Standards for Protecting Payment Card Information (PCI)
University Standards: STN-U5380.01A

Effective: June 9, 2023

Authority

POL-U5380.01 Protecting Payment Card Information (PCI)

See Also

FRM-U5380.01A Authorizing Bank Card Handler – Form

Responsible Department

Policy Owner: Financial Services Director
Responsible Department: Assistant Director, Treasury Services

Purpose of Standards

The purpose of these standards is to outline required internal controls for the handling of payment cards used as a method of receiving payment for goods and services. The controls are designed to prevent and detect the misuse of consumers' bank card information and are to be incorporated into a department PCI plan based on their operations and payment card system.

Definitions

Card Handler
Any individual who receives, processes, or has access to credit or debit card information, or supervises or is responsible for those people who receive, process, or have access to credit or debit card information for the purpose of receiving payments. Anyone who is responsible for point-of-sale devices, as well as Parking Pay Stations (self-service payment devices), is also considered a card handler.

Media
All paper and electronic media (including computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder data.

Payment Cards
Credit or debit cards used as a form of payment.

Point of Sale Device
A hardware system for processing card payments that includes software to read card data either through a chip, magnetic strip and/or near field (RFI) embedded in the card.

Table of Contents

Responsibilities of Department Employees

Department Heads

Department Heads are responsible for:

1. Developing an internal department PCI plan in partnership with Treasury Services to ensure a thorough understanding of the internal control requirements and to provide adequate compliance oversight.

2. Addressing payment card issues and internal control concerns promptly and brought to the attention of Treasury Services when appropriate.

3. Ensuring a physically secured office environment which includes, but not limited to, keeping payment card terminals in a secure location with limited physical access.

4. Responding to Treasury Services in a timely manner regarding credit card company inquiries or related issues.

Authorized Card Handlers

Authorized Card Handlers are responsible for:

1. Complete any training as required by Treasury Services.

2. Following the department's PCI plan and seeking guidance when needed.

3. Promptly reporting payment card issues or internal control concerns to their supervisor.

4. Notifying the Department Head of any perceived internal control concerns that are not addressed by the department plan.

Supervisors of Card Handlers

Supervisors of Card Handlers are responsible for:

1. A thorough understanding of the department's PCI plan to provide adequate compliance oversight of employees under their purview.

2. Promptly reporting payment card issues or internal control concerns to the Department Head, and/or Treasury Services when appropriate.

3. Notifying the Department Head of an internal control concern(s) that are not addressed by the department's PCI plan.

Authorizing Card Handlers

1. Authorization to Handle Credit Card Transactions Required

No employee may process credit card payments without written authorization by Treasury Services. See *Authorization of Card Holders Form* (FRM-U5351.03A). Authorized cardholders are strictly prohibited from allowing unauthorized employees from handling credit cards.

Financial managers may delegate the role of authorizing card handlers to a supervisor via the *Authorizing Card Holders Form* (FRM-U5351.03A). Delegating this role does not relieve the Financial Manager of the responsibilities outlined in these standards.

2. Department Head Ensures PCI Training Completed Prior to Employee Handling Bank Card Transactions

Employees are to complete training as required by Treasury Services. Department heads must wait for notification from Treasury Services before allowing the employee to begin processing bank card transactions.

Failure to complete required training may subject an employee or department to forfeit credit card handling permissions.

3. Department Head to Notify Treasury Services Immediately When an Employee's Log-In Permissions Need to be Removed

If using Transact, or some other system that requires employee log-in permissions to process cards or access card information for refunding purposes, the department head is to notify Treasury Services immediately when an employee is to be terminated or their job duties no longer include using the card system so Treasury Services can remove the employee's permissions and authorization.

For those departments that host their own systems, a permission granting and termination process must be documented in the department's internal PCI plan.

