**Cloud & Data Security Framework 구축**

**제안요청서**

2024. 4

**에쓰-오일 주식회사**

**목 차**

[I. 프로젝트 추진 개요 4](#_Toc164855737)

[1. 회사 소개 4](#_Toc164855738)

[2. 추진 배경 4](#_Toc164855739)

[3. 주요 추진 목표 4](#_Toc164855740)

[4. 추진 일정 (잠정) 4](#_Toc164855741)

[II. 프로젝트 추진 내용 5](#_Toc164855742)

[1. 현황 5](#_Toc164855743)

[2. 추진 범위 5](#_Toc164855744)

[3. 프로젝트 산출물 10](#_Toc164855745)

[4. 예상 구축 일정 13](#_Toc164855746)

[III. 제안서 작성 내용 13](#_Toc164855747)

[1. 프로젝트의 이해 13](#_Toc164855748)

[2. 프로젝트 수행 방안 13](#_Toc164855749)

[3. 프로젝트 관리 및 지원방안 14](#_Toc164855750)

[4. 구축비용 14](#_Toc164855751)

[5. 기타 제안 (추가) 14](#_Toc164855752)

[6. 제안사 소개 15](#_Toc164855753)

[IV. 제안 안내 15](#_Toc164855754)

[1. 일반사항 15](#_Toc164855755)

[2. 제안서의 효력 17](#_Toc164855756)

[3. 제안서 작성지침 17](#_Toc164855757)

[4. 제안서 제출 17](#_Toc164855758)

[V. 보안 요구사항 18](#_Toc164855759)

[1. 사이버보안 관리 18](#_Toc164855760)

[[첨부 01] 제3자 보안 통제 요건 22](#_Toc164855761)

[[첨부 02] 제3자 보안 준수 약정서 24](#_Toc164855762)

[[첨부 03] 제3자 정보보호 서약서 26](#_Toc164855763)

[[첨부 04] 제3자 사이버보안 교육 확인서 31](#_Toc164855764)

[제3자 사이버보안 교육 확인서 31](#_Toc164855765)

[[첨부 05] 제3자 보안점검 확인서 32](#_Toc164855766)

[[첨부 06] 보안 확약서(참여인력용) 33](#_Toc164855767)

[[첨부 07] 투입인력 이력 양식 34](#_Toc164855768)

# 프로젝트 추진 개요

## 회사 소개

1. 회사명칭: 에쓰-오일 주식회사 ([www.s-oil.com](http://www.s-oil.com))
2. 본사주소: 서울특별시 마포구 백범로 192 (공덕동)
3. 업 종: 석유정제업
4. 종업원수: 3,111명 (`23. 12월 말 기준)
5. `23년 매출액: 35 조원

## 추진 배경

* + 회사는 주요 IT시스템 구축 방식을 자체 구축(On-premise) 방식에서 Cloud 방식으로   
     전환을 추진 중임
  + 임직원의 협업 및 커뮤니케이션 개선을 위해 임직원 OA 환경을 Microsoft Cloud 환경으로 확장 검토 중
  + 이에 따라, 사이버보안의 적용 범위도 Cloud 환경으로 확대 검토가 필요함
  + Cloud 환경에서도 현재의 사이버보안 수준 이상으로 운영할 수 있는 사이버보안 프레임워크 설계가 필요함
  + 기존 업무 환경과 Cloud 환경이 공존하는 Hybrid 업무환경에서 회사의 중요 데이터를 안전하게 저장∙활용할 수 있는 일관된 통제 방안 수립이 필요함

## 주요 추진 목표

1. Data & Mobile 보안 강화
2. Cloud Security Framework 구축

## 추진 일정 (잠정)

1. 프로젝트 기간 : 2024년 5월 ~ 2024년 10월 (6개월)
2. 계약 Process

****

# 프로젝트 추진 내용

## 현황

* On-premise IT/OT 환경에서의 사이버보안 프레임워크 구축 및 운영 중임

## 추진 범위

* 추진 범위의 각 항목은 별도 표시가 없는 한 IT, OT 모두 수행 대상으로 함

1. **사업관리 (공통)**

| **번호** | **구분** | **주요 활동** |
| --- | --- | --- |
| 1 | 사업 관리 | * 일정/품질/이슈 관리 등 * 최소 총괄 PM (Project Manager) 1명과 PL(Project Leader) 2명으로 프로젝트 관리 인원을 구성할 것   \* 해당 과제 수행을 위해 투입되는 인력은 클라우드 보안 관련 5년 이상의 구축/컨설팅 경력 보유 인력으로 제안 필요   * PL은 Cloud Security Framework 구축 또는 Data Mobile 보안 강화 업무 중 하나만을 수행하며 겸업해서는 안됨 * Global 인력이 참여하는 경우, 커뮤니케이션 방안 |

1. **Cloud Security Framework 구축**

| **번호** | **구분** | **주요 활동** |
| --- | --- | --- |
| 1 | 클라우드 보안 프레임워크 수립 | * 클라우드 환경에서의 안전한 보안 체계 구축을 위해, 클라우드 관련 주요 보안 도메인을 기준으로 표준 보안 프레임워크 수립 (NIST CSF 기반 + Cloud 특성) * 클라우드 환경에서 고려해야 할 주요 사이버 보안 영역 선정하여 수립   + 계정 및 권한 관리, 접근통제   + 클라우드 데이터 보안   + 애플리케이션 및 서비스형 플랫폼(PaaS) 보안   + 클라우드 위협탐지 및 대응(보안관제 및 취약점관리 등)   + 클라우드 복원력(BCP & DR, 백업 등)   + 네트워크 및 인프라 보안   기타 필요한 영역 |
| 2 | 클라우드 기술적 보안 아키텍처 수립 | * NIST CSF 프레임워크의 Function 기준으로 표준 보안 아키텍처를 구성   + Function 별 주요 보안통제   (IDENTIFY) 자산 관리, 보안 위험 식별 등의 통제  (PROTECT) 접근 통제, 인식 및 교육, 데이터 보안 등의 통제  (DETECTION) 이상행위 탐지 및 보안 모니터링 관련 통제  (RESPOND) 침해 분석 및 대응 관련 통제  (RECOVER) 복구 및 개선 관련 통제   * + Asset별 주요 보안통제   Device (Server, PC, Mobile, etc.)  Networks  Applications  Data  Users  Compliance  쿠버네티스, 컨테이너 등 클라우드 특성 반영 자산   * + Native Security Tool & Service 도입 상세 설계 * Foundational Controls (필수) 검토 및 도입 (e.g. IAM, 네트워크 접근통제(방화벽정책), 저장 및 전송 시 암호화, 보안 로그 수집 등 * Basic Controls (추가적) 검토 및 도입 (e.g. WAF, 취약점 진단, Detection & Response 도구 등) * Risk-based Controls (위험평가기반) 검토 및 도입   (e.g. Firewall manager 등)   * + Advanced Security Tool & Service 도입 상세 설계   (e.g. CASB, CSPM, CWPP) |
| 3 | 클라우드 서비스 모델별 보안 요건 도출 | * 도출된 요건을 기반으로 클라우드 프레임워크 기반으로 클라우드 보안지침 개정 (RACI 포함)   + IaaS 도입/운영/폐기시 보안 요건 도출   + PaaS 도입/운영/폐기시 보안 요건 도출   + SaaS 도입/운영/폐기시 보안 요건 도출 * 멀티 클라우드 도입/운영/폐기시 보안 요건 도출 |
| 4 | Cloud Landing Zone 구축 | * 도출된 보안요건을 토대로 한 아키텍처를 기반으로 한 Azure Landing Zone 상세 설계(설정) 및 구축   + 클라우드 운영/관제 방안 도출   + Native 보안솔루션 및 3rd Party 보안솔루션 사용 기준 작성   + 관제 솔루션 구성 및 연동방법   + 관제로그 규모 별 최적 설정 가이드 * 관리자 교육 실행(온/오프라인) 포함   + 교육 자료/교재 작성 |

