FIMIL, INC.

VSA Core v2022

Vendor Security Alliance Core questionnaire — focused security and privacy assessment covering key controls, CCPA/CPRA, and GDPR requirements.

March 20, 2026

Security Questionnaire Response

trust.fimil.dev

security@fimil.dev

Response Summary

Answer	Count	Percentage
Yes	77	70.6%
Partial	13	11.9%
No	15	13.8%
N/A	4	3.7%
Total	109	100%

Service Introduction

12/15 controls satisfied

ID	Question	Answer	Explanation
SI-1a	Company name.	YES	Fimil, Inc. — a Delaware C Corporation.
SI-1b	Company website.	YES	https://fimil.dev
SI-1c	Primary contact for security inquiries.	YES	security@fimil.dev — 48-hour acknowledgment SLA per SECURITY.md.
SI-2a	Describe the service being evaluated.	YES	Fimil is a unified application security platform that orchestrates open-source security scanners (SAST, SCA, Secrets, IaC, Container) behind a single dashboard with finding deduplication, priority scoring, and policy enforcement.
SI-2b	What data does the service process on behalf of customers?	YES	User email and name, OAuth tokens for Git provider integration, and temporarily processed source code (ephemeral, never persisted). Scan findings stored in tenant-isolated PostgreSQL.
SI-3a	Is the service hosted in the cloud, on-premise, or hybrid?	YES	Cloud-hosted on DigitalOcean Kubernetes (SaaS). An Enterprise self-hosted deployment model is also available for on-premise installation.
SI-3b	Which cloud providers are used?	YES	DigitalOcean (infrastructure, managed PostgreSQL, container registry), Cloudflare (CDN/DDoS), Stripe (payments), Resend (email), PostHog (analytics).
SI-3c	Data center locations.	YES	US-based DigitalOcean data center region. Single-region deployment currently.
SI-4a	Technology stack used.	YES	Python/FastAPI backend, React/TypeScript frontend, PostgreSQL, Redis, Celery, Docker containers for scanner isolation, Kubernetes on DigitalOcean.
SI-5a	Most recent penetration test report available?	NO	No external penetration test has been conducted. This is the primary remaining gap (ISO A.5.35 FAIL).
SI-5b	Information Security Policies available for review?	YES	Comprehensive policy suite: ISMS Policy, Access Control Policy, Data Governance Policy, Change Management Policy, Incident Response Plan, People Security Policy, and Vendor Risk Management Policy.
SI-5c	Data Flow Diagram available?	PARTIAL	Architecture and data flow documented in technical documentation. No standalone visual data flow diagram maintained yet.
SI-5d	SOC 2 Type II or ISO 27001 certification available?	NO	ISO 27001 and SOC 2 controls implemented with comprehensive policy suite. Certification audits planned but not yet completed.
SI-5e	Privacy Policy available?	YES	Privacy Policy at /privacy, Cookie Policy at /legal/cookies, DPA at /legal/dpa, Acceptable Use Policy at /legal/acceptable-use.
SI-5f	Sub-processor list available?	YES	Sub-processor list published in trust center with DPAs executed for all vendors: DigitalOcean, Stripe, Resend, PostHog.

Data Inventory

4/14 controls satisfied

ID	Question	Answer	Explanation
DI-1	Do you process driver's license or State ID numbers?	NO	Fimil does not collect or process driver's license or State ID numbers. The platform handles application security scanning data only.
DI-2	Do you process financial data?	NO	No financial data is processed directly. Payment processing is handled entirely by Stripe; Fimil does not store credit card numbers or bank details.
DI-3	Do you process Social Security Numbers?	NO	Fimil does not collect or process Social Security Numbers.
DI-4	Do you process passport numbers?	NO	Fimil does not collect or process passport numbers.
DI-5	Do you process biometric data?	NO	Fimil does not collect or process biometric data.
DI-6	Do you process health, insurance, or medical data?	NO	Fimil does not collect or process health, insurance, or medical data.
DI-7	Do you process precise location or GPS data?	NO	Fimil does not collect precise location or GPS data. IP addresses are logged for security monitoring only.
DI-8	Do you process voice recordings?	NO	Fimil does not collect or process voice recordings.
DI-9	Do you process audio or video data?	NO	Fimil does not collect or process audio or video data.
DI-10	Do you process email addresses?	YES	Email addresses are collected for user authentication, account management, and transactional notifications (scan results, critical findings alerts).
DI-11	Do you process names?	YES	User full names are collected during registration for account identification and display within the platform.
DI-12	Do you process log data (IP address, time, browser)?	YES	IP addresses, timestamps, and user agents are logged for security monitoring, audit trails, and threat detection (brute force, credential stuffing).
DI-13	Do you process telephone numbers?	NO	Fimil does not collect or process telephone numbers.
DI-14	Do you process tracking data (cookies, pixels)?	YES	Cookie consent mechanism with Accept All / Reject Non-Essential / Customize options. Analytics (PostHog) requires explicit consent. DNT browser signal respected. Full consent audit trail maintained.

