

Identity and Authentication Access Policy

Approved By: \\S\ James Palmer CSC Loss Prevention Director December 31, 2011 Date	PCI Policy # 1200 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 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 MWR PROGRAM in its entirety, including all workforce members, except for employees who have point-of-sale access to one card number at a time to facilitate a single transaction. Further, the policy applies to all vendors and company systems, network, and applications that process, store or transmit sensitive information.

4.0 Policies

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

Procedures for identification and authentication to cardholder data will be documented, implemented and known to affected parties.

An automated access control system which requires documented approval by authorized parties specifying required privileges will be utilized to comply with the following policies, as applicable:

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.

Access needs for each role including the systems /devices/data and level of access will be defined. Access will only be granted based on defined roles.

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.

Privileged Accounts

Access to privileged user IDs is restricted to the least privileges necessary to perform job responsibilities.

Vendor Remote Access Policy

Remote vendor accounts apply to any vendor who accesses, supports and maintains system components, and the accounts should be disabled when not in use.

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.

Vendors/service providers should use unique authentication credentials for each customer. They are subject to the two-factor authentication requirements for remote access as outlined below.

Individual Access Policy

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

Controls will be in place for additions, deletions, and modifications of user ID, credentials and other identifiers objects.

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 users, administrators and all 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.

Strong cryptography must be used to render authentication credentials unreadable during transmission and storage.

Password attributes for non-consumer users and administrators are:

1. Passwords require a minimum length of at least 8 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 15 minutes, the user will be required to re-enter the password to re-activate the session.

Document and communicate authentication procedures and policies to all users including:

- Guidance on selecting strong authentication credentials
- Guidance for how users should protect their authentication credentials
- Instructions not to reuse previously used passwords
- Instructions to change passwords if there is any suspicious the password could be compromised.

Administration of Passwords and Authentication Mechanisms

All additions, deletions, and modifications of User IDs, credentials, and other identifier objects, and their specified privileges, will be documented and authorized by a qualified employee.

A user's identity will be verified before modifying and authentication credentials.

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

Authentication mechanisms must be linked to an individual account and not shared. Physical and logical controls must be in place to ensure only the intended account can use that mechanism to gain access.

Access will be deactivated or removed 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 and monitored while in use.

All users who have access to cardholder data will receive formal training on MWR Program's password policies and procedures. Training will be documented.

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

Database Access Policy

All access to any database containing cardholder data will be authenticated, including access by applications, administrators and all other users.

Only programmatic methods (such as stored procedures) will be used for all user access to, queries of, and actions on (such as move, copy, delete) any database containing cardholder data.

User access to queries and user actions on databases are through programmatic methods. Only database administrators have the ability to directly access or query databases.

Application IDs for database applications can only be used by the applications and not by individual users or other non-application processes.

A user's identity will be verified before modifying any authentication credential.

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 Form(s)

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: 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*
- *Name Change from 'Logical Access Policy'*