University of Colorado Boulder

CREDIT CARD ACCEPTANCE
PROCEDURAL STATEMENT

Source: Associate Vice Chancellor for Budget and Finance
Approved by: Senior Vice Chancellor & Chief Financial Officer
Effective Date: April 1, 2011

1. Purpose

The purpose of this procedure is to establish the requirements and procedures for accepting credit cards as a method of payment for goods or services provided by campus departments at CU-Boulder.

This procedure applies to all campus departments that accept debit or credit card payments for goods or services provided to external entities and customers of the University, as well as internally to other University departments.

2. Reference

Colorado Revised Statutes 24-17-102 Control System to be Maintained
http://www.michie.com/colorado

Payment Card Industry Data Security Standard (PCIDSS)
https://www.pcisecuritystandards.org

Acceptance of Payment Card Cost and Risk APS
https://www.cu.edu/ope/aps/4056

CU Treasurer Card Merchant Guide
http://www.cu.edu/articles/upload/Card%20Merchant%20Guide.pdf

CU-Boulder Campus-wide IT Policies – including private data standards
http://www.colorado.edu/avcit/campus-policies

3. Responsibility

It is the responsibility of CU Boulder campus Organizational Unit heads to ensure compliance with this procedure and the Acceptance of Payment Card Cost and Risk APS.

4. Definitions

Acquiring Bank – The bank that sponsors the University of Colorado to the payment card system. At this time our Acquiring Bank is Wells Fargo Payment Services.

Fees – Every transaction incurs a “discount” and “processing” fee to the credit card system. In addition, there may be set-up fees in order to begin accepting credit card payments. Other

costs also might include the cost of equipment used for processing card payments, supplies, annual security maintenance costs, as well as other items.

Outsourcing agreement – A contract for an outside vendor to provide card processing software, hardware and or internet accessibility for accepting payment cards on behalf of the department.

Payment Card Industry Data Security Standard (PCIDSS) – Required standards for the protection of cardholder data, both in electronic and paper form, issued by the Payment Card Associations (Visa, MasterCard, Discover, and American Express) and enforced by the University's Acquiring Bank.

Payment Card Information – Includes any information relating to a cardholder's account with a payment card company. This includes cardholder name, card number, expiration date, and the contents of a card's magnetic stripe, as well as other information related to the payment transaction.

Payment Card Merchant Guidelines – Guidelines posted on the Treasurer's web site regarding the acceptance of payments cards.

5. Procedure

A. General

The Campus Controller, the Treasurer's Office, and the IT Security Office must approve all payment card processing activities at CU Boulder. Prior to approval, the campus department will be set up within the centralized University banking and accounting environment. Third parties using the campus network for credit card processing shall have card processing activities approved by the IT Security Office.

If a department is processing and/or storing payment card information in an electronic environment, the IT Security Office will review the department's information security measures as completely meeting the requirements of the PCIDSS. Approval will not be granted for departments that do not comply with PCIDSS.

Campus departments are responsible for continued compliance with PCIDSS and annual completion of the self-assessment questionnaire provided by the University Treasurer.

Existing merchants who are found to be out of compliance with either PCIDSS, university policies, or campus standards will be reported to the University Treasurer, IT Security Office, and Campus Controller. A determination whether to terminate payment card processing may be made by the Associate Vice Chancellor & CIO or the Associate Vice Chancellor for Budget and Finance & Campus Controller. Depending on the nature of the infraction, responsible employees may be subject to disciplinary action, as appropriate under University rules.

B. Approval for the Acceptance of Credit Card Payments

The Campus Controller and IT Security Office will check for compliance with the following provisions when approving new or reviewing existing credit card accepting merchants:

1. Compliance

- Comply with the Payment Card Industry Data Security Standards and technical requirements.

- Complete an annual certification of compliance with the PCIDSS.

2. Costs

Fees assessed by the credit card processor (e.g. MasterCard/Visa) are the fiscal responsibility of the department and may not be passed on to the cardholder in discrimination of accepting a card payment.

Any labor or expenses associated with bringing systems into compliance are the responsibility of the department owning the system.

