FIMIL, INC.

Compliance & Security Report

Comprehensive overview of security controls, compliance frameworks, and data protection practices.

March 20, 2026

CONFIDENTIAL

trust.fimil.dev

security@fimil.dev

Compliance Frameworks

Framework	Status	Description
SOC 2 Type II	IN PROGRESS	Controls aligned with Trust Services Criteria. Formal audit planned post-seed.
ISO 27001:2022	IN PROGRESS	ISMS framework established with comprehensive policy suite and controls implemented. Certification planned for 2027.
NIST CSF 2.0	IN PROGRESS	Comprehensive mapping to the six CSF functions (Govern, Identify, Protect, Detect, Respond, Recover). ~75% coverage implemented; pending external validation.
CIS Controls v8	IN PROGRESS	Implementation-focused security controls aligned across all 18 control groups. ~70% coverage implemented; formal gap assessment and external validation pending.
OWASP ASVS Level 2	IN PROGRESS	Application Security Verification Standard covering authentication, session management, access control, input validation, and API security. Core to our identity as an AppSec platform.
GDPR	IN PROGRESS	EU General Data Protection Regulation. Privacy policy, DPAs, cookie consent with audit trail, and breach notification implemented. DSAR automation and DPIAs in progress.
CCPA/CPRA	IN PROGRESS	California Consumer Privacy Act and California Privacy Rights Act. Privacy disclosures and cookie consent implemented. Consumer request workflows in progress.
CSA STAR Level 1	IN PROGRESS	Cloud Security Alliance STAR Level 1 self-assessment completed via CAIQ v4 (261 questions across 17 security domains). Self-assessment published on trust center. Formal registry submission planned.
FedRAMP Li-SaaS	IN PROGRESS	Low-Impact SaaS authorization prerequisites in progress: System Security Plan, Continuous Monitoring Plan, network boundary documentation, and federal incident reporting procedures completed. FIPS 140-2 KMS integration and 3PAO engagement pending.
FedRAMP	PLANNED	Full Federal Risk and Authorization Management Program authorization at Moderate baseline. Requires 3PAO assessment and JAB or Agency authorization.
Cyber Essentials	IN PROGRESS	UK government-backed cybersecurity certification. All five technical controls implemented: firewalls (Cloudflare WAF), secure configuration (container hardening), user access control (RBAC with MFA), malware protection (scanner isolation, Falco monitoring), and security update management (Dependabot, Trivy). Formal self-assessment certification pending.
SLSA Framework	IN PROGRESS	Build provenance attestation via GitHub Actions, SPDX SBOMs generated for all container images, and Cosign keyless image signing implemented. Formal SLSA L2 assessment and registry pending.

Data Protection

4/5 controls implemented

Control	Status	Description
Encryption at Rest	IMPLEMENTED	Database encryption at rest via managed provider (AES-256). Application-layer encryption using Fernet (AES-128-CBC with HMAC-SHA256 authentication) for sensitive fields including OAuth tokens and API credentials.
Encryption in Transit	IMPLEMENTED	TLS 1.2+ enforced on all connections. HSTS enabled. Certificate management via Let's Encrypt with automated renewal.
Data Classification	IMPLEMENTED	Four-level classification scheme (Public, Internal, Confidential, Restricted) with defined handling requirements per level.
Data Retention & Deletion	IMPLEMENTED	Documented retention schedules per data category. Source code is ephemeral — cloned, scanned, and deleted (never persisted). Configurable report retention. Automated DSAR export and erasure endpoints with anonymization.
Key Lifecycle Management	PARTIAL	Versioned encryption key rotation via MultiFernet — new data encrypted with latest key, old data decryptable with any known key. Re-encryption tooling for key migration. KMS integration planned for FIPS 140-2 requirements.

