

<별표 5-2> 보안관리방안 <신설 2015.4.8> <개정 2016.11.10>

단계	세부사항
입찰	○ 입찰 공고 이전에 투입이 예상되는 자료·장비 가운데 보안관리가 필요한 사항에 대하여 금융회사 또는 전자금융업자의 내부관리기준과 관련 법규를 검토하고 필요한 보안요구 사항을 마련 ○ 입찰 공고시에 금융회사 또는 전자금융업자가 자체 작성한 중요정보, 부정당업자 제재조치, 기밀 유지 의무 및 위반시 불이익 등을 정확히 공지 ○ 제안서 평가요소에 자료·장비·네트워크 보안대책 및 중요정보 관리 방안 등 보안관리 계획의 평가항목 및 배점기준 마련 ○ 업체가 입찰제안서에 제시한 용역사업 전반에 대한 보안관리 계획이 타당한지를 검토하여 사업자 선정시에 이를 반영
계약	○ 계약서 작성 초기 단계부터 정보보안사항 포함여부에 대한 검토 실시 ○ 용역사업에 투입되는 자료·장비 등에 대해 대외보안이 필요한 경우 보안의 범위·책임을 명확히 하기 위해 사업수행 계약서와 별도로 비밀유지계약서 작성 ○ 비밀유지계약서에는 비밀정보의 범위, 보안준수 사항, 위반시 손해배상 책임, 지적재산권 문제, 자료의 반환 등이 포함되도록 명시 ○ 용역사업 참여인원은 금융회사 또는 전자금융업자의 사전 동의 없이 용역업체가 임의로 교체할 수 없도록 명시 ○ 금융회사 또는 전자금융업자의 요구사항을 사업자에게 명확히 전달키 위하여 작성하는 과업지시서·계약서(입찰 공고 포함)에 인원·장비·자료 등에 대한 보안조치 사항과 정보유출 및 부정당업자에 대한 손해배상 내용 등을 정확히 기술 ○ 용역업체가 사업에 대한 하도급 계약을 체결할 경우 원래 사업계약 수준의 비밀 유지 조항을 포함토록 조치 ○ 규정 제7조 각호에 규정한 사항의 준수를 위하여 외부주문업체 등의 협조가 요구되는 사항
수행	[인력] ○ 용역사업 참여인원에 대해서는 '정보 유출' 방지 조항 및 개인의 자필 서명이 들어간 보안서약서 징구 ○ 용역사업 수행前 참여인원에 대해 법적 또는 금융회사 또는 전자금융업자의 규정에 따른 비밀유지 의무 준수 및 위반시 처벌내용 등에 대한 보안교육 실시 * 유출 금지 대상정보 및 정보 유출시 부정당업자 제재조치 등에 대한 교육 병행 ○ 금융회사 또는 전자금융업자는 사업 수행 중 업체 인력에 대한 보안점검 실시, '유출금지 대상 정보' 외부 유출여부 확인 [자료] ○ 계약서 등에 명시한 중요정보를 업체에 제공할 경우 자료관리 대장을 작성, 인계자·인수자가 직접 서명한 후 제공하고 사업완료시 관련자료 회수 ○ 용역사업 관련자료 및 사업과정에서 생산된 모든 산출물은 금융회사 또는 전자금융업자의 파일 서버에 저장하거나 금융회사 또는 전자금융업자가 지정한 PC에 저장·관리 ○ 용역사업 관련 자료는 인터넷 웹하드·P2P 등 인터넷 자료공유사이트 및 개인메일함에 저장을 금지하고 금융회사 또는 전자금융업자와 용역업체간 전자우편을 이용해 전송이 필요한 경우에는 자체 전자우편을 이용하고, 첨부자료 중 중요정보 포함자료는 암호화 후 수신

	○ 금융회사 또는 전자금융업자가 제공한 사무실에서 업체가 용역사업을 수행할 경우, 유출금지 대상 정보가 포함된 자료는 매일 퇴근시 시건장치가 된 보관함에 보관 ○ 용역사업 수행으로 생산되는 산출물 및 기록은 금융회사 또는 전자금융업자가 인가하지 않은 비인가자에게 제공·대여·열람을 금지 [사무실·장비] ○ 용역사업 수행장소는 금융회사 또는 전자금융업자 전산실 등 중요시설과 분리하고 CCTV·시건장치 등 비인가자의 출입통제 대책을 마련 ○ 용역업무를 수행하는 공간에 대한 보안점검을 정기적으로 실시 ○ 용역직원이 노트북 등 관련 장비를 외부에서 반입하여 내부망에 접속시 악성코드 감염여부 및 반출시마다 자료 무단반출 여부 확인 ○ 인가받지 않은 USB메모리 등의 휴대용 저장매체 사용을 금지하며 산출물 저장을 위하여 휴대용 저장매체가 필요한 경우 금융회사 또는 전자금융업자의 승인하에 사용 [내·외부망 접근시] ○ 금융회사 또는 전자금융업자는 개발시스템과 운영시스템을 분리하고, 용역업체는 업무상 필요한 서버에만 제한적 접근 허용 ○ 용역사업 수행시 금융회사 또는 전자금융업자 전산망 이용이 필요한 경우 - 사업 참여인원에 대한 사용자계정(ID)은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 차등 부여하되 허용되지 않은 금융회사 또는 전자금융업자의 내부분서 접근 금지 - 계정별로 부여된 접속권한은 불필요시 즉시 해지하거나 계정을 폐기 - 참여인원에게 부여한 계정은 별도로 기록 관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력 확인 - 금융회사 또는 전자금융업자는 내부서버 및 네트워크 장비에 대한 접근기록 이상 여부를 정기 점검 ○ 용역업체에서 사용하는 PC는 인터넷 연결을 금지하되, 사업수행상 연결이 필요한 경우에는 금융회사 또는 전자금융업자의 보안통제하에 제한적 허용 ○ 용역업체 사용 전산망에서 P2P, 웹하드 등 인터넷 자료공유사이트로의 접속을 원천 차단
완료	○ 사업 완료 후 생산되는 최종 산출물 등 대외보안이 요구되는 자료는 대외비 이상으로 작성·관리하고 불필요한 자료는 삭제 및 폐기 ○ 용역업체에 제공한 자료, 장비와 중간·최종 산출물 등 용역과 관련된 제반자료는 전량 회수하고 업체에 복사본 등 별도 보관 금지 ○ 용역사업 완료 후 업체 소유 PC·서버의 하드디스크·휴대용 저장매체 등 전자기록 저장매체는 복원이 불가능한 방법으로 완전 삭제 후 반출 ○ 용역사업 관련자료 회수 및 삭제조치 후 업체에게 복사본 등 용역사업관련 자료를 보유하고 있지 않다는 대표자 명의의 협약서 징구