

Business continuity and disaster recovery

Version	1.0
Effective date	27 October 2026
Owner	Robin Ashford
Applies to	The Final Frame platform, its data and the company's ability to operate
Review	27 October 2027
MPA CSBP	OR-1.2, OR-1.3

Approved by Robin Ashford, Founder, 27 October 2026

What must keep working

1. Customers can sign in, see their projects and download their content.
2. No customer content or audit trail is lost.
3. Uploads, QC and deliveries resume once service returns.

Generative features (artwork, film reading, enrichment) can wait.

What protects the data

Data	Protection
Cloud SQL (PostgreSQL 17, europe-west2)	Highly available (REGIONAL): primary in europe-west2-a, standby in europe-west2-c, automatic failover. Automated daily backup at 03:00 UTC, 30 kept. Point-in-time recovery, 7 days of transaction logs. Deletion protection on. Query Insights on. Maintenance window Sunday 02:00 UTC. db-autorecover restarts or fails over an instance that stops answering
Org buckets	europe-west2. Soft delete keeps a deleted or overwritten object for 30 days
Per-Org KMS keys	Cloud KMS, europe-west2. A destroyed key makes its bucket unreadable for good
Secrets	Secret Manager, with versions
Container images	Artifact Registry, every release tag kept
Source	GitHub, plus full clones on two Macs
Deploys	The release manifest names each part's release, so any part can be rolled back on its own (see the Change management policy)

Customers keep their own originals of the media they send to Final Frame. Their contract says so.

Recovery targets

RPO is how much data may be lost. RTO is how long until service is back.

Scenario	Target RPO	Target RTO	What delivers it
Bad deploy	0	15 minutes	The part rolled back in one command: API traffic to the previous revision, the app pointer, or the jobs' image

Scenario	Target RPO	Target RTO	What delivers it
Rows deleted or corrupted by a bug or a person	5 minutes	4 hours	Point-in-time recovery to a clone, then copy the rows back
Object deleted or overwritten	0, within 7 days	4 hours	Soft delete restore
Zone failure	0	15 minutes	Automatic failover to the standby in the second zone
Region failure (europe-west2)	Database 24 hours	48 hours	Restore the latest backup in another EU region, rebuild services there from Terraform. Customers hold their own originals
Loss of a Mac	0	1 day	Code is in GitHub. Credentials in the password manager
Loss of Robin for a period	n/a	n/a	See "Key person" below

Database backups stay in an EU location. The availability SLO is the everyday measure: 99.5% of minutes a month on QA, 99.9% on production, with an error-budget policy. Production is built highly available from day one.

Testing

- Record the result in the runbook's rehearsal table. The first rehearsal, on 7 October 2026, took 8 minutes 40 seconds; on 20 October 2026 QA was restored from a backup in a real outage.
- Restore one soft-deleted object once a quarter.
- Tabletop a region loss once a year.
- Record every test in the risk register with the date, the time taken and anything that failed.

Key person

Final Frame has one person. If Robin cannot work:

- The platform runs without intervention. No routine task needs a human.
- A sealed recovery pack, held by a named trusted person, gives access to the password manager and the Google Cloud owner account.
- Customers are told in their contract that Final Frame is founder-run.

Communication during an outage

Robin emails affected Org contacts when an outage passes one hour, and again when it ends. The public status page is www.final-frame.com/status: the live checks, the incidents of the last 90 days and the maintenance windows. Outages count against the SLO.