Security Questionnaire

This document is Taktly's pre-filled response to the Cloud Security Alliance Consensus Assessments Initiative Questionnaire (CAIQ-Lite). Use it to satisfy your security review without a custom questionnaire pass.

Effective 2026-04-27. For follow-up questions or a CAIQ Full response, email security@gettaktly.com.

STATUS LEGEND

- YES — Implemented as described.
- PARTIAL — Implemented with documented limitations.
- NO — Not implemented today; on the roadmap.
- N/A — Not applicable to Taktly's architecture.

AIS - Application & Interface Security

AIS-01 — YES

Are application security policies documented, enforced, and reviewed at least annually?

Yes. Engineering follows secure-coding practices documented in our internal runbook. Security-relevant code paths (authentication, authorization, data export, billing) are reviewed before any deployment to production. The runbook is reviewed annually and after any material incident.

AIS-02 — YES

Is sensitive data identified and encrypted both in transit and at rest?

Yes. TLS 1.2+ for all in-transit connections (TLS 1.3 enforced where supported). AES-256 at rest for the Postgres database, file storage, and database backups via Supabase.

AIS-03 — YES

Are software development controls in place to prevent code-level vulnerabilities (e.g. injection, XSS, CSRF)?

Yes. Application is built on Next.js with parameterized SQL via Supabase client (no raw SQL string concatenation), JSX auto-escaping for XSS, and same-site cookies for CSRF protection. Dependency vulnerabilities are monitored via GitHub Dependabot.

AIS-04 — NO

Are independent third-party penetration tests conducted?

Not yet. Planned post-SOC 2 Type I audit. Internal code review and platform-provided security scanning are in place today.

AAC - Audit Assurance & Compliance

AAC-01 — NO

Do you have a recent SOC 2, ISO 27001, or equivalent third-party attestation?

Not yet. SOC 2 Type I targeted for completion within the current fiscal year via Vanta or Drata. Sub-processors carrying Taktly's workload (Supabase, Vercel, Stripe, Resend) all hold SOC 2 Type II.

AAC-02 — PARTIAL

Are independent audits or vulnerability assessments performed at least annually?

Internal review is performed quarterly. Independent third-party audits begin with the SOC 2 Type I engagement (in flight).

AAC-03 YES

Are security control statements available for customer review?

Yes. The /trust page (https://gettaktly.com/trust) and this CAIQ-Lite document describe all material security controls. Additional documentation (architecture diagram, incident response runbook) available on request to security@gettaktly.com.

BCR - Business Continuity & Resilience

BCR-01 YES

Are documented backup and recovery procedures in place?

Yes. Supabase performs daily automated backups with point-in-time recovery enabled. Backup procedures are documented in our internal runbook.

BCR-02 PARTIAL

Are recovery time and recovery point objectives (RTO/RPO) defined?

RTO target: 4 hours. RPO target: 24 hours (matches daily backup cadence). Formal SLA terms available on request as part of an enterprise agreement.

BCR-03 YES

Are backups tested at least annually for restoration?

Restoration is tested quarterly via Supabase's point-in-time recovery feature.

BCR-04 PARTIAL

Is there a documented business continuity plan?

Lightweight BCP focused on incident response and recovery is documented; expanded plan in development as part of SOC 2 prep.

CCC - Change Control & Configuration Management

CCC-01 YES

Are changes to production systems documented, reviewed, and tested before deployment?

Yes. All production changes go through GitHub-based code review and CI before reaching production via Vercel deployments. Database schema changes go through versioned SQL migrations.

CCC-02 YES

Is there a documented change-management process for emergency changes?

Yes. Emergency hotfixes follow an expedited process with post-hoc review documented in the deployment log.

CCC-03 YES

Are unauthorized configuration changes detected?

All production changes flow through git; out-of-band changes are detectable via deployment logs and Vercel/Supabase audit trails.

