THE CALIFORNIA MARITIME ACADEMY

POLICY NO. 208.19

ISSUE DATE: March 13, 1997 **REVISION DATE: February 15, 2000**	**POLICY: Physical Security to IS Facilities and Resources**
REFERENCE:	
APPROVED: **/s/ Jerry A. Aspland**	

I. Policy Statement

The California Maritime Academy's (the Academy's) Information Technology (IT) resources and facilities must be protected against unauthorized access. This is to help ensure that critical and confidential campus information is adequately controlled. Access to all computer rooms, wire closets, desktops and laptops with sensitive information, along with *significant processing hardware* must have physical restriction on access. Refer to *Hardware Purchases and Maintenance, P*olicy 208.9.

The Information Systems (IS) Department is responsible for protecting network and communications hardware and all other IS facilities and resources. Department managers are responsible for protecting the critical IT hardware in their area of responsibility. Persons with badges, keys, access codes, or access cards to critical IS facilities and resources are responsible for users of such identification and protective devices.

II. Principles

Access to every office, computer room, and work area containing sensitive information should be physically restricted. Management responsible for the staff working in these areas must determine the appropriate access control method. Visitor or third-party access to Academy offices, computer facilities, or other work areas containing sensitive information should be controlled by guards, receptionists, or other staff.

Employees should not permit unknown or unauthorized persons to pass through doors, gates and other entrances to restricted areas. Employees should not attempt to enter restricted areas in Academy buildings and facilities without proper access authorization. When employees leave the Academy or their job description no longer requires access to critical IS facilities and resources, badges should be collected and any access codes,

passwords, or other security device must be deactivated. Refer to *Access to Computer Resources, P*olicy 208.1.

III. Deployment

All requests for access to IS must be submitted to and approved by the IS Department which will determine if there is a valid business need. Badges and access will only be granted with appropriate authorization.

IV. Technical Architecture

All significant processing hardware should be installed in an environmentally controlled facility with a reasonable level of Heating, Ventilation and Air Conditioning (HVAC). Visitors, such as maintenance and repair personnel, should be escorted at all times. A manual visitors log must be maintained for all visitors to the facility.

Tapes will be stored in a physically secured and environmentally controlled location, and will not be released to personnel without authorization from the data owner. Tapes created for backup and recovery purposes should be stored at a secure offsite location. Tapes must be administered and maintained in accordance with the corporate backup and recovery policy. Backup tapes should be periodically checked to ensure integrity of backup data.

Computer rooms must have and maintain an adequate level of fire suppression equipment. Equipment must be maintained and inspected in accordance with local requirements. For computer rooms located in flood prone regions, system hardware should be located above normal flood levels or must maintain an adequate level of water detection equipment.

V. Monitoring

The IS Department is responsible for periodically reviewing the list of persons who have access to critical IS facilities and resources and significant processing hardware to ensure the access is still appropriate.

VI. Documentation Requirements

The IS Department is responsible for retaining a complete and up-to-date list of all Academy or non-Academy personnel with access to critical IS facilities, resources and *significant processing hardware.*

VII. Definitions

Significant Processing Hardware: Any hardware worth more than $7,500 or that is not easily replaced or processes critical applications.

VIII. References

Access to Computer Resources, Policy 208.1
Hardware Purchases and Maintenance, Policy 208.9