Security CORE Controls

36/45 controls satisfied

ID	Question	Answer	Explanation
CORE-1	Do you maintain a data classification policy?	YES	Data Governance Policy (FIMIL-DGP-001) establishes four-level classification: Public, Internal, Confidential (user PII, scan results), and Restricted (encryption keys, OAuth tokens).
CORE-2	Is customer data encrypted in transit?	YES	TLS 1.2+ enforced for all public-facing traffic via cert-manager with Let's Encrypt. HSTS enabled. HTTP redirected to HTTPS.
CORE-3	Is customer data encrypted at rest?	YES	MultiFernet encryption (AES-128-CBC + HMAC-SHA256) with versioned key rotation for sensitive fields. Database encryption via DigitalOcean managed PostgreSQL. S3 backups encrypted.
CORE-4	Do you have a process for managing encryption keys?	PARTIAL	Encryption keys stored as environment variables via Kubernetes Sealed Secrets. MultiFernet versioned key rotation implemented for seamless encryption key transitions. KMS integration not yet in place.
CORE-5	How do you control access to customer data?	YES	Five-level RBAC (Operator > Admin > Security > Developer > Viewer) enforced at every API endpoint. Row-level tenant isolation via TenantScopedModel with ContextVar enforcement.
CORE-6	Do you require MFA for internal access to production systems?	YES	TOTP-based MFA with recovery codes implemented in the application with two-step login flow and encrypted secret storage. Production Kubernetes access controlled via DigitalOcean authentication and Kubernetes RBAC.
CORE-7	Do you support SSO for internal authentication?	YES	OAuth2/OIDC federation supported with GitHub and generic OIDC providers for user authentication, available on all plans.
CORE-8	What is your internal password policy?	YES	Minimum 12 characters with mixed case, digit, and special character requirements. Argon2id (memory-hard) hashing with salt. Account lockout after 5 failed attempts (30-minute cooldown).
CORE-9	Do you support SSO for customer authentication?	YES	OAuth2/OIDC with GitHub and generic OIDC providers. SSO available on all plans at no additional cost.
CORE-10	Does the application support customer-enforced MFA?	YES	TOTP-based MFA implemented with recovery codes, two-step login flow, and encrypted secret storage. Users can enable MFA on their accounts.
CORE-11	Do you have a formal Information Security Program?	YES	ISMS Policy (FIMIL-ISMS-001) establishes the formal ISMS aligned with ISO 27001:2022, supported by a comprehensive policy suite covering access control, data governance, change management, and incident response.
CORE-12	Are InfoSec policies reviewed at least annually?	YES	ISMS Policy defines annual policy review cadence. Policies are version-controlled in Git. Statement of Applicability tracks control implementation status.
CORE-13	Do you have an information security risk management program?	YES	Risk Assessment (FIMIL-RISK-001) uses a 5x5 likelihood-impact matrix identifying 15 risks with documented treatment plans and remediation timelines.
CORE-14	Do you perform background checks on employees?	PARTIAL	People Security Policy documents background verification requirements for all roles. Not yet exercised as currently sole founder.
CORE-15	Are personnel required to sign confidentiality agreements?	PARTIAL	People Security Policy mandates confidentiality agreements for all personnel. Policy documented and ready; not yet exercised as currently sole founder.
CORE-16	Do you have procedures for termination including access revocation?	YES	People Security Policy includes offboarding checklists with access revocation. Technical controls support immediate user deactivation, session invalidation, and API token revocation.
CORE-17	Do you perform regular vulnerability scanning?	YES	Fimil's own platform orchestrates 12 scanners (Semgrep, Bandit, Trivy, Grype, OSV-Scanner, Gitleaks, TruffleHog, Checkov, Hadolint, Syft) in CI/CD on every push and PR.
CORE-18	What is your timeframe for patching critical vulnerabilities?	YES	Formal patch management SLA: Critical 24h, High 7d, Medium 30d. Trivy blocks deployment of containers with critical vulnerabilities. EPSS enrichment prioritizes actively exploited CVEs. Dependabot provides automated dependency update PRs.
CORE-19	Do you perform penetration testing?	NO	No external penetration test or independent security audit has been conducted. This is the primary remaining gap (ISO A.5.35 FAIL).
CORE-20	Are endpoint devices centrally managed with standard security configurations?	PARTIAL	People Security Policy documents device security requirements (full-disk encryption, screen lock). Currently sole founder; formal MDM to be deployed as team grows.

