TBG Security's Statement of Compliance with 201 CMR 17.00

TBG Security, as your IT security provider, has always kept the security of our customer's data and password information under the highest level of cryptographic encryption. In compliance with the new data protection law that became effective in Massachusetts as of March, 1 2010 we offer this statement as part of your compliance.

(1) TBG Security has developed, implemented, and maintains a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to;
   (a) it's size, scope and type of business
   (b) it's available resources
   (c) the amount of stored data; and
   (d) the need for security and confidentiality of both consumer and employee information.

(2) The safeguards contained in our program are consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which TBG Security may be regulated.

(3) TBG Security has designating one employee to maintain the comprehensive information security program.

(4) TBG Security has identified and assessed reasonably foreseeable internal and 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.

(5) TBG Security has developed security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.

(6) TBG Security will impose disciplinary measures for violations of the comprehensive information security program rules.

(7) TBG Security does not allow terminated employees access to records containing personal information.

(8) TBG Security has taken reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations

(9) TBG Security has placed reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers.

(10) TBG Security regularly monitors our CISP 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; and upgrading information safeguards as necessary to limit risks.

(11) TBG Security reviews 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.

(12) TBG Security documents responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

17.04: **Computer System Security Requirements**

TBG Security's written, comprehensive information security program establishes and maintenances a security system covering its computers, including any wireless system that, at a minimum, and to the extent technically feasible, shall have the following elements:

(1) Secure user authentication protocols including:

(a) control of user IDs and other identifiers;

(b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

(c) 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;

(d) restricting access to active users and active user accounts only; and

(e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

(2) Secure access control measures that:

(a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and

(b) 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;

(3) TBG Security encrypts all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

(4) TBG Security monitors our systems, for unauthorized use of or access to personal information.

(5) TBG Security encrypts all personal information stored on laptops or other portable devices;

(6) For files containing personal information on a system that is connected to the Internet, TBG Security employs up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.

(7) TBG Security employs up-to-date versions of system security agent software which include malware protection and up-to-date patches and virus definitions.

(8) TBG Security provides education and training of employees on the proper use of the computer security system and the importance of personal information security.

For more information on how we achieved compliance or how we can assist your organization in achieving compliance with 201 CMR 17.00 please contact us at compliance@tbgsec.com