API 연계 솔루션
구축 시방서

2026. 11.



성신여자대학교
SUNGSHIN WOMEN'S UNIVERSITY

Ⅰ. 일 반 사 항

1. 목적

본 시방서는 API 연계 솔루션 도입을 위한 신규 S/W 도입·설치하는데 있어서 구매조건 및 규격 명시와 계약 시 이행되어야 할 세부 내용을 규정함에 있다.

가. “갑” : 성신여자대학교 (이하 “갑”이라 함)

나. “을” : 계약업체 (이하 “을”이라 함)

2. 사업명

API 연계 솔루션 도입

3. 사업기간

계약일로부터 90일 이내

4. 소프트웨어 설치장소

성신여자대학교 IT운영팀 시스템실

5. 사업 범위

다음 각 호의 사항을 준하며 세부내역은 “Ⅱ. 특수조건”과 “규격서”에 따른다.

6. 입찰자격조건

가. 국가를 당사자로 하는 계약에 관한 법률시행령 제12조(경쟁입찰의 참가자격) 및 동법 시행규칙 제14조(입찰참가자격요건의 증명)에 의한 유적격자로 기간 내 입찰등록을 마친 업체

나. 제품 품질의 신뢰성과 원활한 운영을 위하여 직접 물품공급이 가능한 업체이며, 제조사(또는 국내지사)로부터 물품공급 및 기술지원확약서를 제출할 수 있는 업체이어야 한다.

7. 무상유지보수

무상유지보수기간은 S/W 전체를 검수일로부터 1년으로 한다.(메이저 업그레이드 포함)

8. 계약조건

가. “을”은 시방서에 명시된 물품일체를 일괄 공급방식으로 납품·설치하여야 하며 “을”이 납품하는 물품은 입찰등록 마감일을 기준으로 제조사가 단종하는 기종이어서는 안되며, 기 생산된 제품의 성능향상을 발표하고 모델명을 달리한 경우도 이에 해당하는 것으로 본다.

나. “갑”은 설치된 시스템이 본 시방서에서 요구하는 성능, 사양을 수용할 수 없다고 판단되면 “을”에

게 설치 변경을 요구할 수 있으며 “을”은 이에 응하여야 한다.

다. 소프트웨어 구매·설치 시방서에 해석상의 이견이 있을 때에는 “갑”의 해석에 따르고, 시방서에 명시되지 않은 사항은 “갑”의 국가를 당사자로 하는 계약에 관한법률과 기타계약에 관한법령, 예규를 준용한다.

라. 소프트웨어 설치에 따른 운반, 설치 시험 등을 할 때에는 사전협의 후 승인을 받아 시스템 및 프로그램을 설치하고, 시스템의 정상적인 설치와 관련하여 발생되는 경비는 “을”이 부담한다.

마. 검수 완료 후에라도 본 시스템의 운영과 관련된 “을”의 책임으로 발생되는 모든 사고와 그로 인한 손해에 대해 “을”이 변상 조치하여야 한다.

Ⅱ. 특 수 조 건

본 특수조건에 명시될 사항은 시스템을 구매·설치하는 데 있어서 “갑”과 “을” 간에 성립되어야 할 구매 물품의 설치·납품조건, 방법 및 시험운영, 교육지원 등 계약 이행에 관한 사항에 대하여 적용하며 계약문서로서의 효력을 가진다.

1. 구매조건

가. 납품하는 물품의 모든 구성품은 물품의 세부 규격을 100% 만족시키는 정품, 완제품, 신품으로 공급되어야 한다.

나. 납품·설치하는 시스템 및 관련 S/W에 대하여 H/W 구성, 통신망(LAN) 연결 등이 “갑”의 완전한 목적수행에 전혀 지장이 없도록 하여야 하며, 품질의 신뢰성, 제품의 안정성과 “갑”의 기존 시스템과의 호환성에 아무런 문제없이 일괄 납품, 설치해야 한다.

다. 모든 소프트웨어는 라이선스를 포함한 정품으로 납품하고 원소유자의 저작권을 침해하지 않아야 한다. 이 경우 “갑”이 필요하다고 인정되는 경우를 제외하고 최신 버전을 납품하여야 한다.

2. 시스템 납품 및 설치

가. “을”은 “갑”이 도입하고자 하는 제품의 안정적인 납품 및 설치를 위해 계약체결 후 7일 이내에 사업수행계획서를 작성하여 제출하여야 한다.

나. 제품의 납품·설치는 “갑”의 업무에 지장을 초래하지 않는 시간을 이용하여 작업하여야 하며, 기존 시스템의 운용에 전혀 지장이 없도록 하여야 한다.

다. “을”은 시스템을 설치할 때 “갑”의 운영 중인 서버 및 부대장비, 네트워크 등에 전혀 지장이 없도록 완벽한 호환과 정상가동이 이루어지도록 하여야 하며, 손상 시에는 “을”의 비용으로 즉각 원상복구 하여야 한다.

라. 기존 전산장비의 접속 및 상호연동을 위하여, 기존 장비들의 환경을 변경할 필요가 있을 시에는 “갑”의 승인을 얻은 후 “을”의 책임하에 조치하여야 한다.

3. 제품 검수

가. 검수의 대상범위는 본 시방서에 의한 시스템의 납품, 설치 및 기존 서비스의 정상 가동여부에 대한 확인과정을 포함한다.

