CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

COMMONWEALTH OF MASSACHUSETTS
Office of Consumer Affairs and Business Regulation
10 Park Plaza, Suite 5170, Boston, MA 02116
(617) 973-8700 FAX (617) 973-8799
www.mass.gov/consumer

JAY ASH
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

JOHN C. CHAPMAN
UNDERSECRETARY

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 designed as a useful tool to aid in the development of a written information security program for a small business or individual that handles "personal information." Each item, presented in question form, highlights a feature of 201 CMR 17.00 that will require proactive 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 kept, accessed or transported off your business premises?
- 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 reasonable steps to select and retain a third-party service provider that is capable of maintaining appropriate security measures consistent with 201 CMR 17.00?
- Have you required such third-party service provider by contract to implement and maintain such appropriate security measures?
- 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, to the extent technically feasible, 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?