STEPHEN F. AUSTIN
STATE UNIVERSITY
Office of the General Counsel

POLICY SUMMARY FORM

Policy Name: Payment Card Acceptance and Security

Policy Number: 14.8

Is this policy new, being reviewed/revised, or deleted? Review/Revise

Date of last revision, if applicable: 7/28/2015

Unit(s) Responsible for Policy Implementation: Vice President for Finance and Administration

Purpose of Policy (what does it do): The purpose of this policy is to apply best security practices to ensure the protection of payment card information by complying with Payment Card Industry (PCI) Data Security Standards (DSS).

Reason for the addition, revision, or deletion (check all that apply):

☒ Scheduled Review ☐ Change in law ☐ Response to audit finding

☐ Internal Review ☐ Other, please explain:

Please complete the appropriate section:

Specific rationale for new policy:

Specific rationale for <u>each</u> substantive revision: Reporting responsibilities clarified. Cross-referenced policy 14.14, Information Security Incident Response and Reporting.

Specific rationale for deletion of policy:

Additional Comments:

Reviewers:

Judi Kruwell, Director of Financial Services
Danny Gallant, Vice President for Finance and Administration
Damon Derrick, General Counsel

Payment Card Acceptance and Security

Original Implementation: July 21, 2009
Last Revision: ~~July 28, 2015~~*July 24, 2018*

Purpose

T~~he purpose of t~~his policy *affirms the university's intent*~~is~~ to apply best security practices to ensure the protection of payment card information by complying with Payment Card Industry (PCI) Data Security Standards (DSS). This policy is supplemental to any other information security policies currently in effect at Stephen F. Austin State University ~~(university)~~.

Definitions

*An **affiliated organization** is an entity that uses systems connected to the university network or assets or equipment owned by the university to process, transmit, or store cardholder information.*

*The **cardholder** is the customer to whom a credit card or debit card has been issued or the individual authorized to use the card.*

***Payment card** is a general term which includes both debit cards and credit cards.*

***Payment card information** is any personally identifiable information associated with a cardholder (e.g., cardholder name, account number, expiration date, address, social security number, personal identification number and card validation code).*

***Payment Card Industry (PCI) Data Security Standards (DSS)** are the result of collaboration between the five major credit card brands to develop a single approach to safeguarding cardholder data. The standards apply to all entities that store, process, and/or transmit cardholder data and covers technical and operational system components included in or connected to cardholder data.*

*A **payment processor** is any individual, department, school, or other functional area accepting payment cards in exchange for goods or services on behalf of the university or an affiliated organization.*

~~Resources Covered~~*General*

All computers, electronic devices, or other resources at the university used in the processing, transmitting and storing of cardholder information are governed by this policy and subject to PCI-DSS requirements. This includes servers which store payment card information; workstations which are used to enter payment card information into a central system; *and* cash

registers, point-of-sale terminals connected to a phone line or the university network,~~;~~ and any other devices through which the payment card information is transmitted. Also covered are ~~Web site~~ *website* storefronts that redirect customers to another ~~Web site~~ *website* to enter payment information. In addition, all paper forms or receipts containing cardholder data are also covered under this policy.

~~**Covered Groups**~~

This policy applies to all university departments, faculty, staff, students, temporar*y employees*~~ies~~, vendors, associated entities, or any others who process, transmit, store or handle cardholder information in physical or electronic format on behalf of the university. This policy also applies to any affiliated organizations with cardholder information that is processed, transmitted, or stored on systems connected to the university network or through assets or equipment owned by the university.

