Point-to-point Encryption (P2PE), Wi-Fi, Analog and Global System for Mobile (GSM) usage 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 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 to ensure its adequacy and relevance. 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

University of South Alabama will ensure 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 Office of Information Security approved P2PE solutions are eligible for network scope reduction or removal. For implementation and eligibility verification, an advanced approval from the Office of Information Security 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 cardholder data transactions and transmission in the university environment.

- If a PTS device is connected with analog, it is permitted for cardholder data transactions and transmission in the university environment.
- If a PTS device is connected with Global System for Mobile (GSM, also known as Cellular), it is permitted for cardholder data transactions and transmission in the university environment.

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