INFORMATION SECURITY PLAN

Introduction

Mount Holyoke College has established the following plan in compliance with the provisions of the following federal and state laws and regulations: the Financial Services Modification Act of 1999 (Gramm-Leach-Bliley); the Fair and Accurate Credit Transactions Act (FACTA) of 2003 (P.L. 108-159): the "Identity Theft Red Flag Rules" of the Federal Trade Commission (16 CFR Part 681): and the Massachusetts "Security Breach Law of 2007" (M.G.L. c.93H) together with the regulations contained in the "Standards for the Protection of Personal Information of Residents of the Commonwealth (MA 201 CMR 17.00). The federal laws and regulations require financial institutions to maintain a comprehensive information security plan to insure that confidential financial data is protected. FACTA specifically requires institutions considered "creditors" that maintain certain financially related "covered accounts" to establish a program designed to detect, prevent and mitigate identity theft that might arise in the course of doing business. The Massachusetts law requires that certain entities maintaining and utilizing "personal information" about individuals notify the individual and designated state officials whenever they have reason to believe that their information may have been compromised or put at risk due to a security breach, or that their information was wrongly obtained or used by an unauthorized party.

This policy, together with the companion Program for Complying with the Standards for the Protection of Personal Information (the "WISP"), supplements the Responsible Use of Computing Resources at Mount Holyoke College and other College policies that protect student information and records, employee information, financial accounts, information technology services and related sensitive information maintained by the College.

Definitions

An account is a continuing relationship established by any person and the College (when acting as a creditor) to obtain a product or service from the College for personal, family, household or business purposes.

The term "breach of security," for purposes of compliance with the Massachusetts statute, means the unauthorized acquisition or unauthorized use of unencrypted data or encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the Commonwealth. A good faith but unauthorized acquisition of personal information by the College, or an employee or agent of the College, for the lawful purposes of the College is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Confidential financial information (as defined by Gramm-Leach-Bliley) consists of information that the College obtains through the process of offering financial products or services to the College community. Examples of these products and services include student financial aid, employee home mortgages and employee computer loans. Similar information provided to the College by another financial institution is also considered confidential financial information for purposes of this plan. Examples of confidential financial information include bank and credit card account numbers, income and credit histories, personal tax returns and social security numbers. Confidential financial information may exist in both paper and electronic forms.

A covered account is an account offered or maintained by the College acting as a creditor (1) that involves or is designed to permit multiple payments or transactions for personal or family purposes; or (2) for which there is a reasonably foreseeable risk of harm to the person holding an account or to the College from identity theft.

The College acts as a creditor when it regularly extends, renews or continues credit.

Identifying information is any name or number that may be used alone or in conjunction with other information to identify a specific person, including any:

- Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
- Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- Unique electronic identification number, address, or routing code; or
- Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).

The term, "personal information," for purposes of compliance with the Massachusetts statute, is defined as first and last name (or first initial and last name) in combination with any one of the following: (a) Social Security number; (b) driver's license or state identification card number; or (c) a financial account, credit card or debit card number, with or without any required security code, access code, PIN or password that would permit account access.

Identity theft is an attempted or committed fraud using the identifying information of another person without authority.

A Red Flag is a pattern, practice or specific activity that indicates the possible existence of identity theft.

A service provider is any third party that provides services to the College in support of its offering, opening and administration of covered accounts. Service providers relating to this program include: providers of student and employee health insurance; third-party retirement and other benefits administrators; financial institutions that administer the College's tuition payment plan; governmental and private student loan providers; electronic billing and payment partners; and collections agencies.

Financial Information Security Plan

Plan Coordinators

The Directors of Human Resources and Student Financial Services and the Comptroller will act as joint plan coordinators.

