CAMPUS POLICY DIRECTIVE

MARITIME MOBILE DEVICE POLICY

Policy Number	Responsible Department	Effective Date	Page
13-002	Information Technology	May 10, 2013	Page 1 of 12

1. PURPOSE

This policy directive establishes Maritime College's standards for the effective and secure use and management of mobile devices. To preserve the integrity, availability and confidentiality of Maritime Campus and SUNY data, this document establishes standards for the use of mobile devices and their connections to campus and SUNY networks. This document also outlines the procedures for managing risks associated with the loss and theft of mobile devices that store Maritime data and the provisions in governing Bring Your Own Device (BYOD).

In addition, this policy directive seeks to establish controls to ensure compliance with New York State Cyber Security Policy P03-002, Communication and Network Management Policy, Portable Devices.

2. SCOPE

This policy directive applies to:

1. Maritime College and all current and future subsidiary/affiliated entities of the college.

2. All directors, officers and employees of Maritime College or employees of any future Subsidiaries or Affiliated Agencies of Maritime College.

3. Any third-party entity or person who is authorized to use, or possess a mobile device owned, managed or controlled by Maritime, including any mobile device account.

4. All existing, upgraded and newly provisioned mobile devices that connect to a Maritime campus managed network – whether or not the campus purchased or employee is participating in the BYOD program.

3. DEFINITIONS

1. App Store - Any platform for uploading and downloading applications for free or for purchase to a mobile device.

2. Encryption - The process of transforming plain text data to render it unintelligible through the use of a cipher key that is able to encode and decode information. This technique is used to secure data on a device and make it available only to authorized users with the credentials to view the data. It is an important security tool to protect the confidentiality of information and mitigate the threat of unauthorized access to data.

3. GPS tracking system - Global positioning system that may be used to identify and monitor the location of objects and people in real-time.

4. Laptop computers – Battery or AC-powered personal computers that are small and light enough to be easily transported. They are conveniently used in temporary spaces such as on airplanes, in libraries, temporary offices, and at meetings, but also are used as in-dashboard monitors of company cars. Notebooks and "ultrabooks" are categorized as laptops.

5. Mobile device - Any easily transportable device that is capable of receiving and/or transmitting data to and from Maritime or SUNY information resources. Examples of currently existing mobile devices include, but are not limited to, smartphones, tablets, laptop computers, computers installed in a vehicle, and pagers as well as portable devices like RFID scanners, bar code readers and USB drives. In this policy, it is interchangeable with "portable computing device.

6. Personal, private and sensitive information ("PPSI") - Any information where unauthorized access, disclosure, modification, destruction or disruption of access to or use of such information could severely impact Maritime College, its critical functions, its employees, its

customers, third parties, or citizens of New York . This term shall be deemed to include, but is not limited to, the information encompassed in existing statutory definitions.

PPSI includes, but is not limited to:

a) Information which, pursuant to law, is confidential such as medical information subject to HIPAA, FERPA or SUNY 6608.
b) Information concerning a person which, because of name, number, personal mark, or other identifier, can be used to identify that person alone or in combination with:
   - Social Security Number;
   - driver's license number or non-driver identification card number;
   - mother's maiden name; or
   - Financial account identifier(s) or other information which would permit access to a person's financial resources or credit.
c) Information used to authenticate the identity of a person or process (e.g., PIN, password, passphrase and biometric data). This does not include distribution of one-time-use PINs, passwords, or passphrases.
d) Information that identifies specific structural, operational, or technical information, such as maps, mechanical or architectural drawings, floor plans, operational plans or procedures, or other detailed information relating to electric, natural gas, steam, water supplies, nuclear or telecommunications systems or infrastructure, including associated facilities, including, but not limited to:
   - training and security procedures at sensitive facilities and locations as determined by the New York State Office of Homeland Security (OHS)
   - descriptions of technical processes and technical architecture;
   - plans for disaster recovery and business continuity; and
   - reports, logs, surveys, or audits that contain sensitive information.
e) Security related information (e.g., vulnerability reports, risk assessments, security logs).

f) Other information that is protected from disclosure by law or relates to subjects and areas of concern as determined by Maritime executive management.

