

Business Continuity & Disaster Recovery Plan

How Workplacer maintains availability and recovers from disruption.

1. OVERVIEW

Workplacer runs on a serverless, cloud-native architecture that provides high availability and rapid recovery by design. Backup is the responsibility of Workplacer; customers do not need to perform or manage backups. This plan covers architecture resilience, backup and recovery, defined disaster scenarios, recovery objectives, and communication.

2. ARCHITECTURE RESILIENCE

- **Application (Vercel):** serverless functions with automatic scaling; global edge network with automatic failover; zero-downtime atomic deployments; instant rollback to any previous deployment.
- **Database (Neon PostgreSQL):** compute/storage separation; continuous write-ahead-log backup with point-in-time recovery; multi-AZ storage redundancy within the region.
- **File storage (Vercel Blob):** multi-AZ object storage; 99.999999999% (11 nines) durability.
- **Background processing (Inngest):** automatic step-level retries; idempotent, safely re-executable functions; independent queue durability.

3. BACKUP & RECOVERY

Parameter	Value
Backup method	Continuous write-ahead-log (WAL) streaming
Backup frequency	Continuous — every transaction is captured
Point-in-time recovery	Restore to any point within the retention window
Retention window	7 days (rolling)
Encryption	AES-256 at rest, TLS 1.3 in transit
Geographic redundancy	Multi-AZ within the selected region (EU)

4. DISASTER SCENARIOS & RESPONSE

Application outage

Step	Action	Time
1	Automated alerting (Sentry)	Immediate
2	Assess scope — check provider status	5 min
3	If code-side: roll back to last known good deployment	< 5 min
RTO		< 15 min

Database corruption or data loss

Step	Action	Time
1	Identify the point of corruption	15 min
2	Initiate point-in-time recovery to a point before corruption	10 min
3	Verify data integrity on the restored branch	15 min
4	Switch connection to the restored branch and validate	20 min
RTO		< 1 hour

Region-wide outage

Step	Action	Time
1	Monitor provider status pages	Immediate
2	If prolonged: initiate cross-region deployment	2 hours
3	Restore database from backup in an alternate region	1 hour
RTO		< 4 hours

Security breach

- Rotate all secrets and API keys; invalidate active sessions.
- Review audit logs to determine scope.
- Notify affected customers within 72 hours where personal data is affected (GDPR Art. 33).
- Remediate the underlying vulnerability, prioritized by severity.

5. RECOVERY OBJECTIVES

Metric	Target
RPO (Recovery Point Objective)	Near zero — continuous backup
RTO — Application (once engaged)	< 15 minutes
RTO — Database (once engaged)	< 1 hour
RTO — Full region failover (once engaged)	< 4 hours

The recovery time objectives above express the time required to **execute each recovery procedure once engineering has engaged** with the incident. They are technical recovery targets, not a guaranteed end-to-end restoration time from the first moment of failure. Data durability is independent of response time: continuous backup maintains a near-zero recovery point objective, so a delayed response affects availability, not data loss — no committed data is lost even if remediation begins some hours after an out-of-hours failure.

6. RESPONSE COVERAGE

Automated monitoring and alerting operate 24/7. The most common disruptions are absorbed by automated resilience with no human intervention required: global edge failover, database multi-AZ redundancy, zero-downtime deployments with instant rollback, and automatic retries on background jobs. These protect availability around the clock, including outside working hours.

Incidents that require manual intervention (e.g. rolling back a faulty deployment, or a point-in-time database restore) are handled by engineering during standard working hours, and on a best-effort basis outside them — automated alerting ensures such incidents are detected at any hour, with remediation beginning as soon as an engineer engages. Formal after-hours on-call coverage will be introduced as the team scales.

7. COMMUNICATION & ESCALATION

Incidents are escalated by severity: automated alerts trigger initial response; unresolved or customer-facing incidents escalate to engineering leadership and, for outages exceeding one hour or any data breach, to the founder. Affected customers are notified by email for critical incidents (target: within one hour), with a data-protection-authority notification within 72 hours where personal data is affected.

8. TESTING CADENCE

The recovery procedures above are exercised on the following planned cadence:

Exercise	Frequency
Deployment rollback	Quarterly
Database point-in-time restore	Quarterly
Secret rotation drill	Semi-annually
Full disaster-recovery simulation	Annually

This document summarizes Workplacer's business continuity and disaster recovery posture for due-diligence purposes. It should be read alongside our Data Processing Agreement and Information Security Risk Management summary.