graine.ai

GRAINE TRUST CENTER · DOCUMENT

Incident and Breach Notification Commitments

GR-PUB-11 · Version 1.1

Approved — effective 3 November 2026

DOCUMENT ID	VERSION	CLASSIFICATION
GR-PUB-11	1.1	Public

GRAINE AI · MAVRIX AI PRIVATE LIMITED

Document control

DOCUMENT ID	GR-PUB-11
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	Security incidents and personal-data breaches that affect the Graine AI business platform or its customers' data

Contents

1. In short
2. What Graine tells a customer
3. The clocks
4. The customer's duty, and how Graine helps
5. When Graine is the Data Fiduciary
6. Reaching Graine
7. Severity levels
8. After a serious incident
9. What is in place and what is being rolled out
10. What customers do
Related documents
Revision history

1. In short

As of 3 Nov 2026, Graine AI commits to the following.

- 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 the incident is open. This is a term of Graine's data processing agreement, which is available on request.
- 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 India's DPDP Rules, the customer, usually the Data Fiduciary, must tell each affected person and the Data Protection Board (from 13 May 2027). Graine gives the customer what it needs to do so.
- You can write to Graine at founders@graine.ai at any hour. Graine has no staffed 24×7 operations centre yet.

A personal-data breach is any unauthorised processing, disclosure, alteration, loss or destruction of personal data that harms its confidentiality, integrity or availability. Graine confirms a breach when it has established that one happened. Notice does not wait for the investigation to finish.

2. What Graine tells a customer

The notice goes to the customer's 24-hour contact (section 10) and states, so far as known:

ITEM	WHAT THE NOTICE SAYS
Nature and extent	What happened, and which systems, workspaces and kinds of data were involved
Timing	When it happened and when Graine found it
Data and people affected	The categories of personal data and the approximate number of people and records
Likely consequences	What may follow for the people affected
Measures	What Graine has done and will do to contain it and prevent a repeat
Contact	A person at Graine who can answer questions

If Graine does not yet know everything, it sends what it has and fills in the rest as it learns it. The first notice is not delayed to complete the picture. Updates follow at least every 24 hours while the incident is open.

3. The clocks

WHO	CLOCK	BASIS
Graine to the customer	24 hours from confirming	A contract term. The DPDP Rules set no deadline for a processor to tell its customer
Graine to CERT-In	6 hours from noticing a specified incident	The Directions of 28 April 2022, where they apply to Graine

WHO	CLOCK	BASIS
The Data Fiduciary to each affected person	Without delay	Rule 7(1)
The Data Fiduciary to the Data Protection Board	A description without delay; detailed information within 72 hours	Rule 7(2)

The Rules' breach duties apply from 13 May 2027. Graine applies its process now where it already does.

4. The customer's duty, and how Graine helps

Where Graine processes personal data for a customer, the customer decides why and how it is used and carries the Data Fiduciary's duties. Under Rule 7(1) it tells each affected person, in plain words, what happened, the likely consequences for them, what has been done, how they can protect themselves and whom to contact. Under Rule 7(2) it tells the Board without delay, and within 72 hours adds the broad facts and reasons, the measures taken, any findings about who caused the breach, the steps to prevent a repeat, and a report on the notices given to people.

Graine gives the customer the facts it needs for each step. The 24-hour notice leaves the customer time for its own report.

5. When Graine is the Data Fiduciary

For personal data Graine decides about itself, such as dashboard account details, billing contacts and the requests people send it, Graine is the Data Fiduciary. It then tells each affected person and the Board itself, in the way section 4 describes (Rule 7(1) and 7(2)).

6. Reaching Graine

Send an incident report to founders@graine.ai with "Security incident" in the subject. Say who you are, what you saw, when, and which workspace, agent or key is involved. The founders receive this mailbox.

Graine does not offer a staffed 24×7 security operations centre. Today one founder is on call and is alerted by an external uptime monitor; routing the platform's own alerts to the on-call person is Being rolled out, and a second person for a two-person rota is Planned by 31 Mar 2027. Until then, an out-of-hours response depends on that founder seeing an alert or a report. The 24-hour clock runs from the moment Graine confirms a breach, whatever the hour.

7. Severity levels

Graine's incident procedure, approved on 3 Nov 2026, sorts an incident into one of four levels. The level decides who is brought in and which notices are due. If in doubt, the higher level is used.

LEVEL	WHAT IT MEANS
Critical	A confirmed or likely personal-data breach, one workspace reaching another's data, or the whole platform failing
High	A suspected breach, an exposed high-value credential, or a major service degraded for several customers
Moderate	Limited impact, such as one customer's campaign stuck
Low	Low impact, or a report not yet confirmed

8. After a serious incident

After a Critical or High incident Graine holds a blameless review. It looks at the timeline, the cause and what failed to catch it, not at who to blame. Each lesson becomes a recorded action with an owner.

9. What is in place and what is being rolled out

As of 3 Nov 2026:

AREA	STATUS
An email contact for incident reports, answered by the founders by hand	In place
The same contact published on the Trust Center and in a security.txt file	In place
Hash-chained audit trail and Security log, which customers can read to see what changed in their workspace	In place
Health checks, metrics and heartbeats to an external uptime monitor	In place
Incident register with the notice clocks	In place (since 4 Nov 2026)
Alerts routed to an on-call person	Being rolled out
Recording of Graine staff access in the customer's audit trail	In place (since 4 Nov 2026)
Logging of reads of recordings and transcripts	Being rolled out
Written incident procedure, approved on 3 Nov 2026	Approved (3 Nov 2026)

10. What customers do

1. Keep a 24-hour contact current: a person or team, an email address watched at all hours, and a phone number. Give it to Graine in writing. Graine cannot notify a customer whose contact is out of date.
2. Tell Graine at once about anything unexpected in the workspace, such as unknown members, unfamiliar API keys or calls nobody started.
3. Know your own duties to the Board and to the people you call, and to CERT-In where its Directions apply to you.

Related documents

- Security Overview
- Vulnerability Disclosure Policy
- Business Continuity Overview
- 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	Controls live after the 4 Nov 2026 deploy	Status update; the approval of 3 Nov 2026 stands