Privacy Policy

Revision Date April 1st, 2025

At Portfolio ThinkTank, together with our affiliates and subsidiaries, we believe that privacy is more than a legal requirement—it's a cornerstone of trust. Our advisory clients entrust us with sensitive financial and personal information, and we take that responsibility seriously. Whether you're planning your financial future or simply exploring our tools, we want you to know we're committed to treating your information with care, transparency, and respect. This document outlines the policies and protections we have in place to keep your data safe and to give you meaningful control over how it's used.

PRIVACY POLICY/REGULATION S-P

Definitions

- **PII (Personally Identifiable Information)**: Personally Identifiable Information refers to any information that can be used to distinguish, trace, or link to the identity of an individual, either directly or indirectly. This includes data such as name, address, email, IP address, phone number, and other identifiers. PII encompasses a broad range of data and applies to both Users and Advisory Clients, regardless of whether a financial relationship exists.
- **NPI (Nonpublic Personal Information)**: A subset of PII, NPI refers specifically to personally identifiable financial information provided by an individual in connection with seeking or receiving a financial product or service from the Company. NPI protections apply primarily to Advisory Clients and are subject to specific requirements under GLBA and Regulation S-P.
- **Investor**: An investor may be either a user or an advisory client.
- **Company**: Refers to Gravity Investments, Portfolio ThinkTank, or any affiliated entity subject to this policy.

- **NPI (Nonpublic Personal Information)**: Information provided by an individual in connection with obtaining a financial product or service from the Company that is not publicly available. This includes data tied to an advisory relationship or submitted in the course of financial services.
- **User**: A general website visitor or software user who may or may not be an advisory client. Users may interact with marketing content or services but do not have an established fiduciary relationship.
- **Advisory Client**: A person or entity that has an established investment advisory relationship with the Company. This relationship is governed by executed agreements and is subject to fiduciary obligations.
- **Employee**: Includes all regulated professionals, employees, contractors, and technical workers with privileged access to systems containing NPI, regardless of employment status.

Examples of NPI (as applied to Advisory Clients)

Data Element	Covered as NPI?	Notes
Full Name	Yes	Identifies an individual when associated with financial services
Email Address	Yes	Especially when linked to an advisory relationship or login credentials
Social Security #	Yes	Sensitive identifier, always protected
Account Numbers	Yes	Includes brokerage, bank, or other investment-related accounts
Holdings / Positions	Yes	Investment data linked to identifiable individuals
Residential Address	Yes	Used for client communications or compliance purposes
Phone Number	Yes	Contact information associated with financial account
IP Address	Possibly	When linked to a user account or used for authentication
Device Type	Possibly	Not NPI by itself; may be protected when linked to authenticated sessions or logs

Data Element	Covered as NPI?	Notes
Date of Birth	Yes	Frequently required for identity verification
Transaction History	Possibly	If connected to PII
Clickpaths / Mouse Events / Session Recordings	Possibly	Treated as NPI if identifiable or used to reconstruct client interactions with financial tools or if tied to authenticated advisory clients or used for decision tracking

The Company views protecting its advisory clients' private information as a priority and, pursuant to the requirements of the Gramm-Leach-Bliley Act (the "GLBA"), the Company has instituted the following policies and procedures to ensure that such information is kept private and secure.

This policy serves as formal documentation of the Company's ongoing commitment to the privacy of its advisory clients. All employees will be expected to read, understand and abide by this policy and to follow all related procedures to uphold the standards of privacy and security set forth by the Company. This Policy, and the related procedures contained herein, is designed to comply with applicable privacy laws, including the GLBA, and to protect confidential and proprietary personal information of advisory clients.

In the event of new privacy-related laws or regulations affecting the information practices of the Company, this Privacy Policy will be revised as necessary and any changes will be disseminated and explained to all personnel.

Scope of Policy

Voluntary Alignment with Consumer Privacy Bill of Rights

The Company voluntarily aligns its privacy practices with the spirit of the Consumer Privacy Bill of Rights, including principles of transparency, individual control, respect for context, data security, access and accuracy, limited collection, and accountability. While not legally binding, this framework reflects the Company's commitment to responsible data stewardship.

To support these principles, the Company offers clients the ability to request deletion or correction of their personal data by contacting our compliance team at [privacy {@} gravityinvestments.com] or via any official communication channel. Requests will be handled promptly, subject to legal or regulatory data retention requirements.

This Privacy Policy applies to all nonpublic personally identifiable information collected from or about advisory clients. It does not extend to non-client users unless such users initiate a financial relationship with the Company.

Information Collected and Purpose

The Company collects the following categories of data:

- Personally identifiable information submitted during account creation or advisory onboarding;
- Technical metadata from use of Company websites and applications (e.g., IP address, device type, log files);
- Analytics and marketing cookies to improve user experience and measure the effectiveness of campaigns.
- Statements or Spreadsheets provided by you.

This information is collected for legitimate business purposes including compliance with regulatory requirements, delivering financial services, enhancing cybersecurity, and improving customer support and product development. Data collected from general Users (non-clients) is treated according to its sensitivity and legal classification, but is not subject to the same fiduciary handling as NPI for advisory clients.

