Payment Card Industry
Data Security Standard
Self-Assessment Questionnaire A Guide

PCI DSS Version:

V3.1, Rev 1.1

Prepared for:

The University of Tennessee Merchants
The University of Tennessee Foundation Merchants

Prepared by:

The University of Tennessee System Administration
Information Security Office

26 February 2016

THE UNIVERSITY OF TENNESSEE

Table of Contents

Introduction

This document has been created to help all UT merchants completing Payment Card Industry Data Security Standard (PCI DSS) Self-Assessment Questionnaire (SAQ) A. SAQ A is for card-not-present, e-commerce merchants who retain only paper reports or receipts with cardholder data, do not store cardholder data in electronic format, and do not process or transmit any cardholder data on merchant systems or premises. In addition, all elements of all payment pages that the customer sees originate only and directly from a PCI DSS validated third-party service provider. When answering the questions in SAQ A, refer to this document for help with understanding what PCI DSS is asking.

All questions must be answered. A “Yes” response means that the expected testing has been performed and that all elements of the requirement are being met as stated. A “No” response means that some or all of the elements are not being met or are in the process of being implemented. If you answer “No,” you must have a remediation plan and estimated date of compliance (see Part 4 of SAQ). An “N/A” response means that no elements of the requirement apply to your merchant area, and each of these responses requires a supporting explanation in Appendix C of the SAQ.

Unanswered questions mean non-compliance by the merchant. If any of the information here says you are required to have certain documentation, these are the things you will be asked for if you are ever audited. If you do not have these documents, create them. Not having the documentation means non-compliance by the merchant. Saying you have the items, but not producing them when audited can cost your department fines and possible loss of your Merchant ID (MID).

Most of the written documentation requirements found within the SAQ are covered by existing UT policyies, or in the **Merchant Documentation Templates** and **PCI Standards and Procedures for UT/UTFI Merchants** sections found on UT’s PCI Compliance website at http://security.tennessee.edu/pci-dss-compliance-information/. Should you choose not to use the templates, you must make certain you have each requirement included in your own version of documentation. **Please note that any requirement not included in these policies or document templates will need to be produced by the merchant and are noted in red.**

If you have questions about this document, please contact Sandy Lindsey in the University of Tennessee System Administration Information Security Office (UTSA ISO) at (865) 974-8907, or sandy@tennessee.edu.

Before you Begin

Please read the SAQ section labeled “Before you Begin” carefully to ensure you are completing the correct SAQ. If the items listed for SAQ A merchants do not match your current procedures, please contact the Treasurer’s Office. If your procedures ever change from those you listed when you applied for the MID, you must contact the Treasurer’s Office at once. The procedures detailed for the MID you requested are specific to that MID. Any changes to the procedures may cause a change in the SAQ type required and the Treasurer’s Office, as well as your Chief Business Officer, will need to know.

Section 1. Assessment Information

Part 1: Merchant and Qualified Security Assessor Information

Part 1a: Merchant Organization Information

- This should be the contact information for the individual responsible for completing the SAQ.
  - The person listed here will be the primary contact if there are any questions or problems regarding the information in the SAQ, as well as for assessments, audits, and data breaches.
  - The person who completes the SAQ should be the same person who is attesting to the information in the SAQ by signing Part 3b.
  - Company Name should be University of Tennessee or University of Tennessee Foundation.
  - For DBA, each merchant area should use the DBA name assigned by the UT Treasurer’s Office or UTFI when the Merchant ID was applied for, unless a name change has since been approved by the Treasurer’s Office/UTFI and Elavon. Include the MID, as well.
  - Include the complete URL for your payment site.

Part 1b: Qualified Security Assessor Company Information (if applicable)

- A Qualified Security Assessor (QSA) is a company approved by the PCI Security Standards Council to conduct PCI DSS on-site assessments.
  - **The UTSA ISO does internal on-site assessments for merchants at UT and UTFI, so this section should be left blank.**
  - QSAs are organizations contracted to do assessments.
    - ♦ You are required to have a QSA perform your assessment if:
      - You are a Level 1 or Level 2 merchant, which is based on the quantity of transactions; and/or
      - Your acquiring bank has determined that there are certain increased risk factors (i.e., a past data breach).
      - UT and UTFI do not currently fall under either of these categories.

