Stephen F. Austin State University

Payment Card Security Handbook

For PCI DSS version 3.2

Version 1.0 - May 31, 2019

CONFIDENTIAL INFORMATION

Revision History

Changes	Approving Manager	Date
Initial Publication	B. Stringfield/M. Greene	5/31/2019

Contents

INTRODUCTION AND SCOPE

Introduction

This document explains Stephen F. Austin State University's payment card security requirements as required by the Payment Card Industry's Data Security Standard (PCI-DSS) Program. The university's management is committed to these security practices to protect information utilized by the university in attaining its business goals. All employees are required to adhere to the practices described within this document.

Scope of Compliance

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, Stephen F. Austin State University's cardholder environment consists only of limited payment applications (typically point-of-sale systems) connected to the internet, but does not include storage of cardholder data on any computer system.

Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in Self-Assessment Questionnaire (SAQ) C, version 3.2 revision 1.1, released January 2017. Should Stephen F. Austin State University implement additional acceptance channels, add additional connected systems, begin storing cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ C, it will be the responsibility of Stephen F. Austin State University to determine the appropriate compliance criteria and implement additional procedures and controls as needed.

1.1 Build and Maintain a Secure Network

Responsible Parties – Information Technology Services

1.1.1 Firewall Configuration

Firewalls must restrict connections between untrusted networks and any system in the cardholder data environment. An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. Access to the internet must be through a firewall, as must any direct connection to a vendor, processor, or service provider. (PCI Requirement 1.2)

Inbound and outbound traffic must be restricted by the firewalls to that which is necessary for the cardholder data environment. All other inbound and outbound traffic must be specifically denied. (PCI Requirement 1.2.1)

Perimeter firewalls must be installed between any wireless networks and the cardholder data environment. These firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. (PCI Requirement 1.2.3)

Firewall configuration must prohibit direct public access between the internet and any system component in the cardholder data environment as follows:

- Direct connections are prohibited for inbound and outbound traffic between the internet and the cardholder data environment. (PCI Requirement 1.3.3)

- Outbound traffic from the cardholder data environment to the internet must be explicitly authorized by management and controlled by the firewall. (PCI Requirement 1.3.4)

- Ensure the firewall allows only established connections into the network and denies any inbound connections not associated with a previously established session. (PCI Requirement 1.3.5)

Any mobile and/or employee-owned computers with direct connectivity the internet (for example, laptops used by employees), which also have the ability to access the organization's cardholder data environment must have a local (personal) software firewall installed and active. This firewall must be configured to specific standards, and not alterable by mobile and/or employee-owned computer users. (PCI Requirement 1.4)

1.2 Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Responsible Parties – Information Technology Services

1.2.1 Vendor Defaults

Vendor-supplied defaults must always be changed before installing a system on the network. Examples of vendor-defaults include passwords, SNMP community strings, and elimination of unnecessary accounts. (PCI Requirement 2.1)

Default settings for wireless systems must be changed before implementation. Wireless environment defaults include, but are not limited to: (PCI Requirement 2.1.1)

- Default encryption keys;

- Passwords;

- SNMP community strings;

- Default passwords/passphrases on access points;

- Other security-related wireless vendor defaults as applicable.

Firmware on wireless devices must be updated to support strong encryption (such as WPA or WPA2) for authentication and transmission of data over wireless networks.

1.2.2 Configuration Standards for Systems

Configuration standards for all system components must be developed and enforced. Stephen F. Austin State University must insure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. (PCI Requirement 2.2)

Configuration standards must be updated as new vulnerability issues are identified, and they must be enforced on any new systems before they are added to the cardholder data environment. The standards must cover the following:

- Changing of all vendor-supplied defaults and elimination of unnecessary default accounts;
- Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server; (PCI Requirement 2.2.1)
- Enabling only necessary services, protocols, daemons, etc., as required for the function of the system; (PCI Requirement 2.2.2)
- Implementing additional security features for any required services, protocols or daemons that are considered to be insecure; (PCI Requirement 2.2.3)
- Configuring system security parameters to prevent misuse;
- Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (PCI Requirement 2.2.5)

System administrators and any other personnel that configure system components must be knowledgeable about common security parameter settings for those system components. They must also be responsible to insure that security parameter settings are set appropriately on all system components before they enter production. (PCI Requirement 2.2.1)

System administrators are responsible to insure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (PCI Requirement 2.5)

1.2.3 Non-Console Administrative Access

Credentials for non-console administrative access must be encrypted. To be considered "strong cryptography," industry-recognized protocols with appropriate key strengths and key management should be in place as applicable for the type of technology in use: (PCI Requirement 2.3)

- Must use strong cryptography, and the encryption method must be invoked before the administrator's password is requested;
- System services and parameter files must be configured to prevent the use of telnet and other insecure remote login commands;
- Must include administrator access to web-based management interfaces;
- Use vendor documentation and knowledge of personnel to verify that strong cryptography is in use for all non-console access, and that for the technology in use, it is implemented according to industry best practices and vendor recommendations.

