Written Information Security Program ("WISP")

Summary

This policy has been developed to ensure compliance with the Gramm Leach Bliley Act and Massachusetts General Laws c. 93H and 201 CMR 17.00 et seq. and Connecticut General Statutes Section 42-471 regarding data security and protection of employee, client and other personal information to which Firm employees or third party vendors may have access.

This policy is intended to provide assurances as to the level of the Firm's commitment and good faith efforts in protecting financial, client, and employee information within the control of the Firm and its employees. This is a dynamic process and the Firm is continually re-evaluating its internal policies, testing its systems, as well as the specific action steps incorporated into these policies. As part of this process, the Firm will continue to introduce additional safeguards and policies as the Firm grows and as its systems expand and are updated to ensure all data and personal information continues to be secure. This and all referenced policies regarding security and information protection will be reviewed and updated, if necessary, no less than annually. All material changes to this document and all referenced policies, procedures, and training requirements are reviewed and approved by senior management of the firm annually, at a minimum, prior to dissemination and training of staff. Should any exceptions be requested to this or any related security policy, said request will require review and approval by a firm principal, with such approval being documented, setting forth the exception granted and the justification therefor. Employees, including any temporary and contract employees, are made aware of substantive changes to this and all referenced policies through classroom training, or e-mail communications. In addition, all current policies and procedures are available to staff on a shared network drive.

Confidentiality and Privacy

Pursuant to the Gramm-Leach-Bliley Act, the Fair and Accurate Transactions Act of 2003 and Title 16, Part 681 Identity Theft Rules, Fair Credit Reporting Act by the Federal Trade Commission pursuant to 15 U.S.C 1681s(a)(1) (and the regulations issued thereunder) as they relate to financial institutions for which the Firm is a service provider, Massachusetts General Laws c. 93H and 201 CMR 17.00 et seq.,as well as the Rules of Professional Conduct and Firm policy, all Firm lawyers, other professionals, employees, independent contractors, and third party vendors must take appropriate measures and make commercially reasonable best efforts to preserve and protect Confidential, Personal and Internal information.

1. Definitions

a. Confidential Information - personal or client related information, which may include but not be limited to financial information, for which there is an expectation of privacy and which may be protected by attorney/client privilege, statute, regulation, or Firm policy.

b. Employee – for purposes of this WISP, employee shall include any and all full-time, part-time, temporary or seasonal employees, independent contractors, consultants and volunteers.

c. Personal Information - information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, alien registration number or a health insurance identification number.

d. Internal Information – information, including financial information, of the Firm that must be protected against unauthorized disclosure, access or transmission due to proprietary, ethical or privacy considerations.

e. Public Information - information that may or must be open to the general public, with no existing local or national legal restrictions on access or usage.

2. Employee Access Any employee access to privileged or personal information is authorized for business purposes of the Firm only and is based on the sensitivity of the information and the employee's need to know. We remind employees regularly of their obligations regarding privileged and personal information and have established and continually maintain security standards and procedures to help protect against unauthorized access or disclosure of non-public privileged and personal information for which we have been entrusted, including steps to:

- Limit access to privileged and personal information to appropriate individuals for legitimate business reasons and as permitted by law or applicable ethics rules;
- Prohibit unlawful, unauthorized and/or unethical use, access, or disclosure of privileged, Confidential, Personal, and/or Internal information;
- Train our employees in the proper use, handling, storage and destruction of Confidential, Personal and Internal information;
- Obtain agreements of third party vendors with authorized access to Confidential, Personal and/or Internal Information to protect the confidentiality of this information;
- Protect against any anticipated threats or hazards to the security of such information, including but not limited to risks of identity theft and fraud.
- Review these safeguards on a regular basis

Confidential and personal information concerning clients and employees must not be disclosed to anyone either within or outside of the Firm, other than those who have a legitimate need to know the information to perform the business of the Firm. In this connection, all information obtained in representing a client or in relation to any employee must be considered confidential unless it is, beyond any doubt, public information. This confidentiality rule is broader in scope than the attorney-client privilege, and also includes all privileged information. A breach of the Firm's WISP and any other policy incorporated or referenced therein may result in disciplinary action by the Firm, up to and including termination. The duty to preserve Confidential, Personal and Internal information will continue even after a lawyer, other professional, employee or third party vendor is no longer associated with the Firm.

