Information Security Plan

This Information Security Plan (Plan) describes Mountain State School of Massage safeguards to protect information and data (Protected Information) in compliance with the Financial Services Modernization Act of 1999, also known as the Gramm Leach Bliley Act, 15 U.S.C. Section 6801. These safeguards are provided to:

- Protect the security and confidentiality of Protected Information;
- Protect against anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of Protected Information that could result in substantial harm or inconvenience to any customer.

This Information Plan also provides for mechanisms to:

- Identify and assess the risks that may threaten Protected Information maintained by Mountain State School of Massage;
- Designate employee responsible for coordinating the program;
- Design and implement a safeguards program;
- Adjust the plan to reflect changes in technology, the sensitivity of Protected Information, and internal or external threats to information security;

Identification and Assessment of Risks to Customer Information

Mountain State School of Massage Therapy recognizes that it has both internal and external risks. These risks include, but are not limited to:

- Unauthorized access of Protected Information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties

Employee Responsible for Coordinating the Program

The Director will be responsible for coordinating the program.

Safeguards Program

I - Employee Management and Training

During employee orientation, each new employee in departments that handle protected information will receive proper training on the importance of confidentiality of protected information. Each new employee will also be trained in the proper use of computer information and passwords. Further, departments with more than one employee, responsible for maintaining protected information, will provide ongoing updates to its staff. These training efforts should help minimize risk and safeguard covered data and information security.

II - Physical Files

All files and physical documents with protected information will be stored in locked fireproof file cabinets. These cabinets are located in offices with limited access; only authorized personnel have keys to these offices. The offices will always be closed and locked when unoccupied. Authorized personnel are responsible for ensuring that no unauthorized personnel gain access to these files or the information in them. Paper documents that contain protected information are shredded at time of disposal.

III - Information Systems

Information systems include network and software design, as well as information processing, storage, transmission, retrieval, and disposal MSSM has a password protected, encrypted network. It currently does not make wireless access available to students; if it does, the student wireless access will be hosted on a separate network - one that contains no protected information. MSSM will take reasonable and appropriate steps consistent with current technological developments to make sure that all protected information is secure and to safeguard the integrity of records in storage and transmission.

IV - Management of System Failures

The school will maintain effective systems to prevent, detect, and respond to attacks, intrusions and other system failures. Such systems will include staying current with security patches made available by software vendors; maintaining appropriate filtering or firewall technologies; alerting those with access to covered data of threats to security; imaging documents and shredding paper copies. Data will be backed up every ten minutes to a secure offsite server, and every hour to an encrypted local external hard drive as well as other reasonable measures to protect the integrity and safety of information systems.

V - Continuing Evaluation and Adjustment

This plan will be subject to periodic review and adjustment, especially when due to the constantly changing technology and evolving risks. The Director will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of student/customer data and internal or external threats to information security.

Effective: 07/1/2019 | Updated: 12/16/2020

601 50TH STREET, CHARLESTON, WV 25304
Phone: 304-926-8822 · Fax: 304-926-8837
info@mtnstmassage.com · www.mtnstmassage.com