

Physical Access Policy

Approved By: <u>\\S\ James Palmer</u> CSC Loss Prevention Director <u>December 31, 2011</u> Date	PCI Policy # 1300 Version # 1.1 Effective Date: 12/31/2011 Revision Date: 12/31/2014
---	--

1.0 Purpose

The purpose is to implement policies and procedures to ensure that physical access controls exist that ensure that all cardholder data can only be accessed by authorized personnel.

2.0 Compliance

PCI DSS Requirement 9

3.0 Scope

This policy applies to MWR PROGRAM in its entirety, including all workforce members.

4.0 Policy

Procedures for restricting physical access to cardholder data will be documented, implemented and known to affected parties.

Facility Access Policy

Facility entry controls will be implemented to limit and monitor physical access to systems that store, process, or transmit cardholder data.

All sensitive areas will have video cameras and/or access control mechanisms to monitor individual physical access. "Sensitive areas" does not include areas where only point-of-sale terminals are present. The cameras and/or access control mechanisms will be protected from tampering. The collected data will be audited and correlated with other entries on a daily basis, and will stored for at least three months unless otherwise restricted by law.

Physical access to publicly accessible network jacks, wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines will be restricted with physical and/or logical controls. All network ports used to host visitors are not enabled with DHCP (Dynamic Host Configuration Protocol).

Controls Over Visitors Policy

Documented procedures to help personnel easily distinguish between onsite personnel and visitors in areas where cardholder data is accessible include:

- Method to identify new onsite personnel or visitors
- How to change access requirements
- How to revoke or terminate onsite personnel and expired visitor identification (such as badge)

Physical access for onsite personnel to the sensitive areas includes the following:

- Access must be authorized and based on individual job function
- Access is revoked immediately upon termination and all physical access mechanisms are returned or destroyed.

Procedures for identifying and authorizing visitors will be documented and implemented. These procedures will include:

- All visitors will be authorized and escorted at all times before entering areas where cardholder data is processed or maintained.
- All visitors are identified and given a badge or other identification, which clearly identifies them as a visitor, and which has an expiration time/date. Visitors are required to surrender the device before leaving the facility or on the time/date of expiration.
- Granting new badges, changing access requirements, and revoking terminated onsite personnel and expired visitor badges.
- Access to the badge system is limited to authorized personnel.
- A visitor log will be used to maintain a physical audit of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted.
- Visitor's log will document the visitor's name, the firm represented, and the onsite personnel authorizing physical access. Visitor logs

will be retained for a minimum of three months, unless otherwise restricted by law.

Media Controls Policy

All media back-ups will be stored in a secure location, preferably in an offsite facility, such as an alternate or backup site, or a commercial storage facility. The security of these facilities will be reviewed at least annually.

All paper and electronic media (including computers, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder data will be physically secured.

Strict control will be maintained over the internal and external distribution of any kind of media that contains cardholder data such that the media is classified as sensitive and will only be sent by secured, traceable, courier.

Management will approve in advance any and all media being moved from a secured area.

Strict control will be maintained over the storage and accessibility of media that contain cardholder data. Inventory logs will be maintained and media inventories will be conducted at least annually.

Media containing cardholder data will be destroyed when it is no longer needed for business or legal reasons. The means of destruction for hardcopy materials will be cross-cut shred, incineration or pulping so that cardholder data cannot be reconstructed. Electronic data will be destroyed using a method (purge, degauss, or shred) which ensures that cardholder data cannot be reconstructed.

Secure storage containers used for materials that are to be destroyed.

Device Controls Policy

Procedures for protecting devices that capture payment card data via direct physical interaction with the card will be documented and implemented. These procedures will include:

- Maintaining a list of devices

- Periodically inspecting devices to look for tampering and substitution
- Training personnel to be aware of suspicious behavior and to report tampering or substitution of devices
- Procedures for inspecting devices including frequency of inspection

5.0 Responsibility

The Security Officer, with Executive Management supervision, is responsible for leading compliance activities that bring THE COAST GUARD MWR PROGRAM into compliance with the PCI Data Security Standards and other applicable regulations.

6.0 Forms

Form 1301 - Visitors Log
Form 1302 - Card Holder Data Inventory Log
Form 1303 - Removal Log for Media
Form 1304 - Media Destruction Log

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: 7/01/1999

First revision date: 12/31/2011

- *Revisions for PCI DSS Version 2.0*

Second revision date: 12/31/2014

- *Revisions for PCI DSS Version 3.0*