나. “을”의 입회 하에 현장확인 검사를 실시하고 규격확인이 곤란하거나 미흡한 경우 “을”은 관련 증빙서류를 추가로 제출하여 “갑”이 인정할 수 있도록 하여야 한다.

다. “을”은 검수에 필요한 시스템 개요와 운영관련 기술을 “갑”에게 충분히 제공하여야 하며 시험가동과 검수에 필요한 물품은 “을”이 무상으로 제공하여야 한다.

라. “을”은 소프트웨어 설치 후 시험가동을 실시한 후 그 결과, 문제가 없을 경우 검수 요청을 하여야 하며, 시험가동 시 발견되는 오류나 불합리한 문제점, 시스템 보안요구 등에 대해서는 즉시 조치하여야 한다.

마. 최종 검수 결과 시스템 운영이 불가하다고 판단되거나 소프트웨어 하자발생으로 계약조건을 이행하지 못하는 것으로 판단될 시 “갑”의 요구에 의해 “을”은 납품·설치한 모든 소프트웨어

를 철거 및 회수해야 하며 기존 장비를 원상태로 복구하여야 하며 그 비용은 “을”의 부담으로 한다.

4. 교육 및 운영지원

가. “을”은 시스템 운영 및 장애 조치 등에 필요한 기술이전을 “갑”의 담당자에게 충실히 이행하여야 하며 “갑”이 자체 유지관리 능력을 갖출 수 있도록 S/W에 대한 운영자 교육을 실시하여야 한다.

나. “을”은 시스템 검수 후 다음과 같은 사항을 지원하여야 한다.

1) 납품 시스템(S/W)의 전반적인 보완, 개선작업

2) 장애 발생시 신속한 복구 및 기술 지원

3) “갑”이 요구하는 기존 연계 서비스를 솔루션을 활용한 API 연계로 전환 작업 지원

5. 유지보수 및 기술지원

가. 무상 유지보수기간 중 “을”은 “갑”이 항상 기기를 최적의 상태에서 사용할 수 있도록 유지보수하여야 하며, 유지보수에 소요되는 부품 및 제반 비용은 “을”의 부담으로 한다.

나. 장애 발생 시 “갑”의 감독하에 이루어져야 하며 장애처리 결과 보고서를 제출하여야 한다.

다. “을”은 무상 유지보수 기간에 소프트웨어가 최신버전으로 업그레이드가 필요할 때에는 무상으로 지원하고, “갑”이 요구할 경우 기능 개선 및 보완작업을 실시하여야 하며 상세한 내역은 상호 협의에 따른다.

라. 무상 유지보수기간 이후라도 “갑”이 시스템 확장, 타 기종과의 연결, S/W 업그레이드 등을 시행할 경우, 기술을 요하는 사항에 대하여 적극 지원하여야 한다.

6. 제출서류

가. 계약시 제출 서류

○ 납품시스템(S/W)의 제조사 또는 저작권자의 「제품공급 및 기술지원 확약서」 원본 1부

나. 납품·설치시 제출 서류

○ 납품 소프트웨어의 상세명세서(Information List) 1부.

○ 납품 소프트웨어의 물품별 단가 산출 내역서(낙찰가 기준) 1부.

○ 비밀유지계약서 1부.

○ 대표자·참여인원의 보안서약서 각 1부.

다. 검수 시 제출 서류

○ 대표자·참여인원의 보안확약서 1부.

○ 소프트웨어 라이선스 1부.

7. 보안유지

가. “을”은 본 시스템 설치와 관련하여 “갑”의 정보보안 정책 및 규정을 준수하여야 한다.

나. “을”은 사업기간 및 유지보수 수행에 사용되는 인원, 문서, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 [붙임 1~15]에 해당하는 보안 관련 준수사항을 지켜야하며 보안상 결격 사항이 없도록 조치해야 한다.

다. “을”은 본 시스템 설치와 관련하여 취득한 “갑”의 시스템 환경, 운영에 관한 정보나 개인, 시설 등에 관한 일체의 내용에 대하여 타인에게 제공, 누설 및 그 목적 외의 용도에 이용하여서는 아니되며, 위의 의무를 위반한 경우 “을”은 모든 민·형사상 책임을 진다.

라. “을”은 “갑”이 요구하는 제반 보안사항을 충실히 이행해야하며, 대표자 및 참여인력의 보안서약서 및 보안확약서 등 관련서류를 제출해야 한다.

마. 시스템실 출입시 출입대장에 기재하는 등 “갑”이 요구하는 보안사항을 충실히 이행하여야 한다.

바. “을”은 설치 기술 인력을 임의로 교체할 수 없으며, 인력 변동 시 “갑”에게 즉시 보고하여야 하며, 사전에 “갑”의 승인을 얻어야한다.

사. 사업수행으로 생산된 산출물, 기록 등은 “갑”이 허락하지 않은 타인에게 제공 또는 대여, 열람을 금지한다.

아. “을”은 무상 유지보수기간 내 납품시스템의 보안상 문제점이 발견되면 즉각 그 대책을 수립하여 해결하여야 한다.

자. “을”은 국가정보원의 보안업무규정에 의거 신원증명 제출 요구가 있을 때에는 즉시 제출하여야 한다.

차. “을”은 보안성 검토 과정에서 “갑”이 요구하는 보안 조치 사항을 이행하여야 하며, 무상 유지보수기간 중 신규로 발견된 취약점에 대해서도 보안 패치를 제공하여야 한다.

