Executive Security Overview

Mindshine Technologies Inc. · Document 01 · Version 1.1 · August 12, 2026 · Status: **Operating**

The platform

TIVA Cortex is a data-governance platform: governed data pipelines (sources, typed data elements, mappings, processing rules, targets), business workflows with human and AI participants, project-scoped AI agents, published governed applications, and models trained on governed data. **TIVA Flow** orchestrates the underlying execution engine and multi-agent workflows. The architecture is LLM-agnostic and integrates with customer-approved model providers; customer-controlled API keys are supported. **Customer data is never used by Mindshine to train foundation models.**

The security program — what is actually running

Unlike a policy binder, Mindshine's program is built around a **continuous-audit system of record**: an audit portal with an append-only, hash-chained evidence log, automated collectors, and scanners whose every failing check becomes a tracked issue with a recorded disposition.

- **Continuous scanning.** The application codebase is scanned each audit cycle; infrastructure is scanned weekly — CIS Kubernetes benchmarks against the runtime, and AWS-account scans (Prowler) under a dedicated read-only `SecurityAudit` IAM role.
- **Hardened runtime.** Non-root containers, read-only root filesystems, RuntimeDefault seccomp, resource limits, digest-pinned data stores, and an admission policy constraining privilege-granting operations at the API server — verified live after every deploy.
- **Controlled change.** Images are built exclusively by CI behind a verify gate (tests, dependency audit, secret scan); infrastructure changes only through versioned overlays and declarative applies; customer configuration changes are versioned commits by construction (Dolt).
- **Least-privilege access.** Staff SSO federated to Google Workspace with MFA at the identity provider; a central authorization policy on every project operation; no direct human access to production data stores — cluster access only via a single audited jumpbox.
- **Account hardening (verified August 2026).** EBS encryption-by-default, EBS snapshot public-access block, a strict IAM password policy (14+ characters, full complexity, 24-password reuse prevention, 90-day rotation), and dedicated `SecurityAudit` / `Support` IAM roles.

Assurance status — stated plainly

A management-prepared **SOC 2 readiness assessment is complete** (documents 17 and 18), produced from the continuous-audit evidence base and an independent adversarial review. Mindshine is **not yet SOC 2 certified**: examination by a licensed CPA firm (Type I, then a Type II observation window) is the scheduled next step, and an independent penetration test is planned to complement continuous automated scanning. Open items are disclosed per document — not papered over.

Owner: CTO (Ken Bakke); executive oversight: CEO (Igor Babushkin). **Review:** at least annually and upon material change. **Contact:** security@mindshine.com.