Privacy Policy Statement

We respect the privacy of all clients and prospective clients (collectively termed "customers" per federal guidelines), both past and present. It is recognized that customers have entrusted our firm with non-public personal information and it is important that both access persons and customers are aware of firm policy concerning what may be done with that information. Federal law gives the customer the right to limit some but not all sharing of personal information. It also requires us to tell you how we collect, share, and protect your personal information. The firm provides customers with the privacy policy on an annual basis, and at any time, in advance, if the privacy policy is expected to change.

The firm collects personal information about customers from the following sources:

- Information provided to us complete their plan or investment recommendation;
- Information provided via engagement agreements and other documents completed in connection with the opening and maintenance of an account;
- Information customers provide verbally; and
- Information received from service providers, such as custodians, about account transactions.

Types of Nonpublic Personal Information We Collect:

We collect nonpublic personal information about you that is either provided by you or obtained by us with your authorization. This can include but is not limited to: your Social Security Number, Date of Birth, Banking Information, Financial Account Numbers and/or Balances, Sources of Income, and Credit Card Numbers or Information. When you are no longer our customer, OHIS will continue to adhere to this Privacy Policy with your information.

The firm does not disclose non-public personal information about our customers to anyone, except in the following circumstances:

- When required to provide services our customers have requested
- When our customers have specifically authorized us to do so;
- When required during the course of a firm assessment (i.e., independent audit); or
- When permitted or required by law (i.e., periodic regulatory examination).
- For marketing by OHIS – to offer OHIS's products and services to clients;
- For joint marketing with other financial companies;
- For affiliates' everyday business purposes – information about client transactions and experience; or
- For non-affiliates to market to clients (only where allowed).

If you are a new customer we may begin sharing your information on the day you sign our agreement. If a client decides to close his or her account(s) or becomes an inactive customer, OHIS will adhere to the privacy policies and practices as described in this Privacy Policy. However, you can contact us at any time to limit our sharing.

Federal law allows you the right to limit the sharing of your NPI by "opting-out" of the following: sharing for non-affiliates' everyday business purposes – information about your creditworthiness; or sharing with affiliates or non-affiliates who use your information to market to you. State laws and individual companies may give you additional rights to limit sharing. Please notify us immediately if you choose to

opt out of these types of sharing.

OHIS restricts access to clients' personal and account information to those employees who need to know that information to provide products or services to its clients. OHIS maintains physical, electronic, and procedural safeguards to guard clients' non-public personal information.

In addition to OHIS's listed access persons, any IT persons or other technical consultants employed at the firm may also have access to non-public client information at any time. An on-site or off-site server that stores client information, third-party software that generates statements or performance reports, or third-party client portals designed to store client files all hold the potential for a breach of non-public client information.

To mitigate a possible breach of the private information, OHIS uses encryption software on all computers and evaluates any third-party providers, employees, and consultants with regard to their security protocols, privacy policies, and/or security and privacy training.