Privacy & Data Rights

4/5 controls implemented

Control	Status	Description
Cookie Consent & Tracking	IMPLEMENTED	Granular cookie consent with Accept/Reject/Customize options. Three categories (Necessary, Functional, Analytics). Full audit trail with IP, user agent, timestamp, and consent version. DNT signal respected.
Privacy Notices & Transparency	IMPLEMENTED	Privacy Policy, Cookie Policy, and Data Processing Agreement published. Data collection practices disclosed per GDPR Articles 13-14 and CCPA requirements.
Data Subject Request Handling	IMPLEMENTED	Admin API endpoints for data export (GDPR Article 15) and erasure (GDPR Article 17) with full user data portability. Anonymization preserves audit trail while removing PII. Session invalidation on erasure.
Data Protection Impact Assessments	IMPLEMENTED	Formal DPIA process (FIMIL-DPIA-001) per GDPR Article 35 with six defined trigger criteria, step-by-step assessment methodology, fillable template with risk matrix, DPO review and sign-off workflow, and maintained DPIA register.
International Data Transfers	PARTIAL	DPAs executed with all subprocessors. Standard Contractual Clauses (SCCs) for EU-to-US transfers planned for annexation to DPA.

Access Control

4/4 controls implemented

Control	Status	Description
Role-Based Access Control	IMPLEMENTED	Five-level RBAC hierarchy enforced at every API endpoint. Tenant-level isolation with row-level data separation.
Authentication Security	IMPLEMENTED	Strong password policy (12+ chars, Argon2id hashing), TOTP-based MFA with recovery codes, account lockout after failed attempts, automated brute force and credential stuffing detection. OAuth2/OIDC federation supported for customer SSO.
Privileged Access Management	IMPLEMENTED	Privileged operations logged with full attribution. Impersonation restricted with 1-hour session caps and complete audit trail.
Access Reviews	IMPLEMENTED	Automated access review reports via operator portal: stale user detection (90+ days inactive), unused API token auditing, privileged user inventory across tenants. Automated deprovisioning on account deactivation with bulk token revocation.

Infrastructure Security

6/6 controls implemented

Control	Status	Description
Container Hardening	IMPLEMENTED	All containers run as non-root with read-only filesystems, dropped capabilities, and no-new-privileges flag. Scanner containers are fully network-isolated.
Network Segmentation	IMPLEMENTED	Kubernetes network policies enforce strict pod-to-pod communication rules. Scanner workloads run with no network access.
Runtime Monitoring	IMPLEMENTED	Falco-based runtime security monitoring with custom detection rules for process anomalies, file integrity changes, and container drift.
Vulnerability Management	IMPLEMENTED	Container image scanning (Trivy) in CI/CD blocks deployment on critical vulnerabilities. SAST scanning (Semgrep, Bandit) runs on own codebase via GitHub Actions. Fimil scans its own repositories through the platform.
Asset Inventory	IMPLEMENTED	Formal asset register (FIMIL-AM-001) with 25+ assets classified across infrastructure, software, data, external services, and code repositories. Quarterly review cycle with ownership tracking and lifecycle management.
Web Application Firewall	IMPLEMENTED	Cloudflare WAF deployed with managed rulesets for OWASP Top 10 protection, bot management, and rate limiting at the edge.

Application Security

5/5 controls implemented

Control	Status	Description
Secure Development Lifecycle	IMPLEMENTED	CI pipeline enforces linting, testing, type checking, SAST (Semgrep, Bandit), and container scanning. Pre-commit hooks catch issues before code reaches the repository. Fimil scans its own repositories through the platform.
Input Validation & Injection Prevention	IMPLEMENTED	Pydantic schema validation on all API inputs. ORM-based parameterized queries prevent SQL injection. CSRF protection via double-submit cookie pattern.
Secret Management	IMPLEMENTED	Sealed secrets for production credentials. API tokens stored as SHA256 hashes. Secret scanning in pre-commit hooks and CI pipeline.
Rate Limiting & Abuse Prevention	IMPLEMENTED	Distributed rate limiting per endpoint category. Automated brute force detection and IP blocking. Credential stuffing detection with alerting.
Threat Modeling	IMPLEMENTED	Formal threat model (FIMIL-TM-001) using STRIDE methodology covering the three highest-risk areas: scanner execution pipeline, authentication & session management, and multi-tenant data isolation. 16 threats identified with likelihood/impact scoring and prioritized remediation. Reviewed annually or upon significant architecture change.

