**PRAIRIE VIEW A&M UNIVERSITY**
**UNIVERSITY ADMINISTRATIVE PROCEDURE**

# 21.01.02.P0.03 Credit Card Collections Security

Approved November 6, 2013
Next Scheduled Review: November 2018

## UAP Purpose

Prairie View A&M University (PVAMU) accepts credit cards as payment for goods and services provided. Authorized departments may accept credit card payments in person, or over the telephone. PVAMU's Cashiers Department is the only authorized department that may accept credit card payments by mail. The purpose of this University Administrative Procedure (UAP) is to ensure compliance with Section 2.5 of System Regulation 21.01.02 Receipt, Custody and Deposit of Revenues.

## Definitions

**Confidential Information** - information that is exempt from disclosure requirements under the provisions of applicable state or federal law, e.g., The Texas Public Information Act.

**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 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 In order to accept credit and/or debit cards as a method of payment, 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.

1.2 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.

1.3 Credit card payments received in person must not be processed without proper card holder picture identification presented.

1.4 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 card holder 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 Office of Information Technology Services (ITS).

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 Authorized departments will assign a unique ID to each person with computer access.

3.4.3 Authorized departments will restrict physical access to cardholder data.

3.5 **Regular Network Monitoring and Testing**

3.5.1 Authorized departments will track and monitor all access to network resources and cardholder data.

3.5.2 Authorized third party security vendors will test security systems and processes quarterly.

3.6 **Information Security Policy Maintenance**

3.6.1 The ISO will review and update all University Rules and UAPs relating to information security on a biennial basis.

3.7 **Annual Certification**

3.7.1 The Office of Treasury 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 Services and the ISO. The reports will be maintained in accordance with the Record's Retention Schedule.

3.8 **Training**

3.8.1 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 titled Payment Card Industry Data Security Standards annually.

**Related Statutes, Policies, Regulations and Rules**

System Regulation 21.01.02 Receipt, Custody and Deposit of Revenues

**Contact Office**

| | |
|---|---|
| Office of Treasury Services | 936- 261-1890 |
| Office of Information Resources Management | 936-261-9350 |