Steward Advisors
Helping Families Make Wise Financial Choices

Privacy Policy

Our clients place a great deal of confidence in us, and as such it is imperative that we maintain their privacy and hold the confidentiality of the information provided to us in the highest regard.

Steward Advisors, LLC ("Steward") collects a variety of personal data from clients. The type of information collected and maintained varies depending on each client's situation, but may include any of the following:

- Application data (names, addresses, phone numbers, social security numbers, employment information, birth dates, etc.);
- Transaction data (trade history, dividend and interest payments, deposits, withdrawals, gifts, and transfers);
- Asset data (family assets, titling, valuation, and other asset specific information);
- Third party data (information from accountants, attorneys, and other advisors such as tax returns/tax information, estate planning information, life and other insurance information, etc.);
- Employment data (benefit plans, 401k or other retirement plan information, other employer related plans if applicable); or
- Personal data provided by clients (goals, objectives, special needs or situations, etc.).

At any time, various members of the Steward staff have access to any or all items in a client's personal file. Principals and staff members may not divulge any information of any kind to any person, except as follows:

- To other advisors as a client may authorize from time to time;
- To securities firms and/or other financial services providers in the course of arranging a transaction on the client's behalf;
- To vendors (such as hosting providers and software service providers) as necessary to provide services to clients. When we disclose client data to vendors, it is done under an obligation of confidentiality, and we only disclose as much of the information as is necessary to provide services.
- To comply with legal or regulatory requirements or legal process;
- To defend a principal or employee of Steward;
- To comply with regulatory authorities such as the FINRA, SEC, or state level regulators; or
- At a client's written request, to outside parties with whom Steward does not have a working relationship (e.g., attorneys, accountants, securities and other brokers).

At all times Steward will attempt to disclose only such information as necessary to fulfill requirements of a particular circumstance. A client may prevent disclosures of information via written request stating a desire to block disclosure and acknowledging that Steward's ability to effectively fulfill its duties may be hampered or limited by such a request.

A client may not prevent disclosure of information in the following circumstances:

- When required by regulatory or legal authorities;
- To defend a principal or employee of Steward; or
- When required in the course of the service of legal process, court order, or subpoena.

It is Steward company policy that no client personal information is to be shared in any situation except as outlined above. Discussions with third parties, except while providing service, shall not include client names, personal information, or any readily recognizable information that might identify a client. Measures should be taken to prevent client information from being viewed by third parties, even to the extent of removing client files from desktops if a bystander might "accidentally" view them.

All electronic correspondence that contains client information is safeguarded to the extent possible. This includes all the following:

- All computer access requires a unique password. All computers automatically sign out after 15 minutes of inactivity and require password authentication to log back in.
- Backup tapes, disks or other media used to provide backup copies of electronic information are stored in a secure manner onsite or when taken offsite. "Secure manner" is defined as strongly encrypted (AES 256-bit) or locked in a safe or strongbox that requires either a key or a combination for access.
- No documents, files, or other client information are removed from company offices by any employee without authorization from a principal of the firm.
- Any document containing client information that is not archived is destroyed by means of a shredder. Any backup tape or disk to be destroyed is shredded if possible. If that is not possible, the disk or tape is destroyed in such a manner as to make the media nonfunctional and nonrecoverable.

In the event the Chief Compliance Officer (CCO) becomes aware of breaches by way of self-identification, employee notifications, or by other means, the CCO will be responsible for conducting a prompt investigation into the breach to determine its scale, affected persons, reasons for the breach, and a determination of what steps or actions should be implemented going forward to prevent future such breaches. More so, in the event client information has been compromised, the company, through its CCO, shall provide prompt notification to affected clients indicating, at a minimum, the nature of the breach, what steps the firm is taking to resolve the matter, and how the client can contact the company for more information.

Steward Advisors, LLC

As adopted September 1, 2024