FPL CAPITAL MANAGEMENT PRIVACY POLICY

FPL Capital Management views protecting private information regarding its clients and potential clients as a top priority. Pursuant to the requirements of the Gramm-Leach-Bliley Act (the "GLBA") and guidelines established by the Securities Exchange Commission regarding the Privacy of Consumer Financial Information (FTC Rule 314), the Company has instituted the following policies and procedures in an effort to ensure that such nonpublic private information is kept private and secure. This policy also outlines what the Company and its associated persons are allowed to use the confidential personal information collected in connection with its advisory activities.

FTC Rule 314 defines "consumer" as an individual who obtains or has obtained a financial product or service from a financial institution primarily for personal, family, or household purposes, or for that individual's legal representative. Generally, an individual is a consumer if he or she provides nonpublic information to the Company in connection with obtaining or seeking to obtain investment advisory services, whether or not the Company provides such services to the individual or establishes a continuing relationship with the individual.

"Customer" is defined as a consumer who has an on-going relationship with the institution. Generally, a customer is a consumer who has an investment advisory contract with the Company (whether written or oral) and/or the Company regularly effects or engages in securities transactions with or for a consumer even though the Company does not hold assets of the consumer.

While these terms have specific definitions, for the purposes of the Company's policies, both consumers and customers will be collectively referred to as "clients" (or "potential clients" or "former clients" where applicable).

This policy serves as formal documentation of the Company's ongoing commitment to the privacy of its clients. All Associated Persons will be expected to read, understand, and abide by this policy, as well as to follow all related procedures to uphold the standards of privacy and security set forth by the Company. This Policy, and the related procedures contained herein, is designed to comply with applicable privacy laws, including the GLBA, and to protect nonpublic personal information of the Company's clients.

The Company is aware that the SEC has proposed amendments to FTC Rule 314 that set forth more specific requirements for safeguarding personal information against unauthorized disclosure and for responding to information security breaches. When these new amendments are adopted, or in the event that new privacy-related laws or regulations affecting the information practices of the Company are adopted by federal or state regulators, this Privacy Policy will be revised as necessary and any changes will be disseminated and explained to all personnel.

A. Scope of Policy

This Privacy Policy covers the practices of the Company and applies to all nonpublic personally identifiable information, including information contained in consumer reports, of our current and former clients.

B. Overview of the Guidelines for Protecting Client Information

In FTC Rule 314, the Securities and Exchange Commission (the "SEC") published guidelines, pursuant to section 501(b) of the GLBA, that address the steps a financial institution should take in order to protect client information. The overall security standards that must be upheld are:

1. Ensuring the security and confidentiality of client records and information;
2. Protecting against any anticipated threats or hazards to the security or integrity of client records and information; and
3. Protecting against unauthorized access to or use of client records or information that could result in substantial harm or inconvenience to any client.

C. Responsibility

1. Each Associated Person has a duty to protect the nonpublic personal information of clients collected by the Company.
2. Each Associated Person has a duty to ensure that nonpublic personal information of the Company's clients is shared only with Associated

Persons and others in a way that is consistent with the Company's Privacy Notice and the procedures contained in this Policy.

3. Each Associated Person has a duty to ensure that access to nonpublic personal information of the Company's clients is limited as provided in the Privacy Notice and this Policy.

4. No Associated Person is authorized to sell, on behalf of the Company or otherwise, nonpublic information of the Company's clients.

5. Associated Persons with questions concerning the collection and sharing of, or access to, nonpublic personal information of the Company's clients must look to the Company's CCO for guidance.

6. Violations of these policies and procedures will be addressed in a manner consistent with other Company disciplinary guidelines.

D. Information Practices

The Company limits the use, collection, and retention of client or potential client information to what we believe is necessary or useful to conduct our business or to offer quality products, services, and other opportunities that may be of interest to our clients or potential clients.

The Company collects nonpublic personal information about clients and/or potential clients from various sources. These sources and examples of types of information collected include:

1. Product and service applications or other forms, such as client surveys, agreements, etc., which typically request name, address, telephone number, social security number or taxpayer ID number, date of birth, employment status, annual income, and net worth;

2. Information about transactions with the Company and account custodian(s), such as account balance, types of transactions, parties to the transactions, and investment history.

