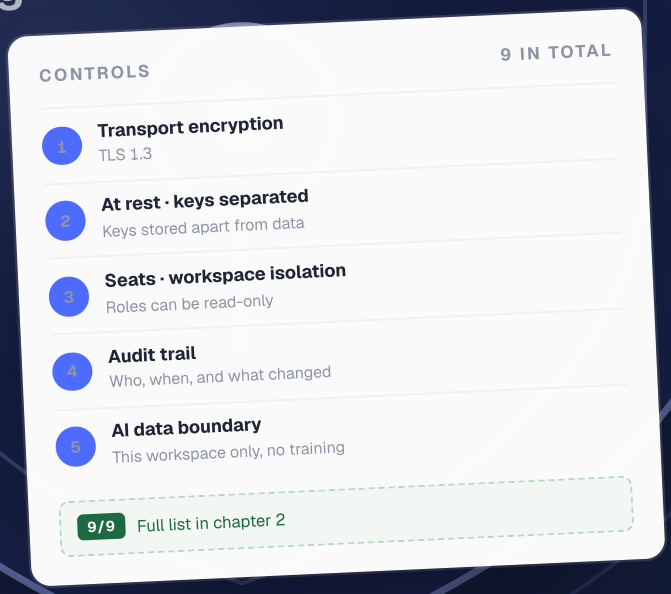
Onsites AI

SECURITY WHITEPAPER · EDITION 2.0

Security & Data Residency

Who holds the data, in writing

Encryption, access control, audit, backup and deletion timelines, AI data boundaries, and disclosure — each with what we do and who is responsible. No unverifiable adjectives.



Version
Edition 2.0

Published
November 2026

Applies to
Cloud · Dedicated · Self-hosted

Document ID
ONS-SC-EN-2.0

© 2026 Onsites AI · Regenerated with each release; latest edition at onsitesai.com/download.html

Contents

01 **Processor roles and data boundaries** Who controls, who processes, what the AI can touch 03

02 **Encryption, access, and audit** How the nine controls are implemented 04

03 **Residency, backup, lifecycle** Where data sits, how long it stays, how it is deleted 05

04 **Questionnaire and disclosure** Short answers, vulnerability reporting, contacts 06

Summary

Onsites AI treats customer data as data held in trust. Both cloud and self-hosted deployments have encryption, access control, and audit trails; on self-hosted, all of it can stay inside your own network. This document describes how each of the nine controls is implemented, and states plainly which side owns which part — because the hard part of a security review is rarely a gap, it is an unclear boundary.

9 controls	**TLS 1.3**	**1** business day	**3** deployments
Built in, mappable to a questionnaire	In transit everywhere; encrypted at rest too	To acknowledge a security report	Cloud, dedicated, self-hosted boundaries

The nine controls at a glance

01 TRANSPORT TLS 1.3	**02 AT REST** Storage media encrypted	**03 KEYS** Stored apart from data
04 SEATS Roles, narrowable to read-only	**05 ISOLATION** Workspaces cannot see each other	**06 SHARING** Links with expiry and open limits
07 AUDIT Who, when, what changed	**08 BACKUP** Automatic on paid plans, exportable	**09 AI BOUNDARY** This workspace only, no training

PURPOSE

For security reviews, vendor questionnaires, and compliance checks. Usable as the attachment to a submission.

APPLIES TO

Cloud SaaS, dedicated cloud, and self-hosted. Where behaviour differs, the difference is called out.

STATEMENT

Describes built-in product behaviour; it is not a third-party certification. Independent audits are commissioned separately.

FEEDBACK

Edition 2.0, November 2026. Corrections and security reports: support@onsitesai.com.

01

ROLES & BOUNDARIES

Who controls, who processes, what the AI can see

The first question in any security review is about roles: whose data is it, who processes it, and whether processing hands it to anyone else. Our split is simple — the customer is the controller, we are the processor, and the only sub-processors are infrastructure and models, which change with deployment.

1.1 Three roles

Controller

The customer

Decides what is collected, how long it is kept, and who may see it. Seats, roles, and permissions are yours to configure; export and deletion are yours to trigger.