In addition to having primary responsibility for overseeing the safeguarding and appropriate use of confidential financial information in their respective areas, the coordinators will work with other College departments and with outside advisors as necessary to:

- Identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of confidential financial information
- Evaluate the effectiveness of the current safeguards
- Regularly monitor the plan
- Make any needed changes to improve the plan
- Identify third-party providers with access to confidential financial information and assure that the College's contracts with them insure that such information is protected

Identification of Risks and Risk Assessment

Risks, both internal and external, include (but are not limited to) the following:

- Unauthorized access of confidential financial information
- Compromised system security as the result of unauthorized access, including corruption of data or systems
- Interception of confidential financial information during transmission
- Loss or misplacing of paper or stored electronic records containing confidential financial information, resulting in unauthorized access
- Responding to unauthorized requests for confidential financial information
- Unauthorized transfer of confidential financial information through third parties
- Improper destruction of confidential financial information, resulting in unauthorized access

Recognizing that risks change with changes in technology, the College will regularly review the plan and our processes to insure that they continue to provide effective protection for confidential financial information.

Processes for Protecting Confidential Financial Information

The College provides training for employees who work with confidential financial information consisting both of general information of issues of compliance with privacy and security regulations and of more specific policies and procedures within their particular department and job function.

General training includes review of the College's responsible use of computing resources policy and guidelines for working with confidential information, including safe computing practices.

Access to confidential financial information is limited to employees who have a business reason to have such information. Employee access is reviewed periodically. Data bases containing confidential financial information are password protected. Paper files are stored in secured areas.

The College's Library, Information and Technology Services division takes steps to insure that the technological infrastructure safeguards the integrity of records in storage and transmission and safeguards confidential financial information.

Records containing confidential financial information are encrypted when transmitted or stored on laptops or other portable devices.

The College has a records retention policy that includes the retention and disposal of confidential financial information. Disposal methods include shredding on site, contracting with a third party disposal service, deleting electronic documents and erasing documents stored electronically.

If the College has reason to believe that a situation has occurred during which data containing confidential information was compromised, the following steps will be taken:

- Move immediately to control further compromise by removing the machine from the network, shutting down the server or taking other appropriate steps to halt further damage
- Activate the College's process for dealing with compromised computers
- Investigate to determine the extent to which confidential information may have been compromised
- If the investigation determines that there is a reasonable likelihood that confidential information has been compromised, notify affected individuals that their personal information may have been inadvertently compromised and encouraging them to contact their financial providers and to scrutinize their financial records

- Take appropriate measures to mitigate the risk of any future compromising of confidential information

Oversight of Third Party Providers

The College regularly reviews its contractual relationships with third party providers who have access to confidential financial information to insure that they understand their obligations under GLB.

Review and Revision of the Confidential Financial Information Plan

The plan coordinators will review the plan with the Privacy and Security Regulations Task Force regularly and the plan will be revised as needed.

Identity Theft Prevention Program

Identifying Red Flags

The College has considered the following factors in identifying Red Flags for covered accounts:

- The types of covered accounts that the College offers and/or maintains
- The methods the College uses to open accounts
- The ways in which the College allows access to its covered accounts
- Any previous problems with identity theft involving College accounts

The College has determined that the following accounts may constitute covered accounts:

- Student and employee loan accounts. These financial accounts maintained by the College include Perkins accounts for student loans and employee computer loans and salary advances.
- Student and employee accounts receivable. These financial accounts maintained by the College include tuition, room and board charges, parking fees, library fines and other miscellaneous charges.

The Red Flag regulations require that the College perform an assessment of the potential risk of identity theft associated with its covered accounts, based in part on the College's history with identity theft incidents. Since the College has not experienced any previous reported incidents of identity theft on any covered account, the College has determined that there is a low probability of identity theft problems.

Detecting Red Flags

Red Flags may include, but are not limited to:

- documents, such as identification/stored value cards, that appear forged;
- presentation of student or employee information that is inconsistent with information in storage;
- inaccurate personal identification information, such as social security numbers or addresses;

- alerts, notifications or other warnings received from service providers, such as fraud detection services, student loan administrators, banks or other third-party entities who have access to College-maintained information;

- suspicious documents;

- suspicious personal identifying information;

- unusual or suspicious activity in covered accounts;

- notices from customers, victims of identity theft, Public Safety Department or other law enforcement authorities regarding possible identity theft.

