Standard Administrative Procedure (SAP)

21.01.02.L1.01 Credit Card Collections

Approved: September 1, 2010
Last Revised: February 24, 2014
Next Scheduled Review: February 24, 2016

Standard Administrative Procedure Statement

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

Applicability
The purpose of this SAP is to describe the requirements for Payment Card Industry (PCI) compliance and prevent and control credit card fraud by identifying and training employees with payment processing responsibilities. It applies to all TAMIU employees who process credit card payments.

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 University department that processes or receives payments with credit/debit, checks, or cash for services or goods rendered.

Payment Card Industry Data Security Standard (PCI DSS): A set of comprehensive requirements for enhancing payment account data security which was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., to help facilitate the broad adoption of consistent data security measures on a global basis.

Procedures and Responsibilities

To be considered PCI compliant, a completed SAQ must be submitted to the TAMU System Office with a confirmation of compliance status.
1. **CREDIT CARD SECURITY**
   TAMIU and the Payment Card Industry take the safeguarding of cardholder data very seriously. Failure to comply with University 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. **Departments are financially responsible for fines resulting from security breaches that originate from payment card systems in their operations.**

   PCI Security Standards can be found at [https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org).

2. **MERCHANT RESPONSIBILITIES:**
   2.1 Before a merchant department may receive credit card payments, it must adhere to the security and internal controls manual provided by the Comptroller’s Office (which meets Payment Card Industry Data Security Standard (PCI DSS) requirements) and University Rules (see 24.99.01.L1: Security of Electronic Information Resources). These controls are both technical and procedural, and merchant department supervisors will be responsible for monitoring and checking adherence by their merchant department employees.

   2.2 Merchant departments are responsible for complying with all rules and procedures issued by the TAMIU Comptroller and with all PCI Data Security Standards. They must also provide assistance in completing the annual PCI questionnaire. Merchant departments are responsible for notifying the University Police Department, OIT Security (if applicable – see SAP 29.01.99.L1.08 - Incident Management), and the TAMIU Comptroller in the event of a suspected security breach.

   2.3 Merchant departments must submit an application to Comptroller’s office to obtain new or replacement equipment. This application can be obtained in the Comptroller’s office.

3. **COMPTROLLER RESPONSIBILITIES:**
   3.1 The TAMIU Comptroller is responsible for administering the Texas A&M International University credit card program and for ensuring that merchant departments are provided with updates on all rules, procedures, and security standards. In addition, the Comptroller will: coordinate with the merchant bank on the merchant’s behalf - including cases of a suspected security breach; distribute and coordinate the preparation of the annual PCI questionnaire by each merchant department; work closely with the merchant department and OIT to ensure that all necessary security procedures are in place to ensure protection of sensitive credit card data; assess service charges to merchant department accounts for credit card transactions, and submit the completed PCI SAQs to System Office. For more information on transaction service charges, please contact the TAMIU Comptroller.

   3.2 The Comptroller’s Office will be responsible for replacements or acquisition of new equipment for any campus merchant. Approval from OIT is required prior to purchasing equipment.

   3.3 The Comptroller’s Office will prepare and distribute the Internal Controls Manual.
4. **OIT NETWORK AND SECURITY GROUPS RESPONSIBILITIES:**
   4.1 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 Office of Information Technology (OIT) Network and Security groups prior to implementation. Subsequent changes must be approved prior to implementation. This includes the purchase of equipment to process payments.
   4.2 The OIT Network and Security Groups will ensure all equipment and software must comply with current PCI security standards. Non-compliant equipment or software must either be reconfigured or replaced.
   4.3 The OIT Network and Security groups will perform vulnerability scans of PCI computer systems and will require configuration changes to eliminate vulnerabilities. (See SAP 29.01.99.L1.33: Network Scanning and Vulnerability Assessments). This is, both, in preparation for and in addition to vendor scans that are required for PCI compliance. Vulnerabilities must be mitigated as soon as practical. In order to meet University security requirements, the OIT Network and Security groups’ standards may be stricter than the PCI requirements.
   4.4 The OIT Network and Security groups are responsible for approving the configuration of merchants' PCI computer systems.

5. **REQUIRED TRAINING:**
   Merchant staff who answer questions on the annual PCI questionnaire 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 through TrainTraq. Annual refresher courses are also required.

6. **DISPOSAL OF SURPLUS OR NONFUNCTIONAL EQUIPMENT:**
   When a department no longer needs a particular device to swipe or read credit cards, that card-reader must be returned to the TAMIU Comptroller for appropriate disposal.

7. **PCI SAQ QUESTIONNAIRES**
   In addition to the initial PCI Compliance Questionnaire completed during setup, an annual PCI self-assessment questionnaire is required to be completed. PCI self-assessment questionnaire B will be completed by the Comptroller and questionnaires A and C will be completed by OIT.

**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, Rules or Requirements**

- Supplements System Regulation 21.01.02, Receipt, Custody and Deposit of Revenues
- University Rule 24.99.01.L1, Security of Electronic Information Resources
- University SAP 29.01.99.L1.33, Network Scanning and Vulnerability Assessments
- University SAP 29.01.99.L1.08, Incident Management
Appendix

Payment Card Industry Data Security Standards (PCI DSS)

Contact Office

For clarification or interpretation, contact the Business Office (Comptroller).