

『부산-김해경전철』

전산 보안설비 유지보수 용역 과 업 지 시 서

2020. 7. 8.

I. 일반사항

1. 과업명 : 『부산-김해경전철 전산 보안설비 유지보수 용역』

2. 정 의

본 과업지시서는 부산-김해경전철(이하 “발주기관”)에서 운영 중인 전산 보안설비의 집중적인 관리를 통한 정보보안 사고로부터 안전하게 보호하기 위하여 설치 또는 적용되어 있는 전산 보안설비에 대한 최적 성능유지와 장애 예방관리 및 장애복구 및 재발 방지를 위한 각종 조치 등을 위한 유지보수의 계약(이하 “전산 보안설비 유지보수 용역”)에 관한 사항으로, 유지보수 용역을 계약함에 있어 부산-김해경전철과 유지보수 계약업체(이하 “계약상대자”) 간에 체결되는 일반계약 내에 명시되지 않는 부분에 대하여 이행되어야 할 세부내용을 규정하며 계약의 일부가 된다.

3. 목 적

본 용역은 부산-김해경전철에서 운영하고 있는 「전산 보안설비」의 유지보수 계약을 통하여 보안시스템 및 보안솔루션을 최적으로 유지하고, 신속한 장애대응을 통하여 업무 자료의 안전한 관리 및 업무 서비스에 만전을 기하는데 그 목적이 있다.

4. 용역 기간

- 계약기간 : 2020년 8월 7일(착수일) ~ 2021년 8월 6일(1년)
- 사업예산 : 금101,838,000원(금일억일백팔십삼만팔천원/년,VAT포함)
- 입찰방법 : 제한경쟁입찰(실적제한, 자격제한)

5. 유지보수 대상

“유지보수 대상 “이라 함은 “발주기관 “의 <별첨 2>에 명시된 전산 보안설비 목록을 대상으로 한다.

※ <별첨 2> 2020년 전산 보안설비 유지보수 대상 목록 참조

6. 입찰 참가자격 기준 : 다음 각 항목을 구비한 업체나 자격조건을 갖춘 업체
- 가. 지방자치단체를 당사자로 하는 계약에 관한 법률 시행령 제13조(경쟁입찰의 참가자격) 및 동법 시행규칙 제14조(입찰참가자격 요건의 증명)에 의한 자격을 구비한 자로서
- ① 소프트웨어산업진흥법 제24조에 의거 소프트웨어사업자(컴퓨터관련 서비스사업)로 등록 및 정보통신공사업법 제14조에 의한 정보통신공사업 등록을 필한업체
- 나. 제안서 공고일 기준 3년 이내 정보통신설비 유지보수 용역실적 중 소요 예산(1억원/합산, VAT제외) 이상의 유지보수 실적을 보유한 업체
- 다. 안정적인 기술지원을 위하여 주요장비(UTM, 방화벽, NAC, 망연계, DLP, 통합로그 등)에 대한 제조사 또는 제조사가 인정하는 공급사의 기술지원확약서를 착수계 제출 시 제출 가능한 업체 (제출 대상장비는 <별첨 2> 참조)

II. 특수사항

1. 제출서류

- ① 낙찰자는 낙찰자 결정 후 및 계약 후 14일 이내에 유지보수 및 제반 책임 수행에 대한 다음 서류와 함께 착수계를 “발주기관”에 제출하여야 한다.
- ※ 제반 서류 및 제출기한은 <별첨 1> “전산 보안설비 유지보수 용역 제출서류”에 명시되어 있으므로 기한 내 제출하시기 바랍니다.
- ② 상주인력에 대한 보유 자격증 증빙자료 1부.
- ※ 운영중인 보안설비와 네트워크시설 장비의 중요성과 기술적 특수성을 감안하여 정보처리분야의 전문자격증(CCNA, Linux Master, 네트워크 관리자, 정보처리산업기사 중 1종[같은 분야 상위등급 자격등도 인정]) 보유자의 확인서류 첨부

2. 유지보수의 범위

- 가. 유지보수 대상 시스템의 유지관리를 위한 정기점검 및 장애 복구
 - 유지보수 대상 시스템은 매월 1회 이상 정기점검 하여야 한다.
 - 중요정보의 유지관리를 위한 백업(Configuration, 보안정책)을 실시
 - 유지보수 대상 시스템에서의 장애발생 시 정상적 업무 수행을 할 수 있도록 복구하여야 한다.
 - 유지보수 대상 시스템의 가능 범위 내에서의 최신의 버전으로 업그레이드 한다
- 나. 발주기관이 시스템 점검을 요청하거나 장애처리 등의 사유로 긴급(수시) 조치를 요청한 경우 신속히 이에 응하여야 하며, 조치 후 그 결과에 대한 보고서를 제출 하여야 한다.
- 다. 정보보호 소프트웨어의 적용대상이 되는 각종 보안설비의 OS, 서비스 Patch, 정책 Patch, DB에 대하여 정기적으로 운영환경을 점검하고, 최적 상태로 운영될 수 있도록 기술 자문 및 업무지원을 수행하여야 한다.
- 라. “계약상대자”는 유지보수 대상 시스템의 원활한 운영 및 신속한 장애 대처를 위하여 유지보수요원 1인을 발주기관이 지정하는 장소에 주2일 이상 상주하여 점검 및 운영, 지원업무 수행을 실시하여야 한다.
- 마. “계약상대자”는 유지보수 대상 전산 보안설비의 유지관리 및 해당 소프트웨어가 적용된 각종 장비에 대한 장애예방, 장애분석, 성능관리 등의 조치를 수행하고, 재발 방지를 위한 기술 자문에 성실히 임해야 한다.

