

Vendor Security Summary

PHASE TRANSITIONS AI

Phase Transitions (Pty) Ltd · Reg 2026/448729/07 · Johannesburg, South Africa · graham@phasetransitions.ai · trust.phasetransitions.ai

What we do. Phase Transitions builds and operates custom data and AI software for business clients. We connect to a client's accounting and bank data, reconcile it through software we write, and present it as a secure dashboard plus an AI analyst. Under POPIA we act as an operator; the client remains the responsible party. We own our intellectual property and control our infrastructure.

Data we handle. Business accounting and bank-transaction data, and for some clients investment data. Most engagements put no personal information in reach of the AI layer; where one does, it is tokenised first.

01 KEY CONTROLS

- **Read, never write.** The AI reads finished, reconciled numbers. It cannot author or change them, and makes no automated decisions. A write guard at the transport layer enforces this.
- **Per-client isolation, verified by a test.** One database per client, with its own credentials. An automated test in CI asserts each client sees only its own rows and that a misconfigured connection is rejected.
- **Minimal AI exposure.** The AI sees read-only data at query time and stores nothing at rest; where an engagement puts personal information in its reach, it is tokenised first. No training on client data.
- **Encryption.** AES-256 at rest (platform-managed); TLS 1.2+ in transit.
- **Resilience.** Daily database backups with a tested restore and a known recovery time. A written cross-system incident-response plan (POPIA, Cybercrimes Act, FSCA/PA Joint Standard). A written data-storage policy.
- **Access.** Managed passwordless authentication (Auth0) with deny-by-default allowlisting. Least-privilege, read-only database roles for the AI. Secrets kept out of source control.

02 SUB-PROCESSORS

Provider	Role
Render	Hosting and per-client PostgreSQL databases
Cloudflare R2	Raw data and document storage (EU)
Auth0 (Okta)	Identity and authentication
Anthropic	AI analyst layer (read-only; signed DPA with EU SCCs)
Files.com	Managed SFTP / partner-data ingress

Provider	Role
Resend	Transactional email (one-time codes)
GitHub	Source control and CI

Phase Transitions is the contracting entity. Each is SOC 2 and/or ISO 27001 certified. Data-processing agreements are in place; copies available on request.

03 POSTURE AND CURRENT LIMITS

- A SOC 2 and vendor-DDQ posture, self-assessed against the standard, available in full under NDA.
- Technology E&O and Cyber insurance is in force.
- Encryption at rest is platform-managed. There are no customer-managed keys yet.
- Request-level access auditing covers login-based deployments. Read-only static deployments have no sign-in, so carry no per-user audit trail.

Full pack under NDA: graham@phasetransitions.ai