Policy 3-070: Payment Card Acceptance

Revision 1. Effective date: December 8, 2008

I. Purpose and Scope

A. Purpose.

This policy governs the acceptance of payment cards (e.g. Visa, MasterCard, American Express, and Discover) by the University. Being able to provide this payment option to University customers - including students, staff, parents, patrons, and patients - comes with significant responsibility to maintain cardholders' security and to mitigate the risk of fraud. The University, as a merchant, must adhere to strict security guidelines established by the Payment Card Industry or face significant financial penalties. In addition to such penalties, any compromise of cardholder information undermines public confidence in the University's ability to maintain appropriate stewardship over confidential information entrusted to it. Lack of compliance in a single area of the University could jeopardize the University's ability to accept credit cards in any area.

Hence, all departments and units accepting payment cards must abide by this policy.

B. Scope.

[reserved]

II. Definitions

A. Merchant Account - An account set up through a financial institution that provides a merchant with the ability to accept payment cards as payment for goods or services.

B. Merchant Fees - Charges assessed by payment processors and credit card companies for payment card transactions.

C. Payment Card - Credit cards or debit cards. Examples include Visa, MasterCard, American Express, and Discover.

D. Electronic Equipment - Payment card terminals, point of sale registers, kiosks, or computers where payment card software resides.

E. E-Commerce -The ability to accept payment cards over the internet for various goods or services. E-commerce functionality may be provided by approved in-house developed applications (UPay) or via a compliant third party software solution.

F. Payment Card Industry Data Security Standards (PCI DSS) - Security standards developed collaboratively by the major card issuers that must be adopted by all merchants accepting payment cards. These standards, which are updated from time to time, are intended to protect cardholder information from fraudulent use.

G. E-checks - The mechanism for accepting payments over the internet whereby the account holder provides bank routing and account number information. Payments authorized in this manner are directly debited from an individual's checking or savings account.

H. Certified Server - A server, computer, or point of sale device through which cardholder data is passed or stored. This equipment is PCI DSS certified by undergoing monthly scans and otherwise meeting all requirements for security. Only certified servers may be used for payment card data, even if the data's presence in the server is transitory.

I. Third Party Software - Commercially available software acting as a surrogate to the UPay system to provide services related to the processing of payment cards.

J. Qualified Security Assessor - An organization that has been certified by the Security Standards Council to validate an entity's adherence to PCI DSS.

III. Policy

A. Approval to Accept Payment Cards or E-Checks - University departments and units must receive approval prior to accepting payment cards or e-checks. Approval is granted by Financial and Business Services through its Income Accounting & Student Loan Services Office. Once approval is granted, Financial and Business Services works with the University's banking partner to establish the needed merchant accounts. They also work with the department or unit to ensure user training takes place, and all other requirements are met before payment cards may be accepted.

B. Payment Card Acceptance- Once merchant accounts are enabled for a department or unit, the department has an ongoing responsibility to understand security requirements, comply with PCI DSS standards, and to maintain proper business practices as described further in various Rules, Procedures, and Guidelines associated with this policy. Departments and units are responsible for paying all fees and other costs associated with accepting payment cards, including internal fees for administering the University's compliance program. Such costs may be passed on to the card holder.

C. Compliance with PCI DSS Standards - University leadership is committed to protecting confidential cardholder information. Departments and units accepting payment cards are expected to adhere to these standards, which are updated

periodically, and to enforce the compliance of third party service providers. They are also expected to attend the initial training and periodic refresher training necessary to understand and stay current with these standards. More detail on the PCI DSS standards is available at the following website: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml. The standards can be summarized as follows:

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

Financial and Business Services, through its Income Accounting & Student Loan Services Office; and the Office of Information Technology, through its IT Compliance Office have been assigned responsibility for assessing, determining, and monitoring compliance with these standards. As a result, responsibility for determining how to apply these standards and for assessing deficiencies is shared among these named areas.

D. Sanctions for Non-Compliance - University departments or units that transact business using payment cards in a manner that deviates from this policy are subject to various financial and other sanctions. These may include termination of merchant accounts, financial penalties and costs associated with a security breach, penalties and costs associated with bringing a non-compliant application into compliance, and/or possible disciplinary action of the staff involved - up to and including termination of employment.

E. Use of Third Party Software - The University has spent considerable time and resources developing compliant e-commerce applications (UPay and UMarket) and evaluating various third party solutions to meet unique business needs.

Departments and units whose needs cannot be met through these pre-approved applications must request prior approval from the Associate Vice President for Financial and Business Services before considering or acquiring third party solutions. Third party vendors must provide proof of PCI DSS compliance on an ongoing basis.

F. Hosting Servers- Payment card related websites or software owned or managed by a university department or unit must be hosted on a server certified by a qualified security assessor as well as the IT Compliance Office.

G. Secure Transmissions - To ensure that proper business practices and security are maintained, only secure and approved processes are allowable for transmitting payment card information. Any unapproved processes, including email, are not allowed to transmit or store payment card information.

H. Security Breaches - All known or suspected security breaches of cardholder information must be reported immediately to the Income Accounting and Student Loan Services Office as well as the IT Compliance Office. Please see University of Utah Policy 4-004, University Information Technology Resource Security Policy, for additional reporting requirements. Departments and units must cooperate fully with any resulting investigation.

Sections IV- VII are for user information and are not subject to the approval of the Academic Senate or the Board of Trustees. The Institutional Policy Committee, the Policy Owner, or the Policy Officer may update these sections at any time.

IV. Policies/ Rules, Procedures, Guidelines, Forms and other Related Resources

A. Policies/ Rules

1. R3-070A: Credit Care Guidelines
2. R3-070B: Credit Care Security (PCI DSS) Standards
3. R3-070C: Credit Card Rule – Health Sciences

B. Procedures, Guidelines, and Forms.

1. P3-070A: Credit Care Guidelines (see pages 3 & 4)

C. Other Related Resources.

1. PCI Security Standards Council

V. References

A. Policy 3-051: Banking Policy

B. Policy 4-002: Information Resources Policy

C. Policy 4-003: World Wide Web Resources Policy

D. Policy 4-004: University Information Technology Resource Security Policy

VI. Contacts

The designated contact officials for this regulation are

A. Policy Owner(s) (primary contact person for questions and advice): Controller

B. Policy Officer(s): Vice President for Administrative Services

See Rule 1-001 for information about the roles and authority of policy owners and policy officers.

VII. History

A. Current version. Revision 0

1. Approved by Board of Trustees December 8, 2009 with Effective Date of December 8, 2008.

2. Editorial Revisions

a. Editorially revised August 17, 2022 to move to current template.

b. Editorially revised August 24 2009 to update rules, owner and officer.

B. Renumbering

1. Not Applicable.