University of Massachusetts Payment Card Industry (PCI) Compliance Guide

Treasurer's Office December 2022 PCI Version 4.0

Table of Contents

I. Overview

The Payment Card Industry Security Standards Council, or PCI SSC, was formed in 2006, as an open global forum to develop, maintain and manage PCI Security Standards, including the Data Security Standard (DSS).

The Council is comprised of five global payment brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. Each of these payment brands recognizes the PCI DSS as the technical requirements for their data security compliance programs. Each also recognizes Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs) certified by the PCI Security Standards Council as being qualified to validate compliance to the PCI DSS.

The University provides proof of PCI compliance on an annual basis by filing a PCI DSS Self- Assessment Questionnaire (SAQ) to its acquiring financial institution. The PCI DSS SAQ is a validation tool consisting of two components: (1) Requirements to comply with PCI DSS standards and (2) a Validation of Compliance whereby Merchants verify and demonstrate their compliance status.

PCI DSS compliance is continuous and is part of the everyday "business as usual" process. Compliance to PCI DSS standards at the University is mandatory. Each Merchant is responsible for providing proof of compliance on an annual basis, running quarterly security scans on all relevant IP addresses and for maintaining compliance throughout the year. All documents and notices of compliant or non-compliant situations should be forwarded to the appropriate campus E-commerce representative and the Treasurer's Office.

Non- adherence to PCI -DSS can subject the University to significant financial and reputational risks. Failure to comply can result in:

- Fines and penalties imposed by payment card institutions and banks.
- Monetary costs associated with legal proceedings, settlements, and judgments; and
- Suspension of the Merchant account and the inability to accept payment cards for payment

II. Purpose

The purpose of this guide is to provide the University with resources, requirements, and procedures, needed to protect Cardholder Data from loss or misuse.

III. Roles & Responsibilities

- Campus E-commerce representatives and the Treasurer's Office will work with Merchants to provide the necessary guidance in the areas of PCI Compliance, internal controls (including central processing of chargebacks and refunds), reporting and reconciliation.
- The Director of Merchant Services, at the Treasurer's Office, has the authorization to approve and set up new, or modify existing Merchant accounts, and has the authority to suspend the account of a Merchant who is not in compliance with the University of Massachusetts Administrative Standards for The Treasurer's Fiscal Procedure No. 08-01- Merchant Debit and Credit Card Receipts[1], or PCI DSS Standards.
- Merchant's failure to follow the PCI DSS standards subjects the University to fines and penalties. Any fines will be the responsibility of the campus.
- Use of any unauthorized or non-compliant third- party credit card processing vendors or equipment must be immediately terminated.
- Any Merchant accepting credit card payments in any format is required to continuously adhere to and complete the appropriate PCI SAQ (Self-Assessment Questionnaire) and submit SAQ annually to the Treasurer's Office within the requested deadlines.
- Campus IT will assist the Merchants with the transmission of quarterly scan results and the annual SAQ documentation [2], and the validation of such will be sent to and tracked by the Treasurer's Office to the acquiring bank.
- Campus E-commerce representatives are responsible for providing a current list of all individuals who meet the standards for PCI Awareness training to Treasurer's Office. This includes individuals who have access to or process cardholder data, and those who help set up merchant sites. Failure to complete new hire and annual training will result in the loss of access to Merchant sites and the cardholder data environment until training is completed.

[1] Treasurer's Fiscal Procedure No. 08-01 and Treasurer's Office Administrative Standards for The Treasurer's Fiscal Procedure no. 08-01 Merchant Debit and Credit Card Receipts can be found on the Treasurer's website – Cash Management portal- Merchant Services

[2] **The Campus Written Information Security Policy (WISP) will be used as a guide for technical requirements in the SAQ, and adherence to the WISP to protect credit card data will be validated annually by the Campus CISO or designee on the SAQ**

IV. Getting Started Accepting Credit Cards

To become a University Merchant, you must first contact your Campus E-commerce representative and together, obtain approval from the Treasurer's Office. Additionally, there are several things to consider prior to moving forward with credit card acceptance:

Things to consider:

- How do you wish to obtain credit card payments?
  - Online,
  - in-person,
  - or both?
- Will you be taking credit card information over the phone? If yes, what type of phone lines do you have (analog, digital, VOIP- do they record?) Will your staff accept calls remotely?
- Will you be accepting credit card payments via the mail?
- Will you be using a third- party vendor to collect credit card data? **If yes, have you verified that the Third-party can process with one of our central processors (list of central processors found on the Treasurer's website)?**
  - Note- Contact the Treasurer's Office for assistance with verifying processor use if needed prior to moving forward with contract
- Have you contacted your IT support person to help with setting up the Merchant site? Have you discussed your infrastructure needs with them?
- Have you discussed a budget for the initiative?
  - Do you have an idea of price and volume?
  - Have you reviewed the The Treasurer's Office website to understand all costs associated with credit card acceptance (payment gateway or equipment cost, transaction fees, processing fees, interchange fees, Qualified Security Assessor PCI Compliance review fee).

Additional Steps to take:

- Review The Treasurer's Office website (Cash Management/Merchant Services) to obtain documentation to request a Merchant ID/gateway and review required contract language regarding PCI DSS compliance
- UPST & the Treasurer's Office must review third-party contracts prior to signing.
- Contact "resources needed" areas prior to signing contract
- All staff that will be involved with credit card processing (reconciliation, customer service, accepting payments, IT support, etc.) must take the PCI Compliance training at new hire and annually.

V. Types of Acceptance & SAQs

The way that a Merchant accepts credit card payments will determine the PCI requirements needed to keep the payment card data secure. To assist Merchants with the process, the PCI Security Standards Council created documents for each type of payment acceptance, and these documents, called self-assessment questionnaires (SAQs), are used during the initial Merchant set-up, annually, and on an ongoing basis, to report compliance with the PCI DSS requirements.

