Security Overview

HELMSTED, INC.

Data Security Practices for Registered Investment Adviser Clients

July 24, 2026 · Version 1.1

> *This document supplements the security overview at helmsted.ai/security and is intended for compliance due diligence purposes. Retain alongside the executed Data Processing Addendum in your firm's WISP vendor documentation.*

Purpose of This Document

Regulation S-P requires registered investment advisers to conduct reasonable due diligence on service providers that handle client nonpublic personal information. This security overview is provided by Helmsted to support that requirement.

1. Company and Platform Overview

Company	Helmsted, Inc., a Delaware corporation
Platform	AI-assisted financial technology platform for independent registered investment advisers
Data role	Helmsted acts as a service provider / data processor on behalf of each adviser firm. Where an adviser offers a client-facing portal, end clients accept separate portal terms of use governing portal access and related consents; those terms do not make Helmsted an investment adviser, fiduciary, or independent controller of client data, which Helmsted continues to process on behalf of the adviser firm.
Data processed	Client financial documents, planning outputs, advisory communications (where active), client portal inputs and conversations (where active), AI-generated summaries, and AI-derived analytical data
Hosting	Cloud-hosted infrastructure. All Adviser Client Data is stored and processed in the United States. See Section 6 for named infrastructure providers.

2. Data Security Controls

Helmsted is an early-stage company, and its security program continues to mature. The following describes Helmsted's current security practices and intended direction.

2.1 ENCRYPTION

Data at rest	AES-256 encryption for all stored Adviser Client Data
Data in transit	TLS 1.2 or higher for all data transmitted between clients and Helmsted infrastructure
Key management	Encryption keys managed through cloud provider key management service with regular rotation

2.2 ACCESS CONTROLS

Authentication	Multi-factor authentication for Helmsted personnel access to production systems
Authorization	Role-based access controls. Access to Adviser Client Data limited to personnel who require it to provide the Platform.
Privileged access	Privileged access to production systems is logged and monitored
Offboarding	Access revoked promptly upon termination or role change of Helmsted personnel

2.3 NETWORK AND INFRASTRUCTURE SECURITY

Network segmentation	Production, staging, and development environments are logically separated
Firewalls	Network-level and application-level firewalls restrict inbound and outbound traffic
Vulnerability management	Vulnerability monitoring and patching of infrastructure and dependencies

3. Data Handling Practices

3.1 DATA MINIMIZATION

When processing client financial information, the platform assembles only the data fields relevant to the specific task being performed. Sensitive identifiers are masked at the application layer before being transmitted to AI processing components.

3.2 AI PROCESSING — ZERO DATA RETENTION

Helmsted holds Zero Data Retention (ZDR) agreements with each of its third-party AI API providers, currently Anthropic, PBC, OpenAI, L.L.C., and xAI Corp. Under these agreements, the provider does not retain any input or output data after an API call completes; data is processed in memory and immediately discarded. This means client financial information submitted for AI analysis is never stored by these providers and cannot be used for model training, fine-tuning, or any other purpose. Where Helmsted uses open-source or self-hosted models, those models run in secure, controlled environments under equivalent protections. This commitment is unconditional and applies to all data types processed

through these AI providers, including documents, planning context, communications data, and AI-derived outputs.

3.3 DATA RETENTION

Audit logs	Retained minimum 5 years. First 2 years in immediately accessible storage, consistent with Rule 204-2 or applicable state recordkeeping requirements.
AI processing records	Model version, prompt version, and output timestamps retained alongside audit logs
Source documents	Retained per the applicable agreement with the adviser firm
Deletion	All deletion events are logged with timestamp and reason. Hard deletion is restricted.

3.4 DATA SEGREGATION

Each adviser firm's data is logically segregated. One adviser firm cannot access another firm's client data.

4. Audit Logging and Traceability

Helmsted maintains append-only audit logs covering significant data processing events. Each entry records: timestamp, event type, adviser and client record identifiers, file identifiers and SHA-256 hash of uploaded documents, AI model and prompt version, and the adviser user ID associated with the action. Logs are not modified or deleted in the ordinary course by adviser users or Helmsted operations staff.

5. Incident Response

5.1 INCIDENT RESPONSE PROGRAM

Helmsted maintains written incident response procedures covering detection, containment, investigation, remediation, and notification for security incidents involving Adviser Client Data.