Part 2: Executive Summary

Part 2a: Type of merchant business (check all that apply)

- Ensure you have checked at least one of these choices.
  - If “Others” is checked, please specify the type.
  - Check the appropriate box(es) for the payment channel(s) used in your merchant area for all MIDs.
  - Check the appropriate box(es) for the payment channel(s) covered by this SAQ only.
  - The payment channels in your merchant area may be different than the payment channel(s) covered by this SAQ if you have more than one MID.

Part 2b: Description of Payment Card Business

- State how and in what capacity your merchant area stores, processes, and/or transmits cardholder data.
  - Give a short description.

Part 2c: Locations

- List the types of facilities to be included in the on-site PCI reviews.
- For each type of facility, list EVERY location where credit card payments are processed for this MID.

Part 2d: Payment Applications

- Check “Yes” or “No” for whether you use one or more Payment Applications.
- Please provide the following information regarding the Payment Applications your organization uses:
  - Payment Application
    - Payment Applications are those that store, process, or transmit cardholder data as part of authorization or settlement.
    - Examples of Payment Applications include:
      - Paciolan, Inc.
      - VeriFone, Inc.
      - Elavon Merchant Services
  - Version Number
    - You should always have the latest available version of the Payment Application.
    - If you do not have the latest version of the Payment Application, contact the provider.
  - Application Vendor
    - This is the company with who you are working that supplies and maintains the Payment Application.
  - Is application PA-DSS Listed?
    - UT and UTFI merchants should be using only PA-DSS applications and these are reviewed and approved by the Treasurer’s Office.

  - PA-DSS Listing Expiry date (if applicable)
    - The newest POS devices may auto-update, so make sure your device does this.
    - Otherwise, remember that the Payment Applications are updated every 12-18 months, so this date must not be older than that range.
    - Please call your Payment Application provider if you need help determining the latest version and Last Expiry date.

<u>Part 2e: Description of Environment</u>

- Give a brief summary description of the environment covered by this assessment.
- **Check "Yes" to using network segmentation to affect the scope of your PCI DSS environment, as each affected campus has a Cardholder Data Environment (CDE) for handling SAQ C merchants.**

<u>Part 2f: Third-Party Service Providers</u>

- Does your company have a relationship with one or more third-party agents?
  - **All UT and UTFI merchants should check "Yes" for this.**
  - A third-party agent, or service provider, provides payment-related services, directly or indirectly, and/or stores, processes, or transmits cardholder data.
  - <u>If you have a contract with another organization dealing with payment card processing, you have a relationship with a third-party agent.</u>
  - Examples of third-party agents are gateways (e.g., TouchNet) and web-hosting companies.

<u>Part 2g: Eligibility to Complete SAQ A</u>

- **You must check all six of these boxes in order to be eligible to complete SAQ A.**
  - If you store paper reports or cardholder data on paper, you must meet all items in Requirement 9.

Section 2: Self-Assessment Questionnaire A

- **Please enter the Self-assessment completion date.**

Implement Strong Access Control Measures

<u>Requirement 9: Restrict physical access to cardholder data</u>

- 9.5: Are all media physically secured?
  - **You cannot answer "N/A" to this question if your store paper receipts and reports!**
  - **PCI DSS requires written procedures for securely storing all media.**
  - This will be in the merchant's internal documentation.
  - Media for SAQ A merchants is paper only, so this means any kind of paper receipts and paper reports related to payment card transactions.
  - Do not allow media to be left to unauthorized viewing, copying, or scanning.
  - Keep media stored in a locked area where minimal people have access and be able to show those people are the only ones with keys and/or swipe access.

