HONEST CONTROLS — NO UNEARNED BADGES

How we protect client and talent data.

Encryption, tenant isolation, monitoring, and subprocessors — plus a clear statement of what we can and cannot attest to today.

In production

TLS, hashed auth, PostgreSQL RLS, RBAC, Stripe for cards, CI secret scanning, scheduled BOLA checks.

Multi-tenant

Company workspaces are isolated. Cross-tenant access is forbidden — even when jobs start on a bot.

Contact

security@weremoteit.com for vulnerabilities, controls questions, and DPA requests.

We are not SOC 2 or ISO 27001 certified today, and we do not publish a SOC 3 summary. This leave-behind matches the live /security page.

CONTROLS IN PRODUCTION TODAY

Web portal, Telegram, and Discord hiring flows.

Transport & identity

- HTTPS/TLS for browser and bot traffic
- Supabase Auth — passwords hashed, never plaintext
- Role-based access: client, talent, admin

Tenant isolation

- PostgreSQL row-level security (RLS) by workspace
- Company-scoped jobs, billing, applicants, escrow
- Scheduled cross-tenant (BOLA) access checks

Payments & storage

- Card data via Stripe (PCI DSS Level 1) — no full PANs on our servers
- Encrypted storage at rest (Supabase managed PostgreSQL)
- Private resumes / signed URLs for CV access

Engineering hygiene

- Automated dependency and secret scanning in CI
- Security regressions tracked and remediated
- API routes use service role only with RBAC

OUR ATTESTATIONS — NOT VENDOR BADGES

Status is explicit. No fake seals.

NOT COMPLETED

SOC 2 Type I

Internal readiness and evidence collection in progress; no auditor report yet.

NOT AVAILABLE

SOC 2 Type II

Needs Type I + observation period. Shareable under NDA only when issued.

NOT PUBLISHED

SOC 3

Public summary only after a completed SOC 2 programme — no badge before then.

NOT CERTIFIED

ISO 27001

We are not ISO 27001 certified.

NOT CERTIFIED

HIPAA

Not designed for PHI. Do not store protected health information on the platform.

VENDORS THAT PROCESS DATA ON OUR BEHALF

Vendor certifications apply to the vendor — not to WeRemoteIT as a whole.

Vercel
App hosting & serverless APIs · HTTP requests, logs · Global edge (primary US)

Supabase
DB, auth, file storage · Profiles, jobs, messages, tokens · US managed Postgres

Stripe
Payments & billing · Payment tokens (not full PANs on our servers)

Resend
Transactional email · Recipient addresses & notification content · US

Telegram / Discord
Optional bot channels · Messages/commands when linked · Per platform

DPAs
Enterprise DPAs on request — support@weremoteit.com or security@.

Checkout partners (e.g. Dodo Payments where enabled) process card flows as shown at purchase time. Escrow/USDC rails are separate product surfaces.

MONITORING — AND WHAT WE DO NOT OFFER YET

Direct beats overpromise.

Monitoring & incident response

- Health checks every five minutes → on-call engineering
- Scheduled security advisor snapshots for DB policy regressions
- Security events logged for tenant-isolation violations
- Documented IR runbook with severity and escalation
- No 24/7 staffed SOC — critical alerts handled as quickly as practicable

Not available today

- SOC 2 Type II report or SOC 3 public summary
- Formal HIPAA / ISO 27001 / platform PCI attestation
- Guaranteed EU-only data residency (confirm before onboard)
- Paid bug bounty (good-faith reports still welcome)
- Automated enterprise questionnaire trust centre

SECURITY CONTACT

Report a vulnerability. Ask about controls. Request a DPA.

We respond to good-faith security reports and aim to acknowledge them within a few business days. Please do not publicly disclose until we have had reasonable time to investigate and remediate.

security@weremoteit.com
Vulnerabilities, controls, reports under NDA when available

Live page
https://weremoteit.com/security — always the source of truth

Account hygiene
https://weremoteit.com/docs/talent/security.html

Email security@ | Open /security | Privacy policy