

MASSACHUSETTS DATA SECURITY COMPLIANCE CHECKLIST
(as of November 2009)

The checklist below outlines the items required to achieve compliance with the final data security regulations issued in Massachusetts (201 CMR 17.00 et seq.). While the effective date of the regulations have been delayed a number of times, they currently are set to become effective March 1, 2010. Note also that the state has made a number of revisions to the regulations since they were originally issued. A discussion of some of the changes can be found at <http://www.jacksonlewis.com/legalupdates/article.cfm?aid=1828>. This checklist represents the latest version of the regulations issued, as of November 13, 2009.

The Regulations establish minimum standards for protecting and storing personal information about Massachusetts residents contained in paper or electronic format. The regulations apply to any businesses or individuals that own or license personal information about a Massachusetts resident. The Regulations define "own or license" to mean "receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment."

The chart below provides a checklist to assist in the compliance process. When evaluating whether the Company's program meets the requirements under the Regulations, the following items should be taken into account:

- the size, scope and type of business,
- the amount of resources available,
- the amount of stored data, and
- the need for security and confidentiality of both consumer and employee information.

**Massachusetts Data Security Compliance Checklist:
Minimum “Information Security Program” Requirements**

<i>Requirements for Every Information Security Program</i>	<i>Status</i>
<p>In General:</p> <ul style="list-style-type: none"> ➤ Program must be in writing. ➤ Program must be developed, implemented, maintained and monitored. ➤ Program must have administrative, technical, and physical safeguards and be reasonably consistent with safeguards for protection of personal information and information of a similar character set forth in any applicable state or federal regulations 	
<p>Appoint Key Person: Designate one or more employees to maintain the program.</p>	
<p>Risk Assessment:</p> <ul style="list-style-type: none"> ➤ Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of personal information ➤ Evaluate and improve current safeguards for addressing identified risks through such steps as: <ul style="list-style-type: none"> ○ ongoing employee (including temporary and contract employee) training; ○ ensuring employee compliance with policies and procedures; ○ detecting and preventing security system failures. 	
<p>External Employee Access: Develop security policies addressing whether and how employees may keep, access and transport records containing personal information outside of the Company’s business premises.</p>	
<p>Discipline: Impose discipline when the Company’s program is violated.</p>	
<p>Protocols for Termination of Employment: Establish procedures to immediately terminate access by terminated employees to personal information by physical or electronic access, such as deactivating their passwords and user names, changing locks, retrieving IDs, and so on.</p>	

<p>Oversee Service Providers. A service provider is "any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to the Regulations.</p> <p>To adequately oversee service providers, the Regulations require that covered entities:</p> <ol style="list-style-type: none"> 1. Take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information consistent with the Regulations <u>and</u> any applicable federal regulations; and 2. Require such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract will be deemed to satisfy this requirement even if the contract does not require the service provider to maintain the appropriate safeguards, as long as the contract was entered into no later than March 1, 2010. However, it is recommended that these contracts be amended to include similar provisions as soon as possible, as there may be similar requirements under federal or state law (such as HIPAA or data security laws in Maryland, Oregon or Nevada). 	
<p>Physical Access and Storage: Impose reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers.</p>	
<p>Monitor Security Program Performance: Establish procedure for regular monitoring to ensure program is operated in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information, and upgrade information safeguards as necessary.</p>	
<p>Annual Assessment of Scope of Security Program: At least once per year (or whenever there is a material change in business practices that reasonably affects the security or integrity of records containing personal information), reviewing the scope of the program's security measures for adequacy.</p>	
<p>Document Breach Response: Document steps to respond to breach of security and post-breach review of events and actions taken, if any, to make changes in program.</p>	

<p><i>Additional Requirements if Personal Information is Electronically Stored or Transmitted</i></p>	<p>Status</p>
<p>The additional elements below apply at a minimum, <u>and to the extent feasible</u>:</p> <ul style="list-style-type: none"> ➤ to every person that owns or licenses personal information about a resident of the Commonwealth <u>and</u> electronically stores or transmits such information, and ➤ be part of a security system established and maintained by such person that covers the person's computers, <u>including</u> any wireless system. 	
<p>Implement Secure User Authentication Protocols that:</p> <ul style="list-style-type: none"> ➤ control user IDs and other identifiers; ➤ reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; ➤ 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; ➤ restrict access to active users/user accounts only; and ➤ block access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system. 	
<p>Implement Secure Access Control Measures that:</p> <ul style="list-style-type: none"> ➤ restrict access to personal information to those who need such information to perform their job duties; and ➤ assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls. 	
<p>Encryption: Encrypt all transmitted records and files containing personal information that will travel across public networks, and transmitted wirelessly.</p>	
<p>Mandatory Encryption for Portable Devices: Encrypt all laptops or other portable devices that store personal information.</p>	
<p>Monitor IT System Use and Access: Perform reasonable monitoring for unauthorized use of <u>or</u> access to personal information.</p>	

Firewall/Malware/Virus Protection: Implement reasonably up-to-date firewall, system security agent software, malware and reasonably up-to-date patches and virus definitions that are reasonably designed to maintain the integrity of the personal information on a system connected to Internet. System also should be designed to receive current security updates on a regular basis.	
Training: Train and educate employees on the proper use of the computer security system and the importance of personal information security.	