Physical Access Policy

Approved By:	PCI Policy # 1300 Version # 2.0
\S\ James Palmer CSC Loss Prevention Director 31 December 2011 Date	**Effective Date:** 31 December 2011

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 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

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 should have cameras. The collected data will be audited and correlated with other entries and stored for at least three months, unless otherwise restricted by law.

Physical access to publicly accessible network jacks, wireless access points, gateways, and handheld devices will be restricted.

Controls Over Visitors Policy

Copyright © 2008-2011 TurboPCI, Inc. All rights reserved.

Procedures will exist to help personnel to easily distinguish between employees and visitors in areas where cardholder data is accessible.

All visitors will be authorized before entering areas where cardholder data is processed or maintained.

All visitors will be given a token, such as a badge or access device, which identifies them as non-employees, and will be required to surrender the device before leaving the facility or on the date of expiration.

All visitors to sensitive areas must complete a visitor's log which will be maintained 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.

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 identified as confidential 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 contains cardholder data such that it is inventoried and securely stored.

Media containing cardholder data will be destroyed when it is no longer needed for business or legal reasons. The means of destruction will be cross-cut shred, incineration or pulping of hardcopy materials. Electronic

Copyright © 2008-2011 TurboPCI, Inc. All rights reserved.

data will be destroyed using a method (purge, degauss, or shred) which ensures that cardholder data cannot be reconstructed.

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 PCI Templates

PCI Template 1301 - Visitors Log
PCI Template 1302 - Card Holder Data Inventory Log
PCI Template 1303 - Removal Log for Media
PCI Template 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: 07/01/1999
Revision date: 12/31/2011

Copyright © 2008-2011 TurboPCI, Inc. All rights reserved.