3. Information received from consumer reporting agencies, such as credit reports.

E. **Disclosure of Information to Nonaffiliated Third Parties – "Do Not Share" Policy**

The Company has a "do not share" policy. We do not disclose nonpublic personal information to nonaffiliated third parties, except under one of the GLBA privacy exceptions, as described below. Since the Company currently operates under a "do not share" policy, it does not need to provide the right for its clients to opt out of sharing with nonaffiliated third parties, as long as such entities are exempted as described below. If our information sharing practices change in the future, we will implement opt out policies and procedures, and we will make appropriate disclosures to our clients.

F. **Types of Permitted Disclosures – The Exceptions**

In certain circumstances, FTC Rule 314 permits the Company to share nonpublic personal information about its clients with nonaffiliated third parties without providing an opportunity for those individuals to opt out. These circumstances include sharing information with a non-affiliate (1) as necessary to effect, administer, or enforce a transaction that a client requests or authorizes; (2) in connection with processing or servicing a financial product or a service a client authorizes; and (3) in connection with maintaining or servicing a client account with the Company.

1. **Service Providers**. From time to time, the Company may have relationships with nonaffiliated third parties (such as attorneys, auditors, accountants, brokers, custodians, and other consultants), who, in the ordinary course of providing their services to us, may require access to information containing nonpublic information. These third-party service providers are necessary for us to provide our investment advisory services. When we are not comfortable that service providers (e.g., attorneys, auditors, and other financial institutions) are already bound by duties of confidentiality, we require assurances from those service providers that they will maintain the confidentiality of nonpublic information they obtain from or through us. In addition, we select and retain service providers that we believe are capable of maintaining appropriate safeguards for nonpublic information, and we will require contractual agreements from our service providers that they will implement and maintain such safeguards.

2. **Processing and Servicing Transactions.** The Company may also share information when it is necessary to effect, administer, or enforce a transaction requested or authorized by clients. In this context, "necessary to effect, administer, or enforce a transaction": includes what is required or is a usual, appropriate, or acceptable method:
   - **a.** To carry out the transaction or the product or service business of which the transaction is a part, and record, service, or maintain the clients account in the ordinary course of providing the financial service or financial product;
   - **b.** To administer or service benefits or claims relating to the transaction or the product or service of which it is a part;
   - **c.** To provide a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product to the client or the client's agent or broker.

3. **Sharing as Permitted or Required by Law.** The Company may disclose information to nonaffiliated third parties as required or allowed by law. For example, this may include disclosures in connection with a subpoena or similar legal process, a fraud investigation, recording of deeds of trust and mortgages in public records, an audit, or examination, or the sale of an account to another financial institution.

By understanding how the Company shares data with its clients, their agents, service providers, parties related to transactions in the ordinary course of business, or joint marketers, the Company endeavors to ensure that client data is shared only within the exceptions noted above.

G. Privacy Notice

The Company has developed a Privacy Notice, as required under FTC Rule 314, to be delivered to clients initially and to current clients on an annual basis. The notice discloses the Company's information collection and sharing practices and other required information. The notice will be revised as necessary any time information practices change.

H. Privacy Notice Delivery

1. **Initial Privacy Notice -** As regulations require, all new clients receive an initial Privacy Notice at the time the client relationship is established (i.e., upon execution of the agreement for services).
2. **Annual Privacy Notice -** The GLBA regulations require that disclosure of the Privacy Policy be provided to existing clients on an annual basis. The Company will deliver its annual Privacy Notice in conjunction with the annual offer of its ADV Part 2 or disclosure document meeting the requirements of Rule 204-3.

J. Revised Privacy Notice

FTC Rule 314 requires that the Company amend its Privacy Policy and promptly distribute a revised disclosure to clients, if there is a change in the Company's collection, sharing, or security practices.

K. Joint Relationships

If two or more individuals jointly obtain a financial product or service from the Company, the Company may satisfy the initial, annual, and revised notice requirements by providing one notice to those individuals jointly.

L. Information Security Program

Safeguarding of Client Records and Information Under FTC Rule 682

The Company has implemented internal controls and procedures designed to maintain accurate records concerning client personal information. The Company's clients have the right to contact the Company if they believe that Company records contain inaccurate, incomplete, or stale information about them. The Company will respond in a timely manner to requests to correct information.

