11. Point-to-point Encryption (P2PE), Wi-Fi, Analog and Global System for Mobile (GSM) usage policy

Overview

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, Stanford University has established a formal policy and supporting procedures for Point-to-point Encryption (P2PE), Wi-Fi, Analog and Global System for Mobile (GSM) usage policy. This policy is to be implemented immediately. It will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding Stanford University’s needs and goals. This policy only applies Point-to-point Encryption (P2PE), Wi-Fi, Analog and Global System for Mobile (GSM) with internet connections for payment card processing and transmission.

Policy

Stanford University will ensure that that Point-to-point Encryption (P2PE), Wi-Fi, Analog and Global System for Mobile (GSM) usage adhere to and comply with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

- Only PCI Security Standard Council approved P2PE solutions are eligible for network scope reduction or removal. For implementation and eligibility verification, an advanced approval from UIT Compliance Services team is required.
- If a PIN Transaction Security (PTS) device or a PCI workstation is connected with Wi-Fi, the PTS device or the PCI workstation must be implemented with a PCI SSC approved P2PE solution.
- Wi-Fi connection alone is prohibited for card holder data transactions and transmission in Stanford environment.
- If a PTS device is connected with analog, it is permitted for card holder data transactions and transmission in Stanford environment.
- If a PTS device is connected with Global System for Mobile (GSM, also known as Cellular), it is permitted for card holder data transactions and transmission in Stanford environment.

Responsibility for Policy Maintenance
Administrative Systems 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.