SAMPLE TEMPLATE

Massachusetts Written Information Security Plan

Developed by:

Jamy B. Madeja, Esq.
Erik Rexford
Buchanan & Associates
33 Mount Vernon Street
Boston, MA 02108

617-227-8410
www.buchananassociates.com
jmadeja@buchananassociates.com

Each business is required by Massachusetts law to evaluate security risks and solutions in relation to the size, scope and nature of the business and the attendant risks of unauthorized access to or use of personal information. Jamy B. Madeja, Esq. of Buchanan & Associates has developed this template as part of a tailored seminar presentation and as a sample for use by authorized businesses, not as a definitively sufficient "WISP" for any business. However, any business is welcome and encouraged to contact Buchanan & Associates for more information about an affordable way to obtain authorization to use the template, and for any relevant updates in this rapidly evolving area of law.

[INSERT COMPANY OR ENTITY NAME]
[NOTE: SELECT CAREFULLY WHERE MULTIPLE ENTITIES CO-OPERATE]

WRITTEN INFORMATION SECURITY PLAN

[INSERT DATE]

[NOTE: If any element of the following Sample/Template is not operationally feasible or appropriate for a particular business, be sure to delete that element from the company-specific WISP. Otherwise, it would be a liability exposure to establish a written policy and not to comply with it].

I. OBJECTIVE:

The objective of [INSERT COMPANY NAME] in the development and implementation of this comprehensive written information security program ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of personal information of residents of the Commonwealth of Massachusetts, including our employees, and to comply with our obligations under 201 CMR 17.00 (the "regulations"). The WISP sets forth our procedure for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of residents of the Commonwealth of Massachusetts.

For purposes of this WISP, "personal information" is as defined in the regulations: a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

II. PURPOSE:

The purpose of the WISP is to better: (a) ensure the security and confidentiality of personal information; (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and (c) protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

III. SCOPE:

In formulating and implementing the WISP, [INSERT COMPANY NAME] has addressed and incorporated the following protocols:

(1) identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information;

(2) assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;

(3) evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;

(4) designed and implemented a WISP that puts safeguards in place to minimize those risks, consistent with the requirements of 201 CMR 17.00; and

(5) implemented regular monitoring of the effectiveness of those safeguards.

IV. DATA SECURITY COORDINATOR:

[INSERT COMPANY NAME] has designated [INSERT EMPLOYEE NAME] to implement, supervise and maintain the WISP. This designated employee (the "Data Security Coordinator") will be responsible for the following:

a. Implementation of the WISP including all provisions outlined in Section VII: Daily Operational Protocol;

b. Training of all employees;

c. Regular testing of the WISP's safeguards;

d. Evaluating the ability of any of our third party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access, and requiring such third party service providers by contract to implement and maintain appropriate security measures;

e. Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information;

f. Conducting an annual training session for all owners, managers, employees and independent contractors, including temporary and contract employees who have access to personal information on the elements of the WISP. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with our requirements for ensuring the protection of personal information.

V. INTERNAL RISK MITIGATION POLICIES:

To guard against internal 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 the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

- We will only collect personal information of clients, customers or employees that is necessary to accomplish our legitimate business transactions or to comply with any and all federal, state or local regulations.

- Access to records containing personal information shall be limited to those employees whose duties, relevant to their job description, have a legitimate need to access said records, and only for this legitimate job-related purpose.

- Written and electronic records containing personal information shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements. Our frequent business records needs and associated retention and secure destruction periods are included in Attachment A: Common Business Record Needs **[*to be completed by Company after evaluating usual business record needs*]**.

- A copy of the WISP is to be distributed to each current employee and to each new employee on the beginning date of their employment. It shall be the employee's responsibility for acknowledging in writing, by signing the attached sheet, that he/she has received a copy of the WISP and will abide by its provisions. Employees are encouraged and invited to advise the WISP Data Security Coordinator of any activities or operations which appear to pose risks to the security of personal information. If the Data Security Coordinator is him or herself involved with these risks, employees are encouraged and invited to advise any other manager or supervisor or business owner.

