Privacy Policy

THE BROUGHTON INVESTMENT GROUP, INC. ("BIG") is a registered investment adviser. This document describes its privacy policies and procedures.

At a minimum, BIG will annually review and update these policies and procedures. BIG may conduct interim reviews in response to significant compliance events, changes in business arrangements, and regulatory developments.

BIG will maintain copies of all policies and procedures that are in effect or were in effect at any time during the last five years.

BIG's goal is to maintain the highest ethical and professional standards for employee conduct. This manual is only a guide and cannot cover employee and/or supervised person's conduct in every conceivable situation that may arise in the course of BIG's business. In the event of any uncertainty, an officer, director, affiliate, supervised person, or employee of the firm should ask a supervisor or the Chief Compliance Officer ("CCO") for advice on compliance with this manual and/or the applicable securities laws.

Electronic Communications

If electronic communications are used to comply with the annual delivery of BIG's ADV filing and/or Privacy Policy requirement, BIG will either attach these documents to an email communication or will inform its clients in an email with an embedded hyperlink to BIG's website, where the most current ADV filing, and Privacy Policy can be viewed. Prior to distributing materials in this manner, BIG will obtain prior authorization from its clients. BIG will use an electronic authorization form or will obtain electronic authorization via its investment advisory contract. BIG will retain this authorization as part of its required books and records.

Information Collected and Shared

BIG's privacy policy statement is given to clients at the initial signing of the client contract and mailed or emailed with client consent once annually, if the policy is updated. The CCO will document the date the privacy policy was delivered to each client for each year if an annual delivery is required. BIG may collect information about clients from the following sources:

- Information received from client on applications, via other forms, or during conversations;
- Information about client's transactions with BIG or others; and
- Information provided by a consumer reporting agency.

Below are the reasons for which BIG may share a client's personal information:

- With specific third parties as requested by the client (see Sample 11);
- 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 marketing by BIG – to offer BIG'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 a client decides to close his or her account(s) or becomes an inactive customer, BIG will adhere to the privacy policies and practices as described in this manual, as updated.

Storing Client Information

BIG uses various methods to store and archive client files and other information. Third party services or contractors used have been made aware of the importance BIG places on both firm and client information security. BIG also 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. In addition to electronic protection, procedural safeguards, and personnel measures, BIG has implemented reasonable physical security measures at its home office location.

In addition to BIG'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, BIG uses encryption software on all computers and carefully evaluates any third-party providers, employees, and consultants with regard to their security protocols, privacy policies, and/or security and privacy training.

Additionally, any records containing non-public information (NPI), will be stored securely in accordance with the provisions in the Privacy Policy section of BIG's Code of Ethics.