Onsites AI

SECURITY WHITEPAPER · EDITION 2.0

보안 및 데이터 레지던시 백서

데이터가 누구 손에 있는지 분명히 밝힙니다

암호화, 접근 제어, 감사, 백업과 삭제 일정, AI 데이터 경계와 취약점 제보까지 항목별로 당사의 방식과 책임 주체를 명시합니다. 검증할 수 없는 “기업급 보안” 같은 형용사는 쓰지 않습니다.



버전	발행	적용 범위	문서 번호
2.0판	2026년 11월	클라우드·전용 클라우드·셀프호스팅	ONS-SC-KO-2.0

© 2026 Onsites AI · 본 문서는 제품 업데이트에 맞추어 갱신됩니다. 최신 버전은 onsitesai.com/kr/download.html 에서 확인하십시오.

목차

CONTENTS

01 **처리 역할과 데이터 경계** 누가 통제하고 누가 처리하며, AI가 접근할 수 있는 범위 03

02 **암호화, 접근 제어, 감사** 아홉 개 통제 항목의 구체적 방식 04

03 **레지던시, 백업, 수명 주기** 데이터 위치, 보관 기간, 삭제 방식 05

04 **보안 설문과 제보 절차** 자주 묻는 질문, 취약점 제보, 연락처 06

요약

Onsites AI는 고객 데이터를 고객이 위탁한 자산으로 취급합니다. 클라우드와 셀프호스팅 두 경로 모두 암호화, 접근 제어, 감사 로그를 갖추고 있으며, 셀프호스팅을 선택하면 모든 데이터를 고객의 네트워크 안에 둘 수 있습니다. 본 문서는 아홉 개 통제 항목의 방식을 항목별로 설명하고, 어느 부분을 당사가 책임지고 어느 부분을 고객이 책임지는지 명시합니다. 보안 평가에서 가장 어려운 것은 “취약점이 있다”는 사실이 아니라 “경계가 불분명하다”는 점입니다.

9개	TLS 1.3	1 영업일	3 가지 형태
내장 통제 항목 설문 항목에 그대로 대응	전 구간 전송 암호화 저장 데이터도 동일하게 암호화	보안 보고서 확인 기한	클라우드, 전용 클라우드, 셀프호스팅의 각 경계

아홉 개 통제 항목 개요

01 전송 TLS 1.3	**02 저장** 저장 매체 암호화	**03 키** 데이터와 분리 보관
04 권한 시트 단위 부여, 읽기 전용으로 축소 가능	**05 격리** 워크스페이스 간 상호 비가시	**06 공유** 외부 링크에 유효 기간과 횟수 설정
07 감사 수행자, 시각, 상세 내용	**08 백업** 유료 워크스페이스 자동 백업, 내보내기	**09 AI 경계** 현재 워크스페이스만 읽기, 재학습 없음

문서 용도

보안 평가, 공급업체 설문, 컴플라이언스 검토에 사용하며 회신 첨부 자료로 바로 제출할 수 있습니다.

적용 범위

클라우드 SaaS, 상용판 · 전용 클라우드, 셀프호스팅의 세 가지 형태이며 차이가 있는 부분은 별도로 표시했습니다.

고지

본 문서는 제품에 내장된 기능을 설명하며 제3자 인증과 동일하지 않습니다. 법정 보안 인증과 업종별 컴플라이언스 평가는 별도로 위탁해야 합니다.

버전 및 피드백

2.0판, 2026년 11월. 오류 정정과 보안 제보는 support@onsitesai.com 으로 보내 주십시오.

01

ROLES & BOUNDARY

누가 통제하고, 누가 처리하며, AI는 무엇에 접근하는가

보안 평가의 첫 질문은 역할입니다. 데이터는 누구의 것이고, 누가 처리하며, 제3자에게 넘어가는지입니다. Onsites AI는 고객이 컨트롤러, 당사가 처리자이며, 재처리자는 인프라와 모델 두 종류입니다.

1.1 세 가지 역할

데이터 컨트롤러

고객(귀사)

무엇을 수집하고 얼마나 보관하며 누구에게 보여줄지 결정합니다. 시트, 역할, 권한과 내보내기·삭제를 귀사가 직접 정합니다.

데이터 처리자

Onsites AI

귀사 설정대로 저장·검색하고 초안과 문서를 만듭니다. 자체 목적으로 쓰지 않고 워크스페이스 간 재사용도 없습니다.

재처리자

인프라와 모델

클라우드에서는 인프라와 당사가 호출하는 모델 서비스가 해당합니다. 셀프호스팅은 둘 다 고객이 제공하며 당사는 보유하지 않습니다.

1.2 AI 호출 한 건의 네 가지 경계 지점

경계 내부

워크스페이스 데이터

대화, 고객, 문서, 파일. 본 워크스페이스 구성원만 권한에 따라 봅니다.

