V1.0

Status	Effective April 28, 2026
Effective	April 28, 2026
Canonical source	https://secapi.ai/trust

Vendor Security Due Diligence Questionnaire (DDQ)

Version 1.0 — Effective April 28, 2026. This DDQ summarizes secapi.ai's customer-facing security, privacy, and operational posture. It accompanies the Data Processing Agreement and Master Services Agreement / Terms of Service. A downloadable PDF is provided for procurement and legal review at `/trust/ddq.pdf`.

This DDQ summarizes secapi.ai's ("**Provider**") security, privacy, and operational posture for use by Customer procurement, legal, and security review teams. It is intended to accompany Provider's Data Processing Agreement and Master Services Agreement / Terms of Service.

For questions, request follow-ups, or to discuss a specific compliance framework, contact `security@secapi.ai`.

1. Company information

Question	Response
Legal name of company	Arcade Group, Inc. (operating as secapi.ai)
Year founded	2025
Headquarters	Wyoming, United States
Employee count (FTE + contractor)	< 25
Public-facing product URL	https://secapi.ai
Documentation URL	https://docs.secapi.ai
Status page URL	https://secapi.ai/status
Trust page URL	https://secapi.ai/trust
Primary security contact	security@secapi.ai
Primary commercial contact	support@secapi.ai
Privacy / DPO contact	security@secapi.ai (Privacy Officer function)

2. Service description

Question	Response
What does Provider do?	Provider operates a SEC-data API platform (secapi.ai) that delivers SEC filings, ownership data, enforcement actions, and derived analytics through a REST API, MCP tools, SDKs, and a hosted dashboard.
What customer data is processed?	Account data, API usage telemetry, billing data (via Stripe), and support correspondence. The Services are not intended to process special-category Personal Data. See the DPA Annex I.D for full categories.
Is Provider a Controller, Processor, or Sub-processor?	Provider acts as a Processor with respect to Customer Personal Data submitted through or generated by Customer's use of the Services.
Where is Customer data stored?	Primary databases and object storage are hosted in US regions. Cloudflare edge nodes serve cached read-only public assets globally. International transfers are governed by the SCCs (see DPA Section 5).
Is the service multi-tenant?	Yes. Tenant isolation is enforced at the application layer using tenant-scoped query filtering and per-organization rate limiting.

3. Compliance and certifications

Question	Response
SOC 2 Type 1	**In scope; observation window not yet started.** Vanta/Drata engagement is scheduled. Target Type 1 audit completion: Q3–Q4 2026. See `secapi.ai/trust#soc2` for the live status.
SOC 2 Type 2	Targeted to follow Type 1 audit completion (12-month observation window).
ISO 27001	Not certified. May be added to roadmap based on customer demand.
HIPAA	Not in scope. Provider does not Process Protected Health Information.
PCI-DSS	Not in scope. Payment instruments are tokenized and held by Stripe; Provider does not store cardholder data.
FedRAMP	Not in scope.
GDPR	Compliant. Provider acts as a Processor. See the DPA.
UK GDPR	Compliant. UK Addendum to SCCs is incorporated by reference into the DPA.
CCPA / CPRA	Compliant. Provider does not "sell" Personal Data as defined by the CCPA.
FADP (Switzerland)	Compliant. Swiss adaptations to SCCs apply.
Other regional compliance	Available on request. Contact security@secapi.ai.

4. Security organization

Question	Response
Is there a designated security leader?	Yes. The CEO is the executive sponsor for security; a designated security operations function reviews the threat model, audit baselines, and incident response.
Is security training mandatory for personnel?	Yes. All personnel with access to Customer data complete security and privacy training upon onboarding and annually.
Is there a documented information security policy?	Yes. Internal policies cover access control, encryption, incident response, vendor management, and data handling. Customer-facing summaries are at `secapi.ai/trust`.
Are background checks performed?	Yes, where permitted by law, for personnel with access to Customer data.
Is there a confidentiality / NDA in place with personnel?	Yes. All personnel are subject to written confidentiality obligations covering Customer data.

