# Information Security Policy

**Mindshine Technologies Inc.** · Document 03 · Version 1.1 · August 12, 2026 · Status: **Operating**

## Governance

Security responsibility is assigned: the **CTO (Ken Bakke)** owns the security program with executive oversight by the **CEO (Igor Babushkin)**; HR-side controls (onboarding, training, offboarding) are owned by HR (Igor Golovaty). Policies, the control catalog (76 mapped SOC 2 controls), and quarterly management evidence reviews are recorded on the audit system of record — quarterly SOC 2 evidence reviews were held May 30 and August 8, 2026.

## Risk management

A **risk register** with likelihood/impact scoring, mitigations, and residual actions is maintained and reviewed quarterly; mitigations are verified against the actually-implemented controls, not against intentions. The 2026 annual security risk assessment is on file. Deficiencies from any source (scanner, collector, review) become tracked issues with an append-only lifecycle; closure is mechanical — an issue closes only when re-detection passes or a disposition with rationale is recorded.

## Asset management

Material assets have named owners: source repositories (Bitbucket), container images (ECR, built only by CI), the EKS runtime and its namespaces, data stores (versioned configuration in Dolt, operational PostgreSQL, S3, EBS), and the audit portal. A **data map** covering every data class — including encryption status and personal-data inventory — is maintained and verified against the estate.

## Access control

Access follows least privilege and business need (document 04). Production data stores allow **no direct human access**; the cluster is reachable only through a single audited jumpbox. A central authorization policy gates every project operation in the product.

## Monitoring & review

Security-relevant activity lands on an **append-only, hash-chained audit log** whose chain is verified on read; failed logins are durably logged. Application code is scanned every audit cycle; infrastructure weekly (CIS Kubernetes benchmarks; AWS Prowler scans under a dedicated read-only `SecurityAudit` role). Control effectiveness is re-verified continuously — "implemented" in this package means *re-detected as operating*, not asserted once.

## Exceptions

Deviations require a recorded disposition (accepted risk with rationale, false positive with evidence, or an assigned remediation owner) on the issue ledger. No silent exceptions.

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