# SAP 21.01.02.T0.01     Credit Card Information Receipt, Custody, and Security Procedures

| | |
|---|---|
| Approved: | August 1, 2008 |
| Revised: | July 6, 2015 |
| Reviewed: | March 3, 2023 |
| Next Scheduled Review: | March 3, 2028 |

## Procedure Summary

The purpose of this procedure is to identify the process that must be followed when processing credit card information and to identify the necessary controls to protect the information being processed at Tarleton State University (Tarleton or university). The Texas A&M University System Regulation 21.01.02, *Receipt, Custody and Deposit of Revenues* requires its system members to adhere to industry security standards to protect cardholder data and complete the *Payment Card Industry Data Security* training.

## Definitions

Cardholder Information Security Program (CISP):  Visa's Cardholder Information Security Program (CISP) is designed to ensure that all merchants that store, process, or transmit Visa cardholder data, protect it properly.  To achieve CISP compliance, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard.

PCI:  The PCI Standard is the result of collaboration between the four major credit card brands to develop a single approach to safeguarding sensitive data.  The PCI standard defines a series of best practices for handling, transmitting and storing sensitive data.

Cardholder Data:  Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, Card Validation Code CVC 2 (MasterCard), Card Verification Value CVV2 (VISA), Card member ID (Discover) or CID – Card Identification Number (American Express) (e.g. three- or four-digit value printed on the front or back of a payment card.)

System Administrator / Data Custodian:  An individual who performs network/system administration duties and/or technical support of network/systems that are accessed by other people, systems, or services.  Only full-time and permanent part-time employees of the university and/or third party vendors approved by Information Technology Services and/or the Office of Business Services may function as system/network administrators and/or data custodians.

# Procedures and Responsibilities

## 1. ON-LINE PROCESSING

All on-line transactions using credit card verification and processing shall be handled through a Payment Card Industry Data Security Standard (PCI DSS) approved vendor. Departments must consult the Office of Business Services and Information Technology Services prior to purchasing software that collects and transmits credit card information.

## 2. GENERAL PROCESSING CONTROLS

### 2.1 Protection of Stored Data

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

2.1.2 The card-validation code (three digit value printed on the signature panel of a card) shall not be stored in university and/or division/departmental databases, log files, or point-of-sale products.

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

2.1.4 Account numbers must be stored securely in databases, logs, files, and backup media (for example, by means of encryption or truncation).

2.1.5 Under no circumstances will it be permissible to obtain or transmit credit card data by e-mail, fax or other network device that does not meet security requirements.

### 2.2 Access to Cardholder Data

2.2.1 Access to all cardholder data shall be restricted to employees with a legitimate need-to-know.

2.2.2 Security controls through the university's identification card system are in place to prevent unauthorized individuals from gaining access to facilities and equipment.

2.2.3 Cardholder data printed on paper must be physically protected against unauthorized access such as by maintaining it in a locked area or shredding.

2.2.4 Written procedures shall be developed and be implemented to handle secure distribution and disposal of backup and other electronic media containing sensitive cardholder data. These 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.

    2.2.5    Cardholder data must be destroyed or deleted before the paper or electronic media is physically disposed of, using methods such as shredding or sanitization.

### 2.3  Information Security Policies

    2.3.1    A criminal background check is performed on each employee with access to sensitive cardholder data.

    2.3.2    All third parties with access to sensitive cardholder data must be contractually obligated to comply with PCI DSS card association security standards.

    2.3.3    Departments must comply with the PCI Data Security Standard Payment Card Industry Data Security Standard. https://www.pcisecuritystandards.org/

    2.3.4    Exceptions to this policy may be granted only after a written request from the unit has been reviewed and approved by the university Office of Business Services.

## 3.  RESPONSIBILITIES

Each department head/account manager is charged with the responsibility to ensure that the above procedures are implemented in their respective areas.

## Related Statutes, Policies, or Requirements

System Policy *21.01, Financial Policies, Systems and Procedures*

System Regulation *21.01.02, Receipt, Custody, and Deposit of Revenues*

Tarleton Information Technology Standard Operating Procedure – Security of Electronic Resources

## Contact Offices

Office of Business Services
254.968.9107

Office of Information Technology/Chief Information Officer
254.968.9395