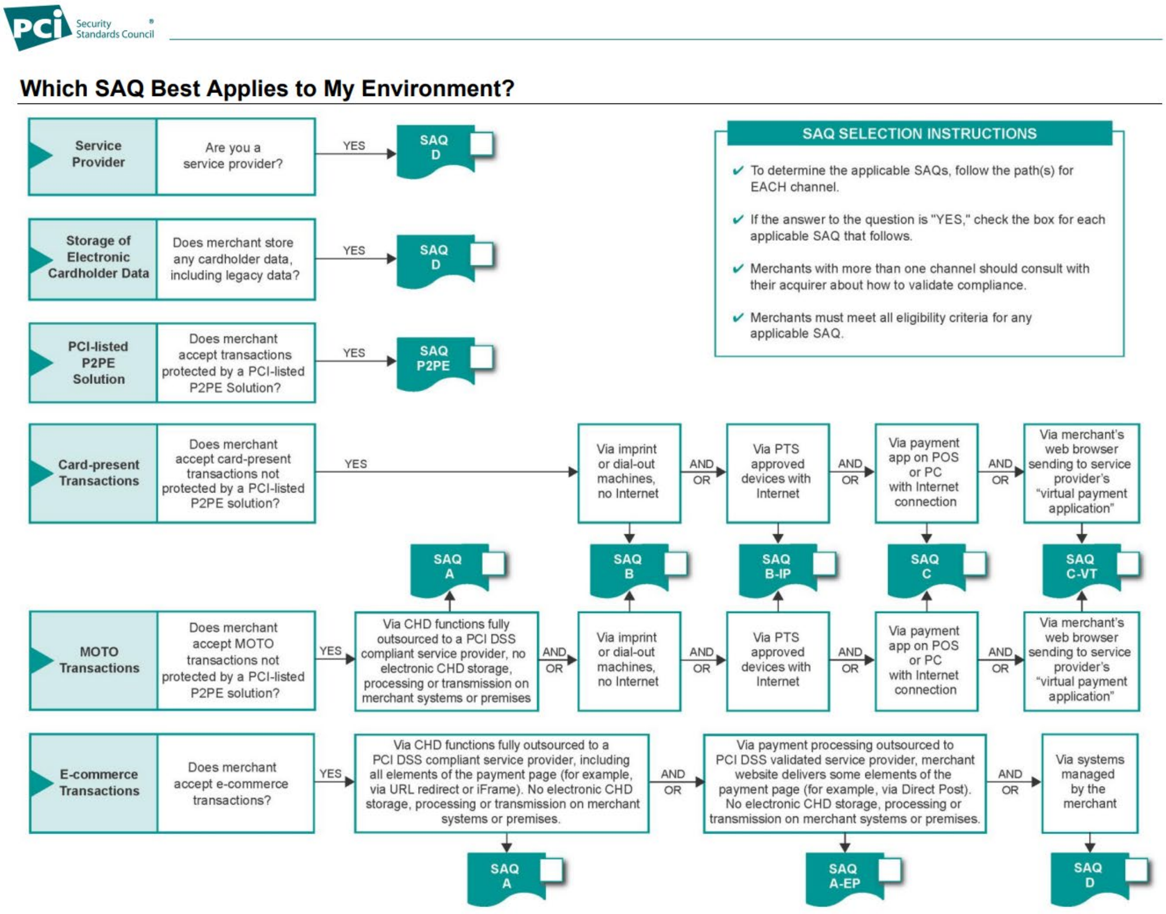
At the initial set-up, or during a significant change to the flow of the payment card data, a Qualified Security Assessor (QSA) will review the PCI Compliance requirements specific to the Merchant site and report the “compliant” results to the Treasurer’s Office prior to a live credit card payment being processed.

Annually, the Merchant will complete the SAQ appropriate for their Merchant site and submit the documentation to the Treasurer’s Office during the Annual PCI Compliance Audit. All SAQ documentation must result in a “compliant” status, and if there are areas where the Merchant is not compliant, an action plan must be developed to return the Merchant to a compliant status as quickly as possible. In most cases, and at the discretion of Treasurer’s Office, the Merchant may be restricted from using the Merchant site until a “compliant” status can be restored.

For each requirement on the SAQ, the Merchant will indicate whether the requirement is “in place,” “in place with compensating controls,” “in place with remediation,” “not applicable,” and/ or “not in place.” **If any requirement indicates anything other than “in place” or “not applicable,” the Treasurer’s Office must be notified immediately, and an action plan must be developed**. Additionally, the use of compensating controls can only be used when approved by the Treasurer’s Office.

Choosing the Correct SAQ

Depending on the way that your department or area is taking credit cards, one of several different SAQ forms can be used. The type of form is dependent on the way cards are stored, processed, or transmitted. The PCI Council has updated a flowchart to assist in choosing the correct SAQ, and it is presented here. If you have any questions about which SAQ to use, please contact the Treasurer's Office. After the flowchart, each SAQ is described in more detail. Please note that for new implementations, the University prefers to use solutions that line up with SAQ-A (online transactions) or SAQ P2PE (in-person) requirements, because the PCI compliance requirements have been greatly reduced based on these solutions.



Which SAQ Best Applies to My Environment?

SAQ SELECTION INSTRUCTIONS

- ✔ To determine the applicable SAQs, follow the path(s) for EACH channel.
- ✔ If the answer to the question is "YES," check the box for each applicable SAQ that follows.
- ✔ Merchants with more than one channel should consult with their acquirer about how to validate compliance.
- ✔ Merchants must meet all eligibility criteria for any applicable SAQ.

Security Standards Council
Service Provider
Are you a service provider?
YES
SAQ D
Storage of Electronic Cardholder Data
Does merchant store any cardholder data, including legacy data?
YES
SAQ D
PCI-listed P2PE Solution
Does merchant accept transactions protected by a PCI-listed P2PE Solution?
YES
SAQ P2PE
Card-present Transactions
Does merchant accept card-present transactions not protected by a PCI-listed P2PE solution?
YES
Via imprint or dial-out machines, no Internet
AND OR
Via PTS approved devices with Internet
AND OR
Via payment app on POS or PC with Internet connection
AND OR
Via merchant's web browser sending to service provider's "virtual payment application"
SAQ A
SAQ B
SAQ B-IP
SAQ C
SAQ C-VT
MOTO Transactions
Does merchant accept MOTO transactions not protected by a PCI-listed P2PE solution?
YES
Via CHD functions fully outsourced to a PCI DSS compliant service provider, no electronic CHD storage, processing or transmission on merchant systems or premises
AND OR
Via imprint or dial-out machines, no Internet
AND OR
Via PTS approved devices with Internet
AND OR
Via payment app on POS or PC with Internet connection
AND OR
Via merchant's web browser sending to service provider's "virtual payment application"
E-commerce Transactions
Does merchant accept e-commerce transactions?
YES
Via CHD functions fully outsourced to a PCI DSS compliant service provider, including all elements of the payment page (for example, via URL redirect or iFrame). No electronic CHD storage, processing or transmission on merchant systems or premises.
AND OR
Via payment processing outsourced to PCI DSS validated service provider, merchant website delivers some elements of the payment page (for example, via Direct Post). No electronic CHD storage, processing or transmission on merchant systems or premises.
AND OR
Via systems managed by the merchant
SAQ A
SAQ A-EP
SAQ D

Self -Assessment Questionnaire – SAQ-A

For Merchants that are outsourcing the account data functions to a PCI DSS validated and compliant third party and are only retaining paper reports or receipts (no electronic) with account data, an SAQ-A will be used. These Merchants will utilize online E-commerce, or mail/telephone order **(card-not present)** payments. Additionally, the Merchant will not store, process, or transmit any payment card data in electronic format on their systems or premises, and will not retain or receive any electronic documents containing payment card data. Finally, all elements of the payment page(s) or form(s) delivered to the customer's browser will originate directly from the PCI compliant third-party.

