



DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

COMMONWEALTH OF MASSACHUSETTS
OFFICE OF CONSUMER AFFAIRS & BUSINESS REGULATION
10 Park Plaza, Suite 5170 Boston, MA 02116
(617) 973-8700 FAX (617) 973-8799 TTY/TDD (617) 973-8790
www.mass.gov/consumer

DANIEL O'CONNELL
SECRETARY OF HOUSING AND
ECONOMIC DEVELOPMENT

DANIEL C. CRANE
UNDERSECRETARY OF
CONSUMER AFFAIRS AND
BUSINESS REGULATION

Small Business Guide For Formulating A Comprehensive Written Information Security Program

While the contents of any comprehensive written information security plan required by 201 CMR 17.00 must always satisfy the detailed provisions of those regulations; and while compliance with those regulations will be evaluated taking into account (i) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program, (ii) the amount of resources available to such person, (iii) the amount of stored data, and (iv) the need for security and confidentiality of both consumer and employee information; the Office of Consumer Affairs and Business Regulation is issuing this guide to help small business in their compliance efforts. **This Guide is not a substitute for compliance with 201 CMR 17.00.** It is simply an aid to be adapted to the particular circumstances of a particular small business or individual that handles "personal information" and is trying to come up with a conforming plan.

Having in mind that wherever there is a conflict found between this guide and the provisions of 201 CMR 17.00, it is the latter that will govern, we set out below this "guide" to devising a security plan (references below to "we" and "our" are references to the small business or individual to whom the real plan will relate):

COMPREHENSIVE WRITTEN SECURITY PLAN

I. OBJECTIVE:

Our objective, in the development and implementation of this comprehensive written information security plan ("Plan"), is to create effective administrative, technical and physical safeguards for the protection of personal information of residents of the Commonwealth of Massachusetts, and to comply with our obligations under 201 CMR 17.00. The Plan sets forth our procedure for evaluating 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 Plan, "personal information" means 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,



Better businesses. Smarter consumers.



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. PURPOSES:

The purpose of the Plan is to:

- (a) Ensure the security and confidentiality of personal information;
- (b) Protect against any anticipated threats or hazards to the security or integrity of such information
- (c) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

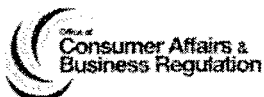
III. SCOPE:

In formulating and implementing the Plan, we will (1) identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information; (3) evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks; (4) design and implement a plan that puts safeguards in place to minimize those risks, consistent with the requirements of 201 CMR 17.00; and (5) regularly monitor the effectiveness of those safeguards:

IV. DATA SECURITY COORDINATOR:

We have designated _____ to implement, supervise and maintain the Plan. That designated employee (the "Data Security Coordinator") will be responsible for:

- a. Initial implementation of the Plan;
- b. Training employees;
- c. Regular testing of the Plan's safeguards;
- d. Evaluating the ability of each of our third party service providers to protect, in the manner required by 201 CMR 17.00, the personal information to which we have permitted them access; and taking the steps reasonably necessary to ensure that such third party service provider is applying to such personal



information protective security measures at least as stringent as those required to be applied to such information under 201 CMR 17.00.

- e. Reviewing the scope of the security measures in the Plan 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 Plan. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with the firm's requirements for ensuring the protection of personal information.

V. INTERNAL RISKS:

To combat 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. To the extent that any of these measures require a phase-in period, such phase-in must be completed on or before January 1, 2010:

Internal Threats

- A copy of the Plan must be distributed to each employee who shall, upon receipt of the Plan, acknowledge in writing that he/she has received a copy of the Plan.
- There must be immediate retraining of employees on the detailed provisions of the Plan.
- Employment contracts must be amended immediately to require all employees to comply with the provisions of the Plan, and to prohibit any nonconforming use of personal information during or after employment; with mandatory disciplinary action to be taken for violation of security provisions of the Plan (*The nature of the disciplinary measures may depend on a number of factors including the nature of the violation and the nature of the personal information affected by the violation*).
- The amount of personal information collected must be limited to that amount reasonably necessary to accomplish our legitimate business



purposes, or necessary to us to comply with other state or federal regulations.

