

UTAH STATE UNIVERSITY

POLICIES AND PROCEDURES MANUAL

Title: Credit Card Handling and Acceptance Policy
Policy Number: C3875
Effective Date: November 8, 2006
Issuing Authority: Office of VP Business and Finance

Scope of Policy

This policy outlines the University's rules and procedures for the proper handling of credit and debit card transactions, including system requirements and the responsibilities of University employees that process credit card transactions or maintain card holder information. These rules and procedures are intended to assure timely handling of credit cards transactions and aid in the safeguarding and proper disposal of credit card information. Failure to follow this policy will result in the loss of credit card processing privileges.

Definitions

1. Credit card payments can be accepted either via the:
 - a. Secure website (e-mail is not acceptable)
 - b. Over the counter (In-Person)
 - c. Telephone
 - d. Mail
2. The University may accept any or all of the following credit cards at various locations:
 - a. Discover
 - b. MasterCard
 - c. Visa
 - d. American Express
3. Compliance requirements within this policy are derived from the following statutes, regulations or credit card association rules:
 - a. Federal Gramm-Leach-Bliley Act (GLBA)
 - b. Payment Card Industry Data Security Standards (PCI DSS):
 - i. American Express Data Security Program (DSS)
 - ii. Discover Data Security (DISC)
 - iii. MasterCard Site Data Protection (DSS)
 - iv. Visa Cardholder Information Security Program (CISP)
 - v. Payment Application Data Security System (PA DSS)
 - c. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
 - d. Federal Educational Rights and Privacy Act (FERPA)
 - e. Red Flag law (Red Flag)

4. Personal Identifiable Information (PII) is information that can be used by others to steal one's identity. This includes:
- a. Cardholder's name
 - b. Credit Card number
 - c. Cardholder Verification Value (CVV2) – 3 or 4-digit code number generally located on the back of the credit card.
 - d. Address

Policy

1. Any University department that wishes to accept credit cards as payment for goods and/or services must first submit a written request to Directory of Treasury Services for approval before credit card merchant numbers are issued. This request will include a copy of the department's procedures as outlined in Procedures 2A, section 2 below. A review of processes and system needs will be conducted to prevent duplication of systems on campus.
2. Each credit card system that is used to process credit card transactions is required to provide a PA DSS certificate for the defined version before it becomes operational in the USU business environment.
3. Requests for Proposal (RFP) applicants that involve a credit card payment processing component will only consider systems with the submission of a PCI DSS or PA DSS certificate. In addition, the plans for installing and implementing the system must have the approval of the PCI Compliance Officer to ensure it meets all University security requirements before purchase.
4. Departments using third-party vendor software or systems to process PII or credit card transactions must demonstrate that the vendor is compliant with Payment Card Industry Data Security Standards (PCI DSS). In addition, the department must have the approval of the Director of Treasury Services and PCI Compliance Officer to ensure that the system meets all University security requirements before it may accept and process any credit card payments.
5. All credit card transactions will be encrypted and transmitted on USU's PCI Network. All terminal devices will be reviewed and approved by the PCI Compliance Officer before being added to or leaving the PCI Network. A device is required to have a fresh install before coming on the network to prevent contamination. A device leaving the PCI Network is required to be cleaned to prevent leakage of sensitive information.
6. All credit card systems housed at USU will be required to have an assigned database administrator to perform the required daily security duties. All servers

that pass, store, or transmit credit card information are required to be housed in a Data Center environment. This will ensure that the systems meet the minimum security requirements.

7. University personnel who receive and/or process credit card information must properly safeguard the data and record the transaction(s). This policy applies to all University personnel who handle PII data during the processing of any transaction, or who retain, store and/or safeguard or dispose of PII data.
8. Only University employees (full or part time) are permitted to handle PII data as defined under this policy and in accordance with the procedures outlined below.
9. Mandatory initial credit card security training and subsequent training sessions for system or procedural enhancements will be coordinated by the USU CARD. All employees who process or oversee credit card transactions will be required to participate. Employees must also sign a credit card security ethics certification to document their understanding and willingness to comply with all University policies and procedures. This certification will be maintained in the employees' personnel files.
10. Budget Unit Heads, Deans, or Directors must request that the Human Resources Department perform a criminal background check (386.5.3) and/or credit check (386.5.7) before any new or transferring employees are permitted to handle credit card transactions or data. If an existing employee is underperforming, background checks must be completed. There should be no outstanding or unexplained items resulting from these checks.
11. All credit card terminals and web applications must be closed out and reconciled on a daily basis. Departments maybe responsible to assure that their cost centers have been credited by the merchant services processor or bank. Furthermore, departments are responsible for responding to any disputes, also called chargebacks, within specified time limits (maximum 10-15 days) or funds will be debited automatically from their cost centers. Departments need to reconcile by the close of the month's end between charges and Banner.
12. Departments and Employees must comply with all requirements of the University's Computer Management Policy (Number 551) and Appropriate Use Policy (number 550) to protect the integrity and privacy of data within the University's computers, computer systems and networks.
13. Access to PII data must be restricted. All data must be safeguarded from fire and theft and stored in a locked environment until disposed of.
14. All PII information **must** be cross-shredded 90 days after the transaction was processed.

