Security & Architecture Overview

Henosis CRM — Vendor Security & Technical Due-Diligence Packet

PREPARED BY
Henosis Technologies, LLC

DOCUMENT VERSION
1.0

DATE
18 May 2026

CLASSIFICATION
Confidential — for evaluation

AUDIENCE
Prospective customer security review

CONTACT
support@henosis.solutions

Contents

PART I

Henosis CRM — Security & Architecture Overview

Henosis Technologies, LLC · Document version 1.0 · 18 May 2026 · Confidential — provided for evaluation under the parties' confidentiality terms.

1. Purpose & scope

This document describes the architecture, security controls, data-handling practices, and compliance posture of the Henosis CRM application (`app.henosis.solutions`) and supporting infrastructure. It is intended to support a prospective customer's vendor security review.

We have written this to be **accurate to our current implementation**, not aspirational. Where a control is on our roadmap rather than in production today, we say so explicitly. Henosis is an early-stage company; we believe transparency about what we do and do not yet have is the right basis for an enterprise relationship.

2. Company & product overview

Henosis is a multi-tenant B2B SaaS CRM purpose-built for business-development and account-management teams at alternative-asset service providers (fund administrators, prime brokers, fund-accounting firms, compliance vendors, placement agents, legal firms). It manages contacts, accounts, deals, tasks, meetings, projects, proposals (including e-signature), analytics, and AI-assisted workflows.

- **Hosting model:** fully managed cloud SaaS; no on-premise or customer-managed infrastructure.
- **Data residency:** United States — primary data store hosted in AWS US West (Oregon, `us-west-1`).
- **Tenancy:** logical multi-tenancy with database-enforced isolation (§4).

3. Architecture & hosting

Layer	Technology	Provider	Region
Frontend (SPA)	React 18 + TypeScript, static build	Vercel (hosting + CDN, TLS termination)	Global edge / US origin
Application API & business logic	Serverless edge functions (Deno)	Supabase Edge Functions	US
Database	PostgreSQL with Row-Level Security	Supabase (managed Postgres)	US (AWS us-west-1)
Authentication	Managed auth (JWT sessions)	Supabase Auth	US
Object storage	Bucket storage with per-tenant path scoping, size/MIME limits	Supabase Storage	US

There is no customer-operated component. All traffic is served over HTTPS; the database and storage are not exposed to the public internet except through authenticated, RLS-enforced APIs.

A complete list of third-party processors that may handle personal data is in the accompanying **Sub-processor List**.

4. Multi-tenancy & data isolation

Henosis is logically multi-tenant. Isolation is enforced **at the database layer**, not only in application code:

- Every tenant-scoped table has PostgreSQL **Row-Level Security (RLS)** enabled.
- All tenant-scoped policies resolve through a single central membership function, `user_belongs_to_tenant(tenant_id)`, which returns true only if the authenticated user is a member of that tenant. A user's identity is taken from the verified session JWT — it cannot be spoofed by the client.
- Server-side edge functions that operate with elevated database privileges independently verify tenant membership from the caller's JWT before performing any tenant-scoped write.
- There is **no client-trusted tenant identifier** on protected paths; a request for another tenant's data is denied by the database regardless of what the client sends.

The result: a defect or manipulated request in the client cannot read or write another tenant's data, because the deny decision is made by Postgres.

5. Encryption

- **In transit:** all client, API, and database connections use TLS 1.2+ (HTTPS enforced by Vercel and Supabase; database connections are TLS-encrypted).
- **At rest:** customer data, backups, and storage objects are encrypted at rest with AES-256 by our infrastructure providers (Supabase / Vercel).
- **Application-layer credential encryption:** third-party integration credentials (e.g., connected-mailbox tokens) are **additionally** encrypted at the application layer with **AES-256-GCM** (96-bit IV, authenticated encryption) using a dedicated key held in a secrets store outside the database — so a database compromise alone does not expose integration secrets.
- **Payment data:** card data is handled entirely by Stripe (PCI DSS Level 1). Henosis stores only billing metadata (plan, seat count, card last-4, status) and never full card numbers.

