

Built for confidential portfolio data — auditable by construction.

Noesis is a portfolio analytics platform for family offices. Its defining property is that **every figure traces to a worked calculation and the AI assistant is structurally unable to invent a number**. The same discipline runs through the security architecture below.

222

AUTOMATED TESTS,
INCL. CROSS-TENANT
ISOLATION

100%

MUTATIONS & AI TOOL
CALLS AUDIT-LOGGED

0

KNOWN DEPENDENCY
VULNERABILITIES (PIP-
AUDIT)

Zero

CLIENT DATA USED FOR
AI MODEL TRAINING

1 Tenant isolation, enforced in the database

- **PostgreSQL Row-Level Security on every business table** — each row carries its owner; the database itself refuses cross-tenant reads and writes.
- **FORCE RLS**: the policy binds even privileged table owners.
- Application sessions are pinned to one tenant; isolation is exercised by automated cross-tenant tests on every change.
- **Dedicated single-tenant instances available** — your office's data on its own stack.

2 Authentication & session hygiene

- Short-lived signed sessions (60 min) with silent renewal.
- **Instant revocation**: sign-out or a password change invalidates every outstanding session, server-side.
- Login throttling with logout backoff against credential stuffing; CSRF double-submit protection.
- Hardened response headers: content-type sniffing off, framing denied, referrer suppressed, HSTS under TLS.
- Role-gated writes — governance artifacts (e.g. policy targets) are admin-only.

3 Auditability by construction

- **Every figure opens its full worked calculation** — formula, inputs, method, as-of date.
- Excel exports are proven equal to the screen, cell for cell, by automated tests.
- Every imported row is traceable to its upload batch; every mutation and assistant tool call is written to an **in-product, read-only audit log**.
- Money is stored as exact integer minor units — no floating-point drift; reconciliation identities are asserted in tests.

4 The AI boundary

- Ask Noesis is an **orchestrator, not a calculator**: the model plans; the deterministic engine computes.
- The model never receives raw tables and has no database access — only five strict, typed tools.
- Every numeric claim in an answer must carry an engine citation; uncited numbers are rejected before display.
- Served under commercial API terms with **no training on your data**; per-user rate limits; every question and tool call audited.
- No API key configured → the assistant is off. It never falls back to guessing.

5 Data handling & portability

- Data enters via reviewed workbook imports — validated atomically; a batch either fully loads or fully fails.
- One-command backups of database and document store with a tested restore path; encryption at rest per deployment (cloud-volume or dedicated-instance disk).
- **No lock-in**: every table and report exports to Excel at any time, methodology sheet included.
- Benchmark data via your licensed sources or a clearly-labelled free feed — your choice, same template.

6 Engineering discipline & roadmap

- Reproducible containerized deployments; production mode fails fast on default secrets.
- Continuous dependency vulnerability scanning — currently clean.
- Full audit trail of product decisions and methodology maintained alongside the code.
- **Roadmap**: SOC 2 Type I track, SSO/SAML, custodian & administrator feeds, key management via cloud KMS.