3. 지원내용

- 가. “계약상대자”는 유지보수 대상 장비에 대하여 발주기관의 추가적인 점검 요청 시 “발주기관”의 업무에 지장을 주지 않는 범위 내에서 최적의 상태로 가동될 수 있도록 하기 위하여 점검을 하고 보고서를 제출하여야 한다.
- 나. “계약상대자”는 “발주기관”의 기술적 변경 요구시 변경이 가능한 경우 이에 응하여야 하며, “계약상대자”는 기술적인 변경에 소요된 부품 대금은 유상으로 지원하여야 한다.

- 다. “계약상대자”는 유지보수를 수행한 모든 처리 내역을 소정의 관련서식에 의거 담당자의 확인을 득하여야 한다.
- 라. 장애 발생시 “시스템” 수리가 장기간 소요된다고 판단될 때에는 별도의 동일 기종이나 그 이상의 시스템을 임시 대체하여 업무의 공백이나 차질을 초래하지 않도록 조치하여야 한다.
- 마. “계약상대자”는 기존 네트워크 LAN케이블에 대한 유지보수에 대해서는 무상 처리하고 해당 범위는 “발주기관” 모든 사업장을 포함하며, “발주기관”은 “계약상대자”에게 LAN케이블 외의 필요 자재를 지원한다.
- 바. 네트워크 LAN케이블에 대한 유지보수는 분기 및 수시로 진행되는 “발주기관” 조직개편 및 인사이동으로 인한 케이블 신·증설, 이전 등을 포함하며, 그 소요자재 비용은 ‘마’항과 같이 처리한다.
- 사. “계약상대자”는 S/W Version Upgrade시 이를 “발주기관”에게 즉시 통보하고, 그 소요비용은 유상으로 처리한다.(단, S/W 하자담보 책임기간은 사업을 종료한 날부터 1년으로 한다)
- 아. “발주기관”은 유지보수 대상시스템과 관련된 사항에 대하여 “계약상대자”에게 교육 지원을 요청할 수 있으며 “계약상대자”는 무상으로 교육을 지원하여야 한다.

4. 장애발생 통보 및 처리

- 가. “계약상대자”는 장애발생시 통보받은 시간으로부터 4시간 이내에 유지보수 요원을 파견하여, 24시간 이내에 장애처리 및 원인규명을 하여야 한다.
- 나. “계약상대자”는 시스템의 수리가 24시간 이상 소요된다고 판단될 경우에는 별도의 동종 기기로 대체하고 업무에 차질이 없도록 조치하여야 하며, 동종 기기로 대체하고 기능이 정상 작동하게 임시 조치한 이후 수리시간에 대한 지체상금은 면하기로 한다.
- 다. 유지보수(정기점검, 장애복구 등) 시간은 “발주기관”의 복무관리규정에서 정한 근무시간을 원칙으로 하며 “발주기관”의 긴급 및 장애복구 중 근무

시간 초과 시 유지보수 시간을 연장 요구할 수 있으며, 이때 “계약상대자” 는 이에 응하여야 한다.

라. 도착시간 지연으로 장비의 이상발생이 신속히 해소되지 않았을 경우, 발주자는 해당 장비에 대하여 다음과 같이 지체상금을 공제한 후 유지보수료를 지급할 수 있다. 다만, 천재지변 등 발주자가 인정하는 불가항력적인 사유로 인하여 발주자의 승인을 받은 경우에는 예외로 한다.

※ 지체상금 = 월 유지보수료 × 2.5/1000 × 지체시간

5. 대금지급

가. “계약상대자” 는 월 단위의 유지보수료에 대하여 “유지보수확인서 “를 전산담당자의 확인을 거쳐 해당 월 종료 익월 10일 이내 “발주기관 “에게 제출하여 대금지급을 청구하며 “발주기관” 은 청구를 받은 날로부터 30일 이내에 계좌입금방법으로 “계약상대자” 에게 지급한다.

나. 유지보수비는 일할계산 방식으로 하며, 1월 미만일 경우에는 월 유지 보수비의 30분의 1에 해당하는 비율로 계산한다.

6. 실비정산

가. “발주기관” 이 작업수행을 요청하거나 “계약상대자” 의 요청에 의하여 “발주기관” 이 승인한 다음 각 호의 업무수행 시 “발주기관” 은 실비를 보상할 수 있다.