5. Authentication and access control

Question	Response
How are API requests authenticated?	API keys (32-byte randomly generated, SHA-256 hashed at rest; raw keys are never persisted server-side) and short-lived WorkOS bearer tokens.
Is multi-factor authentication enforced for administrators?	Yes. MFA is required for administrative dashboard access and for production infrastructure access.
Is single sign-on (SSO) supported?	SSO via WorkOS Connect is on the roadmap. Contact security@secapi.ai for current status.
How is least privilege enforced?	Production access is limited to a documented operations group using hardware-backed keys and ephemeral credentials. Application-tier access is tenant-scoped at the query level.
Are API keys rotatable?	Yes. Customers can rotate keys at any time via the dashboard.
Is session timeout configured?	Yes. Dashboard sessions time out after a documented inactivity window; administrator sessions have shorter timeouts.

6. Encryption

Question	Response
Encryption in transit	TLS 1.2 or higher for all customer-facing endpoints. Mutual TLS for application-to-database connections. Strong cipher suites only.
Encryption at rest	AES-256 (or equivalent industry-standard symmetric encryption) for primary databases, object storage, backups, and secrets.
Key management	Cryptographic keys are managed by the underlying cloud provider's key management service (KMS). Application secrets are stored in Infisical with scoped access.
Are customer-managed keys (CMK / BYOK) supported?	Not currently. Available on roadmap; contact security@secapi.ai if required.

7. Network and infrastructure security

Question	Response
Where is the application hosted?	Railway (managed cloud platform) in US regions, with Cloudflare as the global edge / CDN / WAF layer.
Is there a Web Application Firewall (WAF)?	Yes. Cloudflare WAF is deployed in front of all customer-facing endpoints.
Is there DDoS protection?	Yes. Cloudflare DDoS mitigation is enabled.
Is the network segmented?	Yes. Application, database, and admin tiers are network-isolated.
Is intrusion detection / prevention deployed?	Yes. Edge WAF rules and application-tier anomaly detection alert via Sentry.
Are public ports limited?	Yes. Only HTTPS (443) is exposed publicly. All other ingress is denied by default.

8. Vulnerability management and secure development

Question	Response
Is a Secure Development Lifecycle (SDLC) followed?	Yes. Code changes require pull-request review, automated tests, and security scanning before merge.
Are static application security tests (SAST) run?	Yes. CodeQL, Semgrep, gitleaks, and trufflehog run on every change. Findings are triaged with severity-based SLAs.
Are dynamic application security tests (DAST) run?	DAST is performed as part of internal penetration testing engagements.
Are dependencies scanned for known vulnerabilities?	Yes. Dependabot and equivalent tooling track CVEs. Security patches are applied per documented severity SLAs.
Is third-party penetration testing performed?	An internal comprehensive auth-boundary audit and threat model were completed in April 2026 (zero high-severity exploitable findings). External penetration testing is on the SOC 2 program roadmap.
Is there a published responsible disclosure / vulnerability disclosure policy?	Yes. Email `security@secapi.ai` to report a vulnerability. Provider commits to a one-business-day acknowledgment.
Is there a bug bounty program?	Not currently. Under evaluation.

9. Logging, monitoring, and incident response

Question	Response
Are security-relevant events logged?	Yes. Authentication events, administrative actions, configuration changes, and error events are logged centrally.
What is the log retention period?	Operational logs: 30 days (rolling). Audit logs of administrative actions: 12 months. Tenant-scoped customer-visible logs: as documented in the dashboard.
Is there 24x7 monitoring?	Yes. Sentry alerts and BetterStack uptime monitoring page the on-call engineer for critical incidents.
Is there a documented incident response plan?	Yes. Severity classification, escalation paths, communication templates, and post-incident review requirements are documented internally. Customer-facing summary at `secapi.ai/trust#security`.
What is the breach notification timeline to customers?	Without undue delay, and in any event within 72 hours of becoming aware of a Personal Data Breach affecting Customer Personal Data. See DPA Section 6.
What is the public status page?	https://secapi.ai/status (BetterStack-backed live dashboard with incident history).