ID	Question	Answer	Explanation
CORE-21	Is the production network segmented?	YES	Kubernetes network policies segment the production network. Scanner containers run with --network=none for complete isolation. Ingress-only access with TLS.
CORE-22	Are production systems uniformly configured and hardened?	YES	All production workloads run as immutable Docker containers with standardized configurations: non-root, read-only filesystem, cap_drop ALL, no-new-privileges, resource limits.
CORE-23	Is network traffic encrypted over public networks?	YES	TLS 1.2+ enforced for all public traffic via cert-manager. HSTS headers enabled. Auth cookies set with Secure flag.
CORE-24	Do you use standard cryptographic frameworks (no custom cryptography)?	YES	All implementations use standard libraries: Argon2id for passwords, MultiFernet (AES-128-CBC + HMAC-SHA256) for field encryption with key rotation, SHA-256 for token hashing, secrets module for random generation.
CORE-25	Do you have a security awareness and training program?	PARTIAL	People Security Policy documents role-specific training requirements. Currently sole founder with deep security domain expertise; formal training program framework ready for team scaling.
CORE-26	Do you have breach detection and anomaly monitoring with alerting?	YES	Security alert system with brute force detection, credential stuffing detection, API anomaly detection, and suspicious scan pattern detection. Falco provides runtime container integrity monitoring.
CORE-27	Are all security events logged in production?	YES	Audit logging tracks 40+ action types with user_id, IP, timestamp, action, resource_type, and resource_id. Structlog JSON output with request correlation IDs.
CORE-28	Do you have a Security Incident Response Program?	YES	Incident Response Plan (FIMIL-IRP-001) with four severity levels, incident commander role, response phases, and breach notification procedures aligned to GDPR and CCPA timelines.
CORE-29	How is the IRP tested?	PARTIAL	IRP documented with technical capabilities implemented (Incident model, SecurityAlert, auto-blocking). DR test completed March 2026 validated recovery procedures. Tabletop exercises and simulated drills planned but not yet conducted.
CORE-30	Do you have a formal SLA for incident response and client notification?	YES	IRP defines response timelines by severity. SECURITY.md provides 48-hour acknowledgment SLA. Breach notification aligned to GDPR 72-hour and CCPA requirements.
CORE-31	Do you perform static code analysis?	YES	Semgrep and Bandit run in CI/CD on every push and PR. Ruff linter and ESLint with strict TypeScript rules enforce code quality.
CORE-32	Do you have secure development lifecycle practices?	YES	Change Management Policy documents SDLC security integration. CI pipeline runs linting, tests, SAST, and container scanning. Pre-commit hooks enforce code style and secret scanning.
CORE-33	Do you monitor vulnerabilities in third-party dependencies?	YES	Trivy, Grype, and OSV-Scanner provide SCA scanning. EPSS enrichment for exploit probability. Reachability analysis distinguishes direct from transitive dependency vulnerabilities.
CORE-34	Do you maintain a bill of materials for third-party libraries?	YES	Syft SBOM scanner generates software bill of materials. Poetry and npm lockfiles track all dependency versions.
CORE-35	Does the customer-facing application have standardized roles and permissions?	YES	Five standardized roles: Operator, Admin, Security, Developer, and Viewer with enforced permissions at every endpoint.
CORE-36	Are audit trails available for customer data access?	YES	Comprehensive audit logging with 40+ event types. Admin dashboard access to verbose logs with filtering. CSV export for offline analysis.
CORE-37	Does the application support custom data retention policies?	YES	Report retention configurable at 30 days. Data Governance Policy defines retention schedules for all data categories. Account closure and deletion procedures documented.
CORE-38	Is API rate limiting implemented?	YES	Redis-backed sliding window rate limiting: auth endpoints at 10 req/min, general API at 100 req/min. Configurable thresholds.
CORE-39	How are API keys stored and managed?	YES	API tokens are SHA-256 hashed before storage; plaintext shown only once at creation. Tokens are scoped, revocable, and tracked with audit trails.
CORE-40	How do you conduct internal audits?	YES	Comprehensive internal compliance assessment against ISO 27001 and SOC 2. Statement of Applicability tracks control status. Compliance Register monitors regulatory obligations.
CORE-41	Have you completed any external audits or certifications?	NO	No external audit or independent security assessment has been conducted. External penetration testing and certification audits are planned.
CORE-42	Which security and privacy standards do you comply with?	YES	Controls aligned with ISO 27001:2022 and SOC 2 Type II. GDPR and CCPA compliance tracked in Compliance Register. Formal certification not yet obtained.

