STEPHEN F. AUSTIN
STATE UNIVERSITY
Handbook of
Operating Procedures

Payment Card Acceptance and Security

Purpose

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). 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 university.

Persons Affected

This policy applies to all faculty, staff, students, contractors, volunteers, and third-parties who store, process, transmit, have access to, or can affect the security of payment card data in physical or electronic format on behalf of or in association with the university. This includes any entity that utilizes any part of the university network infrastructure for payment card transaction services. 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 the university. 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 the university will state in their contract that they are and will remain compliant with the PCI-DSS at all times.

Policy

Stephen F. Austin State University takes steps to 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.

A. Applicability

All computers, electronic devices, or other resources at the university used in payment card processing are governed by this policy and subject to PCI-DSS requirements. This includes but is not limited to 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.

B. Responsibilities

The vice president for finance is responsible for oversight of the PCI compliance program.

The vice president for finance will also designate program representative(s) who 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. Oversight of the PCI-DSS program is delegated to the Director of Treasury and Student Business Services.

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.

Procedures

A. 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. 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 equipment and systems used to process, transmit, and/or store payment card data must be approved by the designated program representative(s). Payment cards cannot be processed, transmitted, and/or stored using the university's network unless all technical controls required by the PCI-DSS and other applicable university policies are approved by the designated program representative(s).

University departments and affiliated organizations must obtain advance approval from the program representative(s) designated by the vice president for finance 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). University departments and affiliated organizations 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 designated program representative(s). 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 environment.

B. 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, understand and will comply with these policies and procedures.

C. Incident Response

All security incidents, including mishandling or misplacement of payment card data, suspected exposure or theft of payment card information or the like, must be reported in accordance with SFA HOP 06-106 Information Security Incident Response and Reporting. 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.

D. Security Measures

1. All equipment, software, and business processes must comply with current PCI security standards.

2. In addition to completing the initial PCI Compliance Questionnaire during setup, each merchant is required to complete an annual PCI self-assessment questionnaire.

3. Credit card numbers should only be stored electronically as a last resort, and then only in full compliance with the most recent PCI DSS requirements.

4. Card data should never be transmitted over end user technologies such as email, texting, instant messenger, or any other application.

5. Merchant departments must ensure that the storage of printed cardholder data (such as merchant copies of receipts or daily batch reports), are secured in a location with access limited to those with a legitimate business need.

6. Before engaging with third party service providers who support the transaction process (through software, equipment, hosting, personnel, etc.), merchant departments must ensure the vendor can prove PCI compliance, can take contractual responsibility for cardholder security to the extent of their control, and can commit to ongoing PCI security compliance.

E. 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.

Related Statues or Regulations, Rules, Policies, or Standards

SFA HOP 05-208 Receipts and Deposits
SFA HOP 06-107 Information Security Management
SFA HOP 06-106 Information Security Incident Response and Reporting

PCI Security Standards
Payment Card Security Handbook
ITS Policy Handbook

Responsible Executive

Senior Vice President for Organizational Effectiveness

Forms

Statement of Intent to Comply with the University Policy for Payment Card Acceptance and Security

Revision History

September 1, 2023 (original)
April 21, 2025

Non-Educational Policy