

How Infraxus handles your financial data.

A consolidated read on the controls, providers, data handling, residency, AI handling, operator boundary, incident response, sub-processors, and exit terms behind the Control Sprint and the Engagement. Written at the level a procurement reviewer expects, with the technical specifics named.

01 Infrastructure.

Production runs on three providers, each SOC 2 Type II attested. Attestation applies to those providers; Infraxus does not hold its own SOC 2 attestation. Attestation links available on request.

DATABASE · AUTH · STORAGE

Supabase

Postgres with row-level security. Auth and session management. SOC 2 Type II.

BACKEND · INGESTION

Render

Backend services and ingestion. Service-role keys held only in Render-side environment. SOC 2 Type II.

FRONTEND HOSTING

Vercel

Marketing site and the Portal frontend, served from Sydney region with global CDN. SOC 2 Type II.

AI PROVIDER ROUTING

OpenRouter · Anthropic

AI calls route via OpenRouter to Anthropic. Prompts are not logged by default and your data is not used to train models.

02 Controls by layer.

Portal.

LAYER 03 · SURFACE

AUTH MAP ROLE MFA AUDIT

Named users only. User-to-client mapping enforced through user_client_map. Role-based view restrictions. MFA enforced on all Portal accounts. SSO available on request. Named-user audit log exportable at any time. Sessions expire on a configurable schedule; a named user can be revoked in minutes, not days.

Application.

LAYER 02 · TRANSIT AND AT REST

TLS 1.2+ AES-256 SERVICE-ROLE

Every connection terminates TLS 1.2 or higher. Every persisted byte sits behind AES-256. Service-role keys only for backend access. No long-lived bearer tokens shared with operators.

Database.

LAYER 01 · PER-CLIENT ISOLATION

POSTGRES RLS DAILY SNAPSHOTS 7-DAY PITR

Per-client data isolation. Every query is scoped to the requesting user's mapped clients through row-level security. A named user only ever sees the clients they are mapped to. Daily automated snapshots with seven-day point-in-time recovery.

03 Data handling, two pathways.

The Sprint and the Engagement are different shapes of work. The shape of access changes; the standard does not.

Sprint pathway.

10 BUSINESS DAYS · EXPORT-BASED · TIME-BOUNDED

- You provide agreed exports. We work from those exports.
- No live integration. No persistent connection into your accounting system.
- Encrypted working environment for the build window.
- Outputs delivered only to the contacts you name.
- NDA available on request.

Engagement pathway.

CONTINUOUS · NAMED-USER · ISOLATED

- Monthly accounting export plus operating data agreed at scoping.
- Per-client isolated environment with row-level security.
- Portal access for named users only. Reviewed pack each cycle.
- CSV export at any time.
- Monthly review, 30 days' notice from either side.

Data is exchanged by a method agreed with each client and stored in access-controlled, MFA-gated cloud storage, never on local disk.

The Portal is optional. Clients who prefer it can stay fully export and Excel based, with no hosted surface.

04 AI handling.

AI calls route through OpenRouter to Anthropic. Prompts are not logged by default and your data is not used to train models. Data is sent per query only. The query layer (Ask Your Numbers) operates under the same terms.

Every AI output is reviewed and signed off by the founder before it reaches the Portal. Nothing publishes unreviewed. AI produces analysis; it does not take accountability for what the numbers mean. The published Portal pack is the operator's call, not the model's.

05 Data residency.

Sydney (ap-southeast-2) is the default region for the database and for the Portal hosting. Other regions, including Frankfurt (eu-central-1) and US-east (us-east-1), are supported and can be provisioned before the engagement begins. Residency is fixed at the start of an engagement and does not change without a written request.

06 Operator controls.

Infraxus is founder-operated, so the operator's own access is part of the security boundary. MFA is enforced on every account that touches client data, hosting, database, application, email, and AI provider. Admin credentials are held in 1Password. Devices are disk-encrypted. Client working data lives in access-controlled, MFA-gated cloud storage, never on local disk.

07 Incident response.

If a security incident affecting your data is confirmed, you are notified within 72 hours with what happened, what was affected, and the remediation taken. Handled directly by the operator, consistent with the AU Notifiable Data Breaches scheme and the NZ Privacy Act 2020.

08

Sub-processors.

The outside services below process client data on behalf of Infraxus. The current list is available on request, as is a Data Processing Agreement (DPA).

PROCESSOR	ROLE	REGION
Supabase	Database, auth, session management	Sydney, AU
Render	Backend API, ingestion	Singapore
Vercel	Portal and marketing site frontend hosting	Sydney, AU + global CDN
OpenRouter	Routing layer for AI requests to Anthropic	United States
Anthropic	AI model provider	United States
Dropbox	Access-controlled working storage for client data	Operator account, MFA-gated

09

Exit.

The Excel calculation engine is client-owned from day one of the Sprint. It contains the full calculation engine: three-way forecast, working-capital cycle, KPI logic, scenario layer, and assumption block.

If the Engagement ends, the workbook stays with you. The Portal is decommissioned within 30 days. A full CSV export of historical data is provided. There is no proprietary system that must be subscribed to in order to keep using the work, and no part of the calculation logic that lives somewhere you cannot see.

10

Procurement FAQ and contact.

Common review-team questions: provider attestation links, the sub-processor list, the DPA, residency for non-AU clients, MFA scope, SSO availability for the Portal, the named-user audit log, and the incident notification window. All available on request.

For specific questions, email security@infraxus.com. Better to answer a hard procurement question upfront than to find out about it three weeks into the Engagement.