6. Authentication & access control

END-USER AUTHENTICATION

AUTHORIZATION

HENOSIS PERSONNEL ACCESS

7. Application & development security

- **SDLC:** all changes land on a `dev` branch via pull request; production is a separate `main` branch promoted only by reviewed PR. No direct commits to production.
- **Change management:** every database schema change is a version-controlled migration file applied exclusively by an automated CI/CD pipeline (GitHub Actions). There is no manual/ad-hoc DDL on production.
- **Code review:** changes are peer-reviewed before promotion; a structured security-focused review is run before production promotion.
- **Input handling:** all database access is via parameterized queries (Supabase SDK / PostgREST); forms are schema-validated (Zod); React provides default output encoding against XSS; CSV/Excel imports are field-allowlisted to prevent mass-assignment.
- **Public endpoints** (e.g., e-signature signing links) are rate-limited per IP (e.g., 10 signature submissions/hour, 30 token lookups/hour) and validate a server-issued access token; authentication endpoints are additionally protected by the managed auth provider's native abuse controls.
- **Browser hardening:** HTTP responses set HSTS (TLS pinning), `X-Frame-Options: DENY` / `frame-ancestors 'none'` (clickjacking), `X-Content-Type-Options: nosniff`, a restrictive `Referrer-Policy`, and a `Permissions-Policy` disabling camera/microphone/geolocation and similar APIs. A Content Security Policy is in monitored rollout and moves to enforced mode after validation.
- **Dependency management:** dependencies are pinned and managed via lockfile; production builds strip debug logging.
- **Secrets:** held in provider secret stores (Supabase function secrets, Vercel environment variables); not in source control.

8. Data management

- **Customer data ownership:** the customer owns all data it inputs. Henosis processes it solely to provide the Service, as a processor under the customer's instructions (see Terms of Service / DPA).
- **Data we process:** account & profile data, customer-input CRM records (contacts/accounts/deals/proposals/notes/tasks), connected-mailbox email metadata and message content (only if a user connects a mailbox), billing metadata, and usage/diagnostic logs. We do **not** process payment-card data, PHI (HIPAA), or financial-account data (GLBA).
- **Residency:** United States (AWS us-west-1).
- **Retention:** retained while the account is active. On termination, a 30-day export window is provided, after which customer data is deleted; backups age out on their normal cycle.
- **Portability / deletion:** customers can export their data from the application (CSV/Excel). Deletion requests are honored per the Privacy Policy and DPA.
- **Backups:** automated, encrypted daily backups managed by the database platform. Enhanced point-in-time recovery (sub-24h RPO) is a planned hardening item (§13).

9. Sub-processors

Henosis uses a small set of well-established US-based sub-processors (database/auth, payments, email delivery, mailbox sync, hosting/CDN, AI features, error monitoring). The full list with purpose and data location is provided in the **Sub-processor List** included in this document. Customers receive advance notice of material sub-processor changes per the DPA.

10. Logging, monitoring & audit

- **Application audit logging:** security-relevant and data-change events are written to an append-style audit log with a strict insert policy (a row can only be written for the acting user within their own tenant).
- **E-signature audit trail:** every proposal-signing action (created, sent, viewed, signed, declined, expired, reminder) is recorded with actor, IP, user-agent, and timestamp, tenant-isolated.
- **Operational logging & error monitoring:** structured operational event logging plus application-level error monitoring (Sentry integration) for detection and diagnostics.
- Logs are scoped per tenant and subject to the same RLS isolation as customer data.

11. Vulnerability management & testing

- We conduct **internal security reviews against the OWASP Top 10 (2021)**, including code review, taint analysis, and dependency audit. Critical/High/Medium findings from our most recent review cycle have been remediated and tracked.
- An **independent third-party penetration test is planned as part of our SOC 2 program** (§13); we will share a summary/letter of attestation with customers under NDA once completed.
- Security-relevant patches to managed providers (Supabase, Vercel, Stripe) are applied by those providers; application dependencies are updated on a rolling basis.

12. Incident response & breach notification

- We maintain logging and monitoring to detect security events and a defined process for triage, containment, and remediation.
- In the event of a personal-data breach, we will notify affected customers and applicable regulators **as required by law — within 72 hours of becoming aware where GDPR applies** — with the nature of the incident, data involved, and remediation steps.
- A formalized, tested incident-response runbook is being finalized as part of launch operational readiness.

