Payment Card Policy

University Operations – Financial Management

CWU Policy 202-04

Effective: May 29, 2024

Policy Review Date: YEAR

Policy Executive: Senior Vice President – Finance and Administration

Responsible Office/Unit: Finance and Business Auxiliaries

Policy Statement:

Applicability:

Content:

---

(1) Policy

A. It is the policy of the University to allow acceptance of payment cards as a form of payment for goods and services upon written approval from the financial systems functional manager. The University requires all Merchants that accept payment cards to do so only in compliance with the Payment Card Industry Data Security Standard (PCI DSS) and in accordance with the requirements outlined in this policy document and accompanying procedure.

B. The PCI DSS is a mandated set of requirements agreed upon by the five major credit card companies. These security requirements apply to all transactions surrounding payment cards and the merchants/organizations that accept these cards as forms of payment.

C. This policy and Appendix - Payment Card Procedure provides the requirements for processing, transmission, storage and disposal of cardholder data. This is to reduce the institutional risk associated with the administration of credit card payments by university departments to ensure proper internal controls and compliance with the PCI DSS.

(2) Scope

A. This policy applies to all University entities involved in payment card processing as well as all other external or internal agencies that store, process or transmits cardholder data on behalf of the University.

(3) Authority

A. In accordance with the provisions of the PCI DSS the university is required to implement technical and operational safeguards designed to protect cardholder data.

(4) Roles and Responsibilities

A. The financial systems functional manager is the business owner and approving authority for all merchant accounts and financial transactions and is responsible for the development and enforcement of this policy. The Office of Information Security, in collaboration with major stakeholders, will be involved in the ongoing policy development.

(5) Policy Maintenance

A. The chief information security officer and the financial systems functional manager shall review and recommend any changes to this policy statement at least annually or more frequently as needed to respond to changes in the regulatory environment and internal business practices.

(6) Implementation

A. Failure by an individual to comply with the University payment card policy or procedure may result in disciplinary action up to and including termination for university employees, contract termination in the case of contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion in the case of a student. Violations specific to the PCI DSS may result in:

B. Loss of the department or business unit's ability to accept credit cards as a form of payment; and

C. Fines of up to $500,000 per incident (as imposed by the payment card brand).

D. The University reserves the right to pursue appropriate legal actions as a result of a violation of the University payment card policy.

(7) The financial systems functional manager or other designee through the senior vice president for finance and administration is responsible for this policy and relevant procedure Appendix A.

History:

Responsibility: Finance and Administration; Authority: ELT/UPAC; Reviewed/Endorsed by: ELT/UPAC; Review/Effective Date: 06/04/2014, 05/29/2024; Approved by: A. James Wohlpart, President
Reformatted and Assigned new Policy Number - Previous Policy CWUP 2-70-040, June 2025
Attached Procedure CWUR 7-70-040 as Appendix A, June 2025

Appendix A - Payment Card Procedures

(1) Scope

A. In order to accept credit card payments, the University must prove and maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS). This procedure applies to all University entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. For the intent of this document, a department or other functional unit that has been approved to process payment card transactions is known as a Merchant.

(2) Procedures

A. In the course of doing business at the University it may be necessary for a department or institutional functional area to accept payment cards for payment. The University requires all departments that accept these payments to do so only in compliance with the PCI DSS, CWU 202-04 Payment Card Policy and in accordance with the following procedures.

B. Card Acceptance Handling

1. The opening of a new merchant account for the purpose of accepting and processing payment cards must be approved by the financial systems functional manager before accepting payment cards.

2. Interested departments should contact the Accounting department to begin the process of accepting payment cards. Steps include:

    a. completion of a Merchant Application;

    b. completion of required training; and

    c. reading and sign-off on the Payment Card Processing and Security Agreement, including ensuring ongoing compliance with all requirements of the applicable policies;

3. Each Merchant is responsible for maintaining internal controls that prevent payment card breaches and protect sensitive card holder information. In accepting payment cards, departments acknowledge they are responsible for hiring qualified employees, training employees on proper procedures, and ensuring that their employees adhere to all applicable University policies and procedures.

4. Any Merchant accepting payment cards on behalf of the institution must designate an individual within the department who will have primary authority and responsibility within that department for payment card transactions and PCI DSS compliance requirements. This individual is referred to as the Merchant Department Responsible Person (MDRP). The Merchant must also specify a person of secondary responsibility should matters arise when

the MDRP is unavailable. Any changes in the MDRP or secondary person must be conveyed to the accounting department within 2 business days. This list will be maintained as Attachment 1 to this procedure.

5. Specific details regarding processing and reconciliation will depend upon the method of payment card acceptance and type of merchant account. Detailed instructions will be provided when the merchant account is established and are also available by contacting the Accounting department.

6. All service providers and third party vendors that provide payment card services must be PCI DSS compliant and be on the University approved payment card vendor list. Merchants who contract with third-party service providers must maintain a list that documents their service providers and also:

    a. ensure contracts include language that states that the service provider or third party vendor is PCI DSS complaint and will protect all cardholder data;

    b. annually audit the PCI DSS compliance status of all service providers and third-party vendors with an understanding that a lapse in PCI DSS compliance will result in the termination of the relationship; and

    c. coordinate with the Information Services department for the installation of any software patches, upgrades, or fixes associated with the third-party vendor system(s).

C. Payment Card Data Security

1. The University requires all merchants develop business processes that specifically avoid storing of cardholder data in any form to reduce compliance requirements.

2. E-mail will never be used to transmit payment card or personal payment information, nor will it be accepted as a method to supply such information If payment card data is received in an email then:

    a. the email will be replied to immediately with the payment card number deleted stating that "Central Washington University does not accept payment card data via email as it is not a secure method of transmitting cardholder data"; and

    b. the email will be securely destroyed as per section C.4 below.

3. Fax machines used by a Merchant to receive payment card information must be a standalone machine in a controlled environment with the appropriate physical security controls, as dictated by the PCI DSS. Sending of payment card data using a fax machine is not permitted.
4. University departments who are not Merchants must direct all individuals who pay a bill by credit or debit card to the Cashier’s Office or to its website. At no time will any department direct individuals to general-purpose kiosks for online credit card payments

D. Storage and Destruction

1. Cardholder data, whether collected on paper or electronically, must be protected against unauthorized access at all times. This includes the following requirements:

2. Physical security controls are in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents or electronic files containing cardholder data.

3. No database, electronic file, or other electronic repository of information will store the full contents of any track from the magnetic stripe, or the card-validation code.

4. Portable electronic media devices must never be used to store cardholder data. These devices include, but are not limited to, the following: laptops, compact disks, floppy disks, USB flash drives, personal digital assistants and portable external hard drives.

5. Cardholder data must not be retained any longer than a documented business need, after which it must be deleted or destroyed immediately following the required retention period. The maximum period of time the data may be retained is ninety (90) days. A regular schedule of deleting or destroying data will be established by the Merchant to ensure that no cardholder data is kept beyond the record retention requirements. All cardholder destruction must be in compliance with the PCI DSS.

6. Purchasing Card data must be protected in a similar manner and institute the above components, particularly as it relates to storage and disposal of cardholder data.

E. Reporting of a Security Incident

1. In the event of a breach or suspected breach of security, the Merchant must immediately contact the Security Services department in order to execute the CWU 204-05 Incident Management policy

(3) Procedure Maintenance

A. The chief information security officer and the financial systems functional manager will review and recommend any change to this procedure statement at least annually or more frequently as needed to respond to changes in the regulatory environment and internal business practices.