CAL MARITIME

ACADEMY POLICY MANUAL

Policy Title:	**Local Software Development Security**
Policy Number:	AF 07-005
Policy Administrator:	Kurtis D. Lohide, Vice President for Administration and Finance
Policy Initiator:	Jason Wenrick, Chief Information Officer
Authority:	Integrated CSU Administrative Manual (ICSUAM) Section 8000: Information Security Policy
Effective Date:	August 1, 2013
Revised Date:	
Approved:	Thomas A. Cropper, President

Purpose: The California Maritime Academy must ensure that all locally developed network accessible software is secured and maintained during its entire lifecycle.

Scope: This policy applies to all locally developed network accessible software on university computers or on the campus network.

Accountability: It is the responsibility of the Chief Information Officer to administer this policy and ensure compliance.

Policy: It is the policy of the California Maritime Academy to require that all locally developed network accessible software must be free from security vulnerabilities, including but not limited to:

- vulnerabilities exposing the hosting system to compromise or use in relay attacks
- vulnerabilities allowing an attacker to perform unauthorized actions at the application level or operating system level
- vulnerabilities in authentication
- vulnerabilities in authorization
- insecure use of user supplied data
- insufficient, improper, or incorrect use of encryption
- unintended exposure of information
- predictable system generated secrets
- vulnerabilities exposing a user to attack from a malicious third party web server
- Denial of Service vulnerabilities resulting from undefined behavior

Procedures:

All locally developed network accessible software will be subject to IT ISO security review at any time.

All vulnerabilities discovered in locally developed network accessible software, no matter who discovers them nor how, must be remediated in a timely fashion.

The name of the person who is responsible for software maintenance must be identified. This person must not be a student assistant. If CMA/IT is responsible, then CMA/IT should be identified as the software maintainer.

Software maintainers must be able to demonstrate to CMA/IT that they have the knowledge required to properly maintain the software. The maintainer must implement CMA/IT-specified requirements and recommendations. The software maintainer must have working knowledge of secure programming and will be required to respond to security alerts.

The software maintainer's job description must specify sufficient time to handle software maintenance responsibilities. Security responses must be performed in a timely manner and often require immediate action of the software maintainer.