NEXADVISORS

NexAdvisors, LLC
Policy Regarding Privacy

Purpose and Scope

The purpose of this policy regarding privacy (this "Policy") is to ensure that the NexAdvisors, LLC ("the Company") policies and procedures regarding the use and handling of Personal Information (as defined below) comply with all requirements of applicable law.

General Policy

The Company is committed to protecting the non-public personal information that it receives from time to time with respect to current and prospective individual Clients in connection with the provision of its investment advisory or other services. Non-public personal information, which is generally obtained from applications, forms and other documentation, as well as from specific transactions between the Client and the Company, may include, among other things, the Client's name, address, social security number or tax identification number, bank account information, financial information, investment objectives, actual investments made and other information with respect to the investment advisory or other services provided to or on behalf of the Client by the Company ("Personal Information"). To that end, the Company has adopted this Policy to:

(i) ensure the security and confidentiality of Personal Information;

(ii) protect against anticipated threats or hazards to the security or integrity of Client records and other information; and

(iii) protect against unauthorized access to or use of Personal Information that could result in substantial harm or inconvenience to Clients.

Federal Requirements

Protecting the confidentiality and security of Personal Information is a top priority for the Company. In general, the Company shall not use or disclose Personal Information for any purpose other than in connection with the servicing of a Client's account and as may be required by applicable law. The Company's employees and other associated persons (including service providers) shall be prohibited from disclosing Personal Information to third-parties unless required by operation of law, and, in such event, only in a manner permitted by Regulation S-P or other applicable law (each, a "Permitted Disclosure" and collectively, "Permitted Disclosures"). All such employees and other associated persons must at all times adhere to this Policy, and the Chief Compliance Officer shall be responsible for enforcing this Policy.

All Personal Information shall be governed by this Policy, whether or not such information is derived from applications, agreements, forms or other documentation, or in connection with specific transactions between the Company and its Clients, and including any such information that may be created, sent, received and/or stored by the Company. In that connection, as noted above, all of the Company's employees and other associated persons (including service providers) shall at all times endeavor to:

(i) ensure the security and confidentiality of Personal Information;

(ii) protect against anticipated threats or hazards to the security or integrity of Client records and other information; and

(iii) protect against unauthorized access to, or use of, Personal Information that could result in substantial harm or inconvenience to Clients.

The Company has physical, procedural and electronic safeguards that facilitate the Company's compliance with applicable law pertaining to safeguarding the security, confidentiality and integrity of Personal Information. Personal Information shall be collected by the Company under the supervision of the Chief Compliance Officer, and stored in one or more databases in accordance with the Company's Policy Regarding Recordkeeping. Such database(s) shall only be accessible by authorized employees and other associated persons of the Company and at all times the information stored therein shall remain subject to this Policy.

Notice and Disclosure

Content of Notice

Regulation S-P requires the Company to provide Clients with a "clear and conspicuous" notice (a "Privacy Notice") that accurately reflects its privacy policies and practices. The Privacy Notice shall generally describe the following:

(i) the Company's policies and practices to protect Personal Information;

(ii) categories of Personal Information that are collected;

(iii) categories of Personal Information that are disclosed;

(iv) if applicable, categories of Personal Information disclosed about former Clients and categories of affiliates' and non-affiliated third-parties' that may receive Personal Information; and

(v) if applicable, conditions under which Personal Information may be disclosed to affiliates and non-affiliated third-parties.

Based on the foregoing, the Company shall provide an initial Privacy Notice to each new Client no later than when the relationship is established with such Client, and an annual Privacy Notice to each existing Client within 90 days following the end of the Company's fiscal year.

Delivery Requirements

In accordance with applicable law, a description of this Policy shall be included in all of the Company's new account documentation and shall be delivered to all existing Clients annually, generally within 90 days following the end of the Company's fiscal year. The Company shall also promptly deliver to existing Clients a modified or revised Privacy Notice prior to:

(i) disclosing a new category of Personal Information;

(ii) disclosing Personal Information to a new category of non-affiliated third-parties; or

(iii) disclosing Personal Information about a former Clients to a non-affiliated third-party.

A revised Privacy Notice is not required to be delivered if the Company discloses Personal Information to a new non-affiliated third-party if such third-party was adequately described in a prior notice.

Privacy Notices may be provided to Clients in conjunction with other information that the Company desires to use or disseminate, so long as the Privacy Notice is clear and conspicuous. Privacy Notices shall be delivered in such a manner that each Client can reasonably be expected to receive actual notice in writing, or, if the Client agrees, electronically.

A copy of the Company's current general Privacy Notice is attached as **Appendix D** hereto.

Disclosure to Affiliates

The Company and its employees may share Personal Information of any employee or affiliate with any other affiliate Company provided such sharing is in the course of offering products or services to such affiliates and the affiliate is notified of the confidential nature of the Personal Information.

