붙임 **연구원 정보화 사업 자체 보안성 검토 결과**

□ 대상 사업

부 서 명	사 업 명	비 고
교통물류본부 철도운영연구실	○ TRIPS International Edition 실증 기술지원 및 요구사항 반영을 통한 시제품 개발	철도운영연구실-29 (2026.02.26.)
사업특성	○ SW 개발(인터페이스 및 기능 수정)	

□ 검토 개요

○ 본 보안성 검토는 「**TRIPS International Edition 실증 기술지원 및 요구사항 반영을 통한 시제품 개발 사업**」 사업에 한함

○ 사업특성 등을 고려하여 전반적으로 준수해야 하거나 권고되는 내용들을 포괄적으로 검토함

○ 위 정보화사업은 제안요청서 구성요건 및 **자체 수립한 보안대책을 준수**하여 추진하고, **기타 알려지지 않은 공격 및 보안취약점에 대하여 지속적으로 관리**하여야 함

□ 검토 결과

【 공통 사항 】

○ SW 운용 시 디폴트 계정·패스워드는 삭제 또는 변경하고, 관리자 페이지 접근통제 및 불필요 서비스 제거

○ 개발에 사용하는 장비는 취약점이 제거된 최신 버전으로 운영하고 주기적으로 보안패치 적용 및 보안취약점 점검 수행

○ 자체 수립한 보안대책을 준용하고, 이외 세부사항은 「국가 정보보안 기본지침」·「과학기술정보통신부 정보보안 기본지침」·「국가사이버안전관리규정」 등 관련 규정 준수

【 SW 개발 보안 】

○ 정보시스템을 개발 또는 변경할 경우 관련 법 및 지침 준수

- 전자정부법, 행정기관 및 공공기관 정보시스템 구축·운영지침, 소프트웨어 개발보안 가이드 등

- 「국가정보 보안 기본지침 제27조(소프트웨어 개발 보안) ~ 제30조(누출금지정보 유출시 조치)」를 준용

○ 소스코드 작성 시 **소프트웨어 개발보안*** **(시큐어코딩)을 적용하고** 신규 및 변경 구축된 홈페이지/응용프로그램은 **실제 운영 이전에 취약점 점검 및 조치를 반드시 수행**(운영 이후 연 1회 이상)

* 소프트웨어 개발보안 : 전자정부법 제45조, 행정기관 및 공공기관 정보시스템 구축·운영 지침 제52조의 '소프트웨어 보안약점 기준' 69개 항목

※ **(정보시스템 취약점)** 정보통신기반보호법 제9조, 주요정보통신기반시설 취약점 분석·평가 항목

※ **(홈페이지 취약점)** 국가정보보안기본지침 제53조, 전자정부서비스 웹 취약점 표준 점검 항목(홈페이지 SW(웹) 개발보안 가이드)

※ **(모바일 앱 취약점)** 행정안전부 "모바일 전자정부 서비스 관리 지침" 보안취약점 점검기준(별표 1~3)에 따른 취약점 점검 및 조치

- 소프트웨어 설계 단계부터 보안을 고려하여 설계

- CC인증서 또는 성능평가 결과확인서를 획득한 소스코드 보안약점진단도구를 사용하여 소스코드 내 잔존 취약점 제거

- 개발한 소프트웨어의 코드 및 리소스 파일 등에 대한 무결성 검증 절차 수립·준수 및 정보시스템 탑재·운용 이전에 무결성 검증 수행

○ 소프트웨어 버전 관리를 위한 형상관리시스템(SVN)은 **인가된 사용자만이 소스 프로그램에 접근**할 수 있도록 접근통제

○ 시스템 관리자, 개인정보 취급 및 관리자 등이 중요(개인정보 포함) 정보시스템에 접속 시, ID/PW 방식 이외에도 OTP·PKI·생체인식 등 **다중 인증방식 도입 권고**

