Student Information & Security Program

Cosmetology School
OF ARTS & SCIENCES

Compliance with the Gramm-Leach-Billey Act
Financial Privacy Rule & Safeguards Rule

485 E 5th St N. Burley, Idaho, 83318. Phone 208-678-4454, email:csas@pmt.org

Purpose of the Policy
The Gramm-Leach-Billey Act (Public Law 106-102 provides consumers the right to the protection of their nonpublic personally identifiable information and requires financial institutions possessing such information about consumers to publish a privacy policy ('policy') and implementing an information Security Program (the "Program"). This policy is published on the school's website and a notice on the web. The information Security Program applies to the Cosmetology School of Arts & Sciences.

General Privacy Policy
The school carefully protects all nonpublic personal information in our possession regarding students and their families. The school will not release nonpublic, private, personal, or financial information about our students or applicants to any third party, except as specifically provided in this policy. The school will release certain nonpublic personal information to federal and state agencies, government contractors, students loan providers/servicers, and other parties as necessary for the administration of the federal student aid programs, for enforcement purpose, for litigation, and for use in connection with audits or other investigations. Disclosure is permitted to law enforcement or emergency services agencies in the performance of their duties or when student safety or health may be in jeopardy. The school will not sell or otherwise make available personal information for marketing purposes to any third party at any time.

Protection of personally Identifiable Information
The school employees follow office procedures and password-protected computer systems to ensure the security of paper and electronic records. The school does not disclose specifics of its internal security procedures to students or the public to protect the effectiveness of those procedures.

Access to social security numbers and other personally identifiable information is strictly limited to those school officials with a need-to-know. Each department director is responsible for enforcement of this policy about the information within his/her office. Ms. LaDonn Goodfellow is responsible for overall control of information release and will resolve any disagreements and make final decisions as necessary in accordance with this policy.

The school's information is an important asset that is critical to providing an effective and comprehensive learning environment, openly communicating ideas, providing outstanding community service, and supporting the schools' operations and its offering of education services. This information includes sensitive and personal student, faculty, and staff data as well as the school's operational data. To maintain effectiveness and protect individuals, the school's information assets must be protected from misuse, unavailability, destruction, and unauthorized disclosure or modification. The executive leadership of the school is committed to protecting the value of the school's information assets. The school is committed to establishing and maintaining a program that preserves the confidentiality, integrity, and availability of information and information systems.

This responsibility is addressed by:

- Continually assessing risks and defining appropriate protection strategies
- Complying with applicable legal and regulatory requirements
- Protecting the reputation, image, and competitive advantage of the school
- Supporting the school's strategic mission and goals
- Maintaining partnership with administrative units and staff to ensure a collaborative approach to information security.

The school deals with numerous threats and challenges including data loss or theft, malicious software (e.g. viruses, worms, trojan horses), identify theft, social engineering, phishing scams, and other risks associated with new technologies. Security measures also must be implemented to comply with several laws and regulations that address student information (FERPA), financial information, individuals' privacy data and individuals' health information.

Policies and procedures provide the foundation of an effective Information Security Program and define minimum requirements for protection of information.

Designation of Representative(s)

Ms. LaDonn Goodfellow is designated as the program officer who is responsible for coordinating and overseeing this information security program. She may designate other representatives of the school to oversee and coordinate elements of the program. Questions regarding implementation or interpretation of the program should be directed to her of her designees(s). Please note: the definition of a customer as used herein is anyone about whom the school collects, views, or keeps any type of financial information. Customers can be students, parents of student (or other relatives) employees, and vendors.

Program Objectives

- Protect the Security and confidentiality of customer records and information.
- Identify and assess the risks to student information in each relevant area and evaluate the effectiveness of the current safeguards for controlling these risks.
- Select appropriate service providers and contract with them to implement safeguards.
- Evaluate, test and monitor the program and make changes as necessary.

Risk Assessment

The following is a list of potential threats to customer financial information's that the program is intended to mitigate.

- Unauthorized access to data through software applications.
- Unauthorized use of another information system user's account and password.
- Unauthorized use of another information systems user's account and password.
- Unauthorized viewing of printed or computer displayed customer financial information

- improper storage of printed customer financial data information. Improper destruction of printed material that contains customer financial information.