1. **Data & Mobile 보안 강화**

|  |  |  |
| --- | --- | --- |
| **No.** | **주요 요구사항** | **상세 요구 사항** |
| 1 | 현황 분석 | * **전사 데이터 현황 분석**   + 부서별 데이터 처리 흐름 및 요구사항 확인 * 설문조사, 인터뷰 병행 * 연구개발, 프로젝트 조직 데이터 현황 분석 필수 * 지역본부/지사/출장소, 저유소(배차센터)/파견소, 직영주유소, 데이터센터, 고객센터, 해외지사 포함 당사 전 사업장 및 위탁업무 사업장 대상 (단, 필요 시 원격 업무수행)   + 상주/비상주 외주인력 데이터 처리현황 포함 * **데이터 인벤토리 및 데이터 흐름도 개발** * **AS-IS 보안시스템 데이터 통제 현황 분석** |
| 2 | 데이터 거버넌스 구축 | * **Critical/Sensitive 데이터 분류 기준 수립**   + 데이터 분류 및 처리 가이드라인 수립 * **데이터 및 단말기 보안에 관힌 내부 정책/지침 개정**   + 상주/비상주 외주인력 환경 포함 * **동종업계 데이터 처리현황 벤치마킹 및 모범사례 분석** |
| 3 | 데이터 및 모바일 보안 프레임워크 설계 | * **On-premise 및 M365 도입(Hybrid) 업무환경을 고려한 데이터 & 모바일 보안 프레임워크 설계** * **데이터 및 모바일 보안 프레임워크 내에서 세부 보안 정책 수립**   + On-premise 환경 데이터 통제 강화방안 수립   + 테넌트 보안통제 정책 (Tenant security control policies)   + 주요 M365 서비스 (Exchange, SharePoint, OneDrive, Teams)에 대한 보안 정책   + 데이터 분류 기준에 따른 보안 정책 (암호화 및 데이터 내보내기 제어 포함)   + 모바일 장치 내의 데이터보안을 위한 모바일 보안 정책   + 보안 Framework 설계 결과 이행을 위한 M365 필요 보안 라이선스 및 3rd party 보안솔루션 검토   + 유출 관점에서 M365 Weak Point 및 주요 사용 시나리오별 유출 통제 방안 도출   + 외주 인력에 대한 M365 서비스 사용 범위 및 보안정책 수립 * **수립된 보안 정책 이행**   + 상위 보안정책 기반 M365 보안기능 이행 (MS Intune 사용자 배포 포함)   + 운영이관을 위한 운영 매뉴얼 문서화   + 운영업체 선정을 위한 요건 정의 및 평가항목, 운영 품질평가방법(SLA) 문서화   + 운영업체 선정 후 운영자 교육 실시 * **데이터 및 모바일 보안 모니터링 체계 수립**   + M365 및 On-premise 통합 업무환경에 대한 사용자 데이터보안 모니터링 체계 수립   + Remote Work를 위한 모바일기기의 업무 활용에 따른 데이터 유출 경로를 적극적으로 모니터링   + 효과적인 보안 모니터링 활동을 위해 기 구축 보안시스템 활용, 자동화 구현 방법 모색 |
| 4 | 데이터 보안을 위한 변경 관리 계획 수립 | * **데이터 및 모바일 보안 프레임워크 정책 이행을 위한 계획 수립**   + 보안 정책/지침 수립, 공표 및 구현 계획   + 계획에 따른 사용자 가이드 개발(사용 지침 공지 등)   + 운영/업데이트 공지에 대한 세부설정(예: 이메일 알림) * **부서별 자율 데이터보안 업무 프로세스 및 매뉴얼 작성**   + 프로젝트 후 각 부서별 자율적으로 데이터보안 업무수행이 가능하도록 업무프로세스 수립 및 매뉴얼 작성 |

※ 수행내역은 기술협상 및 프로젝트 진행과정에서 일부 변경(추가/수정/삭제)될 수 있음

※ 업무 범위 설정 시, 반드시 전 영역에서 On-premise 및 Cloud(M365)의 Hybrid 환경을 고려해야 함

## 프로젝트 산출물

| **번호** | **구분** | **주요 산출물** |
| --- | --- | --- |
| 1 | 사업 관리 | * 착수/중간/종료보고서 * 이슈보고서 (이슈 발생 시) * 일정계획서(WBS), 작업명세서(SOW) * 주간보고서/회의록 |
| 2.1.1 | 클라우드 보안 프레임워크 수립 | * 클라우드 보안 프레임워크 문서 (보안 영역별 컴플라이언스 점검 체크리스트) |
| 2.1.2 | 클라우드 보안 아키텍처 수립 | * 클라우드 보안 아키텍처 * 클라우드 보안 NIST CSF도메인별 필요 보안 서비스 * 클라우드 Asset 유형별 필요 보안 서비스 * 클라우드 보안 Advanced Security Controls 도입 검토서 |
| 2.1.3 | 클라우드 서비스 모델별 보안요건 도출 | * 클라우드 보안 지침 (국문/영문) |
| 2.1.4 | Landing Zone 구축 | * Azure Landing Zone 구성 완료 보고서 * Azure Landing Zone 서비스에 대한 상세 설정 및 운영 매뉴얼 * Azure Landing Zone 테넌트 내 인프라 구성도 및 클라우드 보안 흐름도 |
| 2.1.5 | 기타 클라우드 보안 산출물 | * 기존 On-Premise 운영 시스템을 클라우드 연동 시 보안 가이드   + 시스템 종류 별 마이그레이션 가이드 (개인정보시스템, 중요정보 보유 등) * 클라우드 서비스와 On-Premise API 연동 시 보안 가이드 * 클라우드용 주요 신기술 적용 보안가이드 (현시점 공개 기준)   + Azure w/Copilot, Sentinel w/Copliot, CNAPP 등 * 클라우드 보안 Awareness을 위한 교육장표 * 클라우드 보안 비용산정 모델 * 클라우드 포털 보안 권한 부여 가이드 |
| 2.2.1 | 현황 분석 | * 요구사항 분석 보고서 * 데이터 처리현황 분석 방안 및 계획서 (설문조사, 인터뷰 일정 포함) * 전사 데이터 처리 현황표 (부서별 인벤토리, 데이터 흐름도) * 연구개발, 프로젝트 조직 데이터 처리 현황 분석 보고서 * 상주/비상주 외주인력 데이터 처리현황표 |
| 2.2.2 | 데이터 거버넌스 구축 | * Critical/Sensitive 데이터 분류 기준 검토 결과보고서 * 현 내규/지침 등 개정방안 검토보고서 및 내규/지침 개정본 * 연구개발, 프로젝트 조직 데이터 처리현황 분석 및 개선방안 검토 결과보고서 * 동종업계 데이터 처리현황 벤치마킹 보고서 / 모범사례 분석검토보고서 * 데이터 중요도 평가기준 검토결과보고서 * 데이터 종류별 보존연한 검토 결과보고서 * 현 국내외 영업비밀/산업기술 컴플라이언스 현황 및 당사 현황 조사결과 보고서 |
| 2.2.3 | 데이터 및 모바일 보안 프레임워크 설계 | * 데이터보안 프레임워크 수립 결과보고서 * 테넌트 보안통제 정책서 * 주요 M365 보안서비스 정책서 * 모바일 보안 프레임워크 설계 결과보고서 및 이행계획서 * M365 필요 보안 라이선스 및 3rd party 보안솔루션 검토보고서 * M365 Weak Point 및 주요 사용 시나리오 별 유출 통제 방안 검토보고서 * 외주 인력 M365 서비스 사용 범위 및 보안정책 검토보고서 * M365 요구사항 분석서, 구현설계서, 보안솔루션 구성도, 솔루션별 설정정책서, 운영자매뉴얼 등 구축 및 운영이관을 위한 제반 문서 (MS Intune 포함) * 운영업체 선정을 위한 요건정의서(RFP), 업체선정 평가표 * 운영 품질 평가서(SLA) 및 계약 문구 * M365 및 On-premise 통합 업무환경에 대한 사용자 데이터보안 모니터링 방안 보고서 / 모니터링 자동화 방안 검토보고서 (SIEM/SOAR 연계 포함) |
| 2.2.4 | 데이터 및 모바일보안  변화관리 계획 수립 | * 데이터 및 모바일 보안 정책 이행을 위한 계획서 * 사용자 가이드 (사용 지침 공지, 매뉴얼, 운영/업데이트 공지) * 부서별 자율 데이터보안 업무 프로세스 정의서 및 사용자 매뉴얼 |
| 3 | 임원 보안 교육 | * 임원 대상 사이버보안 교육 프로그램 정의서 * 임원 대상 사이버보안 교육 자료/교재 (영문) |
| 4 | 임원보고서 | * 경영층 보고서 (영문) * 중간/종료 보고서 요약본 (영문) |

