

System and Application Development and Maintenance Policy

Approved By: \\S\ James Palmer CSC Loss Prevention Director 31 December 2011 Date	PCI Policy # 1500 Version # 2.0 Effective Date: 31 December 2011
--	--

1.0 Purpose:

The purpose is to implement policies and procedures to ensure that all Coast Guard Morale, Well-Being and Recreation Program (MWR) systems and applications are developed and maintained to be free of security vulnerabilities.

2.0 Compliance:

PCI Requirement 2, 6

3.0 Scope:

This policy applies to all MWR Program employees, contractors, consultants, temps, and other workers (called "users") who utilize MWR Program-provided IT resources described herein in their assigned job responsibilities. Further, the policy applies to all systems, network, and applications that process, store or transmit sensitive information.

4.0 Policy:

Only necessary and secure services, protocols, daemons, etc. as required for the function of the system will be enabled. Security features such as SSH, S-FTP, SSL, or IPsec VPN will be used for any required services, protocols, or daemons that are considered to be insecure. Insecure services include NetBIOS, file-sharing, Telnet, FTP, etc.

Security Patch Rules

All system components and software will have the latest vendor-supplied software version and/or patches installed within one month of release. Documentation will be kept which shows the system

components and software have been upgraded with the new version/patch.

A process, such as subscriptions to alert services, will be in place to identify newly discovered security vulnerabilities. Standards will be updated as necessary to address new vulnerability issues.

Software Development Policy

All software applications developed will be based on industry best practices and incorporate information security throughout the software development lifecycle (SDLC).

All patches and system configuration changes will be tested on a test environment prior to deployment.

There will be separation of duties between the development, test, and production environments.

All accounts, usernames, and passwords used in the development or testing of applications will be removed prior to the production system becoming active.

Custom code will be reviewed for potential coding vulnerabilities prior to release to production.

Change Management Policy

All system and software configuration changes will follow change control procedures.

The change control procedures will include the documentation of the impacts, management sign-off by appropriate parties, documented testing of operational functionality, and back-out procedures.

Web Application Development Policy

All web applications will be developed based on secure coding guidelines such as the Open Web Application Security Project guidelines.

Custom application code will be reviewed to identify coding vulnerabilities.

The review of custom application code will focus on the detection of common coding vulnerabilities, including invalidated input, broken access control, broken authentication and session management, cross-site scripting (XSS) attack, buffer overflows, injection flaw, improper error handling, insecure storage, denial of service, and insecure configuration management.

Web-Facing Application Policy

All web-facing applications will be protected against known attacks by either having all customer application code reviewed or by installing an application layer firewall in front of web-facing applications.

5.0 Responsibility:

The MWR Director/Officer is responsible for leading compliance activities that bring the Coast Guard – MWR into compliance with the PCI Data Security Standards and other applicable regulations, most notably Commandant Instruction 5260.5, Privacy Incident Response, Notification and Reporting Procedures for Personally Identifiable Information (PII).

6.0 PCI Template(s):

Change Control Procedure Document (*You will need to create*)

7.0 Definition(s):

Definitions for technical terms can be found in Appendix A of your MWR PCI Compliance Workbook.

8.0 Policy History:

Initial effective date: 07/01/1999

Revision One: 12/31/2011