Pocket Fund — Security Overview

For private equity firms

SOC 2 infra | AES-256 at rest | TLS 1.2+ | 34 isolation tests | 9-tier RBAC | MFA available

Where your data lives

All data processed and stored on enterprise-grade SOC 2 Type II infrastructure: Supabase (Postgres, AWS US), Vercel (application hosting), and AI processing via OpenAI, Anthropic, Google, and Azure — all on API tiers with no model training on customer data. Full sub-processor list on page 2.

Encryption

In transit: TLS 1.2+ (TLS 1.3 negotiated when client supports). HTTPS enforced via HSTS.

At rest: AES-256 via Supabase-managed disk encryption. File storage encrypted at rest.

Tenant isolation

Every record in scoped tables tagged with `organizationId`. Server-side middleware enforces on every API route — no client-trusted path. Verified by:

- **34 automated cross-organization integration tests** run on every deploy
- **268 explicit org-scope checks** across 45 API route files
- Cross-org access returns HTTP 404 (not 403) to prevent enumeration

Customers can run live isolation checks from Settings → Security and download a JSON report.

AI & LLM data handling

OpenAI, Anthropic, Google, and Azure API tiers — all contractually do not train models on customer data. Your CIMs, LOIs, and memos never feed any model.

Access controls & rate limiting

- **Authentication:** Supabase Auth with optional TOTP-based 2FA (Google Authenticator, Authy, 1Password)
- **Org-wide MFA:** admins can require all members to enroll 2FA
- **9-tier RBAC:** admin, partner, principal, vp, associate, analyst, ops, member, viewer
- **Rate limiting:** general (600 req / 15 min), AI (10 req / min), writes (30 req / min) — all per user/IP
- **Standard hardening:** helmet, CORS allow-list, JWT-based sessions

Audit logging

60+ distinct action types across 9 resource types tracked with user ID, organization ID, resource ID, timestamp, severity. Customer admins view, filter, and export their organization's audit log directly from the Admin Dashboard. Categories: authentication, deal lifecycle, document operations, memo operations, user management, and system operations.

Sub-processors

Provider	Service	Region	Cert.
Supabase	DB, auth, storage	US (AWS)	SOC 2 Type II
Vercel	Application hosting	Global	SOC 2 Type II
OpenAI	GPT-4o	US	SOC 2 Type II
Anthropic	Claude	US	SOC 2 Type II
Google	Gemini	US	SOC 2
Microsoft Azure	Document Intelligence	US	SOC 2 Type II, ISO 27001
Apify	Web search	US/EU	SOC 2
Resend	Transactional email	US	SOC 2 Type II
Sentry	Error monitoring (sanitized)	US	SOC 2 Type II

Compliance roadmap

- **SOC 2 Type I:** in progress; target completion date available on request
- **SOC 2 Type II:** following Type I
- **Annual penetration test:** planned for next quarter
- **GDPR:** DPA available on request; data deletion within 30 days post-termination

Contact

Security & compliance: security@pocket-fund.com

Urgent issues: tech@pocket-fund.com