graine.ai

GRAINE TRUST CENTER · DOCUMENT

Security Overview

GR-PUB-04 · Version 1.4

Approved — effective 3 November 2026

DOCUMENT ID	VERSION	CLASSIFICATION
GR-PUB-04	1.4	Public

GRAINE AI · MAVRIX AI PRIVATE LIMITED

Document control

DOCUMENT ID	GR-PUB-04
VERSION	1.4
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: dashboard, public API, SDKs, and hosted voice, chat and in-app agents

Contents

1. In short
2. About Graine and this document
3. Where we stand
4. How the platform is built
5. Your data: where it lives
6. Workspace isolation, roles, approvals, API keys and sign-in
7. Application and API security
8. Voice and AI specific controls
9. Monitoring, logging and incident response
10. Availability and recovery
11. Vendors and sub-processors
12. People and policies
13. Testing and assurance
14. What you do
15. Reporting a vulnerability and contacts
In place, being rolled out, planned
Related documents
Revision history

1. In short

This document describes how Graine AI protects customer data, and what it does not yet do. Every statement is true as of 3 Nov 2026. A control that is not live for every customer is labelled "Being rolled out" or "Planned".

- Graine holds no SOC 2 report and no ISO/IEC 27001 certificate. Preparation for both is in progress. No independent penetration test has been done; one is planned.
- Workspaces are isolated from each other. Roles and approvals limit what people can do. A hash-chained, append-only audit trail records changes, and customers can verify it.
- The website, dashboard, API and call-streaming sockets accept TLS 1.2 or 1.3 only. Hosting, database and storage providers encrypt stored data.
- Call records, agents and organisation configuration are held in India (Mumbai); call recordings in the United Kingdom; API keys and the knowledge-base index in the United States. Other vendors' locations are on the Sub-processor List, or marked "On request".
- Graine does not use customer data to train or fine-tune AI models.
- Graine tells an affected customer of a personal-data breach within 24 hours of confirming it.
- An incident register and retention controls are In place (since 4 Nov 2026). On-call alerts, backup restore tests and authenticator-app sign-in are Being rolled out. Single sign-on is Planned.

2. About Graine and this document

Graine AI is the trading name of Mavrix AI Private Limited, an Indian company based in Noida and Bengaluru. Graine provides a platform on which businesses build AI agents that place and answer phone calls, run call campaigns, chat on websites, and run inside the customer's own mobile apps through public, MIT-licensed SDKs for iOS, Android, Kotlin Multiplatform, Flutter and React Native.

The founders are Graine's top management and are accountable for security and privacy. Rishabh Bhanot (Founder) is the Information Security Lead and the Privacy and Grievance Officer, appointed on 3 Nov 2026; the Information Security Lead owns this document. Graine's consumer mobile product is separate and outside its scope.

Three status words are used, always with an as-of date:

WORD	MEANING
In place	Works for customers in production today
Being rolled out	Built or being built; not yet live for everyone, or off until a customer switches it on
Planned	Not started; a target date is given where one is set

"In progress" is used only for the SOC 2 and ISO/IEC 27001 programmes.

3. Where we stand

As of 3 Nov 2026:

FRAMEWORK OR ASSURANCE	STATUS	WHAT IT MEANS
SOC 2 Type I and Type II	In progress	Graine is preparing for a Type I audit, to be followed by a Type II observation period. Neither is complete, and only an independent audit firm can issue the report. No SOC 2 report is held.
ISO/IEC 27001:2022	In progress	Graine is building its information security management system to the standard. The audit for a certificate has not taken place. No certificate is held.
India: Digital Personal Data Protection Act, 2023	Aligned controls, programme in place (self-assessed)	There is no DPDP certificate. The DPDP Rules' duties on notice, safeguards, breach, retention, rights and grievances apply from 13 May 2027; Graine applies its process now where it already does.
GDPR	Processor terms on request	Where Graine processes EU personal data for a customer, it acts as processor. A data processing agreement is available on request, with Standard Contractual Clauses for EU or UK data.
HIPAA	Not offered	No business associate agreement is offered.
Independent penetration test	Planned	None has been done. Internal reviews are described in section 13.

