Incident Response Policy

PURPOSE

The most effective and least costly way to defend a computer network from threats and attacks is to put in place defense mechanisms and develop solid response procedures before an attack occurs. With a strong and swift response, the issue can be contained and fixed, thereby greatly increasing the survivability and security of the network. In addition, these efforts should limit system downtime, work stoppage and maximize the ability of law enforcement to apprehend the perpetrators.

The purpose of this policy is to define the response of Massachusetts Maritime Academy (MMA) to computer security incidents involving MMA information, systems, applications, hardware, staff members and students.

SCOPE

This policy applies to all MMA computer security incidents. A computer security incident is defined as any attempt, successful or unsuccessful, to disable, compromise, bypass, alter, or by any other means maliciously misuse MMA information, systems, applications, and hardware.

DEFINITIONS

FBI – Federal Bureau of Investigation

FERPA – Family Educational Rights and Privacy Act

HIPPA – Health Insurance Portability and Accountability Act

NCCIC – National Cybersecurity & Communications Integration Center

POLICY

- A computer security incident can be caused by a number of possible actions. Examples of these include, but are not limited to:
    - Unauthorized access to data, especially confidential data (HIPAA, FERPA), personally identifiable information (PII) or credit card data;
    - Outbreak of malware, such as a worm, virus, Trojan Horse, ransomware or botnet;
    - Reconnaissance activities, such as scanning the network for security vulnerabilities;
    - Denial of Service (DoS) attack;
    - Website defacement or hacking;
    - Destructive data manipulation attack;
    - Interference of any type with IT operations;
    - Impersonation of a member of the Academy campus community through electronic and/ or social media, spoofing, or setting up any web presence that purports to be, or

might reasonably be perceived to be, an official MMA website or social media group, page or account;
    - Exploit of a security weakness, such as an unpatched server vulnerability.

- Staff members are required to report computer security incidents to either their manager or to the MMA Help Desk. Students must report computer security incidents to their Company Officer or to the MMA Help Desk.
- All reported computer security incidents must be responded to in a timely manner and handled appropriately, based on the severity of the incident.
- An incident report form must be completed and retained for each incident. The form should be updated as the incident response progresses and contain details regarding the evidence found, the response steps taken and communication
- In response to a security incident, the MMA IT team, in conjunction with additional staff members, will address the following:
    - **Detection** – Corroborate and define the incident.
    - **Assessment** – The incident's severity should be classified (see chart below) based on available information to determine whether network communications require closure or aspects of the Disaster Recovery plan require implementation.
    - **Forensics** - Data related to the incident shall be gathered and analyzed as it is vital to the investigation to have this information. Any logs from affected devices should be kept to aid in the forensic analysis.
    - **Containment** – Measures shall be taken to separate the impacted system(s) from the rest of the Academy's computing environment, if at all possible.
    - **Recovery** – System(s) shall be restored to normal operation as soon as possible, following the applicable procedures for system recovery.
    - **Post-Mortem** – An analysis of the incident, MMA's response to the incident, and lessons learned must be reviewed as soon as the incident has been closed. This includes a review of a post-incident report for any incidents classified with a severity of high.
- An incident's severity should be classified based on the chart below. One or more conditions present in the Characteristics column will determine the severity level.

Incident Response Policy

Incident Severity	Characteristics	Response Time	Incident Manager	Who to Notify	Post-Incident Report Required
High	Significant adverse impact on a large number of systems, services and/or people Potential large financial risk or legal liability to the Academy Threatens confidential or PII data Significant and immediate threat to human safety High probability of propagating to a large number of other systems and causing significant disruption	Immediate	Chief Information Officer	President All Vice Presidents Public Safety Office Media Relations Department managers MA State Police FBI NCCIC	Yes
Medium	Adversely impacts a moderate number of systems, services and/or people Adversely impacts a non-critical enterprise system or service Adversely impacts a departmental scale system or service Disrupts a building or departmental network	Within 4 hours	Appointed by the Chief Information Officer	All Vice Presidents Department managers	No, unless requested by the Chief Information Officer or other appropriate administrator

	Moderate risk of propagating and causing further disruption				
Low	Adversely impacts a small number of non-critical individual systems, services, or people Disrupts a small number of network devices or segments Little risk of propagation and further disruption	By end of next business day	Technical support staff member	Chief Information Officer Department managers	No
FA	"False Alarm" - used for suspicious activities which upon further investigation are determined not to be a computer security incident.				

- Awareness of the requirement to report any suspected computer security incidents is a component of the required Information Security Awareness Training Program for staff. Such training shall be administered as part of the new hire on-boarding process, as well as on an annual basis.

- Additional, role-specific training is administered to IT and other staff as merited by job responsibilities and access level.

1. For incidents involving payment card information (PCI), the following procedures must be adhered to in addition to MMA's procedures. These procedures have been recommended by VISA and MasterCard (and other affected payment card brands) if the compromise involves credit card data:

    - http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html
    - http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf

Incident Response Policy

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 collection bargaining agreements.

RESPONSIBILITY

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

This policy will be added to the Academy's Emergency Operations Plan (EOP) and it will be posted on the Academy's public website.

REFERENCES

Framework SANS Top 20 Controls	Regulations and Requirements PCI DSS - MA 201 - HIPAA	Supporting Standards and Procedures
CSC 18	PCI DSS 12.9	

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	5/9/2016	Anne Marie Fallon	Added SANS framework and made additional edits.
2.1	7/8/2016	Anne Marie Fallon	Added severity table.
2.2	8/10/2016	Anne Marie Fallon	Continued to edit policy.
2.3	8/29/2016	Anne Marie Fallon	Incorporated feedback from Tara McEnroe.
2.4	1/27/2017	Anne Marie Fallon	Added EOP and Academy website as locations for publication of policy.