Rittmann Capital Management

Privacy Policy

Confidentiality, Proprietary Data and Privacy of Customer Personal Information

1. Proprietary Data; Confidentiality. Any information regarding advice furnished by the Firm to Client Accounts, the Firm's recommendations and analyses and other proprietary data or information about the Firm or Client Accounts is strictly confidential and may not be revealed to third parties. Such information is the property of the Firm. Disclosing such information to any third party, without the permission of the Compliance Officer, is grounds for an Employee's immediate dismissal. This confidentiality obligation continues even after the termination of employment.

2. Privacy of Customer Personal Information -- Information Security Program. It is the Firm's policy to protect, through administrative, technical and physical safeguards, the security and confidentiality of financial records and other nonpublic personal information concerning Client Accounts (including in each case, potential Client Accounts and former Client Accounts). This includes protecting against any anticipated threats or hazards to the security of such information and unauthorized access to or use of such information.

a. The Compliance Officer. The Firm has designated Kate Rittmann as the Compliance Officer to coordinate its information security program. The Compliance Officer is responsible for (i) assessing existing risks to nonpublic personal information, (ii) developing ways to manage and control these risks, (iii) monitoring third-party service provider arrangements to ensure information security, and (iv) testing and revising the program in light of relevant changes in technology and threats to Client Account information.

b. Identifying Internal and External Risks to Customer Information. The Compliance Officer reviews reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information, including risks relating to (i) Employee training, (ii) changes to the Firm's information systems, including network and software design, information processing, storage, transmission and disposal, and (iii) procedures to detect, prevent and respond to attacks, intrusions or other system failures. The Compliance Officer assesses the likelihood and potential damage of these risks and the sufficiency of any safeguards in place to control these risks. The Compliance Officer meets periodically with Employees to review and implement the program and is available to answer questions regarding the program.

c. Information Safeguards. Employees may not disclose the identity, affairs or investments, or other personal information, of any Client Account, potential Client Account or former Client Account to anyone outside of the Firm, except as may have been authorized by the client or as may be required in servicing the Client Account (such as disclosure to a brokerage firm at which such Client Account is held) or for the business of the Firm (such as to the Firm's auditors and lawyers or as required by law). Employees should direct to the Compliance Officer any questions about whether information is confidential or any disclosure is permitted. This confidentiality obligation continues even after the termination of employment.

To protect the confidentiality of the Firm's confidential and proprietary information and the confidentiality of existing, former or potential Client Accounts, Employees should take the following additional security precautions:

1. Documents containing confidential and proprietary information may not be taken from the Firm's offices without the prior consent of the Compliance Officer, and any copies removed from the Firm's offices must be returned promptly. Photocopies of confidential and proprietary information may be made only as required, and all copies and originals of such documents must be disposed of in a way that keeps the information confidential, such as shredding. When not in use, all paper copies of confidential and proprietary information must be kept off desk tops, conference tables or any other place where such copies would be visible to persons who are not authorized to have access to such information.

2. All computer drives containing confidential and proprietary information must be accessible only by the use of passwords issued by the Firm, and all authorized users of such computer drives must log off when leaving a terminal through which they are authorized to access any such computer drive.

3. Physical access to any non-electronic confidential and proprietary information must be limited by either locking or monitoring access to the offices and storage areas where such information is located.

The Compliance Officer regularly tests and otherwise monitors the effectiveness of the Firm's information safeguards and revises them, as necessary. The Firm will notify Employees of any revisions to the safeguards. The Firm will provide Clients with a notice of its privacy policy on an annual basis.

d. Third Party Service Providers. At times, the Firm may enter into one or more agreements with third parties under which the Firm may provide access to confidential information to those third parties. If this occurs, the Firm will (i) include in the relevant agreements provisions protecting confidential information to the extent required by law, (ii) take reasonable steps to select and retain service providers that can maintain appropriate safeguards for the confidential information at issue and (iii) require these service providers to implement and maintain such safeguards. Employees should direct any questions about these agreements or the disclosure of information pursuant to them to the Compliance Officer.

Evaluating and Updating of the Program

The Compliance Officer will evaluate and adjust the Firm's information security program in light of the results from testing and monitoring the program and any material changes to the Firm's operations, business arrangements or any other circumstances that may have a material effect on the Firm's information security program.