Information Security Program components

- Access to the School's information systems is limited to authorized personnel. Authorized personnel are assigned a username and a password to gain access to the appropriate information system. Approval of access to the various modules in the school's information systems is given by different managers. For example, access to the financial aid information system requires the Financial Aid Directors approval and access to the school's salary information system requires authorized by the CFO
- Passwords may not be shared
- Students requiring access to customer financial information are given their own account and password with appropriate privileges assigned.
- Computer terminals used to display customer financial information are not to be left unattended with customer financial information displayed.
- In unsecure areas, all users must log off their computer terminals when are away from their work area.
- Computer terminals are to be placed to prevent causal viewing by unauthorized personnel.
- Entry access to the Business office and Financial Aid office are limited to authorized personnel only with keys.
- Printed copies of customer financial information are to be handled only by authorized personnel and kept in areas with restricted access.
- Printed financial documentation and information of customers (including, but not limited to, credit card information, social security information, including social security numbers, bank information, loan information, salary, and other personal financial information) must be kept always secured. This type of information cannot be left in full view of unauthorized individuals. Records with customer financial information are in several areas, including, but not limited to, filing cabinets, folders, information from emails, information from phone calls, whether verbal or written, binders, cash drawers, credit card machines, information in computer documents. Access to these areas is limited to authorized personnel only.
- Customer financial information, regardless of where the information is housed or how it is kept (in computer systems/programs, email, paper copies, etc.) is confidential and is not available to anyone except those who have legitimate purpose for the information that is related to the school's mission. The following are examples of customer financial information that is confidential. This list is not all inclusive.
    - Salary and benefit information for an employee
    - Wage information for students
    - Social Security Numbers (Employees, Students, Vendors, Etc.)
    - Credit card information
    - Loan information
    - Bank information

- Dates of birth
- Home addresses and phone numbers

Offices must be kept locked when unattended or unsupervised

Fraudulent attempts to obtain information will be reported to the appropriate office staff/ individuals.

Consequences
Disciplinary measures for employees, up to and including termination, may be imposed for breaches of the security components of this program. Disciplinary measures for students, up to and including termination of enrollment, may be imposed for breaches of the security components of this program.

Monitoring and Testing
This program shall be reviewed periodically and adjusted as and when necessary. The school will monitor software updates and new releases for security software and implement appropriate upgrades and new releases in a timely fashion. In addition, the school CEO & CFO shall hold such formal and information meetings with appropriate employees on an as needed basis to review the effectiveness of the program and revise as necessary. Any suspected information security breach or issue should be reported immediately to the school administration.

Employee Training and Management
In keeping with the objectives of the program, The Cosmetology School of Arts & Sciences shall create, implement, maintain, and enforce a comprehensive educational program that prepares employees with the knowledge needed to enforce the information security program which includes

- Biannual webinar presentations on Cyber Security Compliance, Threats, Risks and Breach responsibility
- A printed copy of the college's information security program
- Enactment of a Clean Desk Policy requiring unattended desks to have a locked computer and items with personally identifiable information be securely contained. Passwords should not be visible and instead kept in a secure location.

The program officers shall work with the schools management to ensure that employees are meeting the exceptions outlined in this program.

The Program Officer will ensure that passwords are updated through the server.

External Breach Monitoring
Confirmed breaches should be reported by sending an email to FSASchoolCyberSafety@ed.gov : cpssaid@ed.gov or CALL the Education Security Operations Center at 1-202-245-6500

The email should include the following information:

- Date of Breach (suspected or known)
- Impact of Breach (# of records affected etc.)
- Method of Breath (Hack, accidental disclosure, etc.)
- Information security program point of contact email and phone details
- Remediation Status (Complete, in process-with detail, etc.)
- & Next Steps as needed

The Cosmetology School of Arts & Sciences should maintain continuous reporting with FSA as in continues to discover the breach so FSA can collaborate with the post-secondary institution to resolve the issue.

Post Incident analysis

After breach occurs, the program officer will review the incident material and summarize potential changes to current processes in order to prevent further breach vulnerability. The program officer will communicate process improvements by updating the Program and or sharing procedural changes through out the college.