FIMIL, INC.

MVSP v2.0

Minimum Viable Secure Product checklist — 25 baseline security controls for B2B software.

March 20, 2026

Security Questionnaire Response

trust.fimil.dev

security@fimil.dev

Response Summary

Answer	Count	Percentage
Yes	18	72.0%
Partial	4	16.0%
No	1	4.0%
N/A	2	8.0%
Total	25	100%

Business Controls

3/8 controls satisfied

ID	Question	Answer	Explanation
1.1	Vulnerability disclosure policy — Publish a vulnerability disclosure policy with testing scope, legal safe harbor, and contact details. Respond to reports within reasonable timeframes.	YES	SECURITY.md published with responsible disclosure policy, testing scope, safe harbor provisions, and security@fimil.dev contact. 48-hour acknowledgment SLA.
1.2	Customer testing — Enable customers to test the security of your application on request.	PARTIAL	No formal customer penetration testing process, but customers are not contractually blocked from testing. Security whitepaper published at /security.
1.3	Self-assessment — Perform security self-assessments using the latest MVSP release, at least annually.	YES	Comprehensive internal compliance assessment performed (ISO 27001 + SOC 2 mapping) with documented findings, gap analysis, and remediation plans.
1.4	External testing — Contract a security vendor to perform comprehensive penetration tests at least annually.	NO	No external penetration test or independent security audit has been conducted. This is the primary remaining gap (ISO A.5.35 FAIL).
1.5	Training — Implement role-specific security training for all personnel involved in product development and management.	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.
1.6	Compliance — Comply with applicable industry security standards (e.g., PCI DSS, HITRUST, ISO 27001, SSAE 18) and laws (e.g., GDPR).	PARTIAL	ISO 27001 and SOC 2 controls implemented with comprehensive policy suite. Certification audits planned but not yet completed. GDPR and CCPA requirements tracked in Compliance Register.
1.7	Incident handling — Notify relevant parties about security breaches involving sensitive information within 72 hours.	YES	Incident Response Plan (FIMIL-IRP-001) defines four severity levels, response phases, and breach notification procedures aligned to GDPR 72-hour and CCPA timelines.
1.8	Data handling — Ensure media sanitization processes based on NIST SP 800-88 for storage media holding unencrypted production data.	NA	Cloud-hosted on DigitalOcean managed infrastructure. No physical storage media under Fimil's control. Media sanitization is the cloud provider's responsibility under the shared responsibility model.

Application Design Controls

8/8 controls satisfied

ID	Question	Answer	Explanation
2.1	Single Sign-On — Implement SSO using modern, maintained, industry-standard protocols for all customers at no additional cost.	YES	OAuth2/OIDC federation supported with GitHub and generic OIDC providers. SSO available on all plans at no additional cost.
2.2	HTTPS-only — Redirect HTTP to HTTPS. Scan and address TLS issues. Include HSTS header. Set auth cookies as Secure.	YES	TLS enforced in production (REQUIRE_TLS=True). HSTS enabled. Auth cookies set with Secure, HttpOnly, and SameSite=lax flags. TLS managed via cert-manager with Let's Encrypt.
2.3	Security headers — Apply relevant security headers (CSP, X-Frame-Options). Disable caching for sensitive API responses.	YES	Nginx configuration includes Content-Security-Policy, X-Frame-Options, and X-Content-Type-Options headers. CORS configuration restricts cross-origin requests. Cloudflare WAF with managed rulesets provides additional protection.
2.4	Password policy — No character limits, allow 64+ characters, no secret questions as sole reset mechanism, email verification of changes, store hashed and salted with memory-hard function, enforce lockout.	YES	Password policy enforces 12+ characters with complexity requirements. Argon2id (memory-hard) hashing with salt. Account lockout after 5 failed attempts (30-minute cooldown). Email verification for SaaS registration. No secret questions used.
2.5	Security libraries — Use modern, maintained security frameworks and template languages that escape outputs and sanitize inputs.	YES	FastAPI with Pydantic validation for all API inputs. SQLAlchemy ORM prevents SQL injection. React JSX auto-escapes output. CSRF double-submit cookie pattern with constant-time comparison.
2.6	Dependency patching — Keep third-party dependencies up to date. Apply medium+ severity patches. Prioritize KEV.	YES	Dependabot configured across all repos for automated dependency updates. Trivy image scanning in CI/CD blocks critical container vulnerabilities. EPSS enrichment for exploit prioritization. Patch management SLA: Critical 24h, High 7d, Medium 30d.
2.7	Logging — Log authentication events, CRUD operations, security config changes, and data access. Include user ID, IP, timestamp, action, and object. Retain 30+ days. No sensitive data in logs.	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. Secret redaction prevents sensitive data in logs.
2.8	Encryption — Use modern encryption for data in transit and at rest, including backups.	YES	TLS 1.2+ for data in transit. MultiFernet (AES-128-CBC + HMAC-SHA256) with versioned key rotation for sensitive fields at rest. Database encryption via DigitalOcean managed provider. Backups compressed and stored in S3 with encryption.