8. 기타사항

가. 본 시방서에 명시된 모든 조항은 최소한의 사양, 시방만을 규정하였으므로 상세히 기술되지 않았거나 누락된 사항에 대하여 관리상 문제가 발생하지 않도록 사전 조치하여야 한다.

나. “갑”과 “을”은 본 시방서의 내용을 수정할 필요가 있을 경우 별도의 합의서를 작성할 수 있다. 단, 이 경우 합의서 내용이 본 시방서와 상이하거나 상충될 경우 합의서가 우선 적용된다.

다. 본 구매 규격에 대하여 “갑”과 “을”간의 해석에 차이가 있을 때에는 관계법령과 일반관례에 따르며 소송 관할법원은 “갑”의 주소지를 관할하는 법원으로 한다.

라. “을”은 현장에서 발생할 수 있는 모든 안전사고 및 피해를 사전에 예방하여야 하며, 필요시 안전수칙준수교육 및 위험방지책을 강구하여야 한다.

마. “을”이 납품하는 “시스템”에서 비롯되는 면허, 특허권, 의장권, 공업소유권, 지적소유권의 침해로 인한 모든 문제와 소송으로부터 “갑”은 전적으로 면책하고, 이를 “을”의 부담으로 한다.

Ⅲ. 구 축 규 격

1. 종류와 수량

품명	세부내역	수량	비고
소프트웨어	○ API 연계(Gateway + APIM) S/W	2식	이중화

2. 품목 및 주요기능

구분	세부내역	수량	비고
API 연계 S/W	○ **서버 이중화 구성** - 시스템의 고가용성(HA) 확보를 위해 서버 이중화 구성을 원칙으로 하며, 특정 서버 장애시에도 서비스 중단이 없는 무중단 운영 환경을 구축 - 로드밸런싱(Load Balancing)기능을 통해 트래픽을 효율적으로 분산 제어하여 서비스 부하를 방지하고 최적의 응답속도를 유지 - Active-Active 다중 노드 구성으로, 노드 장애 시 처리 중인 요청을 정상 노드로 자동 재배분 - 다중 노드 간 정책・라우팅 설정을 자동 동기화 - 물리 서버, 가상화(VM), 컨테이너 환경에 설치 가능하며 인터넷이 차단된 망분리 환경에서 설치・패치 가능 ○ **출입 사용자 제한 및 인증(보안) 기능** - AuthKey / IP 제한 / API 유효성 점검 / API 필드 전문 암복호화 - OAuth 2.0, JWT, mTLS, API Key, HMAC, Basic 등 다중 인증 방식을 지원하고 API별・사용자 별로 분리 적용 - Public/Private API 접근 제어, IP 허용・차단 목록, CORS 제어 및 JSON/XML 요청 검증(스키마, 크기) - 송수신 전문 및 지정 필드 단위의 암복호화・마스킹과 로그 암호화 저장을 지원 ○ **Transaction 관리** - 유량제어(요청횟수 제어), 동시호출건수 제어, 실패내역 재전송 - IP・사용자・API 단위 유량 제어(초・분당 호출 수, 일・월 쿼터)와 한도 초과 시 처리 방식(거부・대기) 설정 - 타임아웃・재시도 정책(최대 횟수, 간격, 대상 오류 유형) 설정, 장애 서비스 자동 차단 및 중복 요청 방지 ○ **통합 API 생성** - APIM 관리자 웹 페이지를 통해 개별 소스 코딩 없이 API	2식	서버 이중화 구성

구분	세부내역	수량	비고
	생성 - Script를 통한 비즈니스 로직 구현, 제약 없는 확장 (JavaScript 등 표준 언어 기반 Low-Code 변환 지원) - DB 연동 및 CRUD 처리 기능 - DB Connection 확인 및 SQL 실행 결과값 화면에 표시 - 파라미터 일괄 입력(엑셀 업로드, 복사 등) 기능 - 운영서버 반영 전 테스트 기능(개발DB 등) - DB 테이블·SQL·저장 프로시저, 파일(CSV, XML, JSON, 고정길이 전문), 기 구축된 REST/SOAP 인터페이스를 표준 REST API로 생성·재발행 - 요청 파라미터·응답 스키마 매핑, 데이터 타입 변환, 필수값 검증 규칙을 화면에서 정의 - OpenAPI 3.0 규격 명세 자동 발행, 화면 내 시험 실행 및 백엔드 없이 사용 가능한 모의 응답 기능 - JSON, XML, 고정길이 전문 간 메시지 포맷 변환과 동기/비동기 호출 패턴 변환 **○ API 스케줄** - 특정 시간/ 주기별 API를 자동 호출하는 스케줄링 기능 **○ 이기종 시스템 연계** - JDBC 기반 DB, HTTP/HTTPS 기반 REST·SOAP, 파일(FTP, SFTP), 메시지 큐(JMS, Kafka 등), TCP/IP 소켓 방식의 연계 지원 - SDK/Library 기반 사용자 정의 커넥터 개발·등록 지원 **○ 서비스 오케스트레이션** - 복수의 API·DB·메시지 큐 호출을 순차·병렬로 구성하는 업무 흐름을 소스코드 작성 없이 GUI(Drag & Drop)로 정의 - 여러 시스템의 데이터를 조합하여 하나의 API로 제공, 조건 분기·반복·예외 처리 및 스케줄 실행 - 업무 흐름 정의의 반출·반입 및 개발·검증·운영 환경 간 이관, 비동기 처리(콜백·실패 건 재처리) 지원 **○ 데이터 연계** - 데이터 수집·변환·적재 작업을 주기·이벤트 기반으로 실행하고 실패 건 격리 및 재처리, 원천·대상 간 건수 대사 - 대용량 조회 결과의 스트리밍·분할 전송을 지원하며 DB Link 연계를 표준 API 기반 연계로 전환 가능 **○ API 관리** - 개발된 API 버전, 정책 관리(보안정책, 로그정책 등) 기능 - API 호출 현황 확인 및 API 구간별 세부 로그 확인 기능 - 라우트·서비스·사용자 단위 정책 구성, 인증·유량		

