

POLICY NO. 208.18

ISSUE DATE: March 13, 1997	POLICY: Data Confidentiality,
REVISION DATE: February 15, 2000	Security, and Handling
REFERENCE:	
APPROVED:	
/s/ Jerry A. Aspland	

I. Policy Statement

Data is an important asset of The California Maritime Academy (the Academy). Academy data must be classified according to the importance, sensitivity and criticality of the data.

Data residing in all forms, including printed, electronic, magnetic or optical must be handled appropriately according to the classification. Access to any Academy data/information must be restricted on a need-to-know basis as defined by the *data owner*.

II. Principles

Accurate, timely, relevant and properly protected information is absolutely essential to the Academy's operation. To ensure that information is properly handled, all access to, use of, and processing of Academy information must be consistent with related Academy information systems policies and procedures. This policy reflects the minimum requirements for handling proprietary and confidential Academy information in all forms.

All data should have a data owner. Data ownership should be based on functional responsibility. All users, including Academy and *non-Academy personnel*, are responsible for protecting Academy campus data.

All permanent and temporary Academy personnel must sign a confidentiality agreement stating that they understand and will be in compliance with this campus policy.

III. Deployment

Policy 208.18 Data Confidentiality, Security, and Handling Page 2

Employees will receive access to confidential or private campus information only after expressed authorization from the data owner has been obtained. When not being used by authorized workers, or when not clearly visible in an area where authorized persons are working, all hardcopy and computer media (floppy disks, tapes, CD-ROM's, etc.) containing confidential or private information should be locked in a physically secure area/enclosure.

Academy information may not be removed from the Academy's premises unless prior written approval from the data owners has been obtained. If data is lost or disclosed to unauthorized parties, its owner must be immediately notified. Confidential or private campus information must not be reproduced unless required for performance of campus work or when authorized by the responsible manager.

IV. Technical Architecture

The elimination of residual information must ensure that the information cannot be recovered. For example, degaussing, which subjects media to strong electro-magnetic fields, is a method to ensure that residual data cannot be recovered.

V. Monitoring

The IS and Human Resources departments are responsible for collecting all computer hardware, working materials, confidential information and other Academy property before Academy employees and non-Academy persons receive their final paycheck. This includes, but is not limited to, hard-copies and electronic storage devices,

VI. Documentation Requirements

None.

VII. Definitions

Data Owner: A designated person who is responsible for the integrity, completeness and accuracy of Academy data.

Non-California Maritime personnel: Contractors, vendors, customers, temporary employees, or affiliates.

VIII. References

None.