○ 비밀번호는 숫자·문자·특수문자 등을 조합하여 **8자리 이상 적용**하고, 비밀번호 **유효기간을 설정**하여 주기적으로 변경

○ 사용자가 정보시스템 등에 연속해서 특정 회수(5회) 이상 **로그온 실패할 경우 접속이 중단**되도록 시스템 설정

○ 주기적인 관리자 패스워드 변경

- 초기 패스워드를 안전한 암호로 변경 운용

○ 비대면 정보화 용역사업의 경우 관리적·기술적 보안대책을 수립·시행

-「국가·공공기관 용역업체 보안관리 가이드라인 제3장」을 준용

【 데이터베이스 보안대책 】

○ **중요정보(개인정보 포함)**는 유출되더라도 복호화가 불가하도록 **DB 암호화** 조치

- 수집한 개인정보 및 고유식별 정보에 대해 「**가명정보 처리 가이드라인**('24.2.5., 개인정보보호위원회 발간)」을 반드시 준수

- 중요정보는 **1차 백업 및 2차 백업을 수행**하고, 백업시스템은 인터넷 및 외부망과 **연계를 차단**하여 자료 유출 대비

- 개인정보 등의 중요정보 백업 시, 암호화 전송 및 저장

○ DB 관리자와 DB 사용자를 **구분하여 관리**하고 DB의 중요도와 응용프로그램 및 사용자 유형 등에 따른 **접근통제** 정책 수립·이행

○ 로그인시 DB 관리자·유지보수자 및 사용자의 안전한 인증 수행

○ 사용자가 DB에 직접 접근할 수 없도록 우회접근 차단

○ 해킹 및 각종 장애 등으로부터 DB 가용성을 저해하지 못하도록 보안대책 수립·시행

○ 사용자별 DB의 모든 접근 기록 및 SQL 수행내역 기록 등을 1년 이상 저장 유지

【 원격지 개발 보안대책 】

○ 용역업체가 발주기관 이외 장소에서 개발 작업을 수행하고자 요청할 경우 '국가 정보보안 기본지침 제13조제1항제1호'에 따른 용역업체 작업장소에 대한 보안 요구사항 등 관리적·기술적 보안대책을 수립·시행

○ 발주기관과 용역업체가 협의하여 원격지 개발 장소 사전 선정

- 사전 협의되지 않은 장소에서의 원격지 개발은 금지
- 출입장소, 복도 등에 CCTV·잠금장치 등을 통해 비인가 출입차단 (출입관리기록부 비치)

○ 용역업체가 자체 구축한 장소에서 원격지 개발을 수행할 경우 다음 사항을 준수

- 개발망은 용역업체의 내부망·인터넷망 등과 분리하여 독립망으로 운영
- 사전등록한 휴대형 저장 장치만 연결·사용

○ 개발PC는 다음의 사항을 준수하여 안전하게 관리

- 개발업무 외 사용 금지
- 백신 및 보안프로그램 설치·운용
- 운영체제 등 최신 보안상태 유지
- 불필요한 프로그램 설치 금지 및 불필요한 포트 비활성화
- 비인가자의 사용이 불가하도록 접근통제
- 부팅·윈도우·화면보호기 패스워드 설정
- 자료유출 방지를 위한 문서보안 솔루션 등 적용
- 개발자별로 개발PC를 할당하고 공유 사용을 금지

○ 개발·테스트 서버 등 정보시스템은 다음의 사항을 준수하여 안전하게 관리

- 관리자 계정과 일반 사용자 계정을 분리
- 계정별로 권한을 구별하여 부여하고 접근통제 수행
- 안전한 비밀번호 사용
- 모든 정보시스템 접근 시에는 사용자 인증을 선행
- 정보보호제품을 활용하여 해킹 및 비인가자의 접근을 통제

○ 원격지 개발과 관련한 수행내역 및 정보시스템 접속 이력 등 로그를 저장하고 1년 이상 유지(위·변조 방지)