1.3 Protect Stored Cardholder Data

Responsible Parties – Information Technology Services, Merchants

1.3.1 Prohibited Data

Processes must be in place to securely delete sensitive authentication data (defined below) post-authorization so that the data is unrecoverable. (PCI Requirement 3.2)

Payment systems must not store sensitive authentication data in any form after authorization (even if encrypted). Sensitive authentication data is defined as the following:

- The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance; (PCI Requirement 3.2.1)
- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance; (PCI Requirement 3.2.2)
- The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance. (PCI Requirement 3.2.3)

1.3.2 Displaying PAN

Stephen F. Austin State University will mask the display of PANs (primary account numbers), and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show, at most, only the first six and the last four digits of the PAN. This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts. Policies and procedures for masking the display of PANs must mandate the following: (PCI Requirement 3.3)

- A list of roles that need access to displays of full PAN is documented, together with a legitimate business need for each role to have such access;
- PAN must be masked when displayed such that only personnel with a legitimate business need can see the full PAN;
- All other roles not specifically authorized to see the full PAN must only see masked PANs.

1.4 Encrypt Transmission of Cardholder Data Across Open, Public Networks

Responsible Parties – Information Technology Services

1.4.1 Transmission of Cardholder Data

In order to safeguard sensitive cardholder data during transmission over open, public networks, Stephen F. Austin State University will use strong cryptography and security protocols. These controls will be implemented as follows: (PCI Requirement 4.1)

- Only trusted keys and certificates are accepted;

- The protocol in use only supports secure versions or configurations;
- The encryption strength is appropriate for the encryption methodology in use.

Industry best practices (for example, IEEE 802.11i) must be used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment. Weak encryption (for example, WEP, SSL) is not to be used as a security control for authentication or transmission. (PCI Requirement 4.1.1)

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat. (PCI Requirement 4.2)

1.5 Use and Regularly Update Anti-Virus Software or Programs

Responsible Parties – Information Technology Services

1.5.1 Anti-Virus Protection

All systems, particularly personal computers and servers commonly affected by viruses, must have installed an anti-virus program which is capable of detecting, removing, and protecting against all know types of malicious software. (PCI Requirement 5.1, 5.1.1)

For systems considered to be not commonly affected by malicious software, Stephen F. Austin State University will perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. (PCI Requirement 5.1.2)

All anti-virus programs must be kept current through automatic updates, be actively running, be configured to run periodic scans, and be capable of as well as configured to generate audit logs. Anti-virus logs must also be retained in accordance with PCI requirement 10.7. (PCI Requirement 5.2)

Steps must be taken to insure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. (PCI Requirement 5.3)

1.6 Develop and Maintain Secure Systems and Applications

Responsible Parties – Information Technology Services

1.6.1 Risk and Vulnerability

Stephen F. Austin State University will establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.

Risk rankings are to be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data. (PCI Requirement 6.1)

All critical security patches must be installed within one month of release. This includes relevant patches for operating systems and all installed applications. All applicable non-critical vendor-supplied security patches are installed within an appropriate time frame (for example, within three months). (PCI Requirement 6.2)

Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. (PCI Requirement 6.4.6)

1.7 Restrict Access to Cardholder Data by Business Need to Know

Responsible Parties – Information Technology Services, Merchant

1.7.1 Limit Access to Cardholder Data

Access to Stephen F. Austin State University's cardholder system components and data is limited to only those individuals whose jobs require such access. (PCI Requirement 7.1)

Access limitations must include the following:

Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities; (PCI Requirement 7.1.2)

Privileges must be assigned to individuals based on job classification and function (also called "role-based access control). (PCI Requirement 7.1.3)

1.8 Assign a Unique ID to Each Person with Computer Access

Responsible Parties – Information Technology Services

1.8.1 User Accounts

The following must be followed for all user accounts that have access to the system or systems that are part of the payment environment:

- Assign all users a unique ID before allowing them to access system components or cardholder data; (PCI Requirement 8.1.1)

- Limit repeated access attempts by locking out the user ID after not more than six attempts; (PCI Requirement 8.1.6)

- Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID; (PCI Requirement 8.1.7)

- If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. (PCI Requirement 8.1.8)

1.8.2 Vendor Accounts

All accounts used by vendors for remote maintenance shall be enabled only during the time period needed. Vendor remote access accounts must be monitored when in use. (PCI Requirement 8.1.5)

1.8.3 User Authentication

In addition to assigning a unique ID for each user, ensure proper user-authentication management for non-consumer users (i.e.: employees and contractors) and administrators on all system components by employing at least one of the following methods to authenticate all users: (PCI Requirement 8.2)

Passwords/phrases must meet the following: (PCI Requirement 8.2.3)

- Require a minimum length of at least seven characters.

- Contain both numeric and alphabetic characters.

Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.

Change user passwords/passphrases at least every 90 days. (PCI Requirement 8.2.4)

Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used. (PCI Requirement 8.2.5)

Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use. (PCI Requirement 8.2.6)

1.8.4 Remote Access

Secure all individual non-console administrative access and all remote access to the cardholder data environment using multi-factor authentication. (PCI Requirement 8.3)

- Incorporate multi-factor authentication for all non-console access into the cardholder data environment for personnel with administrative access. (PCI Requirement 8.3.1)

- Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network. (PCI Requirement 8.3.2)

Document and communicate password/authentication policies and procedures to all users. (PCI Requirement 8.4)

Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: (PCI Requirement 8.5)

- Generic user IDs are disabled or removed;
- Shared user IDs do not exist for system administration and other critical functions;
- Shared and generic user IDs are not used to administer any system components.

Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all appropriate personnel. (PCI Requirement 8.8)

1.9 Restrict Physical Access to Cardholder Data

Responsible Parties – Information Technology Services, Merchant

1.9.1 Physically Secure All Areas and Media Containing Cardholder Data

Appropriate facility entry controls must be used to limit and monitor physical access to systems in the cardholder data environment. (PCI Requirement 9.1)

Using video cameras, access control mechanisms, or both, individual physical access to sensitive areas shall be monitored. Collected data shall be reviewed and correlated with other entries. This data shall be stored for at least three months, unless otherwise restricted by law. (PCI Requirement 9.1.1)

All publicly accessible network jacks must have physical and/or logical controls to restrict access to the secure network by unauthorized personnel. (PCI Requirement 9.1.2)

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

All media must be physically secured. (PCI Requirement 9.5)

Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include: (PCI Requirement 9.6)

- Media must be classified so the sensitivity of the data can be determined; (PCI Requirement 9.6.1)
- Media must be sent by a secure carrier or other delivery method that can be accurately tracked; (PCI Requirement 9.6.2)
- Management approval must be obtained prior to moving the media from the secured area. (PCI Requirement 9.6.3)

Strict control must be maintained over the storage and accessibility of media containing cardholder data. (PCI Requirement 9.7)

1.9.2 Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI Requirement 9.8)

Hardcopy media must be destroyed by shredding, incineration, or pulping so that cardholder data cannot be reconstructed. (PCI Requirement 9.8.1.a)

Containers storing information waiting to be destroyed must be secured (locked) to prevent access to the contents by unauthorized personnel. (PCI Requirement 9.8.1.b)

1.9.3 Protection of Payment Devices

Devices that capture payment card data via direct physical interaction with the card (such as swipe readers and any other payment terminals) must be protected. This protection must include preventing the devices from being tampered with or substituted. (PCI Requirement 9.9)

Stephen F. Austin State University must maintain an up-to-date list of devices. Employees shall be instructed to maintain the integrity and currency of the inventory. The list should include the following: (PCI Requirement 9.9.1)

- Make and model of all devices;
- Location of each device (for example, the address of the site or facility where the device is located);
- Device serial number or other method of unique identification.

The payment devices must be periodically inspected. Check surfaces to detect tampering (for example, addition of card skimmers to devices). Checks must also be made that will detect substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). (PCI Requirement 9.9.2)

Employees and contractors who interact with the payment devices must be provided with training that enables them to be aware of attempted tampering or replacement of devices. Training should include the following: (PCI Requirement 9.9.3)

- Employees must verify the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices;
- Employees must be instructed not to install, replace, or return devices without verification from management. The inventory list (required previously) must be updated by the employee when device locations are changed or new devices are added;
- Employees need to be aware of suspicious behavior around devices (for example, attempts by unknown or unauthorized persons to unplug or open devices).

1.10 Regularly Monitor and Test Networks

Responsible Parties – Information Technology Services

1.10.1 Audit Log Collection

Stephen F. Austin State University will implement technical controls that create audit trails in order to link all access to system components to an individual user. The automated audit trails created will capture sufficient detail to reconstruct the following events:

- All actions taken by any individual with root or administrative privileges; (PCI Requirement 10.2.2)
- All invalid logical access attempts (failed logins); (PCI Requirement 10.2.4)
- Any use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges. (PCI Requirement 10.2.5)

Stephen F. Austin State University's log generating and collecting solution will capture the following data elements for the above events:

- User identification; (PCI Requirement 10.3.1)
- Type of event; (PCI Requirement 10.3.2)
- Date and time; (PCI Requirement 10.3.3)
- Success or failure indication; (PCI Requirement 10.3.4)
- Origination of event; (PCI Requirement 10.3.5)
- Identity or name of affected data, system component, or resource. (PCI Requirement 10.3.6)

1.10.2 Audit Log Review

Stephen F. Austin State University's systems administrators will perform daily review of the audit logs. This review may be manual or automated but must monitor for and evaluate: (PCI Requirement 10.6.1)

- All security events;
- Logs of all system components that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD), or that could impact the security of CHD and/or SAD;
- Logs of all critical system components;
- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

The audit review must also check the logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment. (PCI Requirement 10.6.2)

Subsequent to log review, systems administrators or other responsible personnel will follow up exceptions and anomalies identified during the review process. (PCI Requirement 10.6.3)

Stephen F. Austin State University must retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). (PCI Requirement 10.7)

1.11 Regularly Test Security Systems and Processes

Responsible Parties – Information Technology Services, Merchant Services

1.11.1 Testing for Unauthorized Wireless Access Points

At least quarterly, Stephen F. Austin State University will perform testing to ensure there are no unauthorized wireless access points (802.11) present in the cardholder environment. (PCI Requirement 11.1)

The methodology must be adequate to detect and identify any unauthorized wireless access points, including at least the following:

- WLAN cards inserted into system components;
- Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.);
- Wireless devices attached to a network port or network device.