※ 산출물은 기술협상 및 프로젝트 진행과정에서 일부 변경(추가/수정/삭제)될 수 있음

※ 제출되는 산출물은 필요 시, 국, 영문으로 각각 제출하여야 하며, 산출물 중 (영문) 표기된 경우 국, 영문으로 작성 필요

※ 모든 방안, 결과보고서, 정책서 등에는 해당 결론에 대한 논리적 판단 근거의 적합성 확인을 위한 제반 문서가 같이 제출되어야 함

## 예상 구축 일정

1. 프로젝트 기간 : 2024년 5월 ~ 2024년 10월

# 제안서 작성 내용

* 제안서에는 아래와 같은 내용이 포함되어 있어야 함.

## 프로젝트의 이해

1. 프로젝트의 목적 및 범위
2. 프로젝트의 핵심 Issue에 대한 분석
3. 제안의 특장점
4. 추진 전략
5. 기대 효과

## 프로젝트 수행 방안

1. 수행 방법론
2. 단계별 추진 전략 및 세부 수행 방안

**(II-2 추진 범위, II-3 프로젝트 산출물 참조하여 작성)**

* 1. 컨설팅 각 방법론에 따른 구체적인 수행 내역과 단계별 산출물 정리
  2. Data & Mobile 보안 강화 방안
  3. Cloud Security Framework 구축 방안

## 프로젝트 관리 및 지원방안

1. 프로젝트 추진 일정
2. 예상 구축 일정을 참고하여 인력, 위험 및 이슈 등을 포함한 상세 일정 제시
3. 수행 조직 및 인력
4. 프로젝트 인력 투입 계획 및 이력 사항
   1. 상세 추진일정에 따른 WBS를 세분화하여 Task 별 투입인력 기술
   2. 투입인력의 상세 이력사항 제시 (첨부 7 참조)
5. 프로젝트 관리 방안
   1. 품질보증을 위한 관리, 절차, 점검 방법에 대해 구체적으로 기술
6. 보안관리 방안
   1. 투입인력 보안관리 방안에 대한 구체적 제시
   2. 프로젝트와 관련하여 입수 및 생성한 정보유출 방지 방안에 대해 상세히 기술
7. 보안시스템 설계, 구축, 운영 방안 및 업체선정 방안
   1. 설계, 구축, 운영업체 선정, 운영 이관, 운영자 교육, 안정화 등 보안시스템 설계 단계부터 운영 안정화 단계까지의 제반 방안 제시
8. 사용자 교육 방안
   1. 보안시스템 운영을 고려한 임직원 변화관리 및 사용자 교육 실시에 대한 구체적인 방안 제시
9. 기술이전 방안

## 구축비용

1. 세부 공수 및 금액 제시 (업무/모듈별 기술 등급 및 M/M)  
   (기술제안서: 금액 제외, 가격제안서: 금액 포함)

## 기타 제안 (추가)

1. Cloud & Data Security Framework 구축 및 주요 업무 기능의 항목별 수행여부 제시 (Yes/No)
2. 제안요청서의 요구사항 외의 제안사 추가 제안 사항
3. 역량 강화, 선진화를 위한 교육 지원 방안 등

## 제안사 소개

1. 연혁 및 일반: 제안사 회사 연혁 및 주요 현황
2. 재무현황
3. 조직 및 인력: 회사 내 수행 조직 및 인력 구성
4. 동종업체/유사업체에 대한 컨설팅 수행 사례 (본 사업과 유사한 사례)

# 제안 안내

## 일반사항

* 제안사는 제안사의 책임으로 본 프로젝트를 이행하여야 하며, 하도급을 불허함

단, 컨소시엄 구성은 허용함.

