PRIVACY PROTECTION POLICY

May 2018

Background

Privacy Protection

Regulation S-P ("Reg S-P") requires registered investment advisers to adopt and implement policies and procedures that are reasonably designed to protect the confidentiality of nonpublic personal records. Reg S-P applies to "consumer" records, meaning records regarding individuals, families, or households. Reg S-P does not explicitly apply to the records of companies, investors in a private fund, or individuals acting in a business capacity, but corresponding Federal Trade Commission ("FTC") rules may impose similar disclosure and safeguarding obligations. The Company is committed to protecting the confidentiality of all non-public information regarding its Customers, Investors, prospects, and Supervised Persons ("Nonpublic Personal Information").

Reg S-P requires the Company to provide its Customers with notices describing the Company's privacy policies and procedures. These privacy notices must be delivered to all new Customers upon inception of an arrangement, and at least annually thereafter. Reg S-P does not require the distribution of privacy notices to companies, to investors in a private fund, or to individuals acting in a business capacity, but the Company provides initial and annual privacy notices to all Customers and Investors as a best practice.

Guiding Principles

The Company will seek to limit its collection of Nonpublic Personal Information to that which is reasonably necessary for legitimate business purposes. The Company will not disclose Nonpublic Personal Information except in accordance with these policies and procedures, as permitted or required by law, or as authorized in writing by the Customer or Investor. The Company will never sell Nonpublic Personal Information.

With respect to Nonpublic Personal Information, the Company will strive to: (a) ensure the security and confidentiality of the information; (b) protect against anticipated threats and hazards to the security and integrity of the information; and (c) protect against unauthorized access to, or improper use of, the information. Notify the Company promptly of any threats to, or improper disclosure of, Nonpublic Personal Information.

Although these principles and procedures apply specifically to Nonpublic Personal Information, Supervised Persons must be careful to protect all of the Company's proprietary information.

Risks

In developing these policies and procedures, the Company considered the material risks associated with privacy protection. This analysis included risks such as:

- Company trade secrets are not protected from unauthorized access by Supervised Persons or third-party service providers;
- Nonpublic Personal Information is not recorded accurately or protected from inadvertent alteration or destruction;
- Nonpublic Personal Information is not protected from unauthorized access by Supervised Persons or third-party service providers;

- Nonpublic Personal Information can be accessed, copied, or destroyed by physical or electronic intrusions;

- False or misleading disclosures are made to Customers or Investors about the use or protection of Nonpublic Personal Information;

- Third-party service providers have adopted inadequate policies and procedures to protect Nonpublic Personal Information;

- Company fails to comply with applicable state privacy laws;

- Company uses information obtained from affiliates for marketing purposes without ensuring that affected individuals have been given adequate notice and an opportunity to opt out; and

- Company fails to comply with applicable international privacy laws;

The Company has established the following guidelines to mitigate these risks.

Policies and Procedures

What this Policy Covers

This Policy covers our use and treatment of personally identifiable information (also referred to as PII, personal data, "Personal Information", or "Nonpublic Personal Information"):

- that the Company may collect when a Customer, Investor, or prospect (collectively, "Customer") accesses or uses our services or website in any manner (collectively, the "Services");
- provided to the Company as described below; and
- unless you are notified another policy applies.

By accessing or using the Company's Services, a Customer acknowledges and agrees that they consent to the practices and policies outlined in this Policy.

This Policy also explains a Customer's choices about how the Company uses information about the Customer. A Customer's choices include how one can object to certain uses of information about the Customer and how one can access and update certain information about the Customer.

The Company does not knowingly collect or solicit personal information from children or anyone under the age of 16 or knowingly allow such persons to use, access or register for the Services. Neither the Company's website, Services, nor this Policy, are directed to such persons.

What Information is Collected about Customers

a. Information provided to the Company:

The Company receives and stores any information a Customer knowingly provides. A Customer can choose not to provide the Company with certain information, but then a Customer may not be able to register with the Company or take advantage of some of the Company's features or receive the Company's mailings, articles, thought pieces, etc. Unless another policy applies, the Company may also collect and use information submitted through any support or customer portal related to the Services.

If a Customer has provided the Company with a means of contacting the Customer for particular purposes, the Company may use such means to communicate with the Customer for those purposes. If a Customer

previously provided the Company with such information but no longer wishes to receive such communications, a Customer can indicate their preference by sending an email to compliance@mosaicrei.com.

b. Information the Company receives from other sources:

The Company may receive information about Customers from:

- other Service users (e.g. if a Customer's email address is mentioned in feedback or designated as a contact); and
- third-party services (e.g. if a Customer links another account he/she owns to the Services, the Company may receive a Customer's name and email address as permitted by the Customer's profile settings in order to authenticate the Customer). The information the Company receives depends on the settings, permissions and privacy policy controlled by that third-party service. A Customer is responsible for checking the privacy settings and notices in these third-party services to understand what data may be disclosed;

How the Company Uses Information it Collects

How the Company uses the information it collects depends in part on which Services are provided to a Customer, how a Customer uses them, and any preferences a Customer has communicated to the Company.

The Company may use information about a Customer:

- to provide the Services requested;
- to register a Customer for events (for example, an information event or distribution list notification of current offerings, Services, market updates, thought pieces, articles, postings, etc.);
- for security (to authenticate a Customer, verify accounts and activity, monitor suspicious or fraudulent activity, etc.);
- to provide support, as applicable;
- to operate and maintain the Services offered;
- to process Company interaction with a Customer;
- to communicate with a Customer about the Company's Services;
- to protect the Company's legitimate business interests and legal rights; and
- with a Customer's consent: the Company uses information about a Customer where the Customer has given the Company consents to do so for a specific purpose not listed above.