ID	Question	Answer	Explanation
CORE-43	Do you share customer data with third parties?	PARTIAL	Sub-processors (DigitalOcean, Stripe, Resend, PostHog) process limited customer data as documented. DPAs executed with all vendors. No data is sold.
CORE-44	Is your Privacy Notice externally available?	YES	Privacy Policy at /privacy, Cookie Policy at /legal/cookies, DPA at /legal/dpa, AUP at /legal/acceptable-use. All publicly accessible.
CORE-45	Do you have a responsible disclosure and vulnerability reporting policy?	YES	SECURITY.md published with responsible disclosure policy, testing scope, safe harbor provisions, and security@fimil.dev contact with 48-hour acknowledgment SLA.

Privacy Introduction

0/0 controls satisfied

ID	Question	Answer	Explanation

USA Privacy (CCPA/CPRA)

9/14 controls satisfied

ID	Question	Answer	Explanation
USP-1	Can you provide data breach notification to the state Attorney General within required timeframes?	YES	Incident Response Plan (FIMIL-IRP-001) includes breach notification procedures with timelines aligned to CCPA requirements and state AG notification.
USP-2	Do you inform consumers of the categories of data collected and the purposes before or at the time of collection?	YES	Privacy Policy at /privacy discloses categories collected (email, name, log data, cookies), purposes, and legal bases before data collection occurs.
USP-3	Do you have a mechanism to provide a copy of collected personal information to a consumer within 45 days of a verifiable request?	YES	Admin API endpoints implemented for GDPR data export (DSAR fulfillment). Data subject rights procedures documented in Data Governance Policy with automated export capability.
USP-4	Do you have a mechanism to delete a consumer's personal information upon verifiable request?	YES	Admin API endpoints implemented for GDPR data erasure. Account deletion with cascading data disposal including user deactivation, session invalidation, and token revocation.
USP-5	Is the deletion request cascaded to your service providers?	YES	DSAR erasure API handles internal data deletion. DPAs with sub-processors include data deletion requirements and are triggered as part of the erasure workflow.
USP-6	Does your website disclose the categories of information collected, sources, purposes, and third parties with whom data is shared?	YES	Privacy Policy at /privacy provides comprehensive disclosure of data categories, collection sources, processing purposes, and sub-processor list with sharing details.
USP-7	If you sell personal data, do you disclose the categories sold and categories disclosed for business purposes?	NA	Fimil does not sell personal data. No categories of data are sold to third parties.
USP-8	If you resell personal information received from another business, do you provide explicit notice and opt-out to consumers?	NA	Fimil does not resell personal information. This scenario is not applicable.
USP-9	If you sell personal data, do you inform customers and provide an opt-out mechanism?	NA	Fimil does not sell personal data. No opt-out mechanism is needed.
USP-10	Do you provide the same level of service regardless of whether consumers exercise their CCPA rights?	YES	Fimil does not discriminate against users who exercise privacy rights. Service level and pricing are identical regardless of CCPA rights exercised.
USP-11	Do you provide a minimum of two contact methods for consumer privacy requests?	YES	Privacy requests can be submitted via security@fimil.dev email and through the contact form on the website at /contact.
USP-12	Is a publicly available CCPA rights notice available on your website?	YES	Privacy Policy at /privacy includes CCPA rights disclosure covering the right to know, delete, and opt-out, with instructions for exercising these rights.
USP-13	Do you provide a 'Do Not Sell My Personal Information' link or equivalent mechanism?	NA	Fimil does not sell personal data. Cookie consent mechanism allows users to reject non-essential cookies. DNT browser signal is respected as automatic opt-out.
USP-14	Do you provide privacy training for personnel handling personal information at least annually?	PARTIAL	People Security Policy documents privacy training requirements. Currently sole founder with privacy policy expertise; formal annual training program to be implemented as team grows.

GDPR Privacy

16/21 controls satisfied

ID	Question	Answer	Explanation
GDPR-1	Does the data remain the property of the Controller (customer)?	YES	Terms of Service and DPA confirm customer data remains the property of the customer. Fimil acts as a data processor only.
GDPR-2	Do you follow the Controller's instructions for data processing?	YES	DPA at /legal/dpa defines data processing scope and instructions. Fimil processes customer data only as necessary to provide the security scanning service.
GDPR-3	Do you refrain from using sub-processors without advance notification or consent from the Controller?	YES	Sub-processor list published in trust center. DPA requires notification of sub-processor changes. All current sub-processors are disclosed with DPAs executed.
GDPR-4	Do your sub-processors have equivalent security and privacy controls?	YES	Vendor Risk Management Policy requires security assessment for all vendors. Tier 1 vendors (DigitalOcean, GitHub, Stripe) maintain SOC 2 certification. DPAs executed with all sub-processors.
GDPR-5	Do you cooperate with Regulators?	YES	ISMS Policy and Incident Response Plan include regulatory cooperation procedures. Compliance Register tracks regulatory obligations including GDPR supervisory authority requirements.
GDPR-6	Do you keep all received information confidential?	YES	Data classified as Confidential or Restricted per Data Governance Policy. MultiFernet encryption with key rotation for sensitive fields, tenant isolation, RBAC, and secret redaction in logs protect all received information.
GDPR-7	Do you report data breaches within 72 hours?	YES	Incident Response Plan (FIMIL-IRP-001) defines breach notification procedures with explicit GDPR 72-hour timeline for supervisory authority notification.
GDPR-8	Do you assist the Controller in managing breach consequences?	YES	IRP includes customer notification procedures and cooperation during incident response. Post-incident review and root cause analysis shared with affected customers.
GDPR-9	Do you keep records of all processing activities?	YES	Audit logging tracks 40+ action types with full attribution. Data Governance Policy documents processing activities. Compliance Register maintains records of processing by legal basis.
GDPR-10	Do you assist the Controller in responding to data subject rights requests?	YES	Data Governance Policy documents data subject rights procedures (access, rectification, erasure, portability). DPA commits to assisting controllers with DSAR fulfillment.
GDPR-11	Do you delete or return all personal data at end of contract?	YES	Data Governance Policy documents data disposal procedures for account closure. DPA includes data return/deletion obligations. Source code is ephemeral by design.
GDPR-12	Do you have adequate measures to protect personal data?	YES	Multi-layered protection: TLS in transit, MultiFernet encryption at rest with key rotation, Argon2id for passwords, TOTP-based MFA, RBAC, tenant isolation, audit logging, security monitoring, and container hardening.
GDPR-13	If not established in the EU, have you appointed an Article 27 representative?	NO	No Article 27 representative appointed yet. As a US-based company processing EU data, this appointment is planned as the EU customer base grows.
GDPR-14	Are DPO contact details available on your website privacy notice?	PARTIAL	Privacy Policy lists security@fimil.dev as the contact for privacy inquiries. Formal DPO appointment with dedicated contact details to be established as organization scales.
GDPR-15	Is data processed only as long as needed for the stated purpose?	YES	Data Governance Policy defines retention schedules for all data categories. Source code is ephemeral (clone-scan-delete). Report retention configurable at 30 days. Session data expires in 24 hours.
GDPR-16	Are all parties committed to confidentiality?	YES	People Security Policy mandates confidentiality agreements. Sub-processor DPAs include confidentiality obligations. Data classified and handled per Data Governance Policy.
GDPR-17	Do you assist the Controller in responding to data subject requests?	YES	DPA commits to assisting controllers with DSAR fulfillment. Data Governance Policy documents procedures for access, rectification, erasure, and portability requests.
GDPR-18	Do you cooperate with the Controller on Data Protection Impact Assessments (DPIA)?	YES	DPA includes DPIA cooperation commitment. Formal DPIA process implemented with template and register. Risk Assessment methodology and Data Governance Policy provide the framework for privacy impact assessments.
GDPR-19	Do you refrain from onward transfers of personal data outside the EEA without Controller permission?	PARTIAL	Infrastructure is US-based (DigitalOcean). DPA addresses international data transfers. Standard Contractual Clauses (SCCs) to be incorporated as the EU customer base grows.

ID	Question	Answer	Explanation
GDPR-20	Are personnel handling personal information trained in privacy obligations at least annually?	PARTIAL	People Security Policy documents privacy training requirements. Currently sole founder with privacy expertise; formal annual privacy training to be implemented as team grows.
GDPR-21	If handling sensitive personal data, are personnel subject to background checks?	PARTIAL	People Security Policy documents background verification requirements. Fimil handles minimal personal data (email, name). Not yet exercised as currently sole founder.