These privacy and confidentiality expectations are incorporated in the Firm's Employee Manual, with all employees required to acknowledge (in writing) that they have read and understand these expectations. To the extent that the Firm conducts training, including without reservation Privacy/Data Protection Training, all employees shall be required to attend such training and must certify that they have attended such training.

Server Room Security

The Server room is secured with restricted access to only the System Administrator, Executive Director and Assistant Director and Support Services. This room is climate controlled and equipped with dedicated air conditioning and ventilation systems to ensure temperature and humidity are automatically monitored and maintained at acceptable levels. The system is monitored through e-mail alerts that detect temperature and humidity above normal levels.

No office space is accessible to a client or third party vendor without prior consent and unless accompanied by an employee of the Firm.

Computer and Technology Operations Policy

General The computer systems and networks (including hardware and software), communications systems (including, but not limited to, telephones, fax machines, modems, network communication devices and software) and other equipment (including, but not limited to, laptops, desktops, monitors, printers, and other peripherals) belonging to or otherwise in the possession of the Firm are the property of the Firm and are to be maintained solely by the Firm. These systems are provided for use in conducting the business of the Firm, although reasonable incidental personal use by employees is permitted. The use of any Firm system for commercial purposes other than that of Firm business is prohibited. The Firm reserves the right to obtain access to any and all communications and information or data transmitted by, received from, or stored in any system at any time and without prior notice. No employee should have any expectation of privacy when using any of the Firm's computers, systems and networks, or other equipment.

Network Security The network shall be maintained to minimize the risk of corruption of data and unauthorized internal and external access. Firewalls, malware/virus/spyware protection and secure connections, with login ID's and strong password protection protocols, shall be in place, with the regular updating of security patches (as they become available) for all firm owned servers, desktops and laptops. All servers are maintained in a secure server room, accessible only by the Systems Administrator, Support Services, and the Executive Director.

Antivirus definition updates are performed automatically on a daily basis. Security patches are performed weekly and WSUS updates are performed on a monthly basis, unless there a critical patches, in which case these updates are performed immediately. Systems Administrator checks weekly to be sure all machines have been properly updated.

The Firm patches critical vulnerabilities that arise as to applications utilized by the Firm within a reasonable time following availability (with the goal of installing such patches within one week of availability.)

The Firm continues to work with IT consultants to strengthen its security and disaster recovery/business continuity protocols. Should a vulnerability be discovered, the Firm works with its network consultant to resolve this vulnerability within ninety (90) days.

Laptop/Removable Storage Device Security The Firm issues laptops and/or removable storage devices (i.e. thumb or flash drives) to attorneys, due to the need to work remotely when necessary. To protect the integrity and confidentiality of the information that may be maintained on laptops and removable storage devices and also prevent unauthorized access to the Firm's systems remotely through Citrix, the Firm employs a multi-level security protocol which includes:

1. All laptop hard drives and removable storage devices are encrypted using TruCrypt, requiring a unique Firm issued password access the laptop or removable storage device;
2. Laptops will be set to "time out" after thirty (30) minutes of inactivity, requiring the user to log back in to the system;
3. Laptops must not be left unattended at any time in any location outside of the Firm's offices and the Laptop User's locked residence, including but not limited to a car, court, airport or restaurant.

4. In the event a Firm laptop is stolen, it must immediately be reported to the Systems Administrator so that he can restrict any future access to the Firm systems through that laptop and also notify the appropriate local law enforcement personnel or agency as appropriate.

User ID's and Passwords The Firm's systems can be accessed only by entering a password. Passwords are intended to prevent unauthorized access to information and do not confer any right of privacy upon any Firm employee as to any information stored within any Firm system or electronic device (including e-mail and voicemail) that originated through non-client or Firm related use. So, even though Firm employees may maintain passwords for accessing Firm systems, this is solely for the protection of confidential and privileged client and Firm files; employees should have no expectation of privacy with regard to their usage of Firm systems.

To avoid unauthorized access and potential liability from breaches of confidentiality, positively no one other than an individual with an assigned User ID and password may access any Firm system. Any other system access requests (system integrators, consultants) must be approved in advance by the Executive Director or Systems Administrator. To ensure system security, the Firm may require additional levels authentication for system access from outside the Firm's offices.

