Security Overview

visibilityhr.com/security · Effective January 1, 2027 · Replaces the Security Overview effective October 1, 2026

Visibility HR, LLC provides the Visibility HR platform. Our clients trust it with the information of the people they hire and develop. This page describes how we protect it. A more detailed description of our controls is available to clients on request, and our Privacy Statement explains how the information is used.

Where the platform runs

The platform is hosted on Amazon Web Services in the United States. Production runs in an east-coast region; backups are kept for a rolling fourteen days in a separate west-coast region. Each client has its own database. Client data stays in our AWS environment. It is not kept on staff computers or in our offices, except a temporary copy when a specific support case or test requires it; each copy is approved, logged, and deleted within seven days.

How data is protected

All traffic between browsers, integrations, and the platform is encrypted in transit using TLS. Passwords are stored only as salted hashes. The platform sits behind multiple firewalls with intrusion detection, antivirus protection, and 24-hour network monitoring with a rapid-response team. Access within the platform is role-based, so a client controls which of its users can see which records, and activity is logged.

Who can reach it

Access to production systems is restricted to a small number of named Visibility HR staff who need it to run and support the platform. Server access requires multi-factor authentication, and reaching client data requires a further authentication step. Staff are trained on data protection when they join and annually. We do not use client data for anything other than providing and supporting the platform, and we never use it to train artificial-intelligence models. Our AI provider does not use client data sent through its API to train its models either.

Our service providers

A short list of service providers helps us run the platform: AWS for hosting, Amazon SES for email delivery, Affinda for resume parsing, Hireflix for one-way video interviews when a client turns them on, and OpenAI for AI-assisted drafting and summaries when a client uses those features. Each is bound by contract to protect client data and use it only to provide its service. Clients can also connect services they contract with directly, such as Indeed, screening partners like Verified First, other job boards, and integrations built for that client; data goes to those services only when the client turns them on. The current lists, with processing locations, are in Section 2.5 of our Privacy Statement and at visibilityhr.com/terms, and clients receive 30 days' notice before a new service provider handles client data.

If something goes wrong

We maintain a documented incident response plan, reviewed and updated on an ongoing basis. Any staff member who suspects a data incident must alert our CEO and COO within 24 hours. Our response team assesses the incident within 48 hours of being convened, contains it, and documents the cause and the fix. If client data has been accessed, disclosed, or lost without authorization, we notify the affected client without undue delay and in any event within 48 hours of confirming the incident, with what we know, what we have done, and what we recommend, and we support the client with the information it needs for any notices it owes to its people or to regulators.

When a subscription ends

A client may request a full export of its data within ten days after its subscription ends, delivered in a standard format. We delete the client's database from production within 30 days after the subscription ends and from backups within 180 days after that, unless the law requires us to keep something longer.

Testing and review

We run vulnerability scanning on the production environment using AWS security tooling and an independent security consulting firm, and address findings by severity. An independent penetration test is performed annually. We review this page and the controls behind it at least annually and whenever the platform changes in a way that affects security.

Questions

Clients and prospective clients can request our detailed security description, complete a security questionnaire with us, or ask about a specific control by writing to privacy@visibilityhr.com or contacting their account team.