OMS COMBINED STANDARDS DOCUMENT

STANDARDS

PURPOSE AND SCOPE

PURPOSE

This document outlines the procedures and guidelines for accepting payment cards in compliance with Payment Card Industry Data Security Standards (PCI-DSS) and UW Administrative Policy Statement (APS) 35.1. It establishes and defines the responsibilities and requirements for all UW Merchants and Third-Party Service Providers (TPSP) involved in storing, processing, or transmitting payment card data. All merchants and TPSPs must adhere to PCI-DSS standards and APS 35.1. This document also details the process for becoming a UW merchant and outlines the steps for implementing and reviewing new TPSPs.

SCOPE

This applies to the University of Washington Enterprise, including all campuses, UW Medicine and any other areas where payment cards are accepted.

POLICY EXEMPTIONS

There are no exemptions to PCI Compliance. The University is contractually obligated to be PCI Compliant. Merchants may ask for an exemption to an OMS policy, procedure, or standard; but must prove in doing so they remain PCI Compliant. Merchants requesting an exemption will complete the Exemption Request in Appendix D: Links and return to pcihelp@uw.edu. Exemptions to OMS policies, procedures or standards must be approved by the Director or Assistant Director.

All exemptions are reviewed on a case-by-case basis and will be reevaluated annually

A Merchant requesting an exemption may be required for the first year to cover the cost of a full attestation through the University's Qualified Security Assessor. After the first year, provided the merchant passes attestation, OMS staff will conduct follow-up reviews. Any merchant found not in compliance after this full attestation must become compliant within 90 days.

ACCEPTING PAYMENTS

GENERAL

- All merchants will accept
  - American Express
  - Discover
  - Visa
  - MasterCard
- Approved methods of accepting payments
  - Card Present (In-Person)
  - Mail Payments
  - Telephone Payments
  - E-commerce
- Protecting Card Holder Data (CHD)
  - CHD must never be stored electronically.
  - Payment terminals must be a PCI Security Standards Council certified P2PE (Point to Point Encryption) solution and comply with the EMV (chip) standard.
  - Written payment card data must be authorized within one business day of receipt. Any written payment card data that is kept overnight must be locked in a secure area with limited, need-to-know access.
    - After the transaction is authorized, the three digit security code, expiration date, and all but the last four digits of the payment card number must be redacted appropriately or removed from the form and cross-cut shredded.
    - See also: Data Retention

CARD PRESENT (IN PERSON)

- In-person (Cashier Assisted)
  - Every effort must be made to ensure that customers tap, insert or swipe their own payment card or NFC-enabled device (e.g. iPhone, Android phone, Apple Watch, etc.) using the P2PE-compliant terminal.
  - For one-time or special events, OMS has P2PE terminals available for rent.
- Self-service Kiosk
  - When the Kiosk is equipped with an external (customer-facing) P2PE terminal, the device must be physically affixed to the kiosk to prevent tampering or unauthorized removal.
  - P2PE terminals must be inspected daily for tampering, and results documented using an OMS Inspection Log.

    - For added security, it is recommended the Kiosk be physically secured to a wall, floor, etc.
- Near Field Communication (NFC)
    - When the Point-of-Sale devices support it, merchants must accept NFC payments.
        - Examples of NFC: Google Pay, ApplePay, Samsung Pay, etc.

MAIL PAYMENTS

- Mail payments must be processed through an OMS-approved lockbox provider, or via a Merchant Services-approved process that meets PCI DSS requirements.

TELEPHONE PAYMENTS

- Phone payments may be accepted through the following methods:
    - Pass the transaction to a 3rd party Interactive Voice Response (IVR) system approved by OMS
        - Calls originating from an unsecured line (not using IVR) cannot be transferred. Customers must either be instructed to call a secure payment phone line (number) or be called back from a secure payment phone line.
        - Approved IVR systems
            - Campus – PCI Pal
            - UW Medicine – Sycurio
    - Analog phone line and approved P2PE device
    - Any alternative methods must be preapproved by OMS
- Call recording must be disabled on lines used to accept payments.