검색 시

권한 필터링

요청자 시트 권한으로 읽기 범위를 자르며, 권한 없는 기록은 컨텍스트에 넣지 않습니다.

추론 시

모델 호출

이번 요청에 필요한 최소 컨텍스트만 보냅니다. 셀프호스팅은 내부 엔드포인트를 지정해 외부로 나가지 않습니다.

반환 후

답변과 출처

결과에 인용 기록을 표시합니다. 학습 데이터셋에 쓰지 않고 워크스페이스 간 재사용도 없습니다.

그림 1-1 네 가지 경계 지점. 한 단계라도 빠지면 데이터를 모델로 보내서는 안 됩니다. 워크스페이스만 읽고 출처를 요구하는 이유입니다.

1.3 AI 사용의 네 가지 경계

- **현재 워크스페이스만 읽습니다.** Copilot, Harness, Agent Studio, Desk는 세 형태 모두에서 현재 워크스페이스만 읽고 다른 곳은 검색하지 않습니다.
- **답변에는 출처가 붙습니다.** 인용한 대화, 고객 필드, 파일을 표시하며 출처가 없는 내용은 쓰지 않습니다.
- **학습에 사용하지 않습니다.** 고객 데이터는 공유·공개 모델 학습에 쓰지 않습니다. 셀프호스팅의 모델과 키는 고객 제공입니다.
- **전체를 끌 수 있습니다.** AI 기능은 워크스페이스나 구성원 단위로 끌 수 있고, 끈 뒤에도 나머지 기능은 정상 동작합니다.

1.4 세 가지 형태별 역할 차이

구간	클라우드 / 전용 클라우드	셀프호스팅
인프라	당사 운영, 전용 클라우드는 독점 인스턴스	고객 서버와 네트워크
모델과 키	플랫폼 호출, 키는 당사 관리	고객이 엔드포인트와 키 제공, 당사 미보유
데이터 위치	Onsites 인프라, 전용 클라우드는 리전 선택	고객 전산실 또는 프라이빗 클라우드, 완전 오프라인 가능

동일한 소프트웨어와 기능. 역할 차이는 “누가 인프라와 모델을 제공하는가”뿐입니다.

“당사가 볼 수 있는가”에 대하여 클라우드에서는 장애 대응 중 비식별화된 로그에 접촉할 수 있습니다. 대화 본문과 첨부 파일은 운영 대상이 아닙니다.

02 CONTROLS

아홉 개 통제 항목, 항목별 실행 방식

보안 설문은 보통 통제 항목별로 질문합니다. 아래는 “암호화 → 접근 → 기록 → 공유 → AI” 순서의 방식과 책임 주체이며 그대로 대조해 작성할 수 있습니다. 세 형태의 차이는 따로 표시했습니다.

2.1 암호화와 키

구간	방식	책임 주체
전송	전 구간 TLS 1.3, 셀프호스팅은 귀사 게이트웨이 종료·인증서 귀사	클라우드 당사, 셀프호스팅 고객
저장 데이터	당사 인프라 저장 시 암호화, 셀프호스팅은 귀사 스토리지 계층에서 암호화	클라우드 당사, 셀프호스팅 고객
키 관리	키와 데이터 분리 보관, 플랫폼 팀만 접근	클라우드 당사, 셀프호스팅 고객 보유
백업 매체	백업 파일도 암호화, 위치는 배포 형태	3장 참조

2.2 접근 제어

- **시트 단위로 권한을 부여합니다.** 누가 무엇을 보는지는 시트와 역할로 정합니다. 역할은 읽기 전용으로 좁혀 재무·경영진 조회에 쓸 수 있습니다.
- **워크스페이스 격리.** 각 워크스페이스는 상호 격리되어 데이터가 이동하지 않으며, AI 검색도 같습니다.
- **회수는 즉시 적용됩니다.** 시트를 제거하면 접근 권한도 함께 회수되며 별도 조작이 필요하지 않습니다.
- **파일 공유 제어.** 비공개 파일과 폴더를 대상에 맞춰 공유합니다. 외부 링크는 유효 기간과 열람 횟수를 정하고 언제든 폐기할 수 있습니다.

2.3 감사와 추적 가능성

문서와 대화의 상태 변경에는 수행자, 시각, 상세가 모두 기록됩니다. 누가 견적을 보냈고 누가 금액을 바꿨고 누가 계약을 확인했는지 남습니다. 로그는 다른 데이터와 함께 내보낼 수 있어 몇 달 뒤에도 승인 근거가 되며, 일정 기간만 남는 “활동 피드”가 아닙니다. Desk의 동작도 기록됩니다. 무엇을 읽고 쓰고 몇 포인트를 썼는지입니다.

