University of Colorado
Denver | Anschutz Medical Campus

Campus Administrative Policy

Policy Title: Credit Card Acceptance

Policy Number: 2019 Functional Area: Finance

Effective:	February 1, 2011
Date Last Amended/Reviewed:	February 1, 2011
Date Scheduled for Review:	July 1, 2019
Supersedes:	Credit Card Acceptance (July 1, 2010)
Approved by:	Assistant Vice Chancellor for Finance and Administration
Prepared by:	Deputy Controller
Reviewing Office:	Executive Vice Chancellor for Administration and Finance and Chief Financial Officer (CU Anschutz) Senior Vice Chancellor for Administration and Finance and Chief Financial Officer (CU Denver)
Responsible Officer:	Executive Vice Chancellor for Administration and Finance and Chief Financial Officer (CU Anschutz)
Applies to:	University of Colorado Denver University of Colorado Anschutz Medical Campus

---

A. INTRODUCTION

The purpose of this policy 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 the University of Colorado Denver and University of Colorado Anschutz Medical Campus ("university").

It is the responsibility of university campus departments, Fiscal Principals and Fiscal Managers to ensure compliance with this policy.

B. TABLE OF CONTENTS

C. APPLICABILITY AND DEFINITIONS

1. Applicability

This policy 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 from other university departments.

2. Definitions

a. 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.
b. 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, online service charges, as well as other items.
c. 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.
d. 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 Security Standards Council (an industry security coalition) and the Payment Card Associations (Visa, MasterCard, Discover, and American Express) and enforced by the University’s Acquiring Bank.
e. 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.
f. Payment Card Merchant Guidelines - Guidelines posted on the Treasurer’s web site regarding the acceptance of payments cards.

D. POLICY STATEMENT

1. General

The Campus Controller and the Treasurer’s Office must preapprove all payment card processing activities at the university. Each department must be set up within the centralized University banking and accounting environment. Campus departments may not set up their own banking relationships for card processing and card receipts. The Treasurer’s Office negotiates all banking and card processing relationships on behalf of the entire University.

If a department is processing and/or storing payment card information in an electronic environment (in spreadsheets, databases, word processing documents, web server, software, or any electronic form whatsoever) the campus Security Principal must also approve the department's information security measures as completely meeting the requirements of the PCIDSS.

Failure to comply with this policy will result in the immediate termination of payment card processing activity and fines may be levied against the department by the Payment Card Associations. Depending on the nature of the infraction, responsible employees may be subject to disciplinary action, as appropriate under University rules.

2. Accepting Credit Card Payments

Each campus department must comply with the following provisions when accepting card payments:

a. Approval

Request and obtain prior written approval from the Campus Controller and the Treasurer's Office before instituting a process to accept card payments. Campus departments may not set up their own banking relationships for payment card processing and card receipts. The Treasurer's Office negotiates all banking and card processing relationships on behalf of the entire University. If the department is accepting card payments in an electronic processing environment, the campus Security Principal must also approve the department's IT security measures and certify that they meet the security requirements of the PCIDSS.

b. Compliance

i. Comply with the Payment Card Merchant Guidelines.
ii. Comply with the Payment Card Industry Data Security Standards and technical requirements.
iii. Complete an annual certification of compliance with the PCIDSS
iv. If using a third party processor to process and/or handle card payments, the vendor must be certified as being in compliance with the PCIDSS or the Payment Application Data Security Standard (PA-DSS), as applicable. This certification must be obtained before the vendor is contracted for any processing duties, and must be reaffirmed annually. The Treasurer's office can assist with determining whether a vendor is so certified.

c. Cost

i. Fees, discounts and charges 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.
ii. Any labor or expenses associated with bringing systems into compliance are the responsibility of the department owning the

system.

iii. Any costs incurred to comply with PCIDSS or any fines, penalties or charges incurred as a result of a security breach or failure to comply with PCIDSS are the responsibility of the department.

d. Outsourcing

Outsourcing agreements to third party vendors must be preapproved in writing by the Campus Controller and Treasurer's Office prior to the execution of any agreement. All Third party providers must meet the standards set forth by the Payment Card Industry Data Security Standard (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.

e. Training

Provide annual training to employees handling payment card transactions. Employees are required to certify that they understand and agree to abide by the credit card rules. All employees handling payment card information electronically must complete the university online security training.

f. Segregation of Duties

Proper segregation of duties involves two roles:

i. For departments accepting credit cards directly, one person receives payments and handles deposits. For outsourcing, this person needs transaction access to process manual transactions.

ii. 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.

g. 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. Refunds may only be made back to the credit card, not in cash or by check.

h. 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's 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.

i. Reconciliation
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.
Reconciliation should include watching for potentially fraudulent transactions, such as transactions of an unusually high amount, for unusually high quantities, repetitive transactions from the same customer, or payments against zero balance accounts.

j. 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.

k. Information Security
   i. Access to payment card information must be restricted to those who need to know to perform their job duties.
   ii. All credit card numbers stored on a PC or on the campus network, whether in an application specifically designed for card payment processing or in other forms such as a database, spreadsheet, or word processing document must have prior written approval from the Treasurer's Office and adhere to PCI security standards.
   iii. Sending of payment card numbers over the internet must have prior written approval from the Treasurer's Office and adhere to PCI security standards
   iv. Payment card information cannot be sent via email. If a customer sends their card information via email, the message should be printed, the transaction processed, the card information blacked out after successful conclusion of the transaction, and the email deleted immediately. Customers should be notified that email is not secure and to not send any cardholder information using email.
   v. Paper-based credit card processing must have prior written approval from the Treasurer's Office and adhere to PCIDSS security standards. This includes ensuring that cardholder data printed on paper or received by fax is protected against unauthorized access. Once card payment approval has been obtained, delete the cardholder data (blackout credit card numbers – except for the last four digits) or shred it before it is physically disposed. Be sure to design any forms used to collect credit card data along with other data, such as conference registration data, so that credit card data can be detached and destroyed after payment has been processed.
   vi. The department must adhere to the campus information security policy

for use of sensitive and/or classified data.

vii. All systems used in the storage, transmission, or processing of payment card information must be secured based upon the PCIDSS security standards and the university campus policies for information security.

