

Business Continuity & Disaster Recovery Plan

Mindshine Technologies Inc. · Document 09 · Version 1.2 · August 13, 2026 · Status: **Operating** · restore drill recorded

Critical services

Cortex application services, the Flow execution engine, the versioned configuration store (Dolt), operational PostgreSQL stores, object storage (S3), identity (Google Workspace federation), source + CI (Bitbucket), and the EKS runtime (AWS us-east-1).

Recovery objectives

RPO 24 hours · RTO 8 hours, stated per store in a maintained backup/DR inventory that is verified against the actual estate.

Backup strategy – and its strongest property

The estate is **rebuildable from code plus versioned configuration**: images come only from CI (rebuildable from git), infrastructure is declarative (overlays + terraform), and every piece of customer pipeline configuration is a versioned Dolt commit with full history. This makes recovery a re-apply, not an archaeology exercise. Data-store backups are inventoried per store with restricted access; backup expiration governs residual copies (document 13).

Recovery procedure

Documented runbooks prioritize: runtime + networking → data stores from backup/versioned config → application rollout from registry images → verification (the same automated checks that gate normal deploys). DR evidence on file includes 2026 backup-restore/DR test records (May and August).

Restore rehearsal – performed and recorded (13 August 2026)

All four production PostgreSQL stores were restored from same-day dumps into throwaway instances and verified **table-by-table against the live stores**: zero restore errors; residual count differences fully explained by post-dump live traffic. The drill surfaced a real recovery dependency – the analytics store's vector-search schemas require the **pgvector** extension on the restore host – which is now pinned in the recovery runbook. The drill record is evidence on the control register.

Honest open items (disclosed, tracked)

- **Scheduled automated backups** (this drill used deliberate pre-change dumps and volume snapshots; recurring scheduled jobs are the remaining half of this control).

- **Operator redundancy:** a single credentialed platform operator today; runbooks are documented and second-operator onboarding is tracked.
- A disk-usage capacity alert on persistent volumes is a scheduled small improvement.

Customer-hosted deployments

Where Cortex/Flow run in customer-controlled infrastructure, continuity responsibilities are allocated by architecture and contract; Mindshine supplies the rebuild-from-code property (CI images + versioned configuration) and the customer supplies infrastructure-level backup and restore.

Owner: CTO. **Review:** at least annually and after every DR exercise. **Contact:** security@mindshine.com.