정보시스템 보안 운영 지침

제정 2014. 9.18.

제1조(목적) 이 지침은 한국방송통신대학교(이하 “우리대학교”) 정보시스템 보안 운영·관리 업무 전반에 대한 사항을 정함을 목적으로 한다.

제2조(용어 정의) 이 지침에서 사용하는 용어는 다음 각 호와 같다.

1. “사용자”라 함은 총장으로부터 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 자를 말한다.
2. “정보통신망”이라 함은 「전기통신기본법」 제2조2호의 규정에 의한 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송수신하는 정보통신체제를 말하며 정보시스템 일체를 포함한다.
3. “정보시스템”이라 함은 서버·PC 등 단말기, 보조기억매체, 네트워크 장치, 응용 프로그램 등 정보의 수집·가공·저장·검색·송수신에 필요한 하드웨어 및 소프트웨어를 말한다.
4. “침입차단시스템(Firewall)”이라 함은 내부의 네트워크와 외부의 네트워크 사이에 진입 장벽을 구축하는 네트워크 정책과 이를 지원하는 하드웨어 및 소프트웨어를 포괄하는 컴퓨터 보안 시스템을 말한다.
5. “침입방지시스템(IPS, intrusion prevention system)”이라 함은 인터넷 웜 등의 악성코드 및 해킹 등을 통한 침입이 일어나기 전에 실시간으로 침입을 막고 알려지지 않은 방식의 침입으로부터 네트워크와 호스트 컴퓨터를 보호하는 솔루션을 말한다.
6. “분산서비스거부공격방지시스템(DDoS, distributed denial-of-service attack prevention system)”이라 함은 해커가 감염시킨 대량의 좀비 컴퓨터를 이용해 특정 시스템으로 다량의 패킷을 무차별적으로 보내 과다 트래픽으로 시스템을 마비시키는 사이버 공격을 방지하는 시스템을 말한다.
7. “웹 방화벽(Web Application-Firewall)’이라 함은 특정 공격코드 또는 특정 웹어플리케이션만이 가지고 있는 취약점을 우회하는 공격을 방어하는 시스템을 말한다.
8. “서버접근제어시스템’이라 함은 내부망 서버 자산에 인증을 통해 인가자만 접근이 가능하고 비인가자는 차단하도록 만들어진 시스템을 말한다.
9. “정보보안” 또는 “정보보호”라 함은 정보시스템 및 정보통신망을 통해 수집·가공·저장·검색·송수신되는 정보의 유출·위변조·훼손 등을 방지하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위로서 사이버안전을 포함한다.
10. “전자문서”라 함은 컴퓨터 등 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 정보를 말한다.
11. “전자기록물”이라 함은 정보처리능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 기록정보자료를 말한다.
12. “정보보안시스템”이라 함은 정보의 수집·저장·검색·송신·수신 시 정보의 유출, 위·변조, 훼손 등을 방지하기 위한 하드웨어 및 소프트웨어를 말한다.
13. “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
14. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

제3조(업무수행) ① 「한국방송통신대학교 보안업무처리규정」 제3조3항에 의거 대학의 정보통신보안 업무는 정보보안담당관이 수행한다.

② 「교육부 사이버분야 위기대응 실무매뉴얼」에 의거 대학의 사이버 안전을 위한 침해사고 대응 업무를 수행한다.

제4조(운영·관리) ① 우리대학교에서 운영 · 관리중인 모든 정보시스템을 대상으로 침해대응 업무를 수행하되, 정보보안 및 개인정보보호 관련 문제에 대한 1차적 책임은 해당 기관(부서) 또는 개인에게 있으며 이에 대한 자체 보안대책이 강구되어야 한다.

② 정보보안 및 개인정보보호 운영 · 관리 업무는 다음 각 호에 따른다.