SAQ A merchants will confirm that they meet the following eligibility criteria for this payment channel:

- Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions.
- All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers.
- Merchant does not electronically store, process, or transmit any cardholder data on their systems or premises, but relies entirely on a third party(s) to handle all these functions.
- Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
- Any cardholder data that the Merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Additionally, for e-commerce channels:

▪ All elements of all payment pages delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider(s).

Examples of SAQ-A use at the University[3]:

- Online credit card payment acceptance
    - PayPal acceptance
        - Hosted payment buttons
        - API connection to a PCI DSS compliant third-party
    - CyberSource payment gateway
        - API connection to a PCI DSS compliant third-party
    - Blue Snap

NOTE: This type of set up (SAQ A) requires a **Qualified Security Assessor (QSA)** to review the PCI Compliance requirements specific to the Merchant site and report the "compliant" results to the The Treasurer's Office, prior to a live credit card payment being processed. See resource section for QSA information. Additionally, quarterly scans may be required- see SAQ for further details.

Resources needed for SAQ-A Merchants

- **IT support**
    - Support will be needed to ensure that the Merchant set up is PCI Compliant and in accordance with the campus Written Information Security Plan (WISP) (Req 12.1-12.1.4) as well as:
        - Configure and manage system components (Req 2.2.2)
        - Protect stored account data (Req 3.1-3.2.1)
        - Actively monitor industry sources for vulnerability information to address, identify and resolve any security vulnerabilities (Req 6.3.1)
        - Install critical or high security patches within one month of release (Req 6.3.3)
        - Protect public-facing web applications against attacks (Req 6.4.3)
        - Strictly manage User and Administrator access (Req 8.2 - 8.3.9)
        - Perform External & Internal vulnerability ASV scans (Req 11.3)
        - Aid with third party inline frame (iframe) payment form on department website- including ensuring a change and tamper detection mechanism is deployed (Req 11.6.1)
        - Give assistance to Merchants regarding campus security incident response plan (Req 12.10)

[3] A complete list of third-party suppliers currently in use at the University can be found on the Treasurer's website- https://www.umassp.edu/treasurer/cash-management-portal/merchant-services/approved-terminals-devices-and-software-third

- **Telecom support**
    - Phone lines must not be able to record if credit card information is being accepted over the phone (VOIP should be reviewed)

- **Other business needs**
    - Merchant will ensure control over any cardholder data held for business need (Req 9.4.1-9.4.6)
    - Merchant will need to obtain a cross-shredding machine to destroy any paper documents after being obtained for business purposes (Req 3.2.1 & 9.4)
    - Online PCI Compliance training (Req 12.6.1) is required at new hire and annually for those involved in the credit card acceptance process
    - Reconciliation support
        - Merchants will reconcile their credit card receipts and expenses to the PeopleSoft GL monthly or no less than quarterly
            - **NOTE**: Credit card refunds will be applied by the Treasurer's Office to the same payment card that made the original transaction – The Treasurer's Office can make exceptions
    - UPST will assist with managing third-party relationships (Req. 12.8.1-12.8.3 and 12.8.5) and ensure contracts contain required PCI language [4]
    - Campus E-commerce Representative & the Treasurer's Office will collaborate to stay up to date on any changes to the University PCI Compliance program (Req 12.8.4)
        - Merchants will utilize the SAQ to ensure requirements are followed as a daily business practice and notify the Treasurer's Office and Campus E-commerce representative if there are any changes to the Merchant set-up
        - Merchants will complete a SAQ-A during the Annual PCI Compliance audit

[4] Required language can be found on Treasurer's website, cash management portal, merchant services, e-commerce compliance resources

Self -Assessment Questionnaire – SAQ A-EP

Self-Assessment Questionnaire (SAQ) A-EP is used for e-commerce Merchants (card-not-present) that partially outsource their e-commerce payment channel with a website that will control how customers, or their account data, are redirected to a PCI DSS validated and compliant third party.

Although the website does not itself receive account data, and does not electronically store, process, or transmit any account data on their systems or premises, if the website payment page affects the security of the payment transaction and/or the integrity of the page that accepts the customer's account data, then a SAQ A-EP applies.

Additionally, as with the SAQ A, any account data the Merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Due to the increased risk of processing transactions in this manner, the University does not currently have any Merchants with a SAQ A-EP set up. Because of the added number of controls and requirements for this SAQ, if you feel this is your environment, please contact the Treasurer's office prior to implementation. The goal would be to have a solution that can adhere to an SAQ-A environment.

Merchants that wish to utilize their website payment page in the manner described above must thoroughly read the resources needed section below and ensure that consistent IT support is available and approved prior.

NOTE: This type of set up (SAQ A-EP) requires a **Qualified Security Assessor (QSA)** to review the PCI Compliance requirements specific to the Merchant site and report the "compliant" results to the Treasurer's Office, prior to a live credit card payment being processed. See resource section for QSA information.

SAQ A-EP merchants will confirm that they meet the following eligibility criteria for this payment channel:

- Merchant accepts only e-commerce transactions.
- All processing of cardholder data, apart from the payment page, is entirely outsourced to a PCI DSS validated third-party payment processor.
- Your e-commerce website does not receive cardholder data but controls how consumers, or their cardholder data, are redirected to a PCI DSS validated third-party payment processor.
- If merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements (e.g., including PCI DSS Appendix A if the provider is a shared hosting provider).
- Each element of the payment page(s) delivered to the consumer's browser originates from either the merchant's website or a PCI DSS compliant service provider(s).
- Merchant does not electronically store, process, or transmit any cardholder data on their systems or premises, but relies entirely on a third party(s) to handle all these functions.
- Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
- Any cardholder data the merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Resources needed for SAQ-A-EP Merchants

- **IT support**
  - Support will be needed to ensure that the Merchant set up is PCI Compliant and in accordance with the campus Written Information Security Plan (WISP) (Req 12.1-12.1.4) as well as:
    - To install network security controls, secure configuration, and connections (Req 1.1-1.5.1)
    - Configure and manage secure system components and access (Req 2.1-2.2.7 & 6.5.1-6.5.2& 7.2-8.1.1)
    - Protect stored account data (Req 3.1.1-3.3.1.3)
    - Utilize strong cryptography during transmission (Req 4.1-4.2.2)
    - Protect systems and networks from malicious software (Req 5.1-5.4.1)
    - Protect and maintain secure systems and software (Req 6.1.1-6.2.4)

- Identify and address security vulnerabilities (Req 6.3.1-6.3.3)
- Protect public-facing web applications against attacks (Req 6.4.1-6.4.3)
- User and Administrator access strictly managed (Req 8.2 - 8.3.11)
- MFA (Multi-factor authentication) to secure access to CDE (Req 8.4.1-8.6.3)
- Monitor and test access to system components (Req 10.2-10.3.4)
- Review audit logs (Req 10.4-10.5.1)
- Ensure time-synchronization mechanisms in place (Req 10.6-10.6.3)
- External & Internal vulnerability ASV scans and penetration testing (Req 11.3-11.4.5)
- Detect and respond to network intrusions and unexpected file changes (Req 11.5-11.5.2)
- Detect and respond to changes on payment pages (Req 11.6.1)
- Identify, evaluate, and manage any risks to CDE (Req 12.3-12.3.1)
- Assistance to Merchants regarding campus security incident response plan (Req 12.10.1-12.10.3)

