Appendix B

Sample Written Information Security Plan

I. OBJECTIVE:

Our objective, in the development and implementation of this written information security plan, is to create effective administrative, technical and physical safeguards in order to protect our customers' non-public personal information. The plan will evaluate our electronic and physical methods of accessing, collecting, storing, using, transmitting, protecting, and disposing of our customers' non-public personal information.

II. PURPOSES:

a) Ensure the security and confidentiality of our customers' information;

b) Protect against any anticipated threats or hazards to the security or integrity of our customers' information;

c) Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any of our customers.

III. ACTION PLANS:

a) Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems;

b) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information;

c) Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks.

IV. ACTION STEPS:

a) Appoint a specific person or persons within the firm to be responsible for:
   1) initial implementation of the plan;
   2) training of employees;
   3) regular testing of the controls and safeguards established by the plan;
   4) evaluating the ability of prospective service providers to maintain appropriate information security practices, ensuring that such providers

are required to comply with this information security plan, and monitoring such providers for compliance herewith; and
5) periodically evaluating and adjusting the plan, as necessary, in light of relevant changes in technology, sensitivity of customer information, reasonably foreseeable internal or external threats to customer information, changes to our own business (such as mergers or acquisitions or outsourcing), and/or changes to customer information systems.

b) Conduct an annual training session for all owners, managers, employees and independent contractors—and periodic training for new employees—working for the firm on the elements of this information security plan, the contents of the firm's "Privacy Policy," and any other requirements of federal or state privacy laws. All persons in attendance should be required to certify their attendance at the training, their receipt of the firm's privacy policy, and their familiarity with the firm's requirements for ensuring the protection of customers' non-public personal information.

c) Determine reasonably foreseeable **internal** threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems, assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information, and evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks.

Internal Threat	Risk Level	Response
Intentional or inadvertent misuse of customer information by current employees	Low	1) Dissemination of, and annual training, on privacy laws and firm privacy policy. 2) Incorporation of privacy policy guidelines into employee handbook. 3) Employment agreements amended to require compliance with privacy policy and to prohibit any nonconforming use of customer information during or after employment. 4) Employees encouraged to report any suspicious or unauthorized use of customer information. 5) Periodic testing to ensure these safeguards are implemented uniformly.
Intentional or inadvertent misuse of customer information by	Medium	1) Require return of all customer information in the former employee's possession (i.e., policies requiring return of

former employees subsequent to their employment		all firm property, including laptop computers and other devices in which records may be stored, files, records, work papers, etc… 2) Eliminate access to customer information (i.e., policies requiring surrender of keys, ID or access codes or badges, business cards; disable remote electronic access; invalidate voicemail, e-mail, internet, passwords, etc…, and maintain a highly secured master list of all lock combinations, passwords, and keys. 3) Change user-ID's and passwords for current employees periodically. 4) Amend employment agreements during employment to require compliance with privacy policy and to prohibit any nonconforming use of customer information during or after employment. 5) Send "pre-emptive" notices to clients when the firm has reason to believe a departed employee may attempt to wrongfully use customer information, informing them that the employee has left the firm. 6) Encourage employees to report any suspicious or unauthorized use of customer information. 7) Periodic testing to ensure these safeguards are implemented uniformly.
Inadvertent disclosure of customer information to the general public or guests in the office	Low	1) Prohibit employees from keeping open files on their desks when stepping away. 2) Require all files and other records containing customer records to be secured at day's end. 3) Use software program that requires each employee to enter a unique log-in ID to access computer records, and to re-log-in when the computer is inactive for more than a few minutes. 4) Change user-ID's and passwords for current employees periodically. 5) Restrict guests to one entrance point, require them to present a photo ID, sign-in,

		and wear a plainly visible "GUEST" badge or tag; restrict areas within the office in which guests may travel unescorted. 6) Use shredding machines on unused photocopies or other records being discarded before depositing in trash or recycling containers. 7) Ensure secure destruction of obsolete equipment, including computer hardware and software systems. 8) Encourage employees to report any suspicious or unauthorized use of customer information. 9) Periodic testing to ensure these safeguards are implemented uniformly. *{ VERY LARGE FIRMS MAY WISH TO CONSIDER ADDING THE FOLLOWING: }* 10) Require all customer records to be maintained in locked desks or filing cabinets when the records are not being used, or when the office is closed. 11) Install security badge system, requiring employees to use photo ID badges with an electronic strip to open locked internal doors in the office.

d) Determine reasonably foreseeable **external** threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems, assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information, and evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks.

External Threat	Risk Level	Response
Inappropriate access to, or acquisition of, customer information by third parties	Low	1) Install firewalls for access to firm internet site. Include privacy policy on the site. 2) Require secure authentication for internet and/or intranet and extranet users. 3) Establish dial-in protections (such as Caller-ID, Callback, encryption) to prevent unauthorized access.

		4) Require encryption and authentication for all infrared, radio, or other wireless links. 5) Train employees to protect and secure laptops, handheld computers, or other devices used outside the office that contain customer information. 6) Install virus-checking software that continually monitors all files, downloads, floppy disks, CD's, all incoming and outgoing e-mail messages. 7) Establish uniform procedures for installation of updated software. 8) Establish systems and procedures for secure back-up, storage and retrieval of computerized and paper records. 9) Establish procedures to ensure external points of entry to the office are closed, locked and inaccessible to unauthorized persons when the office is closed. 10) Install burglar alarm or other security systems, with training for authorized persons on activation, deactivation, …. 11) Physically lock or otherwise secure the computer room, and if necessary, all areas in which paper records are maintained. 12) Use shredding machines on unused photocopies or other records being discarded before depositing in trash or recycling containers. 13) Ensure secure destruction of obsolete equipment, including computer hardware and software systems. 14) Encourage employees to report any suspicious or unauthorized use of customer information. 15) Periodic testing to ensure these safeguards are implemented uniformly.
Inappropriate use of customer information by third parties	Medium	1) Evaluate the ability of all prospective third-party service providers to maintain appropriate information security practices. 2) Provide all third-party service providers to whom contractual access to premises or records has been granted (including, but

		not limited to, insurance companies being solicited for new or renewal policies, mailing houses, custodial or plant services, equipment or services vendors, affiliates, non-affiliated joint marketing partners, …) with a copy of the Privacy Policy. 2) Require all such third-parties—**by written contract**—to adhere to the Privacy Policy, agree to make no use of any nonpublic personal information on your customers that would be prohibited thereby, or otherwise by law or contract, and agree to hold harmless and indemnify the firm for any inappropriate use of customer non-public personal information. 3) Require all such third-parties—**by written contract**—to return all customer information and all other firm property at the completion or termination, for whatever reason, of the agreement between the firm and the third-party. 4) Prohibit access to customer information (i.e., policies requiring surrender of keys, ID or access codes or badges, disabling remote electronic access; invalidating voicemail, e-mail, internet, passwords, etc…, if applicable) to all such third-parties upon completion or termination, for whatever reason, of the agreement between the firm and the third-party. 5) Change user-ID's and passwords for current employees periodically. 6) Send "pre-emptive" notices to clients when the firm has reason to believe a terminated third-party service provider may attempt to wrongfully use customer information, informing them that the agreement with the firm is no longer in effect. 7) Encourage employees to report any suspicious or unauthorized use of customer information. 8) Periodic testing to ensure these safeguards are implemented uniformly.