Physical Security Policy

PURPOSE
The purpose of this policy is to control physical access to Massachusetts Maritime Academy's (MMA) information technology, hardware and systems in order to reduce the risk of damage to these important resources. Damages include the breach of sensitive information and intellectual property, the compromise of system availability, or the corruption of information integrity.

SCOPE
This policy applies to all MMA faculty, staff, contractors, and third parties who have physical access to MMA facilities, information resources, and systems.

POLICY
Computer equipment shall be installed in suitably protected areas with minimal indication of their purpose, inside or outside the building, so as not to identify the presence of information processing activities.

The following controls shall be implemented:

General Physical Security:

- Whenever possible, doors and entrance locations of facilities shall be locked when unattended and protected during non-business hours by electronic alarms.
- A record of the users of physical access controls such as facility keys shall be kept.
- A record of security related repairs and modifications, such as hardware, walls, doors, and locks, to a facility containing protected health information shall be kept.
- Private desk drawers, personal computers, peripherals, and related equipment shall be locked when not in use.
- Back-up media shall be located off-site to avoid damage from a disaster on the campus.
- Protection must be implemented against fire, flood, and other environmental factors that could damage the resources.
- Access to/use of publicly accessible jacks shall be restricted.

Specific requirements for the Data Center:

- Comply with all requirements listed above.
- The Data Center shall be located in a secure environment protected by keys or card access controls to mitigate unauthorized access and use.
- Data Center access shall be restricted to only authorized personnel and authorized third parties when escorted.
- Fire suppression equipment will be installed within the Data Center.

Physical Security Policy

- Emergency power shutdown controls will be installed.
- Equipment is to be located on racks raised above floor level.
- Annual testing will be performed on all fire and protective systems.
- Environmental controls will be implemented to ensure that temperature and humidity are maintained within limits for the equipment contained therein.
- Electrical power for servers hosting enterprise and departmental services must be protected by uninterruptable power supplies (UPS) to ensure continuity of services during power outages and to protect equipment from damage due to power irregularities. Each UPS should have sufficient capacity to provide at least 15 minutes of uptime to the systems connected to it.
- All network information technology resources must be fitted with effective Surge Protectors to prevent power spikes and subsequent damage to data and Hardware.
- Secured access devices (e.g. access cards, keys, combinations, etc.) must not be shared with or loaned to others by authorized users.

Visitor Security:

- Third party support services personnel shall be granted access to secure areas only when required, authorized, and supervised.

ENFORCEMENT

Any person found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action, up to and including loss of access rights, termination of employment or expulsion from the Academy.

ROLES AND RESPONSIBILITIES

Under the direction of the Vice President of Technology and Library Services, the TLS Directors are responsible for coordinating and establishing procedures and practices which are necessary for compliance with this policy.

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

Physical Security Policy

REFERENCES

Framework SANS Top 20 Controls	Regulations and Requirements PCI DSS - MA 201 - HIPAA	Supporting Standards and Procedures
CSC 10		

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 ITS	Initial draft
2.0	3/7/2018	Anne Marie Fallon	Edits made to policy
2.0	3/21/2018	Anne Marie Fallon	Edits made to policy
2.0	3/21/2018	Anne Marie Fallon	Emailed for review
2.0	4/3/2018		Policy published