# Payment Security Policies and Procedures

For Department/Office of\_\_\_\_\_\_\_\_\_\_

## System Policy: 21.01.02 Receipt, Custody and Deposit of Revenues, Section 2.5

System members accepting credit and/or debit cards as a method of payment must adhere to industry standards to protect cardholder data and must certify annually that the processes and systems used to accept and transmit cardholder data are in compliance with industry standards. Members must complete the payment card industry data security training.

## Policy Implementation Procedures:

**[Bolded notes within brackets, such as this one, are intended to provide information or instruction as you complete this template.** *Italicized sections* *in maroon* **are meant to be filled out by you. Delete these instructions as you complete each section, leaving a clean, complete policy document. Numbers in parenthesis like this** (12.1) **are references to specific sections of the PCI-DSS that call for the policy or procedure in question. These references can be removed or left in.]**

## Definitions

* **Confidential -** information that must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements.)
* **Primary Account Number (PAN) –** The full account number (typically 15 to 19 digits) associated with the customer’scredit or debit account. Typically printed or stamped on the front of the customer’s card, stored on a magnetic strip, and sometimes on an embedded chip.
* **Cardholder Data** – At a minimum, any amount of the PAN greater than the first 5 and last 4 digits. When that threshold is exceeded, the customer name and card expiration date become in scope as cardholder data. If only the first 5 and last 4 digits of a PAN are exposed, then customer name and card expiration date are not considered part of cardholder data.
* **Card** – Here, used generically to refer to debit and credit cards accepted by Texas A&M merchants as a form of payment for goods or services.

## Policy and Procedure Objectives:

(12.1.1) All card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety. Card processing activities must be conducted as described herein and in accordance with the standards and procedures listed in the Related Documents section of this Policy. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI-DSS.

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

## Applicability and Availability

This policy applies to all employees, contractors, and consultants. (12.1) Relevant sections of this policy apply to vendors, off-site contractors, and business partners. The most current version of this policy is available *at X URL or through Y office*.

**[The section immediately below is understood to apply to systems that transmit, process, or store cardholder data through anything other than analog phone lines.]**

## Adherence to Standards

(2.2.a) Documented configuration standards must be maintained for applications, network components, critical servers, and wireless access points. These standards must be consistent with industry-accepted hardening standards as defined, for example, by SysAdmin Assessment Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).These standards must also be consistent with university Standard Administrative Procedure (SAP) 29.01.99.M1 and supporting procedures. **[2.2.b should be captured in your system configuration standard; 2.2.c and 2.2.3.b should be covered in your procedure for new server set-up]**

Configuration standards must include:

* (5.2) updating of anti-virus software and definitions
* (6.1.b) provision for installation of all relevant new security patches within one month
* (8.5.8.b) prohibition of group and shared passwords

## Handling of Cardholder Data

(3.1) Texas A&M System’s records retention policy is founded on Texas Government Code 441.180. The System’s policy is found at <http://policies.tamus.edu>, document 61.99.01. This policy links to Texas A&M System Records Retention Schedule. Credit card receipts are listed under section 4.108.10 – Credit/Debit Card Merchant Receipt found on page 34. The retention period for these items is “expiration of dispute resolution period”. However, the customer’s full card number is not considered a necessary component of the receipt information and can be redacted immediately.

 (3.3) In accordance with Fair and Accurate Credit Transactions (FACTA) law, Primary Account Numbers (PAN) and expiration dates are always hidden or masked on *customer* receipts, both on screen and printable. **[Verify that this is so.]** PANs on the merchant copy of the receipt *are/are not* masked, and thus *do/do not* fall under the document retention policy above. Full PANs on daily batch reports or other retrievable reports are *masked/not masked*.

Those with a need to see full credit card numbers must request an exception to this policy using a written exception process. Instances in which PANs are not masked are done so for the following business reasons: *Insert business justification*.

(4.2.b) Unencrypted PANS may never be transmitted via email, instant messaging, texting/SMS, or other messaging tools. In the event that a customer or 3rd party sends a PAN using such a method, we respond by *Insert your response here. It is recommended that you erase the message from your system and notify the sender that you do not accept PANs in that manner, asking them to resubmit in a secure manner.*

Our department *does/does not* store cardholder data after authorization.