기록 항목	내용	용도
상태 변경	문서와 대화의 상태 전환	승인 흐름 검토, “이 버전은 누가 보냈는가” 확인
권한 변경	시트와 역할의 부여 및 회수	퇴사 인수인계와 감사 증거 확보
AI 실행	읽기 범위, 쓰기 결과, 포인트 소모	에이전트가 경계를 벗어나지 않았는지 확인

2.4 통제 항목이 경로의 어느 구간에 위치하는가

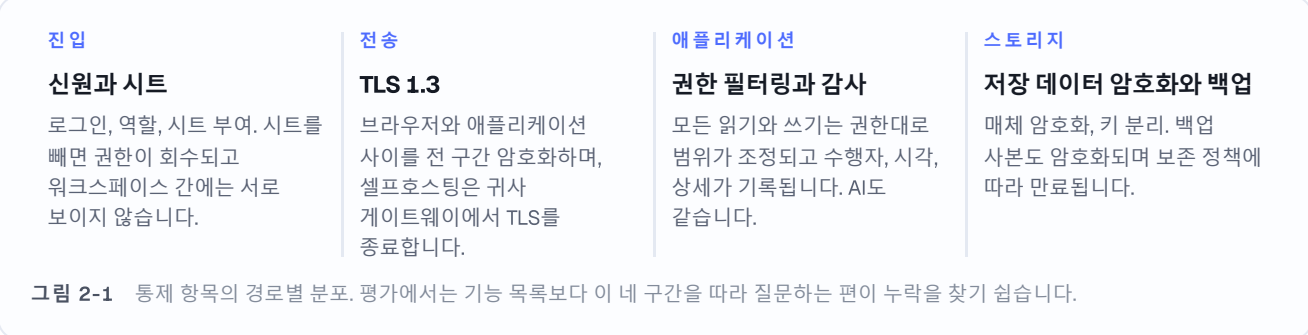


그림 2-1 통제 항목의 경로별 분포. 평가에서는 기능 목록보다 이 네 구간을 따라 질문하는 편이 누락을 찾기 쉽습니다.

검증 방법 평가 단계에서 위 세 항목의 실제 표본(비식별화)을 요청할 수 있습니다. 각 1건이면 충분합니다.

03

RESIDENCY

데이터를 어디에 두고, 얼마나 보관하고, 어떻게 삭제하는가

레지던시는 보통 세 질문으로 나뉩니다. 데이터가 어느 리전에 있는지, 백업을 얼마나 보관하는지, 계약 종료 후 어떻게 삭제하는지입니다. 앞의 둘은 배포 형태로 고르고, 셋째는 내보내기 여부에 달려 있습니다.

3.1 데이터 한 건의 수명 주기



그림 3-1 수명 주기의 네 구간. 미리 합의할 것은 마지막 구간, 즉 삭제 요청자와 백업 보관 기간, 완료 확인 방법입니다.

3.2 세 가지 형태의 레지던시와 백업

형태	데이터 위치	백업	삭제
클라우드 SaaS	Onsites 인프라	유료 워크스페이스 자동	요청 시 실행, 백업은 정책대로 만료
상용판 · 전용 클라우드	인스턴스·리전 선택, 개설 시 고정	자동, 리전은 인스턴스 따름	동일, 리전 불변
셀프호스팅	귀사 전산실 또는 프라이빗	제공 스크립트 실행	귀사 실행, 당사는 절차 제공

리전은 개설 시 고정되며 이후 바뀌지 않습니다. 이전은 신규 인스턴스로 처리합니다.

3.3 내보내기, 요금제 하향, 보존

- **내보내기는 권리이며 기능 스위치가 아닙니다.** 대화, 연락처, 문서를 표준 형식으로 내보낼 수 있고 비용도 받지 않습니다.
- **요금제를 낮춰도 데이터는 삭제되지 않습니다.** 스토리지를 해지해도 기존 데이터는 보존되고 필요할 때 다시 씁니다.
- **무료 버전에는 서버 측 사본이 없습니다.** 무료 워크스페이스는 서버 백업이 없어 정기 내보내기가 유일한 사본입니다.
- **삭제는 확인할 수 있어야 합니다.** 삭제 실행 기록과 백업 만료 시점을 제공해 “삭제했다는데 백업이 남아 있다”는 분쟁을 막습니다.

3.4 보존 정책을 정하는 방법

데이터 분류	권장 보존	사유
대화 및 고객 기록	영업 주기와 동일	사후 지원과 재구매 판단이 대화 이력에 의존합니다.
견적, 계약, 인보이스	세무·회계 요건	대화보다 깁니다. 번호와 금액을 검증할 수 있어야 하고 이전 버전도 보관합니다.
감사 로그	문서보다 김	승인과 분쟁 처리에 “누가 언제 무엇을 바꿨는가”가 필요합니다.
백업 사본	원본보다 짧게	복구용이므로 장기 보관이 불필요하고 만료 시 분쟁 소지도 없습니다.

