Legacy Financial
INDEPENDENT ADVISORS

Data Privacy Policy

Version 2.0
4-1-2024

Contents

Policy Overview

The Company views protecting confidential information regarding its clients and potential clients as a top priority. Pursuant to the guidelines established by the Securities Exchange Commission regarding the Privacy of Consumer Financial Information (Regulation S-P), the Company has instituted the following policies and procedures to ensure that such non-public confidential information is kept private and secure. This policy also outlines what the Company and its Associated Persons are allowed to use the confidential personal information collected in connection with its advisory activities. This Privacy Policy covers the practices of the Company and applies to all non-public personally identifiable information, including information contained in consumer reports, about our current and former clients.
Protected data under this policy includes confidential and sensitive data that may be in the form of electronic files, portable media, hard copies, etc. Confidential and sensitive data includes but is not limited to bank statements, income statements, tax statements, and reports that contain the names of customers. Sensitive data refers to personally identifiable information (PII) and restricted data. PII includes, but is not limited to:

- Social Security Number
- Driver's license number or identification card number
- An individual's full name, email address, phone number, home address, etc.

Restricted data is divided into two categories:

- Personal data - information that identifies and describes an individual.
- Limited data - electronic information whose unauthorized access or loss could seriously affect its members and/or non-members.

All information provided to the organization will be kept in a secure location and will be accessible only by authorized personnel. The company is committed to protecting personally identifiable information and ensures that it is used in accordance with this privacy policy.

Individuals or Companies Who May Have Access to Protected Data

Individuals who are responsible for the handling, processing, and storage of protected data during their time of employment must undergo ongoing training on security awareness and skills, data handling best practices, and incident reporting. These individuals include:

- Technical Staff that conducts the research and operations for which the data was acquired.
- The PPO (Principal Privacy Officer) is responsible for overseeing all data protection activities, including strategic planning and development of a strategy for the company's privacy program.
- The support staff includes secretaries, typists, computer technicians, messengers, etc. Disclosed protected data may be applicable to these people only if it is necessary for them to perform their duties. For example, a legal secretary may have access to protected data only when he/she is drafting documents and not otherwise.

Protected data may be disclosed to individuals or a company who desire to do independent contracting under the following conditions:

- To access protected data, an Independent Contractor or Vendor will be required to sign a Non-Disclosure Agreement and/or Third-Party Service Agreement. The NDA/TSA must be submitted to the Company in hard copy form with a valid signature and original ink signature.
- The organization provides written approval to disclose protected data to the independent researcher.

Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. Our affiliates include: NONE
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies: RAYMOMD JAMES *** To view Raymond James Privacy Policy go to: www.raymondjames.com/privacy-security-and-account-protection*

Limitations on Disclosure

Except as outlined in agreements under which the data was acquired, the organization shall not disclose protected data or other information containing, or derived from, protected data at fine levels to anyone other than Company employees working in the course of their employment or individuals for whom access is authorized under this policy or agreements subjected thereto.

Reasons we can share your personal information	Does Legacy Financial share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes— to offer our products and services to you	Yes	No
For your CPA, Attorney, or other personal advisors	Yes – Upon your request	Yes
For our affiliates' everyday business purposes— information about your transactions and experiences	No	We do not share
For our affiliates to market to you	No	We do not share
For our affiliates' everyday business purposes— information about your creditworthiness	No	We do not share
For nonaffiliates to market to you	No	We do not share

Security Requirements

The organization shall maintain a data management process that addresses data sensitivity, data owner, handling of data, data retention limits, and disposal requirements. Data will be stored for an appropriate period according to the organization's data retention policy and compliance with legal and regulatory requirements. After the retention period, the data will be disposed of securely. Data shall be backed up daily and all backups shall be maintained in a secure manner. No copy or extract of the protected data shall be made available to anyone except a PT/S or independent contractor as necessary for the purpose of the operations and research for which the protected data were made available or acquired by the organization.

Protected data will be encrypted at rest and in transit to protect it from unauthorized access. Additionally, authentication and access control mechanisms should be implemented to ensure that only authorized individuals can access the protected data. The organization shall use monitoring systems to detect unauthorized access attempts or suspicious activity and maintain detailed logs of data access and changes. Physical copies of data shall be stored securely.

The organization shall conduct regular security audits and assessments to identify and remediate vulnerabilities and gaps in data storage and network security.

The organization shall not disclose or otherwise make accessible, protected data to anyone outside of the organization except under limited circumstances. If it is necessary for any fact finder or other third party to have access to protected information, the company shall obtain written authorization from the appropriate person. Any disclosure of such information will be limited only to those facts that are strictly required by law.

Scope and Purpose

This policy covers the use of individually identifiable information that an organization collects and holds about customers. It also describes how to use, store, and secure this information.

Compliance

The Information Security team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Exceptions

Any exception to the policy must be approved by the Information Security team in advance.

Definitions and Terms

- Access Controls: Mechanisms that limit and control access to data and resources based on specified rules and permissions. Access controls enforce authorization and segregation of duties and ensure that only authorized individuals have appropriate access privileges.

- Authentication: The process of verifying the identity of an individual or device to allow access to resources or data. It usually involves providing credentials, such as usernames and passwords, or using more advanced methods like biometrics or multi-factor authentication.

- Backup: Copy of data created as a safeguard against data loss. Backups are typically stored in a separate location to ensure data recovery in case of system failures or data breaches.

- Confidential Data: Information that is not publicly available and requires protection from unauthorized access or disclosure. This includes business plans, supplier lists, marketing strategies, and other information that, if made public, can cause financial or reputational harm to an organization.

- Data Disposal: The process of securely and permanently removing or destroying data that is no longer needed or has reached the end of its retention period. It is important to properly dispose of data to prevent unauthorized access or recovery.

- Data Handling: The procedures and practices involved in the access, manipulation, and storage of data. It includes activities like data entry, data transfer, and data destruction, and should be conducted in compliance with applicable privacy and security policies.

- Data Management: The process of organizing, storing, and maintaining data throughout its lifecycle. It includes activities such as data collection, storage, processing, analysis, and archiving.

- Data Retention: The period for which data is stored and maintained. Data retention policies specify the duration for which data should be retained based on legal, regulatory, or business requirements.

- Encryption: The process of converting data into an unreadable format using cryptographic techniques to protect it from unauthorized access. Encryption helps ensure the confidentiality and integrity of data, both at rest and in transit.

- Personally Identifiable Data (PII): Any information that can be used to identify an individual, either alone or in combination with other data. This includes name, address, social security number, email address, or any other data that can be traced back to an individual.

- Personal Data: Any information that relates to an identified or identifiable individual, including PII. It can include sensitive or non-sensitive information that is linked to an individual.

- Restricted Data: Classified or extremely sensitive data that has strict access controls and is subject to legal or regulatory restrictions. This includes trade secrets, intellectual property, and other sensitive information that require strict access controls and monitoring.

- Sensitive Data: Personal or organizational data that requires a higher level of protection due to its sensitivity or criticality. This includes health records, financial information, biometric data, and other information that, if compromised, can cause significant harm to individuals or organizations.