INFORMATION SECURITY PROGRAM

I. Introduction

In the course of client relationships, Wolfstich Capital, LLC ("Wolfstich Capital") gathers and maintains personal, non-public information regarding its clients' financial circumstances and investment objectives. Sources of such information may include, without limitation, information contained on account applications, written questionnaires, interviews/conversations, information forms and other client interactions; information about transactions with Wolfstich Capital, any affiliates of Wolfstich Capital, or others; information exchanged with qualified account custodians, and information Wolfstich Capital obtains or receives from a consumer reporting agency.

Wolfstich Capital is committed to maintaining the privacy, security and confidentiality of this client information. Our objective, in the development and implementation of this comprehensive written information security program ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of personal information of residents of the Commonwealth of Massachusetts, and to comply with obligations under 201 CMR 17.00. This obligation applies to all persons that own, license, store or maintain personal information about a resident of the Commonwealth. The WISP sets forth our procedures for meeting this objective, and also establishes policies regarding employee training and anticipated actions in the event of a breach of security.

Wolfstich Capital has designated Ted Wolfstich as the Information Security Program Officer ("ISPO"). He bears the primary responsibility for: developing and maintaining the WISP, including assessment of risk, both internal and external, related to information security; for training employees as needed; for annual evaluation of the effectiveness of the WISP, and for handling any breaches of security with respect to client information that may occur.

II. Definitions

Breach of Security – This term means the unauthorized use or acquisition of unencrypted data, or encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates substantial risk of identity theft or fraud against a resident of the commonwealth.

Electronic – This term is related to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encrypted – This term refers to the transformation of data through the use of algorithmic process, or other method, into a form in which meaning cannot be assigned without the use of confidential process or key.

Personal Information – This refers to a client's first and last name or first initial and last name in combination with any one or more of the following (1) Social Security number; (2) driver's license number or state issued I.D. card; (3) financial account number, debit or credit card number. "Personal information" does not include information lawfully obtained from publicly available sources.

Owns or licenses – This refers to someone who receives, stores, maintains, processes or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person – A natural person, corporation, association, partnership or other legal entity.

Record – This refers to any material written, drawn, spoken, or electromagnetic information or images recorded or preserved, regardless of physical form or characteristics.

Service Provider – Any person that receives, stores, maintains, processes or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation.

III. Risk Assessment and Ongoing Monitoring

No less than annually, the ISPO shall perform an assessment of risks to the security of private client and employee information. See Exhibit A for a form of risk assessment to be utilized, subject to change over time.

The ISPO is responsible for determining the manner, method and frequency of monitoring and testing the WISP. Records of such monitoring and testing shall be maintained by Wolfstich Capital, and review of these records should be included in the CCO's Annual Review, conducted pursuant to Rule 206(4)-7.

IV. Elements of Protection of Personal Information

A. Administrative Elements of Protection

a) Upon Wolfstich Capital's adoption of this WISP and annually thereafter, all ongoing employees (including temporary and contract employee) are required to certify in writing his or her understanding and continuing acceptance of, as well as agreement to abide by, the guidelines and polices set forth herein. Additionally, any change or modification to the WISP will be distributed to all employee and they will be required to certify in writing their receipt, understanding and acceptance of the change(s).

b) Wolfstich Capital shall limit the amount of personal information collected in order to do business and shall retain the information only as necessary to provide services requested by Client and to comply with regulatory record retention and other requirements. All client information is to be maintained in Wolfstich Capital's client files which, when not in use are kept in secured filing cabinets accessible only to authorized and appropriate personnel. Information stored on appropriate electronic media shall be similarly protected. Private information received from potential clients may be filed in temporary files, but shall be subject to the same restrictions and limitations as other client files.

c) Adviser personnel are prohibited from sharing or disclosing nonpublic information regarding any client or potential client of Wolfstich Capital, except (i) as necessary to service client accounts including, without limitation, the settlement, billing, processing, clearing, or transferring of client transactions; (ii) as otherwise directed by a client, or (iii) as necessary to comply with regulatory requirements.

d) Adviser personnel may not remove client files or information from Wolfstich Capital's premises unless (i) it is necessary to service client accounts; and (ii) prior approval is obtained from the Chief Compliance Officer.

e) Prior to providing a third-party service provider with access to personal information, Wolfstich Capital will obtain from the third-party service provider a written certification that the service provider has a written, comprehensive information security program that is in compliance with 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth.