4. Documentation of Authorization Must be Maintained.

The financial manager (or department head) must ensure the *Authorized Card Handler Log*:

a) Lists all authorized card handlers,

b) Is updated when:

   i. New card handlers are authorized, and

   ii. Existing card handlers no longer need access following a change in job functions or their departure from the University.

c) Is uploaded to Treasury Services PCI document library as changes occur, and

d) Is reviewed for accuracy at least annually.

Safeguarding Confidential Financial Information

Certain personally identifiable financial information (PIFI) connected to payment cards is considered confidential financial data under certain privacy and security policies, laws, and regulations and must be sufficiently safeguarded.

Data Classification:

The following data, for the purposes of the University's PCI Program, is **classified as Category 3 Data**:

- The cardholder's first name (or first initial) AND last name, OR a student or employee W#, in combination with one or both of the following:

    - Card account number
    - Card security code

The safeguards listed in pages 6 – 13 of these standards must be implemented when handling the data listed above.

Summary of Safeguards

Activity	**Safeguarding Requirements**
Collection of Data	• Payment card information is to be run through point of sale devices. • Collecting payment card over the phone and entering it into the system is prohibited unless specific authorization is granted by Treasury Services.
Storage of Data	Payment card information is <u>not</u> to be: • Written down or stored on paper or • Entered into an electronic document (e.g., MS Word, Excel) • Photographed
Sharing of Data	Payment card information collected is <u>not</u> to be shared with anyone.
Retention of Data	• Payment card information is not to be retained by a University employee any longer than is required to process a payment transaction. • Card information is not to be retained to process a transaction at a later time. All transaction must be processed promptly.
Disposal of Data	If for unusual circumstances payment card information is written down to assist with the transaction, the paper is to be securely shredded and not tossed in a garbage.

Inspecting and Monitoring Point of Sale Devices

1. <u>Point of Sale (POS) Devices are Inspected and Monitored</u>

A procedure must be developed to ensure POS devices are monitored in accordance with these standards. The procedure is to include:

a) Reviewing POS device inspection logs to ensure the logs are being maintained, and

b) Random inspections of devices are conducted (see #4).

2. <u>POS Devices to be Placed in Location with Limited Access</u>

POS devices must be kept in a location with limited physical access by unauthorized personnel and customers. If limiting access is not possible, devices must be strongly secured to prevent theft and tampering.

3. <u>Devices to be Secured When Worksite is Unattended for Extended Period of Time</u>

When there is an extended period of time during which staff is not present on-site, the financial manager is to ensure all card devices are secured, either out of view when no one in attendance of the device or locked away. Whenever possible devices should be inaccessible to customers when unattended for any length of time.

4. <u>Devices to be Inspected Daily</u>

At the start of each shift, designated staff must:

a) Inspect the device for tampering, including the addition of skimming devices,

b) Verify the serial/model number on the device sticker matches the serial/model number displayed electronically on the device.

c) Verify the serial number of the device against the serial number on the inspection log to ensure it has not been replaced with another device,

d) Verify tamper evident stickers or seals covering screw holes or seams on the device have not been removed, re-affixed or altered in any way.

e) Verify that no foreign object (unfamiliar electronic equipment, device, keypad overlay, wire, or cable) is connected to or placed near the device.

f) Verify that there are no modifications (pry marks, or bent, broken, or stressed seams) to the device.

g) Enter initials and the date and time of the inspection along with any findings on the Inspection log, and

h) Report any suspected anomalies immediately to supervisor.

Throughout their shift, card handlers are to continuously monitor individuals near device for suspicious activity and report any suspicious activity to supervisor.

If anyone who shows up attempting to inspect, replace, or repair a device, the card handler is to verify this with their supervisor before allowing them access to the device.

Exception: Parking staff are to randomly throughout the day inspect the pay stations, minimally, at the beginning of each shift.

5. Supervisor Responsible for Responding to Suspicious Activity Reports

If a card handler reports that they suspect a device(s) has been tampered with or replaced, the supervisor is to:

a) Inspect the device to verify that it has been tampered with or replaced,

b) Immediately remove the device from service if it has, and

c) Notify the Financial Manager (if different from Supervisor) and the PCI Team (pci@wwu.edu).