5.2 NOTIFICATION TIMELINE

Helmsted will notify the affected adviser firm in writing without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a confirmed or reasonably suspected incident involving Adviser Client Data, consistent with applicable law and the notification provisions of the applicable Data Processing Addendum. Notices are sent to the compliance contact designated by the adviser firm.

5.3 BUSINESS CONTINUITY AND DISASTER RECOVERY

Helmsted operates a cloud-first platform with all Adviser Client Data stored and processed in the United States, encrypted at rest and in transit, with automated database backups and point-in-time recovery, and no dependence on a physical office. Helmsted maintains a written Business Continuity and Disaster

Recovery plan addressing cloud or provider outages, key-person loss, and cybersecurity events, reviewed at least annually. A standalone summary is available to adviser clients on request.

6. Subprocessors

Helmsted engages the following third-party subprocessors to deliver the platform. All subprocessors are subject to written data protection agreements. The complete and current list is maintained in Exhibit A of the DPA and available from Helmsted on request. Before engaging a subprocessor, Helmsted reviews its security documentation and published attestations (SOC 2 or ISO 27001 where available) and scopes its access to the minimum the service requires; most subprocessors handle client data only transiently during a session, and at-rest storage is concentrated in the managed database and object storage providers. Each subprocessor is bound by a written agreement with data protection obligations no less protective than Helmsted's DPA with the adviser firm, including the obligation to notify Helmsted of security incidents, and Helmsted remains responsible for its subprocessors' acts and omissions. Helmsted tracks subprocessors' published attestations and security advisories on an ongoing basis, and adviser firms receive at least 30 days' advance written notice of material subprocessor changes with a right to object (DPA Section 5.3).

Subprocessor	Service Provided	Data Accessed	Location	Privacy / Trust URL
Vercel Inc.	Hosting and serving of the Helmsted API and web application (compute, edge routing, TLS termination).	Adviser and Client Data transiting the API request/response path. Does not persistently store client financial documents.	United States	vercel.com/legal/privacy-policy
Render Services, Inc.	Hosting of the Helmsted agents service, which orchestrates agent execution and streams session events.	Adviser Client Data processed during agent sessions, including financial documents, agent outputs, and session event streams. Does not persistently store client financial documents.	United States	render.com/dpa
Google LLC (Google Cloud)	Cloud hosting and infrastructure services supporting the Helmsted platform.	Adviser Client Data processed during agent sessions, including financial documents, agent outputs, and session event streams. Does not persistently store client financial documents.	United States	cloud.google.com/terms/cloud-privacy-notice
Supabase, Inc.	Managed PostgreSQL database, authentication, and identity/session management for the Helmsted platform.	All Adviser Client Data at rest: financial document metadata, planning outputs, audit logs, user credentials, and session data.	United States — US West (Oregon)	supabase.com/privacy
Anthropic, PBC	AI API provider. Claude language	Adviser and Client Data submitted to the Claude API	United States	trust.anthropic.com

Subprocessor	Service Provided	Data Accessed	Location	Privacy / Trust URL
	model used to process adviser and client data during agent sessions. Helmsted holds a Zero Data Retention (ZDR) agreement with Anthropic — Anthropic does not retain any input or output data after an API call completes. Data is processed in memory and immediately discarded, and is never used for model training.	during agent execution, including financial document contents and planning context. Under the ZDR agreement, this data is not retained by Anthropic after the API call completes.		
OpenAI, L.L.C.	AI API provider. Used to process adviser and client data during agent sessions. Helmsted holds a Zero Data Retention (ZDR) agreement with OpenAI; OpenAI does not retain any input or output data after an API call completes, and the data is never used for model training.	Adviser and Client Data submitted to the OpenAI API during agent execution, including financial document contents and planning context. Under the ZDR agreement, this data is not retained after the API call completes.	United States	openai.com/ enterprise-privacy
xAI Corp.	AI API provider. Used to process adviser and client data during agent sessions. Helmsted holds a Zero Data Retention (ZDR) agreement with xAI; xAI does not retain any input or output data after an API call completes, and the data is never used for model training.	Adviser and Client Data submitted to the xAI API during agent execution, including financial document contents and planning context. Under the ZDR agreement, this data is not retained after the API call completes.	United States	x.ai/legal
FoundryLabs, Inc. (d/b/a E2B)	Secure sandbox execution environments in	Adviser Client Data loaded into the sandbox for the duration of an agent session,	United States	trust.e2b.dev

