Incident Response Plan

Mindshine Technologies Inc. · Document 08 · Version 1.1 · August 12, 2026 · Status: **Operating**

Preparation

A published security policy defines the **reporting channel (security@mindshine.com), acknowledgement expectations, and severity SLAs**; its presence and content are verified by an automated check each audit cycle. Incident-response roles: the CTO leads response; the CEO owns external communication decisions.

Detection & triage

Signals come from continuous scanning (weekly infrastructure, per-cycle application), the append-only audit log (failed logins are durably recorded), operational monitoring, personnel reports, and customers. Incidents are triaged by severity and impact and recorded in the **incident register**, which is reviewed monthly by an automated collector that files the review as evidence.

Containment

Response can restrict or isolate affected components quickly because credentials are built for it: OAuth bearers expire in ~1 hour, per-app deployment credentials are individually revocable, CI credentials are scoped, and workloads run least-privilege behind an admission policy — limiting blast radius by construction.

Investigation

Evidence and logs are preserved on the tamper-evident (hash-chained) audit log; scope, cause, and impact are determined before closure. Real incidents are handled through the full lifecycle — e.g. **INC-2026-014** (elevated 5xx on the web tier) is on file with its timeline and corrective actions, and an **IR tabletop exercise** (compromised CI token scenario, 2026) tested the plan and recorded lessons learned.

Recovery & notification

Systems are restored from CI-built images and versioned configuration (document 09). Customers are notified when required by contract or applicable law; post-incident reviews feed corrective actions into the tracked issue ledger.

Planned improvement (disclosed)

A threshold alert on login-denial bursts in the audit portal is a scheduled enhancement — detection today relies on durable logging plus review.

Owner: CTO. **Review:** at least annually and after every material incident. **Contact:** security@mindshine.com.