**[You may delete the remainder of this section if you do not store cardholder data on paper or electronically. If you do store cardholder data, University Records Management can direct you to established record management processes compliant with all the relevant statutes, laws, regulations, and legal decisions to which we, as a public university, are subject.]**  (9.7) *University SAP 29.01.99.M1.29-- Data Classification and Protection* applies to the identification and classification of confidential information. *Department name* uses the following classification system to identify media as Confidential: *(directory naming, database naming, numbering system, rubber stamp, filing system, etc.).* Information resources (including hard copies) classified as Confidential due to the presence of cardholder data are logged using the Records Inventory Worksheet provided by University Records Management. Because the log notates the location of Confidential location, the log itself is Confidential and is secured as such.

Cardholder data that meets the following criteria: *Insert criteria. An example would be, “Cardholder data no longer needed for dispute resolution.”*  is *(automatically/manually) (redacted /deleted) on a (daily/weekly/monthly/quarterly)* schedule via *describe method*. **[When cardholder data cannot be removed automatically, also describe your audit process—conducted at least quarterly—to verify that stored cardholder data does not exceed retention requirements.]**

(9.10) **[Be sure to include processes for any cardholder data stored on transportable media as well. This applies equally to paper or electronic material kept on-site AND off-site. Approved destruction methods for hardcopy materials are cross-cut shred, incinerate, or pulping. For electronic media you may purge, degauss, shred, or otherwise destroy electronic media in such a way that data cannot be reconstructed. ]**

(9.7) Distribution, maintenance, and storage of media containing cardholder data, must be controlled, including that distributed to individuals. (9.9) *The Chief Security Officer or similar* performs periodic media inventories to validate the effectiveness of these controls. Confidential media sent or stored offsite is logged by *employee name and/or title* and authorized by *Chief Security Officer or similar.* Confidentialmedia is only released for the following reasons: *(offsite archival storage, analysis or processing by FMO, etc.)*. Confidential media is sent off-site via *(a secured courier or other delivery method that can be tracked. Describe it here.).*

## Access to Cardholder Data

 (7.1, 8.5.1) Access to full cardholder data is restricted to “need to know” based on job duties. Only those with the following job classification or duties are allowed access to cardholder data: *list job titles or duties*

*[Office name]* requires current authorization forms for each employee with access to cardholder data. The authorization form specifies the type and extent of access the employee has, and is signed by management.

 **[If storing electronically]** Procedures for user account creation and management are documented in university SAP 29.01.99.M1.03 Account Management. Access rights to privileged User IDs are restricted to least privileges necessary to perform job responsibilities. User access permissions are handled via the automated role-based control system, described as *[describe how you implement user roles in your access control system]*.

Vendor user accounts [are/are not] permitted in our department’s cardholder data environment. **[If permitted]** Vendor accounts are governed by university SAP 29.01.99.M1.22 Vendor Access. Accounts are disabled except when needed by the vendor and monitored while in use.

## Critical Employee-Facing Technologies

(12.3.5) University SAP 29.01.99.M1.02 Acceptable Use identifies relevant policies and procedures that pertain to aspects of acceptable use of information resources. Within the transaction environment, information technology is restricted to only mission-critical systems.

Remote access to the cardholder data environment *is/is not* permitted. **[If permitted, add the following bullets.]**

* (12.3.10) the storage of cardholder data onto local hard drives and removable electronic media when accessing such data via remote access technologies is prohibited.
* (12.3.10) copy, move, storage and print functions are prohibited during remote access.

For critical employee-facing technologies (inclusive of remote access technologies, wireless technologies, removable electronic media, email usage, internet usage, laptops, and personal data/digital assistants), the following is required:

* (12.3.1) explicit management approval to use the devices
* (12.3.2) that all device use is authenticated with username and password or other authentication item (for example, token)
* (12.3.3) a list of all devices and personnel authorized to use the devices
* (12.3.4) labeling of devices with owner, contact information, and purpose
* (12.3.8) automatic disconnect of remote access technology sessions after a specific period of inactivity
* (12.3.9) activation of remote access technologies used by vendors only when needed by vendors, with immediate deactivation after use.

The attached Departmental Usage Standards includes (12.3.7) a list of information technology products approved for the cardholder data environment and (12.3.6) acceptable network locations for the technology.

