21.01.99.E0.01 Credit Card Information Receipt, Custody, & Security Procedures

Approved October 7, 2005
Revised July 10, 2007
Revised October 21, 2008
Revised July 14, 2011
Revised June 12, 2020
Revised July 30, 2025
Next Scheduled Review: July 30, 2030

Standard Administrative Procedure Summary

The Texas A&M Engineering Experiment Station (TEES) requires the proper handling and security of eCommerce and credit card information throughout the payment process as provided by this Standard Administrative Procedure (SAP). This SAP provides direction for processing and protecting credit card information.

Procedures and Responsibilities

1. GENERAL

   The purpose of this SAP is to outline the required Procedures for processing credit card payments and to define the necessary controls to protect sensitive payment information throughout the transaction lifecycle.

2. ON-LINE PROCESSING

   All online registrations and credit card transactions must be processed through Fiscal Office approved platforms and denominated in U.S. dollars (USD). In cases where a registrant pays using a foreign currency, the amount paid must be equivalent to the stated USD amount at the time of the transaction, based on the applicable exchange rate.

3. GENERAL PROCESSING CONTROLS

   3.1 Protection of Stored Data

      3.1.1 Sensitive cardholder data, including the primary account number (PAN), magnetic stripe data, and expiration date must be properly disposed of when no longer needed. (See section 3.2.5 below)

3.1.2 The full contents of any track from the magnetic stripe shall not be stored in agency and/or department databases, log files, or point-of-sale products.

3.1.3 The card-validation code or value (three- or four-digit number printed on the front or back of a payment card) shall not be stored in agency and/or department databases, log files, or point-of-sale products.

3.1.4 The personal identification number (PIN) or the encrypted PIN block shall not be stored in any form.

3.1.5 All but the last four digits of the account number must be masked when displaying cardholder data.

3.1.6 If storage of account number is absolutely necessary, the data must be secured in accordance with or exceeding the requirements set forth by the Payment Card Data Security Standard (PCI DSS).

3.2 Access to Cardholder Data

3.2.1 Access to all cardholder data shall be restricted to employees with a legitimate business need-to-know. Employees authorized to access such cardholder data shall complete cardholder data security training upon hire and on an annual basis thereafter.

3.2.2 Procedures regarding multiple security controls shall be developed and be in place to prevent unauthorized individuals from gaining access to the facilities and equipment, such as servers, workstations, laptops, and hard drives and media, containing cardholder data. Controls such as using cameras for sensitive areas, using badges that expire, physically escorting visitors in sensitive areas, or using visitor logs to retain an audit trail can be used. The procedures shall be developed under the responsibility of the department head or assigned designee.

3.2.3 Cardholder data received on paper or electronic media must be securely deleted or destroyed before disposal, using methods such as shredding or data sanitization, once the data is no longer required for business or legal purposes.

3.2.4 Procedures must be established for the secure handling, distribution, and disposal of backup media and other electronic storage containing cardholder data. Controls may include

confidential labeling, secure transport via trusted couriers, and disposal techniques that ensure data cannot be recovered. These procedures must be developed under the authority of the department head or their designee.

3.2.5 Cardholder data stored on paper or electronic media must be destroyed or deleted, using methods such as shredding or sanitization, once it is no longer needed.

3.2.6 Unencrypted primary account numbers (PANs) shall not be transmitted via end-user messaging technologies.

3.3 Information Security Policies

3.3.1 Engineering Human Resources must perform a background check on every employee given access to sensitive cardholder data. Any criminal history revealed in this check could result in an employee being denied access.

3.3.2 All third parties with access to sensitive cardholder data or systems involved in the transaction process must be contractually required to comply with all applicable card association security standards, including the Payment Card Industry Data Security Standards (PCI DSS), and accept responsibility for the protection of cardholder data to the extent that is under their control.

3.3.3 Departments are financially responsible for any penalties, fines, or losses resulting from non-compliance with PCI DSS standards or from security breaches originating from their systems or staff.

4. RESPONSIBILITIES

The Agency Director delegates responsibility to all department heads or their assigned designee to ensure that the above procedures are implemented and enforced in their respective departments.

Related Statutes, Policies, or Requirements

Payment Card Industry (PCI) Data Security Standards
University Accounting Services Card Acceptance and Security

Contact Office

TEES Fiscal Office
(979) 458-7430