University Policy Advisory Committee Policy & Procedure Review

Title:	Title: CWUR 7-70-040 Payment Card Policy
Date Submitted:	4/12/2024
Submitted by (Individual):	Brian Holley
Department:	Security Services
Division:	Information Services and Security
Policy Number:	CWUP 2-70-040
Procedure Number:	CWUR 7-70-040

☐ New ☑ Revision

☐ The policy or procedure has been formatted to be consistent with CWUP standards.

The policy and/or procedure change has a budget impact. Yes ☐ No þ
(*If yes, please attach a spread sheet that provides an analysis of the impact.*)

Consultation and Review

Please indicate consultation completed in the preparation of your proposed policy or procedure, including the name of the individual or groups consulted, the date of the consultation, and any written feedback/recommendations from the group consulted.

Date	No Budget Impact	Date	Budget Impact
	Issue-area stakeholders		Issue-area stakeholders
	Provost's Council		Affected budget authority
	Executive Leadership Team		PBAC
	UPAC		Provost's Council
			Executive Leadership Team
			UPAC

Summary of impact: Briefly explain why this policy or procedure has been created/changed.

This procedure has been changed to conform to updated PCI standards.

Summary of policy/procedure:

This procedure defines the requirements for card acceptance handling.

Itemization of changes (revision documents): brief narrative

The update removes some unneeded language and updates the responsible parties.

Policy impact on equity:

1. What does this policy aim to do?

This procedure details the requirements for card acceptance handling.

A. Who benefits from this policy?

The entire university, including students, faculty, staff and administration.

B. Who is left out of this policy?

No one.

2. What are the basic assumptions of this policy?

That appropriate departments will be trained on proper security requirements to handling credit cards..

A. How do these assumptions impact equity?

The ability for a department that is authorized to accept credit cards applies to individuals regardless of race, ethnicity, age, gender, religion, sexual orientation, gender identity, gender expression, disability, economic status and other diverse backgrounds.

For clarification and consultation, contact Dr. Lucinda.Carnell, Interim Vice President of Diversity, Equity, and Inclusion at Lucinda.Carnell@cwu.edu

CWUR 7-70-050 Payment Card Procedures

Reference: CWUP 2-70-040 Payment Card Policy

(1) Scope

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 ~~and/or sensitive authentication 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

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, CWUP 2-70-040 Payment Card Policy and in accordance with the following procedures.

(A) Card Acceptance Handling

The opening of a new merchant account for the purpose of accepting and processing payment cards must~~has to~~ be approved by the ~~Director of Financial Services~~ financial systems functional manager before accepting payment cards. ~~and is done on a case by case basis. No functional area may accept payment cards unless approved by the Director of Financial Services. Any fees associated with the acceptance of the payment card in that unit, will be charged to the unit.~~

1. 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;

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

3. 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 mustshould 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.

4. 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.

5. 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. The current approved vendors list is available on the Security Services web site. 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 shall 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).

(B) Payment Card Data Security

The University requiresrecommends all Merchants develop business processes that specifically avoid storing of cardholder data in any form to reduce compliance requirements. Business processes and procedures that involve the handling and storing of cardholder data must be documented by Merchants and be available for periodic review by the Security Services department. Merchants must have in place the following components in their procedures and ensure that these components are maintained on an ongoing basis:

1. Cardholder data collected are restricted only to those users who need the data to perform their jobs. Each Merchant must maintain a current list of employees with access and review the list monthly to ensure that the list reflects the most current access needed and granted.

2. All equipment used to collect cardholder data is secured against unauthorized use or tampering in accordance with the PCI DSS.

3. E-mail should will never be used to transmit payment card or personal payment information, nor shall will it be accepted as a method to supply such information. In the event that it does occur, disposal as outlined in section C.4 below is critical. If payment card data is received in an email then:

a. the email should 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.

4. Fax machines used by a Merchant to receive payment card information ~~shall~~ 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.

5. ~~All~~ 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~~, unless the kiosk has been specifically identified as authorized to process credit cards.~~

(C) Storage and Destruction

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

1. 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.

2. 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.

3. Portable electronic media devices must~~shall~~ 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.

4. Cardholder data ~~should~~ 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 ~~should~~ 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.

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

(D) Reporting of a Security Incident

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 CWUP 2-70-030 Incident Management policy

(3) Procedure Maintenance

The c~~C~~hief i~~I~~nformation s~~S~~ecurity o~~O~~fficer and the financial systems functional manager~~he Director of Financial Services~~ will~~shall~~ 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.

[Responsibility: Finance and Administration~~President's Office~~; Authority: ELT~~Cabinet~~/UPAC; Reviewed/Endorsed by: ELT~~Cabinet~~/UPAC; Review/Effective Date: 06/04/2014, XX/XX/20XX; Approved by: A. James Wohlpart~~James L. Gaudino~~, President]