THE CALIFORNIA MARITIME ACADEMY

POLICY NO. 208.4

ISSUE DATE: **March 13, 1997** **REVISION DATE:** **February 15, 2000**	**POLICY:** **System Administration**
REFERENCE:	
APPROVED: **/s/ Jerry A. Aspland**	

I. Policy Statement

The California Maritime Academy's (the Academy) Information Technology (IT) environment must be managed and controlled to prevent unauthorized access to Academy information, and to ensure that IT resources are available to authorized users.

All systems at the Academy must have a designated Resource *Owner* who is responsible for managing and administering the IT *resource*. The owner may delegate the responsibility of managing the system to others, such as a *System Administrator*.

II. Principles

Resource Owners or designated System administrators are responsible for managing and controlling their computing resource and configuring their environment to comply with campus policies. The IS Department is responsible for communicating to the System Owners/Administrators requirements on configuring their resource.

III. Deployment

Access to system resources must be granted strictly on an as-needed basis. *Privileged IDs* with access to add or change resource configurations will only be assigned to the resource owner or designated System administrators.

IV. Technical Architecture

Dangerous applications (e.g. *Trivial File Transfer Protocol (TFTP)* or *Telnet* in the UNIX environment, etc.) should be carefully controlled.

Group user profiles should be used when setting up user IDs. Resource owners should also develop individual *baseline configurations* for the resource they are responsible for.

Resource owners of the designated System administrators are also responsible for ensuring all production data files, programs, operating systems and other critical system files are backed up periodically and stored off-site according to the requirements in the Disaster Recovery Plan (DRP).

V. Monitoring

Critical activities such as repeated illegal attempts to gain access, or access to sensitive information will be logged and the System administrators will review the logs for any unusual or unauthorized activities at least weekly.

Security violations will be investigated and appropriate follow-up actions taken by the System administrators. Security violations must be reported to management immediately.

VI. Documentation Requirements

The System administrators are responsible for retaining documentation of current baseline configurations, user profiles, access control lists etc.

VII. Definitions

Baseline Configurations: Defined settings used to either prevent or allow specified user activities. Model specifications used as a standard.

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

Resource: Information Technology resource may be hardware, application software, operating software, network, etc.

System Administrator: A designated person who is responsible for system and user administration functions including system maintenance and add/change/delete access granted. This person may be the same as the resource owner.

Telnet: A UNIX utility that allows a user to login to some other host in the Internet or within a network of hosts.

Trivial File Transfer Protocol (TFTP): A simple file transfer facility that provides the ability to transfer data in both directions between the local host and a remote host without authenticating the sender.

VIII. References

None.