~~Definitions~~

~~**Affiliated Organizations:** An entity that uses systems connected to the university network or assets or equipment owned by the university to process, transmit or store cardholder information.~~

~~**Cardholder:** The customer to whom a credit card or debit card has been issued or the individual authorized to use the card.~~

~~**Payment card:** General term which includes both debit cards and credit cards.~~

~~**Payment card information:** Any personally identifiable information associated with a cardholder (e.g., cardholder name, account number, expiration date, address, social security number, personal identification number and card validation code).~~

~~**Payment Card Industry** (PCI) **Data Security Standards** (DSS) are the result of collaboration between the five major credit card brands to develop a single approach to safeguarding cardholder data. The standards apply to all entities that store, process, and/or transmit cardholder data and covers technical and operational system components included in or connected to cardholder data.~~

~~**Payment Processor:** Any individual, department, school, or other functional area accepting payment cards in exchange for goods or services on behalf of the university or an affiliated organization.~~

Responsibilities

The vice president for finance and administration is responsible for oversight of the PCI compliance program ~~(program)~~. The vice president for finance and administration will designate

specific responsibility for the development, implementation and administration of the program.

The designated program representative(s) will review and approve all requests to accept payment cards, perform all necessary actions to ensure PCI compliance, and respond to any suspected payment card information threat.

Payment card processors will establish and maintain documented procedures for complying with this policy and PCI-DSS.

Requirements

PCI DSS compliance is mandatory for any department or affiliated organization that accepts, captures, stores, transmits, and/or processes payment card information. Only authorized and properly trained employees, vendors, and temporary employees may accept and/or access payment card information. All employees with access to payment card information are required to take payment card training annually. Each person who has access to payment card information is responsible for protecting the information in accordance with PCI DSS and university policy.

Only PCI DSS compliant equipment, systems and methods may be used to process, transmit, and/or store payment card information. All systems used to process, transmit, and/or store payment card data must be registered with the designated program representative. Payment cards cannot be processed, transmitted, and/or stored using the university's network unless Information Technology Services (ITS) has verified existence of all technical controls required by the PCI DSS and other applicable university policies.

Payment card processors must obtain advance approval from the program representative(s) designated by the vice president for finance and administration before accepting payment cards for payment of goods or services, or before entering into any contracts or purchases of software and/or equipment related to payment card processing. Once approved, copies of contracts must be forwarded to the designated program representative(s). Payment processors are required to use the university's preferred service provider. Exceptions may be granted only after a request from the payment processor has been reviewed and approved by the designated program representative(s). When an exception has been granted, the payment processor remains responsible for ensuring the service provider is PCI compliant and provides ongoing certification of compliance. Contracts with third parties with access to payment card information must include language that requires adherence to the PCI DSS.

~~Suspected exposure or theft of payment card information must be reported immediately to one of the following university employees: the vice president for finance and administration or the director of financial services, the controller , the director of audit services, or the chief of police. Additionally, any suspected breach in the network should be immediately~~

~~reported to the director of information technology.~~
Unencrypted wireless, email, fax, and campus mail are not recognized as secure methods for transmitting or accepting cardholder data. Cardholder data must not be transmitted in an insecure manner. Printed receipts or other physical materials containing cardholder information must be stored in a secure environment until they are processed. Payment card information must be destroyed in a secure manner as soon as it is no longer needed.

Suspected exposure or theft of payment card information must be reported immediately to one of the following university employees: the vice president for finance and administration, the director of financial services, the controller, the director of audit services, or the chief of police. Additionally, any suspected breach in the network should be immediately reported to the chief information officer.

Enforcement:

Periodic reviews may be performed to validate compliance with this policy. If the requirements of this policy are not followed, suspension of payment card options may result. Substantial fines may also be imposed by credit card companies if a security breach and subsequent compromise of payment card data occurs.

Employees in violation of PCI DSS and this policy may be subject to a range of sanctions including loss of computer network access, disciplinary action or legal sanctions.

Cross Reference: PCI Security Standards; Receipts and Deposits (3.26)*; Information Security Incident Response and Reporting (14.14)*

Responsible for Implementation: Vice President for Finance and Administration

Contact for Revisions: Vice President for Finance and Administration

Forms: Application for Exception from Use of University Preferred Electronic Payment Service, Statement of Intent to Comply with the University Policy for Payment Card Acceptance and Security, Payment Card Processor Registration Form, Confidentiality Statement

Board Committee Assignment: Finance and Audit