Overview of the Guidelines for Protecting Customer Information

In Regulation S-P, the Securities and Exchange Commission (the "SEC") published guidelines, pursuant to section 501(b) of the GLBA, that address the steps a financial institution should take in order to protect customer information. The overall security standards that must be upheld are:

- Ensure the security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
- Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Employee Responsibility

Employees are responsible for safeguarding nonpublic personal information (NPI) collected by the Company. They must:

- Avoid unauthorized disclosure or use of NPI;
- Share NPI only with those who require access to fulfill their duties;

- Ensure access to NPI is limited and monitored;
- Never sell NPI under any circumstance;
- Refer questions about handling NPI to the Chief Compliance Officer;
- Understand that violations may result in disciplinary actions.

Types of Permitted Disclosures – The Exceptions

Third-Party Integrations and Vendor Oversight

The Company partners with third-party providers to enable secure account linking, investment execution, and payment processing. These relationships are subject to strict confidentiality agreements and are evaluated for security, compliance, and data protection standards. Key third-party providers include:

- **Plaid** – used for secure user-authorized account aggregation; the Company does **not** store any Plaid-related account usernames, passwords, or authentication tokens.
- **Fidelity, APEX, Interactive Brokers (IBKR)** – used for custody, execution, and account servicing as part of advisory functions.
- **Stripe** – used for secure billing and payment infrastructure.

The Company actively monitors and tests its vendor ecosystem and reserves the right to terminate relationships with vendors who fail to meet its technical, compliance, or operational standards within a reasonable remediation period.

Regulation S-P permits the Company to disclose NPI under specific exceptions:

1. Service Providers: The Company may share NPI with nonaffiliated third parties who perform services on its behalf, provided they contractually agree to confidentiality and data usage limitations.
2. Processing Transactions: The Company may disclose NPI when necessary to process or enforce a client transaction, provide account services, or administer benefits.
3. As Permitted or Required by Law: The Company may disclose NPI in response to legal obligations such as subpoenas, audits, or regulatory requests.

Opt-Out

The Company uses analytics and remarketing cookies to better understand how users engage with its websites and to improve the user experience. These cookies may be set by third-party services and may enable targeted advertising.

Users who prefer not to be tracked via cookies may adjust their browser settings to block or delete cookies. Doing so may impact the functionality and usability of certain site features.

Currently, the Company does not share NPI with nonaffiliated third parties for marketing purposes and thus is not required to offer clients an opt-out right. If this policy changes, appropriate opt-out mechanisms and disclosures will be implemented.

Safeguarding Client Records and Information

The Company uses layered technical, administrative, and physical controls to protect client data, including:

- All system-stored passwords are securely hashed and salted to protect against compromise even in the event of unauthorized access;
- Password-protected systems, role-based access, and enterprise-grade firewalls;
- Encrypted communications and secure server infrastructure;
- Locked file cabinets and shredding of paper records when no longer needed;
- Mandatory Two-Factor Authentication (2FA) on all systems that store or route access to investor NPI;
- Reasonable enforcement of password complexity and rotation standards;
- Ongoing dark web monitoring to detect credential exposure risks.

Incident Response and Breach Notification

The Company maintains written incident response procedures to detect, contain, investigate, and respond to suspected or actual data breaches involving PII or NPI. These procedures include:

- Prompt investigation of any suspected unauthorized access, disclosure, or data loss;
- Containment and remediation actions to minimize impact;
- Documentation of findings and internal reporting to the appropriate personnel;
- Notification to affected individuals and regulators, as required by applicable laws and regulations, if a breach is deemed material;
- Continuous improvement of controls and processes to mitigate recurrence.

The Company may notify affected parties by email, phone, or other appropriate means, consistent with the nature and scope of the breach.

Security Standards

The Company maintains safeguards that include physical, electronic, and procedural protections. Access to client data is limited to employees who require it to perform their responsibilities. Security protocols are reviewed at least annually to ensure they remain current.

Two-Factor Authentication (2FA)

The Company enforces mandatory Two-Factor Authentication (2FA) on all supported systems that contain or provide access to investor NPI or any endpoints connected to such systems, regardless of user role or location.

Infrastructure

The Company is adopting a **least privilege access policy**, ensuring that employees and systems are granted only the minimum necessary access to perform their duties. Privileged access is tightly scoped, logged, and periodically reviewed. This principle is core to both our cybersecurity posture and our movement toward Zero Trust architecture.

The Company application (gsphere.net) uses authenticated access, encrypted sensitive data, and SSL communication protocols. See AWS security policies: https://aws.amazon.com/security/

We regularly monitor, log and optimize our security headings across all controlled applications and websites.

Privacy Notice Delivery

1. Initial Privacy Notice: Provided at account opening.
2. Annual Privacy Notice: Delivered each July, as required by GLBA.
3. Revised Privacy Notice: Sent when there are material changes in collection, sharing, or security practices.