- **Telecom support**
  - Phone lines must not be able to record if credit card information is being accepted over the phone (VOIP should be reviewed)

- **Other business needs**
  - Work with facilities to ensure physical access to systems in CDE are restricted (Req 9.2)

  - Obtain a cross-shredding machine to destroy any paper documents that need to be destroyed after being obtained for business purposes (Req 3.2.1 & 9.4)

  - Complete Online PCI Compliance training (Req 12.6.1) at new hire and annually

  - Reconciliation support

    - Merchants will reconcile their credit card receipts and expenses to the PeopleSoft GL monthly or no less than quarterly
        - **NOTE:** Any credit card refund will be applied by the Treasurer’s Office to the same card that made the original card payment – The Treasurer’s Office can make exceptions
- UPST will help to manage third-party relationships (Req. 12.8.1-12.8.3 and 12.8.5) and ensure contracts contain required PCI language (example found on The Treasurer’s Office website)

- The Campus e-commerce representative & the Treasurer’s Office will collaborate to stay up to date on any changes to the University PCI Compliance program (Req 12.8.4)
-
    - Merchants will Utilize the SAQ to ensure requirements are followed as a daily business practice and notify the Treasurer’s Office and Campus e-commerce representative if there are any changes to the Merchant set-up
    - Completion of SAQ-A-EP during Annual PCI Compliance audit

Self -Assessment Questionnaire – SAQ B

Merchants completing a SAQ B wish to take credit card payments in person **(card-present)** rather than online, and utilize standalone, dial-out terminals (point of sale -POS devices) to accept their card payments. The terminals either connect to a phone line or can use wireless/cellular to connect to the processor. In either case, the terminals do not store account data, and can also be used for mail/telephone order payments.

Terminals used in the manner above do not connect to any other systems within the Merchant environment (no ethernet or Internet connection), and if any account data is retained, it is on paper, and the documents are not received electronically.

All POS devices of this nature are ordered directly through the Processor by the Treasurer's Office. The Treasurer's Office will maintain an inventory sheet of all POS devices, by recording their serial number, make and model, and store number. The Merchant must follow SAQ B requirements to always secure the POS terminal and notify the Treasurer's Office immediately of any lost or stolen POS device.

Additionally, the Merchant is required to perform regular inspections of the POS terminal to help detect any changes to the terminal caused by a skimming device. Skimming devices can be attached to the POS terminal (ex. an overlay on the actual device to capture information) or installed within. See below for tips for spotting a skimming device.

POS (Point of Sale) terminals[5]

- Analog (dedicated phone line)
- Wireless (cellular)
- PayPal All-in-One-POS (cellular)
- PayPal/Zettle reader (cellular)

[5] All stand-alone POS terminals must be ordered through The Treasurer's Office

SAQ B merchants may be either brick-and-mortar (card-present) or mail/telephone order (card-not-present) merchants, and do not store cardholder data on any computer system. SAQ B merchants will confirm that they meet the following eligibility criteria for this payment channel:

- Merchant uses only standalone, dial-out terminals (connected via a phone line to your processor) to take your customers' payment card information.
- The standalone, dial-out terminals are not connected to any other systems within your environment.
- The standalone, dial-out terminals are not connected to the Internet.
- Merchant does not transmit cardholder data over a network (either an internal network or the Internet).
- Any cardholder data that the Merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically; and
- Merchant does not store cardholder data in electronic format.

Resources needed for SAQ B Merchants

- **IT support**
  - Support will be needed to ensure that the Merchant set up is PCI Compliant and in accordance with the campus Written Information Security Plan (WISP) Req 12.1-12.1.4) as well as:

  - Protect stored account data (Req 3.1.1-3.3.1.3)

  - Assistance to Merchants regarding campus security incident response plan (Req 12.10.1-12.10.3)

- **Skimming**[6]
    - Terminals must be tracked and protected from tampering (Req 9.5-9.5.1.3) Skimming occurs when devices are illegally installed on the POS terminal to capture or record cardholder data. In addition to keeping the terminal in a secure location, the terminal should be inspected daily to ensure that there are no overlays or tampering that occurred (look for anything loose, damaged, scratched, new cords, sticky tape residue etc.)
    - Requesting that the "dip" /chip card technology is used rather than allowing the customer to "swipe" the card also helps to counter card-present fraud.

- **Telecom support**
    - POTS (plain-old- telephone service) phone lines must be used for any analog machine and be dedicated to the POS terminal (not also used for fax and no digital lines). Please check to ensure a phone line is available prior to ordering an analog POS terminal from The Treasurer's Office. The wireless POS terminal will run off cellular connections and will result in a monthly data fee to the Merchant.

- **Inventory Tracking**
    - The make, model and serial number of the POS terminal must be submitted to the campus e-commerce representative and the Treasurer's Office upon receipt of the new terminal and annually. Additionally, the Treasurer's Office must be notified anytime a department shares their POS terminal with another department or location.

- **Other business needs**
    - Work with facilities to ensure physical access to POS terminals is restricted, and whenever possible, that a terminal is cabled and secured to restricted area. Terminals must be locked away when not in use for extended periods.

    - Work with the Treasurer's Office to ensure that the POS terminal displays only the first 6 and last 4 digits of the credit card on the screen and paper receipts (Req 3.4)

[6] Examples of skimming devices, and best practices to prevent skimming can be found on the PCI SSC website https://www.pcisecuritystandards.org/document_library/

- Merchant must ensure that access to POS terminal is assigned to users appropriately (Req 7.2)

- Use a cross-shredding machine to destroy any paper documents that contain cardholder data after being obtained for business purposes (Req 9.4-9.4.6)

- Complete online PCI Compliance training (Req 12.6.1) at new hire and annually

- Reconciliation support
    - Merchants will reconcile their credit card receipts and expenses to the PeopleSoft GL monthly or no less than quarterly.
        - **NOTE**: Any credit card refund will be applied by the Treasurer's Office to the same card that made the original card payment – The Treasurer's Office can make exceptions

- Obtain assistance from UPST to manage third-party relationships (Req. 12.8.1-12.8.3 and 12.8.5) and ensure contracts contain required PCI language (example found on the Treasurer's Office website)

- Collaborate with Campus e-commerce representative & the Treasurer's Office to stay up to date on any changes to the University PCI Compliance program (Req 12.8.4)
-
    - Utilize the SAQ to ensure requirements are followed as a daily business practice and notify the Treasurer's Office and Campus e-commerce representative if there are any changes to the Merchant set-up
    - Complete the SAQ B during the Annual PCI Compliance audit

Self -Assessment Questionnaire – SAQ B-IP

For Merchants that wish to use PCI approved POS or Point- of -Interaction (POI) devices with an IP connection to the payment processor for their **card-present** transactions, then a Self-Assessment Questionnaire (SAQ) B -IP applies.
These POS or POI terminals are stand-alone (no computer, tablet, mobile phone etc.), and are not connected to any other systems within the merchant environment (this can be achieved with network segmentation to isolate the terminals from other systems). These terminals transmit the account data from the POS or POI device to the payment processor, and if any account data is retained, it is on paper, and the documents are not received electronically.

