MONTGOMERY COLLEGE

Office of Information Technology

IT Plan
GLBA/FSA/PCI/FERPA Security Program

Effective Date:	March 1, 2008
Revision Date:	11/2/2017
Review Date:	November 2, 2020
Version No.:	2.0
Contact:	Information Security and Privacy Director

PROGRAM

I. Preamble

In order to protect critical information and data, and to comply with Federal Law, the Office of Information Technology (OIT), in alliance with the Office of General Counsel (OGC) proposes certain practices in the College information environment and institutional information security procedures. While these practices mostly affect OIT, some of them will impact diverse areas of the College, including but not limited to the Office of Business Services, the Office of Student Financial Aid, the Office of Enrollment Services, the Office of Advancement & Community Engagement, the Office of Student Affairs, the Office of College Libraries & Information Services, and many third party contractors, including food services and the book stores. The goal of this document is to define the College's Information Security Program as it relates to regulated and confidential information, to provide an outline to assure ongoing compliance with federal regulations related to the Program and to position the College for likely future privacy and security regulations

II. Background:

The Gramm-Leach-Bliley Act ("GLBA"), as implemented by the Federal Trade Commission's Safeguards Rules, requires Montgomery College ("College") to develop, follow, maintain and update a comprehensive written information security program (the "Program"). This GLB Security Plan describes the program by which the College intends to:

1. Provide for the security and confidentiality of "covered data and information" (as defined below);
2. Protect against anticipated threats and or hazards to the security and safekeeping of such records; and
3. Protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to students and others who are the subject of such records.

This Plan incorporates the College's existing policies and procedures to the extent applicable and existing practices at the College, including but not limited to FERPA compliance actions. This Plan as a description of the Program is intended to be a document that will be continuously reviewed, refined and amended to better reach the goals of security outlined above.

II. Definitions:

A. "Covered data and information" for the purpose of this policy includes "student and third party non-public financial information" required to be protected under the GLBA. For purposes of this Program, the College also considers covered data and information to include any credit card information received in the course of business by the College, whether or not such credit card information is technically covered by GLB. Covered data and information includes both paper and electronic records.

B. "Nonpublic financial information" is that information the College has obtained from a student or a third party in the process of offering a financial product or service, or such information provided to the College by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CFR § 225.28. Examples of student or third party nonpublic financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and social security numbers, in both paper and electronic format.

C. "College" shall mean and include not only Montgomery College, but also affiliate organizations such as the Montgomery College Foundation.

III. Designation of Representatives and Scope of Program:

A. GLB mandates that the College appoint one or more Information Security Plan Coordinators ("Plan Coordinator"). The College designates the IT Security Manager and the Information Security & Privacy Director as its Plan Coordinators. These Plan Coordinators shall be responsible for coordinating and overseeing the implementation of the Program, including periodic review and updates to the Plan. Any questions regarding the plan and its implementation should be directed to the Plan Coordinators.

B. The Plan Coordinators will work with the relevant offices of the College to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; evaluate the effectiveness of the current safeguards for controlling these risks; and in conjunction with these offices, assist them to design, document and implement a safeguards program, and regularly monitor and test the program.

C. The Program applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the College, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the College or its affiliates. For these purposes, the term nonpublic financial information shall mean any information (i) a student or other third party provides in order to obtain a financial service from the College, (ii) about a student or other third party resulting from any transaction with the College involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person.

IV. Elements of the Program:

A. Risk Identification and Assessment. The College intends, as part of the Program, to undertake to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In implementing the Program, the Plan Coordinators will establish processes for identifying and assessing such risks in each relevant area of the College's operations, including:

- *Employee training and management*. The Plan Coordinators will coordinate with representatives in the College's Human Resources and Financial Aid offices to evaluate the effectiveness of the College's practices relating to access to and use of student and third party records, including financial aid information. This evaluation will include assessing the effectiveness of the College's current policies and procedures in this area. The College IT Security group, in concert with HR, will develop a Security Awareness training program, which will encompass the security issues and topics addressed in this plan.