E-COMMERCE

- E-commerce transactions are cardholder-initiated transactions via the web.
- All E-commerce activity must be conducted through an OMS approved E-commerce application.
- All E-commerce merchants (excluding TouchNet stores) must pass monthly vulnerability scans conducted by OMS' approved scanning vendor (CampusGuard/Qualys).
- University employees are prohibited from processing transactions on behalf of the cardholder through any e-commerce application.
- E-commerce sites must implement CAPTCHA to mitigate the risk of fraudulent card testing which may result in financial and reputational loss to the Merchant and University.
- E-commerce sites must display their contact email address and refund policy on their website and checkout page

- If ACH is offered as a payment option, It must be processed through an OMS-approved e-commerce platform.

PROHIBITED FORMS OF PAYMENTS

FAX PAYMENTS

- Do not process any payment information via fax.
- Contact the customer and arrange an OMS-approved method of payment.
- Cross-cut shred any physical paper copies immediately.
- Do not print the fax if delivered electronically (eFax).
- If received on a physical fax machine, delete the fax from the device and any connected network storage (you may need to contact IT support to ensure complete deletion),
- If received via eFax, the eFax email must be deleted immediately from the email inbox and deleted items folder.

E-MAIL PAYMENTS

- Do not process any payment received through e-mail.
- Do not print the e-mail.
- Contact the customer and arrange an OMS-approved method of payment.
- The email must be deleted immediately from the email inbox and the deleted items folder.

VOICEMAIL PAYMENTS

- Do not process the payment.
- Contact the customer and arrange an OMS-approved method of payment.
- The voicemail must be deleted immediately from the voicemail inbox and the deleted items folder.

SMS/TEXT MESSAGE PAYMENTS

- Do not process the payment.
- Contact the customer and arrange an OMS-approved method of payment.
- The message must be deleted immediately from the device and message history.

CHARGING CONVENIENCE/SURCHARGE/SERVICE FEES

- UW Merchants are not permitted to charge convenience or surcharge fees unless provided an exemption from OMS.

- Merchants may enroll in card brand tuition service fee programs such as the Visa Government and Education Program through an OMS approved platform such as Touchnet PayPath.

MERCHANT RESPONSIBILITIES

GENERAL

- Merchants must ensure that MID information maintained by OMS is current and accurate at all times (e.g. contact information changes, Workday Finance Worktag changes, P2PE 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 approved exemption is on file.
- Merchants will ensure non-centrally managed vendors default passwords are changed and unnecessary default accounts are disabled or removed before installing the system on the network.

BREACH AND INCIDENT NOTIFICATIONS

- Merchants must notify OMS immediately when made aware of any possible breach involving cardholder data, either internally, or through a TPSP.
- Merchants must notify OMS immediately of suspicious activity on any e-commerce site. For example, unexpected repetitive low-dollar 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 or may impact the security of the cardholder environment, must complete annual UW PCI Training.
- Access to payment card data, equipment, and other devices in scope for PCI-DSS must only be given to employees designated and trained in handling payment cards.
- Employees using point of sale (POS) devices must be assigned a unique ID and password to access the device. Password or account sharing is strictly prohibited.
- When an employee is terminated or no longer involved in payment card processing, the merchant must immediately revoke access to all payment card environments, including, but not limited to:

- TouchNet MarketPlace (uStores and uPay) or other e-Commerce Web Portals.
- Payment processor, gateways, and their reporting systems (e.g. FiServ/Clientline, American Express, Heartland/TouchNet, Authorize.Net, CardConnect, etc.).
- 3rd Party Software or Point of Sale Devices (Clover, Volante, etc.).

- The Merchant Responsible Person (MRP), must maintain a current and accurate list of all employees who store, process, or transmit payment card data. This list must include:
  - Hire and termination dates
  - Training history
  - Employee roles (e.g., cashier, manager, supervisor, accountant)
  - Responsibilities related to payment card processing (e.g., payment acceptance, order fulfillment, reconciliation)
- All employees must log into merchant accounts at least once monthly to avoid suspension due to inactivity: e.g. Touchnet, ClientLine (FiServ/Amex), Cvent, etc.

