// SECURITY OVERVIEW · v1

Vendric Labs
Security Overview

How customer data is handled, what is encrypted, and who else touches it. Written for procurement.

Document	Security Overview · v1
Owner	Taylor Marr · founder · taylormarr@vendriclabs.net
Security contact	security@vendriclabs.net
Last revised	2026-05-27
Review cadence	Updated when status changes.

1 · POSTURE

Vendric Labs is solo-founded today, building software that handles consequential records — OSHA logs, incident reports, contractor histories. The product thesis assumes the record outlives the company that shipped it. The security posture is therefore **local-first where possible, audit-grade everywhere**, and built so that a customer can verify their records without our cooperation.

One load-bearing rule: customer submissions to Reeve (incident records, photos, drafted forms, chat) are never used to train any model — ours or a vendor's. We do not opt into vendor training-data programs on the inference endpoints we call. Our forward-looking training corpus consists exclusively of de-identified public regulatory data (OSHA citations, 29 CFR text, court filings). Because those records are public the moment they're filed, we cannot promise that incidents originally reported by a particular customer have never appeared in that public corpus.

2 · DATA LIFECYCLE

Tenant isolation	Each Reeve tenant has its own verification key, storage scope, and audit chain. Cross-tenant inference is architecturally impossible, not just policy-prohibited.
Customer export	Records will export with a cryptographic proof on the Q3 2026 roadmap. The audit chain is verifiable without our cooperation once the customer holds the tenant verification key.

Customer deletion	Customer-initiated deletion is supported. Request via security@vendriclabs.net for current scope and timing. The deletion event is signed into the audit chain so the chain remains verifiable.
Backups	Encrypted; same residency as production.

3 · ENCRYPTION

At rest	AES-256-GCM (Azure Storage Service Encryption).
In transit	TLS 1.3 between client, edge, and origin.
Audit chain	Authenticated per-tenant audit chain.
Future proofs	Tamper-evident selective export on the Q3 2026 roadmap. Carrier-facing record exchange and compliance-proof workflows on the longer roadmap. Cryptographic detail provided under NDA.
Key handling	Per-tenant verification keys, generated at provisioning, never reused, never logged. Provided to customers and auditors on request.

4 · INFRASTRUCTURE

Reeve (live product at vendriclabs.net) runs on **Microsoft Azure, US regions**. All customer records, photos, verification keys, audit chain, and citation index live in Azure storage. The marketing site (vendriclabs.net) is a static Next.js build on Netlify, US edge — it does not handle product data.

Vendric (the local-first personal AI, pre-launch 2026 H2) runs on the user's own machine; conversations never reach a Vendric Labs server.

5 · ACCESS

Production access is currently held by the founder. Access hardening (including documented multi-factor authentication posture across consoles) is in progress. Current status available on request to security@vendriclabs.net.

6 · COMPLIANCE ROADMAP

Audit chain	Live · 2026-05-22
Tenant data isolation	Live · 2026-05-22
Verification keys (partner access)	Live · 2026-05-22
Trust + Security page	Live · 2026-05-24
Documented vulnerability disclosure	Live · 2026-05-24
Selective subpoena export	In build · Q3 2026
SOC 2 Type I	Planned · H2 2026
SOC 2 Type II	Planned · H2 2026 → 12-month observation
Compliance proofs	Design · Q4 2026
Carrier-facing record exchange	Pilot · 2027

We will not name a SOC 2 auditor until one is engaged. We will not claim a certification status we have not earned.

7 · SUBPROCESSORS

Three vendors touch customer data today. The full list lives in **subprocessors.pdf** (and on vendriclabs.net/trust). New subprocessors will appear on the public list before they begin processing customer data.

Microsoft Azure	Reeve product hosting + storage · US
Anthropic	AI inference (Claude Sonnet 4.x family) · US
Netlify	Marketing site hosting + email capture · US

8 · INCIDENT RESPONSE + DISCLOSURE

Vendric Labs is solo-founded today. We aim to respond promptly to security reports and material incidents; we will not put a hard SLA in writing until we can guarantee it. Report a vulnerability at **security@vendriclabs.net**.

9 · AI HANDLING

Reeve's photo-to-hazard analysis and citation grounding run on **Anthropic Claude Sonnet (4.x family)**. We do not fine-tune. We do not opt into vendor training-data programs. Every penalty-bearing output is reviewed by the customer before submission to OSHA — the system drafts, the GC signs.

Full Model Card with per-product detail and human-in-the-loop checkpoints: **model-card.pdf**.

“A page that promises trust isn’t trust. The only trust signal that survives contact with an actual incident is the one you can verify yourself.”

— Taylor Marr, founder