

Business Continuity and Disaster Recovery Policy

Dash Media Limited · Version 1.0 · Effective 27 October 2026 · Review by 27 October 2027 · Owner: Brad Hook, Director, Dash Media Limited

1. Purpose

To describe how our products keep running, how data is backed up, and how we recover from outages, data loss, or the unavailability of the operator.

2. What a disruption looks like for our clients

FLAME and the Values Institute are development tools, not operational systems. If the app is unavailable for a day, a workshop can proceed with the printed Field Guide and the assessment can be taken later. No client process depends on the app in real time. This shapes the targets below: we aim for fast recovery, but an outage is an inconvenience, not an emergency for the client's business.

3. Targets

MEASURE	TARGET
Recovery time objective (how long until the app is back)	24 hours for a full rebuild; minutes for a rollback
Recovery point objective (how much data could be lost)	24 hours (daily backups; point-in-time recovery is not enabled)
Availability	We rely on Vercel and Supabase service levels (both publish 99.9% or higher). We don't offer a separate SLA unless agreed in a client contract

4. Backups

- Supabase takes automated daily backups of the production database, retained for 7 days, stored in the same region (Sydney). This is the Supabase Pro plan's standard backup.
- The app stores no files: there are no uploads, and reports are produced on demand from the database, so the database backup is the whole backup.
- Source code is in GitHub, with the full history. Any commit can be rebuilt and deployed.
- Environment configuration (secrets, variables) is held in Vercel and Supabase. A copy of the variable names (not values) is kept in the repository README so the environment can be reconstructed.
- Restore is tested at least annually by restoring a backup to a staging project and checking that the app runs against it. The test date and result are recorded.

5. Recovery scenarios

Bad deployment. Roll back in Vercel to the previous build. Minutes.

Database corruption or accidental deletion. Restore from the most recent Supabase backup to a new project, repoint the application's environment variables, redeploy. Hours.

Supabase region outage. Wait for the provider; their status page is the source of truth. If the outage exceeds 24 hours, restore the latest backup to a Supabase project in another region and repoint. Participants' data residency statement would be updated and clients informed.

Vercel outage. Wait for the provider. The app is a standard Next.js build and could be deployed to another host from the GitHub repository within a day if the outage were prolonged.

Loss of the Director's device. Nothing irreplaceable is stored locally. A new device needs the password manager, authenticator app recovery, and a fresh clone of the repository.

Compromise of an administrative account. See the Incident Response Policy. Recovery codes for every multi-factor-protected account are stored in the password manager. A sealed offline copy is being arranged (October 2026) with the person named in section 6.

6. Continuity of the operator

Dash Media Limited is operated by one person. If the Director is unavailable for an extended period:

- The products keep running without intervention; nothing requires daily operator action.
- Subscriptions to Vercel, Supabase, GitHub, and the domain registrar are paid by card and renew automatically.
- Evgeniya Ignatova (Programme Management, FLAME) holds sealed instructions, being arranged in October 2026, for reaching the password manager and recovery codes, to be used only if the Director is incapacitated, in order to keep services running or to wind them down and return or delete client data.
- Clients would be notified by that person and offered an export of their data.

7. Review

Reviewed annually, after any restore test, and after any disruption.

8. Version history

VERSION	DATE	CHANGE
1.0	2026-10-27	Initial publication