The University of Alabama at Birmingham

PAYMENT CARD PROCESSING AND SECURITY POLICY

November 15, 2010

Related Policies/Documents

Cash Receipts Policy
Data Protection and Security Policy
Acceptable Use of Computer and Network Resources
Information Disclosure and Confidentiality Policy
PCI Entity Handbook

Definitions

Cardholder Data – Any personally identifiable data associated with the cardholder, to include account number, expiration date, name, address, social security number, card service verification code, or any other data stored on the magnetic stripe of the payment card.

Merchants - Authorized acceptors of payment cards for the purchase of goods, services, or information.

Network members – Acceptors of payment cards for the purchase of goods, services, or information that have been granted direct authorization to perform payment card transactions by the major credit card companies. Generally these include banking and financial institutions.

Payment Application Data Security Standards (PA-DSS) - The Payment Card Industry Security Standards Council program established to help software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and to ensure their payment applications support compliance with the PCI DSS. Payment applications that are sold, distributed or licensed to third parties are subject to the PA-DSS requirements.

Payment Card Industry Data Security Standards (PCI DSS) - A multifaceted set of comprehensive requirements and security standards developed to enhance payment account data security, security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

PCI Entity - Any UAB department, office, section, or affiliated association or group that has been approved to accept, process, transmit, or store credit card transactional or cardholder data as a member, merchant, or service provider operating on behalf of UAB, or in use of the UAB brand name.

Senior Management - Persons in the positions of dean, chair, or division or program director, or persons specifically designated by a dean, chair, or division or program director, that make executive decisions and are authorized to accept risks for the administrative unit in the area of information security.

Service Providers – Any business entity that is not a payment card brand network member or a merchant directly involved in the processing, storage, transmission, and switching of transaction data or cardholder information, or both. This includes companies that provide services to merchants, service providers, or members that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, intrusion detection systems and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.

UAB Enterprise - The University of Alabama at Birmingham, the University of Alabama at Birmingham Health System, University Hospital, The Kirklin Clinic, the University of Alabama Health Services Foundation, the UAB Health Centers, the Ophthalmology Services Foundation, and Callahan Eye Foundation Hospital.

Verification Code – The three or four digit value printed on the front or back of a payment card; Card Validation Code CVC2 (Mastercard), Card Verification Value CVV2 (VISA), Card Member ID (Discover), or the Card Identification Number CID (American Express).

Background

The Payment Card Industry (PCI) Data Security Standards (DSS) are a mandated set of security standards created by the major credit card companies for the purpose of offering merchants and service providers a complete, unified approach to safeguarding cardholder data for all payment card brands. The PCI DSS apply to all payment card network members, merchants, and service providers that process, store, or transmit cardholder data, as well as to all methods of credit card processing, whether manual or computerized.

Purpose

This policy mandates compliance with PCI DSS requirements for processing, storing, transmitting, or handling payment card information. UAB is subject to examination of security measures employed to ensure cardholder data are securely maintained. As such, UAB is committed to adhering to the PCI DSS in order to ensure the protection of cardholder data, limit its liability, and maintain the ability to provide payment card transaction services.

Policy Statement

All UAB payment card processing activities and related technologies must comply with this policy and the PCI DSS in its entirety. Compliance with card processing activities must be maintained as described herein and in accordance with the policies listed in the Related Policies/Documents section of this policy. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of this policy or the PCI DSS.

Scope/Applicability

This policy applies to all UAB employees, contractors, consultants, temporaries, vendors, other third party workers, and any unit that processes, stores, maintains, transmits, or handles payment card information in a physical or electronic format on behalf of the UAB enterprise, or in use of the UAB brand name. This includes any entity that utilizes any part of the UAB network infrastructure for payment card transaction services. Hereafter, these groups shall be referred to as "PCI Entities."

Policy Requirements

Each PCI Entity must be approved by, and registered with, the Office of the Vice President for Financial Affairs and Administration. Refer to the UAB PCI Entity Handbook for approval and registration procedures.

Each PCI Entity must develop, implement, and maintain processes and procedures for conducting secure payment card transaction related activities in accordance with PCI DSS requirements and any other applicable UAB policies.

PCI Entity Senior Management is responsible for ensuring all cardholder data are protected against unauthorized use, disclosure, fraud, or other compromising activity.

PCI Entity compliance with PCI DSS must be validated annually and in the event of any change in the Entity payment card processing environment in accordance with PCI validation standards. Refer to the UAB PCI Entity Handbook for applicable validation procedures.

All payment card transactions must be performed on systems approved by the Office of the Vice President for Information Technology. Approval shall include an annual risk assessment process that identifies threats and vulnerabilities to the payment card processing environment.

Vendor or third-party applications used for payment card processing services must be a PCI Validated Payment Application that meets PA-DSS requirements.

Any known or suspected breach, compromise, or unauthorized access of cardholder data shall be reported immediately to the Entity Senior Management and the Office of the Vice President for Financial Affairs and Administration.

The appropriate Human Resources Department is responsible for ensuring applicable background checks are conducted for all new hires or transfers into positions that will have access to cardholder data or payment card processing activities.

The Office of the Vice President for Financial Affairs and Administration is responsible for overseeing and enforcing a formal PCI compliance and security awareness program in order to educate PCI Entities of the importance of cardholder data security. Security awareness training shall be completed as part of Entity approval and registration, and annually thereafter.

Sanctions

Employees who do not follow this policy and all requirements contained within the appropriate unit procedures may be subject to disciplinary action up to and including termination of employment.

UAB PCI Entities who do not follow this policy and established procedures may be subject to suspension or loss of payment card processing capability and monetary fines.

Vendors or contractors who do not follow this policy and established procedures may be subject to breach of contract penalties.

Exceptions

Any exception to this policy or the established procedures for implementing this policy must be requested in writing in advance and approved by the Office of the Vice President for Financial Affairs and Administration and the Office of the Vice President for Information Technology.

Implementation

The Office of the Vice President for Financial Affairs and Administration will be responsible for governing and enforcing UAB PCI compliance and approving any changes to this policy.

References

Payment Card Industry Data Security Standards (PCI DSS)
Payment Application Data Security Standards (PA-DSS)
Payment Card Industry Self Assessment Questionnaire (SAQ)