구분	세부내역	수량	비고
	제어・변환・로깅 정책의 플러그인 방식 조합 적용 - API・API 그룹 단위 등록・수정・삭제・검색, 무중단 실시간 배포 및 배포 이력 관리・롤백 - 관리자・운영자 역할 기반 권한 분리(설정 변경/데이터 조회/감사 로그 조회) **○ 라우팅 및 부하 분산** - 호스트・URL 경로・HTTP 메서드・헤더 조건 기반 라우팅, API 버전별 동시 운영 및 가중치 기반 단계적 전환(Canary) - Round Robin, Least Connections 등 부하분산 알고리즘 선택 적용과 Health Check 기반 장애 노드 자동 제외・복구 시 자동 편입 - 요청・응답(Header, Parameter, Path, Body)의 추가・삭제・치환 변환 정책 적용 **○ 호출 추적 및 운영 모니터링** - 모든 호출에 고유 요청 ID를 부여하고 게이트웨이부터 백엔드 시스템까지 구간별 소요 시간 추적 - 요청・응답 메타데이터, 사용자, 지연시간, 상태 코드의 감사 로그 기록(로그 생성 후 수정・삭제 불가) - API별・사용자별・오류 유형별 통계 및 실시간 처리 현황 대시보드, 연계 송수신 현황・장애 조회 및 조치 결과 관리 - 오류율 임계값 초과, 연계량 급증・급감 시 관리자 알림 및 외부 알림 시스템 연동 **○ 확장성** - 동일 플랫폼 안에서 AX 전환을 위한 AI 연계 모듈들(AI Gateway,MCP Gateway,MCP서버 등)을 설치, 구성 등 확장 지원		

[붙임 1]

정보화사업 용역직원 보안 준수사항

1. 사업 수행전

가. 참여인원에 대한 보안관리

○ 용역사업 참여인원에 대해서는 각 개인의 친필 서명이 들어간 보안서약서를 작성

○ 용역사업 수행 前 참여인원에 대해 법적 또는 발주기관 규정에 의한 비밀유지 의무를 준수해야 함.

2. 사업 수행시

나. 자료에 대한 보안관리

○ 전산망도·IP현황, 개인정보 등 용역업체에 제공하는 비공개자료는 '자료관리대장'을 작성하여 인계자(해당기관 보안담당관)와 인수자(용역업체 관리책임자)가 직접 서명한 후 인계·인수

○ 용역사업 관련자료 및 사업과정에서 생산된 모든 산출물은 발주 기관의 파일서버에 저장하거나 보안담당관이 지정한 PC에 저장·관리

○ 용역사업관련 자료는 인터넷 웹하드 등 인터넷 자료공유사이트 및 개인메일함에 저장을 금지하고 전자우편을 이용해 자료전송이 필요한 경우에는 자체 전자우편을 이용, 첨부자료 암호화 후 수발신

* 단, 대외비 이상의 비밀은 전자우편으로 수발신 금지

○ 발주기관이 제공한 사무실에서 사업을 수행할 경우 제공한 비공개자료는 매일 퇴근시 반납토록 하며 비밀문서를 제외한 일반문서는 용역업체에 제공된 사무실에 시건장치가 된 보관함이 있을 경우 이에 보관 가능

○ 용역사업 수행으로 생산되는 산출물 및 기록은 보안담당관이 인가하지 않은 비인가자에게 제공·대여·열람을 금지

다. 사무실·장비에 대한 보안관리

○ 용역사업수행 장소는 발주기관이 시건장치와 통제가 가능한 공간을 제공하거나 협의를 통해 同 환경이 구축된 외부 사무실을 사용

○ 용역업체 사무실 또는 용역업무를 수행하는 공간에 대한 보안점검을 정

기적으로 실시하고 필요시 국정원에 지원을 요청

○ 발주기관 사무실에서 용역사업을 수행할 경우 용역 참여직원이 노트북 등 관련 장비를 반출 또는 반입할 때마다 악성코드 감염여부 및 자료 무단반출 여부를 확인

○ 인가받지 않은 USB 등의 보조기억매체 사용을 금지하며 산출물 저장을 위해 보조기억매체가 필요한 경우 보안담당관의 관리하에 사용

라. 내외부망 접근 시 보안관리

○ 용역사업 수행 시 발주기관 전산망 이용이 필요한 경우

- 사업 참여인원에 대한 사용자 계정(ID)은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 부여
- 계정별로 부여된 접속권한은 불필요시 곧바로 권한을 해지하거나 계정을 폐기
- 참여인원에게 부여한 패스워드는 보안담당관이 별도로 기록 관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력 확인
- 보안담당관은 서버 및 장비 운영자로 하여금 내부서버 및 네트워크 장비에 대한 접근기록을 매일 확인하여 이상유무 보고
- 용역업체에서 사용하는 노트북PC는 인터넷 연결을 금지, 다만 사업 수행상 필요한 경우에는 용역업체의 관리책임자가 직접 요청하고 보안담당관은 필요성이 인정될 경우 접속할 노트북을 지정하고 필요한 사이트에만 접속토록 방화벽 등을 통해 통제 후 사용