1. 개인 또는 기관(부서)에서 운영 중인 PC · 서버시스템의 정보보안 및 개인정보보호 강화를 위한 업무 활동으로 사이버보안진단의 날을 수행한다.
2. 정보전산원 시스템운영실에서 관리·운영하는 대학 주요 전산장비 및 S/W 프로그램은 정부 및 정보 보안 관련 유관기관에서 제공 · 권고하는 각종 보안점검 매뉴얼을 참조하여 정보보안 및 개인정보보호 제반 업무를 수행 하며, 침해 예방 및 사고 발생 시 관련 대응 업무는 「교육부 사이버분야 위기대응매뉴얼」에 의한다.
3. 기관(부서) 및 개인이 구축하여 관리 · 운영 중인 S/W형태의 정보시스템은 자체적으로 정보보안 및 개인정보보호 제반 업무를 수행한다.
4. 침입차단시스템 운영함에 있어 신규 정책을 추가하고자 하는 경우 「별표1」에 따라 공문으로 사용신청을 하며 정보전산원장의 승인을 얻은 후 사용한다.
5. 침입차단시스템, 침입방지시스템, 분산서비스거부공격방지시스템, 웹방화벽, 서버접근제어시스템 등 정보보안시스템은 주기적 패치적용, 보안정책 보호와 갱신을 통해 최신성을 유지한다.
6. 개인정보보호시스템 운영은 시스템 영역에서 운영하는 서버용 개인정보검사 소프트웨어와 사용자 스스로 운영하는 PC용 개인정보검사 소프트웨어로 나누며, 서버용에서는 고유식별번호, 비방, 광고 등이 정보시스템에 게시되지 않도록 하는 것에 목적을 두고 운영한다.
7. 서버용 개인정보 검사 소프트웨어의 변경 패턴에 대한 최신 업데이트를 상시적으로 수행하며, 활용을 위해서는 기관(부서)에서 「별표2」에 따라 공문으로 요청하며 정보전산원에서는 활용 방법 및 모듈을 제공한다.
8. PC용 개인정보 검사 소프트웨어는 사용자 PC내에 개인이 보관하고 있는 개인정보파일을 검출/암·복호화 하는 용도로 사용한다.
9. PC용 개인정보 검사 소프트웨어 관리자 검사는 분기별 1회를 원칙으로 수행하며, 해당 결과에 대해서는 문서로 전 기관(부서)에 통보함으로써 개인정보 관리에 최선을 다한다.
10. 정보시스템 보안 정책 및 운영 현황은 대외적으로 유출되지 않도록 관리한다.

제5조(접근관리) ① 대학의 모든 정보보안시스템 및 개인정보보호시스템은 적절한 권한에 의해 접속되어야 한다.

② 대학의 정보보안시스템을 지정된 위치가 아닌 외부에서 접속하고자 할 경우에는 보안이 적용된 가상사설망을 통해 접속하여야 한다.

③ 외부 용역 및 유지보수 업체가 대학의 요청에 의해 정보보안시스템에 접근 할 경우엔 반드시 자필 서명된 「별표3-1, 3-2」의 보안서약서를 제출하여야 한다.

제6조(이용제한) ① 「교육기관 정보보안 기본지침」에 의거 대학 내 · 외부 침해 유발 가능성이 있는 정보시스템(PC, 서버, 네트워크, 응용프로그램 등)에 대해서는 정보통신망 접속을 일시적으로 제한하고, 문제 해결 지원을 통해 조치 완료 후 서비스를 이용할 수 있도록 한다.

② 이외 이용제한 필요 시 「한국방송통신대학교 보안업무처리규정」에 의거 보안심사위원회에 심의를 거쳐 그 여부를 결정한다.

제7조(교육) ① 정보보안 및 개인정보보호와 관련한 사용자 교육을 요청할 시 지원할 수 있다.

② 정보보안 관련 제반 교육은 다음 각 호를 포함한다.

1. 대학 학사/행정종합정보시스템 이용에 관한 사항
2. 전자문서 등 전자기록물 등록 및 이용에 관한 사항
3. 대학 정보보호 관련 규정 및 지침에 관한 사항

4. 대학 정보보호 침해대응 체계 및 처리 절차에 관한 사항

제8조(장비 도입 및 처분) ① 정보보안시스템 도입은 보안적합성 검증 기준 절차에 따라 수행한다.
② 장비의 처분에 관련한 사항은 법령 및 대학 내의 제 규정에 따른다.

