scm.cc security overview

Operator: Persoon.ai Inc. Service: scm.cc production at app.scm.cc. Last reviewed 2026-11-12. Download: PDF.

This overview is written for security and procurement teams. It states what is in place and what is not. scm.cc holds no SOC 2 report, no ISO 27001 certificate and no FedRAMP authorization, and no independent penetration test has been commissioned. This page makes no certification, authorization or compliance claim.

Architecture

scm.cc is a Next.js web application served by Vercel, backed by a Supabase-managed Postgres database with Supabase authentication and object storage. Scheduled jobs (connector syncs, monthly continuous-monitoring runs) run inside the application. Source code lives in GitHub; every change ships through a reviewed pull request with automated test, security and migration gates.

Source connections to customer systems (cloud, code and database security tools) are read-only. scm.cc ingests findings and configuration metadata, not raw Controlled Unclassified Information or document contents.

Tenancy and row-level security

Every customer organization is a separate tenant. Tenant tables carry an organization key and are protected by FORCE row-level security in Postgres; the application connects as a non-owner database role, so a query cannot read another organization’s rows even if application code is wrong. Per-organization trust pages are opt-in.

Encryption, MFA and SSO

- All traffic uses TLS. Data at rest is encrypted by the database and storage providers.
- Connector credentials and OIDC client secrets are additionally encrypted at the application layer with AES-256-GCM. SCIM and auditor tokens are stored only as hashes.
- Users can enroll a TOTP second factor; roles that handle pay data must verify one. MFA is enforced on the operator’s administrative consoles.
- Enterprise organizations can use SAML 2.0 or OIDC single sign-on, SCIM 2.0 provisioning and deprovisioning, and an SSO-only setting.
- Customer-managed keys (BYOK) are not offered.

Logging

Security-relevant events are written to a per-organization audit log: sign-ins and their reason, SSO connection changes, SCIM lifecycle events, auditor-token reads and administrative changes. Members can see auditor access. Production health is checked after every deploy and on a schedule. scm.cc does not run a SIEM or a 24x7 on-call rotation.

Backups and the restore drill

The database is backed up daily by the provider. A restore drill runs on a schedule and its evidence is recorded in the repository (most recent recorded drill: 2026-11-01). scm.cc does not publish an uptime percentage, RTO or RPO commitment, and does not run multi-region failover.

Hosting regions

The application runs on Vercel and Supabase, whose infrastructure runs on AWS. Neither is a FedRAMP-authorized environment for this service. Customer data and application compute are hosted in the United States: the production database is in AWS us-east-1 (verified with the provider on 2026-11-12) and application functions run in Vercel iad1 (Washington, D.C., AWS us-east-1), in the same region as the database. No product, including pay, offers EU data residency. EU and UK personal data is transferred under the Standard Contractual Clauses and the UK Addendum. The decision and evidence are in public issue #2421 (ADR-0024). A future in-boundary hosting path on AWS GovCloud is tracked separately in #1049, with no date promised.

Subprocessors

- Vercel: application hosting and edge delivery.
- Supabase: Postgres database, authentication and storage.
- Cloudflare: DNS and edge.
- Resend: transactional email.
- Stripe: billing and payment processing; card numbers are not stored by scm.cc.
- Anthropic: AI drafting features, only when a customer uses them; receives only the metadata needed for a request.
- GitHub: source connector, only when a customer connects it.

The maintained list is at app.scm.cc/trust/subprocessors.

Vulnerability management and disclosure

Every build runs a dependency audit (high and critical advisories fail the build), a secret scan, a static-analysis gate and container image checks; an unauthenticated DAST probe runs against staging. Dependencies are updated automatically. Confirmed vulnerabilities are remediated against severity targets published on app.scm.cc/legal/security. Report a suspected vulnerability to security@scm.cc; the channel is described in security.txt. There is no paid bug bounty. No independent penetration test has been commissioned yet; the SOC 2 and pen-test timing decision is pending with the owner.

Further documents

A full security questionnaire answer pack (CAIQ-Lite style) and draft contract documents are available on request from sales@scm.cc. Contract drafts are not offered until counsel review and owner approval are complete.