29. Strong Cryptography and Secure Protocols for CHD transmission

Overview
In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, Stanford University 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 for ensuring its adequacy and relevancy regarding to PCI DSS and Stanford University’s needs and goals.

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.

29.1 For Voice over IP (VoIP) transmission, the following three requirements must be met:
- 29.1.1 All the VoIP data must be encrypted with strong cryptography and transmitted by secured protocols.
- 29.1.2 Network segregation must be implemented for the VoIP to transmit cardholder data.
- 29.1.3 VoIP with cardholder data is prohibited for storage in any of Stanford University's systems.

29.2 It is prohibited to transmit CHD via texting messages, instant messages, emails or voicemail.
29.3 FAX transmission with CHD:
- 29.3.1 A FAX machine with an analogue line and with secure access is approved for CHD transmission.
- 29.3.2 Cardinal FAX and Cardinal PRINT should not be used for any process, storage, transmission with CHD.
- 29.3.3 It is prohibited to transmit, store or process any CHD via Stanford’s non-PCI infrastructure or non-PCI network.
- 29.3.4 Prior approval from UIT Compliance Services team is required to install a new FAX line for CHD transmission.

Responsibility for Policy Maintenance
UIT PCI Compliance Services 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.