Payment Card Industry Data Security Standard Self-Assessment Questionnaire C 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 University of Tennessee (UT) and University of Tennessee Foundation, Inc. (UTFI) merchants completing Payment Card Industry Data Security Standard (PCI DSS) Self-Assessment Questionnaire (SAQ) C. SAQ C is for merchants with payment application systems connected to the Internet (i.e., UT's wired network) and NO electronic storage. These payment applications are connected to the Internet because 1) the payment application is on a merchant-owned computer connected to the Internet, or 2) the payment application is connected to the Internet to transmit cardholder data. When answering the questions in SAQ C, 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 policy(s), 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 C 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 C</u>

- **You must check all five of these boxes in order to be eligible to complete SAQ C.**
- The fifth statement is not saying that you are definitely storing cardholder data.
  - This statement is saying if you do store cardholder data that it is <u>ONLY</u> on paper and has not been received via email or other electronic method.
  - If you store cardholder data on paper, you must meet all items in Requirement 9.

Section 2: Self-Assessment Questionnaire C

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

Build and Maintain a Secure Network and Systems

<u>Requirement 1: Install and maintain a firewall configuration to protect data</u>

- **Merchants are responsible for working with the appropriate campus Chief Information Officer and/or Information Security Officer (ISO), and campus network group to get all PCI systems in their scope added to the PCI firewall zone.**
- **The campus network group should have their own documented firewall and router configuration standards.**
- 1.2: Do firewall and router configurations restrict connections between untrusted networks and any system in the cardholder data environment as follows:

    - 1.2.1 (a): Is inbound and outbound traffic restricted to that which is necessary for the cardholder data environment?
        - ♦ **You may answer “Yes” to this question.**
        - ♦ The UTSA ISO works with the campus network groups to verify this requirement is met and maintained.
    - 1.2.1 (b): Is all other inbound and outbound traffic specifically denied (for example by using an explicit “deny all” or an implicit deny after allow statement)?
        - ♦ **You may answer “Yes” to this question.**
        - ♦ The UTSA ISO works with the campus network groups to verify this requirement is met and maintained.
    - 1.2.3: Are perimeter firewalls installed between all wireless networks and the cardholder data environment, and are these firewalls configured to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment?
        - ♦ **You may answer “Yes” to this question.**
        - ♦ The UTSA ISO works with the campus network groups to verify this requirement is met and maintained.
- 1.3: Is direct public access prohibited between the Internet and any system component in the cardholder data environment, as follows:
    - 1.3.3: Are direct connections prohibited for inbound or outbound traffic between the Internet and the cardholder data environment?
        - ♦ **You may answer “Yes” to this question.**
        - ♦ The UTSA ISO works with the campus network groups to verify this requirement is met and maintained.
    - 1.3.5: Is outbound traffic from the cardholder data environment to the Internet explicitly authorized?
        - ♦ **You may answer “Yes” to this question.**
        - ♦ The UTSA ISO works with the campus network groups to verify this requirement is met and maintained.
    - 1.3.6: Is stateful inspection, also known as dynamic packet filtering, implemented—that is, only established connections are allowed into the network?
        - ♦ **You may answer “Yes” to this question.**
        - ♦ The UTSA ISO works with the campus network groups to verify this requirement is met and maintained.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- 2.1 (a): Are vendor-supplied defaults always changed before installing a system on the network?
    - Vendor-supplied defaults include but are not limited to account names, passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.