To facilitate the detection process, Stephen F. Austin State University will maintain an inventory of authorized wireless access points including a documented business justification. (PCI Requirement 11.1.1)

If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), the configuration must be capable of generating alerts to notify personnel. Detection of unauthorized wireless devices must be included in the Incident Response Plan (see PCI Requirement 12.10). (PCI Requirement 11.1.2)

1.11.2 Vulnerability Scanning

At least quarterly, and after any significant changes in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), Stephen F. Austin State University will perform vulnerability scanning on all in-scope systems. (PCI Requirement 11.2)

Internal vulnerability scans must be performed at a minimum quarterly and repeated until passing results are obtained, or until all "high" vulnerabilities as defined in PCI Requirement 6.1 are resolved. Scan reports must be retained for a minimum of a year. (PCI Requirement 11.2.1)

Quarterly external vulnerability scan results must satisfy the ASV Program guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures). External vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scan reports must be retained for a minimum of a year. (PCI Requirement 11.2.2)

For both internal and external vulnerability scans, Stephen F. Austin State University shall perform rescans as needed to validate remediation of failures detected during previous scans, as well as after any significant change to the network. Scans must be performed and reviewed by qualified personnel. (PCI Requirement 11.2.3)

If segmentation is used to isolate the cardholder data environment from other networks, perform tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems. These tests need to be done from multiple locations on the internal network, checking both for improper accessibility from the out-of-scope zones to the in-scope zone as well as the reverse. (PCI Requirement 11.3.4)

For all in-scope systems for which it is technically possible, Stephen F. Austin State University must deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. The change detection software must be integrated with the logging solution described above, and it must be capable of raising alerts to responsible personnel. (PCI Requirement 11.5.1)

For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider). (PCI Requirement 11.5)

1.12 Maintain a Policy that Addresses Information Security for Employees and Contractors

Responsible Parties – Information Technology Services, Merchant Services, Merchant

1.12.1 Security Policy

Stephen F. Austin State University shall establish, publish, maintain, and disseminate a security policy that addresses how the university will protect cardholder data. (PCI Requirement 12.1)

This policy must be reviewed at least annually, and must be updated as needed to reflect changes to business objectives or the risk environment. (PCI Requirement 12.1.1)

1.12.2 Critical Technologies

Stephen F. Austin State University shall establish usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email, and internet usage. (PCI Requirement 12.3)

These policies must include the following:

- Explicit approval by authorized parties to use the technologies; (PCI Requirement 12.3.1)
- Authentication for use of the technology; (PCI Requirement 12.3.2)
- A list of all such devices and personnel with access; (PCI Requirement 12.3.3)
- Acceptable uses of the technologies; (PCI Requirement 12.3.5)
- Acceptable network locations for the technologies; (PCI Requirement 12.3.6)
- Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity; (PCI Requirement 12.3.8)
- Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. (PCI Requirement 12.3.9)

1.12.3 Security Responsibilities

Stephen F. Austin State University's policies and procedures must clearly define information security responsibilities for all personnel. (PCI Requirement 12.4)

1.12.4 Incident Response Policy

The Information Security Officer shall establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. (PCI Requirement 12.5.3)

1.12.5 Incident Identification

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to:

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry);
- Fraud including inaccurate information within databases, logs, files, or paper records.

1.12.6 Reporting an Incident

The Information Security Officer should be notified immediately of any suspected or real security incidents involving cardholder data:

- No one should communicate with anyone outside of their supervisor(s) or the Information Security Officer about any details or generalities surrounding any suspected or actual

incident. All communications with law enforcement or the public will be coordinated by the General Counsel and Information Security Officer;

- Document any information you know while waiting for the Information Security Officer to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

1.12.7 Incident Response Policy

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery, and root cause analysis resulting in improvement of security controls. (PCI Requirement 12.10.1)

Contain, Eradicate, Recover, and perform Root Cause Analysis

1. Notify applicable card associations.

   Visa

   Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact 1-(650)-432-2978. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa's "What to do if compromised" documentation for additional activities that must be performed. That documentation can be found at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_what_to_do_if_compromised.pdf

   MasterCard

   Contact your merchant bank for specific details on what to do following a compromise. Details on the merchant bank (aka. the acquirer) can be found in the Merchant Manual at http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf. Your merchant bank will assist when you call MasterCard at 1-(636)-722-4100.

   Discover Card

   Contact your relationship manager or call the support line at 1-(800)-347-3083 for further guidance.

2. Alert all necessary parties. Be sure to notify:

   a. Merchant bank;

   b. Local FBI Office;

   c. U.S. Secret Service (if Visa payment data is compromised);

   d. Local authorities (if appropriate).

3. Collect and protect information associated with the intrusion. In the event that forensic investigation is required the Information Security Officer will work with legal and management to identify appropriate forensic specialists.

4. Eliminate the intruder's means of access and any related vulnerabilities.

5. Research potential risks related to or damage caused by intrusion method used.

1.12.8 Root Cause Analysis and Lessons Learned

Not more than one week following the incident, members of the Security Incident Response Team (SIRT) and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy, or security control can be made more effective or efficient, must be updated accordingly.

