

KCM INVESTMENT ADVISORS LLC

PRIVACY POLICY and INFORMATION SECURITY PROGRAM

March 1, 2010

Pursuant to SEC best practices and the Commonwealth of Massachusetts Standards for Protection of Personal Information, KCM Investment Advisors LCC (KCM) has adopted a robust Privacy Policy aimed at protecting all client confidential and nonpublic information and to safeguard personal information contained in both paper and electronic records. The objectives of this requirement are to ensure the security and confidentiality of client information in a manner fully consistent with industry standards, and to protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any client.

KCM has a commitment to the safeguarding against unauthorized acquisition or unauthorized use of unencrypted data, or encrypted electronic data for all clients. To this end the following persons are designated to implement, review and revise as necessary a comprehensive information security program: Chief Compliance Officer (CCO), Chief Technology Officer (CTO). The primary objectives for the CCO and CTO are to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and/or integrity of any electronic, paper or other records containing personal information and evaluating and improving, where necessary, the effectiveness of our current safeguards for limiting such risks. To this end, KCM employs;

1. Ongoing employee training
2. Testing of electronic encryption
3. Setting policy for employees relating to the storage, access and transportation of client records.

KCM does not share any nonpublic personal information with any nonaffiliated third parties, except in the following circumstances:

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

KCM's officers and employees ("KCM Personnel") are prohibited, either during or after termination of their employment, from disclosing nonpublic personal information to any person or entity outside of the Registered Investment Advisor / Client relationship, except under the circumstances described above. KCM Personnel are permitted to disclose

nonpublic personal information only to such other KCM Personnel who need to have access to such information to deliver our services to the client.

Security of Client Information

KCM restricts access to nonpublic personal information to KCM Personnel who need to know such information to provide services for the client. Any KCM Personnel who are authorized to have access to nonpublic personal information are required to keep such information in a confidential 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 nonpublic personal information, if appropriate at all, must be conducted by KCM Personnel in private, and care must be taken to avoid any unauthorized persons overhearing or intercepting such conversations.

Privacy Notices

KCM will provide each client with an initial notice of the KCM's privacy policy at the earlier of the time Part II of the KCM's Form ADV is delivered or an account is established. KCM will also provide each client with a new notice of the KCM's current privacy policy at least annually. If, at any time, KCM adopts material changes to its privacy policy, we shall provide each client with a revised notice reflecting the new privacy policies. The Chief Compliance Officer is responsible for ensuring that required notices are distributed to consumers and customers. KCM maintains a web site, and the privacy policy will be posted to the site.

Disposal of Nonpublic Personal Information

KCM will shred, deliver to a document destruction firm, or other render illegible hard copies of any customer or consumer nonpublic personal information in its possession when the KCM deems possession of the information to no longer be necessary.

Nonpublic personal information stored on disk, CD, tape or other electronic media shall be cleared, purged, declassified, overwritten and/or encrypted in such a manner so that any information contained therein cannot be restored or decrypted. After the electronic media is cleared, purged, declassified, overwritten or encrypted, the CTO shall check that the original information is not backed-up or saved on a hard drive, recycle bin or other memories.

The Chief Compliance Officer shall review the adequacy for third-party service provider engaged by the KCM that necessarily obtains access to nonpublic personal client information during the course of their services on behalf of KCM to adopt similar policies and procedures relating to the secure disposal of nonpublic personal information.