- 9.6 (a): Is strict control maintained over the internal or external distribution of any kind of media?
    - **You cannot answer “N/A” to this question if your store paper receipts and reports!**
    - **PCI DSS requires that you have a written policy for maintaining control over internal and external distribution of any kind of media.**
    - Strict control means that you keep a record of the media (even paper!), what kind of data is stored on it, as well as if and how it is sent to any other location.
- 9.6 (b): Do controls include the following:
    - 9.6.1: Is media classified so the sensitivity of the data can be determined?
        - **You cannot answer “N/A” to this question if your store paper receipts and reports!**
        - **You are required to have written procedures for classifying the media in your merchant area.**
        - This will be in the merchant’s internal documentation.
        - See UT Policy IT0115: *Information and Computer System Classification* for the policy.
    - 9.6.2: Is media sent by secured courier or other delivery method that can be accurately tracked?
        - **PCI DSS requires that you have a log that keeps track of this; and**
        - **The log must be authorized by management.**
        - If media is sent from your department to another (i.e., a business office for doing the deposits), keep a log with information showing who took the media and when.
        - Be prepared to show this log.
    - 9.6.3: Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?
        - **PCI DSS requires that you keep a log for tracking all media (paper) that is moved from the secured area.**
        - **Management must approve the process (i.e., sign the log) before moving the media.**
        - Be prepared to show tracking logs for any media that is moved from a secured area, along with proper management authorization.
- 9.7: Is strict control maintained over the storage and accessibility of media?
    - **PCI DSS requires that you have an internal written policy covering the storage and access of any media (paper) and it must define these requirements:**
        - **Controlling storage of media (i.e., where you put it);**
        - **Controlling maintenance of all media (i.e., your procedures for how you keep control over the media); and**
        - **Periodic media inventory (i.e., when is it inventoried, by whom, and what methods are used).**
    - This will be in the merchant’s internal documentation.
- 9.8 (a): Is all media destroyed when it is no longer needed for business or legal reasons?
    - UT Policy FI0120: *Records Management* should cover this, but make sure it applies to your area.

- 9.8 (c): Is media destruction performed as follows:
    - 9.8.1 (a): Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?
        - ♦ This should be in the merchant's internal documentation.
        - ♦ Paper must be properly shredded with a cross-cut shredder, or it can be incinerated or pulped.
        - ♦ If you have a third-party company do the shredding, keep a log that includes information such as who picked up the media, the date, and what was to be shredded.
    - 9.8.1 (b): Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?
        - ♦ Any container storing cardholder data to be destroyed must have a lock on it to prevent access to the contents.
        - ♦ If you are outsourcing your shredding to a company like Cintas, they are to provide you with a locked "to-be-shredded" container.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses security for all personnel

- 12.8: Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows?
    - 12.8.1: Is a list of service providers maintained?
        - ♦ Identify service providers with whom you share cardholder data.
        - ♦ **PCI DSS requires you to keep an up-to-date list of service providers.**
    - 12.8.2: Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment?
        - ♦ **Verify your contract/written agreement with the service provider stays updated and that you know where the contract/agreement is when asked.**
        - ♦ This contract/written agreement must include the service provider's acknowledgement of their responsibility for securing cardholder data.
        - ♦ See UT Policy FI0311 – *Credit Card Processing*, section 13, Outsource Requirements – 3rd Party Service Provider.
        - ♦ The written agreement is likely on file in your campus Business Office or, depending on who the service provider is, in the Treasurer's Office.
    - 12.8.3: Is there an established process for engaging service providers, including proper due diligence prior to engagement?
        - ♦ **Confirm that all policies and procedures have been documented and followed including due diligence before engaging any service provider.**
        - ♦ See UT Policy FI0311 – *Credit Card Processing*, Outsource Requirements – 3rd Party Service Provider.

- 12.8.4: Is a program maintained to monitor services providers' PCI DSS compliance status at least annually?
    - **PCI DSS requires that you have a written procedure stating how you monitor your service provider's PCI DSS compliance status.**
    - This will be in the merchant's internal documentation.
    - ♦ Please email sandy@tennessee.edu should you need assistance finding your provider's compliance status.
- 12.8.5: Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?
    - ♦ Be prepared to show this information, which should be a part of the contract you have with the service provider.
    - ♦ If you do not keep a copy of the contract with your service provider in your merchant area, know where it is kept.
    - ♦ The Treasurer's Office maintains the contract with Elavon.

Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

- There is nothing to complete here for SAQ A.

Appendix B: Compensating Controls Worksheet

- In the rare case you may be able to use compensating controls, use this worksheet to document.
- If you have more than one requirement for which compensating controls apply, you must complete a separate worksheet for each requirement.