## Roles & Responsibilities

(12.5) *Your department’s equivalent to a Chief Security Officer* is responsible for overseeing all aspects of information security, including but not limited to:

* (12.5.1) creating and distributing security policies and procedures
* (12.5.2) monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel
* (12.5.3) (12.9) creating and distributing the security Incident Response and escalation procedures, referenced in SAP 29.01.99.M1.09 Incident Management. The PCI-related security Incident Response plan includes:
	+ (12.9.1) roles, responsibilities, and communication
	+ (12.9.1) coverage and responses for all critical system components
	+ (12.9.1) notification, at a minimum, to *the department head or equivalent*, FMO, and CIS.
	+ (12.9.1) strategy for business continuity post-compromise
	+ (12.9.1) reference or inclusion of incident response procedures from card associations
	+ (12.9.1) analysis of legal requirements for reporting compromises
* (12.9.2) annual testing
* (12.9.3, 12.9.5) designation of personnel to monitor for intrusion detection, intrusion prevention, and file integrity monitoring alerts on a 24/7 basis
* (12.6; 12.6.1.a; 12.9.4) With the HR Liaison, ensuring that all applicable employees (including new employees) are assigned and complete Texas A&M’s online PCI training
* (12.9.6) evolving the incident response plan according to lessons learned and in response to industry developments
* (10.6.a) review security logs at least daily and follow-up on exceptions
* execute an annual (12.1.2) risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment. **[If cardholder data is stored electronically, incorporate your ISAAC report into this assessment.]**

(12.2.a) *Your department’s Information Technology Office or equivalent* shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS (for example, user account maintenance procedures, and log review procedures).

System and Application Administrators shall:

* (12.5.2) monitor and analyze security alerts and information and distribute to appropriate personnel
* (12.5.4) administer user accounts and manage authentication
* (12.5.5) monitor and control all access to data
* (12.8.1) maintain a list of service providers
* (12.8.3) ensure there is a process for engaging service providers including proper due diligence prior to engagement. This due diligence includes verifying that the service provider is has been validated compliant against the appropriate security standard, i.e. PCI-DSS, PA-DSS, etc.
* (12.8.4, 12.4) maintain a program to verify service providers’ PCI-DSS compliant status, with supporting documentation
* (10.7.a ) retain audit logs for at least one year

The HR Liason is responsible for tracking employee participation in the security awareness program, including:

* (12.6.1.b) facilitating participation upon hire and at least annually
* (12.6.2) ensuring that employees acknowledge in writing at least annually that they have read and understand Texas A&M’s information security policy and this Payment Security Policy.
* (12.7) screen potential employees prior to hire to minimize the risk of attacks from internal sources

Upon notification, the Purchasing and Contracts departments will ensure that for service providers with whom cardholder information is shared:

* (12.8.1, 12.4) written contracts require adherence to PCI-DSS by the service provider

(12.8.2, 12.4) written contracts include acknowledgement or responsibility for the security of cardholder data by the service provider. The following statement (or something similar) is required in all contracts with Service Providers.

(Service Provider) acknowledges responsibility for the security of (Department)’s cardholder data and the cardholder data environment which (Service Provider)’s agents or representatives may access or encounter in the course of supporting (Department). (Service Provider) agrees to adhere to the departmental and University security policies as well as the PCI Data Security Standard for the length of the agreement or until (Service Provider) no longer has access to cardholder data or (department)’s cardholder data environment.

## Applicable Legislation, Industry Standards, A&M System Regulations and Rules

* System Policy 61.99.01 – Retention of State Records
* Texas A&M Standard Administrative Procedures (SAP) 29.01.99.M1
* 29.01.99.M1.03 Account Management
* 29.01.99.M1.11 Intrusion Detection
* 29.01.99.M1.18 Security Monitoring
* 29.01.99.M1.21 Information Resources – System Development and Acquisition
* 29.01.99.M1.22 Vendor Access
* 29.01.99.M1.23 Malicious Code
* 29.01.99.M1.29 Data Classification and Protection
* Fair & Accurate Credit Transactions (FACTA)
* Texas Administrative Code Title 1, Part 10, Chapter 202, Subchapter C
* PCI Security Standards

## Appendix [each of these items are additional, required documents that supplement the above policies]

* Incident Response Plan
* Risk Assessment
* Departmental Usage Standards **[to include the following]**
* List of information technology products approved for the cardholder data environment
* **[For departments that transmit cardholder data over a network or the internet]**
	+ the items listed under Adherence to Standards above
	+ (6.3.7) Procedures for reviewing custom internal application and web applications code changes
	+ Documentation of the cardholder data environment’s scope, including a network diagram