

How we protect your payroll & HR data

Payroll data is the most sensitive data an employer holds. i-Tavi Pay is built on a security model that keeps customer data off the application server, encrypts it end to end, isolates every tenant, and records every action in an immutable audit trail. This overview summarises the controls in place; a fuller technical pack is available to IT and compliance teams on request.

DATA RESIDENCY & ARCHITECTURE

- All customer data — including uploaded documents, stored as bytes in the database, not on disk — lives in a managed **PostgreSQL database in AWS Sydney**, encrypted at rest by the platform.
- The **application server holds no customer data at rest**: it runs code only. Compromising the app host exposes no payroll records.
- Secrets (DB credentials, API keys) live in server configuration, **never in source control**.

ACCESS CONTROL & AUTHENTICATION

- Nine predefined roles with granular per-module permissions.
- **Multi-factor authentication (TOTP) enforced for administrators**.
- Per-account lockout, CSPRNG one-time codes, bcrypt password hashing.

AUDIT & RETENTION

- Append-only, **immutable audit log** on every significant create, update and delete.
- 7-year records retention by default (Employment Relations Act s.45).

NETWORK & APPLICATION SECURITY

- Hardened Ubuntu host, automatic security patching.
- Host firewall (default-deny), SSH key-only, fail2ban.

ENCRYPTION

- **At rest**: AES-256, platform-managed.
- **In transit**: TLS 1.3 (TLS 1.0/1.1 refused), HSTS enforced.
- The off-site backup bundle is client-side encrypted (GPG / AES-256) — a leaked backup token is not live access.

MULTI-TENANT ISOLATION

- Every query is scoped by tenant; **PostgreSQL row-level security** as defence-in-depth.
- Independent isolation audit across all API routes, plus a live breach probe — **no cross-tenant leakage**.

BACKUPS & RECOVERY

- AWS Sydney database with **point-in-time recovery** (RPO in minutes).
- Independent encrypted backups daily to **two providers and regions** (Backblaze B2 + Cloudflare R2); 30-day and 12-month retention; automated restore verification with dead-man's-switch monitoring.

- nginx with enforced security headers and Content-Security-Policy.
- Web-application firewall (ModSecurity + OWASP Core Rule Set) and rate limiting.

ASSURANCE & ROADMAP

In place today

- Independent security review, findings remediated
- Encryption, tenant isolation, MFA, WAF, immutable audit (above)
- Daily dual-region encrypted backups + PITR

On the roadmap

- **SOC 2** — readiness programme underway; timeline on request
- **Independent penetration test** — being scheduled with CREST-accredited firms
- **ISO 27001** — under consideration · **SSO/SAML** — planned

No SOC 2, ISO 27001 or completed third-party penetration test is claimed at this time. i-Tavi Pay is operated by **Pro Accountants**, a Fiji chartered accounting practice and Registered Tax Agent that runs its own payroll on the platform.