MHC

ALUMNAE ASSOCIATION

MOUNT HOLYOKE COLLEGE

Information-Security Policy

Date: March 2010

Revised: July 11, 2010

Revised: August 9, 2011

MHC
ALUMNAE ASSOCIATION
MOUNT HOLYOKE COLLEGE

Introduction

The security of Alumnae Association of Mount Holyoke College (Association) information is extremely important. We are trusted by our alumnae and coworkers to protect personal information that may be supplied while conducting business. The following is the Association's Workplace Information Security policy for compliance with Massachusetts regulation 201 CMR 17.00.

"Personal information" as used in this policy is defined the same as it is in 201 CMR 17.02: "a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public." It is important that we treat credit-card information as confidential and that only employees who have a need to know are permitted access to personal information (i.e. credit-card numbers, expiration dates, card holder's name, etc).

It is crucial that employees do not reveal personal information about our organization or our alumnae to outside sources that do not have a need to know such information. All personal information should and will be stored in a secure location and locked or supervised at all times.

This policy covers the security of Association information and must be distributed to all Association employees who have access to personal information, including full time, part time, temporary and student employees and volunteers working on events or segments of events managed by the Association. The senior staff of the Alumnae Association will review and update this information-security policy at least once a year
to incorporate relevant security needs that may develop. Each employee and volunteer referenced above must read and sign a form verifying she or he has read and understands this policy.

Disciplinary Action

An employee's failure to comply with the standards and policies set forth in this document may result in disciplinary action, including termination of employment.

It is unlawful and against Alumnae Association policy to retaliate against anyone who reports a violation of this policy or who cooperates in an investigation regarding non-compliance with this policy. Any such retaliation will result in disciplinary action by the Association, including termination.

MHC
ALUMNAE ASSOCIATION
MOUNT HOLYOKE COLLEGE

Purpose

The purpose of the policy is to establish administrative, technical, and physical safeguards to protect confidential information, whether such information is contained on paper, in electronic records, or exists in any other form. This policy is designed to ensure the security of confidential information, to protect against anticipated threats or hazards to the integrity of confidential information, and to protect against unauthorized access to or use of confidential information in a manner that creates a substantial risk of harm.

Scope

In order to direct the creation of effective administrative, technical, and physical safeguards for the protection of confidential information, this policy sets forth in general terms the Association's requirements for accessing, collecting, storing, using, transmitting, and protecting electronic, paper, and other records containing confidential information.

Protect Stored Data

Employees must protect personal information stored or handled by the Association and its employees. All personal information must be stored securely and disposed of (when no longer needed for business reasons) in a secure manner. Any medium (i.e. paper or electronic) that contains personal information must be protected against unauthorized access. Media no longer needed must be destroyed so that sensitive data is irrecoverable (i.e. shredding, degaussing, disassembly, etc.).

Physical Security
Restrict physical access to personal information, and systems that house that information (ex. computers or filing cabinets storing cardholder data), to protect it from those who do not have a need to access that information. Media include printed or handwritten paper, received faxes, portable electronic media devices, computer hard drives, etc. Employees are prohibited from storing personal information on third party data systems/servers (including cloud servers) not contracted by the Association (i.e. Dropbox, Google docs, iCloud, SugarSync,…)

- Media containing personal information must be securely handled and distributed.
- Media containing stored personal information (especially credit-card account numbers and Social Security numbers) should be properly inventoried and disposed of when no longer needed for business by deleting, shredding, or degaussing before disposal.
- Employees are prohibited from keeping open files containing personal information on their desks when they are not at their desks.
- At the end of the work day, all files and other records containing personal information must be secured in a manner that is consistent with the policy's rules for protecting the security of personal information.
- Computers that contain personal information should be locked when unattended for extended periods of time, such as meal breaks.