Appendix C: Explanation of Non-Applicability

- **If your response to *ANY* requirement is "N/A" in the Special column, you must explain here why that requirement does not apply to your merchant area.**

Section 3: Validation and Attestation Details

Part 3: PCI DSS Validation

- Please add the completion date.
- You must check either "Compliant" or "Non-Compliant".
    - This has to match your responses in Part 4.
    - If even one item in Part 4 is marked with a "No" response, then you must mark "Non-Compliant" in Part 3 and give a Target Date for Compliance.
    - There should be nothing at UT marked "Compliant but with Legal exception," but if you feel this applies to your merchant area, please contact the Treasurer's Office or the UTSA ISO immediately.

Part 3a. Acknowledgement of Status

- You must be able to check all seven of these boxes to confirm that you have done these things.

- Add the version of SAQ (v3.1, Rev 1.1) on the first item.
- Add Qualys as the AVS on the seventh item.

Part 3b. Merchant Attestation

- Signature is required and should be the same as the person shown in Part 1a.
- After completion of the SAQ, forward to your campus Chief Business Officer (CBO) for review and signature.

Part 3c. QSA Acknowledgement (if applicable)

- **You should leave this section blank.**

Part 3d. ISA Acknowledgement (if applicable)

- **You should leave this section blank.**

Part 4. Action Plan for Non-Compliant Status

- **You must check “Yes” or “No” for each requirement.**
  - If any question under a requirement is checked “No,” then you must check “No” for your compliance status on that requirement.
  - If you check “No” for Compliance Status, you must give a remediation date and action for each requirement that is non-compliant.

Glossary

Acceptable Use of Information Technology Resources (AUP) – The University of Tennessee's policy governing the use of the University's information technology resources.

Acquirer – Also known as merchant bank or acquiring bank, an acquirer is the financial institution that provides merchants with payment card processing or merchant accounts. The acquirer works directly with the merchant and acts as a processor to authorize card purchases and provide settlement. The Acquiring Bank has a contract *(merchant account)* directly with the merchant or indirectly through an independent Processor providing the Merchant with a line of credit.

Authentication – Authentication is the process of verifying the identity of an individual, device, or process. Authentication factors include something you know (password/passphrase), something you have (token device, smart card), and/or something you are (biometrics).

Authentication Credentials – Authentication credentials are typically the combination of a user name and authentication factor(s). (see Authentication)

Authorization – Authorization, in the context of access control, determines what a user can do after successful authentication. Authorization, in the context of payment card transactions, occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.

Card Skimmer – A card skimmer is a physical device, often attached to a valid POS or other card-reading device, designed to illicitly capture and/or store information from a payment card.

Cardholder – The customer to whom a payment card is issued or an individual authorized to use the payment card is known as the cardholder.

Cardholder Data (CHD) – Cardholder data is any personally identifiable data associated with a cardholder's account. At a minimum, CHD consists of the full primary account number (PAN), but may also consist of the full PAN plus any of the following: cardholder name, expiration date, and/or service code.

Cardholder Data Environment (CDE) – The cardholder data environment consists of the people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data, including any connected system components.

Compromise – A compromise, also known as data breach, is an intrusion into a computer system that can lead to an unauthorized disclosure or theft, modification, or destruction of cardholder data.

Data Flow Diagram – A data flow diagram uses a graphical representation to show how data flows through an application, network, and/or system. A PCI data flow diagram shows a payment card transaction from start to finish.

eCommerce – eCommerce is an electronic transaction containing payment card and/or cardholder data.

EMV Chip Card Technology – EMV, or chip-and-PIN, technology will replace the much less secure magnetic stripe card in the United Sates in 2015. Chip cards are standard bank cards that have an embedded micro computer chip, and may require a PIN in place of a signature. This type of technology is used to combat fraud.

Encryption – Encryption is the process of converting information into a form that only authorized parties can read with the use of a specific cryptographic key.

File Integrity Monitoring – File integrity monitoring is the technique or technology under which specific files or logs are monitored to detect if they have been modified. When critical files or logs are modified, alerts should be sent to the appropriate Information Security Office.

File-Level Encryption – File-level encryption can be the hardware or software used for encrypting the full contents of specific files.

Firewall – A firewall is a hardware and/or software technology that protects network resources for unauthorized access. A firewall permits or restricts traffic between networks based on a set of firewall rules.

