

Infyva security overview

Version 2026-10-19, generated October 20, 2026. This document lists only controls that are live today. The current version is always at <https://www.infyva.ai/trust>.

Hosting and data location

The application, database and file storage are hosted in the United States by Railway Corporation. Every company that processes personal data for us (10 today) is listed at <https://www.infyva.ai/legal/subprocessors>.

Encryption

- All traffic to the app and the API uses HTTPS (TLS). The API sends HSTS and a strict content security policy.
- Field-level encryption at rest (AES-256-GCM envelope (per-value data key wrapped by a key-encryption key)) for: Interview answer transcripts, Consent record IP address, Consent record browser details, Accommodation requests, Phone numbers on candidate profiles, resumes and text message settings, Resume files.

Access and account controls

- **Tenant isolation.** Every API request is checked against the user's company and role, so one company cannot see another company's candidates.
- **Password storage.** Passwords are stored as bcrypt hashes. Sign-in tokens are short-lived and refresh tokens live in HTTP-only cookies.
- **Staff multi-factor authentication.** Infyva admin accounts must sign in with two-factor authentication. Support sessions that view a customer account are read-only, enforced on the server.
- **Two-factor authentication for your team.** Any user can turn on two-factor authentication with an authenticator app.
- **Required two-factor authentication.** Workspace owners can require two-factor authentication for every member. (Enterprise plan)
- **IP allowlist.** Limit sign-in to your workspace to the IP ranges you list. (Enterprise plan)
- **Session timeout.** Set how long a signed-in session may stay idle before it ends. (Enterprise plan)
- **Password policy.** Set minimum password rules for your workspace. (Enterprise plan)
- **Access review export.** Export who has access to your workspace and their roles, for periodic reviews. (Enterprise plan)
- **Platform audit log.** Every Infyva admin action is logged with who, what, why, when and from which IP address.
- **Workspace audit log.** Owners and admins can see the actions taken in your workspace and export them. (Enterprise plan)
- **Private recordings.** Recordings are kept in private storage, played only through short-lived signed links and deleted after 90 days.
- **Abuse limits.** Sign-in, password reset and privacy requests are rate limited.
- **Log filtering.** Application logs and error reports are filtered to strip email addresses, sign-in links, one-time codes and API secrets.

Data retention and privacy

- Recordings are deleted after 90 days; transcripts and reports after 2 years. The full schedule is at <https://www.infyva.ai/legal/privacy#retention>.
- Data Processing Agreement version 2026-10-19b: <https://www.infyva.ai/legal/dpa>.
- Privacy requests are answered within 30 days: <https://www.infyva.ai/privacy-request>.
- If a security incident affects personal data, customers under the DPA are told within 72 hours. Service status: <https://www.infyva.ai/status>.

What we do not claim

- We do not have a SOC 2 report or an ISO 27001 or ISO 42001 certificate.
- We do not publish penetration test results or promise an annual test.
- We have not had an independent bias audit.

Contact and vulnerability reports

Security questions, questionnaires and vulnerability reports: security@infyva.ai. Please do not access other people's data while testing. Our disclosure details are at <https://www.infyva.ai/.well-known/security.txt>.