Credit-Card Information Handling Specifics

- Destroy cardholder information in a secure method when no longer needed. Media containing card information must be destroyed by shredding or other means of physical destruction that would render the data irrecoverable (shred, degauss, etc.).
- It is prohibited to store the contents of the credit-card magnetic stripe (track data) in any form.
- Except in the case of manual registrations, it is prohibited to store the card-validation code (the three- or four-digit number printed on the signature panel of the card) in any form. Cardholder information for manual registrations will be kept in a secure manner and must be destroyed by shredding or other means of physical destruction that would render the data irrecoverable (shred, degauss, etc) when no longer needed.
- Except in the case of manual registrations, all but the last four numbers of the credit-card account number must be masked (i.e. displayed as x's or *'s) when the number is displayed electronically or on paper. Cardholder information for manual registrations will be kept in a secure manner and must be destroyed by shredding or other means of physical destruction that would render the data irrecoverable (shred, degauss, etc) when no longer needed. Our service provider is Bank of America Merchant Services—Card Service (800) 228-5882, (vendor #4301 3300 1798 0921).

Protect Data in Transit

If personal information needs to be transported physically or electronically, it must be protected while in transit (i.e. to a secure storage facility or across the Internet).

Credit-Card Information Handling Specifics

- Credit-card account numbers must never be e-mailed without using proper encryption technologies (i.e. PGP encryption). Currently we do not have this encryption technology; therefore, e-mailing account numbers is prohibited.
- Media containing credit-card account numbers must only be given to trusted persons for transport to off-site locations.

Restrict Access to Data

Restrict access to personal information to those employees who have a need to know it. No employee should have access to personal information unless he or she has a specific job function that requires such access.

- Each person with computer access will be assigned unique identifications plus passwords (which are not vendor-supplied default passwords). The identifications and passwords shall be reasonably designed to maintain the security of the access controls.

External Risks

To combat external risks to the security and confidentiality of any electronic, paper, or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately.

- The Association shall provide and maintain reasonably up-to-date firewall protection, operating system security patches, designed to maintain the integrity of the personal information, and have them installed on all systems processing personal information.
- The Association shall provide a reasonably up-to-date version of system security agent software, which shall include malware protection, up-to-date patches and virus definitions, and have them installed on all systems processing personal information.
- Computer users are not allowed to turn off, bypass, disable, or otherwise render ineffective any firewall, system security, malware software, updates, or other devices installed or intended to be installed to provide system protection.
- To the extent technically feasible, all personal information stored on laptops or other portable devices must be encrypted, as must all records and files transmitted across public networks or wirelessly, to the extent technically feasible. (Currently we do not have this encryption technology; therefore, e-mailing account numbers and personal information is prohibited.)
- All computer systems must be monitored for unauthorized use of, or access to, personal information.
- There must be secure user-authentication protocols in place, including: (1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning and selecting passwords; (3) control of data-security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect; (4) restriction of access to active users and active-user accounts only; and (5) blocking of access to user identification after multiple unsuccessful attempts.

Security Awareness and Procedures

Keeping personal information secure requires periodic training of employees and contractors to keep security awareness levels high. The following Association policies and procedures address this issue.

- Hold periodic security-awareness training meetings for employees and contractors to review correct handling procedures for personal information.
- Employees are required to read this security policy and verify that they understand it by signing an acknowledgement form. (See Appendix A.)
- Background checks (such as credit and criminal-record checks, within the limits of local law) may be conducted for new employees who handle personal information.
- All third-party service providers shall be required by contract to implement and maintain appropriate security measures for personal information that are consistent with the requirements of 201 CMR 17.03(2)(f)(2) and any applicable federal regulations.

MHC
ALUMNAE ASSOCIATION
MOUNT HOLYOKE COLLEGE

Security Management and Incident-Response Plan

The senior director of finance and administration of the Association is designated as the security officer. The security officer is responsible for communicating security policies to employees and contractors and tracking adherence to the policies. If personal information is compromised, the security officer will oversee execution of the incident-response plan.