DSI - Data Security & Information Lifecycle Management

DSI-01 YES

Is customer data classified by sensitivity?

Yes. Data is classified as: Public (marketing copy), Internal (operational logs), Confidential (customer project content, account data), Restricted (authentication credentials, billing identifiers).

DSI-02 YES

Are data ownership and accountability assigned?

Customer is the owner and Controller of customer-supplied data. Taktly is the Processor. See Data Processing Agreement.

DSI-03 YES

Can customers export and delete their data on demand?

Yes. Self-serve PDF export of all artifacts. Self-serve workspace reset deletes all projects and contents. Account deletion within 24 hours via email request to hello@gettaktly.com.

DSI-04 YES

Is data securely disposed of at end of life?

Yes. Account deletion triggers a full purge from production database within 24 hours. Backup retention follows Supabase's documented schedule (currently 7 days for point-in-time recovery).

DSI-05 YES

Is customer data segregated logically?

Yes. Row-level security (RLS) policies enforced at the Postgres database layer ensure each customer can only access rows belonging to their own user_id. RLS applies even to authenticated database connections.

EKM - Encryption & Key Management

EKM-01 YES

Is data encrypted in transit using strong cryptographic protocols?

Yes. TLS 1.2 minimum, TLS 1.3 enforced where the client supports it. HSTS enabled. HTTP requests redirected to HTTPS automatically.

EKM-02 YES

Is data encrypted at rest?

Yes. AES-256 at rest for production database, file storage, and database backups via Supabase's underlying AWS infrastructure.

EKM-03 YES

Are encryption keys managed securely?

Yes. Encryption keys are managed by Supabase (database) and Vercel (TLS termination) using AWS KMS. Application secrets are stored in Vercel's environment variable system, not in source code.

EKM-04 YES

Are passwords stored using a one-way hash with salt?

Yes. Passwords are hashed with bcrypt by Supabase Auth. Plaintext passwords never reach Taktly's application code or database.

GRM - Governance & Risk Management

GRM-01 PARTIAL

Is there a documented information security policy?

Yes for the items covered in this document and the /trust page. Comprehensive policy document in development as part of SOC 2 prep.

GRM-02 YES

Are security policies reviewed at least annually?

Yes. Annual review is documented in the runbook.

GRM-03 YES

Is there an executive sponsor for the information security program?

Yes. The founder (Vernon Lee) is the executive sponsor for information security and is the responsible party for security incident response.

HRS - Human Resources Security

HRS-01 N/A

Are background checks performed on personnel with access to customer data?

Solo-founder operation. No additional personnel currently have access to production systems. As the team grows, background checks will be performed prior to granting production access.

HRS-02 YES

Are personnel bound by confidentiality agreements?

All personnel (currently the founder) are bound by written confidentiality obligations as part of the corporate operating agreement and any future employment or contractor agreements.

HRS-03 PARTIAL

Are personnel trained on security policies?

Founder is the security owner and is trained. Formal annual security training program will be documented and required as the team grows.

IAM - Identity & Access Management

IAM-01 YES

Are user accounts uniquely identified and authenticated?

Yes. Each end user has a unique account tied to a verified email address. Authentication via email + password (bcrypt-hashed) or magic-link, both backed by Supabase Auth.

IAM-02 PARTIAL

Is multi-factor authentication available?

Magic-link authentication available today (proves possession of email). True MFA via TOTP planned post-launch.

IAM-03 YES

Are administrative accounts gated to a documented allowlist?

Yes. Administrative access to /dashboard/admin is gated by an explicit email allowlist. Anyone outside the allowlist receives a 'Not authorized' response.

IAM-04 YES

Are inactive sessions terminated automatically?

Yes. Session tokens are scoped via Supabase Auth with default expiration. Refresh tokens rotate on use.

IAM-05 PARTIAL

Are user access reviews performed periodically?

