Payment Card Industry Compliance Policy

PURPOSE and BACKGROUND

The purpose of this policy is to ensure that Massachusetts Maritime Academy (MMA) maintains compliance with the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS is a worldwide security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). These standards are a set of comprehensive requirements for enhancing payment data security that was developed by the founding members of the PCI SSC. The PCI SSC is responsible for managing the security standards, while compliance with PCI standards is enforced by the founding members of PCI SSC: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI DSS includes technical and operational requirements for security management, policies, procedures, network architecture, software design and other critical protective measures to prevent credit card fraud, hacking and other types of security vulnerabilities and threats. The standards apply to all organizations that store, process or transmit cardholder data.

These standards are designed to protect cardholder information of students, parents, donors, alumni, customers, and any individual or entity that utilizes a credit card to transact business with the Academy. In addition, these standards help reduce the financial risk or impact associated with a breach of payment card information and protect the Academy's reputation.

SCOPE

This policy applies to those MMA departments that store, process or transmit credit card transactions. These currently include:

Business Office – accept and process credit cards for payment of student accounts, including Continuing Education payments.

Advancement Office - processes credit cards for donations and tickets to alumni events.

This policy **does not** apply to the Parents Association (MMAPA) or the Alumni Association (MMAAA), Chartwells' food service and Follett's bookstore.

DEFINITIONS

Chief Financial Officer (CFO) – The CFO of the Academy has oversight responsibility for this policy. The CFO will also communicate changes to the Chief Information Officer (CIO) in order to facilitate enforcement of this policy.

Credit Card Data - Full magnetic stripe or the PAN (Primary Account Number) plus any of the following: Cardholder name, Expiration date, or Service Code. The term credit card data is interchangeable with payment card data or cardholder data.

Level of Compliance: Credit card companies and financial institutions validate that merchants are rated based on their volume of transactions. The rating that is received determines the process

that a merchant must go through in order to be validated. There are four levels of PCI Compliance, with level 1 being the most stringent and level 4 being the least stringent. If a merchant suffers an attack that has caused account data to be compromised, the merchant level requirement goes up to level 1 automatically.

Merchant - An Academy department or operating unit that has applied for and been approved to accept credit card payments for goods and/or services. A merchant is assigned a specific merchant account, which is used to process all credit card transactions via an Academy-approved payment card processer.

PAN - Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. It is also called an Account Number.

Self-Assessment Questionnaire - The PCI Self-Assessment Questionnaire (SAQ) is a validation tool that is primarily used by merchants to demonstrate compliance to the PCI DSS.

POLICY

General

For the Academy to achieve and maintain PCI compliance, the following requirements must be met:

- All credit card transactions for the Academy need to take place from the Academy's website using Touchnet or on a credit card reader/terminal with an encrypted connection to a third party payment vendor. This will exclude the Academy's network, servers and databases from being part of the payment card environment and will greatly simplify compliance requirements.

- The Academy prohibits any staff member from accepting credit card information or processing credit card payments on behalf of a "customer". This includes storing physical credit cards, as well as writing down credit card numbers for future use.

- It must be confirmed annually that any third party payment vendors and equipment being used by the Academy, such as Touchnet, Heartland or Raiser's Edge, are PCI compliant.

- Credit card readers and processing terminals must be routinely examined for evidence of tampering and any evidence brought to the attention of the Director of Audit and Compliance.

- An accurate list of credit card readers and processing terminals currently in use at the Academy must be maintained and updated on an annual basis.

- All credit card processing machines must be programmed to print-out only the last four or first six characters of a credit card number.
- The manager of a department involved with credit card processing must create and confirm the existence of appropriate procedures for credit card processes, storage, and destruction of card data on an annual basis.

- Any proposal for a new process (electronic or paper) related to the storage, transmission or processing of credit card data must be brought to the attention of and approved by the CFO.

- New credit card merchant accounts or credit card payment processors must be approved by the CFO before being put in place.

- The Academy will contract annually with a qualified third party vendor to complete a PCI Risk Assessment. The deliverable from this engagement will be a written report which identifies any technical risks, gaps or deficiencies which would impact the Academy's PCI compliance. This report will be shared with the Academy's bank by the CFO.

Storage and Disposal

- Credit card data must not be stored on any Academy computer equipment or electronic media, unless it is encrypted and has been explicitly approved for use as part of the Academy's cardholder data environment by the CFO.

- The Academy will perform regular network scans to ensure that unencrypted cardholder data is not present on any Academy-owned computer equipment.

- For paper media (e.g. paper receipts, forms, and faxes), cardholder data should not be stored, unless approved for appropriate business purposes by the CFO and access is limited to individuals with a business need to know. Cardholder data should be "blacked" out on paper media, and disposed of properly (e.g. shredded) when no longer needed for business purposes.

Consequences of Non-Compliance

- PCI non-compliance can result in serious consequences for the Academy, including reputational damage, loss of customers, litigation, and financial costs. Failure to comply with this policy and/or applicable policies, standards, and procedures carries severe consequences which may include:

    - loss of the ability to process payment card transactions,

- departmental repayment of financial costs imposed on the Academy,
- employee disciplinary action, which can include termination of employment.

- The CFO has the authority to restrict and/or terminate merchant account status for non-compliance.

Response to a Security Breach

- In the event of a breach or suspected breach of security, including the suspicion that payment card data has been exposed, lost, stolen, or misused, the merchant must immediately contact the CFO and the CIO.

ENFORCEMENT

Any employee found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action, up to and including termination of employment, per any applicable collective bargaining agreements.

RESPONSIBILITY

This policy is owned by the CFO, who has overall authority to ensure PCI DSS compliance for the Academy, and who will coordinate any and all revisions to the policy.

The Controller shall be responsible for notifying applicable Department Heads about changes to this policy. S/he will be assisted by the CIO and the Director of Audit and Compliance. The Controller is also responsible for the initial setup and ongoing administration of all Academy merchant accounts. Key responsibilities will include approval of merchant applications, procurement of credit card terminals and other equipment, and operations liaison to the Academy's third-party credit card processing vendors.

The Technology and Library Services division is responsible for initiating and overseeing an annual PCI DSS self-assessment and coordinating any remediation activities as required by PCI DSS or other applicable policies and standards. The Technology and Library Services division is also responsible for maintaining and disseminating security policies and procedures that address PCI DSS requirements and testing the Academy's infrastructure and network environment.

REFERENCES

Framework SANS Top 20 Controls	Regulations and Requirements PCI DSS - MA 201 - HIPAA	Supporting Standards and Procedures
	PCI DSS v3.2	

Payment Card Industry Compliance Policy

REVISION HISTORY

This section contains comments on any revisions that were made to this document and the date they were made.

Version Number	Issued Date	Changes Made By	Description of Changes
1.0	8/23/2016	Anne Marie Fallon	Initial Draft
	1/9/2017	Anne Marie Fallon	Continued to update and make edits to draft policy.
	2/16/2017	Anne Marie Fallon	Made edits per Rose Cass.
	2/24/2017		Published on Academy website