MARITIME COLLEGE
STATE UNIVERSITY OF NEW YORK

CAMPUS POLICY DIRECTIVE

INFORMATION SECURITY POLICY

Policy Number	Responsible Department	Effective Date	Page
14-001	Maritime College	Jun 1, 2014	Page 1 of 7

1. POLICY STATEMENT

Maintaining the security, confidentiality, integrity, and availability of information stored on Maritime College's computer systems and data communications infrastructure ("Maritime systems") is a responsibility shared by all users of those systems. All users of Maritime systems are responsible for protecting those resources and the information processed, stored, or transmitted thereby as set forth in this policy in support of the Maritime Information Security Program. Violations of this policy may result in disciplinary action up to and including termination of employment.

2. PURPOSE

To eliminate or reduce, to the maximum extent possible, the risk of unauthorized access, modification, disclosure, or destruction of sensitive information; or the denial of services of authorized users to access information and information systems. This policy sets forth the requirements for incorporation of information security practices into daily usage of Maritime systems.

3. SCOPE

This policy pertains to faculty, staff, students, and all others, including outsourced third parties, to include consultants, contractors, vendors, and volunteers which have access to or manage Maritime Information Systems. It is not intended to unilaterally change the terms and conditions of employment.

4. POLICY

It is the policy and responsibility of the College to fully comply with legal and regulatory requirements governing the collection, retention, dissemination, protection, and destruction of information. Therefore the College is committed to protecting the privacy and confidentiality of information contained in the multiple databases, file shares, print, and other physical files maintained by the College in the regular course of business. Personal information that is confidential in nature will be used only in accordance with the SUNY Maritime College Information Security Program, Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and all applicable SUNY, state and federal regulations.

Select employees at SUNY Maritime College, by nature of their positions and as required for the business of the College, will have access to Personal, Private, and Sensitive Information (PPSI) about students, faculty, staff, alumni, donors, and other constituents of the College which is maintained on Maritime systems and devices or private networks or devices

where College business is being conducted. Employees are obligated to maintain the confidentiality of any such PPSI they encounter.

SUNY Maritime College expects all employees with access to PPSI to deal with that information in a respectful and professional manner. As a matter of policy, the College restricts access to PPSI to only those employees who have a legitimate "job-related reason" for gaining access. Access and release of any student educational records must be in accordance with FERPA regulations. Any personal information viewed or accessed by an employee through College systems or records is not to be shared or released to others unless there is a legally permissible purpose for doing so.

Employee, student, financial, health and medical information contained within SUNY Maritime College information systems and physical files, and in SUNY System Administration systems, are considered confidential. Access to information made confidential by law, policy, or campus practice is limited to those individuals whose position legitimately requires use of this information.

Employees and others with authorized access to confidential data by virtue of their work for SUNY Maritime College must not disclose such confidential data to any person or entity without appropriate authorization, subpoena, or court order.

SUNY Maritime College has classified the following as sensitive data categories:

- **Social security numbers** (as well as national identification numbers for foreign nationals)
- **Passport numbers**
- **Driver's license numbers or non-driver identification card numbers**
- **Financial/banking account numbers, credit or debit card numbers**
- **Financial records & tax documents** (for students, or their family who submit them for financial aid purposes)
- **Education records**: including transcripts, grade information, payment/tuition records, records pertaining to academic standing
- **Student judicial/disciplinary information**
- **Health records**

- ❑ **Home address/telephone information**
- ❑ **Maiden name (or parent's surname prior to marriage)**
- ❑ **Biometric records** (such as fingerprints)
- ❑ **Passwords** (including a person's own password)

For any data types not listed here, employees should make a reasonable judgment about whether that data should be treated as confidential or employee should seek advice from their supervisor, in accordance with Guideline 13 below.

