FINANCIAL ACCOUNTING
UNIVERSITY of WASHINGTON
Merchant Services

OMS STANDARD – MERCHANT RESPONSIBILITIES

Applicability: University of Washington

Standard Title: OMS Standard – Merchant Responsibilities

PURPOSE

This standard establishes the responsibilities required of all UW Merchants accepting payment cards. All University merchants are required to comply with this standard, and the Payment Card Industry Data Security Standard (PCI-DSS), in accordance with Administrative Policy Statement APS 35.1.

SCOPE

This statement applies to any University merchant accepting payment cards.

REQUIREMENTS

GENERAL

- Merchants must document, maintain, and train employees on Payment Card operations procedures for their area.
- Merchants must define and document a departmental policy for processing customer refunds.
- Merchants must ensure that Merchant ID (MID) information maintained by OMS is current and accurate at all times (e.g. contact information changes, Workday Finance Worktag changes, device location changes, etc.).
- Merchants must participate in PCI assessments conducted by OMS.
- Merchants must notify OMS if their Merchant Account is seasonal (one-time or date specific events). All Merchant Accounts will be closed after 18 months of inactivity unless an exemption is on file.

BREACH AND INCIDENT NOTIFICATIONS

- Merchants must notify OMS immediately when made aware of any possible breach involving cardholder data, either internally, or through a Third-Party Service Provider (TPSP).
- Merchants must notify OMS immediately of suspicious activity on any e-commerce site. For example, numerous repeated low-cost transactions (card testing attack).
- Merchants must notify OMS immediately of any theft of or suspected tampering of credit card terminals or devices.

EMPLOYEE/USER ACCESS

- All employees who process payment cards must complete UW PCI Training. This training must be renewed annually.
- Access to payment card data, equipment, and/or other devices in scope for Payment Card Industry Data Security Standard (PCI-DSS) must only be given to employees designated and trained in handling payment cards.
- Employees using point of sale (POS) devices for payment card processing must use their own unique ID and password to access the equipment. Sharing passwords or accounts is forbidden.
- When an employee is terminated or is no longer involved with payment card acceptance, the merchant must ensure access is removed immediately from all payment card environments including, but not limited to:

  - TouchNet MarketPlace (uStores & uPay) or other e-Commerce Web Portals.
  - Payment processor, gateways, and their reporting systems (FiServ/Clientline, American Express, Heartland/TouchNet, etc.).
  - 3rd Party Software or Point of Sale Devices (Clover, Volante, etc.).
- A current and accurate list of employees that store, process, or transmit payment card data must be kept by the Merchant Responsible Person (MRP) including hire/termination dates, training history, and the employee's roles (e.g., cashier, manager, supervisor, accountant, etc.) and responsibilities regarding payment card processing.

DEVICES

- An inventory of all payment card devices must be maintained by the merchant, to include serial number, location of the device, purchase date, and other identifiers.
  - The inventory must be updated when adding, relocating, or decommissioning any payment card devices.
  - The inventory must be verified annually.
- New or replacement payment card terminals must be requested through OMS or through the applicable 3rd Party vendor.
  - If through the applicable 3rd party, OMS must be notified.
- All default passwords on payment card devices must be changed upon implementation.
- Device Inspections:
  - Payment card devices must be regularly inspected for skimming devices and/or other physical tampering.
    - Recommended – at the start of each shift using the device.
  - Inspections must be logged on the OMS inspection form at least monthly.