1) 유지보수 대상 신규장비 반입에 따른 기존 장비 이전설치 시 소요되는 실비는 인건비(근무 시간 내 제외), 재료비, 운송비를 보상

2) 장애 발생으로 비 유지보수 대상 장비의 부품을 교체한 경우의 부품비

3) 화재 및 천재지변 등으로 유지보수 대상 보안설비 사용이 불가능하게 파손된 장비 중 시급을 요하는 장비는 당사자 간에 협의 후 선조치하고 이때 처리한 모든 장비, 인건비, 재료비, 운송비 등 일체 비용

나. “계약상대자” 는 실비보상 청구 시 청구사유 발생일의 해당 월부터 3개

월 이내에 청구하여야 함. 다만, 유지보수 용역계약이 종료 시에는 다음 월 10일까지 청구

7. 책임의 면제

다음의 각 항에 해당하는 사유가 발생한 때에는 “계약상대자”는 “발주기관 “에 대한 의무가 면제되며 이로 인하여 발생하는 손해를 “계약상대자”가 책임지지 않는다. 단, 장애 처리에 대해서는 “발주기관”의 비용 부담과 “계약상대자”의 기술 지원으로 정상 복구시키며, 그 범위는 사전에 합의를 하여 결정한다.

가. 천재지변에 의한 경우

나. 전시와 같은 국가비상사태의 경우

다. “발주기관”의 과실로 인하여 발생한 장애

라. “계약상대자”에게 책임이 없는 사유인 것임을 “발주기관 “이 인정할 때

8. 보안사항

가. 법령 요건

1) 국가정보보안기본지침에 근거하여 “<별첨 6>외주 용역사업 보안특약” 및 부산-김해경전철의 ‘정보화업무처리규정’을 준수하여야 한다.

2) 본 사업 중에 취득한 자료 중 ‘<별첨 6-2>누출금지 대상정보’에 대해 사업수행 중은 물론 사업완료 후에도 비밀을 준수할 수 있도록 사업참여인력 전원은 ‘<별첨 3>보안서약서’ 및 ‘<별첨 4>개인정보보호서약서’를 발주기관에 제출하여야 한다.

3) 지방자치단체를 당사자로 하는 계약에 관한 법률 시행령 제92조 제1항 19조에 따라 ‘누출금지 대상정보’의 외부 유출시 “별첨 6-1”에 따라 처리하고 부정당 업체로 등록한다.

4) 계약상대자는 개인정보보호법 및 개인정보처리방침을 준수하여야 한다. 개인정보처리방침에 따라 민원응대 및 업무수행을 목적으로 주민등록

번호 등의 개인정보를 처리함에 따라, 개인정보보호법이 규정하는 개인정보보호 의무를 반드시 준수해야 한다.

- 5) 계약상대자는 “<별첨 6-2> 누출금지 대상 정보”을 포함하여 과업 수행 과정에서 취득한 자료와 정보에 관하여 사업수행의 전후를 막론하고 “발주기관”의 승인 없이 외부에 유출 또는 누설하여서는 아니 되며, 이를 위반하였을 경우 “사업자 보안위규 처리기준”에 따라 행정조치 되며, 위규 수준에 따른 “위약금 부과”라는 추가 제재를 받을 수 있다.

나. 관리적 보안

- 1) 인적, 물적 자원에 대한 보안정책 및 지침을 수립하여 적용하고, 수시로 보안 진단을 실시해야 한다.
- 2) 외부 인력을 포함한 사업 수행 인력을 대상으로 주기적인 보안교육 실시 및 보안 서약서 작성 등 보안 관리에 철저를 기해야 한다.
- 3) 본 사업 수행 중 취득한 지식에 대하여 과업수행중은 물론 사업이 완료된 후에도 비밀 보안을 준수해야 한다.
- 4) 계약상대자는 사업 수행과정에서 취득한 자료와 정보에 관해서는 사업수행의 전후를 막론하고 “발주기관”의 승인 없이 외부에 유출 또는 누설하여서는 안 되며, 이를 위반 할 시 향후 법적 책임이 있음을 포함한 ‘<별첨 5>보안확약서’를 계약이 완료되는 시점에서 작성 하여 제출한다.

다. 물리적 보안

- 1) 과업수행을 위하여 사무실을 운영 할 경우 원칙적으로 실제 사업에 참여하는 자만 출입을 허용 한다.
- 2) 과업수행을 위한 사무실은 별도 출입문(경보장치 포함)이 설치된 폐쇄 공간으로 하며, CCTV를 설치하여 보안을 강화한다.
- 3) 출입자관리 기록부, 보안점검표를 비치하여 보안 관리를 실시한다.
- 4) 문서나 프로그램 버전 및 처리 지침 등은 관리적 보안과 함께 시건장치, 통제구역 등을 통하여 물리적 보안도 실시한다.