Processor

Onsites AI

Processes data as configured: storing, retrieving, drafting, issuing documents. It is not used for our own purposes and never reused across workspaces.

Sub-processors

Infrastructure and models

On cloud: our infrastructure and the model services we call. On self-hosted: both are supplied by the customer, and we hold neither.

1.2 Four boundary points in one AI call

Inside

Workspace data

Threads, accounts, documents, orders. Visible only to members of this workspace, per their role.

On retrieval

Permission filter

Context is trimmed to what the requesting seat may read; records it cannot open never enter the window.

On inference

Minimum context

Only what this task needs. Self-hosted can target an internal endpoint so nothing leaves the network.

On return

Answer with sources

Every claim cites the record behind it. Nothing is written to a training set or reused elsewhere.

Figure 1-1 Four points where data could leak and what stops it at each. Remove any one and the boundary no longer holds — which is why sources are mandatory, not optional.

1.3 Four rules the AI works under

- **This workspace only.** Copilot, Harness, Agent Studio, and Desk read the current workspace and nothing else, in every deployment.
- **Sources on every answer.** If a claim cannot be traced to a thread, a field, or a file, it is not written into the answer.
- **No training.** Customer data does not train shared or public models. On self-hosted, the model and key are yours by default.
- **Switchable off.** AI can be disabled for a workspace or a member; the rest of the product keeps running without degradation.

1.4 How the roles shift by deployment

On cloud and dedicated cloud we operate the infrastructure and manage the model keys; a dedicated instance fixes its region at provisioning. On self-hosted the customer owns hosts, endpoint, keys, and storage, and can run fully offline. The controls are identical — only the supplier of the bottom layer changes.

> **"Can your staff see our conversations?"** On cloud, support may see redacted logs and error details while troubleshooting; conversation bodies and attachments are not routine support material. If that is unacceptable, self-hosted removes the question entirely.

02

CONTROLS

Nine controls, and how each is implemented

Questionnaires ask control by control, so this chapter answers in the same order: encryption, access, records, sharing, AI. Each row says what we do and who does it, which is what an assessor is actually checking.

2.1 Encryption and keys

Stage	Implementation	Owner
In transit	TLS 1.3 throughout; self-hosted terminates TLS at your proxy with your certificate	Us on cloud; customer on self-hosted
At rest	Encrypted on our storage; on your disks, handled by your OS or storage layer	Us on cloud; customer on self-hosted
Keys	Stored separately from data; platform staff only	Us on cloud; customer holds them on self-hosted
Backups	Backup files are encrypted too; destination depends on deployment	See chapter 3

2.2 Access control

- **By seat and role.** What a person sees follows their seat and role; any role can be narrowed to read-only for finance or management.
- **Workspace isolation.** Workspaces cannot see one another; data does not move between them, and AI retrieval inherits the same limit.
- **Immediate revocation.** Removing a seat revokes access at once.
- **Sharing controls.** Private files and folders shared by audience; public links can carry an expiry and an open limit, and be revoked at any time.

2.3 Audit

State changes on documents and conversations record the operator, the time, and the detail: who sent a quote, who changed an amount, who confirmed a contract. The log exports with the rest of the data, so it can still serve as approval evidence months later rather than living in a rolling activity feed. Desk's actions are logged the same way — what it read, what it wrote, and how many points it spent.

2.4 Where the controls sit on the path

Entry

Identity and seat

Sign-in, role, and seat authorisation; revocation is immediate and workspaces stay isolated.

Transit

TLS 1.3

Encrypted end to end between browser and application; self-hosted terminates at your gateway.

Application

Filter and log

Every read and write is trimmed to permissions and recorded; AI retrieval obeys the same rules.

Storage

Encryption and backup

Media encryption, separated keys, and encrypted backups that expire with the retention policy.

Figure 2-1 Controls along the path. Walking these four segments in a review finds gaps faster than walking the feature list.

How to verify Ask for one redacted sample of each: a state change, a permission change, and an AI execution record. A sample is worth more than a tick in a questionnaire.

03

RESIDENCY

Where it sits, how long it stays, how it is deleted

Residency is usually three questions in one: which region holds the data, how long backups are kept, and what happens on termination. The first two follow from the deployment; the third depends on whether you exported — which is why we keep saying export on a schedule.