Legal bases for processing (for EEA users):

If a Customer is an individual in the European Economic Area (EEA), the Company collects and processes information about a Customer only where the Company has the legal bases for doing so under applicable EU laws. The legal bases depend on the Services provided to a Customer. This means the Company may collect and use a Customer's information only where:

- the Company needs it to provide a Customer with the Services, including providing support and personalized features and to protect the safety and security of the Services;
- it satisfies a legitimate interest (which is not overridden by a Customer's data protection interests);
- a Customer gives consents for the Company to do so for a specific purpose; or
- the Company needs to process a Customer's data to comply with a legal obligation.

Protecting Confidential Information

Supervised Persons will maintain the confidentiality of information acquired in connection with their employment, with particular care being taken regarding Nonpublic Personal Information. Improper use of the Company's proprietary information, including Nonpublic Personal Information, is cause for

disciplinary action, up to and including termination of employment for cause and referral to appropriate civil and criminal legal authorities. Consequently, all Supervised Persons (including long-term consultants and temporary interns) are required to sign and adhere to a confidentiality agreement covering these and other matters.

Nonpublic Personal Information will be restricted to Supervised Persons who have a need to know such information.

All requests by third-parties to review this Privacy Policy, the Company's Compliance Manual, compliance testing results, correspondence between the Company and regulators and other compliance-related documents should be forwarded to the CCO. Supervised Persons are not authorized to respond to such requests without the prior approval of the CCO.

Disclosure of Nonpublic Personal Information

Nonpublic Personal Information may only be provided to third parties under the following circumstances:

- To broker-dealers opening brokerage accounts;
- To accountants, lawyers, and others as directed in writing by Customers or Investors;
- To specified family members as directed in writing by Customers or Investors, or as authorized by law;
- To third-party service providers, as necessary to service Client or Investor accounts; and
- To regulators and others, as required by law.

Supervised Persons should take reasonable precautions to confirm the identity of individuals requesting Nonpublic Personal Information. Supervised Persons must be careful to avoid disclosures to identity thieves, who may use certain Nonpublic Personal Information, such as a social security number, to convince a Supervised Person to divulge additional information. Any contacts with suspected identity thieves must be reported promptly to the CCO.

To the extent practicable, Supervised Persons will seek to remove nonessential Nonpublic Personal Information from information disclosed to third parties. Social security numbers included in any distributed lists or reports must be encrypted.

Nonpublic Personal Information may be reviewed by the Company's outside service providers, such as accountants, lawyers, consultants, and administrators. The Company may review such service providers' privacy policies to ensure that Nonpublic Personal Information is not used or distributed inappropriately.

Prior to providing any third-party service provider with access to personal information about Customers or Investors who are residents of Massachusetts, the Company will take reasonable steps to verify that such service provider has a written, comprehensive information security program that is in compliance with the provisions of Massachusetts statute 201 CMR 17. The CCO will ensure that any new contracts with such service providers include provisions requiring the service provider's implementation of security policies and procedures that comply with 201 CMR 17.

Access to the Company's Premises

The Company's premises will be locked outside of normal business hours. Meetings with Customers and Investors should be held in conference rooms or other locations where Nonpublic Personal Information is not available or audible to others.

Visitors to the Company's offices will not be left unattended in a manner that will permit unauthorized

access to proprietary information.

On an annual basis the CCO assesses whether information security risks associated with the Company's physical office have changed in material ways. The Director of Operations and the CCO will work together to address any newly identified vulnerabilities.

Information Stored in Hard Copy Formats

The Company has implemented the following procedures to protect Nonpublic Personal Information stored in hard copy formats:

- To the extent practicable, Nonpublic Personal Information will be kept in lockable filing cabinets;
- All Nonpublic Personal Information, as well as the Company's proprietary information, should be locked up at the end of each workday;
- Documents containing Nonpublic Personal Information must never be left unattended in public spaces, such as lobbies or conference rooms;
- Documents being printed, copied, or faxed must not be left unattended;
- Supervised Persons will exercise due caution when emailing, mailing or faxing documents containing Nonpublic Personal Information to ensure that the documents are sent to the intended recipients; and
- Supervised Persons may only remove documents containing Nonpublic Personal Information from the Company's premises for legitimate business purposes. Any documents taken off premises must be handled with appropriate care and returned as soon as practicable.

Responding to Privacy Breaches

If any Supervised Person becomes aware of an actual or suspected privacy breach, including any improper disclosure of Nonpublic Personal Information, that Supervised Person must promptly notify the CCO. Upon becoming aware of an actual or suspected breach, the CCO will investigate the situation and 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;
- As applicable, 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 or Investors, and make any such notifications;
- Collect, prepare, and retain documentation associated with the inadvertent disclosure and Company response(s); and

- Evaluate the need for changes to Company privacy protection policies and procedures in light of the breach.

Privacy Protection Training

The CCO or his/her delegate will ensure that all new Supervised Persons have received, reviewed, and understand their obligations to protect Nonpublic Personal Information. The CCO will remind all Supervised Persons of their privacy protection obligations as part of the Company's annual compliance training. If the Program appears to be functioning well and has not undergone material changes then this reminder might appropriately take the form of a broadly-distributed annual email. The CCO may provide training more frequently and/or in person to individuals or groups if:

- Company's policies and procedures, or the threats to Nonpublic Personal Information, change in a material way;

- Company experiences a privacy breach; and/or

- One or more Supervised Persons do not appear to understand their obligations regarding privacy protection.

Changes to this Policy

The Company is committed to complying with data privacy laws in every jurisdiction it does business. As such, the Company may amend this Policy from time to time. Use of information the Company collects now is subject to the Policy in effect at the time such information is used. If the Company makes changes in the way it uses Personal Information, the Company shall notify its Customers.