1.12.9 Security Awareness

Stephen F. Austin State University shall establish and maintain a formal security awareness program to make all personnel aware of the importance of cardholder data security. (PCI Requirement 12.6)

1.12.10 Service Providers

Stephen F. Austin State University shall implement and maintain policies and procedures to manage service providers. (PCI Requirement 12.8)

This process must include the following:

- Maintain a list of service providers; (PCI Requirement 12.8.1)

- Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess; (PCI Requirement 12.8.2)

- Implement a process to perform proper due diligence prior to engaging a service provider; (PCI Requirement 12.8.3)

- Monitor service providers' PCI DSS compliance status; (PCI Requirement 12.8.4)

- Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. (PCI Requirement 12.8.5)

APPENDIX A – PCI SECURITY AWARENESS AND ACCEPTABLE USE POLICY

Stephen F. Austin State University PCI Security Awareness and Acceptable Use Policy

Overview

The intentions for publishing a security awareness and acceptable use policy are not to impose restrictions that are contrary to the established culture of openness, trust, and integrity. Stephen F. Austin State University is committed to protecting all employees, partners, and the university from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Stephen F. Austin State University. These systems are to be used for business purposes in serving the interests of the university, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Stephen F. Austin State University employee and affiliate who deals with payment card information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Stephen F. Austin State University used to process, transmit, or store payment card information. These rules are in place to protect the employees and Stephen F. Austin State University. Inappropriate use exposes Stephen F. Austin State University to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to employees (staff/faculty/students), contractors, consultants, temporary employees, and all other workers at Stephen F. Austin State University, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Stephen F. Austin State University, that is used to process, transmit, or store payment card information, or required to comply with the Payment Card Industry – Data Security Standards (PCI-DSS).

Policy

General Use and Ownership

1. While SFA desires to provide a reasonable level of privacy, users should be aware that the data they create on the university's systems remains the property of Stephen F. Austin State University. Because of the need to protect the network, SFA cannot guarantee the confidentiality of employee's personal information stored on any network device belonging to Stephen F. Austin State University.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

3. IT recommends that any information that users consider sensitive or vulnerable be encrypted.
4. For security and network maintenance purposes, authorized individuals within Stephen F. Austin State University may monitor equipment, systems, and network traffic at any time.
5. Stephen F. Austin State University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. All information on PCI-related systems are classified as confidential. Examples of confidential information include but are not limited to: credit card information, university private, institutional strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System and user level passwords should be changed at a minimum each year.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less.
4. Employees should secure their workstations by logging off or locking (control-alt-delete for Windows users) when the host will be unattended.
5. Use encryption of information in compliance with Information Technology Services (ITS) Security Policies.
6. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the university security standards, including personal firewalls.
7. Postings by employees from a Stephen F. Austin State University email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Stephen F. Austin State University, unless posting is in the course of business duties.
8. All hosts connected to the Stephen F. Austin State University PCI Network, must be approved by the Information Security Officer, and connections will be coordinated through the Office of Information Security.
9. All hosts used by the employee that are connected to the Stephen F. Austin State University PCI Network, owned by Stephen F. Austin State University, shall be continually executing approved virus-scanning software with a current virus database.
10. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Stephen F. Austin State University authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing Stephen F. Austin State University-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Stephen F. Austin State University.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Stephen F. Austin State University or the end user does not have an active license is strictly prohibited. The use of any recording device such as, but not limited to, digital cameras, video cameras, and cell phone cameras, within the premises of all Stephen F. Austin State University properties is prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a Stephen F. Austin State University computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Stephen F. Austin State University account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to IT is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, Stephen F. Austin State University employees to parties outside Stephen F. Austin State University.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Stephen F. Austin State University's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Stephen F. Austin State University or connected via Stephen F. Austin State University's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, in accordance with applicable University Policies.

Definitions

Spam Unauthorized and/or unsolicited electronic mass mailings.

I acknowledge that I have received and read the Security Awareness and Acceptable Use Policy. I understand and agree that my use of University Information Resources is conditioned upon my agreement to comply with this Policy and that my failure to comply with this Policy may result in disciplinary action up to and including termination of my employment.

Note: This acknowledgement can be completed online upon completion of PCI training.

Employee / Contractor / Third Party Signature	Date
Printed Name	Date of Security Awareness Training

APPENDIX B – PERIODIC OPERATIONAL SECURITY PROCEDURES

Stephen F. Austin State University
Periodic Operational Security Procedures

Task	Daily	Monthly	Quarterly	Bi-Annual	Annually	Target Window
Security Policy						
Enterprise Risk Analysis					X	Q1
Policy/standards review					X	Q1
Security awareness orientation					X	Q1
Organizational Security						
Review security policy exceptions compliance			X			Week-1
Asset Classification and Control						
Review system access controls				X		Q2 and Q3
Review access request approvals & audit trail				X		Q2 and Q3
Audit disposal of data and media			X			Week-2
Personnel Security						
Audit terminated employee samples for system, network, application access			X			Week-4
Incident response team meeting			X			Week-1
Physical and Environmental Security						
Visit offsite storage facility and perform media inventory					X	Q3
Review compliance of data center access & visitor logs					X	Q3
System Security						
File Integrity Scan	X					1 a.m.
Review intrusion detection (IDS/IPS) logs	X					8 a.m.
Review all other security and event logs	X					8 a.m.
Device Inspection	x					8 a.m.
External vulnerability scan			X			Week-3
Internal vulnerability scan			X			Week-3
Use a Wireless Analyzer to detect unauthorized wireless devices in use			X			Week-3
Firewall rule set review			X			Week-4
External penetration testing					X	Q2
Internal penetration testing					X	Q2
Data encryption key rotation					X	Q3

