Koffyr Security Brief

Koffyr — the branded client-intake portal for independent insurance agencies. Three COI workflows, one audit trail, zero per-seat fees — works alongside any AMS. (koffyr.com)

Last updated: July 2026 · Shared freely — no NDA required · Contact: security@koffyr.com

HOSTING & ARCHITECTURE

Koffyr runs entirely on AWS in the United States behind the Cloudflare edge (CDN, WAF, DDoS protection). The API is a long-running containerized service on AWS ECS Fargate — no servers we patch by hand — with origin locking so application traffic only reaches AWS through Cloudflare. Web frontends are served from Cloudflare Pages. Background work runs on the same hardened container image (ECS scheduled tasks and queue consumers). Infrastructure is 100% Terraform-managed; changes ship through the same reviewed, gated CI pipeline as application code. CloudTrail, AWS Config, GuardDuty, and Security Hub run account-wide.

TENANT ISOLATION

Isolation is enforced in depth, not at a single layer. Every tenant-owned row carries its organization key, and row-level authorization is enforced by a declarative policy engine (15+ policies) that compiles access rules into per-row SQL filters, backed by service-layer scoping for rules policies can't express. Documents in object storage are keyed under per-tenant prefixes and every fetch passes the same authorization layer. The isolation model was validated by a dedicated authorization sweep (June 2026) covering authorization bypasses, data-filter correctness, policy coverage, and token-bearer endpoints — findings fixed or tracked to closure, with regression tests.

ENCRYPTION

In transit: TLS 1.2 minimum, TLS 1.3 negotiated end-to-end (Cloudflare edge and AWS load balancing both run TLS 1.3-capable policies).

At rest: AES-256 everywhere — database storage encryption and S3 server-side encryption with a dedicated KMS key.

Application-layer field encryption: the most sensitive fields — Tax ID/EIN, email, phone, date of birth, home address — are additionally encrypted above the database with AES-GCM-256 envelope encryption backed by AWS KMS. Data keys are generated per encryption operation, key material is never persisted, and keys are held outside the application database. We do not collect SSNs; payment card data is handled entirely by Stripe and never touches our servers.

AUTHENTICATION

Authentication is built in-house — no third-party identity vendor sees your data. Passkeys (WebAuthn) are the primary mechanism: phishing-resistant, no passwords stored, ever. Email magic links provide a possession-based single-factor alternative, with OTP step-up for sensitive operations. Sessions use short-TTL RS256-signed tokens with refresh rotation and reuse detection.

IMMUTABLE AUDIT TRAIL + E&O EXPORT

Every material action is written to an append-only audit log — immutability is enforced at the application layer (updates and deletes are rejected), retained 7 years with archival to cold storage. Each organization's daily events are sealed with a SHA-256 digest, making tampering evident. A one-click E&O audit export produces a PDF evidence package for any request — built for the conversation with your E&O carrier.

BACKUPS & DISASTER RECOVERY

Continuous database backups with point-in-time recovery, plus scheduled recovery points stored in a locked, immutable, KMS-encrypted AWS Backup vault (weekly points retained 35 days) covering both the database and document storage. Backup-job failures page the on-call engineer. A documented restore runbook is in place; restore drills are scheduled on a defined cadence, with the first full production drill slated ahead of launch (Q4 2026).

SOC 2 & CONTROL PROGRAM

SOC 2 Type I is targeted for Q4 2026. The control program is documented and operating: seven ratified policies (Information Security, Access Control, Incident Response, Change Management, Vendor Management, Risk Assessment, Data Retention & Disposal) mapped to the AICPA Trust Services Criteria (CC1–CC9, C1), with annual review. Automated, non-bypassable CI security gates serve as systematic controls on every change.

SUB-PROCESSORS

The authoritative register lives at koffyr.com/sub-processors (30-day advance notice of changes). Current: AWS (compute, database, storage, KMS), Cloudflare (CDN/WAF/hosting), Twilio SendGrid (transactional email), Stripe (payments — card data never reaches us), Sentry (error monitoring), Mixpanel (anonymized product analytics — no PII), Entrust (RFC 3161 e-sign timestamps — document hashes only), Better Stack (logs/uptime). Authentication and e-signature are in-house — no identity or signature vendor processes your data.

VULNERABILITY MANAGEMENT

Every merge request passes blocking static analysis (SAST), dependency and infrastructure-as-code scanning (SCA/IaC), and secrets scanning in CI, plus automated dependency updates and scheduled dynamic testing (DAST) against a production-like environment. Uploaded PDFs are malware-scanned before processing. We operate a public responsible disclosure program with safe harbor and a 90-day coordinated disclosure window: koffyr.com/responsible-disclosure.

INCIDENT RESPONSE & BREACH NOTIFICATION

A documented incident response policy defines severity tiers, response SLAs (Sev-1 acknowledged in 15 minutes or less during business hours), evidence preservation, and blameless post-mortems. Confirmed breaches affecting personal data are notified to affected customers within 72 hours — contractually committed in our DPA and aligned with GDPR Art. 33/34 timelines.

Questions, security questionnaires, or a deeper walkthrough: security@koffyr.com

Full policies: koffyr.com/security · koffyr.com/sub-processors · koffyr.com/dpa