6. Portable computing device - See "Mobile device."

7. Smartphone – A cellular telephone with built-in applications and Internet access. They are built on a mobile operating system with advanced computing capability and connectivity.

8. Tablet – A one-piece mobile computer that is primarily operated by touchscreen. They are built on a mobile operating system with advanced computing capabilities that allow for app downloads and Internet use.

9. Users - Maritime employees, directors, officers and any other entity or individual provided with an Maritime- mobile device, or anyone using a non-Maritime owned mobile device to access Campus-managed internal networks, applications (including email) or any other forms of data.

4. POLICY

A. In Accordance with This Policy Directive, Users:

1. Employees who are not eligible for an organization-funded mobile device or wish to use their personal device to connect to (Maritime email systems) or other corporate resources, can request access as long as the device meets Maritime requirements and the employee has signed this policy after receiving manager approval of inclusion into the BYOD program.

2. Shall ensure that all portable computing resources and information media (including data stored on mobile devices) are secured to prevent compromise of confidentiality.

3. Shall use care to avoid the risk of any unauthorized person possessing a mobile device or viewing a mobile device screen in use anywhere, including but not limited to a public place, meeting room and any other areas outside of or within Maritime premises.

4. Shall not store or transmit PPSI on a mobile device without installation and use of Maritime and NYS-approved encryption measures and approval of the owner of the PPSI data. According to NYS security policy, all PPSI must be encrypted where stored and when transmitted.

5. Shall ensure that a mobile device containing PPSI is attended at all times or physically secure from unauthorized possession, use, or access.

6. Shall, when traveling, maintain possession of the mobile device, except where other arrangements are required by Federal or State authorities. For example, do not check or place a mobile device in your checked luggage when traveling by air, rail, taxi, or other transportation system.

7. Shall immediately report lost or stolen devices to Maritime Technical Support Center (TSC) that contain Maritime data.

8. Shall utilize only Maritime-approved portable computing devices to access Campus information and its network.

9. Shall complete all required training, including update and refresher training, regarding using and administering mobile computing resources.

10. Shall be aware that as with all other computing devices, there is no expectation of privacy on a device that is used to transact or communicate Maritime Campus business.

11. Shall not obstruct any features that allow Maritime College to "wipe" or manage smartphones and tablets. Security controls must not be bypassed or disabled. Each user has the responsibility to back up any personal data and application downloads since the remote wipe may erase all data on the smartphone or tablet. Maritime bears no legal or financial responsibility for loss or effect to personal data or for applications downloaded by the user to these devices which are lost or affected as a result of this security wipe.

12. Shall provide Maritime with the necessary cooperation and access to enable college staff to install additional security and management software for controlling authorized devices.

13. Agree that the Maritime security policy and standards shall apply to personal devices used by the employee that are connected to the network.

14. Acknowledges that Maritime will not support personal apps and that these apps will be removed if they pose a security threat.

15. Shall agree to and sign the attached acknowledgement form.

5. In Accordance with This Policy Directive, Maritime employees Must Ensure:

1. Secured implementations include review of physical protection, access controls, encryption techniques, archival practices, virus protection and the rules associated with connecting mobile devices to networks and guidance on the use of those devices in public places.

2. Secured implementations include review of physical protection, access controls, encryption techniques, archival practices, virus protection and the rules associated with connecting mobile devices to networks and guidance on the use of those devices in public places.

3. All mobile devices containing MTA data – whether or not they contain PPSI -- must be encrypted. Maritime must provide a mechanism for encrypting or ensuring devices connecting to the network are able to encrypt data.

4. Secured implementations include review of physical protection, access controls, encryption techniques, archival practices, virus protection and the rules associated with connecting mobile devices to networks and guidance on the use of those devices in public places.

