

# Privacy & Data Security Policy

We collect only the information that is required to provide you with the highest quality professional services or that is required by law and regulation. We maintain strict security procedures to protect information that we collect. We collect non-public personal information about you from:

- Applications or other forms we receive from you;
- Transactions with us, our affiliates, or others; and
- Consumer reporting agencies as needed.

We provide non-public personal information (as noted above) to outside vendors only to the extent necessary to complete your financial transactions. Under no circumstances whatsoever will Clarity Wealth Development or its affiliates sell information about you or your business to any vendor, public or private.

Employee access to customer information is restricted to those that have a legitimate need to know in order to provide our professional services or to comply with laws and regulations. Please notify us any time our records contain incomplete or inaccurate information about you.

Protecting your privacy is an on-going process and we will take every precaution to protect your information. Nothing is more important to us than our clients' trust and confidence, and we will take whatever steps necessary to maintain the security of our professional relationships.

## Data Security - How We Protect Your Data

We maintain physical, electronic and procedural safeguards to limit access to all your nonpublic personal information. This includes physical and electronic data security measures, as well as secure connections to off-site platforms. Passwords are changed every three to six months to prevent unauthorized access to sensitive data and systems, which are also protected with two-factor authentication.

(CONTINUED ON NEXT PAGE)

---

Certain systems, including custodians and other third-party platforms, may be vulnerable to unauthorized access to nonpublic personal information. These systems may store sensitive data such as Social Security numbers, dates of birth, and other client-related information. We maintain copies of the privacy policies for all such service providers on file. In addition, we utilize an email archiving solution to retain and monitor all electronic communications in accordance with regulatory requirements.

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

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

CWD will retain records for at least 6 years, or as otherwise required by applicable state or federal law. With respect to disposal of nonpublic personal information, CWD will take reasonable measures to protect against unauthorized access to or use of such information in connection with its disposal.

---