Privacy

Policy
As a Registered Investment Adviser, Prism must comply with certain state and federal privacy rules (or other applicable regulations), which requires Registered Investment Advisers to adopt policies and procedures to protect the "non-public personal information" of natural person Clients and to disclose to such persons policies and procedures for protecting that information. Further, our firm must comply with additional rules and regulations, to the extent that the firm has affiliated entities with which it may share and use consumer information received from affiliates.

Background
The purpose of these requirements and privacy policies and procedures is to provide administrative, technical and physical safeguards which assist employees in maintaining the confidentiality of non-public personal information ("NPI") collected from the Clients (consumers and customers) of an investment adviser. All NPI, whether relating to an adviser's current or former Clients, is subject to these privacy policies and procedures. Any doubts about the confidentiality of Client information must be resolved in favor of confidentiality.

Collection of Information
For collection of information purposes, NPI includes non-public "personally identifiable financial information" plus any list, description or grouping of Clients that is derived from non-public personally identifiable financial information. Such information may include personal financial and account information, information relating to services performed for or transactions entered into on behalf of Clients, advice provided by Prism to Clients, and data or analyses derived from such NPI.

Use of Information
Certain state and federal use of information rules require investment advisers, and other regulated entities, to the extent relevant, to implement limitations on the firm's use of certain consumer information received from an affiliated entity to solicit that consumer for marketing purposes. These rules provide for notice and opt-out procedures, among other things.

Responsibility
The CCO is responsible for reviewing, maintaining and enforcing these policies and procedures to ensure meeting Prism's Client privacy goals and objectives while at a minimum ensuring compliance with applicable federal and state laws and regulations. The CCO may recommend to the firm's principal(s) any disciplinary or other action as appropriate. The CCO is also responsible for distributing these policies and procedures to employees and conducting appropriate employee training to ensure employee adherence to these policies and procedures.

Procedure
Prism has adopted various procedures to implement the firm's policy and conducts reviews to monitor and ensure the firm's policy is observed, implemented properly, and amended or updated, as appropriate,

which include the following:

Non-Disclosure of Client Information

Prism maintains safeguards to comply with federal and state standards to guard each Client's non-public personal information ("NPI"). Prism does not share any NPI with any nonaffiliated third parties, except in the following circumstances:

- As necessary to provide the service that the Client has requested or authorized, or to maintain and service the Client's account;
- As required by regulatory authorities or law enforcement officials who have jurisdiction over Prism or as otherwise required by any applicable law; and
- To the extent reasonably necessary to prevent fraud and unauthorized transactions.

Employees are prohibited, either during or after termination of their employment, from disclosing NPI to any person or entity outside Prism, including family members, except under the circumstances described above. An employee is permitted to disclose NPI only to such other employees who need to have access to such information to deliver our services to the Client.

Safeguarding and Disposal of Client Information

Prism restricts access to NPI to those employees who need to know such information to provide services to our Clients. Any employee who is authorized to have access to NPI is required to keep such information in a secure compartment or receptacle on a daily basis as of the close of business each day. All electronic or computer files containing such information shall be password secured and firewall protected from access by unauthorized persons. Any conversations involving NPI, if appropriate at all, must be conducted by employees in private, and care must be taken to avoid any unauthorized persons overhearing or intercepting such conversations.

Safeguarding standards encompass all aspects of Prism that affect security. This includes not just computer security standards but also such areas as physical security and personnel procedures. Examples of important safeguarding standards that Prism has adopted include:

- Access controls on Client information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing Client information to unauthorized individuals who may seek to obtain this information through fraudulent means (e.g., requiring employee use of user ID numbers and passwords, etc.);
- Access restrictions at physical locations containing Client information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals (e.g., intruder detection devices, use of fire and burglar resistant storage devices);
- Encryption or password protection of electronic Client information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
- Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to Client information (e.g., require data entry to be reviewed for accuracy by personnel not involved in its preparation; adjustments and correction of master records should be reviewed and approved by personnel other than those approving routine transactions, etc.);
- Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into Client information systems (e.g., data should be auditable for detection of loss and accidental and intentional manipulation);
- Response programs that specify actions to be taken when the firm suspects or detects that

unauthorized individuals have gained access to Client information systems, including appropriate reports to regulatory and law enforcement agencies;

- Measures to protect against destruction, loss, or damage of Client information due to potential environmental hazards, such as fire and water damage or technological failures (e.g., use of fire resistant storage facilities and vaults; backup and store off site key data to ensure proper recovery); and Information systems security should incorporate system audits and monitoring, security of physical facilities and personnel, the use of commercial or in-house services (such as networking services), and contingency planning.

Some methods of disposal to ensure that the information cannot practicably be read or reconstructed that Prism may adopt include:

- Procedures requiring the burning, pulverizing, or shredding or papers containing consumer report information;
- Procedures to ensure the destruction or erasure of electronic media; and
- After due diligence, contracting with a service provider engaged in the business of record destruction, to provide such services in a manner consistent with the disposal rule.

Privacy Notices

Prism will provide each natural person Client with initial notice of the firm's current policy when the Client relationship is established. Prism shall also provide each such Client with a new notice of the firm's current privacy policies at least annually. If Prism shares non-public personal information ("NPI") with a nonaffiliated company under circumstances not covered by an exception under state and or federal law, the firm will deliver to each affected consumer an opportunity to opt out of such information sharing.