3.1 Lifecycle of a record



Created

Written to the workspace

Conversations, accounts, documents, and files land in the workspace and are visible per permission.

In use

Daily read and write

Team and AI work on the same record; every write is logged with who did it.

Backed up

Encrypted copy

Paid cloud workspaces back up automatically; self-hosted runs the provided script and stores the media.

Exported / ended

Taken away or deleted

Standard-format export; deletion on request, with backup copies expiring under the retention policy.

Figure 3-1 Four stages. The one worth agreeing in advance is the last: who triggers deletion, how long backups survive, and how completion is confirmed.

3.2 Residency and backup by deployment

Deployment	Data location	Backup	Deletion
Cloud SaaS	Our infrastructure	Automatic on paid plans	On request; backups expire per policy
Dedicated cloud	Instance and backup region chosen at provisioning	Automatic, same region	As above, region unchanged
Self-hosted	Your data centre or private cloud	Script provided with the licence	You execute; we supply steps and checklist

The region is fixed at provisioning and does not change afterwards; moving region is handled as a new instance.

3.3 Export, downgrade, retention

- **Export is a right, not a feature toggle.** Conversations, contacts, and documents export in standard formats; no format lock-in and no export fee.
- **Downgrading does not delete.** Dropping a storage pack or a plan keeps existing data; it is not purged for being over quota.
- **Free workspaces have no server-side copy.** Scheduled export is your only backup — the point most often missed.
- **Deletion is confirmed.** We provide an execution record and the backup expiry date, so "deleted" does not mean "probably still in a snapshot".

3.4 Setting retention

Data	Suggested	Reason
Conversations and accounts	As long as the business	After-sales and repeat purchase both depend on the thread.
Quotes, contracts, invoices	Per tax requirements	Usually longer than conversations; numbers and versions must be reviewable.
Audit log	Longer than the documents	Approvals and disputes need "who changed what, when".

04

QUESTIONNAIRE

Short answers, and how to report a vulnerability

The rows below are the questions that come up in nearly every vendor review. The answers can be quoted directly; for anything else, send your questionnaire and we will fill it in your format rather than replying with a brochure.

4.1 Common questions

Question	Answer
Is customer data used to train models?	No. AI reads only this workspace and is not used to train shared or public models; self-hosted keeps the model inside your network.
Can we choose where data is stored?	Dedicated cloud chooses instance and backup region at provisioning. Cloud uses a standard region; self-hosted is wherever your hosts are.
Can your staff read customer conversations?	On cloud, support may see redacted logs while troubleshooting; conversation bodies and attachments are not routine support material. For stricter separation, choose self-hosted.
Do you keep audit logs, and can we export them?	Yes. State changes, permission changes, and AI executions record who, when, and what; all export with your data.
Can file links be limited and revoked?	Yes. Share by audience, set an expiry and an open limit, and revoke at any time.
What happens to data when we leave?	Standard-format export; deletion on request with an execution record and backup expiry date.
Can AI spending be capped?	Yes. A soft cap warns and continues; a hard cap stops AI calls at the threshold while the rest of the product carries on.

4.2 Reporting a vulnerability

Step 01
Report
Email support@onsitesai.com; it reaches the team that builds the affected product.

Step 02
Acknowledge
Within one business day, with an initial assessment and a named contact.

Step 03
Fix
Scheduled by severity, with progress shared during the work rather than at release.

Step 04
Close out
Findings and any customer-side actions summarised; a checklist if you need to act.

Figure 4-1 Disclosure path. There is no bug bounty, but reporters are credited unless they ask not to be.

4.4 Related documents

Document	Document ID	Use
Product manual	ONS-PM-EN-2.0	Products, scope, deployment options, pricing (21 pages).
Self-hosted deployment guide	ONS-SH-EN-2.0	Feasibility, architecture, requirements, cost (6 pages).
Security and data residency	ONS-SC-EN-2.0	This document, for questionnaires and reviews (6 pages).

Contact Security and compliance: support@onsitesai.com — acknowledged within one business day.
Documents: onsitesai.com/download.html · Self-hosted assessment: onsitesai.com/self-host