If notified by a card holder of suspicious behavior or activity of an individual (e.g., person hovering over and handling a device), the supervisor is to:

a) Attempt disrupting the activity or behavior, IF SAFE TO DO SO,

b) Immediately call University Police (x3911) to report,

c) Observe and note description of individual, and

d) Preserve device and location of activity (e.g., area should be secured off for possible fingerprinting).

If notified by an employee that an individual has showed up claiming to need to inspect, replace or repair device, the supervisor (if not aware of any authorization) is to:

a) Ask the individual to stand aside, and

b) Contact Assistant Director, Treasury Services (x3720) for verification.

c) Turn the individual away if Treasury Services states the person has not been authorized to inspect, replace, or repair device.

d) Contact University emergency number (x3911) to report, WHEN SAFE TO DO SO.

6. POS equipment to be Returned to Treasury Services at the Conclusion of Program

The financial manager must ensure that all POS equipment is returned to Treasury Services at the conclusion of a program, and if applicable, for disposal or return purposes.

Completing Card Transactions

1. Transmission of Bank Card Information via Email or Fax is Not Permitted

In the event that a customer submits cardholder data through an insecure channel (e.g, email or fax):

a) Do not process the payment.

b) Notify the customer that the transaction cannot be processed as submitted and request that payment information be re-submitted via an approved method.

c) Remove any copies of cardholder data from your message prior to replying.

d) If you receive cardholder data via fax, securely destroy any messages or documents containing cardholder data.

e) If you receive cardholder data via email (whether from customer or forwarded internally), immediately delete the email then delete again from your trash folder.

2. Only Certain Departments May Accept Bank Card Information Over the Phone

Only departments with written approval from Treasury Services may accept bank card information over the phone. Employees are to check with their supervisor or department head for this authorization before accepting payment information over the phone.

If a department is authorized, employees are to:

a) Process the payments directly into an approved device during the call.

b) Never enter cardholder data directly into a workstation or unapproved device.

c) Do not write payment card infomration on paper for processing at a later time.

3. Online Payments Must be Customer Initiated

Online payments must be customer-initiated and must not be entered online by WWU staff on behalf of a customer (i.e., never use online payment forms to directly enter payment information at the point of sale). Transactions entered by department staff on behalf of a customer must be processed according to telephone payment procedures directly into a payment terminal/device.

Do not instruct customers to use public workstations or unapproved self-service kiosks or laptops.

4. Declined Cards are not to be Re-Processed

If the Card Handler receives a message from the system that a card was “declined,” the employee is **not** to attempt running the card again. If there are technical issues, such as “card error read” or

"chip malfunction" the card may be run again. A "card declined" is not a technical issue. If a declined message is received from the system, the card handler is to:

a) Notify the customer that the card was declined by the card company, and

b) Ask if they have another card to use.

5. <u>Department Must Notify On-Line Customers if Transaction Not Successful</u>

If your system does not automatically send a notification that the transaction was not successful, contact the customer and advise them of the reason for the unsuccessful transaction.

If your system generates an automated declined response, ensure you understand what the automated messages says so you can be sure to follow through with any obligations stated in the message. For example, if the automated message says, "your card has been declined, you will need to use another card to place your order," you will know the next step is on the customer and you are not try the card again.

6. <u>Bank Card Information is not to be Saved</u>

Bank card information (name, credit card number, expiration date, card verification code) is not to be retained on a computer, on paper, or saved to a thumb drive.

If a card system temporarily is unable to accept cards, the employee is to direct them to the nearest ATM.

DO NOT write down customer payment card information to process later.

Processing Refunds

1. Certain Departments May Process Their Own Refunds

Only departments with their own credit card devices or POS systems and departments with third party software that provides the ability to refund within the software may process their own refunds in accordance with the rules below.

Departments or student groups that use a credit card device for a one-time or temporary event or receive payments via eMarkets must request refunds via a General Refund Voucher.