- 5) 업무수행용 PC, 중요업무 PC에는 패스워드를 도입하여 보안성을 강화한다.
- 6) 업무수행용 PC는 인터넷망과 분리하여 운용하고(과업수행 관련 내부 인트라넷만 사용) 업무상 인터넷 연결이 필요한 경우 별도의 인터넷 전용 PC를 설치하여 사용한다.
- 7) USB Type의 보조기억 매체는 사용하지 않는 것을 원칙으로 하며, 모든 자료는 내장 HDD 또는 등록된 CD에 저장하여 관리하며, 부득이한 경우 발주기관에서 제공하는 보안USB를 사용한다.
- 8) 개인소유의 PC 및 보조기억장치 반입·반출 하려는 경우 발주기관의 승인을 통하여 허용한다.

라. 문서 보안

- 1) 계약상대자는 용역 수행 중 생산된 문서나 활용 중인 책자에 대해 그 중요도에 따라 기밀, 대외비, 일반정보로 분류하여 관리한다.
- 2) 사업관련 자료를 반출 할 경우 발주기관의 승인을 받아 내역을 기록한 후 반출한다.
- 3) 전산담당자 책임 하에 모든 출력물에 대한 외부 유출을 감시하며, 특히 인터넷을 통한 외부 유출을 모니터링(발주기관 허가 후 반출)한다.
- 4) 관련 자료 및 문서는 외부에 노출되지 않도록 문서함에 관리한다.
- 5) 사업 완료 후 반드시 유지보수 기간에 생성된 일체의 자료를 반환하고 관련 자료를 복구가 불가능한 방법으로 파기한다.
- 6) 발주기관의 승인이 없는 한 목적 외 사용 및 제3자에게 자료제공 금지한다.
- 7) 과업 수행에 필요한 기밀자료는 발주기관의 전산담당자 입회하에서만 열람한다.

마. 기술적 보안

1) 서버사용자 및 패스워드 관리

- 패스워드의 길이는 9자 이상을 원칙으로 하고 영문, 숫자, 특수문자를 혼용하여 설정한다.
- 패스워드는 3개월 주기로 변경하도록 하고, 전산담당자의 승인에 따라 과업수행을 위해 제공된 PC 또는 보안USB 이외의 계약상대자

사무실, 개인PC, USB 등 보조기억매체, 클라우드 등에 사용되거나 전송, 저장되어서는 아니된다.

- 2) 장애, 사고 등으로 인한 시스템피해에 대해 최근에 백업한 시점의 내용으로 복구할 수 있는 백업정책을 수립 및 실행한다.
- 3) 시스템 계정 접근시 반드시 발주기관에서 제공한 접근방식을 이용하여야 하며, 주 과업수행자 이외의 참여인력이 접근하는 경우 반드시 발주기관의 승인을 득하여야 한다.

바. 인력 보안

1) 사업 착수 시

- 사업 참여인원 및 대표자에 대해서는 ‘<별첨 3>보안서약서’를 제출하며, 발주기관의 신원조회 요구 시 협조해야 한다.
- 사업 상주인원에 대해서는 신원을 확인(인적사항[이름, 주민번호 앞 6자리, 실거주지 주소, 직장명, 직장 주소), 학력, 경력, 자격증, 자필서명)할 수 있는 서류를 제출하여야 한다.
- 계약상대자는 용역사업 수행 전 참여인원에 대해 법률 또는 규정에 의한 비밀유지의무 준수 및 위반 시 처벌내용 등에 대한 제반교육을 실시한다.
- 계약상대자는 하도급 계약을 체결 할 경우 본 사업계약 수준의 비밀유지 조항을 포함하여야 하며 하도급 업체도 본 계약과 동일하게 절차 및 보안의무를 준수해야 한다.

2) 사업 수행 시

- 계약상대자는 보안인식강화를 위해 주기적으로 자체 보안교육을 실시해야 하며, 발주기관에서 요구하는 보안교육에 참석해야 한다.
- 계약상대자는 임의로 사업 참여인원을 교체 할 수 없고 신상변동(퇴직, 해외여행 등)사항 사유 발생 시 발주기관에 즉시 보고하고 승인을 받아야 한다.

3) 사업 종료 시

- 사업에 참여한 사업자가 활용한 PC 및 서버의 경우, 사업 완료 후

자료의 복구가 불가능 하도록 조치해야 한다.

- 계약상대자는 사업관련 자료를 보유해서는 안되며, 이를 위반 사항 후 법적책임이 있음을 포함한 ‘<별첨 5>보안확약서’ 를 작성하여 제출한다.

9. 변동사항 등의 통보 및 물품의 이동, 개조, 증설 등

- 가. “계약상대자” 는 계약체결 이후 주소, 대표자, 상주인력 등의 주요사항이 변경되었을 경우에는 이를 지체 없이 “발주기관” 에게 통보하여야 하며, 이의 불이행으로 인하여 발생한 손해에 대하여는 “계약상대자” 의 책임으로 한다.
- 나. “발주기관 “은 “유지보수 대상” 과 관련한 장비의 이동, 개조, 증설 등의 사항이 발생한 경우에는 이를 사전에 “계약상대자” 에게 통보하여야 하며 “계약상대자” 는 ” 발주기관 “의 지원 요구시 이에 응해야 한다.