DATA RETENTION

- The security code (CAV2, CID, CVC2, and CVV2) and the expiration date must never be stored on paper or electronically after authorization.
- Only the last four digits of the payment card number may be retained after authorization.
- All paper forms used to collect payment card data must be formatted so that the data can be easily redacted or removed for cross-cut shredding.
- Forms that are appropriately redacted or truncated may be retained according to the appropriate retention schedule. Contact Records Management Services for information pertaining to your department (website in the links section at the end of the document).
- Payment terminal inspection logs should be kept for the last full calendar year plus the current year.
- Secure storage:
  - Physical Payment Card Data may only be stored temporarily (not to exceed one business day). Authorization should occur as soon as possible.
  - Un-redacted Payment Card Data may only be stored in a secured, locked area, with limited access, prior to authorization. Payment Card data must never be stored in any form following authorization.
  - Un-redacted payment card data must never be sent to record storage facilities.
  - All payment card receipts may be kept for up to one year, unless otherwise specified by law for longer storage (e.g., grants, donations, research, etc.). Contact records management services for information pertaining to your department.
  - Electronic Payment Card Data may only be stored through an OMS approved TPSP utilizing tokenization.

  - Electronic Payment Card Data must not be stored on any University device or network including but not limited to the following:
    - Applications or programs that run on a desktop, laptop, mobile device or server.
    - Jump Drives, Flash Drives, or other removable media.
    - Electronic documents (e.g., email, spreadsheets, databases, etc.)

MERCHANT RESPONSIBILITIES

The merchant will:

- Keep OMS up to date on any changes to personnel in positions that can have an impact on PCI.
  - New and leaving employees.
  - Enrollment of new employees into PCI training.
- Keep OMS up to date on any changes to device inventory to include:
  - Make and model.
  - Serial number.
  - Device location.
- Perform periodic inspections of the device to detect tampering or substitution of the device:
  - Verify the serial number matches inventory.
  - Appearance of device has not changed since last inspection.
  - Devices in less secure areas should be inspected more frequently.
    - The device should be visually inspected before and after daily use. The documented inspection should be completed and logged at least monthly.
  - Contact OMS (pcihelp@uw.edu) if any devices appear to have been tampered with.
- Keep OMS up to date on changes to Merchant and TPSP contacts.
  - Any change to name, email, or phone number of primary and secondary contacts should be communicated to OMS.
- Notify OMS of and verify TPSP continuing compliance with PCI DSS:
  - Annually – Merchant will obtain a new or updated Attestation of Compliance (AOC) from the TPSP.
  - Notice of upcoming contract expiration or renewals.

OMS RESPONSIBILITIES

OMS will:

- Record the initial merchant information, TPSP, and device inventory into the OMS database to include:
  - MID.
  - Attestation of Compliance (AOC) information, including expiration
  - Contract information, including expiration.
  - Device inventory.
  - Register devices on campus wi-fi as necessary.
- Assist Merchant and TPSP with implementation:
  - Provide implementation information from our payment processor – FiServ.
  - Order necessary payment card terminals from contracted vendors if applicable.
- Provide notices of upcoming deadlines and events:
  - AOC expiration.
  - Annual compliance assessment.

- Conduct regular compliance assessments and advise Merchants on results.
- Communicate changes to PCI-DSS and related issues to Merchants through Merchant Services Digest.

LINKS

- Office of Merchant Services

  https://finance.uw.edu/merchant-services/

- UW Records Management Services

  https://finance.uw.edu/recmgt/home

- OMS Glossary

  https://finance.uw.edu/merchant-services/resources/glossary

- Payment Card Acceptance Administrative Policy Statement:

  http://www.washington.edu/admin/rules/policies/APS/35.01.html

- Payment Card Industry Data Security Standard (PCI DSS) 3.2.1:

  https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

ADMINISTRATIVE INFORMATION

Version: 1.4

Superseded Standards: None

Date Established: September 9, 2019

Date Effective: April 5, 2022

Next Review Date: April 1, 2026

Contact: Office of Merchant Services – pcihelp@uw.edu

https://finance.uw.edu/merchant-services/

Change Log:

Date	Version	
9/9/19	v1.0	First Publication
9/24/19	v1.1	Update to device inventory information
4/4/22	v1.2	Minor updates and inclusion of FiServ information
3/19/24	v1.3	Breach and Incident notification added
4/08/24	v1.4	Merchant and OMS responsibilities lists added