- Access to records containing personal information shall be limited to those persons who are reasonably required to know such information in order to accomplish your legitimate business purpose or to enable us comply with other state or federal regulations.
- Electronic access to user identification after multiple unsuccessful attempts to gain access must be blocked.
- All security measures shall be reviewed at least annually, or whenever there is a material change in our business practices that may reasonably implicate the security or integrity of records containing personal information. The Data Security Coordinator shall be responsible for this review and shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review.
- Terminated employees must return all records containing personal information, in any form, that may at the time of such termination be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)
- A terminated employee's physical and electronic access to personal information must be immediately blocked. Such terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the firm's premises or information. Moreover, such terminated employee's remote electronic access to personal information must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated. The Data Security Coordinator shall maintain a highly secured master list of all lock combinations, passwords and keys.
- Current employees' user-ID's and passwords must be changed periodically.
- Access to personal information shall be restricted to active users and active user accounts only.



- Employees are encouraged to report any suspicious or unauthorized use of customer information.
- Whenever there is an incident that requires notification under M.G.L. c. 93H, §3, there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in our security practices are required to improve the security of personal information for which we are responsible.
- Employees are prohibited from keeping open files containing personal information on their desks when they are not at their desks.
- At the end of the work day, all files and other records containing personal information must be secured in a manner that is consistent with the Plan's rules for protecting the security of personal information.
- Each department shall develop rules (bearing in mind the business needs of that department) that ensure that reasonable restrictions upon physical access to records containing personal information are in place, including a written procedure that sets forth the manner in which physical access to such records in that department is to be restricted; and each department must store such records and data in locked facilities, secure storage areas or locked containers.
- Access to electronically stored personal information shall be electronically limited to those employees having a unique log-in ID; and re-log-in shall be required when a computer has been inactive for more than a few minutes.
- Visitors' access must be restricted to one entry point for each building in which personal information is stored, and visitors shall be required to present a photo ID, sign-in and wear a plainly visible "GUEST" badge or tag. Visitors shall not be permitted to visit unescorted any area within our premises that contains personal information.
- Paper or electronic records (including records stored on hard drives or other electronic media) containing personal information shall be disposed



of only in a manner that complies with M.G.L. c.
93I.



VI. EXTERNAL RISKS

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately. To the extent that any of these measures require a phase-in period, such phase-in must be completed on or before January 1, 2010:

External Threats

- There must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information, installed on all systems processing personal information.
- There must be reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing personal information.
- To the extent technically feasible, all personal information stored on laptops or other portable devices must be encrypted, as must all records and files transmitted across public networks or wirelessly, to the extent technically feasible. Encryption here means the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the Office of Consumer Affairs and Business Regulation.
- All computer systems must be monitored for unauthorized use of or access to personal information.
- There must be secure user authentication protocols in place, including: (1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (3) control of data security passwords to ensure that such passwords are kept in a location



and/or format that does not compromise the security of the data they protect; (4) restriction of access to active users and active user accounts only; and (5) blocking of access to user identification after multiple unsuccessful attempts to gain access.

- The secure access control measures in place must include assigning unique identifications plus passwords, which are not vendor-supplied default passwords, to each person with computer access to personal information.





DEVAL L. PATRICK
GOVERNOR

TIMOTHY P. MURRAY
LIEUTENANT GOVERNOR

COMMONWEALTH OF MASSACHUSETTS
OFFICE OF CONSUMER AFFAIRS & BUSINESS REGULATION

10 Park Plaza, Suite 5170 Boston, MA 02116
(617) 973-8700 FAX (617) 973-8799 TTY/TDD (617) 973-8790
www.mass.gov/consumer

DANIEL O'CONNELL
SECRETARY OF HOUSING AND
ECONOMIC DEVELOPMENT

DANIEL C. CRANE
UNDERSECRETARY OF
CONSUMER AFFAIRS AND
BUSINESS REGULATION

201 CMR 17.00 COMPLIANCE CHECKLIST

The Office of Consumer Affairs and Business Regulation has compiled this checklist to help small businesses in their effort to comply with 201 CMR 17.00. **This Checklist is not a substitute for compliance with 201 CMR 17.00.** Rather, it is an aid to be adapted to the particular circumstances of a particular small business or individual that handles “personal information,” and that is trying to come up with a conforming plan. Each item, in a question and answer format, highlights a feature of those regulations that requires attention in order for a plan to be compliant.