    - ALL default passwords must be changed for all operating systems, applications, system accounts, POS terminals, software that provides security services, and SNMP community strings.
    - Default account names, such as “Administrator” and “Guest,” must be changed.
    - Be prepared to show documentation of vendor-supplied account/password policies to verify these have been changed.
    - Be prepared to show accounts on random systems.
- 2.1 (b): Are unnecessary default accounts removed or disabled before installing a system on the network?
    - Be prepared to show documentation of vendor-supplied account/password policies to verify these have been changed.
    - Be prepared to show accounts on random systems.
- 2.1.1: For wireless environments connected to the cardholder data environment or transmitting cardholder data, are ALL wireless vendor defaults changed at installations, as follows:
    - **There are multiple firewalls in place which do not allow the wireless network to connect to the cardholder data environment.**
- 2.1.1 (a): Are encryption keys changed from default at installation, and changed anytime anyone with knowledge of the keys leaves the company or changes positions?
    - **You may answer “N/A” to this question.**
    - **Be sure to add the explanation, “Credit card processing is prohibited over the UT wireless network,” in Appendix C.**
    - Check with your local network group to ensure this is being done.
- 2.1.1 (b) Are default SNMP community strings on wireless devices changed at installation?
    - **You may answer “N/A” to this question.**
    - **Be sure to add the explanation, “Credit card processing is prohibited over the UT wireless network,” in Appendix C.**
    - Check with your local network group to ensure this is being done.
- 2.1.1 (c): Are default passwords/passphrases on access points changed at installation?
    - **You may answer “N/A” to this question.**
    - **Be sure to add the explanation, “Credit card processing is prohibited over the UT wireless network,” in Appendix C.**
- 2.1.1 (d): Is firmware on wireless devices updated to support strong encryption for authentication and transmission over wireless networks?
    - **You may answer “N/A” to this question.**
    - **Be sure to add the explanation, “Credit card processing is prohibited over the UT wireless network,” in Appendix C.**
- 2.1.1 (e): Are other security-related wireless vendor defaults changed, if applicable?
    - **You may answer “N/A” to this question.**
    - **Be sure to add the explanation, “Credit card processing is prohibited over the UT wireless network,” in Appendix C.**

- 2.2 (a): Are configuration standards developed for all system components and are they consistent with industry-accepted system hardening standards?
  - **PCI DSS requires that you have documented system configuration standards to be implemented in your merchant area.**
  - For assistance with these system hardening standards, refer to the CIS benchmarks, found at http://benchmarks.cisecurity.org/, or work with your campus CIO/ISO.
- 2.2 (b): Are system configuration standards updated as new vulnerability issues are identified, as defined in Requirement 6.1?
  - **This must be part of the merchant-documented processes in the system hardening standards.**
- 2.2 (c): Are system configuration standards applied with new systems are configured?
  - Be prepared to show how you have applied these configuration standards.
- 2.2 (d): Do system configuration standards include all of the following:
  - Changing of all vender-supplied defaults and elimination of unnecessary default accounts?
  - Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server?
  - Enabling only necessary services, protocols, daemons, etc., as required for the function of the system?
  - Implementing additional security features for any required services, protocols, or daemons that are considered to be insecure?
  - Configuring system security parameters to prevent misuse?
  - Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers?
    - **This must be part of the merchant-documented processes in the system hardening standards.**
- 2.2.1 (a): Is only one primary function implemented per server, to prevent functions that require different security levels from co-existing on the same server?
  - **This must be included in the merchant's internal documentation.**
  - State the server's host name and describe the function(s).
- 2.2.1 (b) If virtualization technologies are used, is only one primary function implemented per virtual system component or device?
  - **If using VMs, this must be described in the merchant's internal documentation.**
  - If virtual technologies are not used, answer "N/A" and explain in Appendix C.
- 2.2.2 (a): Are only necessary services, protocols, daemons, etc., enabled as required for the function of the system (services and protocols not directly needed to perform the device's specified function are disabled)?
  - **PCI DSS states that you must have documentation identifying the enabled services, daemons, and protocols necessary for each system component.**
  - Use secured technologies such as SSH, S-FTP, TLS, or IPSec VPN should be used to protect insecure services like NetBIOS, Telnet, FTP, etc.
    - ♦ **You must include this kind of information in the required documentation.**