For every employee, a unique user account is established by the Systems Administrator following the established approval process. Every user (PC or laptop) has a secure login, requiring entry of a unique strong password, which must be changed annually. All new permanent employees are issued a temporary password. This password takes the user to a screen requiring the user to change the temporary password to a unique strong password that conforms to the firm required format. Once the new password is created, the user can access firm systems. A user is unable to access firm system using the temporary password. The same password is used for both local and network access. Automated reminders are sent to all users concerning the changing of passwords prior to the annual cycle. For network access, the immediate prior password is kept in history. This prior password is blocked from being used for two consecutive annual cycles. Before being allowed to create a new password, the user must authenticate by entering the current password before entering the new password. In the event a new password is not entered, the user will be locked out of the system until reset by the System Administrator and a new password entered. Reset rights are limited to the Systems Administrator or his designated backup(s). Passwords must follow the established protocol established by the Firm (set forth below), and must be encrypted or otherwise securely stored.

Passwords cannot contain the user's account name or parts of the user's full name or his or her social security number and must have a minimum length of six (6) characters, and a complexity using 3 of the following 4 attributes: English upper case; English lower case; base 10 digit or numeric character (0-9); or non-alphabetic printable character. Note: Password entry is masked, preventing passwords from being fully displayed.

If a user has reason to believe that someone has gained unauthorized access to an account, the password should be changed and this should immediately be reported to the Executive Director. Subject to the following limited exception as it relates to non-Firm systems, employees must not share his/her password or otherwise allow any other person (employee or not) to use their account, password, or login for any Firm system, since they will be held responsible for anything that other person does, including activities which may be subject to disciplinary action or criminal prosecution. However, in the case where individual ID's and passwords are not available for non-firm systems, and if access if required by multiple individuals, these assigned ID's and passwords may be shared so that the

firm employees can conduct business as usual. Some examples of sites where shared ID/passwords are allowed are for e-filing and land registry searches.

Access Rights Only approved users will be allowed access to any Firm system or database. Windows operating systems require user authentication prior to access (password protected). System access and expansion of rights can only be authorized by the Executive Director and Systems Administrator.

The Firm has a policy of "segregation of duties" when it comes to assigning and approving user access to Firm systems whenever a new user needs access to the network, case management system or e-mail. This is to ensure that access approval and access administration functions are separate and security levels for staff are defined and documented. This separation of duties is as follows:

- Request Access – Attorney or Manager (conform with specific department protocol)
- Enable Access – System Administrator
- Verify Access – System Administrator

For the case management system, there is a hierarchy of security levels, with employees only given the minimum access necessary for them to perform all functions of their job. When an employee is terminated, all rights are immediately removed. In the case of a job change, rights are adjusted to the level of the position to which the employee has moved. System access and expansion of rights can only be authorized by the Executive Director or other individuals as set forth in a Firm policy.

"Watchguard" firewall technology is used to filter all network traffic. All external connections pass through "Watchguard" to detect and prevent unauthorized network access from outside sources. Windows servers, using domain permissions, prevent unauthorized access from internal sources.

All internal computers directly logged onto the network will automatically "time out" after fifteen (15) minutes of inactivity, requiring re-entry of the user's password. After 3 unsuccessful attempts to gain access, the user will be locked out of the system, requiring a login reset.

Remote Access Access to the Firm's system from remote locations through Citrix can only be approved by the Firm Managing Attorney, Practice Area Managing Attorney or Executive Director and is limited to Firm employees with a legitimate documented need to work remotely and such decision is within their sole and unfettered discretion.

Remote access to the Firm's network is limited to authorized personnel and comes through the firm's Citrix connection, which requires a client installation on the remote station. Once the client is installed, logging in would require the standard domain protocol, using a unique login ID and strong password.

Split tunneling is not permissible and is blocked through Citrix, which does not allow remote access to local resources.

It is against firm policy to work, store or access client files outside of the United States or its territories. This applies to any firm employee or any of its third party service providers.

System Monitoring At the discretion of the Executive Director, the System Administrator may monitor and review activity on any system, including, but not limited to, e-mail, voice mail, and Internet use. Such monitoring and review may be performed at any time without notice. Although individual passwords may be used by users to access Firm systems, users must understand that documents, e-mail messages, and voice mail messages are not private and may be accessed as authorized by the Executive Director at any time without prior notice.

Information Access Regardless of the nature of the use and form of the information, any and all information residing on Firm systems, as between a user and the Firm, is the sole property of the Firm, its clients and licensors, as applicable.