10. 기타사항

- 가. 본 시방서에 명시된 모든 조항은 최소한의 사양, 시방만을 규정 하였으므로 상세히 기술되지 않았거나 누락된 사항에 대해 “계약상대자” 는 시스템 운영상 하자가 발생되지 않도록 사전 조치하여야 한다.
- 나. “계약상대자” 는 만일의 경우 면허, 특허권, 등록된 의장권, 공업소유권 및 지적 유권의 침해로 인한 모든 문제와 소송으로부터 “발주기관” 은 전적으로 면책하고 이를 “계약상대자” 의 부담으로 한다.
- 다. 과업지시서에 대한 이견이 있을 때는 “발주기관” 의 해석에 따르고 과업지시서에 명시되지 않은 사항은 “발주기관” 의 관련 법령과 일반관례에 따르며 과업지시서에 관한 소송 관할 법원은 “발주기관” 의 주소지를 관할하는 법원으로 한다.

<별첨 1>

전산 보안설비 유지보수 용역 제출서류

① 계약 시 : 계약서

1. 상주인력 자격증사본

- 정보처리 분야 산업기사 이상 또는 동등이상의 민간자격증(CCNA, Linux Master, 네트워크 관리자, 정보처리산업기사 중 1종[같은 분야 상위등급 자격 등도 인정])

② 계약후 14일 이내

1. 착수계

2. 공급사 및 제조사 기술지원확약서

- ※ 공지사항 : <별첨 2> 표시된 해당 장비는 발주기관과 공급사 및 제조사의 '제품 및 공급 기술지원협약'를 체결함(협약서 원본은 발주기관 전산담당 '열람')

3. 보안서약서<별첨 3> 및 개인정보보호 서약서<별첨 4>

- 본 용역사업과 관련하여 출입하는 모든 인원

4. 유지보수 수행계획서

- 부산-김해경전철이 보유한 보안설비, 네트워크 설비 등
- 유지보수 참여자 명단

5. 개인정보 위탁계약서

③ 계약 완료시 : “발주기관”이 제공하는 서식의 ‘본 용역사업 관련 자료를 보유하고 있지 않다’는 대표자 명의의 보안확약서<별첨 5>

<별첨 2>

전산 보안설비 유지보수 대상 목록

구 분	HW/SW	제조사	구축연월	모델명(버전)	수량	비 고
시스템 접근제어 (기술지원협약)	HW	휴네시온	2016.12	NGSH-100	1	
	SW	휴네시온	2016.12	H/W 어플라이언스 일체형 NGS V6.0	1	15 Node
통합로그 저장서버 (기술지원협약)	HW	디에스엔텍	2016.12	Log saver H200	1	
	SW	디에스엔텍	2016.12	H/W 어플라이언스 일체형 Log saver V3.0, MY-SQL2008R2	1	
	Agent	디에스엔텍	2016.12	Log saver NET V3.0	20	
DLP (기술지원협약)	HW	HP	2016.12	HP ProLiant DL20 Gen 9	1	
	SW	워터월시스템즈	2016.12	WaterWall V5.0	1	
	Agent	워터월시스템즈	2016.12	Client5.0	200	
유해사이트 차단 (기술지원협약)	HW	소만사	2016.12	Hyboost H100	1	
	SW	소만사	2016.12	H/W 어플라이언스 일체형 WebKeeper 10.0	1	
웹 방화벽 (기술지원협약)	HW	펜타시큐리티 시스템	2016.12	WAPPLES-100 v4.0	1	
	SW	펜타시큐리티 시스템	2016.12	H/W 어플라이언스 일체형 DDoS, SLQ injection ,XSS 웹 위변조 공격 방어	1	
통합보안 장비 (기술지원협약)	H/W	AXGATE	2016.12	AXGATE-2300	1SET (2EA)	
	S/W	AXGATE	2016.12	H/W 어플라이언스 일체형 SSLVPN,VPN,IPS,F/W,Anti-Virus	1SET	200User
네트워크 접근제어 (기술지원협약)	HW	지니네트웍스	2016.12	S20(차단서버), C10(정책서버)	1SET (2EA)	200User
	SW	지니네트웍스	2016.12	H/W 어플라이언스 일체형 Geni Agent 4.0	2	
DMZ 망연계 (기술지원협약)	HW	휴네시온	2016.12	i-oneNet Stream IS 1EA i-oneNet Stream ES 1EA	1SET (2EA)	
	SW	휴네시온	2016.12	H/W 어플라이언스 일체형 i-oneNet v 2.0	2	
제어망 망연계 DB서버 (기술지원협약)	HW	HP	2015.12	HP ProLiant DL380p Gen8	1	
	SW	휴네시온	2015.12	CentOS v5.8, MYSQL v5.5.24	1	
제어망 망연계 (기술지원협약)	HW	휴네시온	2015.12	i-oneNet Stream IS 2EA i-oneNet Stream ES 2EA	2SET (4EA)	
	SW	휴네시온	2015.12	H/W 어플라이언스 일체형 i-oneNet v 2.0	4	
L4 (기술지원협약)	HW	파이오링크	2015.12	FIOLINK 1216K	2	
	SW	파이오링크	2015.12	H/W 어플라이언스 일체형 Load Blance, L4 F/W 기능	2	
L3	HW	한드림넷	2016.12	SG2228G-L3	2	
	SW	한드림넷	2016.12	H/W 어플라이언스 일체형	2	
L2	HW	한드림넷	2016.12	SG2024	1	
	SW	한드림넷	2016.12	H/W 어플라이언스 일체형	1	

