THE INTERNATIONAL

TEXAS A&M **INTERNATIONAL** UNIVERSITY

Standard Administrative Procedure (SAP)

21.01.02.L0.01 Credit Card Collections

First Approved:	**September 1, 2010**
Revised:	**February 24, 2014**
	October 4, 2018
Next Scheduled Review:	**October 4, 2023**

Procedure Statement and Reason for Procedure

Texas A&M International University (TAMIU) offers University departments the convenience of accepting credit cards as payment for goods and services provided.

This SAP establishes the process for accepting credit card payments and ensuring adherence to Payment Card Industry Data Security Standards (PCI DSS) as required by System Regulation 21.01.02, *Receipt, Custody and Deposit of Revenues*.

Procedures and Responsibilities

1. CREDIT CARD SECURITY

TAMIU and the Payment Card Industry (PCI) take the safeguarding of cardholder data very seriously. Failure to comply with TAMIU and/or industry security regulations may result in the revocation of the department's merchant account or, in the case of lost or stolen cardholder data, assessment of severe fines on the department by the bank. Merchant departments are financially responsible for fines resulting from security breaches that originate from payment card systems in their operations.

1.1 Before a merchant department may receive credit card payments, it must develop and implement adequate security and internal controls that meet PCI DSS requirements and TAMIU Rule 29.01.99.L1, *Information Resources*. All equipment, software, and business processes must comply with current PCI security standards. To provide adequate security, the combined efforts of the business and information technology functions of TAMIU are necessary.

1.2 The design and architecture of computer systems and networks associated with credit card processing, as well as the protocols used to transmit such data, must be approved by the TAMIU Office of Information Technology (OIT) prior to implementation. Subsequent changes must be approved prior to implementation.

1.3 All equipment and software, including point of sale (POS) equipment and software, must comply with current PCI security standards. No equipment will be allowed to be used unless approved by the Comptroller's Office. No software, including POS software, will be allowed to be used unless approved by the Comptroller's Office and OIT. Non-compliant equipment or software must either be reconfigured or replaced.

1.4 In addition to the initial PCI Compliance Questionnaire completed during setup, each merchant department is required to complete an annual PCI self-assessment questionnaire (PCI SAQ).

1.5 Merchant departments must ensure that credit card data is never transmitted over end-user technologies such as email, texting, or instant messenger.

1.6 Merchant departments must obtain background checks for individuals authorized to have access to cardholder data and assign TAMIU PCI training upon hire.

1.7 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 legitimate business needs.

1.8 Before engaging with third-party vendors who support the transaction process (through software, equipment, hosting, personnel, etc.), the vendor must prove PCI compliance, contractually take responsibility for cardholder security to the extent of their control, and commit to ongoing PCI security compliance.

1.9 OIT will perform periodic reviews of computer and/or computer networks to ensure that security features are in place and are adequate to secure credit card data. The Comptroller's Office will periodically perform reviews of business procedures to help merchant departments identify ways to better protect cardholder information. Reviews are also available upon request.

2. MERCHANT DEPARTMENT RESPONSIBILITIES

Merchant departments participating in the credit card program must comply with all rules and procedures issued by TAMIU, the Comptroller's Office, and the PCI DSS. Merchant departments will conduct periodic business reviews and assist with the annual PCI SAQ. Merchant departments are responsible for notifying the University Police Department, OIT (if applicable), and the Comptroller's Office in the event of a suspected security breach.

3. COMPTROLLER RESPONSIBILITIES

The Comptroller’s Office is responsible for administering the TAMIU credit card program and for ensuring that participating departments are provided updates on all rules, procedures, and security standards. In addition, the Comptroller’s Office will coordinate with the merchant bank on the merchant department’s behalf in cases of a suspected security breach; distribute and coordinate the preparation of the annual PCI SAQ by each merchant department; work closely with both the merchant department and OIT to ensure that all necessary security procedures are in place to ensure protection of sensitive credit card data; and assess service charges to merchant departments for credit card transactions. The Comptroller’s Office is also responsible for the submission of the completed PCI SAQ’s to the Texas A&M University System Office.

4. OIT NETWORK AND SECURITY GROUPS RESPONSIBILITIES

OIT will perform vulnerability scans of PCI computer systems and will require configuration changes to eliminate vulnerabilities. This is both in the preparation for and in addition to vendor scans required for PCI compliance. Vulnerabilities must be mitigated as soon as practical. To meet TAMIU security needs, OIT security standards may be stricter than the PCI requirements. OIT is responsible for approving the configuration of merchants’ PCI computer system.

5. REQUIRED TRAINING

Merchant department staff who answer questions on the annual PCI SAQ and employees with payment processing responsibilities, including IT staff who support systems that process credit card data, are required to complete an online PCI Security training course assigned by TAMIU. Annual refresher courses are also required.

6. DISPOSAL OF SURPLUS OR NON-FUNCTIONAL EQUIPMENT

When a merchant department no longer needs a particular device to swipe or read credit cards, that card reader must be returned to the Comptroller’s Office.

7. DISCIPLINARY ACTIONS

Violation of this SAP may result in disciplinary action which may include termination for employees, termination of business relationships for contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion for students. Additionally, individuals are subject to loss of TAMIU Information Resources access privileges and civil and criminal prosecution.

Related Statutes, Policies, Regulations, or Rules

System Regulation 21.01.02, *Receipt, Custody, and Deposits of Revenue*

TAMIU Rule 29.01.99.L1, *Information Resources*

TAMIU SAP 29.01.99.L1.08, *Incident Management*

Definitions

Merchant Accounts - Special bank accounts issued by a merchant processing bank (also called a credit card processor) that allow a business to accept credit, debit, gift, and other payment cards.

Merchant Department - Any TAMIU department that processes or receives payments with credit/debit, checks, or cash for services or goods rendered.

Payment Card Industry Data Security Standards (PCI DSS) - The Payment Card Industry Security Standards Council creates these standards for the purpose of safeguarding sensitive cardholder data. The precise security measures required by a department will vary depending on how credit cards are accepted – in person, over the phone, or on the internet – but all are covered in the PCI DSS.

Appendix

Payment Card Industry Data Security Standards (PCI DSS)

Contact Office

Comptroller’s Office, 956-326-2812