* 제안사는 본 제안에 참여한 입찰 경쟁사와 컨소시엄 구성 또는 인력 소싱을 할 수 없으며, 만약 이를 위반할 경우 당사 구매규정에 의하여 최대 3년간 입찰 참여 제한을 받을 수 있음
* 제안사는 컨소시엄을 통해 입찰에 참여할 경우 공동이행만 가능하며, 프로젝트 관련 모든 책임은 주 사업자에게 있음.
* 제안사는 프로젝트 계약 시 프로젝트 참여 인력 전원에 대한 재직확인서를 제출하여야 하며, 제안 사실과 다를 경우 계약 취소 및 일정지연에 따른 손해 배상 청구 등의 불이익이 받을 수 있음
* 기술적으로 가장 합리적이고 비용 대비 기대효과가 가장 클 것으로 판단되는 제안사를 선정함
* 제안발표는 반드시 PM이 진행하여야 하며, 총괄 PM, 수행 PM 등의 구분을 허용하지 않음
* 사업 수행 PM, PL은 프로젝트 전 기간 동안 100% 상주하고 있어야 함
* 본 제안과 관련하여 제출한 서류의 내용이 사실과 다를 경우, 감점 등의 불이익이 주어질 수 있으며, 참가업체는 소명자료 제출 이외의 방법으로 이의를 제기할 수 없음
* 계약 후 밝혀진 위반사항에 대해서는 입찰자는 계약서에 명시된 손해배상 기준에 따라 S-OIL에게 배상하여야 함
* 평가를 통하여 우선 협상 대상자에 선정된 업체는 S-OIL의 요구에 따라 세부업무범위 및 일정 협의를 거칠 수 있으며, 이때 입찰자는 S-OIL의 요구사항을 충족시킬 수 있도록 성실히 노력하여야 함
* 우선 협상 대상자가 S-OIL의 요건을 수용할 수 없을 경우, 차순위 업체와 협의를 진행할 수 있으며 필요에 따라 업체선정과정을 재 시작할 수 있음
* 본 제안요청서의 각종 어휘 및 문구에 대한 해석은 당사가 해석하는 바에 의하며 제안요청서에 대한 이견이 있을 경우에는 제안서 접수이전, 문서 또는 유선의 방법에 의해 확인하되 향후 책임규명을 위해 필요한 경우에는 반드시 문서에 의한 방법으로 문의하여야 함
* 당사는 제안서 평가 및 제안업체 선정 등 관련 제반 업무에 관한 내용을 제안업체에게 통보할 의무를 지지 않음
* 접수된 제안서는 일체 반환을 요구할 수 없으며 제안서 작성과 관련된 제비용은 제안사가 부담함
* 구축 과정 중 취득한 정보는 구축 수행 및 구축 완료 후에도 일체 외부에 유출할 수 없으며, 유출되었을 경우 이로 인해 발생되는 모든 책임을 짐
* 구축 비용은 중도금 50%(중간보고 후), 잔금 50%(검수완료 후)를 해당 지급사유 발생 후 1개월 내 현금 지급
* 본 조항 위반시 위약배상금 및 민, 형사상 책임은 향후 계약서에 명시된 대로 이행
* 본 제안요청서에 언급되지 않은 경미한 사항이라도 본 계약에 의한 “Cloud & Data Security Framework 구축”에 필요하다고 발주자가 인정하는 사항은 수급자의 용역 범위에 포함
* 수급자는 견적서 제출 후 견적 착오 및 현장 작업조건 상이 등의 사유로 계약금액의 증액을 요구할 수 없음
* 평가를 통하여 우선 협상 대상자에 선정된 업체는 계약이행보증보험(10%) 제출 (단 발주자의 내부 규정상 면제 조건에 부합될 경우 면제 가능)

## 제안서의 효력

* 제출된 제안서 및 제안요약서의 모든 내용은 사실에 근거하여야 하며 계약서와 동일한 효력을 가지나 계약서에 명시된 사항의 경우에는 계약서의 사항이 우선함
* 당사는 본 제안과 관련하여 필요하다고 판단되는 경우 추가 제안 또는 추가 자료를 요청할 수 있으며 이에 따라 제출된 자료는 제안서와 동일한 효력을 가짐

## 제안서 작성지침

* 본 제안요청서에 포함된 모든 정보는 비밀이 유지되어야 하며 당사의 허가 없이 그 일부 또는 전부가 유출되어서는 안됨
* 제안서는 파워포인트로 작성함을 원칙으로 함
* 제안서는 A4크기 횡 방향으로 작성하며 제안서 목차 순에 의하여 작성
* 제안서의 내용은 명확한 용어를 사용하여 표현하며 제안 내용 중 [~이 가능하다] [~을 고려한다] [~을 제공할 수도 있다] 등과 같은 애매모호한 표현은 제안서 평가 시 불가능한 것으로 평가함
* 제안 시 제안내용의 근거자료 및 참고자료 등을 첨부하여 제출하여야 함
* 제출된 제안 자료가 부족하거나 확인 등을 위하여 추가 자료가 필요하다고 판단되는 경우 제안사는 당사가 지정하는 일시까지 해당자료를 제출하여야 하며 당사의 별도 요청 및 승낙이 없는 한 일체의 수정, 추가 및 대체할 수 없음

## 제안서 제출

1. **제안서 접수 마감: 2024년 4월 XX일 오전 10시 (온라인 제출)**
2. **제출서류**
   * + 제안서 전체원본 1부 (첨부서류 일체포함)
     + 제안서 및 요약본, 제안발표본 USB 1본
     + 기타 증빙 서류(필요 시)
3. **제출방법** 
   * + 제출서류 및 구비서류 등 기술견적서는 CISO팀으로 제출
     + 프로젝트 견적서는 당사 전자구매 시스템(https://epro.s-oil.com) 으로 제출
4. **제안발표: 2024년 5월 XX일 오후 (발표 순서는 추후 통보)**
5. **문의처**
   * + 에쓰-오일㈜ CISO팀: 김후언 책임매니저 (02-3772-5277, hekim@s-oil.com)
     + 에쓰-오일㈜ CISO팀: 변강욱 책임매니저 (02-3772-5155,james.byeon@s-oil.com)

# 보안 요구사항

## 사이버보안 관리

1. 수급자는 사이버보안과 관련하여 다음 사항을 확인하고 제출하여야 함
2. 인력, 문서, 시스템 등에 관한 보안관리계획
3. 보안 서약서 작성 및 법적 책임에 관한 사항

* 수급자는 계약 업무 착수 전 발주자가 제공하는 **제3자 보안준수 약정서**를 작성 후 발주자에게 제출해야 함
* 수급자는 참여인력의 프로젝트 투입 시 **제3자 정보보호 서약서**를 작성 후 발주자에게 제출해야 함
* 수급자는 계약 종료 시 발주자가 제공하는 **제3자 보안점검 확인서**에 따라 보안점검을 수검하여야 하며, **보안 확약서(참여 인력용)**을 작성하여 제출해야 함

1. 보안 교육실시 및 보고에 관한 사항

* 수급자는 계약 업무 착수 전 발주자의 사이버 보안 인식제고 지침에 따라 사이버 보안 기본 교육을 받고 교육 확인서를 제출해야 함
* 수급자는 사업 투입 전 투입 인력이 수행 업무와 관련한 사이버보안 교육을 수강하였다는 증빙자료를 제출하여 위 사항을 갈음할 수 있음

1. 기밀유지 의무 및 위반 시 불이익에 관한 사항

* 수급자는 본 계약 및 계약내용의 이행과 관련하여 발주자로부터 취득한 비밀 (개인정보 포함 등)을 계약기간과 상관없이 제공자의 사전 서면동의 없이는 절대 제3자에게 제공하거나 누설되도록 하여서는 아니 된다.
* 발주자는 기밀을 유지하도록 수급자의 직원 등에 대하여 감독할 의무가 있으며 수급자는 직원 등의 비밀 누설로 인하여 제공자에게 손해가 발생한 경우 그 손해를 즉시 배상하여야 함

1. 수급자가 내부 네트워크 연결 업체 (에쓰-오일의 정보시스템에 접근 가능한 계정을 부여받아 업무를 수행하는 업체)에 해당하는 경우 아래 발주자가 정한 보안 요건 등을 준수한다.
2. 네트워크 연결 제한 및 최소 권한 원칙

* 네트워크 사용자에 대한 권한을 꼭 필요한 수준으로 최소화하고, Vendor사 별 인원 한정 운영
* 수급자는 VPN을 사용하는 경우 VPN 계정에 대한 관리를 책임지고 수행하며 불특정 유지/보수 인력을 지정하고 해당 인력 에게만 계정을 관리하도록 함