3. Outsourcing

Outsourcing agreements to third party vendors must be preapproved in writing by the Campus Controller, Treasurer's Office and IT Security Office prior to the execution of any agreement. Departments may be required to use preapproved vendors unless there exists a legitimate business need. All third party providers must meet the standards set forth by the PCIDSS. Outsourcing agreements must also comply with Procurement Service Center (PSC) procedures. In the event that the actual processing of credit card transactions is outsourced, various training and duty requirements will differ as noted below, but the principles are the same.

4. Training

The department must provide annual training to employees handling payment card transactions including security content provided by the IT Security Office. Employees are required to annually certify that they understand and agree to abide by the credit card rules. All employees handling payment card information electronically must complete the University of Colorado Information Privacy and Security online security training.

5. Segregation of Duties

Proper segregation of duties involves two roles:

- For departments accepting credit cards directly, one person receives payments and handles deposits. For outsourcing, this person needs transaction access to process manual transactions.
- A monthly reconciliation of receipts, deposits and university accounting records should be performed by a person who does not have access to handle payment cards, cash or deposits. Supervisory review of daily receipt close-out documentation may be done by this person or a third person. For outsourcing, this person should only have access to view transactions, not enter transactions.

6. Refunds

The department must have a written refund policy clearly visible on its website. Refund transactions must be approved by a departmental supervisor and must be properly documented, including the reason for the refund, the approver's signature, and such other details as may be appropriate.

7. Daily Transaction Settlement

The process of obtaining approval for a transaction does not create a request for the bank to make payment. Transactions must be settled *daily* by sending the batch for processing as part of the department close-out procedure then

the buyer's bank will make payment to our bank. Departments with outsourced functions will not have a daily transaction settlement.

8. **Reconciliation**
   A reconciliation should be performed between daily transaction settlements and the general ledger. Departments with outsourced functions will have to reconcile the transactions recorded in PeopleSoft to the transactions recorded in the outsourced system. These should be done daily when activity first commences and no less often than weekly thereafter.

9. **Audit**
   Annual audits must be conducted by a department supervisor to ensure payment card numbers are being safeguarded against unauthorized access. This is required to be completed before the annual certification.

10. **Information Security**
    All systems used to support business functions requiring credit card processing must meet the CU-Boulder Private Data Security Standards.

C. Approval for the Use of the Campus Network For Processing Of Credit Card Payments

When the campus provides network service for events processing credit cards, the campus has certain obligations to ensure that the whole of the campus network is not considered in-scope for PCIDSS compliance requirements. These requirements apply regardless of the type of event being hosted on campus (e.g., an event managed by a campus entity or a third party under contract for using campus space). The Campus Controller and IT Security Office will check for compliance with the following provisions when approving requests to use the campus network for processing of credit card payments. Approval will not be granted should existing campus network services not have the capability to support security requirements for the equipment used by the organization hosting the event.

1. **Event space providers (e.g., UMC, Conference Services, Coors Events Center, Committee on Use of University Facilities) shall:**
   - Ensure that groups hosting events on campus receive information regarding campus and PCIDSS requirements processing of credit card information
   - Coordinate with groups hosting events and ITS providers regarding any additional security requirements required by card processing system vendors. For example, if a point of sales system vendor has provided secure implementation guidelines, the event space provider will need to coordinate with ITS to determine if the guidelines can be implemented.
   - Act on behalf of the groups hosting events on campus when requesting network services.

2. **Organizations hosting events on campus must:**

- Provide and support all card processing equipment in compliance with PCI Security Council Standards.
- Inform event space provider of any additional security requirements for card processing equipment.

D. Notifications

The campus department must immediately notify the IT Security Office when there is a breach in security and payment card information might have been compromised, whether or not there is actual evidence of compromise of the information.

If card information is accepted over the internet or electronically, the campus department must notify the IT Security Office if there are planned or unplanned changes in network configuration, equipment, software, or IP address of the machines on the network that contains the card processing machine(s).

The campus department must immediately notify the Treasurer's Office if there is a change of personnel handling card transactions.