4. How the platform is built

COMPONENT	WHAT IT DOES
Dashboard	Where customers manage agents, campaigns, people, billing and the audit trail
Public API	The interface customer systems call, with scoped API keys
Platform API and orchestration service	Runs campaigns, retries, scheduled calls, webhooks, the audit trail and the credit ledger
Agent configuration service	Stores agents, prompts and versions, and applies approved changes
Telephony gateway	Checks that a call is allowed, then places it through the carrier
Real-time session service and voice runtime	Carry the live conversation: audio, speech recognition, language model, speech synthesis, agent tools
Connection gateway for web and in-app sessions	Admits widget and SDK sessions after checking the publishable key and a signed ticket
Knowledge-base service	Searches the documents a customer uploads for its agents

How data moves, and what protects each step:

FROM AND TO	WHAT MOVES	PROTECTION
Browser or customer system to dashboard and public API	Sign-in, settings, requests to place calls and read records	TLS 1.2 or 1.3 only; HSTS (browsers told to use HTTPS only); two-step password sign-in; scoped API key; per-organisation rate limit; role checked on every request
Graine to customer webhook endpoint	Call events and results	HMAC-SHA256 signature over a timestamp and the exact bytes; private addresses refused. A customer should use an HTTPS endpoint
Phone network to telephony gateway to voice runtime	Call set-up and call audio	Call-streaming sockets use TLS 1.2 or 1.3; the telephone leg is the carrier's, with its protection
Widget or SDK to connection gateway to session service	Chat and call media	Publishable key limited to allowed sites and apps; signed single-use ticket; WebRTC media uses DTLS-SRTP
Voice runtime to speech, language-model and voice providers	Call audio, transcripts, text to speak	HTTPS or secure WebSocket; providers chosen per agent; each is on the Sub-processor List
Platform to recording storage (United Kingdom)	Call recordings	Provider encrypts at rest; the dashboard serves recordings through a route that checks permission and agent access
Platform to primary and dashboard databases	Records and settings	Managed providers; encrypted at rest; every read filtered by workspace
Graine service to Graine service	Internal requests	Shared secret checked in constant time; a route with no secret refuses everything; internal-only routes blocked at the load balancer

This document does not claim separate encryption on traffic between Graine's own services.

5. Your data: where it lives

DATA	LOCATION	HELD BY
Call platform, agents, call records, organisation configuration	India (Mumbai)	AWS and the managed primary database
API keys	United States (N. Virginia)	AWS Secrets Manager
Carrier and push credentials	India (Mumbai)	AWS Secrets Manager
Call recordings and voice samples	United Kingdom	Wasabi, third-party object storage
Knowledge-base search index	United States (N. Virginia)	LanceDB Cloud
Dashboard accounts, billing, workflows and consent records	"On request" (see the Sub-processor List)	Neon, a managed database

Recordings are in the United Kingdom today. For Indian data that is a transfer outside India; for EU data, the United Kingdom has an EU adequacy decision. An India storage option for recordings is Planned; no date is set. The shared cloud does not pin a region per customer. A dedicated instance, or the platform on the customer's own compute, is available for single-jurisdiction processing. Air-gapped deployment is not offered. Speech and language providers process data where they run; see the Sub-processor List.

In transit. Section 4 lists each hop. Older TLS versions are refused; this was verified from outside on 3 Nov 2026.

At rest. Graine's hosting, database and object-storage providers encrypt stored data. Customer-managed encryption keys are not offered. Since 4 Nov 2026, the transcript and the rest of the content of each new business-customer call are also encrypted inside the application, in the primary database, with AES-256-GCM under one platform-wide key protected by a cloud key service. Call recordings, calls stored before that date, and the copies Graine's services keep outside the call record are not covered by this layer and rely on the providers' encryption. New device push tokens and customer-connected credentials are also encrypted under per-workspace keys. Extra encryption of phone numbers inside the application, with a keyed index so search still works, is built and Being rolled out; until its key is set in production, phone numbers rely on the providers' encryption. Carrier and push credentials are kept in a managed secrets store; push credentials are write-only and never shown again, even to Graine staff. API keys are held in the secrets store, encrypted at rest; hashed storage for keys is Being rolled out.

Retention. Call records, transcripts, recordings and contacts are kept for the life of the customer's workspace unless the customer deletes them. Retention settings that delete automatically are In place (since 4 Nov 2026); a period applies only once an Admin sets one. These settings, erasing one person and workspace offboarding cover the main database and recording storage; they do not remove the copy of each call kept in a separate working store, which has no expiry. Some data already expires: memory after 365 days by default (phone-keyed memory ends 90 days after the last conversation), the audit trail after 400 days by default, and the Security log after one year (Being rolled out). After a contract ends, Graine deletes the customer's data from live systems within 30 days of the customer's written instruction, apart from that separate copy. Backups age out on the providers' cycle; monthly database snapshots are kept 12 months. From 13 May 2027 the DPDP Rules require personal data, traffic data and processing logs to be kept at least one year and then erased, unless another law requires longer (Rule 8(3)). The Data Retention and Deletion summary has the detail.