Administrative access list is reviewed monthly. Customer end-user access is managed by the customer themselves; Taktly does not provision end-user accounts on the customer's behalf.

IAM-06 YES

Is least privilege applied to internal access?

Yes. Production database access is restricted to the founder via Supabase service-role keys. Application code uses scoped Supabase keys (anon for public reads, RLS-enforced for authenticated reads). Service-role key usage is limited to admin pages with allowlist gating.

IVS - Infrastructure & Virtualization Security

IVS-01 YES

Where is customer data hosted geographically?

Primary region: AWS US-East (Northern Virginia) via Supabase. Application served globally from Vercel's edge network with US-East as primary origin. EU/Canada residency available on enterprise agreement (in development).

IVS-02 YES

Are network security controls implemented?

Yes. Vercel and Supabase both operate behind AWS-grade network security (WAF, DDoS protection, network segmentation). Application-level network controls include CORS restrictions and CSP headers.

IVS-03 YES

Are systems patched on a timely basis?

Underlying infrastructure (Supabase, Vercel) is patched by the providers under their published SLAs. Application dependencies are scanned via Dependabot; critical security patches are applied within 7 days of disclosure.

IVS-04 YES

Is environment separation enforced (dev / staging / prod)?

Yes. Development, preview (per-PR), and production are separated as distinct Vercel deployments. Database migrations are tested in development before being applied to production via the Supabase SQL editor.

SEF - Security Incident Management & Forensics

SEF-01 YES

Is there a documented incident response plan?

Yes. Incident response runbook covers detection, containment, eradication, recovery, notification, and post-incident review. Available on request to security@gettaktly.com.

SEF-02 YES

Are customers notified of security incidents affecting them?

Yes. Notification target is within 72 hours of confirmed incident affecting customer data, including nature of the incident, data affected, mitigation steps, and recommended customer actions.

SEF-03 YES

Is there a security contact for customer reporting?

Yes. security@gettaktly.com. Acknowledged within 24 hours.

SEF-04 YES

Are logs retained for forensic investigation?

Yes. Authentication events, billing events, admin actions, and application errors are logged with timestamps. Log retention is currently 90 days; extended retention available on enterprise agreement.

STA - Supply Chain Management & Transparency

STA-01 YES

Are sub-processors disclosed to customers?

Yes. Current sub-processor list is published at https://gettaktly.com/trust and in Annex 3 of the Data Processing Agreement.

STA-02 YES

Are customers notified of sub-processor changes?

Yes. At least 30 days' advance notice via email. Customers may object on reasonable data-protection grounds within that period.

STA-03 YES

Are sub-processors held to equivalent security standards?

Yes. Each sub-processor is bound by written terms requiring at least equivalent data-protection obligations, and each currently holds a SOC 2 Type II attestation or equivalent.

TVM - Threat & Vulnerability Management

TVM-01 YES

Are vulnerability scans performed regularly?

Yes. Continuous dependency vulnerability scanning via GitHub Dependabot. Platform-level vulnerability scanning is performed by Supabase and Vercel as part of their managed services.

TVM-02 YES

Are critical vulnerabilities remediated within a defined timeframe?

Yes. Critical vulnerabilities (CVSS 9.0+) are remediated within 7 days. High (CVSS 7.0-8.9) within 30 days. Lower-severity items prioritized in normal sprint cadence.

TVM-03 YES

Is anti-malware protection in place?

Yes. The platform does not accept arbitrary file uploads from end users in normal operation. Logo uploads are restricted by file type and size, scanned by Supabase Storage. Server infrastructure is protected by AWS-level controls.

Contact and follow-up

Need a CAIQ Full response, a custom questionnaire pass, or an updated answer? Email security@gettaktly.com. We respond within one business day.

Other documents available on request: Data Processing Agreement (already published at https://gettaktly.com/taktly-dpa.pdf), Architecture Diagram, Incident Response Runbook, Backup & Recovery Procedures.