# Data Security Breach and Self-Report of Data Breach Requirements (PII requirements

## Policy

Upon signing a Program Participation Agreement (PPA), Mystros Barber Academy agreed to comply with the Family Educational Rights and Privacy Act (FERPA), the U.S. Department of Education's implementing regulations at 34 C.F. R. Part 99, and the Standards for Safeguarding Customer Information, 16 C.F.R. Part 314, issued by the Federal Trade Commission (FTC), as required by the Gramm-Leach-Biley (GLB) Act, P.L. 106-102. Mystros Barber Academy is responsible for complying the limitations on the disclosure of PII in students' education records under FERPA and is subject to Sections 501 and 505(b)(2) of the GLB Act.

The GLB Act, also known as the Financial Services Modernization Act of 1999 (Public Law # 106-102, 113 Statute 1338), regulates the collection, disclosure, and protection of consumers' nonpublic personal information or personally identifiable information (PII) by financial institutions. Section 501 of GLB Act established the following information security standards for financial institutions:

Mystros Barber Academy shall establish appropriated standard for the institution relating to administrative, technical, and physical safeguards-

(1) To ensure the security and confidentiality of students and employees records and information
(2) To protect against any anticipated threats or hazards to the security or integrity of such records; and
(3) To protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any student or employee.

## Program Objectives:

The objectives of this Information Security Program ("Program") are as follows:
• Insure the security and confidentiality of the institution students and employee's information.
• Protect against any anticipated threats or hazards to the security and/or integrity of the institution's Student's and employee's information.
• Protect against unauthorized access to or use of the Institution's students and employee's information that could result in substantial harm or inconvenience to any customer.

## Purpose

For purposes of the Mystros Barbering Academy, Security Program, "student information" means any information about a Student's and/or employee's, or information the institution receives about the student of another financial institution, that can be directly or indirectly attributed to the student. This Security Program, in and of itself, does not create a contract between the student and any person or entity.

## Responsibilities:

**Program Coordinator(s)**
This Program and the safeguards it contemplates shall be implemented and maintained by an employee or employees ("Eros Shaw") designated by the institution's Director. The Program Coordinator shall design, implement and maintain new safeguards as he or she determines to be necessary from time to time. The Program Coordinator shall report to the Director and team members who have responsibility for overseeing the Program. The Program

Coordinator may delegate or outsource the performance of any function under the Information Security Program as he or she deems necessary from time to time.

In the event the Program Coordinator leaves the employment of the Institution, the Director, shall take over the responsibilities of the Program Coordinator until a new Program Coordinator is designate.

## Procedures

1. All records containing customer information shall be stored and maintained in a secure area.

• Paper records shall be stored in a room, cabinet, or other container that is locked when unattended. The Director and Program Coordinator shall control access to such areas.

• All storage areas shall be protected against destruction or potential damage from physical hazards, like fire or floods.

• Electronic customer information shall be stored on secure servers. Access to such information shall be password controlled, and the Program Coordinator shall control access to such servers.

• Student and employee information consisting of financial or other similar information (e.g., social security numbers, etc.) shall not be stored on any computer system with a direct Internet connection.

• All customer information shall be backed up on a [daily] basis. Such back up data shall be stored in a secure location as determined by the Program Coordinator.

2. All electronic transmissions of student and employee information, whether inbound or outbound, shall be performed on a secure basis.

• Social Security, IRS information, or other sensitive financial data transmitted to the Institution directly from students shall use a secure connection, such as a Secure Sockets Layer (SSL) or other currently accepted standard, so that the security of such information is protected in transit. Such secure transmissions shall be automatic. Students shall be advised against transmitting sensitive data, like social security, via electronic mail.

• The Institution shall require by contract that inbound transmissions of student information delivered to the Institution via other sources be encrypted or otherwise secured.

• All outbound transmissions of student information shall be secured in a manner acceptable to the Program Coordinator.

• To the extent sensitive data must be transmitted to the Institution by electronic mail, such transmissions shall be password controlled or otherwise protected from theft or unauthorized access at the discretion of the Program Coordinator.

• The Program Coordinator and third party service shall review all students' applications to ensure an appropriate level of security both within the Institution and with the Institution's business third party server and IRS.

3. All paper transmissions of customer information by the Institution shall be performed on a secure basis.

• Sensitive student information shall be properly secured at all times.

• Student information delivered by the Institution to third parties shall be kept sealed at all times. • Paper-based student information shall not be left unattended at any time it is in an unsecured area.

4. All student information shall be disposed of in a secure manner.

• The Program Coordinator shall supervise the disposal of all records containing student information.

• Paper based student information shall be shredded and stored in a secure area until a disposal or recycling service picks it up.

• All hard drives, diskette, magnetic tapes, or any other electronic media containing student information shall be erased and/or destroyed prior to disposing of computers or other hardware.

• All hardware shall be effectively destroyed.

• All student information shall be disposed of in a secure manner after any applicable retention period.

5. The Program Coordinator shall maintain an inventory of Institution computers, including any handheld devices or PDAs, on or through which student information may be stored, accessed or transmitted.

6. The Program Coordinator shall develop and maintain appropriate oversight or audit procedures to detect the improper disclosure or theft of student information.

## Information Security Policies and Procedures

Detecting, Preventing and Responding to Attacks, Intrusions or Other Systems Failures In keeping with the objectives of the Program, the Institution shall implement, maintain and enforce the following attack and intrusion safeguards:

Norton Anti-Virtus (Mystros Barber Academy)

ONLINE SMART (Compiled Net Code and anti SQL Injection Technology-Encrypted with SSL encryption on DELL Server)

iBackup (Mystros Barber Academy)

ECM-utilizes Educational Compliance Management school interface that is encrypted. The school must be secured with a unique logon ID and password for access to systems.

1. The Program Coordinator shall ensure the Institution has adequate procedures to address any breaches of the Institution's information safeguards that would materially impact the confidentiality and security of customer information. The procedures shall address the appropriate response to specific types of breaches, including hackers, general security compromises, denial of access to databases and computer systems, etc.

2. The Program Coordinator shall utilize and maintain a working knowledge of widely available technology for the protection of student information.

3. The Program Coordinator shall communicate with the Institution's computer vendors from time to time to ensure that the Institution has installed the most recent patches that resolve software vulnerabilities.

4. The Institution shall utilize anti-virus software that updates automatically.

5. The Institution shall maintain up-to-date firewalls.

6. The Program Coordinator shall manage the Institution's information security tools for employees and pass along updates about any security risks or breaches.

7. The Program Coordinator shall establish procedures to preserve the security, confidentiality and integrity of student information in the event of a computer or other technological failure.

8. The Program Coordinator shall ensure that access to student information is granted only to legitimate and valid users.

9. The Program Coordinator shall notify students promptly if their student information is subject to loss, damage or unauthorized access.