University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus
Published on *University of Colorado* (https://www.cu.edu)

APS 4056 - Acceptance of Payment Card Cost and Risk

PDF Version

Policy Profile

Policy Title:	Acceptance of Payment Card Cost and Risk
APS Number:	4056
Effective:	January 1, 2011[1]
Approved by:	President Bruce D. Benson
Responsible University Officer:	Vice President and Chief Financial Officer
Responsible Office:	Treasury
Policy Contact:	Assistant Treasurer, 303-837-2185
Supersedes:	N/A
Last Reviewed/Updated:	January 1, 2011
Applies to:	All organizational units that accept payment card payments across all campuses and system

Policy Snapshot

Brief Description: This policy establishes ultimate authority over payment card activity, assigns responsibility for oversight of campus payment card merchants, and specifies who bears the costs and risks of organizational units accepting card payments.

Reason for Policy: The acceptance of payment cards by organizational units incurs costs and presents significant financial and reputational risks to the university. This policy establishes authority and responsibility for overall management of the university?s payment card programs, clarifying responsibility for approval and oversight of payment card merchants, and assigning responsibility for costs and risks associated with payment card acceptance.

I. Introduction

Payment cards are one of the most convenient but also most costly methods for accepting payment for goods and services. In addition, acceptance of payment cards has inherent risks for the merchant unit and the university. The immediate risk is of a payment transaction being returned to the unit after a good or service is provided to a customer. There is also the risk that any cardholder data within the merchant processing environment, on paper or in electronic form, is compromised and possibly used for fraud. If cardholder data is compromised the negative consequences can be significant financial and reputational risk, for both the merchant department and the university as a whole.

II. Policy Statement

A. Authority for overall management of the university?s payment card programs

   The treasurer of the university, in coordination with the designated campus and system authorities, is responsible for the overall and ongoing oversight and management of the university?s payment card acceptance program. This includes management of the relationship with the university?s acquiring bank, coordination of compliance efforts across the campuses and system with the acquiring bank and Payment Card Associations, and reporting to the president in the event of a breach of cardholder data confidentiality. No organizational unit shall accept card payments without the express approval of the treasury. All merchant units will attain and maintain compliance with the Payment Card Industry Data Security Standard (PCIDSS) and other relevant standards and requirements for processing and securing cardholder data. The treasurer has the authority to temporarily suspend or permanently revoke the ability of a merchant unit to accept card payments at any time within the treasurer?s discretion.

   This authority does not automatically apply to the university?s procurement card program or to non-payment transactional campus banking relationships.

B. Responsibility for and oversight of payment card merchants

On each campus, the vice chancellor/chief financial officer is responsible for the approval of new payment card merchant applications for that campus as well as ongoing oversight of new and existing merchant units. The vice chancellor may delegate these responsibilities in writing. For system units desiring to accept card payments, the system controller is the designated responsible party. This approval and oversight authority includes acceptance of the risks entailed in accepting card payments.

Each campus shall maintain a policy that identifies the roles and responsibilities for oversight of payment card activities for the campus. As per the IT Security Program policy, the campus Information Security Officers shall for their respective campuses provide security standards pursuant to payment card industry standards as well as other federal, state or local regulations. The chief information security officer and the campus information resource oversight authority, as designated in the IT Security Program policy, shall have technical oversight and approval of proposed and current electronic payment processing methods, particularly with respect to the security, integrity, and confidentiality of those methods and cardholder data. Each campus must also maintain procedures for coordinating unauthorized payment card system access or data breach with treasury and the chief information security officer.

C. Responsibility for costs of payment card acceptance

The organizational unit that is the merchant of record for payments is entirely responsible for all costs and other responsibilities of payment card acceptance including, but not limited to, merchant discounts, fees, costs of processing services, equipment, software, maintenance, incident investigation, fines, remediation, and notification to customers. The organizational unit is also responsible for the privacy and security of any cardholder data to which it may become privy, as well as the security and integrity of any web site or web application through which it processes online payments. The unit may contract with third parties authorized by treasury to process cardholder transactions, but remains responsible for meeting their merchant compliance and security obligations.

III. Definitions

Acquiring bank ? the financial institution that sponsors the university into the payment card system, processes card transactions, and settles funds for card payments into university bank accounts.

Merchant ? any organizational unit accepting payment cards in payment for goods or services.

Payment card ? any mechanism used for payments that is issued by a financial institution and processed through a credit card or debit card/ATM processing network.

Payment card association ? associations of payment card issuers that govern payment card acceptance; this includes Visa, MasterCard, Discover, American Express, and JBC.

Payment Card Industry Data Security Standard (PCIDSS) ? the technical standard for the

security and privacy of cardholder data issued and maintained by the Payment Card Industry Security Standards Council or its successor.

IV. Related Policies, Procedures, Forms, Guidelines and Other Resources

1. Other Resources

   For additional information and training, contact Joseph D. Tinucci, Assistant Treasurer, 303-837-2185, joe.tinucci@cu.edu.

V. History

- Originally issued January 1, 2011
- The title of ?IT Security Principals? was replaced with the title of ?Information Security Officers? effective May 1, 2014.

VI. Key Words

Credit card, Credit card processing, Credit card security, Debit card, Merchant Services, Online payments, Payment card, Payments, PCI, PCIDSS, Security

---

1. The title of ?IT Security Principals? was replaced with the title of ?Information Security Officers? effective May 1, 2014.

Attachments:
Video:
Images:
Groups audience:
Office of Policy and Efficiency (OPE)

Source URL: https://www.cu.edu/ope/policy/aps-4056-acceptance-payment-card-cost-and-risk