THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

PAYMENT CARD INDUSTRY COMPLIANCE POLICY

Number: 06.04.17

Division: Finance and Administration – Accounting and Business Services

Date: March, 2021 – Revised August 2, 2022

Purpose: The purpose of this policy is to protect payment card data and to comply with the Payment Card Industry Data Security Standards (PCI DSS) requirements for transmitting, handling, and storage of payment card data.

Scope

The PCI DSS requirements apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data and any system that can alter a system that stores, processes, or transmit cardholder data. The requirements apply to all methods of credit card processing, from manual to computerized.

What is PCI?

The PCI DSS are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The PCI SSC is responsible for managing the security standards, while compliance is enforced by the payment card brands. These standards include controls for handling and restricting credit card information, computer and internet security, as well as the reporting of a credit card information breach. The standards are updated as new technology and data breaches make it evident that new security metrics need to be in place to keep card holder data secure.

Related Documents

- UAH Payment Card Processing and PCI Compliance Procedures
- Payment Card Industry Data Security Standard (Current Version)
- 02.02.01 Protection of Data Policy

Responsibilities and Involvement

All departments and areas accepting credit cards either directly or through a third-party vendor or that maintain or have access to credit card information are required to meet the latest version of the PCI DSS and submit Self-Assessment Questionnaire (SAQ) to the UAH PCI Compliance Review Team annually. Achieving these requirements will serve to mitigate the potential of a data breach and remaining PCI compliant will allow them to continue to take payment cards as a method of payment.

Third-party Security Assurance/Risk Management

It is the responsibility of the Procurement Officers to ensure adequate safeguarding provisions are incorporated in contracts that include any external sharing of protected or private UAH data. Contracts for third-party outsourcing must require explicit provisions to meet PCI DSS safeguarding requirements as specified in law, rule, UAH policy, or contractual obligation.

PCI Compliance Review Team

UAHs PCI Compliance Review Team serves in an advisory capacity to the Associate Vice President for Finance & Business Services and Bursar in guiding and monitoring the University's cardholder data environment to ensure compliance with PCI DSS.

Functions

The PCI Compliance Review Team will perform the following functions:

a) Recommend University-wide policies and procedures to ensure compliance with PCI DSS
b) Assist with the evaluation and monitoring of the cardholder data
c) environment, payment card processes, and vendor relationships
d) Oversee annual PCI DSS self-assessment
e) Support and advise departments to comply with PCI DSS and the University's policies and procedures
f) Facilitate communication of PCI DSS changes and best practices
g) Review requests for new merchant locations and advise the University Controller on recommendations for approval or denial of requests

Membership

The PCI Compliance Review Team is comprised of representatives from several key areas of university operations:

- Associate Vice President for Finance & Business Services
- Office of Counsel
- Office of Risk Management and Compliance
- Procurement & Business Services
- Bursar Office
- Office of Student Affairs
- College of Professional and Continuing Studies
- Charger Card Operations
- Office of Information Technology
- Office of Marketing and Communication
- Office of Sponsored Programs
- Athletic Department

Noncompliance

Noncompliance can result in serious consequences for UAH, including reputational damage, loss of customers, litigation, and financial costs. Failure to comply with this policy and/or applicable policies, standards, and procedures carries severe consequences which may include but are not limited to the loss of the ability to process payment card transactions.

The University Associate Vice President for Finance & Business Services and the Controller each have the authority to restrict and/or terminate merchant account status for noncompliance.

Any known or suspected breach, compromise, or unauthorized access of cardholder data shall be reported immediately to the Vice President for Finance and Administration, the Controller, or the Bursar.

Review: The Vice President for Finance and Administration is responsible for the review of this policy every five years (or whenever circumstances require).