



TEXAS SOUTHERN UNIVERSITY
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: Administration & Finance
AREA: Treasury

Policy 03.05.01

SUBJECT: Accepting and Handling Credit and Debit Card Payments

I. PURPOSE AND SCOPE

- A. The purpose of the Accepting and Handling Credit Card Payments Policy is to establish Texas Southern University's standard for the proper handling of credit and debit card transactions processed through automated systems and/or manual procedures.
- B. The policy applies to all employees, departments, organizations, units and functions of Texas Southern University who accepts, capture, store, transmit and/or process credit or debit card payments received for the purchase of University products and services, for contributions, etc.
- C. The policy also applies to all personnel who support any University effort to accept, capture, store, transmit and/or process credit card information, such as a technical support staff member whose role gives him or her access to computer hardware and software holding credit card information, individuals tasked with shredding credit card information, etc.
- D. The policy and procedures described were created to ensure that credit and debit card information is handled and disposed of in a manner that satisfies the University's obligation to protect such information to the level that meets or exceeds that required by the Payment Card Industry.
- E. To reduce their losses due to credit card fraud, five members of the payment card industry (Visa, Master Card, American Express, Discover and JCB) developed security standards for any organization that accepts, captures, stores, transmits and/or processes credit card information either manually or through an automated system. This set of standards is referred to as the Payment Card Industry's Data Security Standard, or "PCI-DSS."
- F. PCI-DSS is enforced through the contracts that Texas Southern University, as a merchant account holder, has with our merchant banks, i.e., the financial institutions that serve as a liaison between TSU merchants and the payment card companies.

Accepting and Handling Credit and Debit Card Payments - MAPP Policy 03.05.01

G. Since any unauthorized exposure of credit or debit card information could subject TSU to reputational damage and significant penalties, failure to comply with the policy contained within this document will be considered a serious matter. Penalties for non-compliance can include increased credit card transaction fees, a suspension of credit card privileges, and fines in cases where an account is compromised. Therefore, failure by University personnel to comply with this policy may result in the revocation of the ability to process credit and debit card transactions and/or could lead to disciplinary action including termination of employment.

II. PRINCIPLES

A. Texas Southern University is committed to complying fully with the expectations specified by the Payment Card Industry in its Data Security Standard (PCI -DSS). Compliance by TSU requires that:

1. PCI-DSS compliance is mandatory for any department that accepts, captures, stores, transmits and/or processes credit or debit card information.
2. Only authorized and properly trained individuals may accept and/or access credit or debit card information.
3. Credit and Debit Card Payments May Be Accepted Only using Methods Approved by the Office of Treasury and Office of Information Technology.
4. Each person who has access to credit or debit card information is responsible for protecting the information.
5. Credit and debit card information must be destroyed as soon as it is no longer needed.
6. Departments must maintain appropriate checks and balances in the handling of credit and debit card information.
7. Each department that handles credit and/or debit card information must have detailed documented desk procedures for complying with this policy and PCI -DSS.
8. Suspected theft of credit or debit card information must be reported immediately to the following TSU departments: (1) Department of Public Safety, (2) Office of Treasury, and (3) Office of Internal Audit.

B. Failure to comply with these principles, as implemented in this Policy, may result in the revocation of the ability to process credit and debit card transactions and/or could lead to disciplinary action including termination of employment.

III. PROCEDURES TO IMPLEMENT THE UNIVERSITY'S CREDIT AND DEBIT CARD PRINCIPLES

A. PCI-DSS compliance is mandatory for any department that accepts, captures, stores, transmits and/or processes credit or debit card information.

1. Any University department that accepts credit or debit cards for donations and/or as payment for goods and services must comply with PCI-DSS to ensure the security of cardholder information. Compliance with the requirements of this policy (as updated or amended) satisfies the elements of compliance with PCI-DSS.

B. Only authorized and properly trained individuals may accept and/or access credit or debit card information. Prior to processing any credit and/or debit card payments, all personnel must satisfactorily complete one of the trainings held by the Office of Treasury.

1. No individual is authorized to accept, access or support systems housing credit or debit card information until the following requirements are satisfied:
 - a. The individual must be authorized by the Office of Treasury, Office of Information Technology and his/her direct Supervisor.
 - b. Individuals who are new to the role must be trained prior to taking on their credit or debit card handling duties. The individual must be trained in the proper handling of credit and debit card information. Individuals whose credit or debit card handling responsibilities preceded the implementation of this policy should receive training before resumption of credit or debit card processing. The content of the training program must be reviewed and approved by the Office of Treasury and Office of Information Technology to ensure that University objectives are met.
 - c. The individual must acknowledge his or her understanding of this policy and must confirm his or her commitment to comply with all related University policies and procedures before he or she assumes credit and/or debit card handling duties and on an annual basis thereafter. This requirement may be satisfied by the individual physically signing the "Credit and bit Card Security and Ethics Agreement" in Appendix A of this document and submitting it in one of three ways:
 - i. Physical submission to the Office of Treasury,
 - ii. Via email, or
 - iii. Via electronic signature that is signed by his or her University ID and password and that mirrors the terms of the "Credit and Debit Card Security and Ethics Agreement."