In order to protect personal and confidential information maintained by SUNY Maritime College, employees, student workers and other authorized personnel agree to adhere to the following guidelines:

1. Employees understand and acknowledge that improper use of data in the College's information systems is a violation of SUNY Maritime College policy, and it may also constitute a violation of federal and/or state laws.
2. Employees will not provide confidential information to any individual or entity without proper authorization.
3. Employees will not access, use, copy, or otherwise disseminate information or data that is not relevant and necessary to perform their specific job-related duties.
4. Employees will not remove confidential information from College facilities except as specifically authorized to do so.
5. Employees will not share their passwords with anyone (including supervisors and subordinates) or provide access to systems for other individuals using their logon.
6. Employees will not use any confidential College-related data for personal or commercial purposes.
7. Employees will refer all requests for student educational records from law enforcement, governmental agencies, and other external entities to the Registrar. All other Freedom of Information Law (FOIL) requests must be forwarded to the FOIL Officer.
8. Employees will not communicate to the general public the personally identifiable information of any SUNY Maritime College employee or student.

9. Employees will report any unauthorized access to confidential data immediately to their supervisor and to the Information Security Officer as per the Maritime College Incident Response Policy.

10. Employees understand that any improper or inappropriate use of data in the College's information systems may result in disciplinary action pursuant to the applicable collective bargaining agreement, with sanctions up to and including termination of employment.

11. Employees are not permitted to store any sensitive data on external or portable media such as external hard drives, flash drives, CDs, DVDs, tapes, etc. without encryption and with the express written authorization from the Chief Information Officer or the Information Security Officer. Storing such confidential data on local computer drives on office computers or laptops is strongly discouraged. College owned computers (and personal computers which are routinely used for College business) may be scanned periodically to check for confidential information stored on the device.

12. Employees storing confidential data on College servers must, on an operation basis, remove files containing confidential data when it is no longer needed.

13. Employees who are uncertain about what constitutes legitimate use or release of information should always error on the side of caution and refer their questions about appropriateness of a request for personal information from Maritime systems or records to their supervisor before releasing the information.

14. The transmission of confidential information via email (on or off campus) is not permitted unless the transmission is encrypted and between parties who possess a legitimate need-to-know in the performance of their professional duties; and whereby other means of lesser risk is not available.

15. Transmission of an individual's own personal information via email to an external network is only permitted once the requestor has been advised of the College email policy stating "SUNY Maritime College cannot guarantee that the electronic information will be private". If the requestor agrees after being advised, the information may then be emailed to the individual.

16. Transmission of confidential health information via email is not permitted.

17. Employees should encrypt files before transferring to external third parties outside of the campus network.

18. Employees must ensure physical confidential information is kept secure. Keep drawers and file cabinets with confidential information locked; confidential information whether in paper or in any electronic device should not be left on desks or open areas accessible to the public; all confidential information no longer needed or required to be maintained (see SUNY Record Retention Policy) should be properly shredded (crosscut) to ensure confidentiality; and employees should not discuss private confidential information in public where it can be overheard.
19. Ensure that all mobile devices are password protected and kept secure.

PROCEDURES

Supervisors are required to review this policy with each employee assigned to their department. During the department orientation process, supervisors should provide each employee with a description of the type(s) of confidential information their specific position will work with in the performance of their duties. Supervisors shall review this policy on an annual basis with their staff and confirm that each employee has read, understood, and agreed to this policy via signature.

REVISIONS

REVISED BY	DATE

CAMPUS POLICY DIRECTIVE

INFORMATION SECURITY POLICY

Policy Number	Responsible Department	Effective Date	Page
14-001	Maritime College	Jun 1, 2014	Page 6 of 7

RELATED DOCUMENTS

SUNY Procedure #6608

NYS Cyber Security Policy P03-002 – Information Security Policy
SUNY Regulation 6691

Federal Educational Rights and Privacy Act (FERPA)

Health Insurance Portability and Accountability Act (HIPAA)
Gramm Leach Bliley Act (GLBA)

NYS Information Security Breach & Notification Law
NYS Business Law and Technology Law
NYS Governmental Accountability, Audit & Internal Control Act

Other State and Federal regulations governing the acquisition, retention, and dissemination of protected data SUNY system-wide information security policies and requirements
SUNY Policies of the Board of Trustees

Information Security Practices Recommended by NYS
Community Rights & Responsibilities
Other University IT and Information policies

INFORMATION SECURITY POLICY
USER ACKNOWLEDGMENT FORM

Employee Declaration

I, [employee name], have read and understand the Information Security Policy, and consent to adhere to the provisions outlined therein.

_____ _____
Employee Signature Date

_____ _____
Employee Manager's Signature Date

_____ _____
Information Security Officer Signature Date