



POLICY NO. 208.14

ISSUE DATE: March 13, 1997 REVISION DATE: February 15, 2000	POLICY: External Network Access
REFERENCE:	
APPROVED: /s/ Jerry A. Aspland, President	

I. Policy Statement

Information accessible through and transmitted across The California Maritime Academy's (the Academy's) network requires appropriate protection against unauthorized access or use.

The IS (Information Systems) Department is responsible for ensuring that authorized individuals only are permitted to access to resources on the Academy's network. Access to the above resources will be defined by the resource owner.

II. Principles

The *resource owner* is responsible for the security of company information at the user level. All of the Academy's employees, vendors, suppliers, contractors, and other users of the network are responsible for protecting proprietary and confidential information as outlined in the Academy's *Data Confidentiality, Security, and Handling Policy No. 208.18*. The resource owners are responsible for ensuring that every individual using their resource complies with these policies.

External connections to The Academy's network, such as private network connections, modem connections, and Internet connections, can leave the network vulnerable to unauthorized access.

If the Academy's network has external connections, a risk analysis should be performed to determine the nature of controls to be implemented relating to the external connection. All attachments to The Academy's network from external connections must be approved, authorized, and closely monitored by the IS Department.

III. Deployment

Policy 208.14 External Network Access

Page 2

All external network connections to the Academy network must be submitted to the IS Department. Proper authorization, non-disclosure agreements, and the expected duration of connections must be provided to the IS Department at the time the access request is submitted.

The IS Department is responsible for determining that there is a sufficient business need along with each request for external network connections. This includes coordination for access to other system resources (this includes contact with any affected resource owners).

All external network connections must be approved by IS. The approval or denial will be based upon the risk analysis performed and the acquisition of all necessary documentation. IS should ensure that access no longer needed is removed within a 24-hour period.

IV. Technical Architecture

A *commercial firewall* will be placed between a non-Academy network (e.g., private networks, the Internet etc.) and the Academy's network.

Certain dangerous applications, such as *TFTP*, *Telnet*, etc., will be prevented from passing through the external network connection into the Academy's network. A list of approved IP/IPX addresses and user IDs must be documented by the IS Department.

V. Monitoring

The IS Department is responsible for reviewing logs of activities through and on the commercial firewalls at least weekly for unusual activity. Any unusual activity will be investigated immediately. IS will be responsible for testing periodically *firewall* configurations against the approved configurations. Discrepancies discovered during the testing will be resolved.

IS is responsible for monitoring software changes, upgrades, and security holes with vendors, as well as making changes when necessary.

VI. Documentation Requirements

The IS Department is responsible for maintaining and updating the approved external connections including contact names and phone numbers. In addition, IS needs to maintain and update the security approval forms and non-disclosure agreements.

VII. Definitions

Commercial firewalls: Firewall applications that only route TCP and allow filtering based on IP addresses, IDs, and TCP application use.

Data Owner: A designated person who is responsible for the integrity, completeness and accuracy of data or information system resource.

Firewall: A system that sits between an outside network and an organization's internal network, controlling all packet flow between the two.

Telnet: A UNIX utility that allows users 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

Data Confidentiality, Security, and Handling, Policy 208.18