Subprocessor	Service Provided	Data Accessed	Location	Privacy / Trust URL
	which the Helmsted agent runs code and processes adviser-submitted documents during a session.	including financial documents and intermediate outputs. Data does not persist after the session ends.		
Cloudflare, Inc.	Object storage (Cloudflare R2) for adviser-uploaded documents and agent-generated artifacts.	Adviser-uploaded financial documents, agent outputs, and session artifacts stored at rest.	Eastern North America (ENAM)	cloudflare.com/trust-hub
Inngest, Inc.	Managed event delivery and workflow orchestration. Routes and triggers the services that drive Helmsted agent sessions.	Event payloads associated with agent sessions, which may include references to Adviser and Client Data and excerpts of session context.	United States	inngest.com/security
Plus Five Five, Inc. (d/b/a Resend)	Transactional email delivery: platform notifications, authentication emails, and system alerts to adviser users.	Adviser account data (name, email address) and the contents of outbound platform emails. Does not receive client NPI or client financial data.	United States	resend.com/security
Plaid Inc.	Account aggregation provider for the client portal. When a client chooses to connect an external financial account, Plaid connects to the client's financial institution and retrieves account information on the client's behalf. Used only for client-initiated aggregation.	Client-authorized data from connected financial institutions, including balances, holdings, transactions, and account and institution identifiers. Client institution credentials are handled by Plaid through secure tokenized methods and are not stored by Helmsted.	United States	plaid.com/legal
SideGuide Technologies, Inc. (d/b/a Firecrawl)	Web data extraction and crawling service. Used to retrieve and convert publicly available web content into clean, structured data for the platform's research	URLs, search queries, and web-scraping requests submitted by Helmsted, and the publicly available web content retrieved in response. Does not receive client NPI or client financial data.	United States	firecrawl.dev/privacy-policy

Subprocessor	Service Provided	Data Accessed	Location	Privacy / Trust URL
	and analysis features.			

> *Helmsted's AI API providers (Anthropic, PBC; OpenAI, L.L.C.; and xAI Corp.) are each subject to a Zero Data Retention (ZDR) agreement. See Section 3.2 above.*
>
> *Plaid Inc. is engaged for optional, client-initiated account aggregation in the client portal and accesses external account data only when a client chooses to connect an account. Adviser use of Plaid-powered aggregation is governed by the Plaid End Client Terms attached to the pilot agreement.*

7. Personnel and Training

Helmsted is a small early-stage team. All personnel with access to Adviser Client Data are subject to written confidentiality obligations under their employment or contractor agreements. We will publish formal personnel policies (including background-check and security-training programs) as we expand the team and pursue SOC 2 certification.

8. Compliance and Certifications

Reg S-P alignment	Security controls, breach notification procedures, and data handling practices are designed to satisfy service provider obligations under Reg S-P §248.30
AI data retention	Zero Data Retention (ZDR) agreements with Helmsted's AI API providers (Anthropic, PBC; OpenAI, L.L.C.; and xAI Corp.) ensure client data submitted for AI processing is not retained after API call completion
SOC 2	Helmsted is building its architecture toward SOC 2 and intends to pursue SOC 2 certification over time. Helmsted will share a report if and when one becomes available.
Data residency	All Adviser Client Data is stored and processed within the United States
Legal requests	Helmsted will notify affected adviser firms of legal requests for Adviser Client Data to the extent permitted by law

9. Questions and Further Information

Questions about Helmsted's security practices may be directed to:

Helmsted, Inc. — Security and Compliance
privacy@helmsted.ai
helmsted.ai/security

We are happy to walk through any aspect of this overview with your CCO or compliance consultant before you go live.

Helmsted, Inc. is a technology provider — not a registered investment adviser, broker-dealer, or fiduciary. All AI-generated outputs are assistive in nature and require review by a qualified adviser before client reliance or delivery. The subscribing firm retains full regulatory responsibility for its use of the platform and any advice provided to clients.