보 안 서 약 서

본인은 년 월 일부로 _____사업과 관련한 업무를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 나는 _____사업과 관련된 소관업무가 국가기밀 사항임을 인정하고 제반 보안관계규정 및 지침을 성실히 준수한다.
2. 나는 이 기밀을 누설함이 국가이익을 침해할 수도 있음을 인식하고 재직 중은 물론 퇴직 후에도 알게 된 모든 기밀사항을 일체 타인에게 누설하지 아니한다.
3. 나는 기밀을 누설한 때에는 아래의 관계법규에 따라 엄중한 처벌을 받을 것을 서약한다.

가. 전자정부법 제35조(금지행위) 및 제76조(벌칙)

년 월 일

서약자	소속	직급	생년월일		
		직위	성 명		인
서 약	소속	직급			
집행자		직위	성 명		인

개인정보보호 서약서

나 (_____)는 (_____) 업무중에 알게 된 개인정보 및 부산-김해경전철 업무와 관련된 정보에 대하여 업무 수행중이나 업무 수행 후에도 비밀을 지킬 것을 서약 합니다.

또한 부산-김해경전철에서 수집한 개인정보의 보호를 위해 부산-김해경전철에서 정하는 개인정보 보호 관리 규정을 준수할 것이며, 적절한 절차 없이 개인정보를 무단으로 조회, 누출하지 않을 것을 서약합니다.

개인정보 보호와 관련한 비밀의 준수와 개인정보 보호를 위한 법적 준수기준인 “개인정보 보호법”에 명시된 모든 조항과 부산-김해경전철의 개인정보 보호 관리 규정 등 관련된 모든 조항이 포함된다는 것을 충분히 설명 받고 숙지하였습니다.

만약, 이러한 서약에도 불구하고 업무상 알게 된 사항에 대하여 비밀을 누설하거나 정당한 사유없이 조회, 유출, 오용할 경우, 형사상 민사상의 법률 조항에 의거하여 제재를 받을 수 있음을 통고 받았으며, 이러한 제재에 대하여 이의를 제기하지 않을 것을 본인의 자의로 서약합니다.

일시 : 년 월 일
소속 :
성명 : (인)

부산-김해경전철(주) 귀하

보안확약서

본인은 귀 기관과 계약한 _____ 사업의 수행을 완료함에 있어, 다음 각호의 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 금지하겠습니다.
2. 본 업체(단체)는 하도급업체에 대해 상기 항과 동일한 보안사항 준수 책임을 확인하고 보안확약서 징구하였으며, 하도급업체가 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

소 속 :

직 급 :

성 명 :

(서명)

부산-김해경전철(주) 귀하

<별첨 6>

외주 용역사업 보안특약

- ① 사업자는 부산-김해경전철의 보안정책을 위반하였을 경우 <별첨6-1>의 사업자 보안위규처리 기준에 따라 위규자 및 관리자를 행정조치한다.
- ② 사업자는 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 <별첨6-2>의 누출금지 대상 정보에 대한 보안관리계획을 착수계에 기재하여야 하며, 해당 정보 누출시 부산-김해경전철은 국가계약법 시행령 제76조에 따라 사업자를 부정당업체로 등록한다.
- ③ 사업 수행과정에서 취득한 자료와 정보에 관하여 사업수행중은 물론 사업 완료 후에도 이를 외부에 유출해서는 안 되며, 사업종료 시 정보보호담당자의 입회하에 완전 폐기 또는 반납해야 한다.
- ④ 사업자는 사업 최종 산출물에 대해 정보보안 전문가 또는 전문보안 점검도구를 활용하여 보안 취약점을 점검, 도출된 취약점에 대한 개선을 완료하고 그 결과를 제출해야 한다.