Disclosures to Non-affiliated Third-Parties

The Company and its employees and other associated persons generally may only disclose or otherwise give access to Personal Information to a non-affiliated third-party if such third-party has signed a non-disclosure agreement approved by a member of the Legal and Compliance Department, and only in the following situations:

(i) to non-affiliated third-parties (including disclosure to attorneys, accountants, auditors and other service providers) in connection with the administration, processing and servicing of Client transactions;

(ii) to non-affiliated third-parties at the direction or otherwise with the consent of the Client;

(iii) to persons acting in a fiduciary or representative capacity on behalf of the Client;

(iv) to a consumer reporting agency, subject to prior written approval by a member of the Legal and Compliance Department; and

(v) to comply with applicable law or any civil, criminal or regulatory audit, investigation, examination, compliance request or other proceeding, or any subpoena, summons or other order issued by any court or other governmental authority or otherwise pursuant to any judicial process, in each case subject to prior written approval by a member of the Legal and Compliance Department.

Prohibited Uses

Except in connection with Permitted Disclosures, neither the Company nor any of its employees or associated persons shall:

(i) copy, upload, or distribute Personal Information from the Company's databases or other external sources that originate from the Company;

(ii) distribute Personal Information to anyone other than authorized personnel; or

(iii) store, print, download, record or distribute any file or other document containing Personal Information.

Privacy Safeguards

Restricted Access

All Personal Information, as well as all related files and records of the Company and its employees and other associated persons, shall be maintained on a network or system with appropriate access controls (a "Confidential System") to prevent unauthorized access to the Company's premises, including controls to authenticate and grant access only to authorized individuals and entities. Employees and other associated persons of the Company may not access or use Personal Information, unless there is a legitimate business need for such access or use.

Monitoring and Prevention

The Company shall develop monitoring systems and other procedures to detect actual and attempted attacks on, or other intrusions into, facilities and other locations, including electronic locations, where Personal Information is held. Personal Information will be held in secure media. To preserve the integrity and security of Personal Information in the event of computer or other technological failure, these measures will include disaster recovery programs.

Cyber-Security Practices for All Employees

The Company has implemented the following procedures to protect proprietary and Nonpublic Personal Information stored on electronic systems:

- Employees must never share their passwords or store passwords in a place that is accessible to others;
- Employees must lock their computers when they leave their work station unattended for any extended period of time;
- Any theft or loss of electronic storage media must immediately be reported to the Director of IT;
- Any inquiries or requests for representations about the Company's cyber-security controls from third parties, such as Clients, vendors, or government officials, must be forwarded to the CCO;
- Any requests from third parties for independent access to the Company's networks or proprietary data must be forwarded to the Director of IT; and
- The Director of IT or designee is responsible for setting Employee access permissions on the Company's computer network.

On at least an annual basis the Director of IT conducts a cyber-security risk assessment. The Director of IT provides the CCO with a summary of any moderate or high risk vulnerabilities that are identified, as well as a plan to remediate such risks.

Additionally, on an annual basis a member of the Company's information technology team shall:

- Inventory the Company's computers, system hardware, and other IT devices such as smart phones;

- Monitor for unauthorized devices accessing the Company's networks;
- Inventory its software applications, and ensured that software patches are being applied in a timely manner;
- Evaluate likely types of attack, including through penetration testing and vulnerability scans, where appropriate;
- Implement appropriate protections, such as anti-malware software, firewalls and data loss prevention software;
- Test the Company's ability to restore critical data and software in a timely manner;
- Implement standardized secure configurations for user hardware, software, operating systems, and network infrastructure;
- Periodically test to confirm that hardware, software, operating systems and network infrastructure continue to operate according to their standardized secure configurations;
- Appropriately test software applications prior to implementation;
- Encrypt any wireless data transmissions in the Company's offices that could contain sensitive data;
- Limit access to drives and applications that host sensitive data;
- Map external access points to the Company's network;
- Evaluate the cyber-security programs of vendors or other third parties that have independent access to the Company's networks or proprietary data, and, where appropriate, ensured that third party contracts or statements of work include appropriate provisions governing cyber-security;
- Implement adequate access logging capabilities, as well as automated exception reporting capabilities that are reasonably designed to detect malicious activity;
- Test the functioning of the Company's access logging and exception reporting systems;
- Require relatively strong user passwords that must be changed from time to time;
- Encrypt all laptops containing Nonpublic Personal Information;
- Promptly disable access for any terminated Employees; and
- Permanently erase or destroy any electronic storage media that is being discarded.

Working in Public Places

Employees should avoid discussing Nonpublic Personal Information in public places where they may be overheard, such as in restaurants and elevators. Employees should be cautious when using laptops or reviewing documents that contain Nonpublic Personal Information in public places to prevent unauthorized people from viewing the information.

Discarding Information

Employees may only discard or destroy Nonpublic Personal Information in accordance with the Firm's policies. Employees are reminded that electronic and hard copy media containing Nonpublic Personal Information must be destroyed or permanently erased before being discarded.

