FINANCIAL ACCOUNTING
UNIVERSITY of WASHINGTON
Merchant Services

OMS STANDARD – ACCEPTING PAYMENTS

Applicability: University of Washington

Standard Title: OMS Standard – Accepting Payments

PURPOSE

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

SCOPE

This standard applies to any University merchant accepting payment cards.

REQUIREMENTS

1. All merchants will accept American Express, Discover, Visa and MasterCard
2. Available methods of accepting payments
   ALL CARD DATA MUST BE SWIPED, INSERTED, OR ENTERED THROUGH A CERTIFIED P2PE PAYMENT CARD TERMINAL; OR BY THE CUSTOMER THROUGH AN OMS APPROVED E-COMMERCE SYSTEM.
   a. Card Present Transactions
      i. In-person
         1. All efforts must be made by the merchants to have the customer swipe or insert their own cards on the payment terminal as the preferred method of accepting in-person payments.
         2. OMS is working to provide terminals for temporary use events. (This bullet to be updated when contract is signed with vendor)
      ii. Self-service/kiosk
         1. If the P2PE payment card terminal is in a kiosk, the device must be physically secured to the kiosk and inspected for tampering daily utilizing the OMS Inspection Log.
      iii. Near Field Communication (NFC)
         1. For all Card Present Transactions, if the terminal or Point of Sale device are capable, merchants must accept NFC payments
         2. Examples of NFC: Google Pay, ApplePay, etc.
   b. Card-Not-Present Transactions
      i. Mail or other payment form collected on paper (not including fax)

        1. Written payment card data must be authorized immediately, or within one business day of receipt. Any payment card numbers that are kept overnight must be locked in a secure area with limited, need to know access.
        2. After the transaction is authorized, all but the last four digits of the payment card number must be redacted appropriately (see OMS Standard – Merchant Responsibilities) or removed from the form and cross-cut shredded.

    ii. Phone
        1. Phone payments may be accepted over the following methods:
            a. Analog phone line
            b. Cloud 3rd party Voice over Internet Protocol (VOIP) approved by OMS
            c. Pass the transaction to a 3rd party Interactive Voice Response (IVR) system approved by OMS
                i. If the employee stays on the phone line during the IVR process, a Dual Tone Masking process must be used (DTMF).
        2. Payment card information should only be written down if card data cannot be immediately entered directly into the P2PE device.
        3. Written payment card data must be authorized immediately, or within one business day of receipt. Any payment card numbers that are kept overnight will be locked in a secure area with limited, need-to-know access.
        4. After the transaction is authorized, all but the last four digits of the payment card number must be redacted appropriately (see OMS Standard – Merchant Responsibilities) or removed from the form and cross-cut shredded.

    iii. E-commerce
        1. E-Commerce transactions are cardholder-initiated transactions. University employees must not process transactions through their E-Commerce application on behalf of the cardholder.
        2. E-Commerce sites must use CAPTCHA. CAPTCHA assists in preventing the fraudulent “testing” of payment cards which may result in financial and reputational loss to the merchant and University.

3. Prohibited methods of accepting payments
    a. Fax
        i. UW Merchants must not accept credit card payments via fax
        ii. If payment card data is received, ensure the data is purged from the fax and network (you may have to contact IT support to do this)
        iii. Cross-cut shred the fax
        iv. Do not print the fax (if stored electronically) or process the payment. Contact the customer and arrange a different method of payment.
    b. Email
        i. UW Merchants must not accept credit card payments via email.
        ii. If payment card data is received, the email must be deleted immediately from the email box and the deleted folder.
        iii. Do not print the email or process the payment. Contact the customer and arrange a different method of payment.
    c. Entering payment card data on behalf of the customer through a University issued device other than an approved Point-of-Sale or card reader device (i.e. typing payment card information into a web terminal through a keyboard attached to University computer) is not allowed.

4. Charging convenience/surcharge/service fees
    a. UW Merchants, will not charge convenience or surcharge fees.

b. Merchants may enroll in card brand tuition service fee programs such as the Visa Government and Education Program.

LINKS

- Office of Merchant Services

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

- 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:

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

ADMINISTRATIVE INFORMATION

Version:	1.4
Superseded Standards:	None
Date Established:	Aug 7, 2019
Date Effective:	Dec 15, 2020
Next Review Date:	Jan 1, 2024
Contact:	Office of Merchant Services – pcihelp@uw.edu https://finance.uw.edu/merchant-services/

Change Log:

Date	Version	
9/5/2019	v1.1	Added NFC language
12/15/2020	v1.2	Added IVR/DTMF language
6/21/2021	v1.3	Added convenience/surcharge/service fees
1/6/2023	v1.4	Added CAPTCHA requirement