1. 사전점검

* 발주자는 필요 시 사전점검을 요청할 수 있고 수급자는 이를 응해야 함 단, 제3자가 ISMS-P, ISO 27001등 정보보호 관리체계 관련 인증을 획득한 경우 발주자와 협의하여 사전 점검을 수행하지 않을 수 있음

1. 수급자가 내부 네트워크 연결 업체 또는 서비스 아웃소싱 업체에 해당하는 경우 **업무 연속성 계획**을 제출하여야 하며 아래의 내용을 포함하여야 함
2. 서비스 제공 인력의 변경 제한
3. 서비스 제공 인력의 백업 계획
4. 유사시 서비스 수준 협약
5. 수급자는 발주자가 제공하는 **제3자 정보보호 서약서** 및 **사이버보안 교육**을 받은 이후 본 계약 업무를 수행하기 위한 Site 방문 출입을 발주자가 승인할 수 있음
6. 수급자는 본 계약 업무를 수행하기 위해 필요한 출입권한, 시스템, 네트워크 등의 계정 및 권한은 본 계약 기간 내 사용으로 한정함 (추가 사용 기간을 늘리고자 할 경우, 발주자의 승인을 득해야 함)
7. 수급자는 본 계약 업무 착수 전 업무 수행 공간을 발주자와 협의하고 지정된 장소에서 업무를 수행하도록 함 다만, 업무 수행 공간은 잠금 장치 등으로 출입통제가 가능한 공간으로 제한함
8. 수급자는 본 계약 업무를 수행하는 장소가 수급자의 내부이거나 외부 별도 공간 등 회사 외부를 사용하는 경우, 해당 공간에 대해 발주자의 사전 보안 점검을 받을 수 있음 다만, 수급자 내부에서 업무를 수행하는 경우, 보안 정책 확인을 통해 사전 보안 점검을 대신할 수 있음
9. 수급자는 발주자가 제공하는 “제3자 보안 통제 요건”을 준수해야 하며 발주자가 산정하는 위험도 등급에 따라 계약 이후 30일 내 수급자의 보안 점검을 발주자로부터 받을 수 있음 발주자는 위험도 등급에 따라 수급자에 대한 현장 점검을 실시할 수 있으며 수급자는 이에 응해야 함
10. 수급자는 발주자가 요청하는 보안 점검 결과 조치 필요 사항에 대해 조치계획서를 발주자의요청일로부터 30일 이내에 제출해야 하고 이행 조치가 완료될 수 있도록 함
11. 수급자는 필요시 발주사가 제공하는 “제3자 보안 통제 요건”을 요청할 수 있음
12. 수급자는 발주사에서 제공하는 계정/OS접근통제 관련 보안기준을 준수해야 함 수급자는 필요시 발주사에서 제공하는 보안기준을 요청할 수 있음
13. 수급자는 계약 종료 시 계약 업무 수행을 위해 발주자가 발급한 모든 계정 정보를 삭제해야 하며, 추가로 계정이 필요한 경우 계약 이후 명확한 근거를 제출해야한다.
14. 수급자는 계약 종료 후 사용한 업무용 단발기의 반출 시 용역 기간 중 저장된 회사 업무 자료나 각종 산출물을 완전 삭제해야 함
15. 수급자는 본 계약의 용역 업무 수행을 위하여 수급자가 발주자의 사업장으로 반입하는 일체의 전산 장비의 내역을 사전에 발주자에게 통보하여야 하며, 수급자는 수급자의 전산 장비에 사용되는 소프트웨어에 대한 라이선스를 보유해야 하고 발주자가 라이선스 내역을 요구하는 경우 즉시 발주자에게 이를 제출해야 함

아울러 수급자는 아래와 같은 정보보안 통제를 적용해야 함

1. 필수 보안 소프트웨어의 설치 및 최신버전 업데이트 상태 유지
2. 발주자의 전산장비에 불필요한 서비스 및 프로그램의 제거
3. 발주자는 수급자에게 계약 업무 수행을 위해 제공한 자료 및 각종 산출물 관련 문서를 전량 회수하거나 파쇄할 수 있음
4. 발주자가 침해사고 시도 또는 의심스러운 상황을 식별한 경우 수시 점검을 수행할 수 있으며 수급자는 발주자의 보안점검에 응해야 함

[첨부 01] 제3자 보안 통제 요건

| **영역** | **세부 영역** | **항목번호** | **통제항목** |
| --- | --- | --- | --- |
|
| **IDENTIFY** | **Governance (GV)** | TPC 1 | 제3자는 제3자 기술자산에 대한 사이버 보안 AUP(Acceptable Use Policy)를 수립하고 임직원을 대상으로 주기적으로 전파, 교육한다. |
| **PROTECT** | **Access Control (AC)** | TPC 2 | 제3자의 시스템(서버, 애플리케이션 등 모든 자산) 접속 시 안전한 패스워드 설정 규칙을 적용한다. - 최소 길이 : 8자 이상 - 최근 비밀번호 사용 금지 : 최근 4개 이상  - 최소 변경 주기 : 90일 - 계정 잠금 : 10번 이상 틀릴 시 적용  - 화면보호기 : 활동이 없으면 10분 이내에 자동으로 잠금 |
| TPC 3 | 제3자 시스템의 접근 패스워드 및 인증 코드를 기록, 저장, 공개하지 않는다. ※ 메모 부착, 메일 발송, 구두로 전달 등 |
| TPC 4 | 제3자 시스템에 대해 인터넷을 통한 원격 접속 시 Multi-factor 인증을 적용한다. (OTP 등) |
| TPC 5 | 제3자는 클라우드 서비스 이용 시 Multi-factor 인증을 적용한다. (클라우드 기반 이메일 서비스 포함) |
| TPC 6 | 제3자는 에쓰-오일의 정보 및 업무를 처리하는 인력의 교체 또는 퇴직 시 아래의 조치를 취하고 내역을 에쓰-오일로 통보한다.  - 접근권한 변경(시스템과 데이터 대상)  - 계정 삭제 |
| **Awareness and Training (AT)** | TPC 7 | 제3자는 매년 임직원 대상 보안 교육을 실시한다.   - 인터넷 및 SNS 보안  - 임직원 사이버 보안 준수사항  - 사회공학 및 피싱 이메일 보안  - 계정, 패스워드, 인증수단 공유 금지  - 데이터 보안 |
| TPC 8 | 제3자는 개인 이메일을 사용하여 에쓰-오일 데이터를 공유하고 전송하는 것을 엄격히 금지하는 것을 직원에게 알려야 한다.  - 보안서약서에 반영  - 사이버보안 교육에 포함 등 |
| TPC 9 | 제3자는 에쓰-오일의 정책, 절차 및 표준 등 에쓰-오일과 관련된 모든 유형의 데이터를 외부나 인터넷에 공개하는 행위를 금지한다. |
| **Data Security (DS)** | TPC 10 | 제3자는 기술자산과 시스템을 패스워드로 보호해야한다. |
| TPC 11 | 제3자 기술자산 및 시스템의 OS, 소프트웨어, 애플리케이션 등에 대해 정기적으로 패치해야 한다. |
| TPC 12 | 제3자의 기술 자산은 바이러스 백신 (A●) 소프트웨어로 보호해야 한다.  - 백신 업데이트 : 매일 1회 이상  - 정밀검사 : 2주 1회 이상 |
| TPC 13 | 제3자 메일 서버에서 SPF (Sender Policy Framework) 기술을 구현한다. |
| TPC 14 | 제3자는 에쓰-오일 이메일 도메인에 대해서 SPF (Sender Policy Framework) 기능을 적용한다.  - s-oil.com |
| TPC 15 | 제3자는 DNS 서버에 SPF 레코드를 게시한다. |
| TPC 16 | 제3자는 스팸 차단 기능을 사용하여 인터넷에서 들어오는 모든 이메일을 검사해야 한다. |
| TPC 17 | 제3자는 회사의 이메일 도메인을 사용하여야 한다. Gmail 및 Hotmail과 같은 상용 이메일 도메인 사용은 금지한다. |
| **Information Protection Processes and Procedures (IP)** | TPC 18 | 제3자는 퇴사 직원에 대한 보안 절차를 수립하고 적용해야 한다.   - 회사 자산 반납  - 회사 자산에 대한 모든 접근 제거 등 |
| TPC 19 | 제3자는 에쓰-오일에서 제공받거나 업무를 처리 및 저장하는 과정에서 생성, 수정된 데이터는 계약에 명시된 보존기간이 끝났거나 계약이 종료되는 시점에 해당 데이터를 지체없이 완전 삭제 및 파기하고, 삭제 및 파기가 완료 되었음을 증빙할 수 있어야 한다. |
| **Protective Technology (PT)** | TPC 20 | 제3자는 엔드포인트 디바이스에 방화벽 기능이 있을 경우 기능을 활성화 해야 한다. |
| **RESPOND** | **Communications (CO)** | TPC 21 | 제3자는 사이버 보안 침해사고 인지 시 아래의 내용을 준수한다.  - 침해사고 대응 활동 내역 통보  - 사고 발견 후 24 시간 이내에 통보  - 에쓰-오일 담당자 및 계약부서 통보,  threats@s-oil.com으로 전달 |

