THE CALIFORNIA MARITIME ACADEMY

POLICY NO. 208.1

ISSUE DATE: **March 13, 1997** **REVISION DATE:** **February 15, 2000**	**POLICY:** **Access to Computer Resources**
REFERENCE:	
APPROVED: **/s/ Jerry A. Aspland**	

I. Policy Statement

The California Maritime Academy's (the Academy) campus information and the information technology require protection against unauthorized access or use.

Access to campus information, computer resources and facilities must be properly authorized, managed and monitored. Access granted to any Academy information system resources must be appropriate according to the user's job description, and strictly on a need to know basis. In all cases of access, there should be a method to authenticate the identification of the user (e.g. password, access card, etc.).

II. Principles

All shared networks, platforms, computer systems, and applications (including purchased packages) will have access control mechanisms that can uniquely identify and restrict the privileges of each user. This control mechanism must have a method to authenticate the user (in most cases this will be the use of a password). Personal productivity software used on a stand-alone computer should be controlled, however, access control software of the type described above may not be available. Access to these standalone computers should normally be controlled through the physical security in accordance to Policy 208.19, *Physical Security of Information Systems Facilities and Resources.*

All information system resources at the Academy must have a designated "*owner*". The owners are responsible for authorizing, approving, and setting up security access to the Academy employees and *non-Academy persons*.

Once access to resources is granted, users are required to comply with all security policies and procedures.

All users of campus information and system resources are responsible for protecting proprietary and confidential information in accordance with Policy208.18, *Data Confidentiality, Security and Handling.*

This policy applies to access to all platforms, systems, and applications at the Academy. See the table of contents for additional guidance in specific areas.

III. Deployment

All access requests must be submitted to and approved by the designated resource owner. The resource owner may delegate this responsibility to others, however, the resource owner remains principally responsible for the monitoring and review of access to the respective resource. Sufficient personal information must be supplied on the access request and the user must sign an acknowledgment stating that he/she understands and will comply with this policy before access is granted.

Guest and group IDs are discouraged unless a valid business reason is presented. Each ID must be unique to ensure accountability of activities performed with the ID. The owner of the ID/access granted is responsible for the use of the ID/access. *Privileged IDs* will only be granted to authorized personnel with a valid business reason and must be monitored on a routine basis. Privileged IDs should be sparingly granted (typically 2-3 IDs per system).

When a user's job description changes due to termination or transfer, his/her access to all systems must be reviewed by the system owner to determine whether or not any changes/additions/deletions need to be made. The system owners must be informed of any changes in user access immediately (in the case of termination, access must be removed within 24 hours).

IV. Technical Architecture

All logical access granted will have a password or an access code that can be used to identify the person using the access. The password or the access code must conform to Information Systems Security Policy 208.17, *Password Management*. The number of unsuccessful attempts allowed to gain access is three. After three unsuccessful attempts, the access will be suspended.

In systems/applications containing sensitive and confidential information, users will be automatically logged-off after a 15 minute period of inactivity. A password-protected screen saver will be used if the automatic log-off option is not available.

V. Monitoring

All IDs, logon attempts, access to, and activities performed in all systems at the Academy are subject to monitoring regularly by system owners. Any IDs or access that have been unused or dormant for more than 90 days will be suspended or removed.

VI. Documentation Requirements

All access requests and signed acknowledgments will be maintained and kept by the system owners.

VII. Definitions

Non Academy Persons: Contractors, vendors, customers, or affiliates.

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

Privileged IDs: IDs with 'read', 'write' and 'execute' access to powerful applications/utilities, system configurations, or security-related functions, such as 'root' in UNIX, IDs with supervisory rights in Novell etc.

VIII. References

Password Management, Policy 208.17

Data Confidentiality, Security, and Handling, Policy 208.18

Physical Security of Information Systems Facilities and Resources, Policy 208.19