13. Security roadmap

We are transparent about what is not yet in place. Planned, in roughly priority order:

Item	Status
SOC 2 Type I (then Type II)	Roadmap — target post-funding; controls being put in place now
Independent third-party penetration test	Roadmap — part of the SOC 2 program
Multi-factor authentication (MFA)	Near-term roadmap
SSO (SAML / OIDC) for enterprise	Enterprise roadmap
Content Security Policy — enforced mode	In progress — HSTS, frame, content-type, referrer, and permissions policies are enforced today; CSP is in monitored (report-only) rollout and moves to enforced after validation
Point-in-time recovery (sub-24h RPO) on the production database	Near-term hardening
Customer-configurable data-retention controls	Roadmap

14. Compliance posture

- **SOC 2: Not currently certified.** Operational controls (documented access control, change management, data classification, vendor reviews, backups) are being established now; SOC 2 Type I is targeted post-funding.
- **GDPR / UK GDPR:** lawful bases declared in our Privacy Policy; data-subject rights supported; **DPA with EU Standard Contractual Clauses available on request** to business customers.
- **CCPA / CPRA & other US state privacy laws:** addressed via a single comprehensive Privacy Policy; we do not sell or share personal information for cross-context behavioral advertising.
- **CAN-SPAM:** marketing email includes sender identity, physical postal address, and one-click unsubscribe with a suppression list.
- **PCI DSS:** card data handled by Stripe (Level 1); Henosis is out of cardholder-data scope.
- **HIPAA / GLBA:** not applicable — Henosis does not process PHI or financial-account data.

15. Security contact

Security questions, vulnerability reports, or to request the DPA:

Henosis Technologies, LLC

Security & privacy inquiries, vulnerability reports, DPA requests: **support@henosis.solutions**

PART II

Henosis CRM — Sub-processor List

Henosis Technologies, LLC · Document version 1.0 · 18 May 2026 · Confidential — provided for evaluation under the parties' confidentiality terms.

Last updated: 2026-05-18

Henosis Technologies, LLC ("Henosis") engages the third-party sub-processors below to provide the Henosis CRM service. Each processes data only as needed to deliver its function and is bound by data-protection terms. Card data is handled exclusively by Stripe; Henosis does not store full payment-card numbers.

Sub-processor	Function	Data processed	Location
Supabase	Database, authentication, object storage, serverless functions	Account data and all customer-input CRM data; authentication data	United States (AWS us-west-1)
Vercel	Frontend application hosting & CDN	IP address, access logs (no customer CRM records persisted at this layer)	Global edge / US origin
Stripe	Subscription billing & payment processing	Billing contact, plan/seat metadata, card data (held by Stripe; PCI DSS Level 1)	United States
Resend	Transactional & marketing email delivery	Recipient email address, message content	United States
Nylas	Per-user mailbox sync & send (Microsoft 365) and email engagement tracking — only for users who connect a mailbox	Sender/recipient email addresses, message content, open/click events	United States
OpenAI	AI-assisted features (assistant, summarization, subject suggestions, import mapping, project planning)	User prompts and limited customer data submitted to generate outputs. Per OpenAI's API data-usage policy, data submitted via the API is not used to train OpenAI's models	United States
Sentry	Application error monitoring & diagnostics	Error diagnostics and stack traces, which may include limited identifiers	United States

Not sub-processors / not in the data path

- **Firecrawl** — removed from the product 2026-05-07; not used.
- **Perplexity / Grok** — internal research tooling only; not in the product data path.
- **PostHog, Plain, Better Stack** — not currently adopted. This list will be updated and customers notified before any are added.

Change notification

Henosis maintains this list as the single source of truth. Customers receive advance notice of material additions or changes to sub-processors as described in the Data Processing Addendum (available on request), with a reasonable period to object.

PART III

Henosis CRM — Security FAQ

Henosis Technologies, LLC · Document version 1.0 · 18 May 2026 · Confidential — provided for evaluation under the parties' confidentiality terms.

Common questions from vendor security reviews. If your team uses a formal questionnaire (SIG Lite, CAIQ, or your own), send it over and we will complete it directly; this FAQ covers the most frequent items.

HOSTING & ARCHITECTURE

Where is the application hosted and where is data stored?

Fully managed US cloud. Frontend on Vercel (CDN/edge, US origin); database, auth, storage, and serverless functions on Supabase, hosted in AWS US West (Oregon, us-west-1). No on-premise or customer-managed components.

