

## Encryption of Transmitted Cardholder Data Policy

<b>Approved By:</b>  \\S\ James Palmer CSC Loss Prevention Director  31 December 2011 Date	<b>PCI Policy # 1700    Version # 2.0</b>  <b>Effective Date:</b> 31 December 2011
--	--

### 1.0 Purpose

The purpose is to implement policies and procedures to ensure that all sensitive data is protected while in transit to or from the Coast Guard Morale, Well-Being and Recreation Program (MWR) systems.

### 2.0 Compliance

PCI DSS Requirement 4.

### 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 Policy

During transmission over open, public networks, strong cryptography and security protocols (such as SSL/TLS, IPSEC or SSH, etc.) will be used to safeguard sensitive cardholder data. Only trusted keys or certificates will be accepted. When SSL/TLS is used, no cardholder data will be transmitted unless “HTTPS” appears in the URL of the site.

All wireless networks transmitting cardholder data will encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC, VPN, or SSL/TLS. Wired equivalent privacy (WEP) will not be used.

Unencrypted PANs will never be sent by e-mail.

### 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.

## **6.0 PCI Templates**

None

## **7.0 Definitions**

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 date: 12/31/2011*