Infraxus

SECURITY & TRUST

Security & Trust Overview

Infrastructure, controls, and data handling

Contact: security@infraxus.com

Prepared by Infraxus Systems

31 May 2026

INFRASTRUCTURE

How Infraxus is built

> Infraxus runs on a modern cloud stack with Australian data residency. Client financial data is stored in Supabase (ap-southeast-2, Sydney, Australia). The application layer runs on Vercel (syd1, Sydney) and a Python API on Render (Singapore). AI commentary is generated via Anthropic's API through OpenRouter — client data is not retained by Anthropic for training purposes per their API terms of service.

SECURITY CONTROLS

Controls matrix

CONTROL	IMPLEMENTATION	STANDARD
Data residency	Supabase ap-southeast-2 (Sydney, Australia)	Australian data sovereignty
Encryption at rest	AES-256 via Supabase managed infrastructure	Industry standard
Encryption in transit	TLS 1.2+ on all endpoints	Industry standard
Authentication	Supabase Auth with JWT tokens	OWASP
Authorisation	Row-Level Security (RLS) on all client data tables — each client sees only their own data	Zero trust
API security	Service-role key never exposed client-side; all sensitive operations server-side only	OWASP
AI data handling	Financial data sent to Anthropic API for commentary only; not used for model training per Anthropic API terms	Privacy by design
Access control	Per-client isolation via user_client_map; admin access scoped separately	Least privilege
Audit logging	Supabase Auth logs all authentication events; commentary publish events timestamped	SOC 2 aligned
Incident response	security@infraxus.com monitored; affected clients notified within 24 hours of confirmed breach	Best practice

DATAHANDLING

What Infraxus stores and how

What Infraxus stores

Monthly financial data (P&L, cashflow, KPIs), AI-generated commentary, user authentication credentials (email + hashed password only via Supabase Auth).

What Infraxus does NOT store

Raw bank feeds, payment card data, tax file numbers, personal sensitive data beyond email address, bank account details.

Data residency & exit

All client financial data is stored in Sydney, Australia. Clients may request a full data export or complete deletion at any time by contacting security@infraxus.com. Deletion completed within 30 days of verified request.

PROCUREMENTFAQ

Answers procurement teams usually want

Where is client data stored?

Supabase ap-southeast-2 (Sydney, Australia). No data leaves Australia except for AI commentary generation via Anthropic's API, which does not retain client data for training.

Is data encrypted?

Yes. AES-256 at rest via Supabase managed infrastructure. TLS 1.2+ for all data in transit.

Who has access to client financial data?

Only the client's mapped users and the Infraxus account manager for service delivery. No third parties have access.

Do you use client data to train AI models?

No. Per Anthropic's API terms of service, data sent via the API is not used for model training.

Can we export our data?

Yes. Contact security@infraxus.com to request a complete export in CSV format.

Can we delete our data?

Yes. Contact security@infraxus.com. Deletion completed within 30 days of a verified request.

Are you SOC 2 certified?

Not currently. Controls are aligned with SOC 2 principles. Formal certification is on the roadmap as the business scales.

What happens in a security incident?

Affected clients are notified within 24 hours of a confirmed breach via email. We maintain an incident response plan and provide a post-incident report.