【 용역업체 보안관리 대책 】

○ 용역업체는 **계약 후, 용역사업 참여인원* 명단**과 **참여인원별 정보누출 금지사항** 및 **개인의 친필 서명이 들어있는 보안서약서[서식1]**를 연구원에 제출

* ‘**용역업체 참여인원**’ 이라 함은 **용역사업에 참여하는 모든 인력**을 말하며, **주계약업체 뿐만 아니라 사업에 참여하는 하청업체(하도급)** 인력도 포함

○ **용역사업 책임자(연구원)**은 다음과 같은 용역업체 보안관리 절차 준수

- **용역사업 수행 前**, 용역사업 참여인원에 대한 법적 또는 연구원 규정에 따른 **비밀유지 의무 준수 및 위반 시 처벌내용** 등에 대한 **보안교육 실시**

- 용역업체가 **사전에 제출한 용역사업 참여인원명단에 포함된 직원인지 확인 후 사전에 승인된 참여인원에 한하여 출입·작업** 허용

- 용역사업 참여인원의 사업기간 중 **임의교체를 금지**하도록 용역업체에 요구 조치

- **참여인원의 교체가 있거나 참여인원 명단 이외의 직원이 포함되는 경우**에는 출입을 차단한 후 용역업체에 **시정 요구 조치**

- 용역사업 참여인원이 교체된 경우, **교체인원에 대한 보안서약서 징구 [서식1]** 및 **보안교육 등 사전 보안절차 수행 완료 후 작업에 투입** 허용

- 용역사업 참여인원에 대한 **누출금지 대상정보의 외부 누출여부 확인을 위한 수시 보안점검** 실시

- 용역사업 **참여인원 명단, 참여인원 보안서약서 및 대표이사 보안확약서 등 보안서류를 3년이상 보관**하고, 정보보안부서에도 공유

- 사업 종료 시, **용역사업 참여인원 보안서약서[서식1]** 및 **보안확약서 [서식2]** 등 용역업체 보안서류를 확인하고, **SW 악성코드 감염 여부 백신검사 등 보안점검 완료 후 검수 절차 수행**

○ 용역업체 **PC는 외부 인터넷 접속을 차단**하고, **연구원 내 보안정책 적용 (Anti-Virus, PMS, NAC, DRM, 보안USB 등)**

- **'내PC지키미'**를 통한 월 1회 이상 보안점검 실시

- 개발/유지보수 PC는 **연구원에서 승인한 PC만 사용**하도록 조치

○ 용역사업 수행인력에게 발급하는 **계정 및 패스워드의 관리 철저**

- 용역사업 **참여인원의 사용자계정(ID)은 하나의 그룹으로 등록**

  ※ 추측 가능한 계정 또는 기본(default) 계정 발급 금지

- **계정별 정보시스템 접근권한을 차등 부여**하되 **내부문서 접근 금지**

- **계정별로 부여된 접근권한은 불필요 시 해지 또는 계정 폐기**

- 용역사업 참여인원에게 부여한 **비밀번호는 용역사업 책임자(연구원)가 별도 기록·관리**하고 **수시로 저장된 자료 및 작업이력을 확인**

- 용역업체 직원의 작업내용 확인을 위해 **작업이력 로깅 기능 구축**

- **서버·장비 운영자**는 **내부서버 및 네트워크 장비에 대한 접근기록을 매일 확인**하여 **용역사업 책임자(연구원)에게 이상 유무를 보고**

  ※ 관리자 계정인 'root' 계정 등 **시스템에 중대한 영향을 끼칠 수 있는 계정에 대한 용역업체 직원의 단독적인 접근을 불허**

○ 연구원 내·외 **용역사업 수행 장소 및 시스템 입주 공간**(전산실, IDC 등)**에 대한 출입통제 대책을 마련**하고, **정기적**(월 1회 이상) **보안점검**을 실시

