PRIVACY POLICY & DATA SAFEGUARDS RULE MANIFEST

INSTITUTIONAL INFORMATION GOVERNANCE, ENCRYPTION PROTOCOL, & MULTI-TENANT ISOLATION STANDOUTS

REGULATORY COMPLIANCE NOTE: This Standalone Privacy Policy is drafted to explicitly fulfill information security requirements under the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule (16 CFR Part 314), the Federal Trade Commission (FTC) consumer privacy guidelines, and institutional vendor due diligence frameworks required by Registered Investment Advisors (RIAs) and institutional wealth managers.

This Privacy Policy and Data Safeguards Rule Manifest (this **"Policy"**) clarifies the definitive information protocols, collection fields, algorithmic encryption routines, and systemic data lifecycles enforced by **Thesis Financial Technologies LLC**, a Missouri limited liability company with primary office operations out of Chesterfield, Missouri (the **"Company"**). This Policy applies to all account creators, administrative financial professionals, wealth analysts, and system operators (each, a **"User"** or **"Subscriber"**) interacting with the automated software execution stack and data visualization interfaces provided by the Company.

1. LEGAL GROUNDING AND SCOPE OF DATA CUSTODY

The Company serves strictly as a quantitative technology infrastructure developer and multi-tenant software provider. In delivering automated financial parsing arrays and large language model analytics routing, the Company may process Non-Public Personal Information (**"NPI"**) or consumer metadata managed by the Subscriber's advisory practice. This Policy defines the strict guardrails engineered to isolate such data. This Policy does not alter any technical assignments or liability exemptions outlined in the accompanying Master Services Agreement (MSA) or Data Processing Addendum (DPA).

2. TAXONOMETRIC INVENTORY OF COLLECTED VARIABLES

The Company limits its computational collection vectors to details structurally required to deliver market analytics and maintain system boundary integrity:

DATA CATEGORY	SPECIFIC COLLECTED FIELDS & VARIABLES	OPERATIONAL PURPOSE & CONTEXT
Subscriber Credentials	Professional email addresses, user names, firm identifiers, encrypted API authorization tokens, and billing metadata managed via secure checkout portals (e.g., Stripe).	Account provisioning, system access control, multi-tenant billing verification, and enterprise communication logs.
Quantitative Portfolio Inputs	Financial ticker strings, asset transaction matrices, historical cost-basis indices, institutional 13F filing delta strings, and public custodian metadata sheets.	Algorithmic normalization, data visualization map generation, and historical backtesting calculations inside the Data Abstraction Layer.
Transient Prompts & Contexts	Natural language analytical queries, system user prompts, macro financial assessment requests, and variable configuration strings input into dashboard modules.	Dynamic system context construction and secure transmission across Zero-Data-Retention inference pathways.
Technical Telemetry	Anonymized IP strings, login session duration codes, JSON Web Token (JWT) expiration variables, browser metadata, and infrastructure event tracking logs.	Mitigating systematic scraping attempts, enforcement of system resource caps, and preventing vector attacks.

3. DETERMINISTIC DATA SECURITY & MULTI-TENANT ROW-LEVEL ISOLATION

3.1 Multi-Tenant Separation via Row-Level Security (RLS).

The Company isolates data structures at the core relational database layer. By deploying deterministic Row-Level Security (RLS) configurations, each Subscriber's imported portfolio records, token parameters, and custom metrics are tagged to a unique cryptographic tenant hash. System queries executed by the frontend are strictly constrained by verified JSON Web Tokens (JWT). Alternative platform tenants are structurally blocked from viewing, mapping, or inferring any row or attribute matching the Subscriber's corporate boundaries.

3.2 Advanced Cryptographic Baselines.

All data fields captured or input within the Platform interface are fully encrypted in transit utilizing Transport Layer Security (TLS 1.3 or higher) and completely encrypted at rest utilizing Advanced Encryption Standard mechanics with 256-bit parameters (AES-256). Cryptographic key management operations are handled via dedicated hardware isolation clusters inside the primary cloud infrastructure stack.

4. UPSTREAM ARTIFICIAL INTELLIGENCE PROCESSING & NON-RETENTION SAFE HARBORS

4.1 Elimination of Long-Term Retention Pipelines.

To ensure institutional security compliance, the Platform decouples data ingestion from large language model processing layers. Any prompt queries, contextual table extractions, or financial metrics transmitted across the Company's API Abstraction Gateway to third-party model registries (such as OpenAI Enterprise or Anthropic API) are routed strictly through authenticated business endpoints configured for **Zero-Data-Retention (ZDR)**. Upstream server nodes do not write your inputs, prompts, or metadata context payloads to persistent local server logs or non-volatile storage arrays.

4.2 absolute Protection Against Model Calibration & Fine-Tuning.

The Company’s foundational enterprise covenants strictly bar upstream subprocessors from consuming, processing, or scraping Customer Data, custom prompt strings, or proprietary financial metrics for the purpose of training, adjusting, fine-tuning, or checking public base models, neural weights, or algorithmic reasoning graphs. All systemic calculations and outputs remain locked within your active session parameters.

5. DATA RETENTION, EPHEMERAL STATES, AND TTL EXPIRATION MATRICES

The Company prioritizes ephemeral memory layouts over long-term persistent data accumulation. Analytical calculations, transient reporting grids, and chart metadata are managed inside high-speed memory caching structures configured with automated **Time-To-Live (TTL)** expiration rules. Once an operational analytical loop completes or a user session invalidates, cached context objects are automatically rewritten or purged. Persistent database storage is limited exclusively to core account profiles, active transaction ledgers, and configurations required to maintain subscription records across the duration of the Master Services Agreement.

6. STRICT NON-DISCLOSURE & PERMITTED DISCLOSURES

The Company does not sell, rent, monetize, trade, or distribute Subscriber credentials, consumer financial variables, or portfolio metrics to advertising broker networks, corporate aggregators, or unauthorized third-party operators. Information disclosures are restricted exclusively to: (i) trusted infrastructure Subprocessors (e.g., Amazon Web Services for database hosting) who are bound by matching data isolation rules; (ii) explicit commands or data connections authorized directly by the Subscriber's master API setup; or (iii) mandatory regulatory compliance requests issued by a federal court of competent jurisdiction within St. Louis County, Missouri.

7. USER GOVERNANCE RIGHTS AND OPT-OUT CONTROLS

Subscribers maintain complete control over their active data footprint. Users may review, update, or completely purge their custom transaction metrics or system profile settings via the user account panel. Because the Platform operates purely via programmatic API queries and automated alert loops configured directly by the user, there are no un-mapped tracking vectors or marketing beacons. Purging an account coordinates an immediate, systemic cascading deletion command across the active data layer, rendering all historical tenant rows unrecoverable after a security cache flush period of fifteen (15) business days.

8. AMENDMENTS, GOVERNING LAW, AND CONTACT VECTORS

The Company reserves the right to modify this Policy periodically to account for infrastructure scaling, database adjustments, or updates to the GLBA Safeguards Rule. Subscribers will be notified of material modifications via system dashboard highlights. This Policy and all information processing operations shall be governed strictly by the laws of the State of Missouri, with exclusive jurisdictional venue locked to the courts serving St. Louis County, Missouri. Administrative data protection inquiries may be routed to the corporate compliance manager at `compliance@thesis.com`.