THE CALIFORNIA MARITIME ACADEMY

POLICY NO. 208.5

ISSUE DATE: February 15, 2000 **REVISION DATE:**	**POLICY: Information Technology Roles and Responsibilities**
REFERENCE:	
APPROVED: **/s/ Jerry A. Aspland**	

I. Policy Statement

The California Maritime Academy (the Academy) Information Technology (IT) resources must be adequately managed and controlled. Roles and responsibilities must be clearly defined to ensure proper monitoring and control of access to Academy IT resources.

All Academy IT resources must have a designated resource *owner*. The resource owner will be responsible for setting up guidelines for access, granting of access, and for the monitoring of access to their resource.

The resource owner may delegate this authority, however, the resource owner remains responsible for access to their resource.

II. Principles

In accordance to Information Systems Security Policy 208.1, *Access to Computer Resources*, all information resources must have a designated owner. This owner is responsible for authorizing, approving, setting-up, and monitoring of access to their resource.

Any of these functions may be delegated, however, the resource owner still remains responsible for access to their resource.

When these functions are delegated, roles and responsibilities must be carefully delineated and documented. The resource owner must develop procedures to monitor that the delegated functions are being properly handled.

III. Deployment

A steering committee will be developed to ensure that the appropriate party is assigned responsibility or ownership.

The Information Systems (IS) Department has the responsibility for:

- Coordinating the security function of the organization. This includes routing of access forms to appropriate resource owners.
- Developing guidelines for password management and communicating these guidelines to users.
- Ensuring that proper software application development and maintenance procedures are developed, followed, and documented.
- Coordinating with Human Resources to ensure that company property (including confidential information in hard-copy or electronic forms) is collected before Academy employees and non-Academy persons receive their final paycheck.
- Setting guidelines for the installation, physical protection and maintenance of computing and communications hardware.
- Participating in testing and authorization of system software.
- Protecting the campus centralized IT resources with appropriate physical security.

Resource owners are responsible for:

- Updating and reviewing policies as changes are made within their organization and IT environment.
- Managing the security of their resource
- Documenting security violations and response.

There will be a department on campus responsible for:

- Ensuring passwords and all use of the system is in compliance with the policies.
- Reviewing and auditing system software changes.
- Auditing assigned access levels.
- Auditing to ensure that access reports are reviewed.

All Academy employees and users with access to campus systems are responsible for:

- Understanding and complying with information systems security policies.
- Safeguarding campus resources and information by obtaining prior approval from the IS Department for user IDs and modem access, and following password management guidelines.

- Protecting campus resources and IT facilities by abiding by security policies and protecting the campus' proprietary and confidential information.
- Ensuring the smooth flow of campus operations by reporting any breach in information systems security to the IS Department.

IV. Technical Architecture

The overall technical architecture to be used in the organization should be defined in the campus Information Systems strategic plan. The overall structure of security should be contingent upon the technologies and software to be used to meet Cal Maritime's overall goals and objectives.

V. Monitoring

The IS Steering Committee is responsible for monitoring the above mentioned roles and responsibilities.

VI. Documentation Requirements

The IS Department is responsible for developing guidelines for password management. In addition, IS should ensure that proper software application development and maintenance procedures are set and documented.

Resource owners are responsible for updating policies as changes are made within their organization and IT environment. Resource owners are also responsible for setting up guidelines for access to their resource.

System owners have the responsibility of documenting security violations.

VII. Definitions

Owner: A designated person who is responsible for system and user administration functions including system maintenance and add/change/delete access granted.

VIII. References

Access to Computer Resources, Policy 208.1