

SIG Lite — Pre-filled responses for PanGuard AI, Inc.

This document is PanGuard's standard SIG Lite response. It is provided to streamline F500 procurement vendor onboarding. Subsections track the Shared Assessments SIG Lite 2025 question categories. Responses are accurate as of the document date and updated quarterly.

Document date: 2026-05-20 **PanGuard AI Inc. status:** Delaware C-Corp filed 2026-05-12. Stripe Atlas registered agent. Founder: Adam Lin. **Distribution:** This document is provided under NDA with prospective Customers. Do not redistribute.

A. Risk Management

A.1 Information Security Program

- **A.1.1** PanGuard maintains a written information security program. Public version at <https://panguard.ai/legal/security>.
- **A.1.2** Program owner: Adam Lin, Founder & CEO. CSO role planned post-CTO co-founder hire (target Day 30 from 2026-05-20).
- **A.1.3** Program review cadence: quarterly self-review; annual third-party audit beginning with SOC 2 Type 1 (target attestation 2026-10-01).

A.2 Risk Assessment

- **A.2.1** Threat model maintained internally; sanitised version shareable under NDA on request.
 - **A.2.2** Risk register maintained in private repo. Updated on every material change.
 - **A.2.3** Sub-processor risk reviewed quarterly. List at <https://panguard.ai/sub-processors>.
-

B. Security Policy

- **B.1** Written security policy: yes. Public summary at <https://panguard.ai/legal/security>.
 - **B.2** Acceptable use policy: yes. <https://panguard.ai/legal/acceptable-use>.
 - **B.3** Data classification scheme: PUBLIC / INTERNAL / CONFIDENTIAL / CUSTOMER_DATA. CUSTOMER_DATA is treated as the most restrictive.
 - **B.4** Policy review cadence: quarterly.
-

C. Organizational Security

- **C.1** Background checks on personnel: yes, before workspace access.
 - **C.2** Confidentiality agreements with personnel: yes, before workspace access.
 - **C.3** Security awareness training: annual + new-hire onboarding.
 - **C.4** Headcount: 1 (founder). Hire-roadmap public at <https://panguard.ai/about>. Bus factor mitigation in flight via CTO co-founder search.
-

D. Asset Management

- **D.1** Asset inventory maintained: yes.
 - **D.2** Removable media policy: prohibited for production systems. Production access via SSH key + 2FA only.
 - **D.3** Data retention: per <https://panguard.ai/legal/privacy>. CUSTOMER_DATA retained 30 days after workspace deletion, then permanently deleted.
-

E. Human Resources Security

- **E.1** Personnel screening: yes, before workspace access.
 - **E.2** Termination procedures: revoke production access within 4 hours of termination notice.
 - **E.3** Contractor controls: contractor agreements with confidentiality + IP assignment clauses. Currently 0 active contractors.
-

F. Physical and Environmental Security

- **F.1** No PanGuard-owned data centre. All hosting on third-party SOC 2 Type 2 providers (Supabase, Vercel, Fly.io, Cloudflare).
 - **F.2** Office: founder home office (Taipei) — no Customer Data stored locally. Customer Data flows through hosting providers only.
 - **F.3** Physical access controls inherited from hosting providers' SOC 2 Type 2 attestations.
-

G. Communications and Operations Management

- **G.1** Change management: GitHub PR-based. Production deploys require PR review + CI pass.
 - **G.2** Separation of duties: founder operates solo today; separation enforced via least-privilege Stripe / Supabase / Vercel IAM roles. CTO co-founder hire will formalise duty separation.
 - **G.3** Capacity planning: production capacity from hosted providers; auto-scaling enabled.
 - **G.4** Backup: Supabase Postgres point-in-time recovery (7 days). Customer Data backup retention: 7 days.
 - **G.5** Logging: structured logs to Sentry + Supabase audit_logs. Retention 90 days.
-

H. Access Control

- **H.1** Authentication: magic-link email auth via Supabase (passwordless). MFA via emailed one-time code.
 - **H.2** SAML SSO: roadmap target Q3 2026 (alongside SOC 2 Type 1). Not available today.
 - **H.3** SCIM: roadmap target Q3 2026. Not available today.
 - **H.4** Privileged access management: 1 superuser (founder). Audit-logged via Supabase audit_logs.
 - **H.5** RLS: every database table carries `workspace_id`. Row-Level Security policy enforces equality with the JWT claim. Cross-workspace reads provably impossible at the database layer.
 - **H.6** Password policy: N/A (passwordless).
 - **H.7** Failed login lockout: rate-limited at Supabase level (default 5 attempts / 15 min).
-

I. Information Systems Acquisition, Development, and Maintenance

- **I.1** SDLC: trunk-based development. GitHub PR review required for production branch.
 - **I.2** Static analysis: ESLint + TypeScript + dependabot + GitHub security advisories.
 - **I.3** Dynamic application security testing: Pen test scheduled with SOC 2 Type 1 fieldwork (Q3 2026). Not yet engaged.
 - **I.4** Vulnerability disclosure: <https://panguard.ai/legal/responsible-disclosure> (RFC 9116 security.txt at /.well-known/security.txt).
-