- A training session for all current employees will be held on [INSERT DATE] to detail the provisions of the WISP.

- All employment contracts, where applicable, will be amended to require all employees to comply with the provisions of the WISP and to prohibit any nonconforming use of personal data as defined by the WISP

- Terminated employees must return all records containing personal data, in any form, in their possession at the time of termination. This includes all data stored on any portable device and any device owned directly by the terminated employee

- A terminated employee's physical and electronic access to records containing personal information shall be restricted at the time of termination. This shall include remote electronic access to personal records, voicemail, internet, and email access. All keys, keycards, access devices, badges, company IDs, business cards, and the like shall be surrendered at the time of termination.

- Disciplinary action will be applicable to violations of the WISP, irrespective of whether personal data was actually accessed or used without authorization.

- All security measures including the WISP shall be reviewed at least annually beginning March 1, 2010 to ensure that the policies contained in the WISP are adequate meet all applicable federal and state regulations.

- Should our business practices change in a way that impacts the collection, storage, and/or transportation of records containing personal information the WISP will be reviewed to ensure that the policies contained in the WISP are adequate meet all applicable federal and state regulations.

- The Data Security Coordinator or his/her designee shall be responsible for all review and modifications of the WISP and shall fully consult and apprise management of all reviews including any recommendations for improves security arising from the review.

- The Data Security Coordinator shall maintain a secured and confidential master list of all lock combinations, passwords, and keys. The list will identify which employee possess keys, keycards, or other access devices and that only approved employee have been provided access credentials

- The Data Security Coordinator or his/her designee shall ensure that access to personal information in restricted to approved and active user accounts.

- Current employees' user ID's and passwords shall conform to accepted security standards. All passwords shall be changed at least annually, more often as needed (e.g. seasonally).

- Employees are required to report suspicious or unauthorized use of personal information to a supervisor or the Data Security Coordinator

- Whenever there is an incident that requires notification pursuant to the Security Breach Notifications of Massachusetts General Law Chapter 93H: "Security Breaches" (copy attached), the Data Security Coordinator shall host a mandatory post-incident review of

events and actions taken, if any, in order to determine how to alter security practices to better safeguard personal information

VI. EXTERNAL RISK MITIGATION POLICIES:

- Firewall protection, operating system security patches, and all software products shall be reasonably up-to-date and installed on any computer that stores or processes personal information

- Personal information shall not be removed from the business premises in electronic or written form absent legitimate business need and use of reasonable security measures, as described in this policy

- All system security software including, anti-virus, anti-malware, and internet security shall be reasonably up-to-date and installed on any computer that stores or processes personal information.

- There shall be secure user authentication protocols in place that:
    - Control user ID and other identifiers;
    - Assigns passwords in a manner that conforms to accepted security standards, or applies use of unique identifier technologies;
    - Control passwords to ensure that password information is secure.

VII. DAILY OPERATIONAL PROTOCOL

This section of our WISP outlines our daily efforts to minimize security risks to any computer system that processes or stores personal information, ensures that physical files containing personal information are reasonable secured and develops daily employee practices designed to minimize access and security risks to personal information of our clients and/or customers and employees.

The Daily Operational Protocol is effective [*March 1, 2010]* and shall be reviewed and modified as deemed necessary at a meeting of the Data Security Coordinator and personnel responsible and/or authorized for the security of personal information. The review meeting shall take place on or before [*February 28, 2011]*. Any modifications to the Daily Operational Protocol shall be published in an updated version of the WISP. At the time of publication, a copy of the WISP shall be distributed to all current employees and to new hires on their date of employment.

A. **Recordkeeping Protocol:** We will only collect personal information of clients and customers and employees that is necessary to accomplish our legitimate business transactions or to comply with any and all federal and state and local laws.

