Configuration Standards for System Components Policy

Overview

In accordance with the Payment Card Industry Data Security Standards (PCI DSS) requirements, the Office of Information Security has established a formal policy and supporting procedures for developing configuration standards for system components that are consistent with industry-accepted hardening standards. This process will be conducted by authorized personnel with the appropriate technical knowledge and skill sets needed to undertake this activity. The term, System Components, is defined as any network component, server or application included in or connected to the cardholder data environment. This policy is to be implemented immediately. It will be evaluated on an annual basis to ensure its adequacy and relevance.

Policy

The Office of Information Security will develop configuration standards for system components utilizing industry-accepted hardening standards for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives. The list of industry-leading security standards, benchmarks and frameworks to utilize includes, but is not limited to, the following (PCI DSS Requirements and Security Assessment Procedures):

- Center for Internet Security (CIS)
- International Organization for Standardization (ISO)
- SysAdmin Audit Network Security (SANS) Institute
- National Institute of Standards Technology (NIST).Vendor-specific tools and checklists, along with general setup and hardening procedures

Additionally, when configuring system components within the cardholder environment, the following conditions must apply in order to ensure further compliance with the

Payment Card Industry (PCI) Data Security Standards (DSS) Initiatives (PCI DSS Requirements and Security Assessment Procedures, Version 3.0):

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the system configuration standards are consistent with industry-accepted hardening standards.
- Appropriately develop, implement, and adhere to relevant policies and supporting procedures to ensure that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.1.
- Appropriately develop, implement, and adhere to relevant policies and supporting procedures to ensure that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network.
- System configuration standards used for general provisioning, hardening, securing and locking-down of system components are to include the following procedures:
    - Changing of all vendor-supplied defaults and elimination of unnecessary default accounts.
    - Implementing only one primary application per server to prevent functions that require different security levels on the same server.
    - Enabling only necessary services, protocols, daemons, etc.as required for the function of the primary application on the system.
    - Implementing additional security features for any required services, protocols or daemons that are considered to be insecure.
    - Configuring system security parameters to prevent misuse.
    - Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers that aren’t required by the primary application on the system.

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that only one primary function is implemented per server.
- If virtualization technologies are used, then appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that only one primary function is implemented per virtual system component or device.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that only necessary services or protocols are enabled.
- For any required insecure services, daemons, or protocols implemented on system components, ensure they are justified per documented configuration standards.
- Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that security features are documented and implemented for all insecure services, daemons, or protocols.
- Configure system security parameters to prevent misuse.
- System administrators and/or security managers are to have relevant knowledge of common security parameter settings for system components.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that common security parameter settings are included.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that they are set appropriately and in accordance with the configuration standards.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that all unnecessary

functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that enabled functions are documented and support secure configuration.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that only documented functionality is present on the sampled system components.

Responsibility for Policy Maintenance

The Office of Information Security is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

Revision History

February 8, 2019 (Policy Created)

July 15, 2019 (Policy Modified)

Adapted from Stanford University's PCI DSS Policies 1-2019