항목		감 사 장 소	
감 사 팀	감사인 :		

감사대상/범위/목적

1. 보안규칙 및 관계 지침의 업무 프로세스를 중심으로 정보보안시스템의 유효성 및 적합성 확인
2. 정보보안 및 개인정보보호의 실행상태 점검 후 보완을 통하여 조기에 정착시키는데 목적이 있음.

감사결과/지적사항

1.교학처(건), 기획처(건), (건), (건), (건)

2.세부 지적사항- 별첨

정보보안시스템의 유효성 :

☐ ACCEPTABLE ☐ REASON & RECOMMENDATON

감 사 결 론 :

1. 정보보안

2. 개인정보보호

조사자료 명세 및 첨부물: 감사점검표, 부서별 지적사항 및 시정조치 요구서 등

감사결과보고서 배부/회람 :

작 성 :_____ 검 토 :_____ 승 인 :_____

일 자 :____/____/____ 일 자 :____/____/____ 일 자 :____/____/____

[별지 제3-2호 서식] 부서별 지적사항(부적합사항)

부서별 지적사항 (부적합 사항)

부서명	시스템구분 (정보보안/ 개인정보보호)	지 적 사 항	관 련 문 서	요건번호	비 고
각 부서 공 통					
교학처	정보보안				
	개인정보보호				
기획처	정보보안				
	개인정보보호				
사무처	정보보안				
	개인정보보호				

[별지 제4호 서식] 보안감사 시정조치 보고서

보안감사 시정조치 보고서

감사구분	□ 정 기 감 사	□ 수 시 감 사	
부서명		감사일자	
작성자 (피감사부서장)		작성일자	
지적사항 1. 2.			
시정조치계획 및 조치 결과 1. 2. 시정조치 완료 일자 :			
첨 부			

결 재	
직위	서명