Access Control & Identity Management Policy

Mindshine Technologies Inc. · Document 04 · Version 1.1 · August 12, 2026 · Status: **Operating**

Identity lifecycle

Access is authorized before provisioning, adjusted on role change, and revoked promptly at offboarding (joiner/mover/leaver records are kept as evidence — e.g. 2026 executive onboardings are on file). **Quarterly user access reviews** are performed and recorded (Q2 and Q3 2026 reviews on file).

Authentication & MFA

- **Staff:** SSO federated to Google Workspace (OIDC with verified email and domain claims); **MFA is enforced at the identity provider**. Product credentials, where they exist, are bcrypt-hashed.
- **AWS:** console access requires MFA; the account enforces an IAM password policy of **14+ characters, upper/lower/number/symbol, 24-password reuse prevention, 90-day maximum age** (verified in effect August 12, 2026).
- **Honest gap:** a product-native second factor for non-federated accounts is on the roadmap and disclosed as an open matter; MFA today is enforced at the IdP and cloud layers.

Authorization

A **central authorization policy** (`canAccessProject`) is evaluated on every project operation; queries are organization-scoped. The policy is unit-tested across every branch in CI. API access uses **OAuth 2.1 bearer tokens with ~1-hour expiry and per-project scope**; the engine's read-only surface is allowlisted; per-app deployment credentials are hash-stored, auto-rotated on redeploy, and individually revocable.

Privileged access

- **No direct human access to production data stores.** Databases are reached only via backend services, or via `kubectl exec` through the **single audited jumpbox** (SSH key auth), which is the sole cluster chokepoint.
- Workload identity is least-privilege: a minimal cluster role, namespace-local grants, and a **ValidatingAdmissionPolicy** constraining privilege-granting operations at the API server — tested live *as the constrained identity*, including adversarial bypass attempts.
- Machine credentials are scoped: CI uses an IAM user limited to ECR push + EKS describe; the weekly AWS scanner assumes a read-only `SecurityAudit` role (2-hour max session) rather than borrowing write-capable credentials.

Secrets

Secrets are **fail-closed**: services refuse to boot without them and there are no fallback values. A CI gate blocks tracked secret material from ever entering the repository; secret hygiene is scanned continuously.

Owner: CTO. **Review:** at least annually; access reviews quarterly. **Contact:** security@mindshine.com.