Family Fiduciary Services, Inc.
Privacy Policy

Family Fiduciary Services, Inc. is committed to protect personal information of investment advisory clients. As part of this commitment, Family Fiduciary Services, Inc. has adopted the following procedures regarding the retention and transmission of personal information of investment advisory clients who reside in Massachusetts. For purposes of this policy, "personal information" is defined as:

An individual's first name or initial and last name; AND any one of the following:

Social Security number
Financial account number
Driver's license number
Other unique credit identifier

RETENTION OF PERSONAL INFORMATION

Family Fiduciary Services, Inc. will disseminate these procedures to all employees and, on at least an annual basis, conduct employee training on these procedures.

Employee compliance with these procedures will be monitored through periodic and forensic testing performed in conjunction with the firm's annual compliance audit.

The Chief Compliance Officer will remain familiar with current threats to information security and will be responsible for upgrading systems as needed.

All records containing personal data shall be reasonably free from unauthorized access. Records containing personal information shall only be destroyed under the supervision of the CCO or their delegate.

All associated persons of Family Fiduciary Services, Inc. are required to alert their immediate supervisors to any potential threat to the security of personal information.

Possible steps to improve Family Fiduciary Services, Inc's ability to detect, prevent and respond to security failures, as well as a review of internal and external threats to security, will be included in the annual risk and conflict assessment conducted under the supervision of the CCO.

ELECTRONIC STORAGE AND TRANSMITTAL OF PERSONAL INFORMATION

Family Fiduciary Services, Inc. has developed the following user identification protocols:

() Unique usernames and password to internal systems for all employees. CCO retains a log of all internal usernames and passwords. Administrator access may only be assigned

by the CCO or his/her delegate. Access to internal systems will be designed to block access to the system after several unsuccessful attempts.

() Unique usernames and passwords for all external systems including personal information (e.g., access to client accounts at the client's custodian).

() Usernames and passwords will be changed every 3 months. CCO will coordinate the change of internal and external systems.

All records containing personal information transmitted electronically, including wireless transmissions, will be encrypted. Laptops and all portable devices will be encrypted. CCO or his/her delegate will determine the method of encryption.

CCO will ensure that firewall protection, operating system patches, up-to-date-security software, and malware protection are in place and functioning properly.

PERSONS WORKING OUTSIDE THE OFFICE

Personal information is not to be removed from the office, with the following exceptions:

Persons working outside the office (from home or on the road) may access personal information:

() From a home computer that the CCO or his/her delegate has determined meets the firm's security policies;
() Through the firms virtual private network (VPN)
() On an encrypted flash drive
() Through an Internet connection that the CCO or his/her delegate has determined meets the firm's security standards.

RESPONDING TO VIOLATIONS

Any employee who suspects there may have been an attempt to improperly access personal information shall immediately bring this matter to the CCO or his delegate. The CCO will investigate, make any necessary corrections, and document their findings. If the CCO determines that a breach has occurred which may compromise the security of personal information, or that personal information has been lost, they will immediately bring this matter to the attention of the President to begin the client notification process.