3. Notifications

The campus department must immediately notify the Treasurer's Office (who will coordinate with the Campus Controller and ITS Compliance and Security Analyst) when:

a. 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.
b. Change of personnel handling card transactions.
c. If card information is accepted over the internet or electronically and there is any change in network configuration, equipment, software, or IP address of the machines on the subnetwork that contains the card processing machine(s).
4. Customer Liability for Processing Fees and Collection Costs

Customers may be charged for credit card processing fees, attorney fees and other collection costs on transactions that are fraudulent or otherwise noncompliant with cardholder agreements.

E. SETUP PROCEDURE

These procedures include the documents necessary to demonstrate to the Payment Card Industry that the University has performed due diligence in implementing the necessary controls and safeguards to protect the cardholder account information.

Performed by:	Action:
Request to obtain Permission to Accept Credit Payments ***Please allow adequate processing time!***	
Campus Department	1. Review the Credit Card Merchant Guide. 2. Complete the Precard Business Practices Checklist. 3. Contact the Treasurer's Office as indicated at the end of the preceding documents to obtain the following forms to be submitted to the Treasurer: • Credit Card Merchant Application • Payment Card Industry Self-Assessment Questionnaire • Payment Card Industry Data Security Questionnaire (if you want to accept credit cards over the internet)

Treasurer's Office	4. Reviews application and coordinates with department regarding incomplete information or items needing clarification. 5. Conducts an on-site meeting with department to review payment card business practices and performs card acceptance training. 6. Coordinates approval by Campus Controller of the business purpose.
Campus Controller	7. Analyzes business case for accepting card payments; work with department to remedy deficiencies; approves request to accept card payments
Campus Department IT support personnel	8. If applicable, department IT support personnel meet with ITS Compliance and Security Analyst and Treasurer's Office to ensure that the PCIDSS requirements are completely understood and technically feasible for the department to meet.
Campus Department	9. Employees in departments that will be performing payment card transactions sign certification statement agreeing to abide by University credit card polices and Payment Card Industry rules. The form is sent to Treasurer's Office.
Treasurer's Office	10. If necessary, the Treasurer's Office and the ITS Compliance and Security Analyst will work with the department and their software providers to discuss credit card processing standards. Any labor or expenses associated with bringing systems into compliance are the responsibility of the department owning the system. 11. Coordinates approval by ITS Compliance and Security Analyst. 12. Coordinates with the credit card merchant to establish new merchant ID for the department.

F. ACCOUNTING PROCEDURES

Procedures to account for the cost of accepting credit cards depend on who is the merchant of record:

1. **Merchant of Record is the University of Colorado (CU)**
   If the merchant of record is CU, then payment will be received in one of two ways:
   a. Through the Treasurer's Office, which will make all necessary entries, including crediting the departmental speed-type for the revenue, and debiting the departmental speed-type in account 552607 for the fees and charges.
   b. Through the campus depository account, in which case the department shall make the appropriate accounting entries on the Bursar's deposit form. Monthly fees will also be posted through the campus depository account into the department's speedtype and account 552607 for fees and charges.

2. **Merchant of Record is a Third-Party Vendor**
   If the merchant of record is a third-party vendor, such as an online registration and payment service, then they will accept payment on our behalf and remit

payment to the department. If the remittance is the gross sales amount, a separate invoice for credit card and service fees will also be transmitted to us, generally on a monthly basis. Contact Purchasing to set up an SPO and work out any needed contractual agreements for this service.

Some third-party vendors remit payment to us on a net of credit card and service fees basis. In this case two steps are required to properly record the full sale amount and the cost of accepting credit cards and paying the third-party vendor for their service:

a. Deposit the check to revenue.
b. Record credit card and service fee expense and gross up revenues by entering a journal to:
    i. Debit account 552607 (credit card fees) for the amount of the credit card and service fees deducted by the third-party vendor from gross sales.
    ii. Credit the appropriate revenue account (Contact **the Finance Office Help Desk at 303-315- 2250 or see the Auxiliary Revenue Guide).**

Notes

1. Dates of official enactment and amendments:
   July 1, 2010: Adopted by Assistant Vice Chancellor for Finance and Administration
   February 1, 2011: Updated
   February 21, 2019: Formatting Updated

2. History:
   February 21, 2019: Modified to reflect a campus-wide effort to recast and revitalize Campus policy sites into a standardized and more coherent set of chaptered policy statement organized around the several operational divisions of the university. Article links, University branding, and formatting updated by the Provost's office.

3. Initial Policy Effective Date: February 1, 2011

4. Cross References/Appendix:
   - Colorado Revised Statutes 24-17-102 Control System to be Maintained
   - Payment Card Industry Data Security Standard (PCIDSS)
   - CU Treasury – Card Merchant Guide
   - UC Denver – Information Technology Policies