During the course of their employment with the Firm, employees will not copy, print, use or access Confidential, Personal, or Internal Information of the Firm or its clients unless it is performed for legitimate business purposes of the Firm and within the scope of their function with the Firm. Without regard to whether information such as e-mail, voice mail or document files are password-protected, no user may access, read, edit, print, copy, transfer or delete any information maintained by any other user unless specifically authorized by the Executive Director or Systems Administrator.

No employee is permitted to use any Firm system to access any third party's system or computer without specific authorization from the appropriate representative of that system's owner. Other organizations operating computing and network facilities that are reachable via the Firm systems may have their own policies governing the use of those resources. When accessing remote resources from the Firm systems, users are responsible for compliance with the policies set forth in this Policy, as well as the policies of the other organizations.

Persons leaving their employment with the Firm for any reason, may not copy, print or remove any Confidential, Personal, Internal Information or other information without the written authorization of a Managing Attorney.

Clean Desk/Clean Screen Policy The following elements of this policy are intended to ensure that all confidential electronic data remains secure, in particular when an employee are not present in their work areas.

- After thirty (30) minutes of inactivity, all desktops and laptops logged into the network are automatically locked with no information visible on screens;
- Users must lock their computers during business hours when their workspace is unattended for more than thirty (30) minutes (CTL/ALT/DELETE and Lock Computer); and shut down their computers at the end of the day.
- Passwords must not be posted on or under a computer or in any other accessible location;
- Incoming faxes are programmed to be stored in a network folder and not printed automatically. Neither an incoming fax nor the confirmation sheet for an outgoing fax will be printed. Confirmation of an outgoing fax will be delivered electronically to the sender's e-mail address.

Virus Detection Virus/malware detection software is installed on the Firm's servers and Firm-owned PC's and laptops. Updates are downloaded as frequently as they come available.

Under no circumstances should these programs be turned off or circumvented. E-mail messages and documents are common carriers of computer viruses. When a virus is discovered on any Firm system, the user must immediately cease operating the system and notify the Systems Administrator.

Electronic Mail (E-Mail) The Firm maintains e-mail and internet usage policies (see below), including a prohibition of usage for non-business purposes and for non-approved types of communication. These policies are incorporated in the Firm's Employee Manual, with all employees required to acknowledge (in writing) that they have read and understand these policies. The Employee Manual also sets forth specific actions the Firm can take against an employee for willful violation of this or any other Firm policy.

Internet Use The Internet is an important business resource that the Firm provides to employees to assist in research and information-gathering and to send information to clients should be used with this purpose in mind, although reasonable incidental personal use is permitted. The Internet should not be used to communicate client-privileged or sensitive information, unless through an approved secure client portal or extranet. Client privileged or sensitive information must never be transmitted to a personal email account. As with all electronic communications and Firm systems, no employee should have any expectation of privacy with respect to such information.

All systems with internet access, internet access accounts and any downloaded information, as between the Firm and the user, are the property of the Firm. The Firm reserves the right to review and disclose such records or information and to monitor and review on-line activities at any time without notice. Abuse of the privilege of using the internet may result in the loss of access or other corrective action, up to and including termination of employment.

In addition to the above, the Internet may not be used in a manner that would violate any law, regulation or Firm policy, including but not limited to its Anti-Harassment and Equal Opportunity Employment policies. The Firm prohibits and blocks access to sites in the following categories: Adult/Sexually explicit; criminal activities, gambling, hacking, illegal drugs, intolerance, phishing/fraud, spyware, violence, and weapons. Other sites may also be blocked at the Firm's discretion

Outgoing Email Attachments E-mail users have the ability to attach documents, parts of documents and spreadsheets to e-mail messages. Extreme care must be taken so that the attachment does not violate any confidentiality obligations and/or Firm policies, that it is being sent to the correct party and, that it is the correct attachment.

Transmission of Confidential Information (Encryption) When Confidential or non-public Personally Identifiable Information ("PII"), as defined in the Gramm-Leach-Bliley Act, 201 CMR 17.00, CGS Section 42-471 and Firm policy, is to be included in the subject line or body of an e-mail to external recipient or attachment(s) thereto, it is Firm policy that the above referenced e-mail be sent encrypted.

a. **Encryption of E-Mail** - Firm employees must manually encrypt an external e-mail using the firm approved protocol that provides for AES 256 bit encryption. Once the e-mail has been created, the sender must click on the "Encrypt Message" button located on the Outlook ribbon. Once any required documents have been attached as appropriate, the e-mail can be sent. Once sent, the recipient will receive an e-mail which will prompt them to create a password. Once the password has been accepted, the user will then be re-directed to their encrypted inbox. **Note: When a Social Security # or bank issued credit or debit card # appears in the subject line, body or attachment(s) of the outgoing e-mail, the email will automatically be encrypted by the spam filter.**

b. **Encryption of Removable Storage Devices** – If documentation is being provided to a client or opposing counsel on a removable storage device, the device must be encrypted/password protected.

