Privacy Policy & Information Security

The privacy policy statement is given to clients at the initial signing of the client contract and mailed or emailed once annually. The CCO will document the date the PPS was mailed to each client for each year. Jarvis Financial Services Inc (JFS) collects nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other forms;
- Information about your transactions with us or others; and
- Information we receive from a consumer reporting agency.

We do not disclose any nonpublic personal information about you to anyone, except as permitted by law.

If you decide to close your account(s) or become an inactive customer, we will adhere to the privacy policies and practices as described in this notice.

JFS restricts access to your personal and account information to those employees who need to know that information to provide products or services to you. JFS maintains physical, electronic, and procedural safeguards to guard your nonpublic personal information.

The following employees will manage nonpublic information: Matthew Jarvis
The following individuals also have access to this nonpublic information: Matthew Jarvis Nathaniel Jarvis, Cindy Jarvis, Colleen Clark
The following systems may be vulnerable to a breach of your nonpublic information: On-site data storage, off-site backups and third party data providers/aggregators (e.g. Black Diamond/Advent). Our IT service firm also has limited access to non-public data

To mitigate a possible breach of the private information JFS will encrypt all data that individuals have access to or use password sensitive documents. The system will be tested and monitored at least annually.

JFS has taken extensive measures to safeguard the privacy and integrity of the information that it gathers, stores, and archives during its normal business practices. Computer security measures have been instituted where applicable including passwords, backups, and encryption. All employees are informed and instructed on various security measures including the non-discussion and/or sharing of client information, always removing client files from desktops or working areas that cannot be locked or secured, and proper storage of client securities files in locked files or other secured location. JFS uses various methods to store and archive client files and other information. All third party services or contractors used have been made aware of the importance JFS places on both firm and client information security. In addition to electronic and personnel measures JFS has implemented reasonable physical security measures at our home office location, and encouraged all remote locations, if any, to do the same to prevent unauthorized access to our facilities.