- Within 30 days of the publication of the WISP or any update the Data Security Coordinator or his/her designee shall perform an audit of all relevant company records to determine which records contain personal information, assign those files to the appropriate secured storage location, and to redact, expunge or

Buchanan & Associates
33 Mount Vernon Street
Boston, MA 02108
www.buchananassociates.com
617.227.8410

otherwise eliminate all unnecessary personal information in a manner consistent with the WISP

- Any personal information stored shall be disposed of when no longer needed for business purposes or required by law for storage. Disposal methods must be consistent with those prescribed by the WISP

- Any paper files containing personal information of clients or employees shall be stored in a locked filing cabinet. Only department heads and the Data Security Coordinator will be assigned keys to filing cabinets and only those individuals are allowed access to the paper files. Individual files may be assigned to employees on an as-needed basis by the department supervisor.

- All employees are prohibited from keeping unsecured paper files containing personal information in their work area when they are not present (e.g. lunch breaks).

- At the end of the day, all files containing personal information are to be returned to the locked filing cabinet by department heads or the Data Security Coordinator.

- Paper or electronically stored records containing personal information shall be disposed of in a manner that complies with M.G.L. c. 93I sec. 2 (See Attachment D: Standards for disposal of records containing personal information; disposal by third party; enforcement) and as follows:

  (a) paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;

  (b) electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

- The following employees are authorized to access and assign to other employees files containing personal information:

Employee Name	*Department*

- Electronic records containing personal information shall not be stored or transported on any portable electronic device, sent or transmitted electronically

to any portable device, or sent or transported electronically to any computer, portable or not, without being encrypted. The only exception shall be where there is no reasonable risk of unauthorized access to the personal information or it is technologically not feasible to encrypt the data as and where transmitted.

- If necessary for the functioning of individual departments, the department head, in consultation with the Data Security Coordinator, may develop departmental rules that ensure reasonable restrictions upon access and handling of files containing personal information and must comply with all WISP standards. Departmental rules are to be published as an addendum to the WISP.

B. Access Control Protocol:

- All our computers shall restrict user access to those employees having an authorized and unique log-in ID assigned by the Data Security Coordinator

- All computers that have been inactive for 5 or more minutes shall require re-log-in

- After 5 unsuccessful log-in attempts by any user ID, that user ID will be blocked from accessing any computer or file stored on any computer until access privileges are reestablished by the Data Security Coordinator or his/her designee

- Access to electronically stored records containing personal information shall be electronically limited to those employees having an authorized and unique log-in ID assigned by the Data Security Coordinator

- Where practical, all visitors who are expected to access areas other than common retail space or are granted access to office space containing personal information should be required to sign-in with a Photo ID at a designated reception area where they will be assigned a visitor's ID or guest badge unless escorted at all times. Visitors are required to wear said visitor ID in a plainly visible location on their body, unless escorted at all times.

- Where practical, all visitors are restricted from areas where files containing personal information are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containing personal information are stored

- Cleaning personnel (or others on site after normal business hours and not also authorized to have access to personal information) are not to have access to areas where files containing personal information are stored

- All computers with an internet connections or any computer that stores or processes personal information must have a reasonably up-to-date version of software providing virus, anti-spyware and anti-malware protection installed and active at all times.

- An inventory of all company computers and handhelds authorized for personal information storage is contained in Attachment C: Computer and Handheld Inventory, which shall be made known only to the Data Security Coordinator and other managers on a "need to know" basis:

C. Third Party Service Provider Protocol: Any service provider or individual that receives, stores, maintains, processes, or otherwise is permitted access to any file containing personal information ("Third Party Service Provider") shall be required to meet the following standards as well as any and all standards of 201 CMR 17.00. (Examples include third parties who provide off-site backup storage copies of all our electronic data; paper record copying or storage service providers; contractors or vendors working with our customers and having authorized access to our records):

- Any contract with a Third Party Service Provider signed on or after March 1, 2010 shall require the Service Provider to implement security standards consistent with 201 CMR 17.00 (copy attached).

- It shall be the responsibility of the Data Security Coordinator to obtain reasonable confirmation that any Third Party Service Provider is capable of meeting security standards consistent with 201 CMR 17.00.

- Any existing contracts with Third Party Service shall be reviewed by the Data Security Coordinator. These Service Providers shall meet the security standards consistent with 201 CMR 17.00 by March 1, 2012 or other Service Providers will be selected, when feasible to do so.

