PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

21.01.02.P0.03 Credit Card Collections Security
Approved November 6, 2013
Revised October 23, 2023
Next Scheduled Review: October 1, 2028

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to establish the process for accepting credit card payments and ensure adherence to Payment Card Industry Data Security Standards (PCI DSS) as required by System Regulation 21.01.02 Receipt, Custody and Deposit of Revenues.

Definitions

Confidential Information - information that is confidential pursuant to state or federal law. Such information may also be subject to state or federal breach notification requirements. See the Texas A&M University System Data Classification Policies and Procedures for additional information.

Primary Account Number (PAN) – the full account number (typically 15 to 19 digits) associated with the customer's credit or debit account. It is 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 or last 4 digits. When that threshold is exceeded, the customer name and card expiration date is considered as part of the cardholder data. If only the first 5 or last 4 digits of the PAN are exposed, then the customer name and card expiration date is not considered part of the cardholder data.

Card – here, used generically to refer to debit and credit cards accepted by university authorized merchants as a form of payment for goods or services.

Payment Card Industry Data Security Standards (PCI or PCI-DSS) – standards created by the PCI Security Standards Council for the purpose of safeguarding sensitive cardholder data.

Authorized Department or Merchant – any university department or office that is authorized by the Office of Treasury Services to accept credit, debit, gift, or other payment cards.

Merchant Level – this classification is based on transaction volume. Merchants are ranked as Level 1 through 4, Level 1 being the highest volume merchants subject to higher security risk. Any merchant that suffers a credit card data security breach, regardless of transaction volume, is automatically elevated to Level 1.

Official Procedures and Responsibilities

1. GENERAL

1.1 Prairie View A&M University (PVAMU) accepts credit cards as payment for goods and services provided, as well as for philanthropic contributions. Authorized departments may only accept credit card payments in person, online, or over the telephone. The Office of Development is the only authorized department that may accept credit card payments by mail to a designated post office box only.

1.2 In order to accept credit and/or debit cards as a method of payment, or philanthropic gift, departments must protect cardholder data, certify annually that the processes and systems used to accept and transmit cardholder data are in compliance with industry standards, and complete payment card industry data security training annually.

1.3 Credit card information should not be stored on a computer. Credit Card data (account number, expiration date and CVV number) received via telephone must be immediately destroyed with a black extra fine point marker with the exception of the last 4 digits of the card holders account number before filing.

1.4 Credit card payments or philanthropic gifts received in person must not be processed without proper cardholder picture identification presented.

1.5 Upon recording credit card philanthropic donations received by mail in the Office of Development, all credit card information will be destroyed.

1.6 Credit card data submitted via e-mail should never be accepted.

2. APPLICABILITY

2.1 This UAP applies to all credit card collections as defined by PCI-DSS regulations. The intended audience for this UAP includes, but is not limited to, any authorized department/merchant collecting PCI cardholder data information.

3. PROCEDURES AND RESPONSIBILITIES FOR FOLLOWING PCI-DSS CONTROL OBJECTIVES

3.1 Secure Network Building and Maintenance

3.1.1 Computer or computer network security and internal controls should include, but are not limited to:

3.1.1.1 Installation and maintenance of a firewall configuration to protect cardholder data;

3.1.1.2 Prohibited use of vendor-supplied defaults for system passwords and other security parameters; and,

3.1.1.3 Restriction of computer and physical access of cardholder data to authorized personnel.

3.2 Cardholder Data Protection

3.2.1 To accept credit, debit, gift, or other payment cards, departments must obtain prior written permission from the Office of Treasury Services.

3.2.2 Authorized departments are responsible for protecting stored cardholder data in accordance with PCI-DSS standards and maintaining internal credit card processing procedures.

3.2.2.1 Internal procedures must be approved by the Office of Treasury Services and the Information Security Officer (ISO).

3.2.3 Authorized departments will encrypt any transmissions of cardholder data across open, public networks.

3.3 **Vulnerability Management Program Maintenance**

3.3.1 Authorized departments will ensure regular updates of all anti-virus software on all systems commonly affected by malware.

3.3.2 Authorized departments will develop and maintain secure systems and applications.

3.3.2.1 Prior to the purchase and installation of any applications, approval should be obtained from the Office of Treasury Services, the ISO, and the Center for Information Technology Excellence (C.I.T.E.).

3.4. **Strong Access Control Implementation Measures**

3.4.1 Authorized departments will restrict access to cardholder data on a business need-to-know basis.

3.4.2 All users must use a unique ID to access PCI devices and/or systems.

3.4.3 Authorized departments will restrict physical access to cardholder data.

3.5 **Regular Network Monitoring and Testing**

3.5.1 C.I.T.E. will be responsible for monitoring and maintaining the PCI Network.

3.5.2 Authorized third party security vendors will conduct internal, external and segment penetration tests in accordance with PCI standards.

3.6 **Annual Certification**

3.6.1 The Office of Financial Management Services will oversee the annual PCI validation and ensure that it is performed by each authorized department. All departments' validation reports will be provided to the Office of Financial Management Services and the ISO. The reports will be maintained in accordance with the Record's Retention Schedule.

3.7 **Training**

3.7.1 All employees who have access to credit card data, including ITS staff who support systems that process credit card data, are required to complete the TrainTraq course# 11013 titled Payment Card Industry Data Security Standards: PCI – DSS for Merchants annually.

Related Statutes, Policies, Regulations and Rules

System Regulation 21.01.02 Receipt, Custody and Deposit of Revenues

Contact Office

Treasury Services	936- 261-1941
Center for Information Technology Excellence (C.I.T.E.)	936-261-9350