All POS or POI devices of this nature are ordered directly through the Processor by the Treasurer's Office, or Third -Party vendor approved by the Treasurer's Office. The Treasurer's Office will maintain an inventory sheet of all POS and POI devices, by recording their serial number, make and model, and store number. The Merchant must follow SAQ B-IP requirements to always secure the POS or POI terminal.

Additionally, the Merchant is required to perform regular inspections of the POS or POI terminal to help detect any changes to the terminal caused by a skimming device. Skimming devices can be attached to the terminal (ex. an overlay on the actual device to capture information) or installed within. See below for tips for spotting a skimming device

Examples of SAQ-B-IP use at the University[7]:

- Parking systems
- POS terminals connected via ethernet to a secure and segmented network created specifically for PCI.

NOTE: This type of set up (SAQ B-IP) requires a **Qualified Security Assessor (QSA)** to review the PCI Compliance requirements specific to the Merchant site and report the "compliant" results to the Treasurer's Office, prior to a live credit card payment being processed. See resource section for QSA information.

[7] A list of POS and POI devices in use at the University can be found on the Treasurer's website. https://www.umassp.edu/treasurer/cash-management-portal/merchant-services/approved-terminals-devices-and-software-third For a listing of PCI SSC approved devices, visit https://www.pcisecuritystandards.org/

SAQ B-IP merchants will confirm that they meet the following eligibility criteria for this payment channel:

- Merchant uses only standalone, PTS-approved point-of-interaction (POI) devices (excludes SCRs) connected via IP to your payment processor to take your customers' payment card information.
- The standalone, IP-connected POI devices are validated to the PTS POI program as listed on the PCI SSC website (excludes SCRs).
- The standalone, IP-connected POI devices are not connected to any other systems within your environment (this can be achieved via network segmentation to isolate POI devices from other systems).
- The only transmission of cardholder data is from the PTS-approved POI devices to the payment processor.
- The POI device does not rely on any other device (e.g., computer, mobile phone, tablet, etc.) to connect to the payment processor.
- Any cardholder data the merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically; and
- Merchant does not store cardholder data in electronic format.

Resources needed for SAQ B-IP Merchants

- **IT support**
- Support will be needed to ensure that the Merchant set up is PCI Compliant and in accordance with the campus Written Information Security Plan (WISP) Req 12.1-12.1.3) as well as:
  - Network security controls are configured and maintained (Req 1.2.3-1.2.6)
  - Network access to and from the CDE is restricted (1.3.1-1.3.3)
  - Network connections between trusted and untrusted networks are controlled (Req 1.4.3)
  - System components are configured and managed securely (Req 2.2.2-2.27)
  - Wireless environments are configured and managed securely (Req 2.3.1-2.3.2)
  - Protect stored account data (Req 3.1.1-3.3.1.3)
  - Security vulnerabilities are identified and addressed (Req 6.3.1-6.3.3)
  - Access to system components and data is assigned and appropriate (Req 7.2.2)
  - Process and policies are in place to identify users (Req 8.1)
  - Management of users and administrators (Req 8.2-8.2.7)

  - Multi-factor (MFA) must be implemented to secure access to CDE (Req 8.4.3)
  - Perform external and internal vulnerability scans (Req 11.3.2)
  - Perform penetration tests on segmentation controls (Req 11.4.5)
  - Assistance to Merchants regarding campus security incident response plan (Req 12.10.1)

- **Skimming**[8]
  - Terminals must be tracked and protected from tampering (Req 9.5.1-9.5.1.3) Skimming occurs when devices are illegally installed on the POI/POS terminal to capture or record cardholder data. In addition to keeping the terminal in a secure location, the terminal should be inspected daily to ensure that there are no overlays or tampering that occurred (look for anything loose, damaged, scratched, new cords, sticky tape residue etc.)

- **Inventory Tracking**
  - The make, model and serial number of the POI/POS terminal must be submitted to the campus e-commerce representative and the Treasurer's Office upon receipt of the new terminal and annually.

- **Other Business Needs**
  - Work with facilities to ensure physical access to POI terminals and network jacks is restricted, whenever possible (Req 9.1 & 9.2)
  - Work with the Treasurer's Office and the Third-party to ensure that the POS terminal displays only the first 6 and last 4 digits of the credit card on the screen and paper receipts (Req 3.4.1)
  - Utilize a cross-shredding machine to destroy any paper documents that include cardholder data after being obtained for business purposes (Req 9.4-9.4.6)
  - Complete Online PCI Compliance training (Req 12.6.1) at new hire and annually

[8] Examples of skimming devices, and best practices to prevent skimming can be found on the PCI SSC website https://www.pcisecuritystandards.org/document_library/

- Reconciliation support
    - Merchants will reconcile their credit card receipts and expenses to the PeopleSoft GL monthly or no less than quarterly.
        - **NOTE**: Any credit card refund will be applied by the Treasurer's Office to the same card that made the original card payment – The Treasurer's Office can make exceptions

- Obtain assistance from UPST to manage third-party relationships (Req. 12.8.1-12.8.3 and 12.8.5) and ensure contracts contain required PCI language (example found on the Treasurer's Office website)

- Collaborate with Campus e-commerce representative & the Treasurer's Office to stay up to date on any changes to the University PCI Compliance program (Req 12.8.4)

- Utilize the SAQ to ensure requirements are followed as a daily business practice and notify the Treasurer's Office and Campus e-commerce representative if there are any changes to the Merchant set-up

- Complete the SAQ B-IP during Annual PCI Compliance audit

Self -Assessment Questionnaire – SAQ C

The SAQ C will be completed by Merchants that want to use a payment application system and connect this to the Internet. The payment application system[9] and the Internet connection, must be on the same device, or same local area network (LAN), where the LAN is for a single store only, and the physical location of the POS environment is not connected to other locations or systems within the Merchant environment.

This can be achieved by network segmentation to isolate the payment application system and Internet device from all other systems. Additionally, the Merchant will not store account data in electronic format, and any account data that is retained for business purposes must be on paper.

Examples of SAQ-C use at the University:

- Parking and garage systems

NOTE:

The set up requires a great deal of IT Support and infrastructure needs. Discuss with IT prior to contract signing.

Merchants must ensure that they have ongoing IT support to stay compliant during and after the initial set-up.

Additionally, this type of set up (SAQ C) requires a **Qualified Security Assessor (QSA)** to review the PCI Compliance requirements specific to the Merchant site and report the "compliant" results to the Treasurer's Office, prior to a live credit card payment being processed. See resource section for QSA information.

