

Cloud & Infrastructure Security Policy

Mindshine Technologies Inc. · Document 15 · Version 1.1 · August 12, 2026 · Status: **Operating**

Container infrastructure

Cortex and Flow run containerized on **Amazon EKS (us-east-1)**. Both the development and production namespaces run under the same baseline, each with its own weekly CIS Kubernetes scan (production brought under the baseline and continuous scanning in the 13 August 2026 change window). The runtime baseline – verified live after every deploy – is: **non-root images, read-only root filesystems** with scoped writable mounts, **RuntimeDefault seccomp**, resource requests/limits, digest-pinned data-store images, and a **ValidatingAdmissionPolicy** that constrains privilege-granting operations at the API server. Named writable acceptances carry recorded rationale. Images enter the registry only from CI.

Account hardening (verified in effect August 12, 2026)

- **EBS encryption-by-default** – every new volume encrypted.
- **EBS snapshot public-access block** (account level).
- **IAM account password policy**: 14+ characters, upper/lower/number/symbol, 24-password reuse prevention, 90-day maximum age.
- Dedicated **SecurityAudit** (read-only scanning) and **Support** IAM roles – scanners never borrow write-capable credentials.

Network security

External exposure is minimized: product surfaces behind TLS with an origin allowlist, rate limiting, and security headers; the cluster is reached administratively only via the audited jumpbox. Weekly AWS scans review security groups, network ACLs, and public-IP posture; findings are tracked on the issue ledger with recorded dispositions (August 2026: all AWS findings dispositioned – fixed, owner-assigned, or accepted with boundary rationale).

Logging & monitoring

Application and audit events land on the append-only hash-chained log; scanner and collector runs are recorded with start/finish, stats, and findings – the run history itself is reviewable evidence.

Patch management

Application dependencies are gated in CI (critical advisories block); lockfiles pin all trees; base images are rebuilt through CI. EKS add-ons in **kube-system** (CNI, CSI, CoreDNS, kube-proxy) are operated and patched by AWS under the shared-responsibility model and covered by AWS's SOC 2 reports – they are deliberately outside the tenant hardening boundary, with the rationale recorded.

Secrets & backups

Fail-closed secrets (no fallbacks; CI gate against committed secret material); backup/DR per document 09.

Owner: CTO. **Review:** at least annually; scans weekly. **Contact:** security@mindshine.com.