Privacy

As a registered investment adviser, Piton Investment Management, LP, ("Piton"), must comply with SEC Regulation S-P (or other applicable regulations), which requires registered advisers to adopt policies and procedures to protect the "nonpublic personal information" of natural person consumers and clients and to disclose to such persons policies and procedures for protecting that 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 Piton to clients, and data or analyses derived from such nonpublic personal information.

Background

The purpose of these privacy policies and procedures is to provide administrative, technical and physical safeguards which assist employees in maintaining the confidentiality of nonpublic personal information collected from the consumers and clients of an investment adviser. 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.

Responsibility

The Chief Compliance Officer is responsible for reviewing, maintaining and enforcing these policies and procedures to ensure meeting Piton's client privacy goals and objectives while at a minimum ensuring compliance with applicable federal and state laws and regulations. The Chief Compliance Officer may recommend to the Chief Executive Officer any disciplinary or other action as appropriate. The Chief Compliance Officer 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.

Procedures

Piton 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

Piton maintains safeguards to comply with federal and state standards to guard each client's nonpublic personal information. Piton 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 Piton, 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 nonpublic personal information to any person or entity outside Piton, 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

Piton 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 nonpublic personal information is required to keep such information in a secure compartments 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 authorized persons overhearing or intercepting such conversations. Safeguarding standards encompass all aspects of Piton that affect security. This included not just computer security standards but also such areas as physical security and personnel procedures. Examples of important safeguarding standards that Piton 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.);
- Encryption of electronic client information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

Any employee who is authorized to possess "consumer report 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. There are several components to establishing 'reasonable' measures that are appropriate for the firm:

- Assessing the sensitivity of the consumer report information we collect;
- The nature of our advisory services and the size of our operation;
- Evaluating the costs and benefits of different disposal methods; and
- Researching relevant technological changes and capabilities.
- Some methods of disposal to ensure that the information cannot practicably be read or reconstructed that Piton may adopt:

- Procedures requiring 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 Notice

Piton will provide each natural person client with initial notice of the firm's current policy when the client relationship is established. Piton shall also provide each such client with a new notice of the firm's current privacy policies at least annually. If, at any time, Piton adopts material changes to its privacy policies, the firm shall provide each such client with a revised notice reflecting the new privacy policies. The Chief Compliance Officer is responsible for ensuring that required notices are distributed to Piton's consumers and clients.

Employee Responsibilities

All supervised persons are prohibited, either during or after the termination of their employment with Piton, from disclosing Confidential Client Information to any person or entity outside the firm, including family members, except under the circumstances described above. A supervised person is permitted to disclose Confidential Client Information only to such other supervised persons who need to have access to such information to deliver the Piton's services to the client. Supervised persons are also prohibited from making unauthorized copies of any documents or files containing Confidential Client Information and, upon termination of their employment with Piton, must return all such documents to Piton. Any supervised person who violates the non-disclosure policy described above will be subject to disciplinary action, including possible termination, whether or not he or she benefited from the disclosed information.

Maintaining Confidentiality of Private Proprietary Information

To protect the confidentiality of the Firm's confidential and proprietary information and the confidentiality of clients' and potential clients' records, employees should take the following additional security precautions:

- Documents containing confidential information may not be taken from the Firm's offices without the prior consent of the Chief Compliance Officer, and any copies removed from the Firm's offices must be promptly returned. Photocopies of confidential information may only be made as required, and all copies and originals of such documents must be disposed of in a way that keeps the information confidential.
- Physical access to any non-electronic confidential information must be limited by either locking or monitoring access to the offices and storage areas where such information is located.
- Visitors to the Firm's office shall be monitored and/or accompanied by an employee

At times, the Firm may enter into one or more agreements with third parties, pursuant to which the Firm may provide access to confidential information to those third parties. If this occurs, the Firm will protect the privacy of confidential information and include in the relevant agreements provisions protecting confidential information to the extent required by law.