APPENDIX C - GLOSSARY

Term	Definition
Access Control	Mechanisms that limit availability of information or information processing resources only to authorized persons or applications.
Application	Includes all purchased and custom software programs or groups of programs designed for end users, including both internal and external (web) applications.
Approved Scanning Vendor (ASV)	An Organization that validates adherence to the PCI DSS by performing vulnerability scans of Internet facing environments of merchants and service providers. All external vulnerability scans of the Cardholder Data Environment must be performed by an Approved Scanning Vendor.
Attestation of Compliance (AOC)	A form that certifies that you are eligible to perform and have performed the appropriate Self-Assessment Questionnaire.
Audit Log	Chronological record of system activities. Provides a trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results. Sometimes specifically referred to as security audit trail.
Cardholder	Customer to whom a card is issued or individual authorized to use the card.
Cardholder Data (CHD)	Those elements of credit card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date and the Service Code.

Cardholder Data Environment (CDE)	Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.
CAV2, CVC2, CID, or CVV2 data	The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card- not-present transactions.
Compensating Controls	Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must 1) meet the intent and rigor of the original stated PCI DSS requirement; 2) repel a compromise attempt with similar force; 3) be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and 4) be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.
Compromise	Intrusion into computer system where unauthorized disclosure, modification, or destruction of cardholder data is suspected.
Database	A structured electronic format for organizing and maintaining information that is accessible in various ways. Simple examples of databases are tables or spreadsheets.
Disposal	Cardholder data must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, USB storage devices,(Before disposal or repurposing, computer drives should be sanitized in accordance with university policy (ITS Policy Handbook, IT Media Protection Policy 14.1.11). The approved disposal methods are cross-cut shredding, incineration, approved shredding, or disposal service.

EMV	An international standard for smart credit cards that have a built-in chip. The EMV smart card provides greater safety than a magnetic stripe card because it can support sophisticated security methods.
Expiration Date	The date on which a card expires and is no longer valid. The expiration date is embossed, encoded, or printed on the card.
Firewall	Hardware, software, or both that protect resources of one network from intruders from other networks.
Magnetic Stripe Data (Track Data)	Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.
Malware	Malicious software designed to infiltrate or damage a computer system without the owner's knowledge or consent.
Merchant Department	Any department or unit (can be a group of departments or a subset of a department) which has been approved by the university to accept credit cards and has been assigned a Merchant identification number.
Merchant Department Responsible Person (MDRP)	An individual within the department who has primary authority and responsibility within that department for credit card transactions.
Payment Card Industry Data Security Standards (PCI DSS)	The security requirements defined by the Payment Card Industry Security Standards Council and the 5 major Credit Card Brands of Visa, MasterCard, American Express, Discover, and JCB.

PIN/PIN block	Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.
Primary Account Number (PAN)	Number code of 14 or 16 digits embossed on a bank or credit card and encoded in the card's magnetic stripe. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.
Qualified Security Assessor (QSA)	An individual who has been certified by the PCI Security Standards Council to validate a merchant's or service provider's adherence to the PCI DSS.
Report on Compliance (ROC)	A form completed by a Qualified Security Assessor that is used to validate a merchant's or service provider's compliance with the Payment Card Industry Data Security Standard. All level one merchants and service providers as well as level two MasterCard merchants must validate compliance with the PCI DSS by submitting a completed Report on Compliance.
Self-Assessment Questionnaire (SAQ)	A validation tool intended to assist merchants and service providers in self-evaluating their compliance with the Payment Card Industry Data Security Standard. There are multiple versions of the PCI DSS SAQ to meet various scenarios.
Sensitive Authentication Data (SAD)	Additional elements of credit card security information that are required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data and PIN/PIN block.
Service Code	The service code that permits where the card is used and for what.

APPENDIX D – DEPARTMENTAL PROCEDURES

For Department: _____

Insert Department Name

In order to comply with the University's Payment Card Acceptance and Security Policy (Policy 14.8) and the Payment Card Industry Data Security Standards (PCI DSS) as well as good business practices related to the handling of our customers' credit card information, this department at Stephen F. Austin State University (SFA) will take steps to ensure payment card security. These steps include:

1) Ensure employees with access to payment card data are properly trained.

   Employees that process over-the-counter transactions will be trained in the proper procedures for card-present transactions.

   Employees that have access to or process payment card information will complete the online payment card training unless an alternative face-to-face training is attended.

   Criminal background checks will be performed on employees with access to lists, reports, and/or storage areas where payment card information is stored. (It will not be required, if the employee's job only involves taking and immediately processing over-the-counter transactions and the employee does not have access to lists, reports, and/or storage areas where payment card information is stored).

   All employees with access to payment card information must read the University's Payment Card Acceptance and Security Policy (Policy 14.8) and certify their intent to comply with the policy on the "Intent to Comply with University Policy for Payment Card Acceptance and Security" form.

2) Job positions that may have access to credit card equipment and credit card information include:

   a. _____

   b. _____

   c. _____

3) Perform annual PCI DSS Compliance assessment and reviews.