○ **용역업체 사용 전산망은** 방화벽 등을 활용하여 **연구원 업무전산망과 분리 구성**하고 **업무상 필요한 서버에만 제한적 접근 허용**

○ **용역업체 PC는 불필요한 인터넷 사용을 금지**하고, 휴대용 저장매체 이용이 필요한 경우에는 **연구원의 승인 하에 안전하고 인가된 USB 등을 사용** 조치

○ 연구원 및 용역업체 전산망에서 P2P, 웹하드 등 **인터넷 자료공유사이트로의 접속을 차단**

○ 연구원과 용역업체간 전자우편을 이용한 자료 전송이 필요한 경우, **연구원의 전자우편 이용 및 첨부파일 암호화 후 수·발신**

○ 정보통신망도, IP 현황 등 용역업체에 제공할 자료는 '자료인계인수 대장'에 기록 후 수수하고 **무단 복사 및 외부반출 금지**

< 국가·공공기관 용역업체 보안관리 가이드라인 부록2-1.누출금지 대상정보) >

① 연구원 소유 정보시스템의 내·외부 IP주소 현황
② 세부 정보시스템 구성현황 및 정보통신망구성도
③ 사용자계정 및 패스워드 등 정보시스템 접근권한 정보
④ 정보통신망 취약점 분석·평가 결과물
⑤ 용역사업 결과물 및 프로그램 소스코드
⑥ 국가용 보안시스템 및 정보보호시스템 도입현황
⑦ 침입차단시스템(FW)·침입방지시스템(IPS) 등 정보보호제품 및 라우터·스위치 등 네트워크장비 설정 정보
⑧「공공기관의 정보공개에 관한 법률」제9조제1항에 따라 비공개 대상정보로 분류된 연구원의 내부문서
⑨「개인정보 보호법」제2조제1호의 개인정보
⑩「보안업무규정」제4조의 비밀, 보안업무규정 시행규칙 제16조제3항의 대외비
⑪ 그 밖에 공개가 불가하다고 판단한 자료

○ 용역 참여직원이 노트북 등 **정보통신장비를 반출·입 시, 악성코드 감염 여부 및 자료 무단반출 확인** 등 보안조치 이행

- 프로젝트 종료 시, 용역업체 대표자 명의의 보안확약서[서식2] (서명) 제출

○ 사업 완료 후 용역업체의 PC·서버의 하드디스크 등의 **저장매체 탈거 및 완전삭제 후 반출 (내부정보 유출 차단)**

○ 기타 용역업체 관련 보안관리 사항은 「국가·공공기관 용역업체 보안관리 가이드라인」 참고

※ 본 검토사항에도 불구하고, 동 사업과 연관되는 보안사항에 대해서는 관련 법령·규정·지침 및 보안가이드라인을 준수하여 보안대책을 마련하고 이를 사업 수행에 반영하여야 함

[서식 1] 보안 서약서(사업 계약시 제출)

보 안 서 약 서

본인 및 본 사업 참여자는 _____ 사업을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약 합니다.

1. 본 사업을 시행함에 있어 계약서 및 서약서 상의 제반 보안사항의 철저한 이행
2. 사업수행과 관련하여 취득한 제반사항을 제 3자에게 일체 누설하거나 공개하지 않으며 타 용도로 사용 금지하며 사업담당자에게 사업수행 과정에서 생산된 산출물의 제출 및 파기
3. 사업 수행과 관련하여 하도급, 정품·기술공급 확약, 기타 관련 업체 등과 계약·협력 시 본 사업 수준의 보안 사항을 계약사항에 포함(혹은 보안 서약서 수령)하며, 상기 하도급· 협력 업체 등이 보안사항을 위반할 경우 주 사업자로서 동일한 법적 책임을 부담

상기사항을 숙지하고 이를 성실히 준수할 것을 동의하며 관련 규정·법령을 위반하거나 보안사고 발생 시 이에 대한 책임을 다할 것을 서약합니다.