[9] A list of approved Payment Application vendors that are used across the University can be found on the Treasurer's website https://www.umassp.edu/treasurer/cash-management-portal/merchant-services/approved-terminals-devices-and-software-third

SAQ C merchants will confirm that they meet the following eligibility criteria for this payment channel:

- Merchant has a payment application system and an Internet connection on the same device and/or same local area network (LAN).
- The payment application system/Internet device is not connected to any other systems within the Merchant environment (this can be achieved via network segmentation to isolate payment application system/Internet device from all other systems).
- The physical location of the POS environment is not connected to other premises or locations, and any LAN is for a single store only.
- Any cardholder data the Merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically; and
- Merchant does not store cardholder data in electronic format.

Resources needed for SAQ C Merchants

- **IT support**

- Support will be needed to ensure that the Merchant set up is PCI Compliant and in accordance with the campus Written Information Security Plan (WISP) Req 12.1-12.1.3) as well as:
  - Network access to and from the CDE is restricted (1.3.1-1.3.3)
  - System components are configured and managed securely (Req 2.2.2-2.27)
  - Wireless environments are configured and managed securely (Req 2.3.1-2.3.2)
  - Protect stored account data (Req 3.1.1-3.3.1.3)
  - Strong cryptography and security protocols are implemented to safeguard PAN during transmission over open, public networks (Req 4.2.1-4.2.2)
  - Malicious Software is prevented or detected and addressed (Req 5.2.1-5.3.5)
  - Anti-phishing mechanisms protect users against phishing attacks (Req 5.4.1)
  - If applicable, custom software is developed securely (Req 6.2.1-6.2.4)
  - Security vulnerabilities are identified and addressed (Req 6.3.1-6.3.3)
  - Manage changes to system components (Req 6.5.1-6.5.2)

- Access to system components and data is assigned and appropriate (Req 7.2.2-7.2.5)
- Process and policies are in place to identify users (Req 8.1)
- Management and authentication of users and administrators (Req 8.2-8.3.9)
- Multi-factor (MFA) must be implemented to secure access to CDE and configured to prevent misuse (Req 8.4.1-8.5.1)
- Use of application and system accounts & associated authentication factors is strictly managed (Req 8.6.1-8.6.3)
- Audit logs are implemented and managed (Req 10.1.1-10.5.1)
- Time synchronization is in place across systems (Req 10.6.1-10.6.3)
- Wireless access points are identified and monitored (Req 11.2-11.2.2)
- Perform external and internal vulnerability scans (Req 11.3.1-11.3.2.1)
- Perform penetration tests on segmentation controls (Req 11.4.5)
- Network intrusions and unexpected file changes are detected and responded to (Req 11.5.2)
- Acceptable use policies for end-user technologies are implemented (Req 12.2.1)
- Risk analysis is performed (Req 12.3.1)
- Assist merchants with security awareness training regarding phishing and related attacks and social engineering (Req 12.6.3.1)
- Assistance to Merchants regarding campus security incident response plan (Req 12.10.1-12.10.3))

- **Inventory Tracking**
  - The make, model and serial number of the POI/POS terminal must be submitted to the campus e-commerce representative and the Treasurer's Office upon receipt of the new terminal and annually (Req 9.5.1.1).
- **Skimming[10]**
  - Terminals must be tracked and protected from tampering (Req 9.5.1-9.5.1.3) Skimming occurs when devices are illegally installed on the POI/POS terminal to capture or record cardholder data. In addition to keeping the terminal in a secure location, the terminal should be inspected daily to ensure that there are no overlays or tampering that occurred (look for anything loose, damaged, scratched, new cords, sticky tape residue etc.)

[10] Examples of skimming devices, and best practices to prevent skimming can be found on the PCI SSC website https://www.pcisecuritystandards.org/document_library/

- **Other Business Needs**
    - Work with facilities to ensure physical access to CDE and network jacks is restricted, whenever possible (Req 9.1 & 9.2.1-9.2.2)
    - Work with the Treasurer's Office and the Third-party to ensure that the POS terminal displays only the first 6 and last 4 digits of the credit card on the screen and paper receipts (Req 3.4.1)
    - Utilize a Cross-shredding machine to destroy any paper documents that contain cardholder data after being obtained for business purposes (Req 9.4-9.4.6)
    - Complete Online PCI Compliance training (Req 12.6.1) at new hire and annually
    - Reconciliation support
        - Merchants will reconcile their credit card receipts and expenses to the PeopleSoft GL monthly or no less than quarterly.
            - **NOTE**: Any credit card refund will be applied by the Treasurer's Office to the same card that made the original card payment – The Treasurer's Office can make exceptions

    - Obtain assistance from UPST to manage third-party relationships (Req. 12.8.1-12.8.3 and 12.8.5) and ensure contracts contain required PCI language (example found on the Treasurer's Office website)

    - Collaborate with Campus e-commerce representative & the Treasurer's Office to stay up to date on any changes to the University PCI Compliance program (Req 12.8.4)
        - Utilize the SAQ to ensure requirements are followed as a daily business practice and notifying the Treasurer's Office and Campus e-commerce representative if there are any changes to the Merchant set-up
        - Complete the SAQ C during Annual PCI Compliance audit

Self -Assessment Questionnaire – SAQ C-VT

This SAQ option applies only to Merchants that manually enter a single transaction at a time via a keyboard into an Internet-based virtual payment terminal solution that is isolated from other systems and provided and hosted by a PCI compliant third-party service provider.

SAQ C-VT merchants do not store account data on any computer system (not by software or card readers) and any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically**.**

NOTE:

The set up requires a great deal of IT Support and infrastructure needs (ex. VLAN). Discuss with IT prior to contract signing.

Merchants must ensure that they have ongoing IT support to stay compliant during and after the initial set-up.

Additionally, the SAQ C-VT set up requires a **Qualified Security Assessor (QSA)** to review the PCI Compliance requirements specific to the Merchant site and report the "compliant" results to the Treasurer's Office, <u>prior to a live credit card payment being processed</u>. See resource section for QSA information.

SAQ C-VT merchants will confirm that they meet the following eligibility criteria for this payment channel:

- Merchant's only payment processing is via a virtual payment terminal accessed by an Internet-connected web browser.
- Merchant's virtual payment terminal solution is provided and hosted by a PCI DSS validated third-party service provider.
- Merchant accesses the PCI DSS-compliant virtual payment terminal solution via a computer that is isolated in a single location and is not connected to other locations or systems within Merchant environment (this can be achieved via a firewall or network segmentation to isolate the computer from other systems).
- Merchant's computer does not have software installed that causes cardholder data to be stored (for example, there is no software for batch processing or store-and-forward).
- Merchant's computer does not have any attached hardware devices that are used to capture or store cardholder data (for example, there are no card readers attached).
- Merchant does not otherwise receive or transmit cardholder data electronically through any channels (for example, via an internal network or the Internet).
- Any cardholder data the Merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically; and
- Merchant does not store cardholder data in electronic format.