# [첨부 02] 제3자 보안 준수 약정서

**제3자 보안 준수 약정서(안)**

|  |  |
| --- | --- |
| **회사명** |  |
| **주 소** |  |
| **연락처** |  |

당사는 에쓰-오일주식회사(이하 “귀사”라 함)의 영업비밀 보호를 위하여 아래 사항 및 ‘제3자 보안 통제 요건’을 준수할 것을 서약합니다.

1. 당사는 귀사에서 업무를 수행함에 있어 알게 된 영업비밀 기타 모든 회사 경영에 관련된 정보를 제3자에게 제공하거나, 공개 또는 누설하지 않을 것이며, 귀사의 사전 동의 없이 무단 사용하지 않겠습니다.
2. 당사는 귀사로부터 업무수행을 위하여 명시적으로 접근을 허가 받은 시설, 자산 및 정보만을 이용하고, 귀사로부터 부여받은 계정을 해당 용도와 목적으로만 사용하겠습니다.
3. 당사는 귀사가 업무를 위하여 제공한 인터넷, E-mail, fax, 전화 등에 대해서는 영업비밀보호를 위하여 귀사가 일정한 통제나 제한을 할 수 있다는 사실과 전자우편⬝메신저 메시지⬝인터넷 사이트 전자 게시 문서 등 당사가 귀사 네트워크를 통하여 송⬝수신하는 모든 전기통신의 내용을 귀사가 영업비밀 보호 목적으로 실시간 모니터링 또는 사후 검색할 수 있음에 동의하며 해당 내용이 추후 당사에게 불리한 증거로 사용되더라도 이의를 제기하지 않겠습니다.
4. 업무를 위하여 사용하는 사용자 ID, 패스워드 등의 인증 정보를 안전하게 관리하겠습니다.
5. 귀사의 시스템과 수시로 상호작용하거나 업무를 위하여 사용하는 시스템의 보안성과 무결성을 보호할 책임을 갖으며, 귀사가 권고하는 사이버보안 통제와 기술을 적용하겠습니다.
6. 당사는 귀사의 사전 동의 없이는 귀사의 영업비밀을 포함한 기타 경영 정보와 관련된 모든 문서나 자료 및 결과물 등을 어떠한 형태로도 외부로 반출하지 않겠습니다.
7. 당사는 업무가 종결되거나 귀사의 요청이 있는 경우, 귀사가 제공한 모든 자료와 자산을 귀사에 즉시 반납하겠습니다.
8. 당사는 업무수행의 결과 산출된 모든 결과물(보고서, 도면, 시스템, 컴퓨터 프로그램, 장치, 모델 등)에 대한 지식재산권 및 제반 권리가 귀사에 귀속됨을 인정하고, 귀사가 이에 대한 권리를 행사하는데 협조하겠습니다.
9. 당사는 사이버보안 사고를 발견 시 또는 귀사의 자산이나 귀사의 자산과 상호작용하는 당사의 시스템에 의심스러운 행위 발견 시 즉각적으로 귀사에게 통보하고, 사이버보안 사고는 귀사의 침해사고 대응 관련 지침을 준용하여 처리하겠습니다.
10. 당사는 사이버보안 사고 처리 후 귀사의 자산에 끼친 영 향도와 시정조치와 관련된 사항을 표기한 사이버보안 사고 처리 결과 보고서를 귀사 담당자에 제출하겠습니다.
11. 당사는 준거성 검토를 연 1회 실시하여 검토 결과와 증빙을 귀사에 제출하겠습니다.
12. 당사는 귀사로부터 최대 연 1회 정기 사이버보안 점검을 받거나 아래와 같은 상황 발생 시 추가 사이버보안 점검을 받을 수 있음에 동의합니다.  
    가) 의심스러운 활동 발견  
    나) 당사 자산에 대한 사이버보안 사고 발생  
    다) 귀사 자산에 대한 사이버보안 사고 발생
13. 개인정보 처리업무 수탁사인 경우 관련 법령에 따라 관리감독 및 점검을 받을 수 있음에 동의합니다.
14. 필요 시 귀사가 당사의 접근권한을 회수하거나 연결을 비활성화할 수 있음에 동의하며, 이러한 조치가 발생하여도 당사가 본 서약 및 법령을 준수할 의무가 면제되지는 아니함을 인지합니다.
15. 만일 본 서약 사항을 위반하였을 경우에 당사는 법령이 정한 바에 따라 민·형사상의 모든 책임을 부담하겠으며, 본 서약 위반 행위로 인하여 귀사에 발생한 모든 손해를 배상하겠습니다.

**년 월 일**

**대 표 자 : (인)**

**에쓰-오일 주식회사 귀중**

# [첨부 03] 제3자 정보보호 서약서

**정보보호 서약서**

소 속 : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

성 명 : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

주 소 : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

핸드폰 번호 : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

본인은 [에쓰-오일주식회사 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_] 프로젝트에 참여하거나 에쓰-오일에서 서비스를 수행함에 있어 다음과 같은 사항을 준수하겠으며, 하기 사항 위반 시 민사상 손해배상 책임을 부담하며, 또한 그로 인하여 형사상의 불이익을 당할 수 있음을 양지하고 있습니다.