DEVICES

- Merchants must maintain an up-to-date inventory of all payment card devices.
  - Device Information (minimum information required)
    - Model (e.g. Clover Flex 3rd Gen, Ingenico iPP320, etc.)
    - Serial number
    - Physical Location
    - Purchase date
  - The inventory must be updated whenever devices are added, relocated, or decommissioned.
  - Inventory must be verified annually.
- All new or replacement payment card devices must be:
  - Requested through OMS, or
  - Procured via an OMS-approved 3rd Party vendor (e.g. Volante, HP24, etc.)
    - Review all requests with OMS prior to purchase.
    - Provide OMS with retired and replacement device information.
  - Default passwords on payment card devices must be changed upon implementation.
- Device Inspections:
  - Payment card devices must be regularly inspected to ensure integrity and security:
    - Check for skimming devices and/or other physical tampering.
    - Verify serial numbers or other identifying information to ensure devices have not been swapped.
  - All inspections must be logged (electronic or paper). A sample Payment Terminal Inspection Log is available in the Appendix D: Links and on the OMS website

- Inspection Frequency is determined by device location and usage rate.
  - Usage Frequency Samples:
    - Public (e.g. cafeteria) – start of each shift
    - Public and behind a partition (e.g. ticket office) - start of each shift or a minimum of daily
    - Restricted access room or office – weekly
    - In storage: – monthly
- If any evidence of tampering is found, contact OMS (pcihelp@uw.edu) immediately.

REQUIRED DOCUMENTATION

- For each vendor (TPSP) used, Merchants must assist in obtaining the following:
  - Active contract including a signed PCI Compliance Rider.
  - Annual PCI DSS Attestation of Compliance (AOC) and Responsibility Matrix (or equivalents)
  - Dataflow diagram outlining how Card Holder Data moves through UW and vendor networks
- Merchants are required to maintain the following documentation:
  - Departmental payment acceptance process/policy that includes (e.g. Credit Card Handling Policy or Cash Handling Policy):
    - Card acceptance processes
    - Training requirements
    - Refund policy
    - Emergency downtime policy (e.g., “payments not accepted during downtime”)
    - Employees must complete annual acknowledgement of the process/policy
  - Payment Flow diagram or equivalent for each applicable payment channel (e.g. in-person, mail, phone, e-commerce, etc.)
  - Device inspection logs for P2PE payment devices

DATA RETENTION

- Physical Payment Card Data (e.g. written, paper form, etc.)
  - All paper forms used to collect payment card data must be designed to allow easy redaction or removal for crosscut shredding.
  - The security code (CAV2, CID, CVC2, and CVV2) and the expiration date must never be stored on paper or electronically after authorization.
  - After authorization, only the last four digits of the payment card number may be retained.

    - Redacted or truncated forms may be retained. Contact Records Management Services for information pertaining to your department records retention schedule (website in the links section at the end of the document).
- Payment terminal inspection logs must be retained for the previous 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.
    - Prior to authorization, un-redacted Payment Card Data must only be stored in a secured, locked area, with limited access. 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.
    - 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.
            - Removable media (e.g. Jump Drives, Flash Drives, etc.)
            - Electronic documents, including, but not limited to emails, spreadsheets, databases, etc.

MERCHANT ONBOARDING AND MAINTENANCE PROCESSES

BECOMING A MERCHANT

To accept payment cards, a University of Washington entity must first apply through the OMS for a University approved payment processor MID. Prior to applying, a prospective merchant must review PCI DSS rules and familiarize themselves with the Merchant Responsibility requirements.

The prospective University merchant should have the following information prior to applying:

- Merchant Account Details (Note: this information will appear on all customer receipts)
  - DBA name – Review Appendix: DBA Naming Convention
  - Customer Service phone number
  - Physical Address
- Assign a Merchant Responsible Person (MRP) who is responsible for ensuring OMS policies, procedures and standards are followed (e.g. device inventory and inspection, PCI Assessments, merchant issues, etc.).
  - Name
  - Phone number
  - UW Email Address
  - This MUST be a person and not a departmental account
- Fiscal contact name, phone number and UW Email address if different from the MRP.
- Business purpose for accepting payment cards.
  - If the business purpose of the merchant is to facilitate the collection of donations, merchant applications require review and approval from Advancement Operations – please contact Gift Services at 5-9860 or email giftdata@uw.edu
- Workday Worktags assigned to your Merchant Profile
  - Cost Center (CC): Required
  - Resource Code (RS): Required
  - Revenue Category (RC): Required
    - Cannot be “Other Revenue (RC2237)”.
    - If the department does not have a preference, use one of the following, based on the nature of your department:
      - RC4131 - Merchant Receipts - Auxiliary Departments
        RC4130 - Merchant Receipts - Educational Departments
  - Program (PG): – Optional

