ATSway

Security & data statement

You are about to put an entire business into a piece of software. These are the answers to the questions you should be asking - including the ones we would rather you did not.

Generated 16 September 2026. This document is produced from the same source as the security page on our website, so the two cannot disagree.

How the software protects your data

Your data stays in India

ATSway is delivered as your own instance on infrastructure you choose. Most agencies run it in an Indian region, which keeps candidate data inside the country and makes the DPDP question a short one. There is no shared multi-tenant database holding your candidates next to a competitor's.

Encrypted in transit, and at rest where it matters

Every request is HTTPS. Passwords are hashed with Argon2id - not encrypted, hashed, so nobody including us can read one back. Third-party keys you paste into Settings are encrypted in the database with AES-256-GCM under a key held outside it.

Sessions that can actually be revoked

A short-lived signed cookie carries who you are; a long refresh token in the database keeps you signed in and is single-use. Removing a teammate ends their session immediately rather than whenever their cookie happens to expire. A workspace can shorten the session length, restrict sign-in to its own network, and require everybody to set a new password.

Permissions that hold across every screen

Roles decide who works the desk, who sees rates and margins, and who changes the workspace. A recruiter can be held to their own client accounts - and that rule is applied in the queries themselves, so it holds on the reports and the CSV export too, not only on the buttons.

An audit trail you can read

Every stage move, email, decision, export and settings change is written to an append-only activity log with who did it and when. Sign-ins are recorded too, successful and failed, with the device and address. It is on screen in Settings, filterable, and it is the same log the product itself reads - not a separate feed that can quietly stop.

Identifiers are masked before they are stored

An Aadhaar or PAN number typed into the document vault is reduced to its last four characters on the way in. The full number is never written to the database, so it is not in a backup either.

Backups are yours, on your schedule

The whole product is one application and one MySQL database. A nightly dump plus your provider's volume snapshots is a complete backup, restorable without us - we recommend nightly, retained 30 days. Separately, an owner can download the entire workspace from Settings at any moment: every module as a spreadsheet, the settings, and the CVs, in one zip.

One server, nothing phoning home

No analytics scripts, no session recording, no third-party tag on any signed-in page. The app talks to your database, your mail server, and whichever integrations you switch on yourself.

Who else can see it

Your hosting provider

Whoever you run the instance on. You choose them, you contract with them, and we never hold credentials for it.

Your mail server

The SMTP host or connected mailbox you configure. Email the product sends passes through it - candidate names and the message body, nothing else.

An AI provider, only if you enable AI

CV parsing, screening and matching are optional and run on your own API key. When they are off, no candidate text leaves your instance. When they are on, the text of the CV or job being processed is sent for that one request under the provider's commercial terms, which exclude training.

Integrations you connect yourself

An e-signature or assessment vendor, a WhatsApp business provider, a GST portal for e-invoicing. Each is off until you paste a key into Settings, and each receives only what that feature needs.

Us - by exception, not by default

We have no standing access to your instance. If you ask for help with something we cannot reproduce, you grant access for that piece of work and withdraw it afterwards; the activity log records what was done.

If something goes wrong

Detect and contain

Whoever notices - you or us - raises it immediately. The first action is containment: revoking sessions, rotating the affected keys, or taking the instance off the network if that is what it takes.

Tell you within 24 hours

For any incident that touches your data you hear from us the same working day, in writing, with what we know so far - including that some of it is unknown. A silence while we investigate is not an option we take.

Establish what was reached

The activity log and the sign-in history are the record. Because both are append-only and cover every read that leaves the building - every export, every backup - the scope of an incident is a question with an answer rather than an estimate.

Report and remediate

Under the DPDP Act a personal-data breach is reportable to the Data Protection Board and to affected people. We prepare that notification with you, since you are the Data Fiduciary and we process on your behalf. Afterwards you get a written post-mortem: what happened, what we changed, and by when.

Where we stand under the DPDP Act

You are the Data Fiduciary; we are the Data Processor

Your agency decides why and how candidate data is processed. We supply the software and act on your instructions. On a delivered instance this is not a legal fiction - the database is yours and we hold no copy.

Consent and notice are built into the form

The careers page tells an applicant who is collecting their data and what for, before they submit it. Screening answers are recorded as asked, and nothing is inferred about them that they were not told about.

The right to access is one button

Any staff member can produce everything held about a candidate - profile, applications, interviews, documents, messages and notes - as a single file, without a ticket to us.

The right to erasure, without breaking the ledger

A candidate who asks to be forgotten is anonymised rather than deleted: name, contact details, CV and free text go, and the placement they were part of survives as a record with no person attached. Deleting the row outright would destroy an invoice that a tax authority has a copy of, which the Act does not ask for and the law does not allow.

Retention is your policy, and the product helps you keep it

Nothing is deleted automatically, because a retention period is a decision for your business. Settings shows what is stale so the decision is an informed one.

What we deliberately do not do

We do not train models on your data

AI features are optional and run on your own API key. Your candidates and clients are never used to train anything, by us or by the model provider under their commercial terms.

We do not sell or share your database

There is no shared talent pool, no cross-agency matching, and no arrangement where your candidates become someone else's search results. Your instance is yours.

We do not hold your data hostage

One click in Settings produces the whole workspace as a zip of spreadsheets that open in Excel. Invoices export in the format Tally and Zoho Books read. If you leave, you leave with everything, without asking us for it.

We are not ISO 27001 or SOC 2 certified - yet

Those audit an organisation, not a codebase, and we would rather say so than imply a certificate we do not have. The ISO 27001 process is underway. Everything above is something you can verify on your own instance today, and if your procurement needs a questionnaire filled in, send it - we answer honestly, including where the answer is no.