- 2.2.2 (b): Are all enabled insecure services, daemons, or protocols justified per documented configuration standards?
    - **PCI DSS requires that you maintain a list of all enabled insecure services, daemons, or protocols, and the justification for each.**
- 2.2.3: Are additional security features documented and implemented for any required services, protocols, or daemons that are considered to be insecure?
    - **PCI DSS requires that you maintain a list of these additional security features.**
- 2.2.4 (a): Are system administrators and/or personnel that configure system components knowledgeable about common security parameter settings for those system components?
    - Be able to provide verification that system administrators have knowledge of common security parameter settings.
- 2.2.4 (b): Are common system security parameters settings included in the system configuration standards?
    - **These settings must be documented in the merchant's system configurations standards.**
- 2.2.4 (c): Are security parameter settings set appropriately on system components?
    - Be able to show verification of the settings documented in the merchant's system configurations standards.
- 2.2.5 (a): Has all unnecessary functionality—such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers—been removed?
    - Be able to show verification that all unnecessary functionality has been removed.
- 2.2.5 (b): Are enabled functions documented and do they support secure configuration?
    - **PCI DSS requires that you maintain a list of all enabled functions and show they support secure configuration.**
- 2.2.5 (c): Is only documented functionality present on system components?
    - Be able to verify that the only functionality present on the systems are what you have documented.
- 2.3: Is non-console administrative access encrypted as follows:
  Use technologies such as SSH, VPN, or TLS or web-based management and other non-console administrative access.
    - 2.3 (a): Is all non-console administrative access encrypted with strong cryptography, and is a strong encryption method invoked before the administrator's password is requested?
        - PCI DSS requires that strong encryption must be used if using remote login.
        - This is in addition to the two-factor authentication in Requirement 8.3.
        - Always log into the VPN before remoting to that PCI system.
        - If you need assistance with the VPN at your campus, please call your local HelpDesk.
    - 2.3 (b): Are system services and parameter files configured to prevent the use of Telnet and other insecure remote login commands?
        - Disable Telnet and other similar insecure services.
        - Be able to show that these insecure remote login commands are not available for use.

    - 2.3 (c): Is administrator access to web-based management interfaces encrypted with strong cryptography?
        - ♦ Be able to show how administrator access is configured to require strong cryptography.
    - 2.3 (d): For the technology in use, is strong cryptography implemented according to industry best practice and/or vendor recommendations?
        - ♦ Be able to show the vendor documentation verifying that strong cryptography is properly implemented.
    - 2.3 (e): For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols:
      Is there documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS?
        - ♦ Be able to show supporting documentation that verifies POS POI devices are not susceptible to known exploits for SSL/early TLS.
        - ♦ OR do not use SSL/early TLS!
            - ▪ If you are not using SSL/early TLS termination points for connecting POS POI terminals, use "N/A" and state this explanation in Appendix C.
    - 2.3 (f): For all other environments using SSL and/or early TLS:
      Does the documented Risk Mitigation and Migration Plan include the following:
        - Description of usage, including: what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment;
        - Risk assessment results and risk reduction controls in place;
        - Description of processes to monitor for new vulnerabilities associated with SSL/early TLS;
        - Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments;
        - Overview of migration project plan including target migration completion date no later than 30th June 2016.
        - ○ **PCI DSS requires that you include this information in the Risk Mitigation and Migration Plan.**
- 2.5: Are security policies and operational procedures for managing vendor defaults and other security parameters:
    - Documented
    - In uses
    - Known to all affected parties?
    - ○ **PCI DSS requires that these policies and procedures are documented and shared with all affected parties.**

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

- 3.2 (c): Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?
  - **PCI DSS requires that the merchant's internal documentation must include a written process for securely deleting sensitive authentication data.**
  - Sensitive authentication data includes, but is not limited to the card validation code or value (CVC or CVV), personal identification number (PIN), and/or PIN block, and can be used to generate fake payment cards and create fraudulent transactions.
  - Sensitive authentication can be received in card-not-present situations, so you must have procedures for securely deleting the data.
- 3.2 (d): Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted)?
  - 3.2.1: The full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored after authorization?
    This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.
    - ♦ **PCI DSS requires that you have written policies for not storing the contents of any track.**
    - ♦ This will be in the merchant's internal documentation.
    - ♦ Be able to show system components (via incoming data transactions, all logs, history files, trace files, database contents, etc.) do not store the full contents of any track from the magnetic stripe on the back of the card or equivalent data on a chip under any circumstance.
  - 3.2.2: The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored after authorization?
    - ♦ **PCI DSS requires that you have written policies for never storing the CVV/CVC.**
    - ♦ This is found in UT's FI0311 – *Credit Card Processing*, as well as the merchant's internal documentation.
    - ♦ Be able to show system components (via incoming data transactions, all logs, history files, trace files, database contents, etc.) do not store the card verification code or value under any circumstance.
  - 3.2.3: The personal identification number (PIN) or the encrypted PIN block is not stored after authorization?
    - ♦ **PCI DSS states that you must have written policies for never storing the PIN or encrypted PIN block.**
    - ♦ This will be in the merchant's internal documentation.
    - ♦ Be able to show system components (via incoming data transactions, all logs, history files, trace files, database contents, etc.) do not store PINs or encrypted PIN blocks on a chip under any circumstance.

