



Security Training and Awareness Policy

PURPOSE

The purpose of this policy is to ensure that any user who has access to Massachusetts Maritime Academy's (MMA) information technology-based resources has an understanding of MMA's applicable information security policies and a proven understanding of security awareness.

SCOPE

This policy applies to all faculty and staff who have access to MMA's information technology-based resources.

POLICY

Individuals must understand the risks in using today's technology and how to effectively defend against today's cyber threats, both at work and at home. The primary purpose of an effective information security training and awareness program is to establish and sustain an appropriate level of protection for data and technology resources by increasing users' awareness of their information security responsibilities. Specific objectives of this program include:

- Improving awareness of the need to protect information resources;
- Ensuring that users clearly understand their responsibilities for protecting information resources;
- Ensuring that users are knowledgeable about the Academy's information security policies and practices and develop skills and knowledge so they can perform their jobs securely;
- Maintaining compliance with MA 201-CMR 17, Section 2B.01.

All users will be required to complete security awareness training and training with respect to MMA's information security policies upon hire and subsequently at least annually. MMA will maintain records, as it deems appropriate, that confirm a user has received training. Training may be delivered in person or online.

In addition to annual training, reinforcement training such as newsletters, email messages, digital signage, posters, webcasts and other means will be used on campus. The Security Training and Awareness program will also include unscheduled awareness assessments to ensure compliance with the training.

ENFORCEMENT

Any person who does not complete their mandatory security awareness training by the designated date, may be subject to disciplinary action, up to and including loss of access rights, termination of employment from the Academy.



Security Training and Awareness Policy

RESPONSIBILITY

In conjunction with Human Resources, the Infrastructure Technology department will develop and facilitate the Security Training and Awareness program, ensure all staff receive the appropriate security training associated with their responsibilities, and maintain records of training received.

This policy is owned by the Vice President of Technology and Library Services, who will coordinate any and all revisions.

REFERENCES

Framework SANS Top 20 Controls	Regulations and Requirements PCI DSS - MA 201 - HIPAA	Supporting Standards and Procedures
CSC 9-2, 9-3, 9-4	MA 201-CMR 17, Section 2B.01	

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	1/12/2016	Compass ITC	Initial Draft
2.0	1/22/2016	Anne Marie Fallon	Added SANS framework, changed Responsibility section, additions made to Policy section.
2.0	2/5/2016	Anne Marie Fallon	Incorporated edits from other staff. Published this policy.