

Data Protection & Encryption Policy

Mindshine Technologies Inc. · Document 05 · Version 1.1 · August 12, 2026 · Status: **Operating**

Data classification

A maintained **data map** inventories every class the platform holds: staff identity data, organization membership and roles, customer project configuration (column names and rules – not values), customer datasets in per-project stores, and append-only audit records. Each class carries its location, purpose, encryption status, and retention (document 13). PII columns in customer projects must carry access policies – enforced by a per-project audit check with closed-loop fix requests.

Encryption in transit

TLS on all external surfaces; TLS certificate verification is enforced by default in outbound integrations. Web surfaces run behind an origin allowlist (no wildcard CORS), rate limiting, and security headers – verified by automated configuration checks each audit cycle.

Encryption at rest

- **S3:** server-side encryption on platform buckets.
- **EBS: encryption-by-default is enabled account-wide** (August 12, 2026), so every new volume is encrypted; public access to EBS snapshots is blocked at the account level. Verification of pre-existing volumes is a disclosed open matter with a remediation plan.
- Volume disposal uses encrypted-key destruction semantics (document 13).

Secrets & keys

Least-privilege distribution; fail-closed consumption (no fallback values – services refuse to boot without their secrets); a CI gate blocks secret material from entering source control; continuous secret-hygiene scanning. Customer LLM API keys, where supplied, are used only for that customer's configured integrations.

Customer data

Customer information is processed **only** for the service purposes the customer configured. Isolation is structural: per-organization scoping in the product's central authorization policy, per-project data stores, and an isolated namespace per deployed customer application. **Customer data is never used to train foundation models.** Where a customer flags a project as containing regulated data, row sampling to LLM subprocessors is disabled (see document 12 – the Anthropic DPA is in countersignature).

Owner: CTO. **Review:** at least annually and upon material change. **Contact:** security@mindshine.com.