

Steward Advisors, LLC

Privacy Policy

Our clients have placed 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.

We collect a wealth 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);
- Personal data provided by you (goals, objectives, special needs or situations, etc.).

At any time, various members of the Steward Advisors, LLC 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 your 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 our vendors (such as hosting providers and software service providers) as necessary to provide our services to you. When we disclose your data to our vendors, it is done under an obligation of confidentiality and we only disclose as much of the information as is necessary to provide our service to you.
- To comply with legal or regulatory requirements or legal process;
- To defend a principal or employee of Steward Advisors, LLC;
- To comply with regulatory authorities such as the FINRA, SEC, or state level regulators;

At all times Steward Advisors, LLC will attempt to disclose only such information as necessary to fulfill requirements of a particular circumstance.

At a client's written request we will release information to outside parties with whom Steward Advisors, LLC does not have a working relationship (e.g., attorneys, accountants, securities and other brokers).

A client may prevent disclosures of information via written request stating a desire to block disclosure and acknowledging that Steward Advisors, LLC's ability to effectively fulfill its duties may be hampered or limited via such request.

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

- Regulatory authorities;
- When required in the course of the service of legal process, court order, or subpoena.

It is our company policy that no client personal information is to be shared in any situation except as outlined above. Discussions with third parties, except in the course of 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 one's desk top in the event that a bystander might "accidentally" view them.

All electronic correspondence that contains client information must be safeguarded to the extent possible.

All computer access requires a unique password. All computers will 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 to be stored in a secure manner when taken offsite. "Secure manner" is defined as locked in a safe or strongbox that requires either a key or a combination for access.

No documents, files, or other client information are to be 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 to be destroyed by means of a shredder. Any backup tape or disk that is to be destroyed must be shredded if possible. If not possible, the disk or tape must be destroyed in such a manner as to make the media nonfunctional.

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.

This policy may be altered or amended from time to time as necessary; however, any changes made to the policy will not become effective until notice of the changes has been mailed to all effected clientele.

The privacy policy notice should be delivered at the same time as the advisory contract. In addition, an annual privacy policy notice must be made. The preferred method of delivery of the annual notice is with the annual disclosure brochure notice, if possible. Alternately, it may be enclosed in any other correspondence that is sent en masse to all advisory clients.

Steward Advisors, LLC

As adopted June 5, 2014