SOC 2 Control Matrix

Mindshine Technologies Inc. · Document 17 · Version 1.1 · August 12, 2026 · Status: **Current**

Summary of the 76-control mapped catalog. "Operating" = re-detected as operating by continuous testing at the stated date; open areas are disclosed inline, matching the published readiness assessment.

Control environment, risk & communication (CC1–CC3, CC9)

Operating: named security ownership (CTO) with executive oversight; quarterly management evidence reviews (May 30 / Aug 8, 2026 on file); risk register with L/I scoring and quarterly review; vendor & subprocessor register verified against actual data flows; deficiencies tracked append-only with mechanical closure. **Open (disclosed):** a set of organizational policy attestations (ethics, oversight, privacy notice, consent, disclosure) awaits formal sign-off; one LLM subprocessor DPA in countersignature.

Logical access (CC6)

Operating: Google Workspace SSO (OIDC) with IdP-enforced MFA; central `canAccessProject` authorization on every project operation, unit-tested in CI; OAuth 2.1 bearers (~1h, per-project scope); read-only engine allowlist; per-app credentials hash-stored/rotated/revocable; fail-closed secrets + CI secret gate; least-privilege workload identity enforced by admission policy and tested as the constrained identity; no direct human access to production data stores (audited jumpbox chokepoint); AWS IAM password policy + MFA. **Open (disclosed):** product-native MFA for non-federated accounts (roadmap); per-volume encryption verification of pre-existing EBS volumes.

System operations (CC7)

Operating: CI dependency gate (critical blocks); continuous scanning — application per cycle, infrastructure weekly (CIS k8s + AWS Prowler under a read-only role); every failing control becomes a tracked issue with recorded disposition; append-only hash-chained audit log verified on read; published security policy with reporting channel + severity SLAs; incident register with monthly recorded review. **Open (disclosed):** login-denial burst alerting (scheduled).

Change management (CC8)

Operating: single-path-to-production per change type; CI verify gate (tests, audit, secret scan) before any image; overlay/terraform-only infrastructure; versioned customer configuration by construction; deploy↔ commit traceability. **Open (disclosed):** git-host enforced pre-merge review being verified (CODEOWNERS routing already operates).

Availability (A1) · Confidentiality (C1) · Processing integrity (PI1) · Privacy (P)

Operating: resource limits + SPOF inventory; backup/DR inventory with RPO 24h/RTO 8h and rebuild-from-code property; data map per class; PII access-policy checks per project (closed-loop); machine-readable processing contracts, per-stage counts, visible rejects, versioned lineage; personal-data inventory; DSAR runbook (30-day

SLA). **Open (disclosed):** restore rehearsal with recorded results; retention TTL automation; capacity alert; independent penetration test; SOC 2 examination itself.

Full per-control test descriptions and results: the published **SOC 2 Audit Findings Report — Cortex** (readiness assessment), same evidence base.

Owner: CTO. **Review:** every audit cycle. **Contact:** security@mindshine.com.