   Annually, we will confirm compliance with PCI DSS requirements by completing a Self-Assessment Questionnaire (SAQ).

   Annually, we will review PCI certification of every PIN entry device in use and replacement devices will be requested for any that are no longer certified. The list of certified devices is available at https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

Every service provider's PCI DSS compliance status will be reviewed on an annual basis. Instances of non-compliance will be reported to the Director of Administrative Services and the Bursar for assistance in determining appropriate follow-up actions.

4) Card-Present Procedures

a. Always swipe or insert the payment card when the cardholder is present.

b. Do not double swipe. A double swipe may cause a false authorization that will not be honored by the credit card company.

c. Employees should keep the card in their possession during the processing.

d. At the point of sale, the card should be carefully examined to determine if the card is valid.

Visa Card

Visa account numbers always start with a 4. All digits must be even, straight, and the same size. May be embossed with raised letters or the numbers on the card may be flat.

Visa Brand Mark must appear on the front of the card.

The Mini-Dove Design Hologram may appear on the back of the card or on the front of the card above the Visa Brand.

The word "VOID" will appear on the signature panel if the signature panel has been tampered with.

A three-digit verification code is printed in a separate box to the right of the signature panel on the back of the card with the numbers slanted slightly to the left.

MasterCard

MasterCard account numbers always start with a 5. All digits must be even, straight, and the same size. May be embossed with raised letters or the numbers on the card may be flat.

MasterCard Brand (interlocking red and yellow circles) may appear on the front or back of the Master Card.

The three dimensional MasterCard hologram with interlocking circles should reflect light and appear to move when the card is rotated.

The word "VOID" will appear on the signature panel if the signature panel has been tampered with.

A three-digit verification code is printed in a separate box to the right of the signature panel on the back of the card with the numbers slanted slightly to the left.

Discover Card

Discover Card account numbers always start with a 6. All digits must be even, straight, and the same size. May be embossed with raised letters or the numbers on the card may be flat.

"DISCOVER" or "DISCOVER NETWORK" appears on a tamper-evident signature panel. Some cards contain an ultraviolet image that repeats the word "DISCOVER".

A three-digit verification code is printed in a separate box to the right of the signature panel on the back of the card with the numbers slanted slightly to the left.

American Express Cards

All American Express Card Numbers start with a 37 or 34 and are embossed on the front of the card. Some Cards also have the account number printed on the back of the Card and must match the number on the front of the card.

American Express cards have a four digit verification code on the front of the card.

e. Check the expiration date; do not accept cards with a transaction date after the expiration date.

f. Verify the signature panel on the back of the card is signed and check for signs of tampering.

g. If the signature panel is blank, request a signature and ask the cardholder to provide current identification, such as university ID or driver's license.

h. Verify that the Visa, MasterCard and Discover card contain a 3 digit verification code.

i. Debit cards should be processed as a debit card if practical. Debit cards processed as credit transactions will incur higher fees.

j. Verify the magnetic strip is smooth and straight and does not show signs of tampering.

k. Compare name, number, and signature on the card to the transaction receipt.

5) Ensure proper data handling of payment card records.

Payment card data will be treated as confidential information and will be restricted to only those personnel with a "business-need–to-know" security level.

Data that is not absolutely necessary in order to conduct business will *not* be retained in paper format.

Payment card data will not be stored on any computer, thumb-drive, CD, DVD, or other storage device.

The 16-digit account number, also known as the primary account number (PAN), will be masked so that only the last 4 digits are visible when displayed on Point of Sale (POS) terminals or any other electronic display.

The entire 16-digit PAN will not be stored or saved after authorization; however, the last 4 digits of the PAN may be stored when necessary.

Paper media containing payment card information will be destroyed via crosscut shredder immediately after the transaction is processed.

Under no circumstances will the personal identification number (PIN) be recorded, copied, or stored anywhere.

The card verification code (i.e., the three- or four-digit code) used to validate a card-not-present transaction, will NEVER be stored after authorization, even if encrypted.

Employees will not accept or request the PAN or sensitive authentication data, including the magnetic stripe data, card verification code or pin data, via facsimile, e-mail, campus mail, or any other end-user messaging technologies (instant messaging, chat, etc.).

If an email is received that contains the PAN or any other sensitive authentication data, employees will be trained to immediately delete the message from their computers and empty their email trash bin and then notify the sender of the email that the University does not accept payment card information via email and that it should not be attempted again. Employees will **not** notify the sender using the Reply function in the email reader as this may inappropriately transmit credit card information.

Physical access to records will be restricted to staff with a "business-need-to-know" security level. Means such as locked file cabinets and restricted file rooms as well as restricted distribution of such records will be used.

Strict control will be maintained over the internal or external distribution of any kind of media containing cardholder data. Controls will include:

- Classifying media so the sensitivity of the data can be determined;
- Using a secure carrier or other delivery method that can be accurately tracked;
- Obtaining prior approval from management or management's designee before moving media to secure area.

Payment card receipts will be retained as required by the State of Texas Record Retention Schedule and, at the appropriate time, will be shred using a crosscut shredder or PCI DSS approved manner.

If payment card data is shared with any external service provider, we will ensure that:

- A list of providers is maintained;
- A written agreement is executed and retained that defines the provider's responsibility related to the security of this information.