Application Implementation Controls

4/5 controls satisfied

ID	Question	Answer	Explanation
3.1	List of data — Maintain a list of sensitive data types the application processes.	YES	Data Governance Policy (FIMIL-DGP-001) classifies data into four levels: Public, Internal, Confidential (user PII, scan results), and Restricted (encryption keys, OAuth tokens, API credentials).
3.2	Data flow diagram — Maintain an up-to-date diagram of how sensitive data reaches your systems and where it ends up being stored.	PARTIAL	Architecture documented in CLAUDE.md with data flow through scanner pipeline and storage layers. Data Governance Policy covers data handling requirements. No standalone visual data flow diagram maintained.
3.3	Vulnerability prevention — Train developers and implement guidelines to prevent auth bypass, insecure sessions, injections, XSS, CSRF, and untrusted data handling.	YES	OWASP-aware implementation: CSRF double-submit cookies, SQLAlchemy parameterized queries, Pydantic input validation, React auto-escaping, rate limiting, and RBAC. SAST scanning (Semgrep, Bandit) enforces secure coding in CI.
3.4	Time to fix vulnerabilities — Patch application vulnerabilities impacting security within 90 days. Prioritize actively exploited. Publish security bulletins.	YES	Formal patch management SLA: Critical 24h, High 7d, Medium 30d. Trivy blocks critical vulnerabilities in CI/CD. EPSS enrichment prioritizes actively exploited CVEs. Dependabot provides automated dependency update PRs.
3.5	Build and release process — Use version control and a consistent build process with provenance (SLSA Build Level 1). Store credentials separately from source code.	YES	Git version control with CI/CD pipeline, Helm-based deployments, and sealed secrets for credential separation. SPDX SBOMs generated for all container images. Cosign keyless signing via Sigstore. SLSA provenance attestations via actions/attest-build-provenance.

Operational Controls

3/4 controls satisfied

ID	Question	Answer	Explanation
4.1	Physical access — Validate physical security of facilities with layered perimeter controls. Manage key access with logs.	NA	Cloud-hosted on DigitalOcean. No physical facilities under Fimil's control. Physical security is the cloud provider's responsibility under the shared responsibility model.
4.2	Logical access — Limit sensitive data access to users with legitimate need. Deactivate redundant accounts. Regular access reviews. Require MFA for remote access to customer data and production.	YES	Five-level RBAC with tenant isolation enforces least-privilege access. Account deactivation and bulk token revocation supported. TOTP-based MFA with recovery codes implemented. Automated access reviews via Fimil-Ops (stale users, tokens, privileged users).
4.3	Sub-processors — Maintain a list of third-party companies with access to customer data, available to clients. Assess third parties annually.	YES	Sub-processor list published in trust center with DPAs executed for all vendors. Vendor Risk Management Policy defines three-tier classification with annual/biannual review cadence.
4.4	Backup and disaster recovery — Securely back up data to a different location. Maintain and test disaster recovery plans annually.	YES	Nightly PostgreSQL and Redis backups to S3 offsite storage with documented restore procedures (RTO 4h, RPO 24h). DR test completed March 2026 with successful recovery validation.