<별첨 6-1> 사업자 보안위규 처리기준

<별첨 6-2> 누출금지 대상 정보

사업자 보안위규 처리기준

구 분	위 규 사 항	처 리 기 준
심 각	1. 비밀 및 대외비 급 정보 유출 및 유출 시도 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 해킹 시도 나. 시스템 구축 결과물에 대한 외부 유출 다. 시스템 내 인위적인 악성코드 유포	◦사업참여 제한 ◦위규자 및 직속 감독자 등 중징계 ◦재발 방지를 위한 조치 계획 제출 ◦위규자 대상 특별보안 교육 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 관리 소홀 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 사진 촬영 3. 전산정보 보호대책 부실 가. 업무망 인터넷망 혼용사용, 보안 USB 사용규정 위반 나. 웹하드·P2P 등 인터넷 자료공유사이트를 활용하여 용역 사업 관련 자료 수발신 다. 개발·유지보수 시 원격작업 사용 라. 저장된 비공개 정보 비밀번호 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 직속감독자 등 중징계 ◦재발 방지를 위한 조치계획 제출 ◦위규자 대상 특별 보안교육 실시

구분	위규사항	처리기준
보통	1. 기관 제공 중요정책·민감 자료 관리 소홀 가. 주요 현안·보고자료를 책상위 등에 방치 나. 정책·현안자료를 휴지통·폐지함 등에 유기 또는 이면지 활용 2. 사무실 보안관리 부실 가. 캐비닛·책상 등을 개방한 채 퇴근 나. 출입기를 책상위 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. 휴대용 저장매체를 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. PC미빌번호를 모니터옆 등 외부에 노출 바. 비인가 보조기억매체 무단 사용	◦위규자 및 직속 감독자 등 경징계 ◦위규자 및 직속 감독자 사유서/경위서 징구 ◦위규자 대상 특별 보안교육실시
경미	1. 업무 관련서류 관리 소홀 가. 진행중인 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

구분	위규수준			
	A급	B급	C급	D급
위규	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금	부정당업자 등록 계약금액의 10%	계약금액의 7%	계약금액의 5%	계약금액의 3%

<별첨 6-2>

누출금지 대상정보

1. 부산-김해경전철 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. 보안시스템 및 정보보호시스템 도입 현황
7. 침입차단시스템·방지시스템(IPS)등 정보보호제품 및 라우터·스위치 등 네트워크 장비 설정 정보
8. 「공공기관의 정보공개에 관한 법률」 제9조 제1항에 따라 비공개 대상 정보로 분류된 기관의 내부분서
9. 「개인정보보호법」 제2조제1호의 개인정보
10. 「보안업무규정」 제4장 문서보안의 제21조제2항 비밀세부분류지침의 대외비 이상
11. 그 밖에 부산-김해경전철이 공개가 불가하다고 판단한 자료

보안설비 유지보수 용역업체 정보보호 준수사항

본 용역에 참여하는 업체는 다음 사항을 참고하여 정보보호 요구사항을 준수하여야 한다.

가) 일반사항

- ① 부산-김해경전철의 보안업무규정, 지침 및 정보시스템 운영관리 지침을 준수하여야 한다.
- ② 부산-김해경전철의 자산에 접근하기 위해서는 부산-김해경전철의 접근 통제 절차를 준수하여야 한다.
- ③ 부산-김해경전철은 계약서의 보안사항을 준수하고 있는지를 감사할 권한을 가진다.
- ④ 부산-김해경전철의 감사 시 필요한 근거 자료를 제공하고 현장 실사에 적극 협조하여야 한다.
- ⑤ 유지보수의 수행은 현장에서 실시하며, 원격접속은 담당자의 승인을 득한 후 시행 한다.

나) 용역업체의 직원에 대한 보안관리

- ① 참여직원에 대해서 각 개인의 친필 서명이 들어간 보안서약서를 제출한다.
- ② 참여직원은 임의로 교체할 수 없으며, 교체 시 부산-김해경전철의 승인을 받는다.

다) 내부 자료에 대한 보안관리

- ① 업무 수행을 위해 제공하는 내부 자료는 자료관리대장을 작성하여 인수인계 시 직접 서명한다.
- ② 제공된 내부 자료에 대해 복사 및 외부반출을 할 수 없으며, 업무 완료 후 부산-김해경전철에 반환한다.

라) 장비에 대한 보안관리

- ① 통신실 내 노트북을 포함한 임의 전산장비의 반입은 금지한다.
단, 유지보수 대상 장비의 고장에 따른 대체장비 설치 및 장비 점검 시 필요한 작업 수행을 위하여 노트북 등을 반입 할 경우 부산-김해 경전철의 사전 승인을 받아야 한다.
- ② USB 등의 보조기억매체는 사용할 수 없다. 다만, 불가피한 경우는 부산-김해경전철에서 제공하는 보안USB를 사용하여야 한다.
- ③ 승인을 득한 반입된 장비에 대해서만 업무망(제어망) 접속을 승인한다.