- *Information Systems and Information Processing and Disposal.* The Plan Coordinators will coordinate with representatives of the College's IT office to assess the risks to nonpublic financial information associated with the College's information systems, including network and software design, information processing, and the storage, transmission and disposal of nonpublic financial information. This evaluation will include assessing the College's current policies and procedures relating to acceptable use of computing resources and retention policies. The Plan Coordinators will also coordinate with the College's IT office to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

- *Detecting, Preventing and Responding to Attacks*. The Plan Coordinators will coordinate with the College's IT offices and other offices as necessary to evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies.

B. Current Security Practices. The College's Network and Information Security and Privacy Program calls for regular, routine monitoring and assessment of security controls by the IT Security group. Reviews and assessments will also be conducted when new technology is introduced into the College IT environment. The majority of the security safeguards and controls are and will be implemented, operated and monitored by the College's IT staff. Adjustments to the safeguards and controls will be undertaken when indicated by the review and monitoring process.

C. Designing and Implementing Safeguards. The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The Plan Coordinators will, on a regular basis, oversee and coordinate the implementation of safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

D. Overseeing Service Providers. The Plan Coordinators shall coordinate with those responsible for the third party service procurement activities among the office of Procurement, IT and other affected offices to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access. In addition, the Plan Coordinators, in coordination with the office of Procurement, will develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions will require the approval of the Office of General Counsel. These standards shall apply to all future contracts entered into with such third party service providers.

E. Adjustments to Program. The Plan Coordinators are responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the College's operations or other circumstances that may have a material impact on the Program.

F. Applicable College Policies and Standards.

- CP31000 Code of Ethics and Employee Conduct
- CP32101 Employment Practices
- CP34002 Disciplinary Action and Suspension
- CP66001 Acceptable Use of Information Technology
- CP66002 Confidential Data Management and Security
- Network and Information Security and Privacy Program
- GLBA/FSA/PCI/FERPA Security Program
- IT08001 IT Resource Authentication Standard
- IT10001 Server Configuration and Security Standard
- IT11002 Remote Access Standard
- IT11004 Banner Desktop Data Access and Security Management Standard
- IT17002 WEB System and Folder PII Scans

G. **Updated Plan.** This plan updates the College's original GLBA Plan from March 2008.

Approved:

Patrick Feehan - Information Security & Privacy Director

Title

__11/2/2017________________

Date

MONTGOMERY COLLEGE

Office of Information Technology

IT Training
GLBA Training Outline

Effective Date:	March 1, 2008
Revision Date:	11/2/2017
Review Date:	November 2, 2020
Version No.:	2.0
Contact:	Information Security and Privacy Director

Objectives for Gramm Leach Bliley Act (GLBA) Training

- GLBA Overview
- Safeguards Rule
- GLBA Definitions

What is GLBA?

- The Gramm Leach Bliley Act (GLBA) is a comprehensive, federal law affecting institutions. The law requires financial institutions to develop, implement and maintain administrative, technical and physical safeguards to protect the security, integrity and confidentiality of customer information.
- The Federal Trade Commission (FTC) enforces compliance with GLBA.
- The FTC may bring an administrative enforcement action against any financial institution for non-compliance with the GLBA.
- Montgomery College significantly engages in student loan making and provides financial services to student customers. As such, MC falls within the definition of "financial institution" under the GLBA and must comply with the law's requirements".
- "Financial Institution" means any institution the business of which is engaging in financial activities.
- The GLBA is composed of several parts, including:
  - the Privacy Rule (16 CFR 313) and
  - the Safeguards rule (16 CFR 314).
- The FTC has officially stated that any college or university that complies with the Federal Educational Rights and Privacy Act (FERPA) and that is also a financial institution subject to the requirements of GLBA shall be deemed to be in compliance with GLBA's privacy rules if it is in compliance with FERPA (16 CFR 313.1). MC complies with FERPA guidance.
- The FTC has not made a similar exception for an institution of higher education with respect to the Safeguards Rule.

The Safeguards Rule requires all financial institutions to develop an information security program designed to protect "customer information."

