Privacy Policy

Date Created: 2/26/2013
Date Last Revised: 03/09/2017

Table of Contents

Purpose

Clients entrust Selective Wealth Management ("Selective") with confidential financial and identity information, and as good stewards it is our duty to provide every reasonable precaution and protection measure to secure said information. Selective has developed and implemented many safeguards to uphold the security and safety of clients and this document outlines the measures taken.

Information Collection

Selective gathers sensitive data from clients, primarily through the website www.selectivewm.com. Selective obtains information from clients pertaining to account numbers, social security numbers, telephone numbers, addresses, income(s), risk tolerances and investment preferences, in addition to other select pieces of information. This information is used to develop an appropriate investment strategy for each client and complete our qualified custodian's account opening paperwork.

Information Storage

To ensure the protection of client information Selective utilizes multiple means of data storage and backups. Below is a list of the data storage and backup applications.

- *Hard Copy*: Selective keeps all IACs on file in addition to other items pertaining to employee health records, banking information and legal formation.
- *Third Party Cloud Solution*: Selective utilizes a cloud data storage solution which contains all documents and media produced by Selective. This cloud solution is only accessible by individuals with listed usernames and passwords and allows employees to more securely access files.
- *Hard Drives*: Selective keeps three external hard drives which serve as backups for all documents. Two of these hard drives are backed up monthly and the other is used periodically in between. The two monthly backups are stored in a safety deposit box located at a local bank branch.

Customer Information Access

Selective is committed to safeguarding the confidential information of clients - we hold all personal information provided in the strictest confidence. These records include all personal information that is collected from clients in connection with any of the services provided by Selective. Selective will never disclose information to nonaffiliated third parties, except when necessary by law. If Selective were to anticipate such a change in firm policy, Selective would be prohibited from doing so under law without advising you first. Selective uses information provided by clients to help them meet their personal financial goals while guarding against any real or perceived infringements of their rights of privacy.

Selective has contractual agreements with multiple services providers who have access to sensitive client information. We have stringent confidentiality agreements with these providers and expect them to keep information private and protected through their respective company safeguards.

Selective has a web domain (www.selectivewm.com) which current and prospective clients can access. Clients can develop online usernames which allow them to open accounts and view their holdings amongst other things. This domain is protected with industry standard security through a secure server and SSL (Secured Socket Layer). This provides protection to client information from hackers and others who might want to steal sensitive data.

Safeguards

Selective has established its Chief Compliance Officer (CCO) as coordinator of established safeguards. The CCO will be responsible for ensuring that employees have been educated on company policy and adhere to established guidelines.

The CCO will be responsible for monitoring the effectiveness of the established safeguards. At least annually and at most quarterly the CCO will be required to investigate and report on the usefulness of Selective's privacy policies and procedures.

Selective has established multiple avenues of protection to provide the best safeguards possible given the environment. Employees are only given access to files they need limiting the amount of client information that is exposed. Computers are secured with passwords and antivirus to protect from cyber-attacks, and hard drives are stored in a safety deposit box. In addition, offices are secured with dead-bolt locks and additional locking points throughout the building.

Compromised Security

In the event that client information is compromised Selective has outlined steps to isolate and address the issue. Below are the series of steps that will be taken if a situation ever arises:

- Monitor, limit, or temporarily suspend activity in the account until situation is resolved
- Alert the CCO and others in the firm to see if anyone else is reporting an issue
- Identify, if possible, the root of intrusion
- Contact SEC and respective FINRA Coordinator
    - http://www.sec.gov/contact/addresses.htm
    - http://www.finra.org/Industry/Contacts/P016038
- If appropriate, Selective will contact law enforcement agencies
- Contact relevant state authorities
- Contact the compromised client
- Determine whether or not a Suspicious Activity Report (SAR) is required to be filed

Former Clients

If you are no longer a client of Selective, we continue to use, disclose and safeguard client information as described above.

Modifications to Policy

If necessary the CCO will make modifications to this policy and ensure that employees are updated accordingly.