○ 발주기관 및 용역업체 전산망에서 P2P, 웹하드 등 인터넷 자료공유 사이트로의 접속을 방화벽 등을 이용해 원천 차단

3. 사업 완료시

○ 사업완료 후 생산되는 최종 산출물 중 대외보안이 요구되는 자료는 대외비로 작성·관리하고 불필요한 자료는 삭제 및 세단 후 폐기

○ 용역업체에 제공한 제반자료, 장비, 서류와 중간·최종 산출물 등 용역과 관련된 제반자료는 전량 회수하고 업체에 복사본 등 별도 보관을 금지

○ 노트북·보조기억매체 등 전자적으로 기록된 자료는 국정원의‘정보시스템 저장매체 불용처리 지침’에 따라 보안조치

○ 용역사업 관련자료 회수 및 삭제조치 후 업체에게 복사본 등 용역사업 관련 자료를 보유하고 있지 않다는 대표 명의 확약서 작성 필요

[붙임 2]

외주 용역사업 보안특약 조항

① 사업자는 성신여자대학교의 보안정책을 위반하였을 경우 <붙임3>의 위규 처리기준에 따라 위규자 및 관리자를 행정조치하고 <붙임4>의 보안 위약금을 성신여자대학교에 납부한다.

② 사업자는 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 <붙임5>의 '누출금지 대상정보'에 대한 보안관리 계획을 사업제안서에 기재하여야 하며, 해당 정보 누출 시 성신여자대학교는 '국가를 당사자로 하는 계약에 관한 법률 시행령' 제76조에 따라 사업자를 부정당업체로 등록한다.

③ 사업 수행과정에서 취득한 자료와 정보에 관하여 사업수행 중은 물론 사업 완료 후에도 이를 외부에 유출해서는 안되며, 사업종료 시 정보보안담당자의 입회하에 완전 폐기 또는 반납해야 한다.

④ 사업자는 사업 최종 산출물에 대해 정보보안전문가 또는 전문보안 점검도구를 활용하여 보안 취약점을 점검, 도출된 취약점에 대한 개선을 완료하고 그 결과를 제출해야 한다.

[붙임 3]

사업자 보안위규 처리기준

구 분	위 규 사 항	처 리 기 준
심 각	1. 비밀 및 대외비 급 정보 유출 및 유출시도 가. 정보시스템에 대한 구조, 데이터베이스 등의 정보 유출 나. 개인정보·신상정보 목록 유출 다. 비공개 항공사진·공간정보 등 비공개 정보 유출 2. 정보시스템에 대한 불법적 행위 가. 관련 시스템에 대한 해킹 및 해킹시도 나. 시스템 구축 결과물에 대한 외부 유출 다. 시스템 내 인위적인 악성코드 유포	○ 사업참여 제한 ○ 위규자 및 직속 감독자 등 중징계 ○ 재발 방지를 위한 조치계획 제출 ○ 위규자 대상 특별 보안교육 실시
중 대	1. 비공개 정보 관리 소홀 가. 비공개 정보를 책상 위 등에 방치 나. 비공개 정보를 휴지통·폐지함 등에 유기 또는 이면지 활용 다. 개인정보·신상정보 목록을 책상 위 등에 방치 라. 기타 비공개 정보에 대한 관리소홀 2. 사무실·보호구역 보안관리 허술 가. 통제구역 출입문을 개방한 채 퇴근 등 나. 인가되지 않은 작업자의 내부 시스템 접근 다. 통제구역 내 장비·시설 등 무단 사진촬영 3. 전산정보 보호대책 부실 가. 업무망 인터넷망 혼용사용, 보안 USB 사용규정 위반 나. 웹하드·P2P 등 인터넷 자료공유사이트를 활용하여 용역사업 관련 자료 수발신 다. 하자보수 시 원격작업 사용 라. 저장된 비공개 정보 패스워드 미부여 마. 인터넷망 연결 PC 하드디스크에 비공개 정보를 저장 바. 외부용 PC를 업무망에 무단 연결 사용 사. 보안관련 프로그램 강제 삭제 아. 사용자 계정관리 미흡 및 오남용(시스템 불법접근 시도 등)	○ 위규자 및 직속 감독자 등 중징계 ○ 재발 방지를 위한 조치계획 제출 ○ 위규자 대상 특별 보안교육 실시

구 분	위 규 사 항	처 리 기 준
보 통	1. 기관 제공 중요정책·민감 자료 관리 소홀 가. 주요 현안·보고자료를 책상 위 등에 방치 나. 정책·현안자료를 휴지통·폐지함 등에 유기 또는 이면지 활용 2. 사무실 보안관리 부실 가. 캐비넷·서류함·책상 등을 개방한 채 퇴근 나. 출입키를 책상 위 등에 방치 3. 보호구역 관리 소홀 가. 통제·제한구역 출입문을 개방한 채 근무 나. 보호구역내 비인가자 출입허용 등 통제 미실시 4. 전산정보 보호대책 부실 가. 휴대용저장매체를 서랍·책상 위 등에 방치한 채 퇴근 나. 네이트온 등 비인가 메신저 무단 사용 다. PC를 켜 놓거나 보조기억 매체(CD, USB 등)를 꽂아 놓고 퇴근 라. 부팅·화면보호 패스워드 미부여 또는 "1111" 등 단순숫자 부여 마. PC 비밀번호를 모니터 옆 등 외부에 노출 바. 비인가 보조기억매체 무단 사용	○ 위규자 및 직속 감독자 등 경징계 ○ 위규자 및 직속 감독자 사유서/경위서 징구 ○ 위규자 대상 특별 보안교육 실시
경 미	1. 업무 관련서류 관리 소홀 가. 진행 중인 업무자료를 책상 등에 방치, 퇴근 나. 복사기·인쇄기 위에 서류 방치 2. 근무자 근무상태 불량 가. 각종 보안장비 운용 미숙 나. 경보·보안장치 작동 불량 3. 전산정보 보호대책 부실 가. PC내 보안성이 검증되지 않은 프로그램 사용 나. 보안관련 소프트웨어의 주기적 점검 위반	○ 위규자 서면·구두 경고 등 문책 ○ 위규자 사유서 / 경위서 징구