마) 기타 산출물에 대한 보안관리 등

- ① 업무 수행 시 생산되는 모든 산출물은 부산-김해경전철에서 지정한 PC에 저장한다.
- ② 업무 수행으로 생산되는 모든 산출물 및 기록은 부산-김해경전철가 인가하지 않은 자에게 제공·대여·열람을 금지한다.
- ③ 업무 수행으로 생산되는 모든 산출물 및 기록의 지적재산권은 부산-김해경전철에 있다.
- ④ 제3자에 의한 보안사고 발생 시 민·형사상의 모든 법적 책임은 제3자에게 있다.
- ⑤ 보안사고 발생 또는 인지 시에는 즉시 부산-김해경전철에 통보하여야 한다.

<별첨 8>

개인정보처리위탁 계약서

부산-김해경전철(이하 “발주기관”이라 한다)과 _____(이하 “유지보수사업자”이라 한다)는 “발주기관”의 전산 보안설비 통합유지보수와 관련하여 수집되는 개인정보 처리업무를 “유지보수사업자”에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제1조 (목적) 이 계약은 “발주기관”의 개인정보처리업무를 “유지보수사업자”에게 위탁하고, “유지보수사업자”는 이를 승낙하여 “유지보수사업자”의 책임아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는 개인정보보호법, 동법 시행령 및 시행규칙, 「표준 개인정보 보호지침」(행정안전부 고시 제25호)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) “유지보수사업자”는 계약이 정하는 바에 따라 (전산 보안설비 통합유지보수 및 침해사고분석, 개인정보 노출 예방, 사고경위 조사 및 재발방지 대책 수립)을 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.1)

[목적]

1. 개인정보 안전 조치, 노출 예방 조치
2. 침해시도, 해킹, 악성코드 분석을 통한 시스템 안전성 확보조치
3. 시스템 장애분석 및 조치, 사고원인 분석, 재발방지 대책 수립

[사용되는 개인정보의 범위]

보안시스템, 정보시스템, 개인정보보호 시스템의 로그기록에 포함된 모든 개인정보(시스템정보, 연락처, 이름, 주민등록번호 등)

제4조 (재위탁 제한) ① “유지보수사업자”는 “발주기관”의 사전 승낙을 얻은 경우를 제외하고 “발주기관”과의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.

② “유지보수사업자”가 재위탁받은 수탁회사를 선임한 경우 “유지보수사업자”는 당해 재위탁계약서와 함께 그 사실을 즉시 “발주기관”에 통보하여야 한다.

제5조 (개인정보의 안전성 확보조치) “유지보수사업자”는 개인정보보호법 제29조, 동법 시행령 제30조 및 개인정보의 안전성 확보조치 기준 고시(행정안전부 고시 제2011-43호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제6조 (개인정보의 처리제한) ① “유지보수사업자”는 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설

1) 각호의 업무 예시 : 그룹웨어 관리 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 이름, 주소, 연락처 처리 등

하여서는 안 된다.

② “유지보수사업자”는 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보보호법」 시행령 제16조에 따라 즉시 파기하거나 “발주기관”에 반납하여야 한다.

③ 제2항에 따라 “유지보수사업자”가 개인정보를 파기한 경우 지체없이 “발주기관”에게 그 결과를 통보하여야 한다.

제7조 (수탁자에 대한 관리·감독 등) ① “발주기관”은 “유지보수사업자”에 대하여 다음 각 호의 사항을 관리하도록 요구할 수 있으며, “유지보수사업자”는 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속현황
3. 개인정보 접근 또는 접속 대상
4. 목적외 이용·제공 및 재위탁 금지 준수여부
5. 암호화 등 안전성 확보조치 이행여부
6. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② “발주기관”은 “유지보수사업자”에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, “유지보수사업자”는 특별한 사유가 없는 한 이행하여야 한다.

③ “발주기관”은 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 1회 “유지보수사업자”를 교육할 수 있으며, “유지보수사업자”는 이에 응하여야 한다.2)

④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 “발주기관”은 “유지보수사업자”와 협의하여 시행한다.

제8조 (손해배상) ① “유지보수사업자” 또는 “유지보수사업자”의 임직원 기타 “유지보수사업자”의 수탁자가 이 계약에 의하여 위탁 또는 재위탁받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 “유지보수사업자” 또는 “유지보수사업자”의 임직원 기타 “유지보수사업자”의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 “발주기관” 또는 개인정보주체 기타 제3자에게 손해가 발생한 경우 “유지보수사업자”는 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보주체 기타 제3자에게 발생한 손해에 대하여 “발주기관”이 전부 또는 일부를 배상한 때에는 “발주기관”은 이를 “유지보수사업자”에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, “부산-김해경전철”과 “유지보수사업자”가 서명 또는 날인한 후 각 1부씩 보관한다.

부산-김해경전철

경남 김해시 생림대로 38(삼계동 655)

대표이사

(인)

유지보수사업자

○○시 ○○구 ○○동 ○○번지

대표이사

(인)

2) 「개인정보 안전성 확보조치 기준 고시」(행정안전부 고시 제2011-43호) 에 따라 개인정보처리자 및 취급자는 1년에 1회 이상 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.