

PCI Information Security Policy

Approved By: <u>\S\ James Palmer</u> CSC Loss Prevention Director <u>31 December 2011</u> Date	PCI Policy # 1000 Version # 2.0 Effective Date: 31 December 2011
---	--

1.0 Purpose:

The purpose is to ensure that policies and procedures are maintained that address information security for employees and contractors.

2.0 Compliance:

PCI DSS Requirement 12.

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.

4.0 Policies and Procedures

All security policies and procedures will clearly define information security responsibilities for all employees and contractors.

All security policies and procedures will be reviewed and updated annually.

A risk assessment will be performed every year to identify threats and vulnerabilities of sensitive information (especially cardholder data).

Daily operational procedures will be developed and maintained that are consistent with the policies.

Usage policies for critical employee-facing technologies (such as modems and wireless) will be developed to define proper use of these technologies

for all employees and contractors. These usage policies will require the following:

- Explicit management approval;
- Authentication for use of the technology;
- List of all such devices, and personnel who have access to them
- Labeling of all devices with owner, contact information, and purpose;
- Acceptable uses of the technologies;
- Acceptable network locations for the technologies;
- List of MWR-approved products and applications;
- Automatic disconnect of modern sessions after a specific period of inactivity; and
- Activation of modems for vendors only when needed by vendors, with immediate deactivation after use.

Storage of cardholder data on local hard drives, floppy disk, or other external media is prohibited when accessing cardholder data remotely via modem. Also, cut-and-paste and print functions will be disabled during remote access.

Procedures will be developed that assign information security management responsibilities to one or more employees. These responsibilities specifically include:

- maintenance of the security policies and procedures;
- monitoring of security alerts and information;
- security incidence response and escalation procedures;
- administration of user accounts; and
- monitoring and control of all access to data.

Employee Security Education

A formal Security Awareness program will be implemented to make all employees aware of the importance of cardholder data security. All employees will be educated upon hire and at least annually. And all employees are required to acknowledge in writing that they have read and understand the company's security policies and procedures.

Employee Screening

New employees and employees being promoted into positions that give them access to sensitive data will be subject to background checks as limited by law.

Service Providers Policy

All service providers with which cardholder data is shared must adhere to the PCI DSS requirements.

The Coast Guard Morale, Well-Being and Recreation Program (MWR) will exercise due diligence when evaluating potential service providers, to ensure that the providers are in compliance with the PCI DSS standards.

The provider must sign an agreement acknowledging that the service provider is responsible for the security of cardholder data the provider possesses.

All contracted service providers are required to provide proof of compliance with PCI DSS. Copies of the provider's Self Assessment Questionnaire and Attestation of Compliance will serve as proof.

Incident Response Policy

An incident response plan will be implemented to be prepared to respond immediately to a system breach. The incident response plan will:

- designate personnel responsible for responding to a breach;
- define those persons' roles and responsibilities;
- provide for training of the responsible personnel;
- list specific incident response procedures;
- list business recovery and continuity procedures;
- specify data backup processes; and
- describe communication and contact strategies.

The incident response plan will be tested at least annually. It will also be modified and amended as necessary, based on lessons learned and industry developments.

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 Supporting Documents

Policy 1010 - Acceptable Use Policy

Policy 1020 - Security Incident Policy

Policy 1030 - Security Incident Procedures: Response and Reporting Policy

Security Awareness Program

Commandant Instruction 5260.5, Privacy Incident Response, Notification and Reporting Procedures for Personally Identifiable Information (PII)

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

First revision date: 12/31/2011