Security Testing & Penetration Testing Program

Mindshine Technologies Inc. · Document 16 · Version 1.1 · August 12, 2026 · Status: **Automated testing operating · independent penetration test planned**

Automated scanning — operating

Continuous and scheduled: CI dependency audits on every build (critical advisories block), secret-hygiene scanning, application configuration checks (CORS, headers, TLS verification) each audit cycle, **weekly CIS Kubernetes benchmark scans**, and **weekly AWS account scans (Prowler)** under a dedicated read-only role. Every failing check becomes a tracked issue.

Application security testing — operating

Authorization is tested the hard way: the central access policy is unit-tested across every branch in CI, and enforcement controls are exercised **as the identity they constrain** — e.g. server-side dry-run attempts against restricted namespaces under the governed workload identity, including an independent adversarial re-test for bypasses. End-to-end browser tests cover the authenticated user flows. Findings and remediation are tracked on the append-only ledger; closure requires re-detection or a recorded disposition.

Infrastructure testing — operating

Externally exposed components and configurations are assessed weekly by the account scans (security groups, NACLs, public IPs, S3 exposure, IAM). An August 2026 reachability analysis mapped every internet-facing resource in the account and drove per-resource remediation and owner assignments.

Independent penetration testing — planned, honestly stated

Mindshine has not yet completed a third-party penetration test. One is planned as a Phase 2 assurance milestone to complement continuous automated scanning, ahead of the SOC 2 Type I examination. No penetration-test report will be represented as existing until an actual engagement completes; when it does, the executive summary will be available under NDA.

Remediation evidence

Monthly vulnerability-remediation summaries (April–August 2026) are compiled from the ledger; fixed items are closed only after re-scan confirms the control passes.

Owner: CTO. **Review:** program annually; scans weekly/continuous. **Contact:** security@mindshine.com.