Accepting and Handling Credit and Debit Card Payments - MAPP Policy 03.05.01

2. The Office of Treasury is responsible for maintaining a record of all signed agreements for their areas.

C. Credit and Debit Card Payments May Be Accepted Only using Methods Approved by the Office of Treasury and Office of Information Technology

1. Credit and debit card payments may only be accepted in the following manners:
 - a. In person
 - b. Via telephone
 - c. Via FAX
 - d. Via physical mail (not email)
 - e. Through a PCI-DSS-compliant automated system that is entirely hosted by a PCI-DSS-compliant third party organization approved by the Office of Treasury and Office of Information Technology.
 - f. Through an automated system that is hosted in the University data center that does not accept, capture, store, transmit or process credit or debit card information itself, but refers the customer to a PCI-DSS-compliant system hosted by a third party organization, approved by the Office of Treasury and Office of Information Technology, which handles credit and debit card payments on our behalf. The third party system must not return credit card numbers, expiration dates, or verification values to the University-based system

Note – In cases where the use of a PCI-DSS-compliant third party for the capture, storage, transmission and/or processing of credit card payments is not feasible, an exception may be requested for an automated system that handles credit or debit card information on a University-based system, but only if the system can satisfy all PCI-DSS requirements. Exceptions require written approval by the Office of Treasury and Office of Information Technology.

2. Any department that uses a third party organization to accept, store and/or process credit or debit card information on its behalf, except for any third-party organization that already has a campus-wide agreement with the Office of Treasury, must receive from the vendor, on an annual basis, and keep on file documentation indicating that the vendor's system and procedures have been found to be in compliance with PCI-DSS by a firm that has been authorized by the Payment Card Industry to make such an assessment. A

Accepting and Handling Credit and Debit Card Payments - MAPP Policy 03.05.01

copy of this documentation should be submitted to the Office of Treasury and Office of Information Technology.

D. Each person who has access to credit or debit card information is responsible for protecting the information.

1. Individuals who have access to credit or debit card information are responsible for properly safeguarding the data and must comply with all requirements of the Office of Information Technology Policy to protect the integrity and privacy of such information. This policy can be found on the TSU website.
2. The following pieces of information are considered “confidential” within the meaning of the Personally Identifiable Information (PII) Policy and must be protected appropriately from initial capture through destruction regardless the storage mechanisms used (e.g., on computers, on electronic, magnetic or optical media, on paper, etc.):
 - a. Credit or debit card number
 - b. Credit or debit card expiration date
 - c. Cardholder Verification Value (CVV2) – the 3- or 4-digit code number generally located on the back of the credit or debit card.
 - d. Personal identification number (PIN)
 - e. Cardholder’s name, address and/or phone number when used in conjunction with the above fields

Note – The use of Social Security Numbers in conjunction with credit or debit card information is strictly prohibited. The use of Social Security Numbers is highly restricted by the University’s Personally Identifiable Information (PII) Policy. As such, Social Security Numbers never should be used without the approval of the appropriate Information Guardian.

3. Neither the three -or- four-digit credit or debit card validation codes (CVV2) nor Personal Identification Numbers (PIN) may ever be stored in conjunction with credit or debit card information in any form.
4. Point-of-sale devices must be configured to print only the last four characters of the credit or debit card number on both the customer and the merchant receipts, and on any reports that may be produced by the device.
5. Physical documents, such as customer receipts, merchant duplicate receipts, reports, etc., that contain credit or debit card information should be retained only as long as there is a valid business reason to do so, and no longer than 90 days. While the documents are retained, they must be stored in locked cabinets in secured areas with access restricted to authorized individuals on a need-to-know basis. Keys that allow access to such containers must be

Accepting and Handling Credit and Debit Card Payments - MAPP Policy 03.05.01

immediately collected from any individual who leaves the University or whose responsibilities no longer require him or her to access such documents. When combination locks are used, the combination must be changed when an individual who knows the combination leaves the University or no longer requires access to perform assigned work.

