graine.ai

GRAINE TRUST CENTER · POLICY

Vulnerability Disclosure Policy

GR-PUB-09 · Version 1.0

Approved — effective 3 November 2026

DOCUMENT ID	VERSION	CLASSIFICATION
GR-PUB-09	1.0	Public

GRAINE AI · MAVRIX AI PRIVATE LIMITED

Document control

DOCUMENT ID	GR-PUB-09
VERSION	1.0
STATUS	Approved
OWNER	Information Security Lead
APPROVED BY	Rishabh Bhanot, Founder (top management), 3 Nov 2026
EFFECTIVE DATE	3 Nov 2026
LAST UPDATED	3 Nov 2026
NEXT REVIEW	By 3 Nov 2027 (12 months after approval), or on a significant change
CLASSIFICATION	Public
APPLIES TO	www.graine.ai, the Graine dashboard, api.graine.ai, the Graine SDKs, and hosted web and in-app agents

Contents

1. In short
2. Scope
3. How to report
4. What we do
5. Rules for researchers
6. Safe harbour
7. Rewards
8. Contact
Related documents
Revision history

1. In short

If you find a security weakness in Graine AI's systems, tell us at founders@graine.ai. Graine acknowledges every report within 2 working days, assesses it, keeps you informed and fixes confirmed issues. A security.txt file at www.graine.ai names the same contact and points to the Trust Center, where this policy is published. As of 3 Nov 2026, Graine does not run a paid bounty programme.

2. Scope

IN SCOPE	WHAT IT COVERS
www.graine.ai	The website, the Trust Center, the documentation and the public forms
The dashboard	Where customers manage agents, campaigns, people, billing and the audit trail
api.graine.ai	The public API, including API keys and publishable keys
The SDKs	The public, MIT-licensed SDKs for iOS, Android, Kotlin Multiplatform, Flutter and React Native
Web and in-app agents	Hosted chat and call agents that run in a customer's website or app, including the checks that admit a session

Examples of what to report: one workspace reaching another's data; a way around sign-in, roles, approvals or key limits; injection; flaws in webhook signing or session tickets; exposed secrets; and a way to make Graine send requests to internal addresses.

Out of scope

- Customers' own systems: their websites, apps, telephony accounts, webhook endpoints and integrations.
- Services run by other companies, such as hosting, speech, language-model, telephony and email providers. Report a flaw in their service to them; if it comes from the way Graine uses it, tell us too.
- Automated scanner output with no demonstrated impact, and missing headers or settings with no demonstrated impact.
- Denial-of-service testing, social engineering and physical attacks (see section 5).
- Anything not listed above. If you are unsure, ask at founders@graine.ai before you test.

3. How to report

Email founders@graine.ai, in English. Graine does not publish an encryption key for reports today, so keep live secrets and other people's personal data out of the first message, and say if you need another channel. Please include:

1. **Where:** the address, API route, SDK and version, or agent you tested.
2. **What:** the type of weakness and the impact you believe it has.
3. **How:** the steps, requests or proof of concept needed to reproduce it. Use accounts and phone numbers you own.
4. **When:** the time you tested and your source address, so we can find it in our logs.

5. **Who:** how to reach you, and whether you want to be credited, and under what name.

4. What we do

1. **Acknowledge** your report within 2 working days.
2. **Assess** it: we reproduce the issue, judge its severity, and work out which customers or data could be affected.
3. **Keep you informed:** we tell you what we found and update you as the fix progresses. We do not promise a fixed repair time, because it depends on severity and complexity.
4. **Fix** confirmed issues, and tell you when the fix is live so that you can retest.
5. **Credit you,** if you wish, by the name you choose, in any public note we publish about the fix.

An issue that exposes customer data, or lets one workspace reach another, is handled as a security incident under the Incident and Breach Notification Commitments. We use your report and contact details only to assess, fix and reply to you, and do not share your name without your agreement unless the law requires it.

5. Rules for researchers

1. **Keep to your own data.** Test only with accounts you created. Do not access, change or delete another customer's data. If you reach it by accident, stop, do not read or keep it, and tell us.
2. **Take the least data that proves the issue.** One record, or the first few characters of a value, is enough. Do not copy, download or store more.
3. **Do not disrupt service.** No denial-of-service attacks, flooding or load tests. Calls are live conversations with real people, so do not place calls or send messages to anyone who has not agreed to take part.
4. **No social engineering and no physical attacks.** Do not phish, call or message Graine staff, customers or the people their agents talk to, and do not enter any office or facility.
5. **Do not test customers' integrations.** A customer's webhook endpoint, telephony account or app built with our SDKs belongs to that customer.
6. **Report promptly,** once you have confirmed the issue, and do not make any demand in return for a report.
7. **Give us reasonable time.** Do not publish or share details until we have said the issue is fixed or we have agreed a date with you.

6. Safe harbour

Graine supports good-faith security research that follows this policy and will not threaten researchers who follow it with legal action. The formal wording of a safe-harbour commitment is under legal review (target 31 Dec 2026); Graine will publish it here once counsel has approved it.

The commitment is meant for research that follows section 5 and stays within section 2. It cannot speak for customers or vendors, whose systems are out of scope.

7. Rewards

We do not run a paid bounty programme at present, so we cannot offer payment for a report. We credit you on request (section 4).

8. Contact

FOR	CONTACT
Vulnerability reports and questions about this policy	founders@graine.ai

Related documents

- Security Overview
- Incident and Breach Notification Commitments
- Sub-processor List
- Privacy Notice

Revision history

VERSION	DATE	CHANGE	APPROVED BY
1.0	2026-11-03	First issue, approved	Rishabh Bhanot, Founder