Issuer – An issuer, also referred to as issuing bank or issuing financial institution, is the entity that issues payment cards or performs issuing services.

Least Privilege – Least privilege is the principle of having the minimum access and/or privileges necessary to perform the roles and responsibilities of the job function.

Masking – Masking is the act of redacting or concealing CHD when displayed or printed, and is a PCI DSS requirement for when there is no legitimate business need to see the full PAN.

Merchant – The acquiring bank contract with the merchant is informally referred to as a "merchant account." The arrangement is in fact a line of credit and not a bank account. Under the contract, the acquiring bank exchanges funds with issuing banks on behalf of the merchant, and pays the merchant for the net balance of its daily payment card activity.

Merchant’s Internal Documentation – PCI DSS requires that merchants document many specific policies and procedures for processing, storing, and transmitting cardholder data. Many of the internal policies and procedures are documented, for your convenience, in the PCI DSS Internal Policies and Procedures template found on UT’s PCI Compliance website at http://security.tennessee.edu/pci-dss-compliance-information/. Please add your own departmental information where highlighted.

Network Segmentation – Network segmentation isolates system components that store, process, or transmit CHD from systems that do not.

Payment Application – A payment application is a software application that stores, processes, or transmits CHD electronically. Payment applications include Point of Sale systems and eCommerce systems.

Payment Card – A payment card can be a credit card (Visa, AMEX, MasterCard, Discover, etc.) or a debit card.

Payment System – A payment system is any application, system, or process that handles the payment card or cardholder data either electronically or manually.

Personally Identifiable Information – Personally Identifiable Information, or PII, is that information used to identify or trace an individual’s identity. This can include but is not limited to name, address, date of birth, social security number, biometric data, etc.

Personnel – Full-time and part-time employees, temporary employees, contractors, and consultants who are “resident” on the entity’s site or otherwise have access to the cardholder data environment.

PIN – PIN is an acronym for “personal identification number,” the numeric password known only to the user and a system to authenticate the user to that system. A PIN may also be the one used in an EMV chip card where the PIN replaces the cardholder’s signature.

PIN Block – A PIN block is a block of data used to encapsulate a PIN during processing. It is composed of the PIN, the PIN length, and may contain a subset of the PAN.

Policy – A PCI policy contains the rules governing the acceptable use of computing resources, security practices, and guiding development of operational procedures.

POS – POS, or Point of Sale, is the hardware and/or software used to process payment card transactions at merchant locations.

Primary Account Number (PAN) – The primary account number, or account number, is the unique payment card number for credit/debit cards that identifies the issuer and the particular cardholder account.

Procedure – A procedure is the “How to” for a policy and describes how the policy is to be implemented.

Role Based Access Control (RBAC) – Role based access control is an implementation for restricting system access to authorized users based on role.

Separation of Duties – Separation of duties of the practice of dividing steps in a function among different individuals, so one individual cannot threaten the process. It is a measure of checks and balances.

Service Code – The service code is the three-digit or four-digit value in the magnetic stripe that follows the expiration date of the payment card on the track data. It can be used for defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.

Track Data – Track data, also called full track data and magnetic-stripe data, is the data encoded in the magnetic stripe or chip used for authentication or authorization during payment processing. This data can be the magnetic-stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe.

Two-Factor Authentication – Two-factor authentication is a two-step process to verify the identity of a user trying to access a system or network. These factors include: 1) something you know, such as a password, passphrase, or PIN; 2) something you have, such as a token or smart card; and 3) something you are, such as biometric data. For two-factor authentication you must use at least two of these three factors, and cannot use two of the same factor (i.e., a username and a password).

Transaction Data – Data related to an electronic payment card transaction.

UT or UTFI Merchant – A UT or UTFI department/office/organization that collects payments, electronically or manually, via payment card OR is otherwise involved in storing, processing, transmitting, or receiving payment card or cardholder data.

Virtual Payment Terminal – A virtual payment terminal is browser-based access to an acquirer, processor, or third-party service provider website to authorize payment card transactions.

Vulnerability – A vulnerability is a weakness in a system that can result in a compromise or data breach.

Web Application – A web application is general accessed through a web browser or through web services.