OMS GUIDANCE – THIRD PARTY SERVICE PROVIDERS

Applicability: University of Washington

Guidance Title: OMS Guidance – Third Party Service Providers

PURPOSE

This process provides direction on how to request a new Third Party Service Provider (TPSP), the steps needed to implement a new TPSP, the review process Office of Merchant Services (OMS) follows, and ongoing responsibilities for the TPSP, merchant, and OMS. The procedures and guidelines in this document are in support of Payment Card Industry Data Security Standards (PCI-DSS), Administrative Policy Statement (APS) 35.1, and the OMS Standard – Third Party Service Providers – PCI Compliance.

SCOPE

This process applies to all University merchants and TPSPs storing, processing, or transmitting payment card data on behalf of the University or any TSPSs that could affect the security of the University cardholder environment, in support of the OMS Standard – Third Party Service Providers – PCI Compliance. OMS must approve any exceptions to these procedures and guidelines.

OMS' scope is payment card acceptance. 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.

REQUESTING A NEW TPSP

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.

1. The merchant will submit a Vendor Information Form to OMS via pcihelp@uw.edu
2. OMS and the merchant will perform an initial consultation with the merchant
    a. A review the business case for adding the new TPSP
    b. A review of existing contracts with the TPSP or duplication of service currently provided through existing tools
3. 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
4. OMS will make a determination on how to proceed and provide reasons for the determination
    a. Engage with new TPSP
    b. Consolidate into existing contract with requested TPSP
    c. Consolidate into existing contract with different TPSP
    d. Do not proceed
5. If the merchant does not have a Merchant Identification Number (MID) or requires another MID (See Becoming a Merchant in the Links section below), one should be requested at this time

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
- Assist Merchant and TPSP with implementation
  - Provide implementation information from Elavon (Tear Sheet) / E-Commerce Platform (pending)
  - Order necessary payment card terminals from contracted vendors
  - Out of Scope:
    - Install of devices or systems
- Provide notices of upcoming deadlines and events
  - AOC expiration
  - Annual compliance assessment
- Conduct regular on-site compliance assessments and advise Merchants on results
- Communicate changes to PCI-DSS and related issues to Merchants through Merchant Services Digest

MERCHANT RESPONSIBILITIES

The merchant will:

- Update OMS 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
  - The payment terminal inspection logs should be kept for a minimum of three years
  - 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 from the TPSP
  - Notice of upcoming contract expiration or renewals

LINKS

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

- OMS Policies and Procedures
  https://finance.uw.edu/merchant-services/resources/policies-procedures
- Visa Service Provider Registry
  https://www.visa.com/splisting/searchGrsp.do
- PCI Security Standards Council Point-To-Point Encryption Solutions
  https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions
- PCI Security Standards Council Validated Payment Applications
  https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement
- University of Washington General Terms and Conditions
  https://finance.uw.edu/ps/suppliers/terms-conditions

ADMINISTRATIVE INFORMATION

Version: 1.2

Date Established: May 1, 2019

Date Effective: May 1, 2019

Next Review Date: May 1, 2020

Contact: Office of Merchant Services – pcihelp@uw.edu
https://finance.uw.edu/merchant-services/

Change Log:

Date	Version	
4/29/19	v1.0	First Publication
4/30/19	v1.1	Moved Vendor Information Form to separate document
7/1/19	v1.2	Updated naming convention