Is the database exposed to the internet?

No. It is reached only through authenticated, Row-Level-Security-enforced APIs. There is no public/direct database access.

Is this single-tenant or multi-tenant?

Logical multi-tenant with isolation enforced at the PostgreSQL layer (Row-Level Security), not just in application code. A request for another tenant's data is denied by the database.

ENCRYPTION

Is data encrypted in transit and at rest?

Yes. TLS 1.2+ in transit (HTTPS enforced); AES-256 at rest for data, backups, and storage (provider-managed). Third-party integration credentials are additionally encrypted at the application layer with AES-256-GCM using a key held outside the database.

Do you store payment-card data?

No. Stripe (PCI DSS Level 1) handles all card data. We store only billing metadata (plan, seat count, last-4, status).

AUTHENTICATION & ACCESS

How do users authenticate? Is MFA available?

Email + password via managed auth with signed, short-lived JWT sessions. Enforced password policy: ≥10 chars with upper, lower, number, and special character. **MFA is not generally available today; it is on our near-term roadmap.**

Do you support SSO (SAML/OIDC)?

Not today. SSO is on our enterprise roadmap; we can discuss timeline if it is a requirement for your deployment.

Who at Henosis can access customer data?

Production access is restricted to the two founders. A role-gated internal support path exists for troubleshooting and is recorded in audit logs. There is no ad-hoc production database access — all changes go through reviewed source control and CI.

Are roles/permissions enforced server-side?

Yes. Role and tenant membership are enforced at the database layer from the verified session, not trusted from the client.

DEVELOPMENT & CHANGE MANAGEMENT

How are changes deployed to production?

All changes via pull request to a `dev` branch; production (`main`) is promoted only by reviewed PR with a security-focused review. Schema changes are version-controlled migrations applied solely by automated CI/CD — no manual production DDL.

How do you protect against common web vulnerabilities (OWASP Top 10)?

Parameterized queries (no string-built SQL), schema-validated inputs (Zod), default output encoding (React) against XSS, field-allowlisted data imports (no mass assignment), rate-limited public endpoints with server-issued tokens, and secrets held in provider secret stores (not in source).

TESTING & COMPLIANCE

Are you SOC 2 certified?

No, not currently. We are establishing the operational controls now and target SOC 2 Type I post-funding. We will share attestation when available, under NDA.

Have you had a third-party penetration test?

Not yet. We perform internal OWASP-Top-10 security reviews (code review, taint analysis, dependency audit) and have remediated the findings from our most recent cycle. An independent third-party pen test is planned as part of our SOC 2 program; we will share the summary under NDA when complete.

Are you GDPR/CCPA compliant? Is a DPA available?

We support GDPR/UK GDPR (lawful bases declared, data-subject rights, US-transfer safeguards) and CCPA/CPRA (no sale/share for cross-context advertising). A **DPA incorporating EU Standard Contractual Clauses is available on request.** HIPAA/GLBA do not apply — we process no PHI or financial-account data.

DATA HANDLING

Who owns customer data and can we get it back?

You own all data you input; Henosis processes it only to provide the service. You can export your data (CSV/Excel) at any time. On termination, a 30-day export window applies, after which data is deleted (backups age out on their normal cycle).

Are there backups and disaster recovery?

Yes — automated, encrypted daily backups managed by the database platform (Supabase). Enhanced point-in-time recovery (sub-24-hour RPO) is a near-term hardening item on our security roadmap.

Is there an audit trail?

Yes. Security-relevant and data-change events are written to a tenant-isolated, strict-insert audit log; e-signature actions have a dedicated audit trail (actor, IP, user-agent, timestamp). Operational logging and error monitoring (Sentry) support detection and diagnostics.

INCIDENT RESPONSE

What is your breach-notification commitment?

We will notify affected customers and regulators as required by law — **within 72 hours of becoming aware where GDPR applies** — including the nature of the incident, data involved, and remediation. A formalized incident-response runbook is being finalized as part of launch readiness.

SUB-PROCESSORS

Who are your sub-processors?

Supabase, Vercel, Stripe, Resend, Nylas, OpenAI, Sentry — all US-based. See the accompanying Sub-processor List for purpose and data scope. Customers are notified in advance of material changes per the DPA.