Resources needed for SAQ C-VT Merchants

- **IT support**

  - Support will be needed to ensure that the Merchant set up is PCI Compliant and in accordance with the campus Written Information Security Plan (WISP) Req 12.1-12.1.3) as well as:
  - Network access to and from the CDE is restricted (1.3.1-1.3.3)
  - Security controls implemented on any computing device connected to both untrusted networks and the CDE (Req 1.5.1)
  - System components are configured and managed securely (Req 2.2.2-2.27)
  - Wireless environments are configured and managed securely (Req 2.3.1-2.3.2)
  - Protect stored account data (Req 3.1.1-3.3.1.3)

  - Strong cryptography and security protocols are implemented to safeguard PAN during transmission over open, public networks (Req 4.2.1-4.2.2)
  - Malicious Software is prevented or detected and addressed (Req 5.2.1-5.3.5)
  - Anti-phishing mechanisms protect users against phishing attacks (Req 5.4.1)
  - Security vulnerabilities are identified and addressed (Req 6.3.1-6.3.3)
  - Access to system components and data is assigned and appropriate (Req 7.2.2-7.2.5)
  - Process and policies are in place to identify users (Req 8.1)
  - Management and authentication of users and administrators (Req 8.2-8.3.9)
  - Multi-factor (MFA) must be implemented to secure access to CDE and configured to prevent misuse (Req 8.4.1-8.5.1)
  - Use of application and system accounts & associated authentication factors is strictly managed (Req 8.6.1-8.6.3)
  - Assist merchants with security awareness training regarding phishing and related attacks and social engineering (Req 12.6.3.1)
  - Assistance to Merchants regarding campus security incident response plan (Req 12.10.1)

- **Other Business Needs**
  - Work with facilities to ensure physical access to CDE and network jacks is restricted, whenever possible (Req 9.1 & 9.2.1-9.2.2)
  - Work with the Treasurer's Office and the Third-party to ensure that the POS terminal displays only the first 6 and last 4 digits of the credit card on the screen and paper receipts (Req 3.4.1)
  - Utilize a Cross-shredding machine to destroy any paper documents that contain cardholder data after being obtained for business purposes (Req 9.4-9.4.6)
  - Complete Online PCI Compliance training (Req 12.6.1) at new hire and annually
  - Reconciliation support
    - Merchants will reconcile their credit card receipts and expenses to the PeopleSoft GL monthly or no less than quarterly.
      - **NOTE**: Any credit card refund will be applied by the Treasurer's Office to the same card that made the original card payment – The Treasurer's Office can make exceptions

- Obtain assistance from UPST to manage third-party relationships (Req. 12.8.1-12.8.3 and 12.8.5) and ensure contracts contain required PCI language (example found on the Treasurer's Office website)

- Collaborate with Campus e-commerce representative & the Treasurer's Office to stay up to date on any changes to the University PCI Compliance program (Req 12.8.4)

- Utilize the SAQ to ensure requirements are followed as a daily business practice and notify the Treasurer's Office and Campus e-commerce representative if there are any changes to the Merchant set-up

- Complete the SAQ C-VT during Annual PCI Compliance audit

Self -Assessment Questionnaire – SAQ P2PE

Point-to-point encryption (P2PE) is an encryption standard established by the Payment Card Industry, Security Standard Council (PCI SSC), and offers the best protection for payment card data. The standard stipulates that cardholder data is encrypted immediately after the card is used with the merchant's point-of -sale terminal, and it not decrypted until it has been processed by the payment processor. This process ensures that the payment card data never comes into contact with the merchant's systems, reducing the PCI Compliance burden.

The SAQ P2pE will be completed by Merchants that process payments with a validated, PCI -Listed [11] P2PE solution (all controls in the P2PE Instruction Manual provided by the P2PE solution provider must be implemented) and any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Examples of SAQ-P2PE use at the University:

- Freedom Pay
- BlueFin

NOTE: This type of set up (SAQ P2PE) requires a **Qualified Security Assessor (QSA)** to review the PCI Compliance requirements specific to the Merchant site and report the "compliant" results to the Treasurer's Office, prior to a live credit card payment being processed. See resource section for QSA information.

[11] The PCI SSC has a full listing of P2PE solutions on their website , https://listings.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement?return=%2Fassessors_and_solutions%2Fpoint_to_point_encryption_solutions

SAQ P2PE merchants will confirm that they meet the following eligibility criteria for this payment channel:

- All payment processing is via a validated PCI P2PE solution approved and listed by the PCI SSC.
- The only systems in the merchant environment that store, process or transmit account data are the Point of Interaction (POI) devices which are approved for use with the validated and PCI listed P2PE solution.
- Merchant does not otherwise receive or transmit cardholder data electronically.
- There is no legacy storage of electronic cardholder data in the environment.
- Any cardholder data the Merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically; and
- Merchant has implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.

Resources needed for SAQ-P2PE Merchants

- **IT support**
  - Support will be needed to ensure that the Merchant set up is PCI Compliant and in accordance with the campus Written Information Security Plan (WISP) (Req 12.1-12.1.4) as well as:
    - CVV code is not retained upon completion of authorization process (Req 3.3.1.2)
    - Assistance to Merchants regarding campus security incident response plan (Req 12.10)

- **Telecom support**
  - Phone lines must not be able to record if credit card information is being accepted over the phone (VOIP should be reviewed)

- **Inventory Tracking**
  - The make, model and serial number of the POI/POS terminal must be submitted to the campus e-commerce representative and the Treasurer’s Office upon receipt of the new terminal and annually (Req 9.5.1.1).

- **Skimming**[12]
    - Terminals must be tracked and protected from tampering (Req 9.5.1-9.5.1.3) Skimming occurs when devices are illegally installed on the POI/POS terminal to capture or record cardholder data. In addition to keeping the terminal in a secure location, the terminal should be inspected daily to ensure that there are no overlays or tampering that occurred (look for anything loose, damaged, scratched, new cords, sticky tape residue etc.)
- **Other business needs**
    - Department will ensure control over any cardholder data held for business need (Req 9.4.1-9.4.6)
    - Department will need to obtain a cross-shredding machine to destroy any paper documents after being obtained for business purposes (Req 3.2.1 & 9.4)
    - Online PCI Compliance training (Req 12.6.1) is required at new hire and annually for those involved in the credit card acceptance process
    - Reconciliation support
        - Merchants will reconcile their credit card receipts and expenses to the PeopleSoft GL monthly or no less than quarterly
            - **NOTE**: Any credit card refund will be applied by the Treasurer's Office to the same payment card that made the original transaction – The Treasurer's Office can make exceptions
    - Obtain assistance from UPST to manage third-party relationships (Req. 12.8.1-12.8.3 and 12.8.5) and ensure contracts contain required PCI language [13]
    - Collaborate with Campus E-commerce Representative & the Treasurer's Office to stay up to date on any changes to the University PCI Compliance program (Req 12.8.4)
    - Utilize the SAQ to ensure requirements are followed as a daily business practice and notify the Treasurer's Office and Campus E-commerce representative if there are any changes to the Merchant set-up
    - Complete the SAQ-P2PE during Annual PCI Compliance audit

[12] Examples of skimming devices, and best practices to prevent skimming can be found on the PCI SSC website https://www.pcisecuritystandards.org/document_library/

[13] Required language can be found on Treasurer's website, cash management portal, merchant services, e-commerce compliance resources

Self -Assessment Questionnaire – SAQ D

The SAQ D contains **all** PCI DSS requirements, and therefore, is only used by the Treasurer's Office during the annual PCI Compliance Audit as a tool to "roll-up" Merchant responses across the entire University and submit as one document (SAQ D) to our payment processor.

