Maine Maritime Academy
Information Technology Department
Network Acceptable Use Policy

Purpose

This Policy Statement applies to all users of the Maine Maritime Academy ("MMA") network system. Expressly, this policy applies to any person connected to and using any MMA provided network resources, wired or wireless. This Policy Statement establishes important guidelines and restrictions regarding any use of network systems at MMA. MMA's network is a valuable tool for accomplishing MMA's daily academic, educational, public service, and research initiatives.

Definitions

For the purposes of this Policy Statement, the following definitions shall apply:

"*Computing resources*" shall be defined as all devices and services (including, but not limited to, personal computers, laptops, tablets, smart phones, software and services) owned or provided by MMA, the user or otherwise, which are part of or are used to access (1) the MMA network, peripherals, and related equipment and software; (2) *data* communications infrastructure, peripherals, and related equipment and software; (3) voice communications infrastructure, peripherals, and related equipment and software; (4) and all other associated tools, instruments, facilities, and the services that make use of any technology resources owned, operated, or controlled by MMA. *Computing resources* or components thereof may be individually assigned or shared, single-user or multi-user, stand-alone or networked, and/or mobile or stationary.

"Data" shall include all information that is used by or belongs to MMA or that is processed, stored, maintained, transmitted, copied on, or copied from MMA *computing resources*.

"*Forged communications*" (sometimes referred to as "spoofing") shall be defined as e-mails that are made to appear as if they originated from an organization or individual other than the individual from whom the message was actually sent.

"Protected information" shall be defined as *data* that has been designated as private, protected, or confidential by law or by MMA. *Protected information* includes, but is not limited to, employment records, medical records, student records, education records, personal financial records (or other individually identifiable information), research *data*, trade secrets, and classified government information. *Protected information* shall not include public records that by law must be made available to the general public. To the extent there is any uncertainty as to whether any *data* constitutes *protected information*, the *data* in question shall be treated as *protected information* until a determination is made by MMA or other legal authority.

General Policy

Access to MMA's network is provided throughout the campus via both wired and wireless connectivity. All policies and guidelines pertain to both wired and wireless service.

MMA network users are required to comply with federal and state law, MMA policies, and standards of professional and personal ethics. All communications sent via MMA's network shall be consistent with applicable administrative policies, are subject to discovery, and remain the property of MMA.

Individuals to whom MMA network access accounts are assigned are responsible for managing and

monitoring their accounts, and for actions taken with their accounts. Accounts and account passwords are not to be sold, rented, transferred, or shared with any other person.

The following activities are strictly prohibited on MMA's network systems:

- Extension of the network by use of SWITCHES, HUBS, ROUTERS, WIRELESS DEVICES or any other appliance which provides NAT (Network Address Translation).
- Downloading and/or sharing of copyrighted material without the express consent of the copyright owner, including but not limited to MP3 files, movies, and licensed software.
- Accessing and/or attempting to access any computer system without authorization.
- Scanning of any system for open ports or other vulnerabilities.
- Capturing data packets of any kind for any reason.
- Operating any network services including but not limited to DIRECT CONNECT, DHCP, DNS, SMTP, FTP, IRC, or hosting any FILE SHARING SERVERS.
- Using network resources for commercial purposes.
- Sending or relaying SPAM messages.
- Any activity which disrupts the network, including excessive downloading or use of a computer infected with worms and viruses.

Protected Data and Approved Collaboration Services

Protected institutional and personal information shall not be sent via the network unless specific steps are taken to ensure that the transmission is secure and encrypted in accordance with MMA standards, and the personal information is therefore provided this additional level of protection.

Approved methods of sharing *protected institutional and personal information* will be used at all times in order to assure the security and safety of such data. Approved collaboration services and techniques include:

- MS365 - Office, Teams and OneDrive
- SeaFile
- Shared Network Drive(s)
- Zoom
- Mailgate Secure Mail

Anything not listed above should **NOT** be used for official MMA business.

Eligibility

The use of MMA's network is a privilege granted by MMA, in its sole discretion, to facilitate the MMA's mission and operations. Network access will be provided to active faculty and staff, currently enrolled students, long term contractors and MMA Board of Trustees members. Network eligibility ends when an individual's affiliation with the MMA is terminated. Students who are dis-enrolled from MMA will also lose their network privileges.

A special Guest network is provided for conference guests and other visitors. Access to this network may be gained by contacting the Conferences department.

The following items are requirements for maintaining access to Maine Maritime Academy's network

resources:

- Computers and other devices must be registered with MMA's access control system.
- An Anti-Virus program must be installed and kept up to date with current virus signatures and appropriate system patches.
- Computers must be up to date with operating system patches and vulnerability hot fixes.

Cybersecurity Awareness Training

MMA regularly conducts mandatory cybersecurity training and testing. Those users who do not pass routine testing must participate in additional training sessions. Failure to participate may result in the suspension of network privileges.

Personal Use

Employees may use MMA provided network resources for personal use so long as that use does not create any cost to the MMA, does not interfere with the employee's official duties, is brief and its volume or frequency does not disrupt MMA business, does not compromise the security or integrity of MMA data or systems, and is not commercial in nature. It is important to note that while personal use of the network is permitted, records pertaining to those activities are still considered public record, are subject to administrative and legal policies and discovery, and remain the property of MMA.