- MC must comply with the Safeguards Rule.
- There are three types of safeguards that must be considered when a MC department implements safeguards to protect the security, confidentiality, and integrity of customer information:
  - Administrative Safeguards
  - Technical Safeguards
  - Physical Safeguards

Administrative Safeguards include developing and publishing policies, standards, procedures and guidelines, and are generally within the direct control of a department, such as:

- Performing reference and criminal background checks on potential employees.
  - Signing Banner confidentiality and NASFAA Code of Conduct agreements that include standards for handling customer information.

- Providing onboarding policy review and training for all new employees
  - Providing periodic College and unit level training for employees on steps they must take to protect customer information.
- Assuring employees are knowledgeable about applicable policies and expectations.
- Limiting access to customer information to employees who have a business need to see it.
- Referring calls or requests for customer information to staff trained to respond tosuch requests.
- Being alert to fraudulent attempts to obtain customer information and reporting theseto management for referral to appropriate law enforcement agencies.
- Imposing disciplinary measures where appropriate.

Physical Safeguards are also generally within a department's control and include:

- Locking rooms and file cabinets where customer information is kept.
- Ensuring that storage areas are protected against destructions or potential damage from physical hazards, like fire or floods.
- Storing records in a secure area and limit access to authorized employees.
- Disposing customer information appropriately:
- Training staff members on how to dispose of records containing customer personal information.
  - Shredding or recycling customer information recorded on paper and store it in asecure area until the confidential recycling service picks it up.
  - Erasing all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contains customer information.
  - Promptly disposing of outdates customer information according to the Montgomery College RecordRetention Schedule.

Technical Safeguards include:

- Requiring password activated screensavers.
- Requiring strong passwords.
- Requiring periodic password changes and encouraging the use of password vaults.
- Requiring Two Factor Authentication
- Storing electronic customer information on a secure server that is accessible only with a password or has other security protections and is kept in a physically secure area.
- Avoiding storage of customer information on machines with an Internet connection.
- When storing customer information on local desktops cannot be avoided, encrypting customer information placed on local drives.
- Maintaining secure backup media and securing archived data.
- Using anti-virus software that updates automatically.
- Scanning systems regularly to identify and remediate vulnerabilities.
- Obtaining and installing patches that resolve software, hardware and firmware vulnerabilities.
- For shared workstations, employing system restore software to reset the image back to the default after a reboot.
- Maintaining up-to-date firewalls to restrict traffic to only what is necessary to support the business of the College.
- Providing secure remote access services utilizing a VPN.
- Providing central management of security tools and keep employees informed of security risks and breaches.
- Following written contingency plans to address breaches of safeguards.

Associated College Policy and Office of Information Technology Standards

- CP31000 Code of Ethics and Employee Conduct
- CP32101 Employment Practices

- CP34002 Disciplinary Action and Suspension
- CP66001 Acceptable Use of Information Technology
- CP66002 Confidential Data Management and Security
- Network and Information Security and Privacy Program
- GLB/FSA/PCI/FERPA Security Program
- IT08001 IT Resource Authentication Standard
- IT10001 Server Configuration and Security Standard
- IT11002 Remote Access Standard
- IT11004 Banner Desktop Data Access and Security Management Standard
- IT17002 WEB System and Folder PII Scans

GLBA DEFINITIONS:

Customer information is any record containing non-public personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the financial institution or its affiliates.

GLBA applies to customer information obtained in a variety of situations, including:

- Information provided to obtain a financial product or service;
- Information about a customer resulting from any transaction involving a financial product or service between the institution and customer;
- Information otherwise obtained about a customer in connection with providing a financial product or service to the customer.

Non-Public Personal Information means personally identifiable financial information that is:

- Provided by a consumer to a financial institution;
- Resulting from any transaction with the consumer or any service performed for the consumer; or
- Otherwise obtained by the financial institution.

The term also includes any list, description, or other grouping of consumers and publicly available information pertaining to them that is derived using any personally identifiable financial information that is not publicly available.

Examples of Non-Public Person Information (NPI) include:

- Social Security Number (SSN)
- Financial account numbers
- Credit card numbers
- Date of birth
- Name, address, and phone numbers when collected with financial data
- Details of any financial transactions