일반적인 권장 사항이며, 실제 보존 기간은 귀사 업종의 규제 요건을 기준으로 합니다.

계약서에 명시할 세 가지 기한 ① 데이터 내보내기 가능 일수(종료 후 회수 기간), ② 백업 사본 보존 기간, ③ 삭제 완료 후 서면 확인 기한. 이 세 숫자가 “삭제 지원” 체크보다 유용합니다.

04 QUESTIONNAIRE

보안 설문 빠른 참조와 취약점 제보

아래는 공급업체 설문에서 가장 자주 나오는 항목이며 답변을 그대로 인용할 수 있습니다. 더 세부적인 질문은 메일로 보내 주십시오. 일반적인 홍보 자료 대신 귀사의 설문 형식에 맞춰 항목별로 작성해 드립니다.

4.1 자주 묻는 질문

질문	답변
학습에 데이터를 씁니까?	아니요. AI는 현재 워크스페이스의 데이터만 읽고 공유·공개 모델 학습에 쓰지 않습니다. 셀프호스팅의 모델은 고객 제공이며 데이터는 내부망을 벗어나지 않습니다.
저장 리전을 지정할 수 있습니까?	상용판 · 전용 클라우드는 인스턴스와 백업 리전을 지정할 수 있고 개설 시 고정됩니다. 클라우드는 표준 리전, 셀프호스팅은 고객이 결정합니다.
직원이 대화 내용을 봅니까?	클라우드 운영 담당자가 장애 대응 중 비식별화된 로그에 접촉할 수 있습니다. 대화 본문과 첨부 파일은 일상적 운영 대상이 아닙니다. 더 철저한 격리가 필요하면 셀프호스팅을 선택하십시오.
감사 로그가 있고 내보낼 수 있습니까?	있습니다. 상태 변경, 권한 변경, AI 실행 모두 수행자, 시각, 상세를 기록하며 데이터와 함께 내보낼 수 있습니다.
외부 링크를 제한·폐기할 수 있습니까?	가능합니다. 대상에 맞춰 공유하고 유효 기간과 열람 횟수를 정하며 언제든 폐기합니다.
종료 후 데이터는 어떻게 됩니까?	표준 형식으로 내보낼 수 있고, 삭제는 절차대로 실행되며 실행 기록과 백업 만료 시점을 제공합니다.
AI 사용량에 상한을 둘 수 있습니까?	가능합니다. 기본은 소프트 상한(한도 근접 시 알림, 중단 없음)이고 하드 상한으로 바꾸면 도달 시 호출이 중지됩니다. 포인트 소진 시 과금도 일시 중지됩니다.
셀프호스팅을 오프라인으로 업그레이드할 수 있습니까?	가능합니다. 새 버전을 오프라인 패키지로 제공하며, 가져온 뒤 안내에 따라 업그레이드하고 배포 서버의 네트워크 연결을 요구하지 않습니다.

4.2 취약점 제보

STEP 01
제보
support@onsitesai.com 으로 보내면 해당 제품 개발팀에 전달됩니다.

STEP 02
확인
영업일 1일 이내에 접수 확인과 함께 1차 판단과 담당자를 안내합니다.

STEP 03
수정
영향도에 따라 등급을 나눠 일정을 잡고, 진행 상황을 계속 공유합니다.

STEP 04
회고
배포 후 결론을 공유하며, 고객 측 조치가 필요하면 작업 목록을 제시합니다.

그림 4-1 제보 절차. 당사는 포상금 제도를 운영하지 않지만, 익명을 요청한 경우를 제외하고 제보자에게 감사를 표합니다.

4.3 추가 자료가 필요한 경우

특정 형식의 설문 회신, 모의 해킹 보고서, 셀프호스팅 아키텍처 확인서가 필요하면 형식과 마감 시한을 알려 주십시오.

4.4 관련 문서

문서	문서 번호	용도
제품 매뉴얼	ONS-PM-KO-2.0	제품 구성, 기능 범위, 배포 형태와 가격 구조(21쪽).
셀프호스팅 가이드	ONS-SH-KO-2.0	셀프호스팅 적용 시나리오, 아키텍처, 자원과 비용(6쪽).
보안 및 레지던시 백서	**ONS-SC-KO-2.0**	본 문서, 보안 설문과 컴플라이언스 검토용(6쪽).

세 문서 모두 onsitesai.com/kr/download.html 에서 무료로 내려받을 수 있으며 별도 양식 작성은 필요하지 않습니다.

연락처 보안 및 컴플라이언스: support@onsitesai.com
제품 및 문서: onsitesai.com/kr/download.html · 셀프호스팅: onsitesai.com/kr/self-host.html