

## **New Massachusetts Law requires all business to protect personal information.**

*By Julianne McLaughlin*

*Dated: May 21, 2009*

*Massachusetts laws require all business to protect personal information. New law will go into effect January 1, 2010. Now is the time to prepare your business for this enactment of this important law.*

Massachusetts adopted regulations on Sept. 22, 2008, that will require businesses, wherever located, that store or use information about Massachusetts residents, to implement comprehensive information security programs by January 1, 2010. Compliance with this new law, referred to as 201 CMR 17, needs to be met by persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records.

What is considered personal information:

If you store a Massachusetts resident last name and first name on computer or on paper AND also store any of the following information, this is considered "personal information" and the new law is applicable to you business.

1. Social Security number
2. Driver's License number
3. Financial Account number (credit card, debit card)
4. Access code that would allow you to access that person financial information

Requirements and Blue LAN Group, Inc.'s recommendations:

- Designate one employee to design, implement and coordinate the maintenance of the comprehensive information security program;
- Identify and assess internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information in each relevant area of the business's operations
- Develop a security policy for employees who telecommute that take into account whether and how such employees should be allowed to keep, access and transport data containing personal information.
- Consider implementing disciplinary measures for violations of the comprehensive information security program rules.
- Prevent terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.
- Take all reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information, including (i) selecting and retaining service providers that are capable of maintaining safeguards for personal information; and (ii) contractually requiring service providers to maintain such safeguards. Prior to permitting third-party service providers access to personal information, the person permitting such access shall obtain from the third-party service provider a written certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of these regulations.
- Collect the minimum amount of personal information necessary to accomplish the legitimate purpose for which it was collected; retain such information for the minimum time necessary to accomplish such purpose; and permit access to the smallest number of persons who are reasonably required to know such information in order to accomplish such purpose.
- Inventory all paper, electronic and other records, computing systems, and storage media, including

laptops and portable devices used to store personal information, to identify those records containing personal information.

- Regularly monitor and audit employee access to personal information in order to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information.
- Review the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.
- Document all responsive actions taken in connection with any incident involving a breach of security and document all post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of 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 (including email) 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.

Blue LAN Group, Inc. is a full service information technology, web design/development, business services, social media/networking consulting company that provides support to small/medium size businesses, non-profits and schools in Boston, Nashua/NH, Providence/RI, San Diego and San Francisco/CA.

BLG- your one stop for all your technology needs!

###

Blue LAN Group, Inc. is a full service IT consulting company that provides support to small/medium size businesses, non-profits and schools.

Category	Computers, Security, Business
Tags	security, massachusetts laws, personal information, Computers, it security
Email	<a href="#">Click to contact author</a>
Phone	877-258-7711
City/Town	Plymouth
State/Province	Massachusetts
Country	United States
Link	<a href="http://prlog.org/10241298">http://prlog.org/10241298</a>



Scan this QR Code with your SmartPhone to-  
\* Read this news online  
\* Contact author  
\* Bookmark or share online