Vulnerability Management Policy

Mindshine Technologies Inc. · Document 06 · Version 1.1 · August 12, 2026 · Status: **Operating**

Scanning — what actually runs

Surface	Mechanism	Cadence
Application dependencies	CI dependency audit — **critical advisories block the build**; lockfiles everywhere; the scanner itself is pinned	Every build + every audit cycle
Application code & configuration	Automated audit checks (secret hygiene, CORS/headers/TLS config, authorization coverage)	Every audit cycle
Kubernetes runtime	CIS Kubernetes benchmark scans; live pod-spec verification after deploys	Weekly + on demand
AWS account	**Prowler** scans (S3, EC2, IAM, KMS, CloudTrail, RDS, Backup) under a dedicated read-only `SecurityAudit` IAM role	Weekly (scheduled)

Triage & tracking

Every failing check becomes a **tracked issue** on the audit portal's append-only ledger, tagged by layer (code / infrastructure) and detector, with severity from the scanner. Nothing is dropped silently: monthly vulnerability remediation summaries (April–August 2026 on file) are generated from the ledger, not written by hand.

Remediation & risk acceptance

Issues are assigned to owners and remediated by risk; critical and high severity first. Where remediation is not appropriate, the disposition is recorded explicitly with rationale — for example, on the shared AWS account, findings on resources owned by other tenants are **accepted with a documented boundary rationale and owner notification** rather than silently closed (August 2026 review: every AWS finding dispositioned — fixed, assigned to a named owner, or accepted with rationale; zero left undispositioned).

Verification

Closure is **mechanical**: an issue is resolved only when the re-scan re-detects the control as passing, or a recorded disposition explains why not. Fixed account-level items in August 2026 (EBS default encryption, snapshot public-access block, IAM password policy, audit/support roles) were confirmed by re-scan before being closed.

Exceptions

Risk exceptions live on the same ledger with the same append-only lifecycle — documented rationale, compensating controls where relevant, and management visibility through the quarterly evidence review.

Owner: CTO. **Review:** at least annually; ledger reviewed continuously. **Contact:** security@mindshine.com.