보안 일반

1. 모든 프로젝트 수행 장소에는 잠금 장치가 되어 있어야 하며, 모든 사람이 자리를 비울 시에는 반드시 출입문을 잠그고, 개인 서랍이 있는 경우 퇴근 시 반드시 잠근다. 모든 프로젝트 인력은 에쓰-오일이 보안 교육을 수행할 경우 필수적으로 해당 교육을 이수하고 에쓰-오일의 요구가 있을 경우 교육 이수 확인서 및 서약서를 제출하여야 함
2. 컴퓨터가 바이러스에 감염되지 않도록 최신 AntiVirus Program을 설치하여 항상 실행하여야 하며, AntiVirus Program의 바이러스 정보 파일은 하루에 한 번 최신 버전으로 갱신되어야 함 인터넷 등 공개된 영역으로부터 자료를 구할 때 바이러스 감염 여부를 항상 확인하고 감염 여부가 의심스러운 파일은 열어보지 않는다.
3. 개인 소유의 컴퓨터를 업무 목적으로 사용하더라도, 계약 중인 기간 동안에는 컴퓨터를 회사의 영업 목적 또는 기타 회사의 경영진이 허가한 목적을 위해서만 사용하도록 함 컴퓨터에는 적법한 라이선스가 없거나 허가되지 않는 소프트웨어가 설치되어 있지 않아야 함 P2P 자료공유용 소프트웨어(예: uTorrent, BitTorrent 등), 비업무용/Private VPN 및 Private Browser(예: Epic, Tor, Dooble, Brave, Cocoon, Comodo Dragon, Yandex Browser, SRWare Iron, Aviator 등)를 설치하여 사용하지 않는다.
4. 체인메일 및 스팸 메일을 발송하거나 이송(Forward)하지 않고, 부적절한 내용의 정보에 접근하거나 이를 배포하지 않는다. 다른 사람에게 부적절하거나 공격적이거나 무례하게 받아들여질 수 있는 어떠한 내용이라도 접근하거나 배포하지 않는다.
5. 보안 사고가 발생하였거나 의심스런 사건이 인지되는 경우 관리자 또는 보안담당자에게 즉시 보고해야 함 시스템 조사를 직접 하거나 증거 인멸 등의 시도를 해서는 안 되며, 사고를 유발한 것으로 의심되는 개인 또는 조직에게 연락해서도 안 된다.
6. 에쓰-오일의 보안 지침 혹은 이에 준하는 지침에 따라야 하며 만약 출입통제장치나, 보안 소프트웨어 설치 등 에쓰-오일이 요구하는 별도의 보안 준수사항이 있는 경우 양사의 협의를 거쳐 시행한다.
7. 에쓰-오일의 장비 또는 소프트웨어를 포함한 모든 자산을 허가없이 습득 또는 반출해서는 안된다.
8. 에쓰-오일이 아닌 다른 장소에서 근무 시에도 에쓰-오일의 보안 규정을 따라야 함

자료 보안

1. 전산망 구성도, IP 현황, 개인정보 및 기타 비공개 자료를 에쓰-오일의 승인 없이 접근하거나 사용할 수 없다.
2. 프로젝트 수행 과정에서 발생하는 모든 자료 및 산출물은 에쓰-오일의 파일서버 또는 지정한 PC 이외에 저장, 관리하여서는 안 된다.
3. 프로젝트 관련 자료는 인터넷, 웹하드, 인터넷 자료공유사이트 및 개인 메일함에 저장할 수 없으며, 에쓰-오일의 사전 승인없이 전자우편을 이용하여 외부로 자료를 전송해서는 안 된다.
4. 업무 중 제공된 기밀정보 및 비공개자료는 퇴근 시 반납토록 하여야 하며, 잠금 장치가 있는 보관함에 보관해야 함
5. 에쓰-오일의 메일 계정 사용 시 프로젝트/유지보수업무 수행과 관련된 목적으로만 사용하고, 개인적인 자료 송수신 또는 기타 다른 목적으로 사용하지 않는다.
6. 에쓰-오일 자료의 제공 및 수령은 에쓰-오일과 합의된 보안 절차에 따른다.
7. 에쓰-오일 정보 혹은 기밀정보는 need to know base로 공유하며, 반드시 업무상 필요한 사람에게만 제공한다.
8. 에쓰-오일이 제공한 정보는 업무 목적을 달성한 후 즉시 파기하여 PC에 정보가 남아있지 않도록 관리한다.
9. 에쓰-오일의 정보를 노트북 외 불가피하게 USB, 외장하드 등에 저장하는 경우는 안전한 알고리즘으로 암호화하여 보관한다.
10. 저장매체를 이용한 데이터 이동 시 사전에 에쓰-오일의 승인을 받도록 하며, 사후 반납 혹은 삭제를 확인한다.
11. 개인정보, 영업비밀, 계정/비밀번호 등 기밀정보는 PC 내에 평문으로 보관하지 않는다.

시스템 운영 및 유지보수 보안

1. 시스템 접근 필요 시, “최소한의 권한”만을 부여받고 “개인 계정”을 사용해야 하며, 업무 사용이 종료되면 즉시 계정을 반납한다.
2. 개인의 ID/패스워드는 공유하지 않는다.
3. 시스템 변경 작업 시에는 사전에 에쓰-오일의 승인을 득하고, 작업 완료 즉시 통보한다.
4. 원격 콘솔 접속 계정/인력/장비는 사전에 에쓰-오일의 승인을 득한다.
5. 안전한 응용시스템 관리 및 개발 유지보수업무 수행을 위하여 에쓰-오일의 응용시스템 정보보호 관련 지침 등을 준수한다.

사무실, 장비 보안

1. 프로젝트와 관련한 작업의 수행은 에쓰-오일이 지정한 장소에서 이루어져야 하며, 부득이 개인적인 공간 또는 제 3의 장소에서 작업하여야 할 경우에는 잠금 장치 등 적절한 조치를 취한 후 사전에 에쓰-오일의 승인을 얻어야 함
2. 에쓰-오일의 사전 승인 없이 USB 메모리, 카메라 및 기타 휴대용 저장장치 등을 이용하여 프로젝트 관련 자료를 보관할 수 없으며 에쓰-오일 또는 에쓰-오일로부터 위임을 받은 제3자가 노트북, 개인장비 등에 대한 자료 검색을 요청하였을 경우 이에 응하여야 함
3. 개인컴퓨터에는 Power on, 하드디스크, 화면보호기 패스워드를 설정하여야 하며 화면 보호기 암호는 10분으로 설정하여야 함 또한 자리를 비울 시는 화면 보호기를 즉시 실행한다. 암호는 추측하기 어려워야 하고 주기적으로 변경되어야 하며, 이전에 사용된 암호와 동일한 암호를 사용하지 않는다. Cable lock을 이용하여 노트북을 적절하게 보호하여야 함
4. 시스템 안정 및 안전을 확보하기 위한 보안패치를 적용한다.
5. 상주인력은 사전 출입 등록 및 승인 후 출입하며, 비상주 인력은 방문절차에 따라 방문증을 발급 받고 당사 담당 임직원 동행 하에 출입한다.
6. 휴대 및 반입금지 품목 등 출입에 대한 에쓰-오일 보안정책을 준수한다.
7. Clean Desk 실행으로 에쓰-오일의 정보 노출을 방지한다.
8. 근무시간에는 노트북 잠금 장치를 이용하여 보호하고 근무 종료 후에는 사용 중인 노트북을 서랍이나 캐비닛에 넣고 잠근다.
9. 기계실 출입은 업무상 필요한 경우로 국한하고, 업무종료 시 즉각 에쓰-오일에게 통지하고 기계실에서 퇴실한다.