The College's procedures for detecting Red Flags are as follows:

- Student and employee loan accounts and accounts receivable**.** Account disbursements and credits are handled automatically through the College's computer systems, which are protected through information technology monitoring systems and security. The Financial Services and Student Financial Services Departments have in place a verification system requiring individuals seeking information to provide appropriate authentication information.

- Third party vendors**.** The College takes reasonable steps to verify that its third party vendors have the capacity to protect personal information in accordance with Massachusetts law.

- Receipts of Red Flag notices from third party entities. All staff members who may receive notices of security breach or Red Flag notices from law enforcement agencies, service providers, students or employees have been instructed to direct the notice to his or her department manager, who will then report the receipt of the notice to Financial Services.

Responding to Red Flags

When a Red Flag is detected or reported, one or more of the following procedures, as appropriate, will take place:

- The Comptroller or his/her designee will notify the Vice President for Finance and Administration and perform an initial risk assessment of the particular Red Flag.

- Upon completion of the risk assessment, the holder of the covered account will be notified and the Financial Services Department will implement any needed changes to existing security measures, including but not limited to account "freezing", suspension or closure.

- The Comptroller or his/her designee, in consultation with the Vice President for Finance and Administration, will determine whether any additional steps are necessary. Examples of additional steps include: notification of the Public Safety Department and/or other law enforcement officials; notification of LITS staff or outside service providers; and notification of the Trustee Audit Committee.

Oversight

- Overall Program. The Vice President for Finance and Administration is responsible for the development, implementation, oversight and continued administration of the program. The initial program was approved by the Trustee Audit Committee on May 8, 2009.
- Service Providers. When the College engages a service provider to perform an activity in connection with one or more accounts, the College will take appropriate steps to ensure that the service provider performs its activity in accordance with reasonable policies and

procedures designed to detect, prevent, and mitigate the risk of identity theft. Such steps may include:

- Reviewing a copy of that service provider's identity theft policies and procedures.
- Including contract provisions that require service providers to have such policies and procedures in place.
- Requiring that service providers provide timely written notice of Red Flags related to College information.

- Annual Reporting. The Comptroller or his/her designee will review the College's compliance with this policy annually, including an updated assessment of institutional risk, and recommend any necessary modifications to the policy to the Vice President for Finance and Administration.

Address Discrepancy Notifications and Changes of Address

Under the above-mentioned federal law and regulations, the College is also required to establish a process for handling address discrepancy notifications received by the College in connection with its use of consumer credit reports. The College uses credit reports only in limited circumstances in connection with hiring individuals for certain sensitive positions. The College instructs all staff members who use credit reports regarding the handling of notices of address discrepancies.

All requests for replacement of College identification/stored value cards are handled by the Auxiliary Services Department and in-person validation of card replacement requests are required.

Required Notifications under Massachusetts Law Concerning Security Breaches and Wrongful Appropriation or Use of Personal Information of a Massachusetts Resident

In accordance with the requirements of M.G.L.c. 93H, s. 3, the College will provide notice, as soon as practicable and without unreasonable delay, (1) when it knows or has reason to know of a breach of security, or (2) when it knows or has reason to know that the personal information of a Massachusetts resident was acquired or used by an unauthorized person, or used for an unauthorized purpose, to the Massachusetts Attorney General, the Director of Consumer Affairs and Business Regulation ("Director"), and to the affected resident. The College will also, as soon as practicable and without unreasonable delay, provide notice to any consumer reporting agencies and state agencies which the College is subsequently directed to notify by the Director.

The notice to be provided to the Attorney General and Director, and to any other consumer reporting agencies or state agencies identified by the Director, will include at a minimum the nature of the breach of security or unauthorized acquisition or use, the number of residents of the commonwealth affected by the incident at the time of notification and any steps the College has taken or plans to take relating to the incident.

The notice to be provided to the resident will include at a minimum the consumer's right to obtain a police report, how to request a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies. The notification will not include the nature of the breach or unauthorized acquisition or use or the number of residents of the Commonwealth affected by the breach or unauthorized access or use.