University of Colorado
Colorado Springs

UCCS CAMPUS POLICY

Policy Title: Credit Card Acceptance and Security Policy

Policy Number: 500-012 Policy Functional Area: FISCAL

Effective:	June 15, 2011
Approved by:	Pam Shockley-Zalabak, Chancellor
Responsible Vice Chancellor:	Vice Chancellor of Administration and Finance (VCAF)
Office of Primary Responsibility:	AVCFHR
Policy Primary Contact:	Controller’s Office, 719-255-3684
Supersedes:	N/A
Last Reviewed/Updated:	June 15, 2011
Applies to:	Administration, Faculty, and Staff

Reason for Policy: It is the policy of the University of Colorado Colorado Springs (UCCS) to protect the security and confidentiality of all payment cardholder information, at all times, and in whatever forms such information is received for the payment of goods and services.

I. INTRODUCTION

It is the policy of the University of Colorado Colorado Springs (UCCS) to protect the security and confidentiality of all payment cardholder information, at all times, and in whatever forms such information is received for the payment of goods and services.

II. POLICY STATEMENT

A. Authority for the creation of campus administrative policies is found in *The Laws of the Regents*, 1190, Article 3 Section B.8, which states:

The chancellor of the University of Colorado at Colorado Springs shall be the chief academic and administrative officer responsible to the president for the conduct of affairs of the Colorado Springs campus in accordance with the policies of the Board of Regents. The chancellor shall have such other responsibilities as may be required by these *Laws*, the Board, and as may be delegated by the president.

B. Purpose:

This policy provides guidance for the requirements and procedures for accepting credit cards as a method of payment for goods and services provided by campus departments at UCCS.

C. Procedures:

1. General.

The Campus Controller and the Treasurer's Office must preapprove all payment card processing activities at UCCS. 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.

Failure to comply with this policy will result in the immediate termination of payment card processing activity. 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
Each departments who wants to accept credit cards as a method of payment must first go through the Treasurer's Office for approval. The Treasurer's Office will work with the department to go through these three compliance steps:
i. Comply with the Payment Card Merchant Guidelines.
ii. Comply with the Payment Card Industry Data Security Standards (PCIDSS) and technical requirements.
iii. Complete an annual certification of compliance with the PCIDSS.

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

c. 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) and be certified. This certification must be obtained before vendor is contracted and reaffirmed annually. The Treasurer's Office can assist with the vendor certification determination.

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.

d. Training
Employees are required to certify that they understand and agree to abide by the credit card processing policies set forth by the departments annually. All employees handling payment card information electronically must complete the CU Information Privacy and Security course through the hiring process.

e. Segregation of Duties
Proper segregation of duties involves two roles:
   i. For departments accepting credit cards directly, one person receives payments and handles deposits.
   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.

f. Refunds
The department must have a written refund policy clearly visible on its website or other printed material used to advertise credit card acceptance. 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 by cash or check, and never for more than was originally charged to the credit card.

g. 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.

h. 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 usually high amount, for unusually high quantities, repetitive transactions from the same customer, or payments against zero balance accounts.

i. Information Security
   i. Access to payment card information must be restricted to those who have a need to know to perform their job duties.
   ii. It is prohibited to store or retain cardholder information in any electronic form whatsoever, including in spreadsheets, databases, word processing documents, emails, on websites, or by any other electronic means or in any electronic file unless technology is used to store information is PCI DSS or PCI PA-DSS compliant and has the approval of the campus IT Security Principal.
   iii. Payment card information cannot be sent via end user messaging technologies. If a customer sends their card information via email, the message should be printed, the transactions processed, the card information blacked out after successful conclusion of the transactions, and the email deleted immediately. Customers should be notified that email is not secure and to not send any cardholder information using email.
   iv. Paper-based credit card processing must have prior written approval from the Treasurer's Office and adhere to PCI 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, 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.
   v. The department must adhere to the campus information security policy for use of private or restricted data.
   vi. All systems used in the storage, transmission, or processing of payment card information must be secured based upon the PCIDSS security standards and the UCCS campus policy for information security.

3. Notifications.

   The campus department must immediately notify the Treasurer's Office (who will coordinate with the Campus Controller and IT Security Principal) 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 reconciliations.
   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 sub network 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 noncompliant with cardholder agreements.

D. Responsibility:

The security and confidentiality of cardholder information is the responsibility of every employee in this department, whether or not directly involved in processing payment transactions, and each employee is expected to be familiar with the methods used to protect cardholder information.

III. KEY WORDS

A. Acquiring Bank
B. Fees
C. Outsourcing agreement
D. Payment Card Industry Data Security Standard (PCIDSS)
E. Payment Card Information
F. Payment Card Merchant Guidelines

IV. RELATED POLICIES, PROCEDURES, FORMS, GUIDELINES, AND OTHER RESOURCES

A. Administrative Policy Statements (APS) and Other Policies

Colorado Revised Statues 24-17-102 Control System

Payment Card Industry Data Security Standard (PCIDSS)

CU Treasury - Card Merchant Guide

UCCS Information Security Policy

APS 4056-Acceptance of Payment Card: Cost and Risk

Set Up Procedures (to be completed)

B. Procedures

C. Forms

D. Guidelines

E. Other Resources (i.e. training, secondary contact information)

F. Frequently Asked Questions (FAQs)

V. HISTORY

Initial policy approval June 15, 2011