내∙외부망 접근 시 보안

1. 에쓰-오일의 사전 승인을 받지 않은 경우, 업무와 무관할 경우에는 타인의 ID 또는 비밀번호를 도용하는 등의 방법으로 에쓰-오일의 전산망에 접근해서는 안 된다.
2. 에쓰-오일의 사전 승인을 받지 않은 노트북 PC 또는 기타 전산처리장치로 인터넷에 연결하거나 자료를 공유하여서는 아니된다.
3. 에쓰-오일 네트워크 접근 시 에쓰-오일에서 요구하는 보안솔루션을 모두 설치하여 점검을 받은 후 네트워크를 사용한다.
4. 에쓰-오일에서 정보기기의 반입/반출 및 내외부 네트워크 사용을 허용하지 않는 경우 이를 준수한다.
5. 에쓰-오일 보안정책에 위배되지 않는 범위 내에서 네트워크에 접속해야 하며, 에쓰-오일 내외부 네트워크 및 VPN 사용을 위해 사전 승인 등 절차가 필요한 경우 절차를 준수한다.
6. 네트워크 연결 시 개인방화벽을 설치하고 항시 활성화를 유지해야 하며, 접근 요청이 오는 경우 필요 여부를 확인한 후 선별적으로 허용한다.

프로젝트 수행 후 보안

1. 프로젝트 수행 후 기밀 자료는 외부로 유출되지 않도록 하여야 하며, 불필요한 자료는 삭제 또는 세단하여 파기하여야 함 필요 시 에쓰-오일의 요구에 따라 노트북 또는 개인장비를 초기화 한 후 이를 에쓰-오일 보안담당자 또는 업무담당 임직원에게 확인받도록 함
2. 프로젝트 수행 이후에는 에쓰-오일로부터 제공받은 제반 자료, 장비 및 서류 등과 중간∙최종 산출물 등을 즉시 반납하고, 별도로 복사하거나 보관하여서는 안 된다. 이를 확인하기 위하여 에쓰-오일의 요구가 있는 경우 이에 응하여야 함
3. 에쓰-오일의 요구가 있는 경우, 프로젝트 자료 복사본 등 관련 자료를 보관하고 있지 않다는 확인서를 본인 및 소속회사 대표 명의로 제출하도록 함

**작 성 일 : 년 월 일**

**서 약 자 : (인)**

**■ 개인정보의 수집**∙**이용 동의:**

* 수집∙이용 목적 : 프로젝트/서비스 수행 시 에쓰-오일 정보보호서약에 대한 본인여부 확인
* 수집∙이용 하려는 개인정보항목: 소속, 성명, 주소, 핸드폰번호
* 개인정보 보유 및 이용기간: 개인정보의 처리 목적 달성 시까지

※ 위의 개인정보 수집∙이용에 대한 동의를 거부할 권리가 있습니다. 그러나 동의를

거부할 경우, 당사 내부망 접속 및 Mobile Phone 음성통화를 제외한 모든 정보통신

기기 사용에 제한을 받을 수 있습니다.

**☞ 위와 같이 개인정보를 수집∙이용하는데 동의하십니까?**

**□ 동의 □ 동의하지 않음**

20 년 월 일 서약자: (인)

|  |
| --- |
| [첨부 04] 제3자 사이버보안 교육 확인서제3자 사이버보안 교육 확인서 |

**사업명 :**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | **소속 회사명** | | **성명** | | **교육 일시** | **확인(서명)** |
|  |  | |  | |  |  |
|  |  | |  | |  |  |
|  |  | |  | |  |  |
|  |  | |  | |  |  |
|  |  | |  | |  |  |
|  |  | |  | |  |  |
|  |  | |  | |  |  |
|  |  | |  | |  |  |
|  |  | |  | |  |  |
|  |  | |  | |  |  |
|  |  | |  | |  |  |
|  |  | |  | |  |  |
| 교육 담당자 | | (부서) | | (성명) | | |

- 이하 여백 -

# [첨부 05] 제3자 보안점검 확인서

|  |  |  |  |
| --- | --- | --- | --- |
| **사업 명** |  | **수행 기간** | 20 . . ~ 20 . . |
| **소속** |  | **성명/직급** |  |
| **내선** |  | **핸드폰번호** |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **순서** | **점검 항목** | **세부사항** | **확인자** | **서명** |
| 1 | **출입증 회수 확인** |  |  |  |
| 2 | **정보보호 서약서 수취 확인** |  |  |  |
| 3 | **정보보호 교육 이수 확인서 수취 확인** |  |  |  |
| 4 | **부착 보안 스티커 훼손 확인** |  |  |  |
| 5 | **NW 및 시스템 접속 계정 삭제 확인** | NAC 계정 |  |  |
| 서버, DBMS, Application 계정 |  |  |
| OTP |  |  |
| DB 접근통제시스템 계정 |  |  |
| SBC 계정 |  |  |
| VPN 설정 |  |  |
| 6 | **수·발신 자료 회수/파기 확인** |  |  |  |
| 7 | **시스템 보안설정 여부 확인** |  |  |  |
| 8 | **시스템 취약점 제거 확인** |  |  |  |
| 9 | **PC 포맷(완전 삭제)** | 완전 삭제 솔루션 사용 또는 3회 이상 포맷 |  |  |
| **장비 반납 및 반출 승인** | 지원 장비 반납/외부 반입 장비 반출 승인 획득 |  |  |
| 10 | **보안 확약서 제출 확인** | 제3자 대표자 서명 |  |  |

상기 프로젝트 보안 절차를 준수하였음을 확인함

작성일: 년 월 일

Project Manager (S-OIL 소속) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(인/서명)

- 이하 여백 -

# [첨부 06] 보안 확약서(참여인력용)

|  |
| --- |
| **보안 확약서(참여인력용)**  본인은 귀 기관과 계약한 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 사업의 수행을 완료함에 있어, 다음 각호의 보안사항에 대한 준수 책임이 있음을 서약하며 이에 확약서를 제출합니다. 본인은 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 사업수행을 완료함에 있어, 다음 각호의 사항에 대한 보안준수 및 책임이 있음을 서약하며 이에 확약서를 제출합니다.   1. 사업 수행 시 지득한 모든 자료를 반납 및 파기하였음. 2. 지득한 정보에 대한 유출을 절대 금지하겠음. 3. 보안 위규시 관련 법규에 따른 모든 조치와 손해배상을 감수하겠음.   20 년 월 일  서 약 자 (협력업체 임직원)  소 속 :  직 급 :  성 명 : (서명)  생년월일  서약 집행자 (Project Manager (S-OIL 소속))  소 속 :  직 급 :  성 명 : (서명)  **에쓰-오일 주식회사 귀중** |

# [첨부 07] 투입인력 이력 양식

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **성명** |  | | **소속** |  | **직책** |  | **연령** |  |
| **학력** |  | | | | **해당분야근무경력** | |  | |
|  | | | | **자격증** | |  | |
| **본사업 참여임무** | |  | | **사업참여기간** |  | | **참여율** |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **경 력 사 항** | | | | |
| **사업명** | **참 여 기 간**  **(시작연월 ~ 종료연월)** | **담당업무** | **발주처** | **비고** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |