

Vulnerability Disclosure Policy

How to report a security vulnerability in Gradii, what we commit to in return, and the safe-harbour terms for good-faith research.

VERSION	EFFECTIVE	OWNER	REVIEW	CLASSIFICATION
1.0	9 October 2026	Security Lead (Founder)	Annual	Public

Our commitment

If you believe you have found a security vulnerability in Gradii, we want to hear from you. We will work with you to understand and fix it, and we will not pursue legal action against research done in good faith under this policy.

How to report

Email team@gradii.ai with "Security" at the start of the subject line. Please include:

- the affected URL, endpoint or component;
- a description of the issue and its potential impact;
- step-by-step instructions or a proof of concept that lets us reproduce it;
- your name or handle, if you would like to be credited.

Our contact details are also published in machine-readable form at <https://gradii.ai/.well-known/security.txt>.

Please do **not** report vulnerabilities through social media, public issue trackers or the in-product support chat.

What we commit to

Step	Target
Acknowledge your report	Within 3 business days
Initial assessment and severity	Within 10 business days
Fix for critical and high severity	Within 30 days of confirmation
Fix for medium and low severity	Within 90 days of confirmation
Status updates	At least every 14 days until resolved

We will tell you when the issue is fixed. With your permission, we will credit you in our acknowledgements.

In scope

- `gradii.ai` and `www.gradii.ai`, including the web application, dashboards and candidate interview pages
- The Gradii public API (`/api/v2`) and its sandbox
- Embeddable widgets served from `gradii.ai` (careers page, interview and verification embeds)

Out of scope

- Third-party services we use, such as Cashfree, DigiLocker, Plivo, Resend and our cloud providers. Please report those to the vendor directly.
- `docs.gradii.ai` and `status.gradii.ai`, which are hosted by third parties and hold no customer data. Reports there are welcome but are not covered by the response targets above.
- Denial-of-service, load or volumetric testing
- Social engineering, phishing or physical attacks against Gradii staff, customers or candidates
- Automated scanner output without a demonstrated, exploitable impact
- Missing best-practice headers or flags without a concrete attack, clickjacking on pages with no sensitive actions, and self-XSS
- SPF/DKIM/DMARC configuration reports without a demonstrated spoofing impact
- Rate-limit findings on non-sensitive endpoints

Rules of engagement

To stay within safe harbour:

1. **Use your own accounts.** Create a free workspace for testing. Do not access, modify or delete data that belongs to other customers or candidates.
2. **Stop at proof.** If you reach personal data, stop, do not download or keep it, and report immediately. Access only the minimum needed to show the issue.
3. **No disruption.** Do not degrade service for other users, send messages to real candidates, place real phone calls or trigger paid verification checks.
4. **Keep it confidential.** Give us a reasonable time to fix the issue before you disclose it publicly. We ask for 90 days, or less if we agree a fix has shipped.
5. **Follow the law.** Comply with all applicable laws, including the Information Technology Act, 2000.

Safe harbour

If you make a good-faith effort to follow this policy, we will:

- treat your research as authorised, and not bring or support legal action against you for it;
- not report you to law enforcement for activity within this policy;

- if a third party brings legal action over activity within this policy, make it known that your actions were authorised by us.

This safe harbour does not cover activity that breaches the rules above. It also cannot bind third parties or authorities outside our control.

Rewards

Gradii does not currently run a paid bug bounty. We publicly thank researchers who report valid issues, with their consent. Where a report is exceptional, we may offer a reward at our discretion.

Legal requirements on Gradii

Some vulnerabilities may also be cyber security incidents that Gradii must report to CERT-In under its Directions of 28 April 2022, or personal-data breaches under the Digital Personal Data Protection Act, 2023. Reporting to us does not create any obligation for you to report to those authorities.

Manjari Technologies Private Limited ("Gradii") · 316, Neelkanth Corporate Park, Vidyavihar West, Mumbai, Maharashtra, India · gradii.ai/trust-vault

The current version of this document is published at gradii.ai/trust-vault. Printed or downloaded copies are uncontrolled.