

Logical Access Policy

Approved By: <hr/> \\S\ James Palmer CSC Loss Prevention Director <hr/> 31 December 2011 Date	PCI Policy # 1200 Version # 2.0 Effective Date: 31 December 2011
--	--

1.0 Purpose

The purpose is to implement policies and procedures to ensure that logical access controls exist ensuring that all critical data can only be accessed by authorized personnel and that all actions taken on critical data can be traced to known, authorized employees and vendors of the Coast Guard Morale, Well-Being and Recreation Program (MWR).

2.0 Compliance

PCI DSS Requirements 7 and 8

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 vendors and company systems, network, and applications that process, store or transmit sensitive information.

4.0 Policies

The Business Need-To-Know Policy

Access to computer resources and cardholder information will be limited to only those individuals whose job function requires such access, and to vendors for remote maintenance purposes.

All systems with multiple users will be set with the default of “deny all”, only allowing access to computer resources that apply to the employee’s job classification and function.

Vendor Remote Access Policy

Vendor accounts are subject to the two-factor authentication requirements for remote access as outlined below.

Vendor accounts will be enabled for remote maintenance only during a time period which has been established and approved in advance and the accounts will be monitored while in use.

Individual Access Policy

All systems and applications which store critical information will require a unique user name for all users.

All unique user names will require a password, token device, or biometrics to authenticate the user.

Two-factor authentication will be implemented for remote access to the network by employees, administrators and third parties. Two-factor authentication includes use of two different technologies such as dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

All passwords will be encrypted during storage and transmission.

Password attributes for non-consumer users and administrators are:

1. Passwords require a minimum length of 7 characters ;
2. Passwords must contain both numeric and alphabetic characters;
3. Passwords must be changed at least every 90 days; and
4. Passwords can not be repeated for up to 4 generations.

After six repeated failed attempts to log into a user ID, the user ID will be locked out for thirty minutes, or until the administrator enables the user ID.

If the login session is idle for more than 10 minutes, the user will be required to re-enter the password to re-activate the session.

Administration of Passwords

All additions, deletions, and modifications of User IDs will be documented and authorized by a qualified employee.

A user's identity will be verified before performing password resets.

First-time passwords will be set to a unique value for each user and changed immediately after the first use.

Access will be revoked immediately for terminated employees and contractors.

Inactive users will be reviewed and removed at least every 90 days.

User accounts for vendors' remote maintenance will be enabled only during the time period needed.

Password policies and procedures will be communicated to all users who have access to cardholder data.

The use of group shared, or generic accounts and passwords is prohibited.

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 Supporting Documents

Access Authorization and Termination Procedures (*You will need to create*)

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 One: 12/31/2011