Incident Response

3/3 controls implemented

Control	Status	Description
Incident Response Plan	IMPLEMENTED	Documented IR plan with four severity levels, defined response phases, escalation procedures, and communication templates.
Breach Notification	IMPLEMENTED	Customer notification procedures documented with defined timelines aligned to GDPR (72-hour) and CCPA requirements.
Audit Logging	IMPLEMENTED	40+ security-relevant event types logged with full attribution: actor, tenant, IP, user agent, and request correlation ID.

Business Continuity

2/3 controls implemented

Control	Status	Description
Backup & Recovery	IMPLEMENTED	Nightly encrypted backups to offsite storage (S3). Documented restore procedures with RTO of 4 hours and RPO of 24 hours.
High Availability	PARTIAL	Horizontal pod autoscaling with pod disruption budgets. Rolling deployments with zero-downtime guarantee and automatic rollback. Single-region deployment; multi-region failover and Redis HA planned.
Disaster Recovery Testing	IMPLEMENTED	DR test completed successfully (March 2026). Backup restore validated with documented RTO/RPO. Semi-annual testing schedule established.

Vendor Management

2/2 controls implemented

Control	Status	Description
Vendor Risk Assessment	IMPLEMENTED	Three-tier vendor classification with documented risk assessments for all critical and significant vendors.
Data Processing Agreements	IMPLEMENTED	DPAs executed with all vendors who process customer data. Exit strategies documented for critical vendors.

Governance

3/4 controls implemented

Control	Status	Description
Policy Framework	IMPLEMENTED	Comprehensive policy suite: ISMS, Access Control, Data Governance, Incident Response, Change Management, People Security, Vendor Risk Management.
Risk Management	IMPLEMENTED	Formal risk assessment methodology with risk register, treatment plans, and annual review cycle.
Independent Security Review	PLANNED	External penetration test and independent security audit planned.
Continuous Compliance Monitoring	IMPLEMENTED	Continuous monitoring program with automated controls (Dependabot, Trivy, Falco, Cosign) and scheduled manual reviews (quarterly access reviews, semi-annual DR testing, annual risk assessment). Monthly vulnerability reporting and quarterly ConMon status reports.

Supply Chain Security

4/4 controls implemented

Control	Status	Description
Software Bill of Materials (SBOM)	IMPLEMENTED	Syft integrated as a scanner for customer repositories. SPDX SBOMs generated for all container images in CI/CD pipeline via anchore/sbom-action and retained as build artifacts.
Build Provenance & Attestation	IMPLEMENTED	Cryptographic build provenance attestation generated via actions/attest-build-provenance for all container images. GitHub Actions CI/CD provides hosted build platform with OIDC-based identity.
Container Image Signing	IMPLEMENTED	All container images signed with Cosign (keyless via Sigstore/Fulcio) after vulnerability scanning passes. Signatures stored alongside images in the container registry.
Dependency Integrity	IMPLEMENTED	Lockfiles (package-lock.json, poetry.lock) pin dependency versions. Reachability analysis classifies direct vs. transitive dependencies. Dependabot configured for automated dependency updates across all repositories.

Subprocessors

Vendor	Purpose	Location
DigitalOcean	Cloud infrastructure (compute, Kubernetes, managed database)	United States
GitHub	Source code hosting, CI/CD, repository integrations	United States
Stripe	Payment processing and billing	United States
Cloudflare	CDN, DNS, DDoS protection, WAF	Global (anycast)
Resend	Transactional email delivery	United States
PostHog	Product analytics (consent-gated)	United States

Security Questionnaire Results

Questionnaire	Total	Yes	Partial	No	N/A
MVSP v2.0	25	18 (72%)	4 (16%)	1 (4%)	2
CAIQ v4 v4.0	261	171 (66%)	53 (20%)	12 (5%)	25
VSA Full v2021	112	83 (74%)	17 (15%)	11 (10%)	1
VSA Core v2022	109	77 (71%)	13 (12%)	15 (14%)	4

Published Documents

Document	URL
Privacy Policy	https://fimil.dev/privacy
Terms of Service	https://fimil.dev/terms
Data Processing Agreement	https://fimil.dev/legal/dpa
Service Level Agreement	https://fimil.dev/legal/sla
Acceptable Use Policy	https://fimil.dev/legal/acceptable-use
Cookie Policy	https://fimil.dev/legal/cookies
Security Policy	https://fimil.dev/security