- 3.3: Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only personnel with a legitimate business need can see the full PAN?
  - **PCI DSS states that you must have written policies requiring that the PAN is masked when displayed on computer screens, POS screens, paper receipts, faxes and/or paper reports, except for those with a legitimate business need to see the PAN.**
    - ♦ If applicable, you must identify and document those with a legitimate need to see the full PAN, along with the business need.
  - In addition to showing the written policies, be able to show that the full PAN is never displayed unless you have the required documentation for the legitimate business need.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

- 4.1 (a): Are strong cryptography and security protocols, such as TLS, SSH, or IPSEC, used to safeguard sensitive cardholder data during transmission over open, public networks?
  - Examples of open, public networks include but are not limited to:
    - Internet
    - Wireless technologies
    - Global System for Mobile communications (GSM)
    - General Packet Radio Service (GPRS)
  - **PCI DSS requires that these protocols are documented.**
  - Be able to show the configurations for using strong cryptography.
  - Be able to show what security protocol(s) you use.
- 4.1 (b): Are only trusted keys and/or certificates accepted?
  - **PCI DSS requires that these processes are documented.**
  - Be able to show verification that this is happening.
- 4.1 (c): Are security protocols implemented to use only secure configurations, and to not support insecure versions or configurations?
  - **PCI DSS requires that these configurations are documented.**
  - Be able to show configuration and implementation.
- 4.1 (d): Is the proper encryption strength implemented for the encryption methodology in use (check vendor recommendations/best practices)?
  - Follow vendor's documented recommendations or best practices for encryption strength.
  - Be able to show documentation and implementation.
- 4.1 (e): For TLS implementations, is TLS enabled whenever cardholder data is transmitted or received?
  - Does HTTPS appear as part of the browser Universal Record Locator (URL)?
    - ♦ Be able to verify this.
  - Is cardholder data required only when HTTPS appears in the URL?
    - ♦ Be able to verify that no CHD is required *unless* HTTPS appears in the URL.

- 4.1 (f): For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols:
  Is there documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS?
  - Be able to show supporting documentation that verifies POS POI devices are not susceptible to known exploits for SSL/early TLS.
  - OR do not use SSL/early TLS!
    - If you are not using SSL/early TLS termination points for connecting POS POI terminals, use "N/A" and state this explanation in Appendix C.
- 4.1 (g): For all other environments using SSL and/or early TLS:
  Does the documented Risk Mitigation and Migration Plan include the following:

- Description of usage, including: what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment;
- Risk assessment results and risk reduction controls in place;
- Description of processes to monitor for new vulnerabilities associated with SSL/early TLS;
- Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments;
- Overview of migration project plan including target migration completion date no later than 30th June 2016.
  - **PCI DSS requires that you include this information in the Risk Mitigation and Migration Plan.**

- 4.1.1: Are industry best practices (for example, IEEE 802.11i) used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment?
  - **You may answer "N/A" to this question.**
  - **Be sure to add the explanation, "Credit card processing is prohibited over the UT wireless network," in Appendix C.**
- 4.2 (b): Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?
  - **PCI DSS requires that you have a written policy stating that unprotected PANs must not be sent via end-user messaging technologies.**
  - This will be in the merchant's internal documentation.
  - End-user messaging technologies include email, instant messaging, chat, text, etc.

Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

- 5.1: Is anti-virus software deployed on all systems commonly affected by malicious software?
  - UT's *Acceptable Use of Information Technology Resources (AUP)* requires that all users install, use, and regularly update virus protection software.
  - Be able to show that AV is installed on systems processing credit cards.
- 5.1.1: Are all anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits)?
  - This question is asking if you have anti-virus software that is *capable* of detecting, removing, and protecting against all *known types* of malicious software.
    - *Known types* means the classes of malware such as viruses, Trojans, spyware, rootkits, adware, worms, etc.
  - **If you are using the university-supplied product, Microsoft System Center 2012**
  - **Endpoint Protection, then you may answer "Yes" to this question.**
    - Other products are capable of this, as well, but ensure it is a reputable product.
- 5.1.2: Are periodic evaluations performed to identify and evaluate evolving malware threats in order to confirm whether those systems considered to not be commonly affected by malicious software continue as such?
  - Be able to explain when and how these evaluations are performed.
- 5.2: Are all anti-virus mechanisms maintained as follows:
  - 5.2 (a): Are all anti-virus software and definitions kept current?
    - UT's *AUP* requires that you regularly update virus protection software.
    - Microsoft System Center 2012 Endpoint Protection gets its updates via Microsoft Updates.
    - If you get automatic updates for Microsoft Office, you should get Microsoft System Center 2012 Endpoint Protection updates without any changes.
  - 5.2 (b): Are automatic updates and periodic scans enabled and being performed?
    - Be able to verify that automatic updates and scans are still enabled.
  - 5.2 (c): Are all anti-virus mechanisms generating audit logs, and are logs retained in accordance with PCI DSS Requirement 10.7?
    - Requirement 10.7 states that you must retain audit trail history for at least one year, with a minimum of three months immediately available (online, archived, or restored from backup) for analysis.
    - By default, Microsoft System Center 2012 Endpoint Protection audit logs are generated and retained for a year.
    - Be able to show verification that this setting has not changed.
- 5.3: Are all anti-virus mechanisms:
  - Actively running?
  - Unable to be disabled or altered by users?

        - If the computer is in UT's Active Directory, GPOs should be applied to prevent users from making any changes to the application.
        - Be able to show verification that the anti-virus application is actively running and has not been altered.

Requirement 6: Develop and maintain secure systems and applications

- 6.1: Is there a process to identify security vulnerabilities, including the following:
  - Using reputable outside sources for vulnerability information?
  - Assigning a risk ranking to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities?
    - **You may answer "Yes" to this question.**
    - This process is documented in the UTSA ISO's *Vulnerability Scanning Standards*.
- 6.2 (a): Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?
  - **PCI DSS states that you must have a written policy requiring that merchants install applicable vendor-supplied security patches on all hardware and software.**
  - OS updates should be run regularly (preferably with auto-update) and must include the latest security patches.
  - If using Windows, choose "Microsoft Update" instead of "Windows Update" to get updates for Microsoft System Center 2012 Endpoint Protection, Microsoft Office, and other Microsoft apps, in addition to the OS.
  - This also requires that all other applications (i.e., Adobe, Java, browser, in-house apps, etc.) be patched.
  - Be able to show verification that the latest hardware and software patches have been applied.
- 6.2 (b): Are critical security patches installed within one month of release?
  - **PCI DSS states that you must have a written policy requiring that all critical security patches are installed within one month of its release.**
  - Please plan for testing patches as soon as released, if testing is necessary.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

- 7.1: Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows:
  - 7.1.2: Is access to privileged user IDs restricted as follows:
    - To least privileges necessary to perform job responsibilities?
    - Assigned only to roles that specifically require that privileged access?
    - ♦ **PCI DSS says you must have a written policy requiring that access rights for privileged user IDs is restricted to the least privileges ("need to know") to perform job responsibilities.**
    - ♦ This will be in the merchant's internal documentation.
  - 7.1.3: Is access assigned based on individual personnel's job classification and function?

- ♦ **PCI DSS says you must have a written policy requiring that privileges are assigned to individuals based on job classification and function.**
- ♦ This will be in the merchant's internal documentation.

