

Business Continuity and Disaster Recovery Plan

Recovery objectives, backup arrangements and the procedures for the failure scenarios that matter.

Version 1.0 · Last reviewed 22 October 2026 · Owner: Security Lead, security@etropo.com · Current version at <https://trust.etropo.com/resources/business-continuity-plan>

1. Purpose

This plan describes how Etropo keeps the service running and recovers customer data when a component fails, and what customers can expect in each case.

2. Architecture that the plan relies on

- The **application** is stateless and runs as serverless functions on Vercel in the fra1 (Frankfurt) region, with static assets on Vercel's global edge. Every deployment is immutable and kept; any earlier one can be promoted back.
- The **database, authentication and file storage** run on Supabase in AWS eu-central-1 (Frankfurt). Supabase operates the database, applies patches and takes backups.
- **Rate limiting and chat state** are in Upstash Redis. If Redis is unreachable, rate limiting fails open so the service stays available.
- **Source code** is in GitHub; **configuration** is in Vercel environment variables, which keep a history.

3. Recovery objectives

Component	Recovery time objective	Recovery point objective	Mechanism
Application	1 hour	0 (no data in the application tier)	Promote the previous Vercel deployment
Database	4 hours	24 hours	Restore the latest daily Supabase backup
Authentication	4 hours	24 hours	Included in the database restore
Configuration	1 hour	0	Vercel environment variable history

Component	Recovery time objective	Recovery point objective	Mechanism
Source code	1 hour	0	Git, with full history on every developer machine

Point-in-time recovery is not enabled on the database today, which is why the database RPO is 24 hours. Enabling it is on the readiness plan and would bring the RPO to minutes.

4. Backups

- Supabase takes an automated backup of the production database every day, encrypted at rest, kept according to the project's plan.
- File storage (avatars, uploaded invoices) is backed up with the Supabase project.
- Integration data (ad spend, synced sheets) can be re-imported from the source systems after a restore, because the connections and their encrypted tokens are in the database.
- Restoring a backup is a provider operation requested by the Security Lead.

5. Scenarios

Bad deployment. Symptoms: errors or wrong behaviour after a release. Action: promote the previous deployment on Vercel (minutes). If a migration accompanied the release, check that it is backward-compatible before promoting; if not, follow the pull request's recovery note.

Database corruption or data loss. Action: stop writes by disabling the affected feature or placing the application in maintenance, request a restore of the last good backup from Supabase into the project, verify, re-enable. Expected time: within the 4-hour objective; data since the backup is lost and customers are told which window.

Regional outage of Vercel (fra1). Vercel's edge network keeps serving static assets. Functions can be redeployed to another region by changing the project's region setting and redeploying; the database stays in Frankfurt and is reachable from any Vercel region.

Regional outage of Supabase (eu-central-1). The service is unavailable until the provider recovers or a restore into a new project in another region is completed. A cross-region restore is not pre-provisioned; it is a manual operation estimated at several hours plus the 24-hour RPO.

Loss of a vendor. Each vendor on the Subprocessors page has a replacement path: email (Resend) and rate limiting (Upstash) can be swapped within a day; AI providers can be switched through the Vercel AI Gateway configuration; monitoring and analytics are not needed to serve customers.

Compromised credentials or keys. Follow the Security Incident Response Plan: rotate in Vercel, redeploy, revoke sessions.

Loss of a key person. Owner access to every system in scope must be held by at least two people, and this plan plus the documentation in the repository must be enough for the second person to operate the service. Today only the Security Lead holds that access. Access for the Infrastructure Lead is being set up in October 2026 (see Roles and Responsibilities).

6. Testing

- A restore from backup into a separate project is tested at least once a year and the result (time taken, data verified) is recorded. Restore tests were carried out in 2025 and in 2026.
- Rollback by promotion is exercised in normal operations whenever a release is reverted.
- The Incident Response Plan tabletop exercise includes one availability scenario.

7. Communication during an outage

Customers are kept informed through the Updates page on this site and by email to organisation admins for outages longer than one hour. Vendor status pages (Vercel, Supabase) are linked from the update.

8. Review

Reviewed annually, after every test, and after any architectural change. Version 1.0, October 2026.

This PDF is a snapshot. The page at <https://trust.etropo.com/resources/business-continuity-plan> is the current version.