No training on customer data. Graine does not use customer data to train or fine-tune AI models. A custom voice is made only from recordings the customer gives for it. What AI and speech vendors do with data sent to them is set by their own terms. Several use content to improve their models by default unless the customer opts out; Graine has decided to opt out wherever a vendor allows it. The setting for one speech-to-text provider is built and being switched on (Being rolled out), and the opt-outs in the other vendors' settings are owner actions (Planned).

6. Workspace isolation, roles, approvals, API keys and sign-in

- **Isolation.** Every request acts only on the caller's own workspace, and an identifier from another workspace answers "not found". An automated test sends a foreign identifier to every route that takes one. Isolation is enforced in the application, over shared databases. Sub-accounts are separate workspaces that only their parent organisation can manage.
- **Roles.** Every member is an Admin, a Member or View only. Admins can create custom roles with exactly the permissions they choose, and can limit a person to chosen agents. Roles are read live on each request, so a change applies without a sign-out.

- **Approvals.** A Member's go-live, change to a live agent or campaign launch can wait for another person's approval. Nobody can approve their own request.
- **API keys.** Keys carry scopes. A key a Member creates can never do more than a Member can.
- **SDK and widget keys.** Publishable keys work only from the websites and apps a customer allows, and are rate-limited. For in-app agents a customer can also require proof of the app (Apple App Attest or Google Play Integrity) and of the user (a signed identity or the customer's own sign-in). Both are available and off until the customer turns them on.
- **Sign-in.** Stytch provides sign-in. A password sign-in asks for a one-time emailed code; sign-in by emailed code or link relies on control of that inbox. Access reviews that an Admin records are In place (since 4 Nov 2026); an authenticator-app step that Admins can require is Being rolled out. Single sign-on is Planned.
- **Graine staff.** Staff can act inside a customer workspace to support it. Staff access is recorded in the workspace's audit trail, and the customer sees it in the Activity log (In place (since 4 Nov 2026)). Per-person staff identities and staff multi-factor sign-in are Being rolled out.

7. Application and API security

- **A permission on every route.** Every route in the API and dashboard declares the permission it needs. An automated test fails the build for any route that does not.
- **Tests.** Automated suites check workspace isolation, the audit chain, webhook signing and fail-closed internal routes. Two suites run in the build pipeline today; every service's tests are Being rolled out.
- **Webhooks and outbound requests.** Webhooks are signed so a customer can verify them. Webhook deliveries and agent API tools refuse private and internal network addresses.
- **Rate limits and browser protections.** The public API is limited per organisation, with the limit in response headers; SDK session routes and public forms are limited too. The API and dashboard send HSTS and other security headers, and a content-security policy runs in report-only mode.
- **Security log and Security page.** The Security log records every in-app security check each agent makes, with its result and reason, and every change to an agent's security settings, with the member who made it. The Security page shows each agent's protection and the workspace's sign-in and key settings.

8. Voice and AI specific controls

- **AI and recording notice.** An agent can be set to open by saying it is an AI and that the call may be recorded, and an Admin can require this workspace-wide. This is built and Being rolled out. Every rule is off until an Admin sets it, and the dashboard setting is not live yet.
- **Redaction.** A customer can turn on redaction per agent: phone numbers, Aadhaar, PAN, card numbers and email addresses are removed from transcripts before they are stored. It targets those identifiers and does not find every personal detail.
- **Masking on the device.** The in-app SDKs mask PAN, Aadhaar, card numbers, phone numbers and email addresses in the screen context, variables and user traits they send on their own, before they leave the device.

- **Memory.** Memory is off until a customer turns it on. What is saved is redacted first and keyed by a one-way hash of the user id, and one person's memory can be erased. When memory is on, it keeps names and health-related facts; this is a platform-wide setting.
- **Member-only voice clones.** A cloned voice is visible only to the member who made it, and nobody else can put it on an agent in Graine.
- **WhatsApp calls.** A WhatsApp call goes out only when a consent from the person being called is on record.
- **Human oversight.** Approvals (section 6), pausing or cancelling a campaign, stopping a call, and transfer to a person where the call route supports it. Every agent has a maximum call length; the default is 5 minutes.