J. Incident Management

- **J.1** Incident response plan: written, internal-only.
 - **J.2** Breach notification SLA: 72 hours from confirmed breach to Customer notification, per DPA. <https://panguard.ai/legal/dpa>.
 - **J.3** Incident response contact: security@panguard.ai (24/7 monitored, forwards to PagerDuty after-hours).
 - **J.4** Post-incident review: written within 5 business days of incident closure.
-

K. Business Continuity

- **K.1** BCP / DR plan: documented internally. RPO 24h, RTO 4h. Tested quarterly.
 - **K.2** Failover: hosting providers' multi-AZ deployment. No PanGuard-owned hot site.
 - **K.3** Backup testing: monthly point-in-time recovery test against staging.
-

L. Compliance

- **L.1** GDPR: yes, DPA at <https://panguard.ai/legal/dpa>.
 - **L.2** Taiwan PDPA: yes, same DPA covers.
 - **L.3** CCPA / CPRA: yes (privacy policy covers California rights).
 - **L.4** HIPAA: NOT supported. PanGuard is not a HIPAA Business Associate at this stage. Healthcare Customers with PHI: do not use PanGuard in PHI-touching paths.
 - **L.5** PCI-DSS: NOT in scope. Stripe handles all card data — PanGuard does not see card numbers.
 - **L.6** SOC 2 Type 1: TARGET 2026-10-01. Vanta selected as compliance automation platform. A-LIGN as primary CPA candidate. Full roadmap PDF: <https://panguard.ai/samples/soc2-roadmap/PanGuard-SOC2-Roadmap-2026.pdf>.
 - **L.7** SOC 2 Type 2: TARGET 2027-06-30 (post-Type 1 observation window).
 - **L.8** ISO 27001: TARGET 2027 H2 (dual-track with Vanta).
 - **L.9** EU AI Act: PanGuard's product produces evidence packs mapped to EU AI Act. PanGuard itself is a "general-purpose AI provider" candidate — Article 50 compliance is in scope.
-

M. Privacy

- **M.1** Privacy policy: <https://panguard.ai/legal/privacy>.
- **M.2** Data Protection Officer (DPO): Adam Lin, Founder. Email: privacy@panguard.ai.

- **M.3** Data minimisation: Customer Data collected = email + workspace name + opt-in anonymised telemetry. No skill content transmitted by default.
 - **M.4** Cross-border transfers: governed by SCCs (Module Two: Controller-to-Processor). Sub-processors operate in stated jurisdictions; see sub-processor list.
-

N. Insurance

- **N.1** Cyber liability insurance: **TARGET BIND 2026-06-30**. Currently not yet bound — disclosed honestly. PanGuard targets \$1M-\$5M cyber liability coverage tied to SOC 2 audit kickoff.
- **N.2** General liability: same target.
- **N.3** E&O / Tech E&O: same target.

Material disclosure: PanGuard is a pre-Series-Seed company. Insurance binding has not yet occurred. Customers requiring insurance evidence BEFORE binding date can either (a) defer engagement to Q3 2026 OR (b) accept the Founding Customer pricing in exchange for the insurance gap (with PanGuard's commitment to bind by 2026-06-30).

O. Anti-Bribery / FCPA

- **O.1** FCPA training for personnel: yes (founder completed via Stripe Atlas educational materials).
 - **O.2** Anti-bribery policy: yes — gifts > \$100 require written disclosure; no political contributions from corporate funds; no payments to government officials except officially-priced fees.
 - **O.3** Third-party due diligence: sub-processor list maintained at <https://panguard.ai/sub-processors>. No high-risk jurisdiction sub-processors (no Russia, Belarus, Iran, North Korea, Cuba, Syria, Crimea).
-

P. Sanctions Compliance

- **P.1** OFAC sanctions screening: PanGuard checks Customer entity against OFAC SDN list at workspace creation. No service to sanctioned entities.
 - **P.2** Export controls: PanGuard software contains no controlled cryptography beyond TLS / SHA-256 / HMAC. No EAR/ITAR-controlled content.
-

Q. Tax / Identity

- **Q.1** W-9 (US Customers): provided on signed-MSA basis on request.
 - **Q.2** W-8BEN-E (foreign-entity-paying-US-entity): provided on signed-MSA basis on request.
 - **Q.3** EIN: assigned post-Stripe-Atlas (2026-05-12 filing; EIN expected within 15-25 business days, i.e. by 2026-06-15).
-

Documents available on request (under NDA)

- Threat model (sanitised)

- Sub-processor agreements
- Internal incident response plan
- Internal change management procedure
- Audit log samples
- Vanta dashboard read-only access (post-2026-06-01 Vanta contract)
- Penetration test summary (post-Q3 2026 engagement)

Contact: security@panguard.ai

Document control

- **Version:** 1.0
 - **Effective date:** 2026-05-20
 - **Next review:** 2026-08-20 (quarterly)
 - **Owner:** Adam Lin (DPO + CSO acting)
-

This document is provided under the NDA executed between PanGuard AI, Inc. and the receiving party. If no NDA is in place, redistribution is prohibited; please contact security@panguard.ai to execute an NDA before distribution.