[붙임 4]

보안 위약금 부과기준

1. 위규 수준별로 A~D 등급으로 차등 부과

구분	위규 수준			
	A급	B급	C급	D급
위규	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금 비 중	부정당업자 등록	계약금액의 10%	계약금액의 5%	계약금액의 3%

* 위규 수준은 <붙임3> 참고

2. 보안 위약금은 다른 요인에 의해 상쇄, 삭감이 되지 않도록 부과

* 보안사고는 1회의 사고만으로도 그 파급력이 큰 것을 감안하여 타 항목과 별도 부과

3. 사업 종료 시 지출금액 조정을 통해 위약금 정산

[붙임 5]

누출금지 대상 정보

1. 기관 소유 정보시스템의 내·외부 IP주소 현황

2. 세부 정보시스템 구성현황 및 정보통신망 구성도

3. 사용자계정 · 비밀번호 등 정보시스템 접근권한 정보

4. 정보통신망 취약점 분석·평가 결과물

5. 용역사업 결과물 및 프로그램 소스코드

6. 국가용 보안시스템 및 정보보호시스템 도입 현황

7. 침입차단시스템 · 방지시스템(IPS) 등 정보보호제품 및 라우터 · 스위치 등 네트워크 장비 설정 정보

8. 「공공기관의 정보공개에 관한 법률」제9조제1항에 따라 비공개 대상 정보로 분류된 기관의 내부문서

9. 「개인정보보호법」 제2조제1호의 개인정보

10. 「정보시스템 보안운영 규정」제22조의 정보보안 기본 수칙

11. 그 밖에 각급기관의 장이 공개가 불가하다고 판단한 자료

[붙임 6]

개인정보처리 위탁준수사항

정보통신망 운영 및 하자보수 업무를 수행하면서 개인정보 및 개인정보 처리 시스템 접근 시 다음의 사항을 준수하여야 한다.

1. **(용어의 정의)** 본 준수사항에서 별도로 정의되지 아니한 용어는 개인정보 보호법, 같은 법 시행령 및 시행규칙, 「표준 개인정보 보호지침」에서 정의된 바에 따른다.

2. **(위탁업무의 목적 및 범위)** 정보통신망 운영 및 하자보수 수행기관은 계약이 정하는 바에 따라 **(성신여자대학교 API 연계 솔루션 도입)** 목적에만 개인정보 처리 업무를 수행한다.

3. **(재위탁 제한)** ① 수행기관은 성신여자대학교의 사전 승낙을 얻은 경우를 제외하고 성신여자대학교와의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.
② 수행기관이 재위탁받은 수탁회사를 선임하였으면 수행기관은 당해 재위탁계약서와 함께 그 사실을 즉시 성신여자대학교에 통보하여야 한다.

4. **(개인정보의 안전성 확보 조치)** 수행기관은 개인정보 보호법 제29조, 같은 법 시행령 제30조 및 개인정보의 안전성 확보 조치 기준 고시에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조처하여야 한다.

5. **(개인정보의 처리 제한)** ① 수행기관은 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.
② 수행 기관은 계약이 해지되거나 계약기간이 만료되면 위탁업무와 관련하여 보유하고 있는 개인정보를「개인정보 보호법」 시행령 제16조에 따라 즉시 파기하거나 성신여자대학교에 반납하여야 한다.
③ 제2항에 따라 수행기관이 개인정보를 파기하였을 때 바로 성신여자대학

교에 그 결과를 통보하여야 한다.

6. **(수탁자에 대한 관리·감독 등)** ① 성신여자대학교는 수행기관에 대하여 다음 각호의 사항을 관리하도록 요구할 수 있으며, 수행기관은 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속현황
3. 개인정보 접근 또는 접속 대상자
4. 목적 외 이용·제공 및 재위탁 금지 준수 여부
5. 암호화 등 안전성 확보 조치 이행 여부
6. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② 성신여자대학교는 수행기관에 대하여 제1항 각호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, 수행기관은 특별한 사유가 없는 한 이행하여야 한다.

③ 성신여자대학교는 처리위탁으로 인하여 정보 주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수행기관을 교육할 수 있으며, 수행기관은 이에 응하여야 한다.[1)]

④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 성신여자대학교와 수행기관과 협의하여 시행한다.