2. Refunds May be Processed Under Certain Circumstances

Refunds may be processed if all of the following conditions are met:

- It is a credit/debit card sale.
- The refund the original transaction is within 6 months of the refund.
- The refund is to the same card as the original transaction.
- Adequate approvals are obtained at the time of the refund (an employee may not refund if there is no other person available to approve or witness the refund and acknowledge the reason for the refund).
- There is a valid reason for the refund. Valid reasons for refunding include the following:
    - Customer changes their mind,
    - Customer was charged too much,
    - There is not enough stock on hand (typically an online payment),
    - Event has been cancelled, or
    - Other reasonably valid reason approved by a supervisor.

3. Refunds Must be Accounted for and Reconciled

Departments may either record their refunds separately from sales or may net them. Departments who choose to net their sales and refunds understand that there is no accounting record of the refunds.

For departments using third party software that provides the ability to process refunds, there must be someone reconciling the payments and refunds recorded in the third party software to the payments actually received and recorded in Banner. It is the department's responsibility to know whether sales, refunds, and fees are netted to arrive at the amounts actually received and recorded in Banner.

Contact Treasury Services if department needs guidance on how to record the refunds separately from the sales.

4. <u>Documentation of Internal Controls Required for Refund Transactions</u>

For all refunds, the department must maintain evidence that they took the necessary steps to ensure the proper processing of refunds. The department must maintain the evidence for the standard six plus current year archiving standards.

Typical evidence would be a printed original receipt along with the printed refund with initials from two employees – one who is authorized by the department to approve refunds – and the reason for the refund. Other forms of evidence may be acceptable but must be reviewed by Treasury Services for adequacy.

Treasury Services Responsibilities

Treasury Service is responsible for:

1. Implementing updates and overseeing compliance with this standard and the PCI policy,
2. Leading the annual SAQ filing process,
3. Establishing and closing merchant accounts. A merchant account is a type of bank account that allows businesses to accept payments by debit or credit card,
4. Establishing and maintaining relationships with the credit card payment processing providers and issuing banks,
5. Approving any Point of Sale (POS) device or system to be used within the University,
6. Providing advice and recommendations to departments to define the methods of transacting online payments on behalf of the University,
7. Engaging a PCI Qualified Security Assessor in consultation with Information Security Office,
8. Maintaining an inventory of all Western departments that process credit card transactions using a Western approved merchant account including all related devices,
9. Together with Information Security Office and Qualified Security Assessor (QSA), coordinate review of network segmentation configurations and other technical safeguards,
10. Together with Information Security Office, coordinate with Compliance Services and/or Internal Audit to monitor and audit compliance with this standard,
11. Creating PCI training/education,
12. Enforcing this standard including immediate suspension or termination of the ability to process or store credit cards if a school or department fails to comply with this standard or the PCI Standard, and
13. Other duties related to PCI Compliance as determined by the University.

Treasury Services, at its discretion, may revoke a merchant account immediately for failure to comply with this standard or the PCI Standard. Revocation of a merchant account will preclude the school or department from being able to process credit or debit cards.

Information Security Office Responsibilities

The Information Security Office is responsible for:

1. Participating in annual SAQ filing process,
2. Establishing and maintaining an information technology security policy,
3. Assisting Treasury Services, colleges, and departments to identify devices in the PCI DSS scope and ensuring appropriate network segmentation is implemented to protect the card data environment (CDE),
4. Working with Treasury Services, colleges, and departments to ensure appropriate PCI DSS security controls are implemented for devices within the CDE.
5. Conducting appropriate vulnerability scanning of Western systems that transmit, generate or otherwise access credit card information,
6. Performing other monitoring and reviews of computer and/or computer networks to ensure that CDE security controls are in place and are adequate to protect credit card data,
7. Initiating investigations relating to security incidents, and
8. Working with compliance owners on any notifications or disclosures required under law or regulation as a result of a security incident.