- A list of currently known third party service providers is contained in Attachment B: Third Party Service Providers

VIII. Breach of Data Security Protocol: Should any employee know of a security breach at any of our facilities, or that any unencrypted personal information has been lost or stolen or accessed without authorization, or that encrypted personal information along with the access

code or security key has been acquired by an unauthorized person or for an unauthorized purpose, the following protocol is to be followed:

- Employees are to notify the Data Security Coordinator or department head in the event of a known or suspected security breach or unauthorized use of personal information.

- The Data Security Coordinator shall be responsible for drafting a security breach notification to be provided to the Massachusetts Office of Consumer Affairs and Business Regulation and the Massachusetts Attorney General's office. The security breach notification shall include the following:

    - A detailed description of the nature and circumstances of the security breach or unauthorized acquisition or use of personal information;
    - The number of Massachusetts residents affected at the time the notification is submitted;
    - The steps already taken relative to the incident;
    - Any steps intended to be taken relative to the incident subsequent to the filing of the notification; and
    - Information regarding whether law enforcement officials are engaged in investing the incident

Attachment A:
Common Business Records Needs/Associated Retention and Secure Destruction Periods

Record	Time Retained	Destroyed On/Destroyed By

Attachment B:
Third Party Service Providers

Company Name	Contact Information	Services Provided	Contract Date

Attachment C – TO BE KEPT CONFIDENTIAL EXCEPT NEED TO KNOW BASIS:
Computer and Handheld Inventory

Computer Make/Model	*Location*	*Employee Assignment*

Attachment D:

Chapter 93I: Section 2. Standards for disposal of records containing personal information; disposal by third party; enforcement

[Text of section added by 2007, 82, Sec. 17 effective February 3, 2008. See 2007, 82, Sec. 19.]

Section 2. When disposing of records, each agency or person shall meet the following minimum standards for proper disposal of records containing personal information:

(a) paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;

(b) electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

Any agency or person disposing of personal information may contract with a third party to dispose of personal information in accordance with this chapter. Any third party hired to dispose of material containing personal information shall implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation and disposal of personal information.

Any agency or person who violates the provisions of this chapter shall be subject to a civil fine of not more than $100 per data subject affected, provided said fine shall not exceed $50,000 for each instance of improper disposal. The attorney general may file a civil action in the superior or district court in the name of the commonwealth to recover such penalties.

Buchanan & Associates
33 Mount Vernon Street
Boston, MA 02108
www.buchananassociates.com
617.227.8410

PART I. ADMINISTRATION OF THE GOVERNMENT

TITLE XV. REGULATION OF TRADE

CHAPTER 93H. SECURITY BREACHES
[Chapter 93H added by 2007, 82, Sec. 16 effective October 31, 2007.]

Chapter 93H: Section 3. Duty to report known security breach or unauthorized use of personal information

[Text of section added by 2007, 82, Sec. 16 effective October 31, 2007.]

Section 3. (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, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the commonwealth affected by such incident at the time of notification, and any steps the person or agency has taken or plans to take relating to the incident.

Upon receipt of this notice, the director of consumer affairs and business regulation shall identify any relevant consumer reporting agency or state agency, as deemed appropriate by said director, and forward the names of the identified consumer reporting agencies and state agencies to the notifying person or agency. Such person or agency shall, as soon as practicable and without unreasonable delay, also provide notice, in accordance with this chapter, to the consumer reporting agencies and state agencies identified by the director of consumer affairs and business regulation.

The notice to be provided to the resident shall include, but not be limited to, the consumer's right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies, provided however, that said notification shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use.

(c) If an agency is within the executive department, it shall provide written notification of the nature and circumstances of the breach or unauthorized acquisition or use to the information technology division and the division of public records as soon as practicable and without unreasonable delay following the discovery of a breach of security or unauthorized acquisition or use, and shall comply with all policies and procedures adopted by that division pertaining to the reporting and investigation of such an incident.