Additional Resources

- **PCI SSC – Payment Card Industry Security Standards Council**
  - **https://www.pcisecuritystandards.org/**

  This site maintains:

    - Approved Scanning Vendors
    - Point-to-Point Encryption Solutions
    - Approved terminal devices
    - Validated Payment software and payment applications
    - Knowledge training
    - Document library (SAQs, blogs, FAQs)
      - **Merchants should go to this website to obtain the most recent version of the SAQ applicable to their environment**

- **Qualified Security Assessor (QSA) Information**

  The QSA should be contacted early in the project to ensure that they will be able to perform the PCI Risk review and submit their report prior to the "go live" date. The QSA will provide to the department a statement of work, and the department will pay Compass IT directly (campus to utilize UPST process)

  Compass IT Compliance
  2 Asylum Rd, North Providence, RI 02904
  Geoff Yeagley email: gyeagley@compassitc.com
  P: (401) 433-7975

- **Campus and IT Resources**
    - UMass Amherst- Patty Roper (Campus and IT) & Barb Picard (Aux).
    - UMass Boston- Jimmy Sam (Campus) & Wil Khouri (IT)
    - President's – Bradford Smith (UITS) & Kathryn White (Treasury)
    - UMass Dartmouth- Suzanne Audet (Campus), Brian Sullivan (IT)
    - UMass Lowell- Amy Kirchner (Campus), Jim Packard (IT)
    - UMass Chan- Yi Chen (Campus), Emily Martins (IT)

Frequently Asked Questions (FAQ)

This section has been created from questions that have been sent in from the Campuses to the Treasurer's Office and answered by our QSA. This section will continue to be updated as new information becomes available, and Campuses are encouraged to submit questions as often as needed to treasurer_ecommerce@umassp.edu

Question:

> If we have card swipe devices in the environment, how often do we need to perform the skimming reviews on the equipment?

Answer:

> With version 4.0, you should be looking at the level of risk to help determine the frequency. For example, if you have a single reader that you lock up every night, and only perform a few transactions a week, then monthly skimming reviews might be acceptable -since the ability to tamper with the device would be limited. However, if you're running a store where the swipe devices are on the counter and active all the time, then weekly skimming reviews (at a minimum) would make sense.

Question:

> We use PayPal on our website. Sometimes we are using an API to connect PayPal to a third -party provider, and sometimes just a hosted button. With the new SAQ A requirements, would we be required to do ASV scans?

Answer:

> Yes, the ASV scan is an external scan that looks for possible PCI vulnerabilities. You can perform it using Tenable (currently in use at the University), and then submit the scan to them, and they send it back as a "Passing" ASV scan.

Question:

If a payment site goes from a UMass hosted server to a Payment gateway or application (ex. CyberSource or PayPal), is the server considered in scope as a service provider?

Answer:

PCI DSS requirements that refer to the "cardholder data environment" (CDE) are applicable to the merchant website(s) that provide the address (the URL) of the TPSP's (Third party payment provider) payment page/form to merchant customers. This is because the merchant website impacts how the account data is transmitted, even though the website itself does not receive account data. So, the UMass server with a button to the payment would be in scope for the SAQ A. However, you wouldn't be a service provider in this case, you would be considered the merchant, with PayPal and CyberSource being considered the service providers.

Question:

We have vendors who refuse to give us their AOC annually, therefore, I pull verification from the PA-DSS list off the Visa Service Provider list. Under 4.0 will they now HAVE to give us the AOC?

Answer:

Usually, they refuse to give you the ROC, but not the AOC. If they refuse to give you the AOC, you should ask why- The AOC should be the standard, ESPECIALLY if you are already paying them for services. I'd also look at the Visa provider list and make sure they are listed for the services they are providing, and that the date is still good (reach out to the Treasurer's Office for help with this if needed).

Question:

Are we going to have to redo a bunch of the older contracts to make sure we have the language that says they will stay current with PCI? The new contracts have required it, but we have many older contracts that may not have it although all are required to provide the AOC or be on the provider list

Answer:

Best practice would be to get either an addendum or even just something in an email from the vendor in terms of staying current, and what they are responsible for. Most clients wait until the contract is up for renewal to make changes. The key here is to ensure you've done your due diligence, and that the vendor agrees. You could probably draft a one-page agreement for the clients that are missing the updated language that basically says we need to comply with PCI, and one of the requirements is ensuring that our vendors will as well, and then include the language from the Treasurer's Office website, then make a note to revise the contract with the same upon renewal.

Question:

For the requirements that we have typically said NA to, such as vendor default account management when it is in the cloud, and we have no access to the webservers. The explanation now says: *This requirement also applies where a system component is not installed within an entity's environment, for example, software and applications that are part of the CDE and are accessed via a cloud subscription service.* Most of the vendors use a third- party gateway and have no CDE but if they do, will we be able to use the vendor's AOC to validate they are in place and if so, how would we note that for our submission? Should be say "NA" with the explanation that we do not have access and it is the vendor responsibility or "In Place" because we have the AOC?

Answer:

Here is a response for the NA explanation:

"UMass uses a third-party service provider that is responsible for this control. The vendor's AOC was solicited and reviewed as part of this assessment, and it was confirmed that this control has been tested and is in place".

Question:

Our systems do not have any logins, but PCI still is asking questions about system access and unique ID's?

Answer:

In many cases, you may not need a formal login if you have a single reader with a phone line, or connected to a network, but you (or your manager) might have a login to access the payment website where you can look at payments and reports and possibly process a refund or chargeback. This is where those questions come into play, to be able to track who has access to which system.

Question:

What do I need to have on my network diagram?

Answer:

The key here is "network". If the network is in scope, you need to have it documented. So, if you're using an SAQ where the network is not in scope (P2PE, SAQ A, or SAQ B for example), you aren't required to have one. If you're a B-IP, C, A-EP or C-VT, you'll want to have a diagram that shows key network items (workstations, routers, firewalls) and the flow of the PCI Data as it comes in and travels out. Many people simply take the network diagram and draw a red line to represent the flow of the PCI data.