E-Mail/Facsimile Confidentiality Disclaimers Both e-mail and facsimile transmissions will include a confidentiality and non-disclosure disclaimers which are system generated and automatically incorporated at the end of all e-mails (following the sender's signature) and at the bottom of all facsimile cover sheets.

Incoming Email Attachments Attachments received from outside the Firm with .exe, .com, .vbs, .pif, .bat, .shs, .vbe, .vb, .js, .scr, .mfi, .msp, .mst, .jse, .bas, .hta, .shb, .wsh, .wsf, or .wsc extensions often contain

viruses. Although the Firm has systems in place designed to intercept these messages, opening attachments with these extensions is a violation of the Firm's control policy and could infect the entire system. Users who receive e-mail messages containing any of the above extensions at the end of the attachment file name must not attempt to open the attachment. All such messages must immediately be forwarded to the System Administrator.

Software The Firm respects all software license rights for those computer programs that it uses. Users are not permitted to install unapproved software on a Firm PC or laptop. Software that is not approved by the Firm can adversely impact the operation of approved Firm software and compromise the integrity and security of the entire system. To maintain the Firm's compliance with its software licensing agreements, no copy of software may be used unless the Firm has a valid license and no installation may be performed except by the Systems Administrator. Users may not copy any software program from any Firm system, regardless of the intended use, without prior authorization of the Systems Administrator and proper registration of the copy. In addition, the development, storage or transmission of programs that destroy or alter programs or data of others without proper authorization is prohibited.

From time to time, the Systems Administrator will perform random software audits on all systems without notice to users. Any unauthorized software loaded without prior approval will immediately be removed without prior notice.

Employees are prohibited from duplicating any licensed software or related documentation for use on any Firm computer equipment unless the Firm is expressly authorized to do so by agreement with the licensor and the user has been granted permission by the Firm. Unauthorized duplication of software could result in both civil and criminal penalties under the United States Copyright Act.

Employees are not permitted to give Firm licensed software or CDs purchased by the Firm to anyone outside the Firm, including clients, family, or friends.

Voice Mail Firms' voicemail system may be accessed both internally and externally. All users' mailboxes are password protected with unique passwords.

Data Backup

The Firm utilizes an automated offsite backup configuration. Daily backups of data on Firm servers are backed up to an on-site Barracuda device, which is then synchronized to an offsite storage device located in the Barracuda Data Center (also replicated to another Barracuda Data Center). Backup logs are reviewed bi-weekly, unless an error e-mail notification is received. All backed up data is encrypted (AES 256 bit encryption), with only the Systems Administrator and the Executive Director having the key to decrypt the backed up data. In the event the backup encryption key or system password is compromised, the encryption key or password will be changed immediately upon notice, with the new encryption key or password being saved in password protected log file on the server. In the event the automated back-up do not run as scheduled, there will be an e-mail notification.

E-mail is archived utilizing Barracuda Archival System. SQL performs its own back-up of the Prolaw (case management) database each night.

In the event of a failure of the file server, data would be restored from the backup. In the unlikely event of a total loss of accessibility of all office space, all computer files are available through a restoration of the remote back-up of data to new servers.

Personnel

The policies and security expectations set forth in this document are incorporated in appropriate sections of the Firm Employee Manual, with all employees required to acknowledge (in writing) that they have read and understand these policies and expectations.

New Employees Following hiring, all new employees must review and provide a written acknowledgement of receipt of the Employee Manual (including e-mail and internet use, confidentiality/privacy of information, data security protocol, and Firm recourse for violations of policy or breach of any policy or standard established by the Firm), as well as participate in general orientation and training programs. In the event of violation of any policy by an employee, the Firm reserves the right to take appropriate action, up to and including termination.

