PRIME ADVISORS, INC.®

PRIVACY POLICY

Prime Advisors, Inc. must comply with SEC Regulation S-P (and other applicable regulations), that require registered investment advisers to adopt policies and procedures to protect the "nonpublic personal information" of any natural person client ("Client") and to disclose to such persons its policies and procedures for protecting their information. Nonpublic personal information includes nonpublic "personally identifiable financial information" plus any list, description or grouping of Clients that is derived from nonpublic 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 Prime to Clients, and data or analyses derived from such nonpublic personal information.

Certain state laws have the potential to place an increased burden on Prime employees to safeguard information. For example, Prime must comply with the California Financial Information Privacy Act (SB1) if the firm does business with California Clients (see the Privacy Notice section below). In addition, the Massachusetts Office of Consumer Affairs and Business Regulations has adopted data security regulations which protect Clients that reside in Massachusetts. Prime's current privacy practices are designed to address these states' concerns.

Prime's Chief Compliance Officer is responsible for reviewing, maintaining and enforcing these policies and procedures to ensure meeting Prime's Client privacy goals and objectives while at a minimum ensuring compliance with applicable federal and state laws and regulations. Prime's Chief Compliance Officer may recommend to the CEO any disciplinary or other action as appropriate. He is also responsible for distributing these policies and procedures to employees and conducting appropriate employee training.

The purpose of these privacy policies and procedures is to provide administrative, technical and physical safeguards that assist employees in maintaining the confidentiality of nonpublic personal information collected from Prime's Clients. All nonpublic information, 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.

Prime has adopted various procedures to implement the firm's policy and 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

Prime maintains safeguards to comply with federal and state standards to guard each Client's nonpublic personal information. Prime does not share any nonpublic personal information 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 Prime, 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 Client nonpublic personal information to any person or entity outside Prime, including family members, except under the circumstances described above. An employee is permitted to disclose nonpublic personal information 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

Prime restricts access to nonpublic personal information to those employees who need to know such information to provide services to our Clients.

Any employee who is authorized to have access to Client nonpublic personal information 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 non public personal information, 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 Prime 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 Prime has adopted include:

- Access controls on 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 IDs and passwords, etc.);
- Access restrictions at physical locations, 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 of laptops and flashdrives;
- Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into information systems; and
- 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).

Any employee who is authorized to possess Client nonpublic personal information for a business purpose is required to take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. Some methods include:

- Encrypting monthly and quarterly reporting packages when those packages are sent by e-mail;
- Shredding papers containing Client report information;
- 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

Prime will provide each Client, or his or her advisor, with initial notice of the firm's current policy when the Client relationship is established. Prime shall also provide each such Client, or his or her advisor, with a new notice of the firm's current privacy policies at least annually. If Prime shares nonpublic personal information relating to a non-California Client with a nonaffiliated company under circumstances not covered by an exception under Regulation S-P, then Prime will deliver to each affected Client an opportunity to opt out of such information sharing. If Prime shares nonpublic personal information relating to a California Client with a nonaffiliated company under circumstances not covered by an exception under SB1, the firm will deliver to each affected Client an opportunity to opt in regarding such information sharing. If, at any time, Prime adopts material changes to its privacy policies, the firm shall provide each such Client with a revised notice reflecting the new privacy policies.