- 용역(계약)사업 담당인력 보안 서약 서명부 -

* 본 계약 관련 실제 업무 담당 인력이 많을 시 대표자가 간인하여 별도 붙임문서로 서명부 제출
* 본 계약에 주 계약업체 외 하도급 및 기타 협력업체의 연구원 방문 기술지원이 포함될 경우 해당 출입 인력의 서약서 필수 제출

소속(부서)	직책	성명	자필 서명

년 월 일

서약자
(수행업체 대표자)

업 체 명 :
업체주소 :
직 책 :
성 명 : (서명)

[서식 2] 자료관리 확인서(사업 계약시 제출)

자 료 관 리 확 인 서

본인은 계약일(. .)로부터 'OOOOO 사업' 용역을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 용역 관련 자료(노트북, 보조기억매체, 저장 파일 등) 전량을 회수하고, 용역 참가자 소유의 컴퓨터 보관 자료를 완전 삭제하며, 복사본 등 용역사업 관련 자료를 일체 보유하지 않겠다.

2. 자료관리 운영방안

가. 기관의 내부 정보시스템 사용시 시스템 접근권한 명단 및 사용내역에 대하여 주기적으로 점검을 받는다.

나. 자료관리 대장을 비치하여 내부정보 이용시 이를 작성하고, 주기적으로 점검을 받는다.

다. 용역수행시 생산되는 주요 산출물(소스코드, 시스템 구성도 등)들은 지정된 시스템에만 작업·저장한다.

년 월 일

확인자
(수행업체 대표자)

업 체 명 :
업체주소 :
직 책 :
성 명 : (서명)

[서식 3] 누출금지대상 정보 열람 보안서약서(사업 추진 중 필요시 제출)

누출금지대상 정보 열람 보안서약서

본인은 년 월 일부로 "**OOOOO 사업**" 관련 업무 수행을 위한 누출금지대상 정보를 열람함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인(업체대표 포함)은 상기 업무 중 알게 될 일체의 내용이 직무상 기밀 사항임을 인정한다.
2. 본인(업체대표 포함)은 이 기밀을 누설함이 국가안전보장 및 국가이익에 위해가 될 수 있음을 인식하여 업무수행 중 지득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.
3. 본인(업체대표 포함)이 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다.
4. 본인(업체대표 포함)은 하도급업체를 통한 사업 수행시 하도급업체로 인해 발생하는 위반사항에 대하여 모든 책임을 부담한다.

년 월 일

- 용역(계약)사업 담당인력 누출금지대상 정보 열람 보안 서약 서명부 -

* 본 계약 관련 실제 업무 담당 인력이 많을 시 대표자가 간인하여 별도 붙임문서로 서명부 제출
* 본 계약에 주 계약업체 외 하도급 및 기타 협력업체의 연구원 방문 기술지원이 포함될 경우 해당 출입 인력의 서약서 필수 제출

소속(부서)	직책	성명	자필 서명

년 월 일

확약자
(수행업체 대표자)

업 체 명 :
업체주소 :
직 책 :
성 명 : (서명)

[서식 4] 보안확약서(사업 종료시 제출)

보 안 확 약 서

본인 및 본 사업 참여자는 _____ 사업 수행을 완료함에 있어 다음 사항을 준수할 것을 엄숙히 확약 합니다.

1. 용역사업 수행 중 취득한 모든 산출물 및 장비를 반납 하였으며 이외 사업 수행과 관련한 모든 자료를 사업담당자에게 반납 및 폐기

2. 용역수행과 관련하여 취득한 제반사항을 제 3자에게 일체 누설하거나 공개 하지 않으며 타 용도로 사용 금지

3. 본 사업 수행을 위하여 하도급 혹은 기타 관련 업체 등과 계약·협력 하였을 경우 해당 협력업체에 사업종료 후 보안사항에 대한 보안확약서를 받았으며 하도급 업체가 보안사항을 위반할 경우 주사업자로서 동일한 법적 책임을 부담

상기사항을 숙지하고 이를 성실히 준수할 것을 동의하며 관련 규정·법령을 위반하거나 보안사고 발생 시 이에 대한 책임을 다할 것을 확약합니다.