Personnel Files Employee personnel files are maintained by the Executive Director in secure locked cabinets, with all personnel related documents printed to a secure, local printer (non-networked) located in the Executive Director's office. Compensation records are maintained by the Accounting Administrator in a secure office. The contents of these files are strictly confidential and access is limited to only authorized individuals. In accordance with state and federal regulations, all medical information is maintained in separate files and access is strictly limited and may be shared only on a need-to-know basis. All information or reference requests from outside sources regarding any past or present employees of the Firm will be referred to and handled exclusively by the Executive Director. Requests from third parties for information must be made in writing and contain authorization from the employee or former employee.

Departing Employees Immediately following termination of an employee, all passwords, log-in, user ID's, access cards and any other materials necessary to access Confidential, Personal or Internal Information will immediately be de-activated, preventing further access to the office and all Firm systems and said cards or other materials will be returned to the Assistant Director. Following a voluntary resignation, the Firm will determine on a case by case basis whether to waive notice and restrict access immediately. A person leaving the employment of the Firm may not remove any records, files, contacts, calendars or e-mail files in electronic or hardcopy format without approval from the Managing Attorney.

Prior to the departing employee's computer being assigned to another employee (new or current), the former employee's profile will be removed from the computer.

Record Management

The full Records Management Policy is incorporated herein by reference. Due to space considerations, some of the Firm's client and administrative files are stored off-site in secure record storage facilities. The files are housed in secure facilities and transported using bonded and insured employees in monitored and secure vehicles. These files may only be requested and accessed by authorized Firm employees for legitimate business purposes of the Firm. It is against firm policy for any client files to be stored outside of the United States or its territories.

Any and all documents containing Confidential, Personal, or Internal Information shall be stored in accordance with this policy and the Firm's Record Management Policy and, when no longer needed by the Firm, shall be destroyed in accordance with the standards established by the National Association of Information Destruction. The destruction of all files will be evidenced through Certificates of Destruction provided to the Firm by the vendor. Certificates of Destruction will be stored electronically on the Firm's network.

Pursuant to client directives and appropriate local and federal guidelines governing record retention, the Firm's Record Management Policy governs retention and destruction of physical and electronic records. The policy was designed to ensure compliance with federal and state laws and practices, to eliminate accidental or innocent destruction of records, and to facilitate the Firm's operations by promoting efficiency and freeing up of valuable storage space.

When PCs, laptops or copiers are "decommissioned" and replaced, PC's, laptops and copier hard drives are rendered unreadable and unusable and all data unrecoverable.

Discarded paper from all Firm offices containing personally identifiable information must be disposed of in locked recycling containers, which are shredded on-site by a third party vendor for shredding, with destruction being certified (Certificate of Destruction) per the standards established by the National Association of Information Destruction.

Client Credit Card Information

Clients have the option of paying bills and retainers via credit card. Credit card payments can be made in the following ways:

- Chip Card Reader (Reception Desk)
- Telephone
- Payment Portal on the firm's website
- Mail

Chip Card Reader

If a client comes to pay a bill in person in Springfield, his/her credit card will be swiped using the chip credit card terminal at the Reception Desk. An authorization will be signed and a receipt provided to the client. The signed slip will be delivered to Accounting to process. Retainers can immediately be processed by Reception and Accounting. Accounting will record the payment on a temporary matter. This temporary matter is monitored daily. If, after 2 business days, the matter has not been opened in Prolaw, Accounting Manager will follow-up with the Billing Attorney to either open the matter and return the retainer.

Telephone

Calls regarding credit card payments are transferred directly to Accounting. The Accounting staff will take the call and transfer this information onto an authorization form, which is then stapled to a bill.

Payment Portal

The firm utilizes a secure third party processing site for on-line credit card payments. When a payment is entered in the Payment Portal of the firm's website, Accounting receives an email from the merchant for processing, which contains a link to the receipt. Accounting will print out the receipt and enter the payment into the accounting system.

Mail

Completed authorization forms are stapled to the appropriate bill and prepared for processing. To process the payment, the accounting staff will log into the secured website of the credit card processor and enter the payment information. If approved, a receipt is printed and entered into the accounting software using the approval code provided. If rejected, a receipt is printed and the client contacted. The next business day, the accounting staff will log into the secured website of the credit card processor and the batch of the prior business day will be reconciled with the report from the accounting software.

General

Authorization forms that are completed following a telephone call are stored in a locked drawer in Accounting until it can be processed. Authorization forms for retainers received at the Reception Desk will be locked in a drawer until retrieved by the Accounting Department.