The Comprehensive Written Information Security Program (WISP)

- Do you have a comprehensive, written information security program (“WISP”) applicable to all records containing personal information about a resident of the Commonwealth of Massachusetts (“PI”)?
- Does the WISP include administrative, technical, and physical safeguards for PI protection?
- Have you designated one or more employees to maintain and supervise WISP implementation and performance?
- Have you identified the paper, electronic and other records, computing systems, and storage media, including laptops and portable devices, that contain personal information?
- Have you chosen, as an alternative, to treat all your records as if they all contained PI?
- Have you identified and evaluated reasonably foreseeable internal and external risks to paper and electronic records containing PI?
- Have you evaluated the effectiveness of current safeguards?
- Does the WISP include regular ongoing employee training, and procedures for monitoring employee compliance?
- Does the WISP include disciplinary measures for violators?
- Does the WISP include policies and procedures for when and how records containing PI should be allowed to be kept, accessed or transported off your business premises?



Better businesses. Smarter consumers.



- Does the WISP provide for immediately blocking terminated employees' physical and electronic access to PI records (including deactivating their passwords and user names)?
- Have you taken all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such personal information in the manner provided for in 201 CMR 17.00?
- Have you taken all reasonable steps to ensure that your third party service providers with access to personal information are applying to such personal information protective security measures at least as stringent as those required to be applied to personal information under 201 CMR 17.00?
- Is the amount of PI that you have collected limited to the amount reasonably necessary to accomplish your legitimate business purposes, or to comply with state or federal regulations?
- Is the length of time that you are storing records containing PI limited to the time reasonably necessary to accomplish your legitimate business purpose or to comply with state or federal regulations?
- Is access to PI records limited to those persons who have a need to know in connection with your legitimate business purpose, or in order to comply with state or federal regulations?
- In your WISP, have you specified the manner in which physical access to PI records is to be restricted?
- Have you stored your records and data containing PI in locked facilities, storage areas or containers?
- Have you instituted a procedure for regularly monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of PI; and for upgrading it as necessary?
- Are your security measures reviewed at least annually, or whenever there is a material change in business practices that may affect the security or integrity of PI records?
- Do you have in place a procedure for documenting any actions taken in connection with any breach of security; and does that procedure require post-incident review of events and actions taken to improve security?



Additional Requirements for Electronic Records

- Do you have in place secure authentication protocols that provide for:
 - Control of user IDs and other identifiers?
 - A reasonably secure method of assigning/selecting passwords, or for use of unique identifier technologies (such as biometrics or token devices)?
 - Control of data security passwords such that passwords are kept in a location and/or format that does not compromise the security of the data they protect?
 - Restricting access to PI to active users and active user accounts?
 - Blocking access after multiple unsuccessful attempts to gain access?
- Do you have secure access control measures that restrict access, on a need-to-know basis, to PI records and files?
- Do you assign unique identifications plus passwords (which are not vendor supplied default passwords) to each person with computer access; and are those IDs and passwords reasonably designed to maintain the security of those access controls?
- Do you, to the extent technically feasible, encrypt all PI records and files that are transmitted across public networks, and that are to be transmitted wirelessly?
- Do you encrypt all PI stored on laptops or other portable devices?
- Do you have monitoring in place to alert you to the occurrence of unauthorized use of or access to PI?
- On any system that is connected to the Internet, do you have reasonably up-to-date firewall protection for files containing PI; and operating system security patches to maintain the integrity of the PI?
- Do you have reasonably up-to-date versions of system security agent software (including malware protection) and reasonably up-to-date security patches and virus definitions?
- Do you have in place training for employees on the proper use of your computer security system, and the importance of PI security?