  - Credit Ledger Account: Optional
  - PLEASE NOTE:
    - Credit Card related fees and Merchant Service Fees are posted to the same Worktags designated for revenue.
    - A MID may only be associated with one set of Worktags.
- A list of products and /or services that will be offered including:
  - The estimated average dollar amount per sale
  - The estimated highest dollar amount per sale
  - The estimated number of highest dollar sales the prospective merchant will have annually
  - The estimated dollar amount of average monthly sales
  - The estimated dollar amount of annual sales
- Hours of operation
- Months of operation if seasonal
- Method of payment acceptance. Due to payment card requirements, you may have to open separate MIDS for each form of payment acceptance.
  - E-commerce
  - Card Present
  - Mail or Telephone
- For e-commerce, your request to be a merchant will be forwarded to our e-commerce team to begin our TouchNet evaluation process.
- For all prospective merchants accepting payment cards in-person (Point of Sale or Self-service Kiosk) or in card-not-present situations (mail, donation form, or phone), a P2PE payment card terminal must be used.

ACCOUNTING ERROR HANDLING

WORKDAY WORKTAG ERROR RESOLUTION PROCESS

In the event of an error in daily processing due to the Workday Worktags provided by a merchant, OMS will make every effort to contact the merchant and resolve the issue that business day.

To minimize disruption to daily business operations, if the issue cannot be resolved by close of business on the day it is discovered, OMS will resubmit processing using the Cost Center and Resource Code on file for the merchant. All corrections will be documented, and the merchant will be notified of the changes made to their Merchant Profile.

Merchant Services is not responsible for fixing transactions in Workday that were submitted with incorrect or invalid worktags. It is the responsibility of the Merchant's Shared Environment team to make these corrections.

THIRD PARTY SERVICE PROVIDERS (TPSP)

REQUESTING A NEW TPSP

Engaging with OMS does not remove the responsibility of the department to engage with Procurement, IT departments, and any other areas within the University necessary to complete a contract with a TPSP. Per Procurement Services policy, departments must receive approval from Merchant Services before contracting for any payment card acceptance related equipment or services. This requirement applies to orders for ANY dollar amount.

Note: The overall process from request to approval, including the consultation, may take up to 30 days depending on the availability of needed information and the current workload of OMS.

- The merchant will submit a Vendor Information Form to OMS via pcihelp@uw.edu
- OMS and the merchant will perform an initial consultation with the merchant
    - A review of the business case for adding the new TPSP
    - A review of existing contracts with the TPSP or duplication of service currently provided through existing tools
- If no contract or duplicate service exists, OMS and the merchant will begin gathering additional data and add it to the Vendor Information Form and OMS vendor database
- OMS will decide on how to proceed and provide rationale with one of the following courses of action:
    - Engage with new TPSP
    - Consolidate into existing contract with requested TPSP
    - Consolidate into existing contract with different TPSP
    - Do not proceed

REQUIREMENTS

- University merchants must receive approval from OMS prior to contracting with any TPSPs.

- TPSP provided applications must integrate with OMS approved Payment Processor University/State contracted payment processor. TPSP provided applications must be PA-DSS (Payment Application Data Security Standard) compliant.
- TPSP must provide a current AOC and a PCI Responsibility Matrix to OMS annually or upon request.
- TPSP provided terminals must be a PCI Council certified P2PE solution and must comply with the EMV standard.
- TPSP contracts must include the PCI Compliance Rider
- Keep OMS up to date on changes.
    - Any change to name, email, or phone number of primary and secondary contacts should be communicated to OMS.
    - Notice of upcoming contract expiration or renewals

APPENDICES

APPENDIX A: DBA NAMING CONVENTION

To maintain consistency in naming, a merchant will use the following convention when creating a DBA name:

- Maximum of 24 characters including spaces
- Numbers, spaces, hyphens, and capital letters only
- Begin your DBA with a location identifier from the following list
    - UWMC Locations:
        - UWMC
        - UWP
        - UWNC *(UW Neighborhood Clinic)*
        - HMC
        - NWHMC *(Northwest Hospital Medical Center)*
    - UWB *(UW Bothell)*
    - UWT *(UW Tacoma)*
    - All other locations on Campus
        - UW