제9조(기타) 이 지침에 언급되어 있지 않는 정보시스템 보안 및 개인정보보호에 관한 사항은 「한국방송통신대학교 정보보안 기본지침」등 상위 법령 · 규정 및 지침에 따른다.

부 칙

제1조(시행일) 이 지침은 공포한 날부터 시행한다.

「별표1」

방화벽 정책 사용 신청서

1. 책임자 인적사항

성 명		직위(직급)	
소 속			
전 화		e-mail	

2. 담당자 인적 사항

성 명		직위(직급)	
소 속			
전 화		e-mail	

3. 사용 요청 기간

영 구		
임 시		20 . . . ~ 20 . . .

4. 정책 내용

구 분	출발지 IP	목적지 IP	사용 Port
내 용			

5. 목적 및 사유
- 서비스 사유에 대하여 기술 할 것

6. 정책에 대한 보안 유의 사항
- 본 정책에 대한 일체의 내용을 제3자에게 누출해서는 안 됨
- 유출로 인한 보안사고 발생 시 민·형사상의 책임이 있음

한국방송통신대학교 정보전산원장 귀하

「별표2」

서버용 개인정보 검사 소프트웨어 사용 신청서

1. 책임자 인적사항

성 명		직위(직급)	
소 속			
전 화		e-mail	

2. 담당자 인적 사항

성 명		직위(직급)	
소 속			
전 화		e-mail	

3. 사용 요청 기간

영 구		
임 시		20 . . . ~ 20 . . .

4. 요청 내용

구 분	웹서버 종류 및 버전	웹서버 IP	사용 Port
내 용			

※ 웹서버 종류 : Apache Tomcat 6.0.35, Webtob 4.1

5. 목적 및 사유

- 서비스 사유에 대하여 기술 할 것

6. 정책에 대한 보안 유의 사항

- 본 정책에 대한 일체의 내용을 제3자에게 누출해서는 안 됨
- 유출로 인한 보안사고 발생 시 민·형사상의 책임이 있음

한국방송통신대학교 정보전산원장 귀하

「별표3-1」

보안서약서(업체개인용)

본인은 년 월 일부로 _____과 관련한 업무(연구개발, 제작, 입찰, 그 밖의 업무)를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 _____과 관련된 소관업무가 기밀 사항임을 인정하고 제반 보안관계규정 및 지침을 성실히 준수한다.
2. 본인은 이 기밀을 누설함이 이적행위가 됨을 명심하고 재직 중은 물론 퇴직 후에도 알게 된 모든 기밀사항을 일절 타인에게 누설하지 아니한다.
3. 본인은 기밀을 누설한 때에는 아래의 관계법규에 따라 엄중한 처벌을 받을 것을 서약한다.

   가. 「국가보안법」 제4조 제1항 제2호 · 제5호(국가기밀 누설 등)

   나. 「형법」 제99조 (일반이적) 및 제127조(공무상 비밀의 누설)

년 월 일

서약자 소속 직급 생년월일

직위 성 명 인

서 약 소속 직급 성 명 인

집행자 직위

「별표3-2」

보 안 서 약 서 (업 체 대 표 자 용)

본인은 ____년 __월 __일부로 _____관련 용역사업(업무)을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 _____관련 업무 중 알게 될 일체의 내용이 직무상 기밀 사항임을 인정한다.

2. 본인은 이 기밀을 누설함이 국가안전보장 및 국가이익에 위해가 될 수 있음을 인식하여 업무수행 중 지득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.

3. 본인은 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다.

4. 본인은 하도급업체를 통한 사업 수행 시 하도급업체로 인해 발생하는 위반사항에 대하여 모든 책임을 부담한다.

년 월 일

서 약 자 (업체 대표)	업 체 명 :	
	직 위 :	
	성 명 :	(서명)
	생 년 월 일 :	
서약집행자 (담당공무원)	소 속 :	
	직 위 :	
	성 명 :	(서명)
	생 년 월 일 :	