[별표 7] 용역사업 보안 점검표(제27조 관련)

용역사업 보안 점검표

○ 입찰 및 계약시

구분	보안 대책	확인
사업 착수 및 입찰시	중요 정보화 사업의 경우 사업 착수단계부터 사업계획 전반에 대해 적정등급의 비밀 또는 대외비로 분류	
	입찰 공고 이전에 보안관리가 필요한 자료·장비에 대해 투입이전에 관련법규에 따라 등급을 분류하고 필요한 요구사항을 마련	
	입찰 공고 시 누출금지 대상정보, 부정당업자 제재조치, 기밀유지 의무 및 위반 불이익 등에 대해 정확히 공지	
	제안서 평가요소에 보안관리 계획에 대한 평가항목 및 배점기준 마련	
	제안서에서 제시한 용역사업 전반에 대한 보안관리 수행계획의 타당성 검토	
	웹호스팅 등 정보시스템 위탁 운영시 정보보호시스템 구비 및 보안관리 가능 여부 검토	
사업 계약시	발주기관의 요구사항이 과업지시서·계약서에 명확히 명시될 수 있도록 중요 항목(보안조치·누출금지대상·제재조치)을 정확히 기술	
	용역업체가 사업에 대한 하도급 계약을 체결한 경우 원래 사업계약수준의 비밀유지 조항 포함	
	대외보안 필요시 비밀유지 계약서에 비밀정보 범위, 보안 준수사항, 위반시 손해배상 책임, 지적재산권 문제, 자료 반환 등 중요항목 명시	

○ 사업 수행시

구분	보안 대책	확인
인원 및 물리적 보안 관리	사업 참여인원 신원확인 실시	
	사업 참여인원 보안서약서 징구	
	사업 수행 전 참여인원에 대해 비밀유지 의무 준수·누출금지 대상 정보·위반시 처벌내용 등에 대한 보안교육 실시	
	사업 수행 중 참여인원에 대한 보안점검을 실시하여 '누출금지 대상정보'의 외부 누출여부 확인	
	발주기관 내부: 시건장치와 통제가 가능한 공간 제공 여부 발주기관 외부: CCTV·시건장치 등 비인가자 출입통제 대책이 마련된 외부 사무실 이용 여부	
	CCTV 등 통제장치의 관리상태(작동여부, 사각지대 보완 등) 및 기록 확인	
전산망 보안 관리	업체 사용 전산망은 방화벽 등을 활용하여 기관 업무망과 분리구성하고 업무상 필요한 서버에만 제한적 접근 허용	
	업체 PC 인터넷 연결 차단여부 및 인터넷 접속허용 PC에 대한 보안조치	
	비인가 무선 AP(무선공유기, 스마트폰 핫스팟 등) 설정을 금지하고 휴대형 무선모뎀(Wibro, HSDPA, WiFi 등)반입 통제	
	스마트폰·휴대폰을 무선 모뎀으로 활용하지 못하도록 통제수단 강구(PC에 비인가 통신기기 접속차단 S/W설치, 스마트폰 접속단자 봉인조치 등)	
	노트북PC 반입시 무선통신 기능 불능화 조치(driver 삭제 등) 시행	
	기관 외부에서 기관 내부의 시스템 개발 PC 및 기관 시스템에 원격접속 금지	
	업체 직원의 계정은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 부여하되 기관 내부문서 접근 금지	
	업체 직원의 'root' 계정 등 시스템에 중대한 영향을 끼칠 수 있는 계정에 대한 단독 접근 금지	
	계정별로 부여된 권한은 불필요시 곧바로 해지하거나 계정 폐기	
	업체 직원의 작업내용 확인을 위해 작업이력 로깅기능 구축	
	사업 책임자는 서버 및 장비 운영자로 하여금 내부서버 및 네트워크 장비에 대한 접근기록을 매일 확인하여 이상 유무 보고	

구분	보안대책	이행 실태
자료 보안 관리	계약서 등에 명시한 누출금지 대상정보를 업체에 제공할 경우, 자료 인계인수대장을 작성하고, 인계자·인수자가 자필로 서명한 후 제공	
	사업 관련 자료는 웹하드, P2P, 웹오피스, 클라우드 서비스 등 인터넷 자료공유사이트 및 개인 메일함에 저장 금지	
	사업 관련자료 및 모든 산출물은 기관의 파일서버에 저장하거나 사업 책임자가 지정한 PC(인터넷 연결차단)에 저장 및 관리	
	발주기관이 제공한 사무실에서 사업을 수행할 경우 기관이 제공한 비공개 자료는 매일 퇴근시 반납	
	사업 수행으로 생산되는 산출물 및 기록은 비인가자에게 제공, 대여, 열람 금지	
	비밀번호는 정보보안담당관이 별도로 기록·관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력 확인	
전산 장비 및 매체 보안 관리	업체 전산장비는 보안담당관 승인 후 반입·반출 * 반출시 보안담당관 통제하에 저장자료 완전 삭제	
	전산장비 반입·반출시마다 악성코드 감염여부 점검 및 자료 무단 반출입 여부 확인	
	업무망 접속용 전산장비와 인터넷망 접속용 전산장비를 구분하여 활용 및 망간 혼용 금지	
	업체 노트북PC, 휴대용 저장매체 정기 보안점검	
	업체 휴대용 저장매체 사용이 불가피할 경우 보안담당관 승인 후 사용	
	노트북·PC, 휴대용 저장매체는 시건장치가 있는 보관함에 보관	
	인터넷망 접속이 필요한 전산장비사전 지정 및 보안조치 실시	
	업무에 필요한 사이트에만 접속토록 방화벽 등을 통해 통제 * P2P, 웹하드, 메신저 등 인터넷 자료공유사이트 활용 원천차단	
	인터넷 접속허용 전산장비에 사업 관련 자료 저장 금지	
	최신 백신 프로그램 설치 및 주기적인 전체 파일 검사 실시	
	비밀번호·화면보호기 설정 및 정기적 변경	
	비인가 저장매체·통신기기 접속 통제 * 매체제어 미설치 전산정비는 외부기기 연결단자 보안스티커 부착	

○ 완료 단계

구분	보안대책	이행 실태
용역 사업 완료시	사업 완료 후 생산되는 최종 산출물 중 대외보안이 요구되는 자료에 대해 대외비 이상으로 작성·관리하고 불필요한 자료는 삭제 및 폐기	
	업체에게 제공한 사업과 관련된 제반자료는 전량 회수 및 자료관리대장에 기록하고 업체는 복사본 별도 보관 금지	
	업체에 복사본 등 사업 관련 자료를 일체 보유하고 있지 않다는 업체 대표 명의의 보안확약서를 징구	
	업체 소유 PC·서버의 하드디스크, 휴대용 저장매체 전자기록저장매체는 검증필 삭제S/W로 완전 삭제, 보안담당자 승인 후 반출	
	업체에서 설정한 정보시스템의 계정과 비밀번호 변경조치	