SOU Southern OREGON UNIVERSITY

PCI Network - Device Security Procedure

Office: Information Technology
Procedure Contact: IT Infrastructure Manager
Related Policy or Policies: PCI Network - User Accounts, PCI Network - Network Security

Revision History

Revision Number:	**Change:**	**Date:**
1.2	Formatting modification and expansion of Sections B, C	**June 2017**
1.1	Post-QSA Update and rename to “PCI Network - Device Security”	**May 2017**
1.0	Initial Version	**November 2016**

A. Purpose

Devices used to carry out PCI related tasks must be hardened to prevent unauthorized access to sensitive data. This procedure outlines the steps that must be taken to properly secure a device prior to deployment in an environment that contains cardholder data.

B. Definitions

"PCI" stands for "Payment Card Industry".

"DSS" stands for "Data Security Standards".

“User” shall refer to a single person with access to devices and/or network resources.

A “network” is a system of electronic devices interconnected by telecommunication equipment or cables used to transmit or receive information. The bounds of a “network” may be defined by the ability of traffic to pass unimpeded between devices, similar to a broadcast domain, or a specific range of IP addresses, around which connectivity restrictions are based.

A "PCI network" refers to any network as defined above, intended to enable credit card processing.

A “device” is a unit of physical microprocessor equipment, that either resides on a PCI network, or has direct access to the data/traffic on the PCI network.

"CDE" stands for "Cardholder Data Environment". The CDE is the the networks and devices involved in processing credit card transactions.

A “firewall” may be a device as defined above, or a software application, with the capability and intended purpose of filtering traffic in and/or out of a network.

Accessing a device “remotely” refers to any non-console access, or any console access that does not require physical presence at the device.

“OSSEC” is an open-source host-based security tool, implemented in this case for file integrity monitoring.

C. Windows-based Computers

1. Ensure the operating system is a supported version and up to date with available patches.
2. Ensure that the Windows Update service is configured to automatically patch and reboot within 24 hours of an available update.

3. Ensure the firewall on the device is enabled and properly configured to prohibit inbound traffic.
4. Ensure institutional anti-virus software is installed, running, and configured to automatically update.
5. Remove or disable any non-critical user accounts including:
    a. "Guest"
    b. "itadmin"
    c. "itinstaller"
6. Restrict login on the device to users whose job function includes PCI related tasks, and IT personnel tasked with the maintenance of the PCI network and/or devices.
7. No user accounts will be configured in a way that the device can be accessed without authenticating using either a password, a token device or smart card, or a biometric.
8. Ensure no more than six failed consecutive attempts to authenticate will be allowed before locking a user account out of the system.
9. Enable an idle timeout of 15 minutes is set for all users.
10. Disable or uninstall inbound remote access software including:
    a. Remote Desktop Connections
    b. VNC Server
11. Ensure the following unsafe protocols are not allowed to operate on the device:
    a. Telnet
    b. SMTP
    c. FTP
    d. SSL/Early TLS
12. Remove any default SNMP community strings set by the manufacturer or vendor.
13. Unless critical to the operation of PCI related tasks, disable or uninstall third-party plugins including:
    a. Java
    b. Flash
    c. Browser add-ons, including but not limited to search bars
14. Remove any pre-loaded commercial software such as non-standard anti-virus software.

D. Windows-based Monitoring

1. Install logging agent on all Windows computers.
2. Configure logging agent to capture the following information from Windows event logs:
    a. All actions performed by users with local administrative privileges
    b. All failed authentication attempts to the machine
3. Configure logging agent to capture the following information from Windows event logs about user interaction with Windows system components:
    a. Username
    b. Event classification
    c. Event date and dime
    d. Event success or failure
    e. Event origination
    f. Identity of target data, system component, or resource
4. Verify log shipping to graylog server.
5. Retain all captured logs for one year.
6. Retain the most recent three months worth of logs in format and location that allows for immediate analysis.
7. Install OSSEC agent for File Integrity Monitoring on all Windows computers.
8. Configure OSSEC agent to perform weekly checks on critical system files, configuration files, and any other files with relevant contents.
9. Verify OSSEC agent reporting to centralized OSSEC server.
10. Review monitoring data for significant occurrences and security events at least daily using log analysis software.
11. Respond to anomalies detected in log analysis and track using department ticketing system.

E. Network Equipment and Vendor-supplied Devices

1. Ensure the device is running a supported version of its firmware or operating system.
2. Ensure the following unsafe protocols are not allowed to operate on the device:
    a. Telnet
    b. SMTP
    c. FTP
    d. SSL/Early TLS
3. Remove any default SNMP community strings set by the manufacturer or vendor.
4. If a root account exists, set a complex password containing 32 characters (or the maximum allowed, if lower) and store in the password repository.
5. If supported, create individual login accounts for all persons that will need to login to the device for any reason.
6. If supported, ensure no more than six failed consecutive attempts to authenticate will be allowed before locking a user account out of the system.
7. Remove or disable any non-critical user accounts.

F. Physical Inspection

1. All devices must be inspected on a quarterly basis to detect signs of tampering or substitution including:
    a. Card skimmers
    b. Replacement hardware with different or undocumented serial numbers
    c. Wireless network adapters
    d. Keystroke loggers
    e. Any other unauthorized data interception or transmission devices
2. Any suspected tampering, replacement, or other suspicious activity involving devices on the PCI network shall be reported to the PCI contacts in both Information Technology, and Business Services.

G. Inventory

1. An inventory must be kept of all PCI related devices that includes the following details for all devices:
    a. Vendor/Make
    b. Model
    c. Serial number
    d. Date of production implementation
    e. Date of decommission
    f. Purpose on PCI Network
    g. Enabled non-standard functions, services, or protocols (if any)
2. The inventory shall be updated whenever devices are added, relocated, or decommissioned.
3. The inventory must be audited annually to ensure accuracy.
4. Decommissioned devices shall stay on the inventory for 1 year after decommission.

H. Other Devices

Institutional devices that are not described above shall be prohibited from operating in the cardholder data environment without first amending this document to demonstrate proper device-hardening measures have been developed and implemented.

Third-party devices that are not issued or acquired through a PCI-related vendor for the explicit purpose of use on a the cardholder data environment are prohibited from operating on a PCI network.

This procedure may be revised at any time without notice. All revisions supersede prior procedures and are effective immediately upon approval.