Remote Access Policy

PURPOSE
The purpose of this policy is to define the process and requirements for connecting to the Massachusetts Maritime Academy (MMA) network from a remote host. These requirements are designed to minimize damages, which may result from unauthorized use of computing resources. Damages include the breach of sensitive information and intellectual property, damage to public image, damage to critical internal systems, the compromise of system availability, or the corruption of information integrity.

SCOPE
This policy applies to all MMA employees, contractors, and third parties who access MMA applications, systems, or hardware remotely.

POLICY
All remote access to MMA applications, systems and hardware must be authorized, approved and documented. Any access not authorized and approved is forbidden. Due to the risks involved with remote access, MMA will authorize and approve remote access for a very limited number of staff members.

Remote access to specific applications, systems, components and technology infrastructure shall only be granted to personnel with a legitimate business need. The level of access granted and privileges assigned shall be limited to the minimum required to perform the assigned duties.

Staff members authorized to utilize remote access shall ensure that unauthorized users are not allowed access to the MMA network while utilizing these connections. All individuals, while accessing the MMA network, with either company-owned or personal equipment, are a de facto extension of MMA's network and therefore their machines are subject to the same rules and regulations as stated in any applicable MMA policy.

All devices that are connected to the MMA network via remote access must use the most up-to-date anti-malware software and be current on available patches. Security patches for installed operating systems (with auto-update enabled), web browsers, and common applications shall be applied in a timely manner. A personal firewall must be installed and enabled on each applicable device utilizing remote access.

Staff members agree to apply safeguards to protect MMA information assets from unauthorized access, viewing, disclosure, alteration, loss, damage or destruction. Appropriate safeguards include use of discretion in choosing when and where to use remotely accessed data or services and to ensure the prevention of inadvertent or intentional viewing of displayed information.

Remote access to data or services may not be used to copy private, confidential or personal information from any MMA system, hardware or files.

Remote Access Policy

To request remote access, a staff member should contact the MMA Help Desk with the specifics of their remote access needs. The request will be reviewed and the staff member will be contacted with a response regarding whether or not their request has been approved.

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.

REFERENCES

Framework SANS Top 20 Controls	Regulations and Requirements PCI DSS - MA 201 - HIPAA	Supporting Standards and Procedures
CSC 1, 2, 14		

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	3/6/2018	Anne Marie Fallon	Additions made to policy
2.0	3/21/2018	Anne Marie Fallon	Additional edits made. Emailed for review.
2.0	4/3/2018		Policy published

Remote Access Policy