6. For any physical documents that contain credit or debit card information, it is strongly recommended that all but the last four digits of the credit or debit card number be physically cut out of the document. Overwriting the credit or debit card number with a marker is not acceptable since the number can still be viewed in certain circumstances.
7. No lists should be maintained that include entire credit or debit card numbers without the approval of the Office of Treasury and Office of Information Technology.
8. Credit or debit card information may be shared only with individuals who have been authorized to access such data by the Office of Treasury and his/her direct Supervisor.

E. Credit and debit card information must be destroyed as soon as it is no longer necessary.

1. All credit and debit card information must be destroyed as soon as it is no longer needed, and may not be retained for more than 90 days after the transaction is processed.
2. All physical documents that are no longer necessary must be shredded using an appropriate office cross-shredder device, which should be approved by the Office of Treasury.
3. In cases where an Academic or Administrative Department Supervisor is granted an exception that allows an on-campus system to accept, capture, store, transmit and/or process credit card information, the manager must ensure that computer-based data that is no longer necessary is destroyed in the manner described in Appendix B of this document.

F. Departments must maintain appropriate checks and balances in the handling of credit and debit card information.

1. Departments handling credit or debit card transactions must segregate, to the extent possible, all duties related to data processing and storage of credit and/or debit card information. A system of checks and balances should be put in place in which tasks are performed by different individuals in order to assure adequate controls. For example, the same person should not process credit or debit card transactions/refunds and perform the monthly credit and debit card reconciliation. Where staffing permits, it is strongly recommended

Accepting and Handling Credit and Debit Card Payments - MAPP Policy 03.05.01

that the responsibility for processing transactions and refunds be segregated as well.

2. The Department Manager or his/her designee should not process credit and debit card transactions if he/she has responsibility for verifying the original supporting detail records. He or she will verify that the original supporting detail records agree with deposits on the General Ledger Journal. Terminal or web-based reports must not be the only supporting detail record. Segregation of duties should be maintained between the processing and reconciliation functions.
3. The Department Supervisor or his/her designee is responsible for ensuring that Human Resources is aware of any job description changes that are made in support of maintaining the segregation of duties.

G. Each department that handles credit and/or debit card information must have documented procedures for complying with this policy and PCI-DSS. These procedures should be reviewed and approved by both Departmental Management and the Office of Treasury.

1. Each department that handles credit and debit card information must have written procedures tailored to its specific organization that are consistent with this policy and PCI-DSS. Departmental procedures should be reviewed, signed and dated by the Department Supervisor on an annual basis indicating compliance with the University's Credit and Debit Card Policy. These procedures must also be submitted to and approved by their Dean or Vice President, the Office of Treasury, and the Office of Information Technology.
2. These departmental procedures will include, but are not limited to, the following:
 - a. Segregation of duties
 - b. Deposits
 - c. Reconciliation procedures
 - d. Physical security
 - e. Disposal
 - f. Cash register procedures (if applicable)
3. Departmental procedures and controls should be reviewed by the Office of Treasury and the Office of Information Technology.

Note - For assistance in developing departmental procedure contact the Office of Treasury.

H. Suspected theft of credit or debit card information must be reported immediately to the following TSU departments: (1) Department of Public Safety, (2) Office of Treasury, and (3) Office of Internal Audit.

Accepting and Handling Credit and Debit Card Payments - MAPP Policy 03.05.01

1. Any individual who suspects the loss or theft of any materials containing cardholder data, that person must immediately notify the University IT Security Officer and Public Safety.

IV. EXCEPTIONS TO REQUIRED PROCEDURES

- A. It is understood that a unique situation within an individual department may require a permanent or short-term exception to one or more of the above procedures. Such an exception must satisfy ALL of the following conditions:
 1. It must comply with all applicable PCI-DSS requirements.
 2. It must be approved by the Associate Vice President for Treasury and Budget and the Office of Information Technology.
 3. In the case of a permanent exception, it must be included in a department's written procedures.
 4. In the case of a short-term exception, it must be restricted to specific dates or events.

V. APPENDIX A-CREDIT AND DEBIT CARD SECURITY AND ETHICS CERTIFICATION FORM

- A. Appendix A is a statement of understanding and intent to comply with the University Policy and Procedures for accepting and handling credit and debit card payments. Anyone who has access to credit or debit card information must sign the form and submit it to his or her department supervisor on an annual basis.

Accepting and Handling Credit and Debit Card Payments - MAPP Policy 03.05.01

**APPENDIX A –
CREDIT AND DEBIT CARD SECURITY AND ETHICS CERTIFICATION FORM**

**Texas Southern University
Credit and Debit Card Security and Ethics Agreement**

Applicable to: Any individual who accepts, captures, stores, transmits and/or processes credit or debit card information

Effective Date: _____

Many University departments accept credit/debit card information, such as credit/debit card numbers, expiration dates and card verification codes, from donors, purchasers of University publications and services, etc.

