INFORMATON SECURITY PROCEDURES

Introduction

These procedures cover the security of The Foundation at Monroe County Community College's information and must be distributed to all employees. Management will review and update these information security procedures at least once a year to incorporate relevant security needs that may develop. Each employee must read and sign a form verifying they have read and understand Policy 3.07, Information Security Policy, and Procedures 3.07 (a), Information Security Procedures.

Ethics and Acceptable Use Policies

The Foundation at Monroe County Community College expects that all employees conduct themselves in a professional and ethical manner. An employee should not conduct business that is unethical or illegal in any way, nor should an employee influence other employees to act unethically or illegally. Furthermore, an employee should report any dishonest activities or damaging conduct to an appropriate supervisor.

Security of The Foundation at Monroe County Community College information is extremely important. We are trusted by our donors to protect sensitive information that may be supplied while conducting business. Sensitive information is defined as any personal information (i.e., name, address, phone number, e-mail, Social Security number, driver's license number, bank account, credit card numbers, etc.) or Foundation information not publicly available (i.e., clients, financial information, employee information, schedules, technology, etc.). It is important the employees do not reveal sensitive information about The Foundation at Monroe County Community College or our donors to outside resources that do not have a need to know such information.

Disciplinary Action

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

Protect Stored Data

The Foundation at Monroe County Community College will protect sensitive information stored or handled by The Foundation and its employees. All sensitive information must be stored securely and disposed of in a secure manner when no longer needed for business reasons. Any media (i.e., paper, digital storage, backup tape, computer hard drive, etc.) that contains sensitive information must be protected against unauthorized access. Media no longer needed must be destroyed in such a manner to render sensitive data irrecoverable (shredding, degaussing, disassembly, etc.).

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) on any media whatsoever.
- It is prohibited to store the card-validation code (3 or 4 digit value printed on the signature panel of the card) on any media whatsoever.
- All but the last four (4) numbers of the credit card account number must be masked (i.e., xxxxx or *****) when the number is displayed electronically or on paper.

Protect Data in Transit
If sensitive information needs to be transported physically or electronically, it must be protected while in transit (i.e., to a secure 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).
- Media containing credit card account numbers must only be given to trusted persons for transport to off-site locations.

Restrict Access to Data
The Foundation at Monroe County Community College will restrict access to sensitive information (business data and personal information) to those that have a need-to-know. No employees should have access to credit card account numbers unless they have a specific job function that requires such access.

Physical Security
The Foundation at Monroe County Community College will restrict physical access to sensitive information, or systems that house that information (e.g., computers or filing cabinets storing cardholder data), to protect it from those who do not have a need to access that information. Media is defined as any printed or handwritten paper, received faxes, digital storage media, back-up tapes, computer hard drive, etc.

- Media containing sensitive information must be securely handled and distributed.
- Media containing stored sensitive 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.
- Visitors should always be escorted and easily identifiable when in the areas that may contain sensitive information.
- Password protected screen savers should always be used on any computers that may contain sensitive information.

Security Awareness and Procedures

Keeping sensitive information secure requires periodic training of employees and contractors to keep security awareness levels high. The following procedures of The Foundation at Monroe County Community College address this issue:

- Hold periodic security awareness training meetings of employees and contractors to review correct handling procedures for sensitive information.
- Employees are required to read these Information Security Procedures and verify that they understand them by signing an acknowledgement form (see Appendix A).
- Background checks (such as credit and criminal record checks, within the limits of local law) will be conducted for all employees that handle sensitive information.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- The Foundation at Monroe County Community College's Information Security Policy and Procedures must be reviewed annually and updated as needed.

Security Management/Incident Response Plan

The Monroe County Community College Controller is designated as the security officer. The security officer is responsible for communicating security procedures to employees and contractors and tracking the adherence to procedures. In the event of a compromise of sensitive information, the security officer will oversee the execution of the incident response plan.

Incident Response Plan

1. If a compromise is suspected, alert the information security office.
2. The security officer will conduct an initial investigation of the suspected compromise.
3. If compromise of information is confirmed, the security officer will alert the Executive Director of The Foundation at Monroe County Community College and the President of Monroe County Community College and begin informing parties that may be affected by the compromise. If the compromise involves credit card account numbers, the following steps will be performed:
    - Contain and limit the extent of the exposure by shutting down any systems or processes involved in the compromise;
    - Alert necessary parties (Merchant Bank, Visa Fraud Control, law enforcement);
    - Provide compromised or potentially compromised card numbers to Visa Fraud Control within 24 hours;
    - More Information: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html

Appendix A

Agreement of Comply With Information Security Policy and Procedures

_____

Employee Name (printed)

_____

Title/Department

I agree to take all reasonable precautions to assure that The Foundation at Monroe County Community College's internal information, or information that has been entrusted to The Foundation at Monroe County Community College by third parties such as donors, will not be disclosed to unauthorized persons. At the end of my employment or contract with Monroe County Community College and/or The Foundation at Monroe County Community College, 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 sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the Executive Director who is the designated information owner.

I have access to a copy of the Information Security Policy and Procedures, I have read and understand these policies and procedures, and I understand how it impacts my job. As a condition of my employment, I agree to abide by the policy and procedures and other requirements found in The Foundation at Monroe County Community College's security procedures. 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 the Information Security Policy and Procedures to the security officer.

_____ _____

Employee Signature Date

Adopted by the Board of Directors – March 10, 2008