7. **(손해배상)** ① 성신여자대학교 또는 수행기관의 임직원 기타 수행기관의 수탁자가 이 계약으로 위탁 또는 재위탁받은 업무를 수행하면서 이 계약에 따른 의무를 위반하거나 수행기관 또는 수행기관의 임직원 기타 수행기관의 수탁자의 귀책 사유로 인하여 이 계약이 해지되어 성신여자대학교 또는 개인정보 주체 기타 제3자에게 손해가 발생하면 수행기관은 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보 주체 기타 제3자에게 발생한 손해에 대하여 성신여자대학교가 전부 또는 일부를 배상한 때에는 성신여자대학교는 이를 수행기관에서 구상할 수 있다.

[붙임7]

---

1) 「개인정보 안전성 확보 조치 기준 고시」에 따라 개인정보처리자 및 취급자는 1년에 1회 이상 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.

[붙임 7]

보안 서약서

(사업수행자)

본인은 ___년 __월 __일부로 **성신여자대학교 API 연계 솔루션 구축** 업무를 수행함에 있어 다음의 사항을 준수할 것을 서약합니다.

1. 본인은 소관업무의 내용이 직무상 기밀임을 인정하고 제반 보안관계규정 및 지침을 성실히 준수한다.

2. 본인은 이 기밀을 누설함이 국가안전보장 및 국가이익에 위해가 될 수 있음을 인식하고 재직 중은 물론 퇴직 후에도 알게 된 모든 기밀사항을 일체 타인에게 누설하지 아니한다.

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

년 월 일

서 약 자	업 체 명:		
(사업수행자)	직 급:		
	성 명:		(서명)
서약집행자	소 속:		
(사업담당자)	직 급:		
	성 명:		(서명)

[붙임 8]

보안 서약서

(사업수행사)

본인은 ___년 __월 __일부로 **성신여자대학교 API 연계 솔루션 구축** 사업을 수행함에 있어 다음의 사항을 준수할 것을 서약합니다.

1. 본인은 사업을 수행함에 있어 업무상 취득한 정보의 중요성을 깊이 인식하고, 이와 관련된 일체의 내용이 직무상 기밀임을 인정한다.

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

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

4. 본인은 사업수행시 발생하는 위반사항에 대해서도 모든 책임을 질 것을 서약한다.

년 월 일

서 약 자	업 체 명:	
(사업수행사대표)	사업자 번호:	
	성 명:	(서명)
서약집행자	소 속:	
(사업담당자)	직 급:	
	성 명:	(서명)

[붙임 9]

보안확약서

(사업수행자)

본인은 ____년 __월 __일부로 **성신여자대학교 API 연계 솔루션 구축** 사업을 수행을 완료함에 있어, 다음 각 호의 보안사항에 대한 준수 책임이 있음을 서약하며 이에 확약서를 제출합니다.

1. 본인은 사업수행 중 지득한 모든 자료를 반납 및 파기하였으며, 지득한 정보에 대한 유출을 절대 금지 하겠습니다.
2. 본인은 기술 지원 업체에 대해서도 상기 항과 동일한 보안사항 준수 책임을 확인하고 보안확약서를 징구하였으며, 기술 지원 업체가 위의 보안사항을 위반할 경우에 주사업자로서 이에 동일한 법적책임을 지겠습니다.
3. 본인은 상기 보안사항을 위반할 경우에 귀 기관의 사업에 참여 제한 또는 기타 관련 법규에 따른 책임과 손해배상을 감수하겠습니다.

년 월 일

서약자 업 체 명:

직 위:

성 명: (서명)

[붙임 10]

보안확약서

(사업수행사)

본 업체(단체)는 ____년 __월 __일부로 **성신여자대학교 API 연계 솔루션 구축** 사업을 수행을 완료함에 있어, 다음 각 호의 보안사항에 대한 준수 책임이 있음을 서약하며 이에 확약서를 제출합니다.

1. 본 업체(단체)는 업체(단체) 및 사업 참여자가 사업수행 중 지득한 모든 자료를 반납 및 파기하였으며, 지득한 정보에 대한 유출을 절대 금지 하겠습니다.
2. 본 업체(단체)는 기술 지원 업체에 대해서도 상기 항과 동일한 보안사항 준수 책임을 확인하고 보안확약서를 징구하였으며, 기술 지원 업체가 위의 보안사항을 위반할 경우에 주사업자로서 이에 동일한 법적책임을 지겠습니다.
3. 본 업체(단체)는 상기 보안사항을 위반할 경우에 귀 기관의 사업에 참여 제한 또는 기타 관련 법규에 따른 책임과 손해배상을 감수하겠습니다.

년 월 일

서약업체(단체) 대표 업 체 명:

사업자 번호:

성 명: (서명)

[붙임 11]

비밀유지계약서

성신여자대학교(이하 "갑"이라 한다)의 [성신여자대학교 API 연계 솔루션 구축] 업무 수행을 위하여 [○○업체명○○](이하 "을"이라 한다)은(는) 다음과 같이 비밀유지계약을 체결한다.

제1조(목적)

이 계약서는 갑이 사업수행을 위하여 비밀정보를 제공함에 있어 갑의 관련 비밀정보를 보호하기 위함을 목적으로 한다.

제2조(비밀의 내용)

이 계약상 비밀정보란 업무진행 과정에서 갑이 을에게 제공하거나 갑 혹은 그 직원으로부터 지득 혹은 취득하는 갑의 일체의 영업 혹은 기술상의 정보 및 이와 같은 영업 혹은 기술상의 정보에 근거하여 을이 개발하거나 도출하는 일체의 영업 혹은 기술상의 정보(이하 "비밀정보"라 한다)를 말한다. 이와 같은 비밀정보는 서면, 구두 혹은 기타방법으로 제공되는 모든 학적, 교직원 정보, 대학활동, 노하우, 공정, 도면, 설계, 실험결과, 샘플, 데이터, 공시, 방법, 프로그램, 가격표, 거래명세서, 생산코스트, 선전상의 아이디어, 사업정보 등을 모두 포함한다.

