



**POLICY NO. 208.17**

<b>ISSUE DATE:</b> March 13, 1997 <b>REVISION DATE:</b> February 15, 2000	<b>POLICY:</b> Password Management
<b>REFERENCE:</b>	
<b>APPROVED:</b>  /s/ Jerry A. Aspland	

**I. Policy Statement**

When access to any information at The California Maritime Academy (the Academy) is authenticated with a password or an access code, management of those passwords or access codes is essential. Password management helps control the use of a system, *devices*, and access to protected resources.

The Information Systems (IS) Department is responsible for developing guidelines for password management and communicating these guidelines to users. Once distributed, users are responsible for adherence to these guidelines and are responsible for all activities performed with any ID assigned to them.

**II. Principles**

Logical access to any electronic documents containing sensitive information (refer to *Data Confidentiality, Security, and Handling, Policy 208.18*) must be password protected. This password is in addition to the password used by the users in gaining access to the application or platform.

Users and System *Owners* share responsibility for enforcing password security. The Academy management is responsible for ensuring that every individual within their organization complies with these policies.

Refer to Information Systems Security Policy 208.1 *Access to Computer Resources* for policy regarding IDs and access granted to Academy systems.

**III. Deployment**

When there is a request by a user to reset his/her password, the user will be required to provide ID and some type of personal information to prove the user's identity before a

## **Policy 208.17 Password Management**

### **Page 2**

new password is issued. Users will be required to change the temporary passwords immediately.

A password should be disabled as soon as its user leaves the Academy. The IS Department should be notified promptly when people leave the Academy.

When passwords are changed, the new password should be significantly different from the old one (at least three characters must be changed). The password should not be related to the user's job or personal life. A password should be changed immediately if the user suspects that the password has been compromised or is known by another individual. Passwords should never be written down.

#### **IV. Technical Architecture**

The following are recommended password practices:

- Passwords should contain at least six upper or lower case characters
- Passwords must be validated for each logon attempt
- Passwords or access codes should be changed a minimum of every 90 days
- Passwords should not contain more than two consecutively repeated or sequential characters.
- A *grace period* for initial logon will not exceed 14 calendar days
- Passwords will be encrypted in the password files. 'Read' and 'write' access to password files will not be given.
- Passwords should not be hard-coded in software or applications, or stored in clear text in batch files, automatic logon scripts, software macros, terminal function keys, or in other locations where unauthorized users might discover them.

Application of best practices should be dictated by an assessment of risk in the specified area weighed against operational issues (no control should cost more than the risk involved).

#### **V. Monitoring**

Periodically, software will be executed to ensure passwords are in compliance with the policies. The System Owner is responsible for monitoring and reviewing all security violations on a weekly basis (Refer to Information Systems Security Policy 208.4, *Systems Administration*). IS is also responsible for maintaining a current listing of the authorized network users and their passwords.

#### **VI. Documentation Requirements**

## **Policy 208.17 Password Management**

### **Page 3**

System owners are required to keep a log of all security violations and to report these violations to the appropriate system/data owner.

### **VII. Definitions**

*Device:* Academy-owned or personally owned computers such as a desktop, laptop or docked laptop, server, DEC/VAX, UNIX machine or local area network (LAN) workstation.

*Grace period:* The time period a user has before he/she is forced to change the logon password.

*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*

*Systems Administration, Policy 208.4*

*Data Confidentiality, Security, and Handling, Policy 208.18*