9. Monitoring, logging and incident response

In place. The audit trail is append-only and hash-chained. It holds member ids and roles, not names, emails or phone numbers, and a customer can verify it in the dashboard or the API. The Activity log exports as CSV. Services expose health checks and metrics, with heartbeats to an external uptime monitor. Since 4 Nov 2026 there are also a complete audit export with a chain check, an incident register with notice clocks, and a record of staff access in the customer's audit trail.

Being rolled out. Durable forwarding of audit rows between services; daily anchoring of the chain; alerts to an on-call person; logging of reads of recordings and transcripts; and masking of conversation text in platform logs. Until masking is complete, some service logs can still hold phone numbers or fragments of conversations. Graine has no staffed 24×7 security operations centre.

Commitments.

- Graine tells an affected customer of a personal-data breach within 24 hours of confirming it, and updates the customer at least every 24 hours while it is open. This is a term of Graine's data processing agreement.
- Where the CERT-In Directions of 28 April 2022 apply to Graine, it reports the incidents they specify within 6 hours of noticing them.
- Under the DPDP Rules the Data Fiduciary, usually the customer, tells the Data Protection Board without delay and gives detail within 72 hours (Rule 7(2)). Graine gives the customer what it needs. This applies from 13 May 2027.

10. Availability and recovery

Production runs in one AWS region, Mumbai. The primary database is a managed three-node replica set with continuous backup by its provider. Graine does not quote an availability percentage. Scheduled restores of database backups, to show that a backup restores, are Being rolled out. Top management set recovery targets on 3 Nov 2026: a recovery time objective of 24 hours and a recovery point objective 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 to customers. There is no second site or standby today; a decision on one is due by 31 Dec 2026.

11. Vendors and sub-processors

The Sub-processor List names each vendor, what it handles, where, and the basis for any transfer outside India. Graine gives workspace Admins 30 days' notice before it adds or replaces a sub-processor or changes a region, with a right to object. A provider a customer connects with its own account is the customer's processor, not Graine's. 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, obtaining terms where a vendor has none, confirmed regions and review of vendors' assurance reports are Planned.

12. People and policies

Graine's policy set covers information security, access control, incident response, vendor management, data retention, change management, business continuity, privacy and AI use. Top management (Rishabh Bhanot, Founder) approved the policies on 3 Nov 2026, and customers can request them under a non-disclosure agreement through the Trust Center. They define the roles of top management (the founders), Information Security Lead, Privacy and Grievance Officer, Engineering Lead, people owner and internal auditor. Screening, confidentiality agreements and security training for everyone with access are Planned; none has started.

13. Testing and assurance

Graine ran an internal security review on 6–7 Oct 2026 and a security review of in-app chat and calls on 26 Oct 2026, with fixes made in code. These are internal reviews, not independent tests. An independent penetration test is Planned. The SOC 2 and ISO/IEC 27001 programmes are in progress. Until reports exist, a customer can ask for the policies under a non-disclosure agreement, and Graine will complete the customer's security questionnaire and walk through the architecture with the engineers who built the controls. Graine's data processing agreement sets out how a customer can verify these controls: first through reports, a questionnaire and a technical review, and by audit on notice where the agreement allows it.

14. What you do

Security is shared. Graine runs the platform, and the customer decides how it is used. The Shared Responsibility Matrix lists, for each deployment model, what Graine does and what the customer does. The customer's main duties are:

- Give each person the least role they need, limit people to the agents they need, and remove leavers promptly.
- Keep API keys, publishable-key allow-lists and webhook secrets safe, and verify webhook signatures.
- Review and set the protections a workspace controls: approvals, redaction, memory, verified apps and users, and the AI and recording notice once it is live.
- Tell people they are talking to an AI and may be recorded, obtain the consent the law requires, and respect do-not-call and do-not-disturb rules. A workspace do-not-call list is Being rolled out.
- Choose providers and integrations knowingly. The customer's own carrier, WhatsApp account and integrations run on its accounts.

- Own the legal duties of the party that decides why people are called: answer their requests (Graine helps), tell regulators of breaches, and check that the data locations in section 5 suit the law that applies to you.

15. Reporting a vulnerability and contacts

Report a suspected vulnerability to founders@graine.ai. Graine acknowledges a report within 2 working days. A security.txt file at www.graine.ai names the same contact. Say what you found, where, and how to reproduce it. Do not access, change or keep other people's data, and give Graine reasonable time to fix an issue before you disclose it.

FOR	CONTACT
Security questions, vulnerability reports, security questionnaires	founders@graine.ai
Privacy questions, data-rights requests, grievances (Grievance Officer)	founders@graine.ai, or the request form at www.graine.ai/privacy-policy
Data processing agreement	founders@graine.ai

Graine aims to answer a rights request or grievance within 30 days, and never takes more than 90 days (Rule 14(3)).