f) Wolfstich Capital will provide clients with a privacy notice (the "Privacy Notice") when the client engages Wolfstich Capital for advisory or other services. The Privacy Notice describes the types of nonpublic client information Wolfstich Capital collects, the information Wolfstich Capital shares with third parties or with affiliates, the kinds of third parties with which Wolfstich Capital shares information, the policies and practices Wolfstich Capital has in place to protect the confidentiality and security of nonpublic client information; the procedures Wolfstich Capital has in place to permit clients or potential clients to opt out of information sharing arrangements with third parties (inapplicable to Wolfstich Capital so long as Wolfstich Capital only shares information with third parties for purposes of servicing client accounts), and Wolfstich Capital's disposal policy.

g) Wolfstich Capital shall deliver an updated Privacy Notice to all of its clients annually, even if the policy has not changed since the previous year. "Delivery" may, to the extent allowed by law and to the extent consistent with any written agreement with the client, mean notification of the availability of the notice on a website. A copy of a form of the Notice is attached hereto as Exhibit B.

h) Wolfstich Capital shall document any incident involving breach of security and actions taken to make necessary changes to the WISP relating to protection of personal information.

i) All ongoing employees (including temporary and contract employee) are required to certify in writing his or her understanding and continuing acceptance of, as well as agreement to abide by, the guidelines and polices set forth herein. [See Schedule C.] Additionally, any change or modification to the WISP will be distributed to all employee and they will be required to certify in writing their receipt, understanding and acceptance of the change(s). [See Schedule D.]

j) Upon termination of an employee all electronic passwords for computers shall be deactivated and all keys to office shall be immediately retrieved by the ISPO. The terminated employee shall be required to represent that he or she has returned or securely destroyed any private information they might have had in their possession. Third party vendors, such as qualified custodians, shall be immediately notified in writing of the employee's departure.

B. Technical Elements of Protection

a) All computers are set up so they 'lock' when not in use, requiring a password to gain access. After 3 unsuccessful attempts to login the computer will lock up until the incident can be resolved by the ISPO or his/her designee.

b) Employees working remotely must be authorized to do so, and are required to utilize approved secure connections, as established by the ISPO.

c) The IPSO or CCO assigns all user ID's (there are no group or shared ID) and all passwords must have unique identifiers. Upon termination of an employee all electronic passwords for computers shall be immediately deactivated.

d) Wolfstich Capital encrypts all personal information transmitted across public internet or data transmitted wirelessly.

e) Wolfstich Capital prefers that all laptops do not contain any personal information on its hard drive. However, circumstances may require this information on the hard drive of a laptop. In this case, all personal information is required to be encrypted.

f) All personal information files are protected by a firewall and operating system security patches designed to maintain the integrity of the personal information. Wolfstich Capital also uses Kaspersky Anti Virus 2010, a system security agent software program that has malware protection patch and virus protection and receives the most current security updates on a regular basis.

C. Physical Elements of Protection

a) Wolfstich Capital restricts physical and electronic access to records and files containing personal information to only those that need the information to perform assigned duties.
b) All client files are secured at the end of each business day in locked cabinets, desks or rooms to which outsiders, such as cleaning crews and building security, do not have access. Exterior doors are always locked by the last person to leave for the day.
c) Traffic flow in the office is restricted, and no individuals, other than employees, are allowed free access to areas where client information is held.
d) Preferably, laptops and other portable devices will not have any private information stored directly on them. In the event it is necessary to have such information stored directly on a portable device, such devices are required to be encrypted.
e) Wolfstich Capital has undertaken to protect client information in the course of its disposal as well. Employees either utilize personal desk-side shredders or place material to be shredded in a secure retention container until it is shredded. Electronic media will be "scrubbed" prior to disposal. The ISPO is responsible for determining the methods to be used to ensure no usable private information is left on any electronic device at the time of its disposal.
f) Back-up media, such as tapes, flash drives, external hard drives, etc. are required to be encrypted as they are produced, effective March 1, 2010.

V. Employee Training

Upon adoption of this program, upon employment of future employees and at least annually, the ISPO or his designee shall provide employee education and training regarding the relevant aspects of this WISP. A log or other records of such training will be maintained, and employees will be required to acknowledge in writing their understanding of the training content, and their agreement to abide by the WISP. See Exhibit C. In addition, any changes to the WISP will be communicated to all relevant employees (it may not be necessary to convey certain elements of change to some employees – for example, most employees do not need to understand the highly technical aspects of intrusion protection), and such employees will be required to certify in writing their understanding of the change(s). See Exhibit D.

VI. Breaches of Security

All employees of Wolfstich Capital are required to promptly report any breach, suspected breach, or perceived potential for breach of this WISP to the ISPO or CCO. Upon learning of a breach, the ISPO is responsible for: evaluating the severity of the breach; determining actions to be taken to resolve the breach (can the compromised information be retrieved?); determining who needs to be informed of the breach (higher management, regulatory bodies, etc) and communicating information as appropriate; documenting the breach (how it occurred and how it was addressed), and determining actions to be

taken as a result of the breach (change in procedures, retraining of personnel, other disciplinary actions).

