Payment Systems and Vendor Evaluation Policy

Overview

In accordance with the Payment Card Industry Data Security Standards (PCI DSS) requirements, the University of South Alabama has established a formal policy and supporting procedures for payment systems and service vendor's evaluation. This policy is to be implemented immediately. It will be evaluated on an annual basis to ensure its adequacy and relevance.

Policy

The University of South Alabama will ensure that payment systems and service vendors' usage adhere to and comply with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures):

Payment System and Services Vendors include application system and service providers, and any external consulting services that involve PCI DSS compliance.

Vendor evaluation for individual merchant department:

For the evaluation and verification of payment card service providers, the following documents must be submitted to the Office of Information Security for review.

Please note the following:

- The AOC must be valid within twelve months.
- Every vendor must submit the AOC as a service provider, unless an exception is granted by Treasury Office, ISO and UIT Compliance Office.
- If the AOC is not signed by a PCI SSC certified QSA or ISA, the vendor must also submit their current quarter's Approved Scanning Vendor (ASV) report and the current year's penetration test report for external network.

- In a twelve month period, the PCI Compliance team will only accept a maximum of three versions of an AOC from the same vendor for review.

If needed at a later stage of the evaluation, the PCI Compliance team might request that the vendor provide a demo on payment processing workflow through its services.

Vendor and consulting services evaluation for Merchant Services:

Prior to Merchant Services starts the discovery process with a vendor, Merchant Services will contact UIT/AS Compliance Services for the following 30.2.1, 30.2.2 and 30.2.3 assessment. No business engagement or formal purchase orders should be involved with any prospective payment system and services vendors before such assessment is completed and satisfied.

- 30.2.1 Vendors' PCI DSS compliance assessment (please see 30.1 for requirement documents).
- 30.2.2 Initial assessment for vendors' qualification to meet Stanford Minimum Security Standard.
- 30.2.3 Assess vendor systems' feasibility for the integration with Stanford's PCI infrastructure, compliance and security requirements for PCI DSS compliance and Stanford Minimum Security.

For Data Risk Assessment (DRA), the Information Security Office (InfoSec) and the University Privacy Office (UPO) evaluate projects based on all applicable security and privacy laws and regulations as well as University policy.

Notes

Payment card service providers, please note that according to PCI SSC, all of the organizations that process, transmit, and/or store payment card information must be PCI Security Standard Requirements and Security Assessment Procedures (PCI DSS) compliant.

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