제3조(비밀의 정의)

비밀은 공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 합리적인 노력에 의하여 비밀로 유지된 학적, 교직원 정보, 정보시스템 운영 현황, 생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 갑의 경영상의 정보를 말한다.

제4조(정보의 사용용도 제한)

을은 갑으로부터 제공받은 모든 정보나 자료를 관련 계약서에 명시된 본래의 목적에만 사용되어야 하며, 계약의 수행을 위해 갑에 관련된 비밀정보를 제3자에게 제공할 경우, 당해 제3자와 별도의 비밀유지계약을 체결하여야 하며, 반드시 계약서에 제시한바대로 본래의 목적에 관련되어서만 한정적으로 사용되어야 한다.

제5조(정보취급자)

을은 갑으로부터 제공받은 비밀정보를 자사 조직 내 목적상 부합하는 직원들에 한하여 이용하도록 조치하여야 하며 직원 각자에게 비밀유지의무를 주지시켜야 한다. 또한 갑이 요구하는 경우 자사의 관계직원들에 대하여 당해 직원이 확약상의 비밀유지의무를 이행하겠다는 내용의 각서를 징구하는 등 상대방이 만족할 수 있는 적절한 조치를 취하여야 한다.

제6조(자료의 반환)

을은 상대방의 요청이 있으면 언제든지 갑의 비밀정보가 기재되어 있거나 이를 포함하고 있는 제반 자료, 장비, 서류, 샘플, 기타 유체물을 즉시 반환하거나, 갑의 선택에 따라 이를 폐기하고 그 폐기를 증명하는 서류를 갑에게 제공하여야 한다.

제7조(권리의무의 양도)

이 계약의 권리와 의무는 갑의 사전 서면동의 없이는 제3자에게 양도될 수 없다.

제8조(권리의 부존재 등)

① 이 계약상 제공되는 비밀정보에 관한 모든 권리는 갑에 속하고 본 계약은 어떠한 경우에도, 본 계약상 제공된 비밀정보에 관하여 을에게 어떠한 권리나 사용권을 부여하는 것으로 해석되지 않는다.

② 이 계약은 어떠한 경우에도 갑의 향후 어떠한 확정적인 계약의 체결, 제조물의 판매나 구입, 실시권의 허여 등을 암시하거나 이를 강제하지 않으며, 기타 갑이 본 계약상 기술과 관련하여 다른 제3자와 어떠한 거래나 계약관계에 들어가는 것을 금지하거나 제한하지 아니한다.

제9조(내부규정의 준수)

을은 이 계약상의 목적을 위하여 갑의 시설을 방문하거나 이를 이용할 경우, 갑의 제반규정을 준수하여야 한다.

제10조(계약의 분리가능성)

이 계약 중 어느 규정이 법원에 의하여 불법, 무효 또는 집행 불가능하다고 선언될 경우, 이는 계약서의 나머지 규정의 유효성에 영향을 미치지 아니한다.

제11조(손해배상 등)

을이 이 계약을 위반하여 갑 또는 제3자에게 손해를 발생시킨 경우에는 귀책있는 을이 이에 관한 모든 책임을 지고 배상하도록 한다.

제12조(계약기간)

이 계약은 관련 계약 체결일로부터 1년간 그 효력을 가진다.

제13조(분쟁의 해결)

이 계약과 관련하여 분쟁이 발생한 경우 상호 협의에 의한 해결을 모색하되, 분쟁에 관한 합의가 이루어지지 아니한 경우에는 서울북부지방법원을 합의관할로 하여 소송을 통해 분쟁을 해결하기로 한다.

제14조(특약사항)

상기의 계약 일반사항 이외에 을은 아래의 내용을 특약사항으로 정하며, 특약사항이 본문과 상충되는 경우에는 특약사항이 우선 적용된다.

1. 을은 이 계약과 관련하여 정보보안 및 개인정보보호 등 갑의 중요자산 보호 활동을 위하여 교육부 정보보안기본지침 및 개인정보보호법 등 관련 규정 및 법령 준용하여 업무를 처리한다.

년 월 일

회사명 :

주 소 :

직 위 :

성 명 : (인)

[붙임 12]

정보시스템 관리대장

연번	소속	취급자 (성명)	IP	시스템명	종류 (서버·PC등)	제조사	모델명	관리 번호	도입 일자	설치 위치

[붙임 13]

열람·제공자료 관리대장

○ 기관명/부서명 :

○ 사업명(용역명) :

○ 용역업체명 :

연번	자 료 명	인계 및 인수				자료반납	
		인계자	인수자	월일	장소	확인자	월일

[붙임 14]

휴대용 저장매체(전산장비 포함) 반출·입 대장

장비명	장비 식별번호	신청자 성명 (직급)	용도	반출.입 일시 (입/출)	반출.입시 보안조치 점검유무	관리책임자 승인	비고
					백신점검, 자료 완전삭제 확인 등		*IDC에서 영구 반출 또는 폐기 의뢰 문서번호*

[붙임 15]

자료인계인수대장

○ 기관명/부서명 :

○ 용 역 명 :

자료명칭	자료형태	인계인수일시	인계자 성명 (서명)	인수자 성명 (서명)