Associated persons who violate any provision of the WISP may be subject to sanctions, which may include, among other things, education or formal censure; a letter of admonition; fines, suspension, reassignment, demotion or termination of employment; or other significant remedial action.

All disciplinary responses to violations of the WISP shall be administered by the CCO in cooperation with the ISPO, subject to approval, as applicable, by the President, Chief Executive Officer or Board of Directors of the Company. Determinations regarding appropriate disciplinary responses will be administered on a case-by-case basis.

EXHIBIT A – RISK ASSESSMENT

Internal Risks

Potential Risk	Mitigating Action
Employee error may lead to loss of private information.	Adequate training, supervision and cross checks are in place.
Disgruntled former employee could attempt to steal information.	(1) Procedures for immediate retrieval of security cards, keys, renaming passwords, etc are in place. (2) Access to personal information shall be restricted to active users and active user accounts only. (3) Continue to monitor after employee's departure. (4) Notify third parties as necessary to ensure security (i.e., account custodian).
Unauthorized user could gain access to information.	Current employee's user ID's and passwords must be changed periodically.
Visitors to the office could see/steal personal information.	Traffic flow in the office is limited, and files containing private information are not left in public areas.

External Risks

Potential Risk	Mitigating Action
Danger of electronic intrusion into the server system from outsiders.	Firewalls and other protections are installed and kept current.
Disgruntled former employee could attempt to steal information electronically.	(1) Procedures for immediate retrieval of security cards, keys, renaming passwords, etc are in place. (2) Access to personal information shall be restricted to active users and active user accounts only. (3) Continue to monitor after employee's departure. (4) Notify third parties as necessary to ensure security (i.e., account custodian).
Unauthorized user could gain access to information.	Current employee's user ID's and passwords must be changed periodically according to established protocol to protect integrity. Master list of usernames, passwords, etc is secured with extremely limited access, and only by authorized personnel.

EXHIBIT B

(See Next Page)

Please copy the Notice for distribution to clients

NOTICE OF INFORMATION SECURITY PROGRAM
(PRIVACY NOTICE) of

Wolfstich Capital, LLC

This is for your information only. No action is required on your part.

At Wolfstich Capital, LLC, protecting your privacy is very important to us. We want you to understand what information we collect and how we use it. We collect and use "nonpublic private information" in order to provide our clients with a broad range of financial services as effectively and conveniently as possible. We treat nonpublic personal information in accordance with our privacy policy.

"Nonpublic personal information" is nonpublic information about you that we obtain in connection with providing a financial service or product to you.

What Information Do We Collect?

In order to fulfill our obligations to you, we need certain information. Generally, this includes your name, address, social security number, date of birth, account numbers, and information about your income. We may also have access to other sensitive information, such as credit scores, income tax information and so forth.

Where Do We Get This Information?

We may collect nonpublic personal information about you from a variety sources, such as:

- Information we receive from you on applications or other forms;
- Information about your transactions with us, our affiliates or others, such as the custodian(s) of your account(s); and
- Information we receive from non-affiliated third parties, including consumer reporting agencies.

What Information Do We Disclose and To Whom Do We Disclose It?

We do not disclose any nonpublic information about you without your express consent, except as permitted by law and as needed to provide the services you have requested. This applies to current as well as former clients. We restrict access to your nonpublic personal information to those who need to know that information in order to provide products or services to you.

Our "affiliates" are companies with which we share common ownership. We do not currently have any affiliated companies.

Our Security Procedures

We maintain physical, electronic and procedural safeguards to protect your nonpublic personal information. This includes measures to protect your information in the course of its disposal.

EXHIBIT C

INITIAL CERTIFICATION OF COMPLIANCE WITH THE WRITTEN INFORMATION SECURITY PROGRAM OF Wolfstich Capital, LLC

I hereby certify that I have reviewed and understand the Company's Written Information Security Program ("WISP"). I agree to abide by all provisions of the WISP, including my obligation to report any breach, suspected breach, or perceived potential for breach of the WISP.

_____

Signature

_____

Print Name

Dated: _____

EXHIBIT D

ACKNOWLEDGEMENT OF AMENDMENT TO THE WRITTEN INFORMATION SECURITY PROGRAM OF Wolfstich Capital, LLC

I hereby certify that I have received information, training or both regarding amendments to Wolfstich Capital's Written Information Security Program ("WISP"), and that I understand the amendments as explained. I agree to abide by all provisions of the WISP, including my obligation to report any breach, suspected breach, or perceived potential for breach of the WISP.

_____

Signature

_____

Print Name

Dated: _____