Examples:

- UWMC PLAZA CAFE
- UWMC TRIANGLE GARAGE
- UWB COFFEE SHOP
- UW GATEHOUSE 2-1
- UW SOM SURGERY
- UW SOD *(School of Dentistry)*

APPENDIX B: GLOSSARY

ACRONYMS

- AOC – Attestation of Compliance
- CDE – Cardholder Data Environment
- DBA - Doing Business As
- MID - Merchant Identification Number
- MRP - Merchant Responsible Person
- PCI-DSS - Payment Card Industry Data Security Standard
- QSA - Qualified Security Assessor
- ROC - Report on Compliance
- SAQ - Self-Assessment Questionnaire
- TPSP - Third Party Service Provider

DEFINITIONS

Acquirer (or processor) - The financial institution that processes payment card transactions for merchants and is defined by a payment brand as an acquirer. The University of Washington is transitioning from Elavon to Fiserv as our Payment Acquirer.

Attestation of Compliance (AOC) - The Attestation of Compliance is a form for merchants and service providers to attest to the results of a PCI DSS assessment. An AOC is valid for one year (validity dates are included in the form).

Breach (data breach) - A data breach is any security incident in which unauthorized parties gain access to sensitive or confidential information, including personal data (Social Security numbers, credit card numbers, healthcare data) or corporate data (customer data records, intellectual property, financial information).

Card Skimmer - A device installed on a card reader that captures and/or stores the information from a payment card.

Cardholder Data - The full primary account number. Data considered cardholder data when stored along with primary account number include the cardholder name, expiration date, and/or service code.

Cardholder Data Environment (CDE) - The people, processes, and technology that store, process or transmit cardholder data or sensitive authentication data.

Chargeback - A chargeback is a forced transaction reversal in response to a claim of fraud or transaction dispute made by the cardholder. It is the responsibility of the Merchant to investigate the chargeback and confirm whether the chargeback is valid or not.

Credit Card Handling Policy - Outlines the specific procedures and practices an organization must follow to accept payments and securely handle credit card information.

Compromise - Unauthorized disclosure or theft, modification, or destruction of cardholder data.

Convenience fees - Convenience Fees are forms of an alternative payment channel. In other words, if you take a face-to-face payment, you can charge a convenience fee by offering payments online, mail and/or phone. A great example of a convenience fee is a movie theatre ticket. If you buy a ticket in person, there is no fee. If you buy online or via a phone app, there is usually a charge. This charge is a set fee as per Visa's rules it cannot be a percentage. The fee must be properly disclosed and cannot be used for recurring payments.

Doing Business As (DBA) - The operating name of a company, as opposed to the legal name of the company. Washington state law requires all businesses file a DBA when they are using a name other than their legal name (the name used to form the business).

EMV - "Europay, Mastercard, and Visa" – Payment cards that comply with the EMV standard are often called Chip and PIN or Chip and Signature cards. EMV uses embedded microchips on cards to generate unique transaction codes, making them more secure than traditional magnetic stripe cards.

Gateway - Authorizes credit card processing for e-commerce transactions.

Issuer - An entity that issues the payment cards.

Merchant - Any college, school, unit, department, or organization at the University that accepts credit cards as a form of payment for goods and/or services. This includes temporary, seasonal, or one-time events. This includes acceptance of credit cards in any form be it mail, phone, online, or in-person.

Merchant Identification Number (MID) - The account number assigned to University merchants associated with processing credit card payments

Merchant Profile – The collection of merchant information used for accounting purposes and Workday integrations. Includes MIDs, Workday Worktags, Bank Codes.

Merchant Responsible Person (MRP) - A local, designated individual whose role focuses on ensuring the secure, compliant, and efficient handling of credit card transactions. An MRP is required for each MID.

Payment Application - A software application that stores, processes or transmits cardholder data.

Payment Cards - Any credit card, debit card, or pre-paid card with a brand logo on it, such as VISA, MasterCard, American Express, Discover, JCB International, etc.