I recognize that this information is sensitive and valuable and that the University is legally obligated to protect this information against its unauthorized use or disclosure in the manner defined by the Payment Card Industry's Data Security Standard, and should such information be disclosed to an unauthorized individual, the University could be subject to fines, increased credit and debit card transaction fees and/or the suspension of our credit and debit card privileges.

As an individual whose role includes the acceptance, capture, storage, transmission and/or processing of credit and/or debit card information, I agree with the following statements:

I have read the requirements stated in the University's Policy and Procedures Accepting and Handling Credit and Debit Card Information ("Policy").

I understand that I may only accept credit and debit card payments using methods approved by the Office of Treasury and Office of Information Technology.

I understand that as an individual who has access to credit and debit card information, I am responsible for protecting the information in the manner specified within the Policy. Further, I understand that I am also responsible for effectively protecting the credentials (IDs and passwords) and the computers that I may use to process credit or debit card transactions.

I understand that I must destroy credit and debit card information as soon as it is no longer needed using methods prescribed by Policy.

I understand that in cases where I suspect that a breach of credit or debit card information has occurred, I must immediately report the breach to the University IT Security Officer, Public Safety and the Office of Treasury.

If I manage an area that handles credit card information, I understand that I must have appropriate checks and balances in the handling of credit and debit card information, and that I am responsible for having documented procedures in place for complying with Policy.

I agree to comply with the Policy and its documented procedure, and understand that failure to comply with the above requirements may subject me to a loss of credit card handling privileges and other disciplinary measures. For employees, non-compliance could result in termination of employment.

Signature: _____

Date: _____

Print Name: _____

VI. APPENDIX B – PROCEDURES FOR IN-HOUSE APPLICATIONS SYSTEMS THAT HAVE BEEN GRANTED AN EXCEPTION TO HANDLE CREDIT OR DEBIT CARD TRANSACTIONS

A. In cases where an academic or administrative department is granted an exception that allows an on-campus system to accept, capture, store, transmit and/or process credit card information, the department supervisor must ensure that the design of the application and all procedures associated with the application comply with the following additional requirements:

1. System and network controls, approved by the Office of Information Technology, must be implemented to restrict access to authorized individuals and only on a need-to-know basis. The Department Supervisor is responsible for ensuring that access is immediately revoked for any individual who leaves the University or whose responsibilities no longer require him or her to access such information.
2. The three or four-digit credit or debit card validation code (CVV2) must never be captured in any form.
3. Credit or debit card information that is transmitted across a network must be encrypted using a method approved by the Office of Information Technology.
4. No reports should be maintained that list entire credit or debit card numbers without the approval of the Office of Treasury.
5. It is strongly recommended that only the last four characters of the credit or debit card number may be retained in a database or computer file. Retaining the entire credit or debit card number in such circumstances requires the approval of the Office of Information Technology and Office of Treasury. If such approval is granted, the following requirements apply:
 - a. Credit or debit card information held on Texas Southern University computer hard drives or on removable storage media (diskettes, CDs, DVDs, USB storage devices, etc.) must be encrypted using a method approved by the Office of Information Technology.
 - b. Any file containing credit or debit card information stored on electronic or magnetic media (computer hard drives, diskettes, USB storage devices, etc.) that is no longer needed must be electronically “shredded” or wiped using a commercial tool and method approved by the Office of Information Technology. Merely deleting the files is not sufficient, as common computer operating systems typically leave deleted information on such media intact.

- c. No computer that has hosted a software application that accepts, captures, stores, transmits or processes credit or debit card information may be repurposed, donated, sold or sent to surplus until all of the hard drives on that system have been removed from the system and physically destroyed using a method approved by the Office of Information Technology.
- d. The Department Supervisor is responsible for establishing procedures confirming that the required hard drive removal has taken place, and that all removed hard drives are protected against theft and unauthorized access through their destruction.
- e. No computer that has been used to manually enter credit card information received via phone, FAX, mail, etc. into a credit card system hosted by a bank or credit card service organization may be repurposed, donated, sold or sent to surplus until all of the hard drives on that system have either been electronically wiped using a commercial disk wiping tool, or have been removed from the system and physically destroyed. In both cases, the methods used must be approved by the Office of Information Technology. The Department Supervisor is responsible for establishing procedures confirming that the required hard drive wiping or removal has taken place, and that all removed hard drives are protected against theft and unauthorized access through their destruction.
- f. Any piece of non-magnetic/non-electronic media (e.g., CDs, DVDs) that has been used to store credit or debit card information must be cross-cut shredded before being discarded using a shredding device approved by the Office of Information Technology.

