Data Retention & Destruction Policy

Mindshine Technologies Inc. · Document 13 · Version 1.1 · August 12, 2026 · Status: **Operating · TTL automation in progress**

Retention by class

Retention is documented **per data class** in the data map, including where persistent copies live: staff identity data (life of employment + legal minimum), organization membership/roles (life of the organization account), customer project configuration (life of the project — versioned history is the product), customer datasets (customer-controlled; deleted with the project or on request), audit records (append-only by design; retained for the assurance program).

Deletion paths — per asset class, actually implemented

Disposal is defined and verified per class: individual records, data sources, whole projects, and user accounts each have a deletion path with understood cascade semantics; storage volumes are disposed via **encrypted-key destruction** (rendered unreadable rather than scrubbed). Deletion requests from data subjects follow the DSAR runbook with a **30-day SLA**; corrections propagate structurally through pipeline lineage.

Backups

Deleted information may persist in protected backups until normal expiration; the target backup-retention window (35 days) is being written into the data processing terms. Backup access is restricted (document 09).

Honest open items (disclosed, tracked)

- **Automated TTL enforcement jobs are not yet running** — retention is currently enforced by the deletion paths plus manual review; TTL jobs land with the backup rollout and are a disclosed open matter.
- Per-volume encryption verification of pre-existing EBS volumes accompanies this (new volumes are encrypted by default as of August 2026).

Legal holds

Information under a legal or regulatory preservation obligation is retained until the hold is released; holds override scheduled destruction.

Owner: CTO. **Review:** at least annually and with any new data class. **Contact:** security@mindshine.com.