10. Data lifecycle

Question	Response
What is the data retention policy?	Account and operational data is retained for the term of the agreement. Telemetry / usage logs roll off on a documented schedule. Specific retention windows are documented in the Privacy Policy at `secapi.ai/privacy-policy`.
Can a customer request deletion of their data?	Yes. Customers may delete data via the dashboard or by contacting `support@secapi.ai`. See DPA Section 8.
Can a customer export their data?	Yes. Account-scoped data export is available via the dashboard and API.
Is there a data classification scheme?	Yes. Data is internally classified (Public, Internal, Confidential, Restricted) with corresponding handling requirements.
How are decommissioned media handled?	Primary infrastructure is cloud-hosted; underlying physical media is decommissioned by the cloud provider in accordance with their published procedures (NIST SP 800-88 or equivalent).

11. Sub-processors

Question	Response
Is there a published Sub-processor list?	Yes. Available at `secapi.ai/trust#sub-processors`.
What advance notice is given for new Sub-processors?	At least 30 days. See DPA Section 4.3.
Can a customer object to a Sub-processor?	Yes. See DPA Section 4.4.
Are Sub-processors bound by equivalent data protection obligations?	Yes. Provider enters into written agreements with each Sub-processor that impose obligations no less protective than those imposed on Provider under the DPA.

12. Business continuity and disaster recovery

Question	Response
Are backups taken?	Yes. Daily encrypted backups of primary databases with documented restore procedures.
Is there a documented Disaster Recovery (DR) plan?	Yes. The DR plan is reviewed annually and exercised at least once per year.
What is the Recovery Time Objective (RTO)?	< 4 hours for critical services. Available on request.
What is the Recovery Point Objective (RPO)?	< 24 hours. Available on request.

13. Service Level Agreement (SLA)

Question	Response
Is there a customer-facing SLA?	Yes. Tier-based: 99.9% uptime for Commercial (with service credits on breach), 99.5% uptime for Personal/Team (with support response SLAs), best-effort for Free/PAYG. See `secapi.ai/trust#sla`.
What is the support response SLA?	Commercial: 1 business hour. Team: 4 business hours. Personal: 1 business day. Critical bug across all paid tiers: 24 hours.
Are service credits available on SLA breach?	Yes, for Commercial-tier customers. See the SLA at `secapi.ai/trust#sla`.

14. Insurance

Question	Response
Does Provider carry cyber-liability insurance?	Coverage is in place. Specific limits and certificate of insurance available on request under NDA.
Does Provider carry errors-and-omissions / professional liability insurance?	Coverage is in place. Specific limits available on request under NDA.

15. Audits and reports available on request

The following reports / artifacts are available on request, subject to NDA:

- DPA executed copy
- Master Services Agreement / Terms of Service
- Penetration testing summary (when SOC 2 program completes initial pen test)
- SOC 2 Type 1 report (when issued — target Q3–Q4 2026)
- Sub-processor list (also published at `secapi.ai/trust#sub-processors`)
- Threat model executive summary (paraphrased; full internal threat model is not customer-facing)
- Incident response runbook (executive summary)
- Disaster recovery plan (executive summary)
- Insurance certificates

To request, email `security@secapi.ai`.

16. Contact

For questions about this DDQ or to request supporting documentation, contact:

- **Security:** security@secapi.ai
- **Commercial / procurement:** support@secapi.ai
- **Status / incidents:** https://secapi.ai/status
- **Trust page:** https://secapi.ai/trust

End of Vendor Security Due Diligence Questionnaire v1.0.