Out-Sourced PCI Services

Outsourcing simplifies payment card processing but does not guarantee compliance. We must always address policies and procedures for cardholder transactions and data processing. Your business must protect cardholder data when you receive it, and process chargebacks and refunds. You must also ensure that providers' applications and card payment terminals comply with respective PCI standards and do not store sensitive cardholder data. This document explains the requirements to outsource PCI services based on type of service(s) used.

The guidelines below are based on the following assumptions:

- Cal Poly network is not used for this service (wired or wireless)
- Merchant is responsible for conducting due-care/due diligence
- Merchant must provide all the required documentation
- Vendor is PCI DSS certified
- Application is PCI DSS certified and does not store card holder data
- Hardware is PCI DSS certified and does not store card holder data

I. If Web Hosted

A. Obtain required, relevant documents from vendor
    1. Attestation of Compliance (AOC)
    2. Report on Compliance (ROC)
    3. Contract (Confidentiality Agreement)
    4. Vulnerability scan report (certificate from Approved Scanning Vendor [ASV]).
    5. Network Diagram
    6. Card Holder Dataflow (CHD)
    7. Third-Party Vendor Security Questionnaire
    8. Incident Response (this should be included in the contract from vendor)
    9. PCI DSS Requirement 12.8

B. Provide all documentation received from vendor to AFD for review/validation

C. Allow two weeks for AFD review process
    1. If approved:
        i. Approval confirmation sent to requesting department
        ii. Include service as part of the annual PCI assessment
    2. If denied:
        i. Denial notification explaining reason for denial sent to requesting department
        ii. Alternative solution may be needed
            I. Restart approval process

II. Point of Sale (POS) Device(s)

Using PCI Validated Point-to-Point Encryption

A. If using PCI validated point-to-point encrypted (P2PE) device(s), submit the following required documentation to AFD for review/validation. This applies to all units **with or without a merchant account.**

1. Card Holder Dataflow (CHD)
2. Contract (Confidentiality Agreement)

B. Allow 2 weeks for AFD review process

1. If approved:
    i. Approval confirmation sent to requesting department
    ii. Include service as part of the annual PCI assessment
2. If denied:
    i. Denial notification explaining reason for denial sent to requesting department
    ii. Alternative solution may be needed
        1. Restart approval process

Not Using PCI Validated Point-to-Point Encryption

C. If not using PCI validated P2PE device(s)

1. Contact AFD for guidelines or visit http://afd.calpoly.edu/fiscalservices/pci/