Employee Security & Security Awareness Policy

Mindshine Technologies Inc. · Document 11 · Version 1.1 · August 12, 2026 · Status: **Operating**

Onboarding

New personnel receive security expectations, confidentiality requirements, and access appropriate to the role — provisioned through the identity lifecycle in document 04 (Google Workspace SSO; role-scoped product access). Joiner records are kept as evidence (2026 executive onboardings on file). HR ownership: Igor Golovaty; code-of-conduct / confidentiality acknowledgement is collected at hire and annually.

Training

An annual **security-awareness campaign** (2026 campaign on file) covers credential protection, phishing, data handling, incident reporting, and secure working practice. Engineering-specific practice is enforced where it matters most — in the pipeline: the CI secret-scan and dependency gates make the secure path the only path.

Acceptable use

Company systems and information are used for authorized purposes only. Production access rules are structural, not aspirational: no direct human access to production data stores, cluster access only via the audited jumpbox, and MFA at the identity provider.

Incident reporting

Personnel report suspected incidents, credential compromise, or suspicious activity immediately to **security@mindshine.com** (acknowledgement and severity SLAs are published — document 08).

Offboarding

Access is revoked promptly on departure: Google Workspace suspension cuts SSO-federated access; product roles are removed; quarterly access reviews (Q2/Q3 2026 on file) catch any residual grants. Leaver evidence is recorded.

Honest gap (disclosed)

Mindshine does not currently operate a **mobile-device-management (MDM)** fleet; endpoint posture relies on managed identity + browser-based access to production surfaces. An MDM/endpoint-baseline decision is tracked in the program's gap register.

Owner: HR (Igor Golovaty) with CTO for technical controls. **Review:** at least annually. **Contact:** security@mindshine.com.