Responding to Privacy Breaches

If any Employee becomes aware of an actual or suspected privacy breach, including any improper disclosure of Nonpublic Personal Information, that Employee must promptly notify the CCO or a member of the legal compliance team. Upon becoming aware of an actual or suspected breach, the CCO or a member of the legal compliance team will investigate the situation take the following actions, as appropriate:

- To the extent possible, identify the information that was disclosed and the improper recipients;
- Notify appropriate members of senior management;
- Take any actions necessary to prevent further improper disclosures;
- Take any actions necessary to reduce the potential harm from improper disclosures that have already occurred;
- Discuss the issue with legal counsel, and consider discussing the issue with regulatory authorities and/or law enforcement officials;
- Assess notification requirements imposed by applicable state and national regulatory authorities and/or law enforcement officials;
- Evaluate the need to notify affected Clients, and make any such notifications;
- Collect, prepare, and retain documentation associated with the inadvertent disclosure and the Company's response(s); and
- Evaluate the need for changes to the Company's privacy protection policies and procedures in light of the breach.

Privacy Protection Training

The Compliance Department will ensure that all new Employees have received, reviewed, and understand their obligations to protect Nonpublic Personal Information. The CCO or his designee will also remind all Employees of their privacy protection obligations in connection with the Company's annual compliance training.

NexAdvisors, LLC
Privacy Notice

General

As part of the firm's annual requirement, NexAdvisors, LLC ("the Company") is mailing its privacy policy to each of its individual clients. NexAdvisors, LLC has adopted certain procedures designed to maintain and secure the non-public personal information of its clients from inappropriate disclosure to third parties. The policy is designed to meet the standards set forth in the federal regulations.

We are committed to keeping personal information collected from potential, current and former clients confidential and secure. The proper handling of personal information is one of our highest priorities. The Company never sells information relating to its clients to any outside third parties.

The Privacy Policy will be provided to customers initially upon establishing an account and annually or upon request.

Nonpublic Information

We collect and keep only information that is necessary for us to provide the services requested by our clients and to administer clients' business with the Company.

We may collect non-public personal information from clients or potential clients:

- From clients when they complete an application or other form, as well as through written and electronic correspondence and telephone contacts. This includes information such as name, address, social security number, assets, income, net worth, copies of financial documents and other information deemed necessary to evaluate the Client's financial needs.
- As a result of transactions with the Company, its affiliates or others. This could include transactions completed with the Company or information received from outside vendors to complete transactions or to effect financial goals.

Sharing Nonpublic Information

In the normal course of business, the Company may share the non-public personal information of its clients with non-affiliated companies or individuals (i) as permitted by law and as required to provide services to our clients, such as with representatives within the Company, administrators, securities clearing firms, mutual fund companies, insurance companies and other financial services providers, or (ii) to comply with legal or regulatory requirements. The Company may also disclose non-public personal information to another financial services provider in connection with the transfer of an account to such financial services provider. Further, in the normal course of our business, the Company may disclose information it collects about clients to companies or individuals that contract with the Company to perform servicing functions such as:

- Record keeping
- Computer-related services

Good faith disclosure to regulators who have regulatory authority over the Company.

Companies hired to provide support services are not allowed to use personal information for their own purposes and are contractually obligated to maintain strict confidentiality. The Company limits use of personal information to the performance of the specific service requested.

We do not provide personally identifiable information to mailing list vendors or solicitors for any purpose. When we provide personal information to service providers, we require these providers to agree to safeguard such information, to use the information only for the intended purpose and to abide by applicable law.

Internet Access

The Company maintains a corporate website. Any information gathered through the Company's website will be treated in accordance with this Privacy Policy.

Employee Access to Information

Only employees with a valid business reason have access to clients' personal information. These employees are educated on the importance of maintaining the confidentiality and security of this information. They are required to abide by our information handling practices.

Protection of Information

We maintain security standards to protect clients' information, whether written, spoken, or electronic. The Company updates and checks its systems to ensure the protection and integrity of information.

Maintaining Accurate Information

Our goal is to maintain accurate, up to date Client records in accordance with industry standards. We have procedures in place to keep information current and complete, including timely correction of inaccurate information.

Electronic Communication

Should clients send us questions and comments via e-mail, we will share the Client's correspondence only with those employees or agents most capable of addressing the Client's questions and concerns.

We will retain all written communication until we have done our very best to provide the Client with a complete and satisfactory response. Ultimately, we will either discard the communication or archive it according to the requirements under applicable securities laws.

Please note that, unless expressly advised otherwise, our e-mail facilities do not provide a means for completely secure and private communications between us and our clients. Although every attempt will be made to keep Client information confidential, from a technical standpoint, there is still a risk. If the Client wishes, communications with us may be conducted via telephone or by facsimile. Additional security is available to clients if they equip their Internet browser with 128-bit "secure socket layer" encryption, which provides more secure transmissions.

Disclosure of our Privacy Policy

We recognize and respect the privacy concerns of our potential, current and former clients. We are committed to safeguarding this information. As a member of the financial services industry, we are providing this Privacy Policy for informational purposes to clients and employees and will distribute and update it as required by law. It is also available upon request.

****

Annual Offering of the Form ADV Part 2: As part of the firm's annual requirement, NexAdvisors, LLC is making an offering of its Form ADV Part 2 to all Clients. Clients can request a copy of the firm's Form ADV Part 2A at no charge by calling 214-550-8350.