graine.ai

GRAINE TRUST CENTER · DOCUMENT

Business Continuity Overview

GR-PUB-12 · Version 1.1

Approved — effective 3 November 2026

DOCUMENT ID	VERSION	CLASSIFICATION
GR-PUB-12	1.1	Public

GRAINE AI · MAVRIX AI PRIVATE LIMITED

Document control

DOCUMENT ID	GR-PUB-12
VERSION	1.1
STATUS	Approved
OWNER	Information Security Lead
APPROVED BY	Rishabh Bhanot, Founder (top management), 3 Nov 2026
EFFECTIVE DATE	3 Nov 2026
LAST UPDATED	4 Nov 2026
NEXT REVIEW	By 3 Nov 2027 (12 months after approval), or on a significant change
CLASSIFICATION	Public
APPLIES TO	The Graine AI business platform: the call platform, public API, dashboard and the data stores and vendors they depend on

Contents

1. In short
2. What is in place and what is not
3. What this means in practice
4. Vendors Graine depends on
5. How Graine tells you
6. What you can do
7. Contact
Related documents
Revision history

1. In short

This document describes how Graine AI keeps its platform running and recovers from a failure, and what it does not yet do. It describes the approach, not the full continuity plan. Every statement is true as of 3 Nov 2026.

- Production runs in one AWS region, Mumbai. There is no second site or standby today.
- The primary database is a managed three-node replicated cluster with continuous backup by its provider.
- Graine has set recovery targets: a recovery time objective (RTO) of 24 hours and a recovery point objective (RPO) of 24 hours, with a maximum tolerable downtime of 72 hours. They are targets, not yet proven by a restore test (the first is Planned by 31 Dec 2026), and not a commitment. Graine does not quote an availability percentage.
- A tool that verifies restores is built and Being rolled out; no restore test has been run yet, and the first is Planned by 31 Dec 2026. The continuity and disaster-recovery plan was approved on 3 Nov 2026.

2. What is in place and what is not

AREA	WHAT EXISTS	STATUS
Hosting	The call platform, agents, call records and configuration run in one AWS region (Mumbai)	In place
Primary database	A managed three-node replicated cluster with continuous backup by the provider. Monthly snapshots are kept 12 months under the provider's current settings	In place
Releases	The previous release image is kept, so a release can be rolled back	In place
Monitoring	Health checks and metrics on services, with heartbeats to an external uptime monitor	In place
Restore tests	Scheduled restores of database backups, to show that a backup restores. The verification tool is built; no restore test has been run yet. The first is due by 31 Dec 2026, then one every quarter	Being rolled out (tool); Planned (tests)
Deployment pipeline	A reviewed pipeline with approval, a deploy log, pinned images and one-step rollback	Being rolled out
Certificate renewal	Automatic renewal and an expiry alarm for the certificates that calls depend on	Being rolled out
Continuity and disaster-recovery plan	Written and approved on 3 Nov 2026	Approved (3 Nov 2026)
Recovery time and recovery point targets	RTO 24 hours and RPO 24 hours, with a maximum tolerable downtime of 72 hours, set on 3 Nov 2026. Targets, not yet proven by a restore test and not a commitment	Planned (proof by the first restore test, by 31 Dec 2026)
Second site or standby	None today. A decision is due by 31 Dec 2026	Planned (decision by 31 Dec 2026)

Each Planned item shows its date. Until restore tests run, a backup has not been shown to restore by a repeatable test.

3. What this means in practice

Because there is one region and no standby, a failure of that region or of the servers the call platform runs on would stop calls, chat and the API until Graine restores service. Graine's recovery targets (service back within 24 hours, at most 24 hours of data lost) are not yet proven by a test, so Graine does not commit to a restoration time in advance. A customer who needs a committed recovery time for a time-critical process should ask Graine before relying on the platform for it.

The primary database does not depend on a single machine, and the provider backs it up continuously. A backup protects against loss of data. It does not keep calls running while the platform is down.

4. Vendors Graine depends on

DEPENDENCY	VENDOR	IF IT FAILS
Hosting, load balancer, object storage, secrets store	AWS	The platform is unreachable or degraded
Primary database	MongoDB Atlas	Records and configuration are unavailable
Dashboard and its database	Vercel and Neon	The dashboard is unavailable or degraded
Sign-in	Stytch	People cannot sign in
Call recordings	Wasabi (United Kingdom)	Recordings cannot be stored or played
DNS	Cloudflare	Graine's addresses may not resolve
Telephony, speech recognition, language models, speech synthesis	The providers named on the Sub-processor List, chosen per agent	Calls and chats on agents that use the provider are affected

Graine's recovery from a vendor outage depends on the vendor's own recovery. Most vendors include data processing terms in the terms Graine accepted; Graine does not yet have a signed or downloaded copy on file for any of them, and a few vendors publish none. Filing those copies, confirmed regions and review of the vendors' assurance reports are Planned.

5. How Graine tells you

When a disruption affects a customer, Graine's approach is to tell the customer by email, at the 24-hour contact on record where there is one, and to give an expected restoration time once it knows one. There is no public status page today; one is Planned by 31 Mar 2027. A personal-data breach follows the Incident and Breach Notification Commitments, which set a 24-hour notice. Graine has no staffed 24×7 operations centre; to report a problem at any hour, write to founders@graine.ai.

6. What you can do

1. **Plan a fallback for a call that cannot be placed.** Decide in advance whether the contact is retried later, moved to another channel or passed to a person. You can pause or cancel a campaign from the dashboard.
2. **Make your webhook endpoint safe to receive a repeated or late event.** Graine keeps a log of webhook deliveries for 30 days. After an outage on either side, reconcile from the call records in the dashboard or the API.
3. **Keep your own copy of recordings and records you cannot afford to lose.** Do not treat Graine as your only copy.
4. **Keep a 24-hour contact current,** so a notice reaches someone at any hour.
5. **Keep your own telephony, carrier and provider settings documented,** so you can reconfigure if you need to.

7. Contact

FOR	CONTACT
Continuity questions, incident reports, and your 24-hour contact	founders@graine.ai

Related documents

- Security Overview
- Incident and Breach Notification Commitments
- Sub-processor List
- Data Retention and Deletion

Revision history

VERSION	DATE	CHANGE	APPROVED BY
1.0	2026-11-03	First issue, approved	Rishabh Bhanot, Founder
1.1	2026-11-04	Recordings' storage location corrected: the United Kingdom (Wasabi eu-west-3), not France; vendors' processor terms stated (in their terms or offered; Graine's copy not yet on file)	Correction; the approval of 3 Nov 2026 stands