- 용역(계약)사업 담당인력 보안 확약 서명부 -

* 본 계약 관련 실제 업무 담당 인력이 많을 시 대표자가 간인하여 별도 붙임문서로 서명부 제출
* 본 계약에 주 계약업체 외 하도급 및 기타 협력업체의 연구원 방문 기술지원이 포함될 경우 해당 출입 인력의 서약서 필수 제출

소속(부서)	직책	성명	자필 서명

년 월 일

확약자
(수행업체 대표자)

업 체 명 :
업체주소 :
직 책 :
성 명 : (서명)

[서식 5] 자료 인수인계 대장(사업 종료시 제출)

자 료 인 수 인 계 대 장

○ 제공부서명 : ○○○○○실 (용역사업명: ○○○○○○○○○○)

번호	자료명	제공자			수령자				제공 형태	제공일	반납일	확인 (연구원 사업 책임자)	
		직급	성명	서명	소속 (직급)	성명	연락처	서명				제공	반납
1	*(예시) 네트워크 구성도*	*연구원*	*이몽룡*	*자필 서명*	*㈜용역업체 (대리)*	*성춘향*	*(회사번호)*	*자필 서명*	*전자문서, 책자, …*	*2020.05.01*	*2020.11.30*	*변학도*	*변학도*
2													
3													
4													
5													
6													

[서식 6] 산출물 인수인계 대장(사업 종료시 제출)

산 출 물 관 리 확 인 서

사업명 :

서약자 본인은 상기 사업을 수행하며 생성, 취득한 산출물을 연구원에 반환하며, 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인 및 참여 인원이 보유한 사업 관련 자료(노트북, 보조기억매체, 저장 파일 등) 전량을 회수하여 완전히 삭제하며, 복사본 등 관련 자료를 일체 보유하지 않겠습니다.

2. 대상 자료 목록

구분	산출물	내용(용도)	종류(수량)
1	*OOO 인터페이스 시제품*	*OO 설치용 프로그램*	*USB (2EA)*
2	*ㅁㅁㅁ 시뮬레이션 서버*	*ㅁㅁㅁ시험 및 데이터 저장*	*서버 (1EA)*

서약자 본인은 위 내용을 모두 확인하였으며, 위반 시 계약 사항 및 관계 법령에 따라 배상, 처벌될 수 있음을 인지 하였습니다.

20 년 월 일

서약자 (업체 대표)	**업체명 :**	**직위 :**
	생년월일 :	**성명 :** ㊞
서 약 집행자	**소 속 :**	**직위 :**
	생년월일 :	**성명 :** ㊞

[서식 7] 정보화사업 전산장비 반출입 대장(사업 종료시 제출)

전산장비 반출 · 입 대장

<관리책임자: >

연번	반입/반출	장비구분	관리번호(시리얼번호)	사용자	용도	반입일자 반출일자	반입 시 조치(백신, 취약점 점검)	반출 시 조치(자료 완전삭제 등)	관리책임자 확인
2021-1	반입	노트북	103SHBS003885	김보안	유지보수	2021.07.21 2021.07.21	O(1건 치료)	해당없음	서명
2021-1	반출	노트북	103SHBS003887	김보안	수리	 2021.07.26	O(이상없음)	HDD 제거 / 포맷 중 선택	서명
	반입	서버							
	반입	스토리지							
	반입	스위치							
	반입	보안장비							

※반입시 보안 조치 사항 : PC 취약점 점검, 바이러스 등 백신 점검

※반출(수리, 교체, 반납, 폐기 등)시 보안 조치사항 : 하드웨어 분리 후 반출 또는 저장자료삭제(포맷) 후 반출 선택