Incident-Response Plan

- If a compromise is suspected, alert the security officer.
- The security officer will conduct an initial investigation of the suspected compromise.
- If compromise of information is confirmed, the security officer will begin informing parties that may be affected by the compromise. If the compromise involves credit-card account numbers, the security officer will:
    - o Contain and limit the extent of the exposure by shutting down any systems or processes involved in the compromise.
    - o Alert necessary parties (i.e. alumnae, coworkers, merchant bank or other applicable vendors, and law enforcement)
    - o The security officer will conduct a mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

Terminated Employees

- Terminated employees must return all records containing personal information, in any form; in their possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.).
- A terminated employee's physical and electronic access to personal information must be immediately blocked. Such terminated employee shall be required to surrender all keys, Ids, access codes, badges, business cards, and the like, that permit access to the firm's or customer's premises or information. Moreover, such terminated employee's remote electronic access to personal information must be disabled; his/her voicemail access, e-mail access, Internet access, and passwords must be invalidated.

MHC
ALUMNAE ASSOCIATION
MOUNT HOLYOKE COLLEGE

Appendix A – Employee Agreement to Comply Form

Agreement to Comply with Information-Security Policies

Updated August 9, 2011 for compliance with 201 CMR 17.00.

_____

Employee Name (printed)

_____

Title

I agree to take all reasonable precautions to assure that Association internal information, or information that has been entrusted to the Association by third parties such as alumnae, will not be disclosed to unauthorized persons. At the end of my employment or contract with the Association, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorized to use personal information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the Association's senior director of finance and administration.

I have read and understand the information-security policies, and I understand how they affect my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the Association security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information-security policies to the designated security officer, the Association's senior director of finance and administration.

_____

Employee Signature

_____

Date

MHC
ALUMNAE ASSOCIATION
MOUNT HOLYOKE COLLEGE

Appendix B – Volunteer Guidelines

For compliance with Massachusetts 201 CMR 17

Introduction

Class, club, reunion and miscellaneous volunteers from time to time are trusted by our alumnae to protect personal information that may be supplied while undertaking Association-related volunteer activities. "Personal information" as used in these Guidelines is defined the same as it is in 201 CMR 17.02: "a Massachusetts resident's "first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public". The security of this information is extremely important. It is important that this personal information is treated as confidential and that only volunteers who have a need to know are permitted access to it.

Volunteers who have access to personal information are required to abide by this Massachusetts regulation. We recommend that annually, it is the responsibility of class and club officers as well as other volunteers in a leadership capacity for an event for which personal information may be obtained to identify: a) whether they potentially may obtain personal information from a Massachusetts resident (examples include other alumnae, Association or College staff/faculty); and b) if so, those volunteers within their organization who have or may have access to that personal information. Any such volunteer identified by the class or club officers or volunteer leader should be required by the officer or volunteer leader to comply with the Massachusetts regulation, 201 CMR 17, and to sign a Volunteer Agreement to Comply form (sample: Appendix C below).

All violations or suspected violations of information security policies should be reported to the class or club president or treasurer or to the volunteer leader. If the violation includes either the president or treasurer the report must also be made to the vice president. Non-compliance can be cause for disciplinary action up to and including removal of position, criminal and/or civil penalties.

MHC
ALUMNAE ASSOCIATION
MOUNT HOLYOKE COLLEGE

Practical Suggestions for Volunteers

Below are a few suggestions that will help you to comply with 201 CRM 17 during the collection of fees, dues and other revenues. It is recommended that volunteers take all reasonable precautions to assure that personal information is not disclosed to unauthorized persons.

- Credit card transactions –
  - Use a third party vendor that is compliant with the regulation.
    - Examples: PayPal, CyberSource
  - For large events (attendees over 100 and/or registration fees over $100 per attendee), the Association may be able to provide you with assistance upon request.
- Check handling –
  - Safe guard checks received / not yet deposited
  - Deposit checks promptly
  - Track name and check number only.

Rule of Thumb: Never include credit card or banking information in an e-mail. Do not record or copy personal information. If you must record/copy personal information, the document or file must be safeguarded and/or destroyed after intended use. Examples of safeguarding include: lock boxes, locked files and/or, password protected files. Under no circumstances should personal information be transmitted by e-mail.

- At the end of a volunteer's term or specific assignment all information to which access has been granted as a result of the position must be returned or destroyed as applicable. Personal information must never be used for a volunteer's own purposes, nor is the volunteer at liberty to provide this information to third parties without the express written consent of the individual whose information will be released.
- If a compromise is suspected, see page 6 for an incident response plan.