VII. APPENDIX C – UNIVERSITY BUSINESS/ACCOUNTING PROCEDURES REGARDING CREDIT AND DEBIT CARDS

A. General Procedures

- 1. Any University department that wishes to accept credit or debit cards for payment must first submit a written request to the Office of Treasury for approval before merchant account numbers are issued.
- 2. Any or all of the following credit or debit cards may be accepted for payment:
 - a. American Express
 - b. Discover
 - c. MasterCard
 - d. Visa

B. Transaction Handling

1. All credit and debit card payments received and/or processed by departments must be supported by appropriate support documentation as listed below:
 - a. All in-person payments must be supported by pre-numbered receipts, which must be in consecutive order. Voided receipts must also be maintained.
 - b. All payments received through the mail, facsimile, or via telephone must be supported by lists prepared by the mail opener or telephone operator. List entries must not include the entire credit or debit card number. At most, they should include the last four digits of the number.

C. Reconciliation

1. All credit or debit card terminals and web applications must be closed out and reconciled on a daily basis.
2. In addition to normal reconciliation functions, the reconciler will ensure that all transaction receipts, both processed and voided, are accounted for.
3. The Department Supervisor or his/her designee should perform, sign and date reconciliations on a regular basis, but in any case not less than monthly. Reconciliations must compare all credit and debit card payments processed using original supporting documentation, with the monthly General Ledger Journal to assure that all deposits are properly recorded. Reconciliations must be maintained by the department and are subject to review.
4. University departments are responsible to ensure that their organization numbers have been credited by the merchant services processor or bank (through the Office of Treasury). The departments must reconcile transactions listed on their Daily Settlement Reports against their Financial Statement Reports ((using credit and debit card reconciliation methods approved by the Office of Treasury and Office of Information Technology) listed on their respective merchant Websites (TouchNet, Raiser's Edge, etc.) to assure that they have received credit for all processed transactions. Reconciliations must be performed at least monthly and must be signed and dated.

D. Chargebacks

1. Chargebacks are credit or debit card transactions that are returned by the Depository Bank/credit card processor or are disputed by the customer and can result in additional service fees or loss of revenue to the University.
2. A consumer has 90 days to dispute payment. When a dispute takes place, the bank or processor will contact the Department to obtain copies of the receipts or other documentation that substantiates the charge. The Department has a limited

Accepting and Handling Credit and Debit Card Payments - MAPP Policy 03.05.01

amount of time (usually 10 days) to respond, and the due date will be listed on the dispute document accordingly.

3. If the department fails to respond by the deadline or cannot provide documentation, the bank will reverse the payment and "charge back" the Department, which will appear on the Financial Statement as a debit transaction.
4. Departments are responsible for ensuring that any disputes, also called "chargebacks", are handled in a timely manner. Individuals responsible for addressing disputes can submit the corresponding dispute documents to the Student Accounting Department to be researched and resolved or can check the web-based "chargeback" system (i.e. TouchNet, Raiser's Edge, etc.) on a daily basis to identify and respond to consumer disputes within specified time limits (maximum 10-15 days). Failure to respond in the restricted time limits may result in funds being debited automatically from the respective cost centers.
5. Departments are responsible for monitoring disputed charges daily and collecting funds owed after a chargeback occurs if the goods or services were provided to the consumer.

E. Policy and Procedural Changes

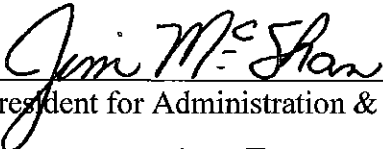
The Office of Treasury will provide departments with updated information whenever a merchant services processor or card association announces significant policy or procedural changes. Please note that these announcements are also made on monthly Merchant Account statements.

VIII. REVIEW AND RESPONSIBILITIES

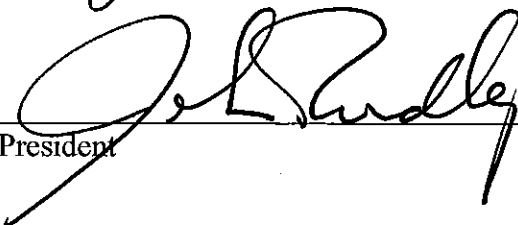
Responsible Party: Associate Vice President, Office of Treasury

Review: Every three years, on or before September 1

IX. APPROVAL



Vice President for Administration & Finance



President

Effective Date: August, 2013