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: 7/24/2018

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

Purpose of Policy (what does it do): This policy defines the requirements and responsibilities for maintaining compliance with the Payment Card Industry's Data Security Standard (PCI-DSS).

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

- [ ] Scheduled Review
- [ ] Change in law
- [ ] Response to audit finding
- [x] Internal Review
- [ ] Other, please explain:

Please complete the appropriate section:

Specific rationale for new policy:

Specific rationale for each substantive revision: The policy is being updated to strengthen Payment Card Industry compliance and incorporate comments resulting from CampusGuard review.

Specific rationale for deletion of policy:

Additional Comments:
Reviewers:

Michaelyn Greene  
Brandon Stringfield  
Payment Card Industry Steering Committee  
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 24, 2018 April 30, 2019

Purpose

This policy affirms the university’s intent 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 defines the requirements and responsibilities for maintaining compliance with the Payment Card Industry’s Data Security Standard (PCI-DSS) at Stephen F. Austin State University (the university/SFA). Achieving and maintaining Payment Card Industry (PCI) compliance mitigates the potential of data breaches and allows our departments and affiliated organizations (merchants) to take payment cards with a level of risk acceptable to the university. This policy is supplemental to any other information security policies currently in effect at the Stephen F. Austin State 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.

General

*Stephen F. Austin State University* will take steps to help ensure full compliance with the PCI-
DSS. All payment card handling activities and related technologies must comply with the PCI-DSS. Payment card handling activities must be conducted as described herein and in accordance with the guidelines in the Payment Card Security Handbook, maintained on the university’s PCI website.

This policy will be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

Applicability

This policy applies to all personnel who store, process, transmit, have access to, or can affect the security of payment card data, including faculty, staff, contractors, and students who are employed or utilized by SFA. This policy also applies to any employee who contracts with a third party vendor to handle and/or process payment card data on behalf of SFA. All vendors, contractors, and business partners who store, process, transmit, have access to, or can affect the security of payment card data on behalf of SFA will state in their contract that they are and will remain compliant with the PCI-DSS at all times.

All computers, electronic devices, or other resources at the university used in the payment card processing, transmitting and storing of cardholder information are governed by this policy and subject to PCI-DSS requirements. This includes but is not limited to servers which store payment card information; workstations which are used to enter payment card information into a central system; cash registers, point-of-sale terminals connected to a phone line or the university network, printers, scanners, and any other devices through which the payment card data is transmitted or on which payment card data is stored. Also covered are website storefronts that redirect customers to another website to enter payment information. In addition, all paper forms or receipts containing cardholder data are also covered under this policy.

This policy applies to all university departments, faculty, staff, students, temporary employees, 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.

Responsibilities

The vice president for finance and administration is responsible for oversight of the PCI compliance program. The vice president for finance and administration will designate specific individuals who will have responsibility for the development, implementation, and administration of the program. These individuals will serve on the PCI Steering Committee and will assist the university in achieving and maintaining compliance with the PCI-DSS and in reducing the scope
items that will need to be compliant with the PCI-DSS.

The vice president for finance and administration will also designate designated program representative(s) who will review and approve all requests to accept payment cards, perform all necessary actions to help ensure PCI compliance, and respond to any suspected payment card information threat.

University merchants will establish and maintain documented procedures for complying with this policy and the PCI-DSS and will follow guidelines established in the Payment Card Security Handbook.

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, or 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 the 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(s). 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 are evaluated by the designated program representative(s).

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). Merchants are required to use the university’s preferred service provider. Exceptions may be granted only after a request from the payment card processor has been reviewed and approved by the PCI Steering Committee. When an exception has been granted, the merchant remains responsible for ensuring the service provider is PCI compliant and providing ongoing certification of compliance to the designated program representative(s).

Cardholder data must not be transmitted or accepted in an insecure manner. Insecure methods of transmitting or accepting cardholder data include but are not limited to unencrypted wireless, email, fax, and campus mail. 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.

Credit card information must not be stored on any electronic device including university network servers, workstations, laptops, tablets, and cell phones unless it is explicitly approved for use as part of the cardholder data PCI-DSS environment.

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 providing ongoing certification of compliance. Contracts with third parties with access to payment card information must include language that requires adherence to the PCI-DSS.

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.

Training

All personnel in positions that store, process, transmit, have access to, or affect the security of payment card data will complete PCI-DSS training upon hire and at least annually. These personnel will also acknowledge, in writing or electronically, that they have read and understand these security policies and procedures, and that they will comply with these policies.

Incident Response
All security incidents, including suspected exposure or theft of payment card information, must be reported in accordance with university policy 14.14, Information Security Incident Response and Planning. All PCI users should be familiar with this policy and are responsible for reporting any incident of theft, fraud, or misuse of payment card data.

**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 payment card companies if a security breach and subsequent compromise of payment card data occurs.

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


**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