15. When an University employee suspects the loss or theft of any materials containing cardholder data, they must immediately notify their supervisor and the Director of Treasury Services, PII Officer, FERPA Officer, and PCI Compliance Officer.
16. Failure to follow these policies may result in the loss of credit card processing privileges as shall be decided by the PCI Compliance Committee.

Procedures

I. GENERAL PROCEDURES

A. All departments are required to:

- 1) Close out and settle their credit card terminals and/or web-based applications daily.
- 2) Reconcile transactions on their Daily Settlement Reports against their Banner E-Print reports to assure that they have received credit for all processed transactions. Reconciliation must be performed at least monthly.
- 3) Handle any consumer disputes. Users must respond to “chargeback” notifications and respond to consumer disputes. Failure to reply by stated deadlines will result in loss of payment credit for the departments.
- 4) Background check on USU Employees; student employees must complete the student background form.
- 5) Have new employee attend training and sign ethic documents before being able to process credit cards.

B. Departments must:

- 1) Retain receipts for a period of 120 days, after which the data must be shredded.
- 2) Display only the last four (4) digits of the credit card number on a receipt.
- 3) Never retain the three- or four-digit validation code (CVV2) in any form.

- 4) Never release credit card information to others in any form.
- 5) Store and secure cardholder data in locked containers in secured areas with limited access. Examples include paper data, such as customer receipts, merchant duplicate receipts, reports, conference applications, etc. Credit Card section will need to be processed and cross-shredded within 5 business days.

C. The Compliance Officer will provide departments with updated information whenever a merchant services processor or card associations announces significant policy or procedural changes.

D. Mandatory initial training and subsequent training sessions for system or procedural enhancements will be coordinated by the PCI Compliance Officer in USU CARD Office. All employees who process or oversee credit card transactions will be required to participate annually.

II. WRITTEN PROCEDURES

A. DEPARTMENTAL PROCEDURES

1. All credit card payments received and/or processed by departments must be supported by appropriate 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. The reconciler will review for consecutive order.
 - b. All payments received through the mail must be supported by lists prepared by the mail opener. Documentation also needs to outline any short-term locked storage, processing, and destroying procedures. Storage is limited to 5 businesses days before processing and shredding credit card information on paper form.
 - c. All payments via telephone need be entered into a payment device at the time of customer provides credit card information. USU employees are forbidden to write down any credit card information.
 - c. All payments received via a web-based application must be maintained in an electronic format on a secured web site or server. No PII or credit card data can be maintained on a desktop or laptop computer hard drive, or other related media (i.e., thumb drives, zip disks).
2. As required by this policy, each department that processes credit card transactions and maintains PII records must have written procedures tailored

to its specific organization. The 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. Departments must submit procedures document(s) to PCI Compliance Officer on an annual bases.
 4. For assistance in developing departmental procedures, contact the PCI Compliance Officer at 435-797-8410.
 5. Departmental procedures should be reviewed, signed and dated by the Budget Unit Head on an annual basis indicating compliance with the University's Credit Card Policy. These procedures also must be submitted and approved by their Dean or Vice President.

B. SEGREGATION OF DUTIES

1. Departments handling credit card transactions should separate, to the extent possible, all duties related to data processing and storage. 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 card transactions and perform the Cost Center reconciliation. The same person also should not process transactions and refunds. In addition, credit card refund processing and monitoring must be performed by different individuals.
2. The Budget Unit Head will contact the Card Office and Controller's Office with any questions regarding the development of mitigating controls. Internal Audits may audit the adequacy of the controls. Department procedures must be updated immediately to reflect the implementations of any mitigating controls.
3. The Budget Unit Head or his/her designee should perform reconciliations on a regular basis, but in any case not less than monthly. Reconciliations must compare all credit card payments processed using original supporting documentation, with the monthly Cost Centers to assure that all deposits are properly recorded. Reconciliations must be maintained by the Department and are subject to review.