In place, being rolled out, planned

As of 3 Nov 2026. The Trust Center at www.graine.ai/trust shows the current status of each control.

AREA	IN PLACE	BEING ROLLED OUT	PLANNED
Access	Workspace and sub-account isolation; roles, custom roles, per-agent access; approvals; scoped API keys; two-step password sign-in; allow-listed SDK keys; verified apps and users (available, off until a customer turns them on); Security log; a permission on every route; and, since 4 Nov 2026, access reviews that an Admin records, removal that also revokes a person's keys and sessions, and a record of staff access in the customer's Activity log	Authenticator app, recovery codes and a workspace setting that requires two-step verification; hashed API keys; per-person staff identities and staff authenticator sign-in	Single sign-on

AREA	IN PLACE	BEING ROLLED OUT	PLANNED
Encryption and network	TLS 1.2 or 1.3 only; browser security headers; encryption at rest by providers; managed secrets store; closed internal routes; signed webhooks; outbound request protection; and, since 4 Nov 2026, encryption of new business-customer call content in the primary database	Phone-number encryption in the application; sealing of internal event messages; signed delivery of call results between our own services; automatic renewal and expiry alarms for the certificates calls depend on	A web application firewall; per-organisation encryption keys for call content; encryption in the application of recordings and of the key-value store's copies of call content
Audit and monitoring	Hash-chained audit trail; Activity log export; health checks and uptime heartbeats; API rate limits on the v2 API; and, since 4 Nov 2026, audit export with chain check and an incident register	Durable forwarding and daily anchoring of the audit chain; alerts to a person; logging of reads of recordings and transcripts; masked platform logs; request limits on the v1 API	—
Privacy and AI	Transcript redaction per agent; memory controls; on-device masking; member-only voice clones; WhatsApp consent record; no training on customer data; an email route for privacy requests and grievances, answered by the Privacy and Grievance Officer; the privacy notice, cookie consent, the request form and published data locations on the website and the Trust Center; and, since 4 Nov 2026, data requests by person, retention controls and workspace offboarding (these do not reach the copy of a call kept in a separate working store)	A data processing agreement on request (a draft is with counsel); AI and recording notice; do-not-call list; default calling hours (off until an Admin switches them on); consent recorded for every dashboard voice clone; redaction by default for new agents; an identity warning on memory; statutory-hold record; short-lived recording links	Per-agent switch to stop recording; India storage for recordings
Resilience and change	Hosting in one AWS region (Mumbai); replicated primary database with provider backups; isolation and audit tests; internal security reviews (not independent tests); the previous release image kept, so a release can be rolled back by hand	Approved production releases with a release record and one-step rollback; restore verification; deploy and change evidence; dependency, secret and container scanning; branch protection	Proof of the recovery targets (RTO 24 hours, RPO 24 hours) by a first restore test, by 31 Dec 2026; a decision on a second site or standby, by 31 Dec 2026

AREA	IN PLACE	BEING ROLLED OUT	PLANNED
Governance	An email contact for security, privacy and grievance reports, answered by the founders; the Sub-processor List and the Trust Center page; the vulnerability-reporting contact and security.txt; the policies, approved on 3 Nov 2026; the Information Security Lead and Privacy and Grievance Officer appointed (Rishabh Bhanot)	—	Vendors' processor terms on file (most are in the terms Graine accepted), confirmed regions and assurance-report reviews; screening, confidentiality agreements and training; SOC 2 audit and report; ISO/IEC 27001:2022 audit and certificate; independent penetration test

The SOC 2 and ISO/IEC 27001 programmes are in progress (section 3). Their audits, and the report and certificate that follow, are Planned.

Related documents

- Sub-processor List
- Shared Responsibility Matrix
- Data Retention and Deletion summary
- Privacy Notice

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; vendor training defaults stated; vendors' processor terms stated (in their terms or offered; Graine's copy not yet on file)	Correction; the approval of 3 Nov 2026 stands
1.2	2026-11-04	Controls live after the 4 Nov 2026 deploy	Status update; the approval of 3 Nov 2026 stands
1.3	2026-11-04	Field encryption of new business-customer call content in place; per-workspace keys for new push tokens and customer credentials	Status update; the approval of 3 Nov 2026 stands
1.4	2026-11-04	What erasure, retention and offboarding do not reach stated	Status update; the approval of 3 Nov 2026 stands