

Privacy Policy Information

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 privacy policy was mailed to each client for each year.

Collection & Sharing of Clients' Personal Information

MWP collects nonpublic personal information about clients from the following sources:

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

Below are the reasons for which MWP may share a client's personal information.

- 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 our marketing – to offer our products and services to clients;

If a client decides to close the account(s) with MWP or otherwise leave MWP's service, MWP will adhere to the privacy policies and practices as described in this notice.

Safeguarding of Clients' Personal Information

MWP restricts access to clients' personal and account information to those employees who need to know that information to provide products or services to the client. MWP maintains physical, electronic, and procedural safeguards to guard nonpublic personal information.

The following employees will manage nonpublic information: David Kevin Luke, Kevin Douglas Michels, Celeste Kennard, and Kaden Collins.

The following individuals also have access to this nonpublic information: James W. Zeberlein and Dan W. Loose.

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

MWP 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. MWP 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 MWP places on both firm and client information security. In addition to electronic and personnel measures MWP 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.

MWP will retain records for at least 5 years, or as otherwise required by applicable state or federal law. With respect to disposal of nonpublic personal information, MWP will take reasonable measures to protect against unauthorized access to or use of such information in connection with its disposal.