4. The Budget Unit Head or his/her designee should not handle or have access to credit card transactions if they are the person reconciling. He or she will verify that the original supporting detail records agree with deposits on the Cost Center Reports. The terminal or web-based reports may not be the only supporting detail record.

C. CHARGEBACKS/DISPUTED TRANSACTIONS RETURNED BY PROCESSOR

1. Credit card transactions that are returned by the Depository Bank/credit card processor or are disputed by the customer result in additional service fees or loss of revenue to the University.

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 amount of time (usually 10 days) to respond.

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 Cost Center as a debit transaction.

2. Departments are responsible for:
 - a. Responding to disputed charged
 - b. Collecting funds owed after a chargeback occurs if the goods or services were provided to the consumer.

D. EXCEPTIONS

1. It is understood that unique situations within individual departments may require permanent exceptions to this policy. Any permanent exception to this policy must be included in a department’s written procedures and must be approved by PCI Compliance Committee and the Vice President for Business and Finance.
2. Unique situations within individual departments may require a limited and/or short-term exception to this policy. Exceptions must be restricted to specific dates or events and must be approved in advance by PCI Compliance Committee and the Vice President for Business and Finance.

III. COMPLIANCE PROCEDURES

A System Administrator is required for any credit card system hosted on campus. For systems that are hosted off-campus, but have terminals residing on the PCI Network, an IT person needs to be identified that will maintain patches and troubleshoot issues for terminals.

System Administrators are responsible for:

1. Making sure their system meets the PCI Requirements.
2. Submit PA DSS to PCI Compliance Officer before installing new system or upgrades.
3. System Administrators will not issue any user accounts or credit card access without the proof that the individual attended the Credit Card Security Training.
4. Remove credit card permissions for any individual that is found NOT adhering to the Credit Card Security requirements.
5. Remove credit card processing privileges for individuals that fail to participate in annual credit card information or for individuals that no longer need permissions.
6. Review logs on a daily bases as outlined in PCI Requirements.
7. Follow the Breached Protocol Procedures outlined by the IT Security Team for systems that may have been potentially compromised.
8. Contact the PCI Compliance Officer with regards to moving equipment on and off the PCI Network.
9. Ensure machines meet the clean device requirements.
10. Ensure all anti-virus software and patches are installed and kept updated on all terminal devices and servers.
11. Document location and procedures for their system.
12. Assist with filling of PCI documentation for their system.
13. Resolve any compliance issues detected by scans or penetration testing.

IV. CREDIT CARD PCI NETWORK PROCEDURES

Every system that passes, processes, or stores credit card information is required to have all application servers, database servers, and terminal/endpoint devices on the appropriate PCI network. Terminals that are used by USU to process credit cards thru an online, third-party vendor are in PCI scope and need to be registered on the PCI Network. In order to get be assigned an address on the PCI network; the following things need to be achieved:

1. All terminal devices need to have a fresh install of their operating system were applicable. Windows based computers should utilize a local WSUS server and Microsoft Security Essentials.
2. System servers will be housed in the central SER data center and have two network cards, one for the PCI network and one for the PCI Network.
3. The URL addresses of all third-party websites processing credit cards must be submitted to USU System Operation team to be added to the web proxy used by these dedicated POS terminals. Proxy configuration information will be given when these are submitted.

4. The MAC address for each terminal device, printer, and/or computer that will be registered in openIPAM to gain access on the PCI Network.
5. The MERU wireless system does not meet the requirements for PCI Compliance. If equipment which will be processing credit cards has wireless capabilities, the MAC address for the wireless network card must be submitted to USU System Operation team to be put on a restriction list to ensure that it can't talk on the wireless network.
6. All terminals need to have a 1-1 relationship with a wall jack/data jack. This is required for the device to obtain an IP address on the PCI Network.
7. All servers and terminal devices moving off of the PCI Network need to have a fresh install of their operating system were applicable to ensure no sensitive data is moved into a less secure area.

The PCI Compliance Officer's approval is required before equipment is placed onto the PCI network. Contact the PCI Compliance Officer with the above list of items requesting that a machine be assigned to the secure network. The Officer will forward the information an IT Network Team member or System Operations Team member who is designated to assist the system admin in registering the device on the PCI Network.