Closed by construction.

The controls below do not depend on a certificate to be true — they are how the system is built. This brief is written to be forwarded to the people who review vendors.

01 · TENANCY AND ISOLATION

TIER	TENANCY	INFERENCE	KEYS
Atelier	Logical multi-tenant, row-level security	Shared dedicated chamber, zero-retention contract	Platform-managed
House	Single-tenant Supabase project, dedicated Postgres	Dedicated chamber, region-pinned, zero-retention	Platform-managed, customer key optional
Sovereign	Single-tenant in your VPC or on-premise	Customer-hosted open weights or dedicated chamber	Customer-managed, bring-your-own-key

02 · THE MODEL LAYER

Our prompt systems and workflows are the value; the model is interchangeable, which is what lets each tier choose its own boundary.

DEFAULT	Anthropic Claude on a zero-data-retention enterprise contract — inputs and outputs are not retained or used for training.
HOUSE TIER	Inference routed through AWS Bedrock with PrivateLink and zero retention, pinned to a region you elect (US, UK, EU, or Singapore).
SOVEREIGN TIER	Run open-weight models in your own VPC, with our orchestrator deployed as a Helm chart. The documents never leave your boundary.
TRAINING	Documents are never used to train any model. No exceptions.

03 · DATA HANDLING

ENCRYPTION	Documents are encrypted at rest with AES-256 and in transit with TLS 1.3.
RETENTION	Document retention defaults to engagement lifetime plus ninety days, configurable down to engagement lifetime.
AUDIT	The audit log is append-only and retained seven years, immutable via object-lock storage.
SUBPROCESSORS	The subprocessor list is published and versioned, and the contracted auditor is named there.

04 · MATERIAL NON-PUBLIC INFORMATION

QUARANTINE	When an engagement is tagged public-company-adjacent, the system flags and quarantines likely MNPI by default.
WALL-CROSSING	Wall-crossing runs through explicit role assignment, a separate chamber, and a separate audit trail.
OVERSIGHT	A compliance-officer role holds read-only access to every engagement in a House.

05 · COMPLIANCE ROADMAP

NOW

- SOC 2 Type I observation period under way, auditor named on the subprocessor list
- Vendor security questionnaire pack ready on request
- Penetration test conducted annually

PLANNED

NEXT

SOC 2 Type II report

AFTER

ISO 27001 certification

ON REQUEST

HIPAA-aligned controls, for families with health-related trusts

We do not claim a certification before it is issued. Where a control is in progress we say so, and name the auditor. None of this is a warranty on a specific engagement — that still depends on document quality, MNPI routing, and reviewer sign-off.