Following processing, authorization forms are stored in a locked cabinet in the Accounting Department until such time as the dispute period has expired, after which the vouchers are shredded. Dispute periods could extend up to 180 days. The Accounting Manager will review all retained authorization forms on a quarterly basis to ensure there are none that have been retained past the dispute deadline.

Redaction Policy

Redaction is the act of striking out or otherwise removing from public record or view any Personal Information not required by law. Personal Information shall include all nine (9) of the sequential numeric characters of a social security number, bank, financial account or loan numbers (including MERS numbers), driver's license numbers, state issued identification card numbers, credit or debit card numbers with access codes, and may include federal identification numbers, if any numbers can directly be connected to or associated with any specific individual. Subject to client directives to the contrary, Personal Information to be redacted also includes all bar codes that appear on any document referred to herein.

Redaction shall be performed upon all forms of documents and data accessible to public (including but not limited to web images, paper documents, certified copies, and metadata). **An original un-redacted version of the actual document provided by a client or third party (whether a true original or copy of an original) must not be redacted and will remain unaltered and maintained and safeguarded by the Firm in a location not accessible by the public.**

Redaction is completed by making a copy of the document requiring redaction and then obscuring the Personally Identifiable Information with a black box prior to making the "official" redacted copy to be used for filing or recording purposes. The method of redaction, whether manual or technological, shall be permanent so as to prevent the public or any unauthorized person from viewing the redacted information.

All redactions must be clearly evident, reflecting where information within a document has been obscured or removed. At the bottom of the first page of the document being redacted, a notation should appear indicating that a black box obscures redacted information. Once this has been done, a new copy of this redacted document should be made which can then be used for filing or recording. The marked up copy of the original document must then be destroyed**. Note: Merely making a copy of the redacted document does not eliminate the need of double checking to be sure information is not still visible. If necessary, this copy may need to be redacted again and recopied prior to filing or recording.**

The firm only uses Adobe Acrobat 9 Pro or Nuance PDF Converter to perform electronic redactions. Provided the document is "secured" when produced, redactions performed using these applications do not need any further action prior to transmission out of the office, since the document is "flattened" and no metadata is accessible.

Third Party Vendors and Temporary or Contract Employees

As needed, the Firm enters into contracts for essential services provided by third party vendors. These services are necessary for the continued operation of the Firm's business.

The Firm shall conduct reasonable due diligence to assess whether the prospective third party service provider or vendor is capable of safeguarding Confidential, Personal and/or Internal Information prior to engaging any person or entity who will have access to such information. Depending upon the nature of the services being provided, these vendors are given varying limited degrees of access to information within the control of the Firm.

While the majority of these vendors do not have access to any of the Firm's systems or client information, some have incidental access to client and employee information, The Firm limits access to only that information absolutely necessary for the vendors to provide the services for which they have been retained and removing access when no longer necessary.

At the commencement of any business arrangement, the Firm requires that each third party vendor execute an agreement containing confidentiality and/or non-disclosure provisions. In the absence of a formal agreement, a Confidentiality/Non-Disclosure Agreement is required.

Security Breach Policy

Pursuant to the Gramm-Leach-Bliley Act, Massachusetts General Laws c. 93H and 201 CMR 17.00 et seq, CGS 36a-701b, the Fair and Accurate Transactions Act of 2003 and Title 16, Part 681 Identity Theft Rules, Fair Credit Reporting Act by the Federal Trade Commission pursuant to 15 U.S.C 1681s(a)(1) (and the regulations issued thereunder) as they relate to financial institutions for which the Firm is a service provider, the Firm has taken steps to ensure that the services provided are conducted in accordance with reasonable policies and procedure by creating this Policy designed to protect the resources against a security breach. A breach can include, but not be limited to, actual or attempted use, access or loss of Confidential, Personal or Internal Information (data theft), compromise of information integrity (damage to data or unauthorized modification), theft or damage to physical IT assets including computers, and data storage devices, misuse of services, information, or assets, infection of systems by unauthorized or hostile software, an attempt at unauthorized access, unauthorized changes to organizational hardware, software, and reports of unusual system behavior.

The intent of the program is to take pro-active measures to identify potential fraudulent attempts to gain Confidential or Personal information, to verify that a security breach has occurred, determine how it occurred and the extent of the breach, take steps to minimize the impact of the breach, implement measures to prevent future breaches, and improve security strength and responsiveness. As such, employees and Third Party Vendors must immediately report any actual or suspected unauthorized access or use of Confidential, Personal, or Internal Information or any violations of any of the policies set forth herein to the Executive Director, as well as any other individuals designated pursuant to other applicable firm policies. It is unlawful and against the Firm's policy to retaliate against any person who reports a violation or suspected violation of this Policy or breach of Confidential, Personal or Internal Information or who cooperates in any review or investigation. Any such retaliation will result in disciplinary action by the Firm, up to and including termination of employment.

