University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

ADMINISTRATIVE POLICY STATEMENT

Policy Title: Payment Card Compliance Program

APS Number: 4056 **APS Functional Area:** **FINANCE**

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.
Effective:	March 1, 2017
Approved by:	President Bruce D. Benson
Responsible University Officer:	Vice President and Chief Financial Officer
Responsible Office:	Treasurer's Office
Policy Contact:	Assistant Treasurer, 303-837-2182
Supersedes:	4056-Acceptance of Payment Card Cost and Risk, January 1, 2011
Last Reviewed/Updated:	March 1, 2017
Applies to:	All organizational units that accept payment card payments across all campuses and system

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* compliance program

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 procedure that identifies the roles and responsibilities for oversight of *payment card* activities for the campus. Procedures must address ongoing monitoring of *merchant* security, annual security assessment for each campus merchant, and coordinating response to any unauthorized payment card system access or data breach with treasury and the chief information security officer. Procedures should also detail what responsibilities the campus Information Security Officers (ISO) choose to delegate to the respective campus information security staff.

As described in APS 6005 - IT Security Program, the campus ISOs shall, for their respective campuses, establish security standards that meet requirements of the PCIDSS as well as other federal, state or local regulations. The chief information security officer and the campus chief information officer, as designated in the IT Security Program policy, shall be responsible for providing technical oversight and approval of existing and proposed electronic payment processing methods, particularly with respect to the security, integrity, and confidentiality of those methods and cardholder data.

C. *Merchant* responsibility

The organizational unit that is the *merchant* of record is responsible for the following:

1. Costs of *payment card* acceptance and compliance

   The *merchant* is 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.

2. Protection of cardholder data

   The *merchant* is also responsible for the privacy and security of any cardholder data that it may collect, access, process or otherwise handle, as well as the security and integrity of any website or web application through which it processes online payments. The unit may contract with third parties authorized by the campus ISO and treasury to process cardholder transactions, but remains responsible for meeting their *merchant* compliance and security obligations established under the PCIDSS.

3. Certification of *payment card* environment

   The *merchant* shall, as part of completing the annual self-assessment questionnaire (SAQ), review the *payment card* processing environment with the campus ISO or designee. If the merchant is using a third party for all or portions of the payment card processing environment, it is responsible for acquiring a statement of compliance from the third party. At the discretion of the ISO, the merchant will facilitate an audit of the third party's compliance. The organizational unit is responsible for providing notification to the campus ISO of any *material change* in the payment card acceptance process and submitting a revised SAQ at the discretion of the campus ISO.

4. Training

   The *merchant* shall ensure that all staff responsible and accountable for handling cardholder data or support systems used for processing cardholder data complete appropriate training annually. The organizational unit

fiscal designee must complete annual self-assessment (i.e., SAQ) training. PCIDSS training is available and organizational units should consult with their campus ISO to determine appropriate training for their staff.

D. Enforcement

The treasurer is responsible for enforcing this policy and will collaborate with the campus ISO and campus controller on any enforcement actions. Any *merchant* failing to comply with this policy will be responsible for fines and/or incident response costs, and/or subject to termination of credit card processing accounts.

III. DEFINITIONS

For purposes of this policy, italicized terms used in this APS are defined in the APS Glossary of Terms or are defined in this APS:

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.

Fiscal Designee [FOR PURPOSES OF THIS POLICY ONLY] - The fiscal manager for the merchant account is the person responsible for the funds that are received and for the management of the staff handling the credit card transactions. In the accounting system, this person is generally referred to as the fiscal principal. This responsibility can be delegated.

Material Change – a significant change to an *organizational unit's* business or IT practices that may implicate the security, confidentiality, integrity, or availability of records containing cardholder data. Examples of material change include: 1) changes to network configuration, security controls, infrastructure, or data flow, 2) replacement of hardware in the cardholder environment, or 3) a major upgrade or replacement of applications in the cardholder environment.

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

A. Campus Policies and Procedures

- CU Boulder
- CU Colorado Springs
- CU Denver | Anschutz Medical Campus

B. Other Resources

- For additional information and training, contact the Assistant University Treasurer 303-837-2182.
- PCIDSS training is available and *organizational units* should consult with their campus ISO.

V. HISTORY

- Adopted: January 1, 2011.
- The title of "IT Security Principals" was replaced with the title of "Information Security Officers" effective May 1, 2014.
- Revised and renamed March 1, 2017. Previous title: Acceptance of Payment Card Cost and Risk.
- Clean-up January 31, 2018. Revised term "Fiscal Principal or Designee" to "Fiscal Designee" since the term "Fiscal Principal" is defined differently in other APSs.

VI. KEY WORDS

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