Secure Protocols for CHD transmission Policy

Overview

In accordance with the Payment Card Industry Data Security Standards (PCI DSS) requirements, University of South Alabama has established a formal policy and supporting procedures concerning the use of strong cryptography and secure protocols. This policy is to be implemented immediately. It will be evaluated on an annual basis to ensure its adequacy and relevance.

Policy

All departments must ensure that the use of strong cryptography and secure protocols adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

- Use strong cryptography and security protocols for safeguarding sensitive cardholder data during transmission over open, public networks.
- Comprehensively document all locations where cardholder data is transmitted or received over open, public networks.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that all cardholder data is encrypted with strong cryptography during transit.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that only trusted keys and/or certificates are accepted.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations.

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the proper encryption strength is implemented for the encryption methodology in use.
- Strong cryptography and secured protocols are defined and approved by PCI DSS.
- For Voice over IP (VoIP) transmission, the following three requirements must be met:
    - All the VoIP data must be encrypted with strong cryptography and transmitted by secured protocols.
    - Network segregation must be implemented for the VoIP to transmit cardholder data.
    - VoIP with cardholder data is prohibited for storage in any of Stanford University's systems.
- It is prohibited to transmit CHD via texting messages, instant messages, emails or voicemail.

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