5. Protection including, but not limited to cryptographic technique and password protection, is installed, updated and in use to protect against unauthorized access to or disclosure of the information stored or processed by these devices.

6. Approval of an individual employee's use of a mobile device is contingent on the employee complying with the requirements for physical protection, access controls, cryptographic techniques, the rules associated with connecting mobile facilities to networks and guidance on the use of these facilities in public places.

7. Training is provided to staff using and administering mobile computing resources to assure their awareness of the controls and precautions that must be implemented and the risks resulting from this way of working.

8. Only authorized personnel may use mobile devices to access Maritime information resources.

6. Maritime Employees Shall Comply with the Following Standards

1. Each agency shall implement a mobile device management solution for managing and controlling devices that access Maritime Campus data. This policy applies to mobile devices provided by Maritime College and to mobile devices not provided by Maritime.

2. Mobile devices which are modified to operate outside the normal operation for which they are designed and manufactured (commonly referred to as "jailbroken") are prohibited from storing Campus data or accessing the Maritime Campus network.

3. Smartphones and tablets that contain Maritime information must have functionality that permits and enables Maritime to remotely wipe (i.e., delete) information from the device.

4. A smartphone or tablet that contains Maritime information must have functionality that cannot be blocked, that permits and that enables Maritime to remotely lock or remove data from the device.

5. Maritime leadership must establish a list of supported and approved mobile devices. Devices not on that list may not be used.

6. Maritime technical staff will track and inventory all Campus-issued and Campus-supported mobile devices.

7. Encryption that meets Maritime's standards is required for all wireless transmission to and from mobile devices that access or contain Campus data.

8. Maritime shall maintain and update a list of non-campus supported devices which have been approved to access Campus information and network as well as maintain an inventory of the registered owner and use.

9. Maritime must be able to identify mobile computing assets that it issues and/or manages as well as be able to identify associated users of these devices.

10. Maritime may determine to limit access to or installation of certain applications on personal mobile devices.

11. Maritime shall allocate resources to educate employees about the potential issues associated with connecting a personal device to a corporate network.

12. Mobile device platforms must offer controls that minimize the effects of a device that exposes PPSI.

13. Only Maritime approved devices, application and app stores for the supply of approved applications will be allowed.

14. GPS may be necessary to locate loss or stolen devices. For this reason, mobile devices that have GPS capability are subject to GPS location monitoring if lost or stolen. Restrictions to this monitoring are subject to management approval.

15. Once Bluetooth pairing has been obtained on authorized devices, Bluetooth discovery must be turned off.

7. Compliance

Maritime College will enforce this policy, including consequences for failure to comply with this policy. Consequences may include up to and including termination of employment.

8. Policy Lifecycle Review

This policy will be reviewed on as needed basis or no less than annually. Such review will include but not be limited to consideration of upgraded and new mobile technologies, experience with this policy, and new and revised applicable legal requirements.

9. Attachments

NYS Cyber Security Policy P03-004

CAMPUS POLICY DIRECTIVE

MARITIME MOBILE DEVICE POLICY

Policy Number	Responsible Department	Effective Date	Page
13-002	Information Technology	May 10, 2013	Page 11 of 12

MOBILE DEVICE POLICY
USER ACKNOWLEDGMENT FORM

This policy is associated with *Maritime's Acceptable Use Policy and NYS controls of mobile devices.* Note that with any similar, overlapping or stricter provisions set forth in both the documents, the more restrictive provisions will be enforced.

Employee Declaration

I, [employee name], have read and understand the Mobile Device Policy, its policy and procedures, and consent to adhere to the rules outlined therein.

_____ _____
Employee Signature Date

_____ _____
Employee's Manager Signature Date

_____ _____
Information Security Officer Signature Date

CAMPUS POLICY DIRECTIVE

MARITIME MOBILE DEVICE POLICY

Policy Number	Responsible Department	Effective Date	Page
13-002	Information Technology	May 10, 2013	Page 12 of 12

Revisions:

REVISED BY	DATE