

Vendor-Supplied Defaults Policy

Approved By: \\S\ James Palmer CSC Loss Prevention Director 31 December 2011 Date	PCI Policy # 1400 Version # 2.0 Effective Date: 31 December 2011
--	--

1.0 Purpose:

The purpose is to implement policies and procedures to ensure that all vendor supplied defaults are changed upon installation. Vendor default passwords and other vendor default settings are well known to hacker communities and are easily determined via public information.

2.0 Compliance:

PCI DSS Requirement 2

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

4.0 Policy:

Vendor-Supplied Defaults

All vendor-supplied defaults will be changed before installing a system on the network (including, but not limited to, passwords/passphrases, wireless keys, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).

Configuration Requirements

Configuration standards will be developed for all system components, including common security parameter settings. All standards will address all known and security vulnerabilities and will be consistent with these industry-accepted system hardening standards:

- Only one primary function will be implemented per server.
- All unnecessary and insecure services and protocols will be disabled.
- System parameters will be configured to prevent misuse.
- All unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers will be removed.

Encryption

All non-console administrative access will be encrypted with technologies such as SSH, VPN, or SSL/TLD.

Firmware on wireless devices will be kept updated to support strong encryption for authentication and transmission over wireless networks.

Hosting Providers

Hosting providers will protect the hosted environment by meeting the specific requirements of PCI DSS.

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, most notably Commandant Instruction 5260.5, Privacy Incident Response, Notification and Reporting Procedures for Personally Identifiable Information (PII).

6.0 PCI Template(s):

PCI Template 1903 – Encryption Key Change Log
Computer Systems Configuration Documentation (*You will need to create*)
Check List for Builds (*You will need to create*)

7.0 Definition(s):

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