Under FTC Rule 682, to protect client and personal information, including consumer report information, the Company maintains the following security measures and safeguards for the storage of, access to, and disposal of client personal information, including consumer report information, obtained and/or maintained in hard copy and/or electronically, as well as access and protections of its computer and information systems:

1. limiting access to nonpublic and consumer report information to those Associated Persons who require the information in order to help us provide services;

2. locking rooms and file cabinets where paper records are stored;

3. protecting storage areas against destruction or potential damage from environmental hazards;

4. storing electronic nonpublic and consumer report information on a secure server that is accessible only with a password;

5. maintaining secure backup media;

6. storing archived data off-line and/or in a physically-secure area;

7. supervising the disposal of records containing nonpublic and consumer report information;

8. shredding nonpublic and consumer report information recorded on paper and storing such material in a secure area until it is collected by a recycling service;

9. erasing all data when disposing of computers, diskettes, magnetic tapes, hard drives, or any other electronic media containing nonpublic and consumer report information;

10. disposing of outdated nonpublic and consumer report information promptly;

11. using anti-virus software that updates automatically; and

12. maintaining up-to-date firewalls.

M. Information Security Program for Massachusetts Clients

Safeguarding of Client Records and Information

Massachusetts legislators recently issued revised regulations establishing detailed standards for businesses that own, license, store or maintain personal information about its residents. Federally registered investment advisers are among those businesses affected by these new guidelines. Since the Company has at least one client residing in Massachusetts or employs at least one person residing in Massachsetts, the new regulations apply to the Company.

This regulation, 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth, applies to "personal information" of any person residing in the Commonwealth of Massachusetts. "Personal Information" is defined as the combination of the Massachusetts resident’s name[1] in combination with any one or more of the following, such resident’s: (a) social security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number. Under this regulation, "personal information" does not include information that is lawfully obtained from publicly available sources.

Under these revised regulations, Investment Advisers must adhere to minimum standards applicable to protecting personal information and maintaining compliant computer systems security requirements.

These regulations become effective **March 1, 2010**.

1. Protecting Personal Information

Under 201 CMR 17.00, Investment Advisers must develop, implement, maintain and monitor a *comprehensive information security program that is written in one or more readily accessible parts*" (hereinafter "WISP") applicable to all records containing personal information on any Massachusetts resident. A WISP must include administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the Investment Adviser; (b) the amount of resources available to the Investment Adviser; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in the WISP must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the Investment Adviser may be regulated.

Without limiting the generality of the foregoing, the WISP shall include, but shall not be limited to:

a. Designating one or more employees to maintain the WISP;

b. Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:

- **i.** ongoing employee (including temporary and contract employee) training;
- **ii.** employee compliance with policies and procedures; and
- **iii.** means for detecting and preventing security system failures.

c. Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.

d. Imposing disciplinary measures for violations of the WISP rules.

e. Preventing terminated employees from accessing records containing personal information.

f. Oversee service providers, by:

- **i.** Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and

ii. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that any contract a person has entered into with a third party service provider prior to March 1, 2012, shall be deemed to be in compliance herewith, notwithstanding the absence in any such contract of a requirement that the service provider maintain such protective security measures, so long as the contract was entered into before March 1, 2010.

g. Reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers.

h. Regular monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.

i. Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

j. Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

N. Computer Systems Security Requirements in Massachusetts

In addition to the safeguards delineated above, Massachusetts regulations mandate guidelines for any person that electronically stores or transmits the personal information of a Massachusetts resident. In conforming to Massachusetts' computer and wireless system security requirements, the WISP must establish and maintain a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, has the following elements:

1. Secure user authentication protocols including:

- **a.** control of user IDs and other identifiers;
- **b.** a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
- **c.** control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
- **d.** restricting access to active users and active user accounts only; and
- **e.** blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

2. Secure access control measures that:

- **a.** restrict access to records and files containing personal information to those who need such information to perform their job duties; and
- **b.** assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

3. Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

4. Reasonable monitoring of systems, for unauthorized use of or access to personal information;

5. Encryption of all personal information stored on laptops or other portable devices;

6. For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.

7. Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

8. Education and training of employees on the proper use of the computer security system and the importance of personal information security.

The CCO will work with the Company's in-house technology department or outside technology vendor to develop and implement a compliant WISP.

The Commonwealth of Massachusetts has published information to assist small businesses comply with the new regulations. This information is updated periodically and may be located at:

http://www.mass.gov/?pageID=ocatopic&L=3&L0=Home&L1=Business&L2=Identity+Theft&sid=Eoca

Some of the documents published by The Commonwealth of Massachusetts include:

- **Frequently Asked Questions Regarding 201 CMR 17.0;**
- **201 CMR 17.00 Compliance Checklist; and**
- **Small Business Guide For Formulating A Comprehensive Written Information Security Program**