# Privacy Policy

## Information Collected and Shared

The privacy policy statement is given to clients at the initial signing of the client contract and mailed or emailed with client consent once annually, if the policy is updated. The CCO will document the date the privacy policy was delivered to each client for each year if an annual delivery is required. OAM collects non-public personal information about clients from the following sources:

- Information it receives from them on applications or other forms;
- Information about their transactions with OAM or others; and
- Information it receives from a consumer reporting agency.

Below are the reasons for which OAM may share a client's personal information:

- With specific third parties as requested by the client;
- For everyday business purposes – such as to process client transactions, maintain client account(s), respond to court orders and legal investigations, or report to credit bureaus;
- For marketing by OAM – to offer OAM's products and services to clients;
- For joint marketing with other financial companies;
- For affiliates' everyday business purposes – information about client transactions and experience; or
- For non-affiliates to market to clients (only where allowed).

If a client decides to close his or her account(s) or becomes an inactive customer, OAM will adhere to the privacy policies and practices as described in this Privacy Policy, as updated.

OAM uses various methods to store and archive client files and other information. Third party services or contractors used have been made aware of the importance OAM places on both firm and client information security. OAM also restricts access to clients' personal and account information to those employees who need to know that information to provide products or services to its clients. In addition to electronic protection, procedural safeguards, and personnel measures, OAM has implemented reasonable physical security measures at its home office location

In addition to OAM's listed access persons, any IT persons or other technical consultants employed at the firm may also have access to non-public client information at any time. An on-site or off-site server that stores client information, third-party software that generates statements or performance reports, or third-party client portals designed to store client files all hold the potential for a breach of non-public client information.

To mitigate a possible breach of the private information, OAM uses encryption software on all computers and carefully evaluates any third-party providers, employees, and consultants with regard to their security protocols, privacy policies, and/or security and privacy training.

The system is tested and monitored at least monthly.

The test conducted by the CCO will include the following activities:

- Attempt to access a random sample of firm devices to ensure that proper passwords are in place to prevent access;
- Attempt to access users' accounts with the proper password to ensure that two-factor authentication prevents system access; and
- Attempt to restore a sample of files and records to ensure that the restoration process is sufficient and properly configured.

The results from the annual test will be documented and utilized as an opportunity to update the Cyber Security & Information Security Policy.

## Identity Theft

The SEC and CFTC (U.S. Commodity Futures Trading Commission), and many state regulators, have published rules concerning identity theft encouraging or requiring investment advisers to train firm personnel to recognize "red flags" in this area. While many of these provisions are also covered in the firm's broader privacy and AML policies, the list below is a brief non-exhaustive listing of the items and information that all OAM personnel should monitor to guard against any breach of a client's identity:

SAFEGUARDING IDENTIFYING INFORMATION

- Individual client's social security numbers
- Corporate or other entity client's tax identification numbers
- Individual driver's license number or other personal identification card
- Passport numbers
- Financial account numbers (credit card, bank, investment, etc.) and any accompanying passwords or access codes

POTENTIAL CAUSES OF IDENTITY INFORMATION BREACHES

- Loss of theft of computers and/or other equipment
- Hacking of computer networks
- Inadvertent exposure of client information to unauthorized individuals (non-locked files, files left on desk, cleaning services, shredding services, etc.)
- Physical break-ins / theft

OAM personnel are instructed to notify and report to the firm's CCO, or other designated principal, if they detect or have reason to believe that any of the above shown red flag activities may have occurred or if any of the red flag information listed may have been stolen or leaked by any firm personnel. The CCO or principal is then tasked with investigating the report and taking appropriate actions. The non-exhaustive list of possible follow-up actions includes notification of the parties involved, notification of appropriate regulatory officials if required, taking remedial actions to assist in the recovery of the stolen information, and possible sanctions of firm personnel if deemed necessary.

## Staff Training

On an annual basis, OAM will conduct a firm-wide training session to ensure that staff members are properly trained and equipped to implement the above policies. New staff members will receive training, led by the CCO, within one (1) month of their initial hire date.

## Records

OAM will retain records for at least 5 years after the year in which the record was produced, or as otherwise required by law. With respect to disposal of non-public personal information, OAM will take reasonable measures to protect against unauthorized access to or use of such information in connection with its disposal.

OAM takes the privacy and confidentiality of all its clients and personnel very seriously. It will continue to make, and document, any changes needed to promote the security non-public information.