Payment Card Industry Data Security Standard (PCI DSS) - The security standard established by the major card brands (Mastercard, Visa, American Express, etc)

Qualified Security Assessor (QSA) - Qualified Security Assessor companies are independent security organizations that have been qualified by the PCI Security Standards Council to validate an entity's adherence to PCI DSS. QSA Employees are individuals who are employed by a QSA Company and have satisfied and continue to satisfy all QSA Requirements. The University of Washington has contracted with Campus Guard as our QSA.

Report on Compliance (ROC) - The formal document the QSA fills out as a result of the annual assessment. Very detailed, and considered confidential.

SAFE-T - SAFE-T is Elavon's Point-to-Point Encryption solution (P2PE). P2PE encrypts the card number at the device, vastly reducing the overall risk landscape for the University and making it far easier to attest to PCI DSS.

Self-Assessment Questionnaire (SAQ) - Reporting tool used to document self-assessment results from a PCI DSS assessment.

Sensitive Authentication Data - Security-related information that is used to authenticate cardholders and/or authorize payments. This information can include card validation codes/values, full track data, and PINs.

Service Fees - The service fee program is a special program restricted to government and education. Education payments must be tuition, tuition-related, and/or room and board. You must be registered in the Visa Service Program to charge the service fee and require a separate merchant ID for the collection of said fees. These service fees can be charged in-person as well as online or mail-order/telephone.

Service Provider - A business entity (not a payment brand) directly involved in the processing, storing, or transmission of cardholder data on behalf of another entity.

Surcharge - Surcharges only apply to credit cards (no debit). Visa, MasterCard, and our merchant processor must be notified 30 days prior to beginning the surcharge. A surcharge must be disclosed (true for all fee types) and listed on the receipt. The amount is limited to the merchant discount rate and cannot exceed 4%. Certain states and banks do not allow surcharging, although Washington currently does.

Third Party Service Provider (TPSP) - Any business entity that is not a payment brand, directly involved in the processing, storage or transmission of cardholder data on behalf of another entity.

APPENDIX D: UNIVERSITY PROCARDS (P-CARD)

Internal payment cards, also known as corporate cards, purchasing cards or ProCards, are not subject to Payment Card Industry Data Security Standard (PCI DSS) compliance because they are considered internal accounts, while PCI DSS primarily focuses on protecting external customer payment data.

Also note, UW ProCards are not allowed to be used to purchase goods or services from other UW departments. As UW merchants, you should not knowingly accept payments from other UW departments via ProCard. The ProCard Allowable and Unallowable Purchases can be found in Appendix D: Links

APPENDIX E: LINKS

- Office of Merchant Services
  - https://finance.uw.edu/merchant-services/
- 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) 4.0.1:
  - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf
- EMV Standard
  - https://www.emvco.com/
- Payment Terminal Inspection Log
  - https://finance.uw.edu/merchant-services/sites/default/files/Uploads/oms-device-inventory-inspection-log.xlsx
- Example Credit Card Handling Policy
  - https://finance.uw.edu/merchant-services/files/Uploads/Example-Credit-Card-Handling-Policy.docx
- Vendor Information Form
  - https://finance.uw.edu/merchant-services/sites/default/files/Uploads/oms-form-tpsp-vendor-info.docx
- Exemption Request Form
  - https://finance.uw.edu/merchant-services/sites/default/files/Uploads/oms-form-exemption-request.docx
- University of Washington General Terms and Conditions
  - https://finance.uw.edu/ps/suppliers/terms-conditions
- PCI Compliance Rider
  - https://finance.uw.edu/ps/sites/default/files/purchmanual/index_files/UW_PCI_Rider_4-20-2020%20%284%29.pdf
- OMS Records Retention Schedule
  - https://finance.uw.edu/recmgt/depts/091302
- ProCard Allowable/Unallowable Purchases
  - https://finance.uw.edu/ps/sites/default/files/allowable_unallowable_April_2024.pdf

ADMINISTRATIVE INFORMATION

Applicability: University of Washington, UW Medicine

Guidance Title: OMS Combined Standards Document

Version: 1.0

Superseded Standards: None

Date Established: June 30, 2025

Date Effective: June 30, 2025

Next Review Date: June 30, 2026

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

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

Send Feedback

mailto:pcihelp@uw.edu?subject=OMS%20Combined%20Standard%20Feedback

Change Log:

Date	Version	
6/30/2025	v1.0	Combined OMS policy document