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
Next Scheduled Review: June 12, 2025

Standard Administrative Procedure Statement

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).

Reason for Standard Administrative Procedure

This SAP provides direction for processing and protecting credit card information.

Procedures and Responsibilities

1. GENERAL

   The purpose of this SAP is to identify the procedures that must be followed when processing credit card information and to identify the necessary controls to protect the information being processed.

2. ON-LINE PROCESSING

   All on-line registrations and sales using credit card verification and processing shall be handled through the channels approved by the Fiscal Office (at this time, TouchNet or Payflow), and denominated in U.S. currency only.

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 division 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 division 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 agency and/or division databases, log files, or point-of-sale products.

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

3.1.6 If absolutely necessary to store, account numbers (kept in databases, logs, files, or backup media) must meet or exceed the standards set forth in the Payment Card Industry Data Security Standard.

3.2 Access to Cardholder Data

3.2.1 Access to all cardholder data shall be restricted to employees with a legitimate need-to-know. Employees with access to cardholder data shall complete online training for cardholder data security upon hire and annually.

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 division head or assigned designee.

3.2.3 Cardholder data printed on paper or received by fax must either be physically destroyed via shredding or sanitization or protected against unauthorized access by maintaining it in a locked area.

3.2.4 Procedures shall be developed and be in place to handle secure distribution and disposal of backup and other electronic media containing sensitive cardholder data. They should include controls such as labeling media as confidential, sending media via secure couriers, or using secure disposal methods that will provide the assurance of non-recoverability. The procedures shall be developed under the responsibility of the division head or assigned designee.

3.2.5 Cardholder data must be destroyed or deleted before the paper or electronic media is physically disposed of, using methods such as shredding or sanitization, once it is no longer needed.

3.2.6 Unencrypted primary account numbers (PANs) shall not be sent 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 obligated to comply with card association security standards, and to take responsibility for security of cardholder data to the extent under their control. See Payment Card Industry (PCI) Data Security Standards.

4. RESPONSIBILITIES

The Agency Director delegates responsibility to all division heads or their assigned designee to ensure that the above procedures are implemented in their respective divisions.

Related Statutes, Policies, or Requirements

Payment Card Industry (PCI) Data Security Standards
TAMU SAP 21.01.02.M0.01, Online Payments
TAMU SAP 21.01.02.M0.03, Credit Card Collections

Contact Office

TEES Fiscal Office
(979) 458-7430