

Security & Privacy Overview

How Gradii protects hiring data: where it lives, how it is encrypted, who can reach it, and what we have and have not been audited for.

VERSION	EFFECTIVE	OWNER	REVIEW	CLASSIFICATION
1.0	9 October 2026	Security Lead (Founder)	Every six months	Public

About this document

Gradii is an AI hiring platform operated by Manjari Technologies Private Limited, Mumbai, India. Recruiting teams use it to source, screen, interview, call and background-verify candidates. That means Gradii processes personal data about people who are not our customers: candidates. We treat that as the central fact of our security programme.

This overview is written for security reviewers, procurement teams and candidates. It describes controls that are **in place today**. Where something is in progress or planned, we say so. The detailed policies behind each section are available under NDA from gradii.ai/trust-vault.

Certifications. Gradii has not yet completed a SOC 2 or ISO/IEC 27001 audit. Our controls are mapped to both frameworks and to India's DPDP Act 2023, and we publish our status for each on the Trust Vault rather than claiming badges we do not hold.

Where your data lives

All primary stores of customer and candidate data are in India.

Store	Provider	Region	What it holds
Application servers	DigitalOcean	Bengaluru, India	The Gradii web app and API
Primary database	DigitalOcean Managed PostgreSQL	Bengaluru, India	Accounts, jobs, candidates, scores, audit logs
File storage	Microsoft Azure Blob Storage	Central India (Pune)	Resumes, interview recordings, verification documents
Cache and sessions	Redis Cloud on AWS	Mumbai, India	Short-lived sessions, OTP state, rate-limit counters

Store	Provider	Region	What it holds
Voice agent runtime	Pipecat Cloud	Asia-South	Live audio for Iris voice calls while a call is running

Some AI and communication providers process data outside India while performing a request, for example a language model scoring an interview transcript. Each one is listed, with its purpose and location, in our public [Sub-processor List](#).

Encryption

- **In transit.** gradii.ai accepts TLS 1.2 and 1.3 only. HTTP Strict Transport Security is set for one year on gradii.ai and all subdomains. Connections from the application to PostgreSQL are TLS-encrypted, and the database rejects connections without TLS. Enabling TLS on the connection to our Redis cache is in progress.
- **At rest.** The managed database, its backups and Azure Blob Storage are encrypted at rest by the provider with AES-256.
- **Application-level.** Third-party OAuth tokens that customers connect (for example calendar and LinkedIn) are additionally encrypted by Gradii with AES-256-GCM before they are stored, using a key held outside the database.
- **Passwords** are hashed with bcrypt (cost factor 12). API tokens are stored only as bcrypt hashes; the plaintext is shown once at creation.

Identity and access

For customers:

- Sign-in with email and password, Google, Microsoft Entra ID, Okta or any SAML 2.0 identity provider.
- Time-based one-time-password (TOTP) two-factor authentication.
- Role-based access with owner, recruiter, hiring-manager and interviewer roles. Users provisioned just-in-time through SSO start with the least-privileged role.
- Every workspace is a separate tenant. Customer data is scoped to the company of the signed-in user, and ownership checks on sensitive routes are covered by automated tests.
- Repeated failed sign-ins are rate-limited. Automated tests cover brute-force, MFA bypass and password-reset abuse.

For Gradii staff:

- Production servers accept SSH keys only. Password and keyboard-interactive login are disabled, and root cannot log in with a password.
- Production access is limited to named engineers who need it. Secrets live in server environment files, never in source control.
- The application runs as an unprivileged user that is blocked by firewall rule from reaching the cloud metadata service, so a server-side request forgery bug cannot read infrastructure credentials.

Candidate data and consent

- **Consent before verification.** Background checks run only after the candidate gives consent. Document retrieval uses DigiLocker, India's government document wallet. The candidate signs in there and chooses what to share, and each DigiLocker request is recorded in an audit log.
- **Interview integrity.** Interview recordings are split into chunks, and each chunk is SHA-256 hashed when it is captured. Any later change to a recording can be detected.
- **Recording is visible.** A recording indicator is shown throughout every recorded interview.
- **AI supports, people decide.** AI scores and summaries help hiring teams; they do not make the hiring decision. We are standardising an explicit AI-disclosure notice across every candidate entry point. See our [AI in Hiring Transparency Notice](#).
- **No model training on customer data.** Gradii does not train or fine-tune foundation models on customer or candidate data.

Retention and deletion

Data	Retention	How it is enforced
One-time passcodes	7 days	Nightly scheduled job
Archived Sparky assistant conversations	15 days after archiving	Nightly scheduled job
HRMS API usage logs	90 days	Nightly scheduled job
Security audit logs	365 days	Nightly scheduled job
Webhook and voice-event diagnostic payloads	30 days	Operator-run purge with dry-run preview
WhatsApp and email message bodies	180 days	Operator-run purge with dry-run preview
Candidate interview data	6 months by default; configurable per customer	On request or at contract end

Customers can request deletion of their workspace or of individual candidates at any time. The full schedule is in our Data Retention & Deletion Policy (available under NDA).

Application security

- Every change to the main branch passes an automated gate before it can deploy: type checking, linting and the full test suite, including dedicated security regression tests.
- Static analysis (SonarQube) is run against the codebase.
- Security headers are sent on every response: HSTS, `X-Content-Type-Options`, `Referrer-Policy`, `Permissions-Policy`, and a `frame-ancestors` policy that limits embedding to approved partner domains.
- Inbound webhooks from payment, messaging and email providers are verified by signature before they are processed.

- Public endpoints are rate-limited through Redis, with an in-memory fallback so that limits still apply during a cache outage.

Infrastructure and operations

- The server firewall exposes only SSH, HTTP and HTTPS. Database and cache are managed services reached over TLS.
- Operating-system security updates install automatically.
- Each deploy builds a new release directory, so a bad release can be rolled back to the previous one in minutes.
- The managed database takes daily backups and supports point-in-time recovery.
- Component health is monitored continuously and published at status.gradii.ai.

Incidents

We keep a written incident response plan with defined severities, an on-call escalation path and regulatory timelines:

- Customers affected by a confirmed personal-data breach are notified without undue delay.
- Reportable incidents are reported to CERT-In within six hours.
- Breaches are reported to the Data Protection Board of India as the DPDP Rules require.

What is in progress

We would rather tell you than have you find out:

- **Independent penetration test.** Planned. Internal security testing and automated regression tests run today.
- **SOC 2 Type II.** Planned. Controls are being mapped and evidence collected.
- **Content Security Policy (script-src).** In progress. A full policy needs an audit of inline scripts first.
- **Web application firewall.** Planned.
- **Formal security awareness training records** for all staff. In progress.

Contact

- Security questions and vulnerability reports: team@gradii.ai with "Security" in the subject. See our [Vulnerability Disclosure Policy](#) and </.well-known/security.txt>.
- Privacy requests and grievances: team@gradii.ai, attention Grievance Officer.

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.