Per M.G.L.A. 93H § 3 - Duty to Report known security breach or unauthorized use of personal information

(a) A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to

the owner or licensor in accordance with this chapter. In addition to providing notice as provided herein, such person or agency shall cooperate with the owner or licensor of such information. Such cooperation shall include, but not be limited to, informing the owner or licensor of the breach of security or unauthorized acquisition or use, the date or approximate date of such incident and the nature thereof, and any steps the person or agency has taken or plans to take relating to the incident, except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may have been affected by the breach of security or unauthorized acquisition or use.

(b) A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the attorney general, the director of consumer affairs and business regulation and to such resident, in accordance with this chapter. The notice to be provided to the attorney general and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to: (i) the nature of the breach of security or unauthorized acquisition or use; (ii) the number of residents of the commonwealth affected by such incident at the time of notification; (iii) the name and address of the person or agency that experienced the breach of security; (iv) name and title of the person or agency reporting the
breach of security, and their relationship to the person or agency that experienced the breach of security; (v) the type of person or agency reporting the breach of security; (vi) the person responsible for the breach of security, if known; (vii) the type of personal information compromised, including, but not limited to, social security number, driver's license number, financial account number, credit or debit card number or other data; (viii) whether the person or agency maintains a written information security program; and (ix) any steps the person or agency has taken or plans to take relating to the incident,
including updating the written information security program. A person who experienced a breach of security shall file a report with the attorney general and the director of consumer affairs and business regulation certifying their credit monitoring services comply with section 3A.

The notice to be provided to the resident shall include, but shall not be limited to: (i) the resident's right to obtain a police report; (ii) how a resident may request a security freeze and the necessary information to be provided when requesting the security freeze; (iii) that there shall be no charge for a security freeze; and (iv) mitigation services to be provided pursuant to this chapter; provided, however, that said notice shall not include the nature of the breach of security or unauthorized acquisition or use, or the number of residents of the commonwealth affected by said breach of security or unauthorized access or use. The person or agency that experienced the breach of security shall provide a sample copy of the notice it sent to consumers to the attorney general and the office of consumer affairs and business regulation. A notice provided pursuant to this section shall not be delayed on grounds that the total number of residents affected is not yet ascertained. In such case, and where otherwise necessary to update or correct the information required, a person or agency shall provide additional notice as soon as practicable and without unreasonable delay upon learning such additional information.

Per M.G.L.A. 93H § 3A - Breaches of security including social security numbers; offer of credit monitoring services required

(a) If a person knows or has reason to know that said person experienced an incident that requires notice pursuant to section 3 and such breach of security includes a social security number, the person shall

contract with a third party to offer to each resident whose social security number was disclosed in the breach of security or is reasonably believed to have been disclosed in the breach of security, credit monitoring services at no cost to said resident for a period of not less than 18 months; provided, however, that if the person that has experienced a breach of security is a consumer reporting agency, then said consumer reporting agency shall contract with a third party to offer each resident whose social security number was disclosed in the breach of security or is reasonably believed to have been disclosed in the breach of security, credit monitoring services at no cost to such resident for a period of not less than 42 months. Said contracts shall not include reciprocal agreements for services in lieu of payment or fees. The person or agency shall provide all information necessary for the resident to enroll in credit monitoring services and shall include information on how the resident may place a security freeze on the resident's consumer credit report. (b) A person that experienced a breach of security shall not require a resident to waive the resident's right to a private right of action as a condition of the offer of credit monitoring services. (c) The department of consumer affairs and business regulation may promulgate regulations interpreting and applying this section.

D. <u>Other Provisions</u>

The Firm has designated the Executive Director to implement, supervise and maintain this Policy and the Executive Director shall be deemed the Data Security Coordinator as set forth in Massachusetts General Laws c. 93H and 201 CMR 17.00 et seq. (as the same may be amended from time to time).

This Policy and the measures detailed herein shall be reviewed at least annually, whenever there is a material change that implicates the security of such Confidential, Personal, or Internal Information and/or when the Firm determines such review is appropriate.