6) Ensure security of payment card devices.

A list of payment card devices will be maintained.

Employees will be trained to be aware of attempted tampering or replacement of payment card devices, including:

- inspecting devices regularly to detect tampering;
- verifying identity of persons claiming to repair devices;
- being aware of suspicious behavior around devices;
- and reporting suspicious behavior or device tampering to management.

7) Ensure all contracts use standard language.

Contracts with third parties with access to cardholder data will include standard language that requires adherence to PCI DSS; and the contracts will be reviewed by legal counsel for proper PCI DSS language.

8) Ensure system configuration at the department level is secure.

University merchants will ensure, through working with the Information Technology department and others, as needed, that:

- Anti-virus software will be implemented, updated, and run at regular intervals;
- Vendor patches will be installed on a timely basis;
- Access will be granted to systems only on a "business-need-to-know" basis.

If external vendors need remote access to service our third-party software, their access will be granted only for the time needed to do the necessary task(s) and then immediately disabled.

9) Ensure all refunds are processed in accordance with credit card rules and regulations.

We will make our refund policy available to all customers.

With the exception of tuition and fee payments, NO CASH OR CHECK REFUNDS are permitted on credit card purchases. This also includes NO CASH BACK at the time of the original sale.

10) Ensure that departmental employees know how to report suspected theft of information or security breach.

Security incident means any deliberate attacks on your communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage the university's reputation. Either way, having a plan in place will allow you to react more quickly and intelligently, and help you control the consequences to you and Stephen F. Austin State University.

React to a security incident by following the steps below:

a. Immediately investigate the incident to determine what has happened, what harm has been done, and if the incident is still in progress.

- If there is any threat whatsoever of physical harm to staff or others (for example, from a burglar) withdraw immediately and call the police.
- If there is no immediate threat, start a written event log by noting date and time of all actions.
- Your first priority is to limit the damage to your customers and the university (as described in the next section), but your next highest priority should be to try to preserve information about the attack.
- If the attack involved physical evidence (such as from a break-in), do not disturb the area, but call the police.
- If the attack affected computers, make every effort to NOT use the computers: DO NOT log on to them, DO NOT turn them off (this is because doing so destroys forensic evidence of what the attackers did and how they did it.). DO disconnect them from all networks and connections.
- Try to identify at a high level what damage has been done. Has sensitive information about the university or its customers possibly been stolen or changed

without permission, or destroyed/deleted? Make an estimate of how sensitive this information is, and how many people have possibly been affected.

b. Take action as soon as possible to limit the scope of the damage. This typically includes preventing further unauthorized access to customer or university information. (Keep in mind, though, that in many cases it is impossible to undo the damage already done.)
   - If there is any chance that damage is still being done (for example, if hackers are still looking at your computer files, or if a computer is still infected with a virus), your first priority must be to limit the damage. Where possible, DO NOT turn computers off, but instead disconnect them from all network connections so that hackers cannot get in (or stay in) and viruses, etc., cannot spread to other devices.
   - If there is any physical damage (for example, broken locks on doors) try to secure the area to prevent anyone else from getting in after the fact.

c. Notify the information security office. All security incidents should be reporting in accordance with university policy 14.14, Information Security Incident Response and Reporting.

d. Complete your investigation as to what happened and why.
   - At a minimum, determine when the attack happened, over what period, what the damage was, (for example, what data was affected, what happened to it, which people were affected), and how the attack succeeded (if it did).
   - Use this opportunity to identify how your security processes and systems could be improved.

e. Start to make any appropriate changes identified in your findings for improving your security processes and systems.

We will ensure that all personnel affected by these procedures are aware of these responsibilities on at least an annual basis.

For Department:_____

Insert Department Name

I have read and understood the policy and procedures for the acceptance of payment cards, and agree to adhere to it.

Name (Print legibly please)	University ID Number	Signature	Date

Terminal Inventory

Department Name:_____

Merchant ID: _____

Date: _____

Verified By:_____

		Location	Equipment Type	Serial Number
Example	Terminal	McKibben Rm 304J	FD100	NT0123456789
Example	Pin Pad	McKibben Rm 304J	FD 35	123CA12345
1	Terminal			
1	Pin Pad			
2	Terminal			
2	Pin Pad			
3	Terminal			
3	Pin Pad			
4	Terminal			
4	Pin Pad			
5	Terminal			
5	Pin Pad			
6	Terminal			
6	Pin Pad			
7	Terminal			
7	Pin Pad			
8	Terminal			
8	Pin Pad			
9	Terminal			
9	Pin Pad			

PCI DEVICE INSPECTION LOG

Inspect all devices that can accept credit card payments daily. A copy of this log may be requested quarterly by the PCI Compliance Team. ***Reminder: this log is only for devices that allow swipe or EMV cards (chip/dip).***

- Check your PCI devices for tampering daily.
- Ensure devices inspected match the terminal inventory
- The inspector's signature is required.
- Note any replacements.

Department Name: _____

Location: _____

Merchant ID: _____

Device Make/Model	Serial Number	Date Inspected	Inspected By	Signature

PCI DEVICE INSPECTION LOG (Continued)

Device Make/Model	Serial Number	Date Inspected	Inspected By	Signature