Status (per plan §10 risk #4): Honest copy. Where we are today, what we ship, and what we are working toward. Hand-edited quarterly. This is the Aug 2026 edition.
Plan reference: `docs/strategy/EXECUTION_AND_MARKETING_PLAN_2026_08_17.md` §3.4 M-9 #3 + D-10.3.
Send to: procurement@finadvantage.online for revisions.

1. Company information

Item	Answer
Legal entity name	FinAdvantage, Inc.
Year founded	2022
Headquarters	Boston, MA (US)
Primary contact	security@finadvantage.online
Procurement contact	procurement@finadvantage.online
DPA / legal contact	legal@finadvantage.online
Privacy contact	privacy@finadvantage.online
Customer count	Series A/B, with a few enterprise pilot customers. Exact count not publicly disclosed.

2. Compliance certifications

Standard	Status	Last reviewed	Comment
SOC 2 Type II	**In progress.** Auditor engaged Q3 2026.	Aug 19, 2026	Type I expected Q4 2026; Type II expected Q1 2027.
ISO 42001 (AI Management Systems)	**Readiness review on Q1 2027 roadmap.**	Aug 19, 2026	We do not claim certification until we have one.
GDPR	Compliant	Aug 19, 2026	DPA template available on request.
CCPA	Compliant	Aug 19, 2026	Privacy policy + data-deletion workflow.
HIPAA	**Not in scope.**	n/a	We do not handle PHI today.

Standard	Status	Last reviewed	Comment
FedRAMP	**Not in scope.**	n/a	No government-cloud deployment today.
PCI DSS	**Not applicable.**	n/a	We do not process card payments.

3. Infrastructure

Layer	Provider	Their compliance
Application hosting	Railway	SOC 2 Type II
Database	Neon (Postgres)	SOC 2 Type II
Object storage	Cloudflare R2	SOC 2 Type II
Identity / auth	Auth0	SOC 2 Type II, ISO 27001, ISO 27018
Application monitoring	Sentry	SOC 2 Type II
LLM routing	OpenRouter	SOC 2 Type II
Transactional email	Resend	SOC 2 Type II

Regions: us-east-1 (primary); us-west-2 (R2 storage).

4. Encryption

- **At rest:** AES-256 (provider-managed keys)
- **In transit:** TLS 1.3 (HTTPS-only; no HTTP fallback)
- **Key management:** Provider-managed (Railway, Neon, Cloudflare, Auth0 each maintain their own key management)
- **Customer-managed keys:** Not currently offered. Roadmap item for 2027.

5. Access control

- **Customer-facing authentication:** OAuth 2.0 + OIDC via Auth0
- **Multi-factor authentication:** Required for all customer admin accounts; recommended for all customer users
- **SSO:** SAML 2.0 + OIDC supported on enterprise tier
- **Internal staff access:** SSO + hardware key (YubiKey) + privileged access management; no standing production access

- **Just-in-time access:** Production access requires a temporary grant via internal approval workflow; access expires within 4 hours
- **Background checks:** All FinAdvantage staff with production access pass a third-party background check before access is granted

6. Tenant isolation

- Every tenant's data lives in a separate Postgres schema
- Cross-tenant reads are impossible by design (`agents/src/services/signal_ingestion/rbac.py`)
- Tenant delete triggers a 24-hour hard-purge queue; all signal records and uploaded workbooks are removed within 24 hours of a delete request

7. Logging, monitoring, and incident response

- **Application logs:** Retained for 30 days; aggregated through Sentry
- **Audit trail:** Per-execution events written to `reliability_events` (Stages A through K today; Stage N and Stage O coming with E-2 PR-1); retained for 1 year
- **Uptime monitoring:** 5-minute interval checks on all customer-facing endpoints; PagerDuty alerting on-call rotation
- **Incident response:** Documented IR plan; quarterly tabletop exercises; we publish material security incidents within 72 hours at status.finadvantage.online
- **As of Aug 19, 2026: no material security incidents on record.**

8. Data handling and retention

Item	Detail
What we store	Uploaded workbooks, generated deliverables, audit-binder metadata (per plan §2 E-2 — `pipeline_triples` table)
What we don't store	Original customer GL outside the workbook upload session; cross-customer data; anything outside the tenant scope
Workbook retention	30 days post-execution unless customer requests earlier deletion
Deliverable retention	1 year; customer can request deletion at any time
Right to delete	GDPR + CCPA — contact privacy@finadvantage.online. Honored within 30 days.

9. Sub-processors

See `docs/trust/TRUST_CENTER.md` §Sub-processors for the full list. Currently: Neon, Cloudflare, Auth0, Railway, OpenRouter, Sentry, Resend. Each sub-processor has a DPA on file; copies available on request.

10. AI governance

- **Model providers:** OpenRouter-routed models (Anthropic Claude, others). Provider list maintained in our internal model registry.
- **Per-execution audit:** every model call is logged with prompt hash, response hash, model id, latency, and outcome (`reliability_events` Stage A)
- **AI risk register:** Internal; available on request under NDA
- **Output QA:** Every deliverable passes through a `reliability_events` Stage F-G-H-K pipeline before delivery; binding failures surface as `NEEDS_REVIEW` (not `COMPLETED`) — per Aug 19 production fix `ef9b4ff1`
- **Provenance:** Per-cell provenance sidecar (`pipeline_triples` table) ships in v1 behind `FA_PROVENANCE_V1` flag; covers every cell in every deliverable with the source workbook, source column, literal SQL chain, and source-text fragment
- **No training on customer data:** Customer data is never used to train upstream models. OpenRouter's no-train policy applies by contract.

11. Business continuity

- **RPO (Recovery Point Objective):** 1 hour
- **RTO (Recovery Time Objective):** 4 hours
- **Backups:** Daily automated Postgres backups; 30-day retention; cross-region replication
- **DR site:** us-west-2 standby; DNS failover via Cloudflare
- **Last DR test:** July 2026; passed (4h RTO achieved)

12. Personnel security

- Background checks for all staff with production access
- Annual security training for all staff
- Phishing-resistant MFA (hardware keys) for production access
- Quarterly access reviews

13. Software development lifecycle

- Code reviews required for all production changes
- No direct pushes to `main`
- Static analysis on every PR (ESLint + tsc)
- Dependency vulnerability scanning (Dependabot)
- Secrets scanning (gitleaks; pre-push hook)
- Pre-deploy: integration test suite (`agents/src/tests`) must be green

- Post-deploy: smoke tests on staging before promoting to production

14. Customer responsibilities

Per our standard terms:

- Customer is responsible for account credentials, MFA setup, and admin-user provisioning
- Customer is responsible for their own data classification and access-control decisions
- Customer must notify security@finadvantage.online within 72 hours of any suspected security incident affecting their FinAdvantage account

15. Where to send the next questionnaire

- **Procurement questions:** procurement@finadvantage.online
- **Security questions:** security@finadvantage.online
- **Privacy / GDPR:** privacy@finadvantage.online
- **DPA requests:** legal@finadvantage.online

We aim to respond to questionnaires within 5 business days.

Aug 2026 edition. Hand-edited quarterly. Next review: end of Q3 2026.
Plan reference: `docs/strategy/EXECUTION_AND_MARKETING_PLAN_2026_08_17.md` §3.4 M-9 #3 + D-10.3.