<u>Requirement 8: Identify and authenticate access to system components</u>

- 8.1.5 (a): Are accounts used by vendors to access, support, or maintain system components via remote access enabled only during the time period needed and disabled when not in use?
  - These vendor accounts can be enabled when needed for access, support, and maintenance, but must be disabled immediately after necessary use.
  - Be able to show verification that the vendor accounts are disabled unless in use.
- 8.1.5 (b): Are vendor remote access accounts monitored when in use?
  - Be able to describe how these accounts are being monitored when in use.
- 8.3: Is two-factor authentication incorporated for remote network access originating from outside the network by personnel (including users and administrators) and all third parties (including vendor access for support or maintenance)?
  - Two-factor authentication must include two of the following items, but not two of the same item:
    - Something you know (i.e., password or passphrase)
    - Something you have (i.e., hardware or software tokens, smart card)
    - Something you are (i.e., biometrics)
  - **PCI DSS requires you to implement two-factor authentication for all remote network access.**
  - Should you need to implement two-factor authentication, contact your campus CIO.

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

- 9.1.2: Are physical and/or logical controls in place to restrict access to publicly accessible network jacks?
  - Be able to describe and show verification of how access is restricted.
- 9.5: Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)?
  - **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.
  - Removable electronic media includes external hard drives, USB flash drives, etc.
  - Media is also any kind of paper receipts, paper reports, and faxes related to payment card transactions.
  - Do not allow media to be left to unauthorized viewing, copying, or scanning.
  - Keep media (including paper) 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 (including 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 (including 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* <u>should</u> cover this, but make sure it applies to your area.
    - If the media is electronic media (e.g., hard drive, external hard drive, USB flash drive, etc.) it must be properly sanitized before reassigning or sending to surplus.
- 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.
        - If the media is paper, it 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.
- 9.9: Are devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution as follows:
    - 9.9 (a): Do policies and procedures require that a list of such devices be maintained?
        - **PCI DSS requires that you keep a documented list of all devices used for card-reading devices.**
        - **Please use the PCI Inventory Log found at** http://security.tennessee.edu/pci-dss-compliance-information/.
        - This applies to POS card swipe devices used for card-present situations, not computer and POS keypads.
    - 9.9 (b): Do policies and procedures require that devices are periodically inspected to look for tampering or substitution?
        - **PCI DSS requires that you have written policies and procedures detailing the inspection of POS card swipe devices.**
        - This will be in the merchant's internal documentation.
    - 9.9 (c): Do policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices?
        - **PCI DSS requires that you have written policies and procedures detailing the training for awareness and reporting regarding your POS devices.**
        - This will be in the merchant's internal documentation.
- 9.9.1 (a): Does the list of devices include the following?
    - Make, model of device
    - Location of device (for example, the address of the site or facility where the device is located)
    - Device serial number or other method of unique identification

  - Be able to show your list of devices with the required information, even if there is only one device in your merchant area.

- 9.9.1 (b): Is the list accurate and up to date?
  - Be able to show that the list is accurate.
  - Show a last updated date.
- 9.9.1 (c): Is the list of devices updated when devices are added, relocated, decommissioned, etc.?
  - Be able to show verification of the accuracy of the documented list.
- 9.9.2 (a): Are device surfaces periodically inspected to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) as follows?
  - **PCI DSS requires that you document your processes for inspecting your PCI devices.**
  - This will be in the merchant’s internal documentation.
  - Be able to show how you inspect your devices during the review.
- 9.9.2 (b): Are personnel aware of procedures for inspecting devices?
  - **PCI DSS requires that you document your processes for how you make your personnel aware of these procedures.**
  - This will be in the merchant’s internal documentation.
- 9.9.3: Are personnel trained to be aware of attempted tampering or replacement of devices, to include the following?
  - 9.9.3 (a): Do training materials for personnel at point-of-sale locations include the following?
    - Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
    - Do not install, replace, or return devices without verification.
    - Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
    - Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer)
      - This is included in the required annual training for all merchants.
  - 9.9.3 (b): Have personnel at point-of-sale locations received training, and are they aware of procedures to detect and report attempted tampering or replacement of devices?
    - The training is a part of the annual training included in UT’s formal security awareness program (Requirement 12.6).
      - **All UT and UTFI merchant employees who do any credit card processing are required to complete the training.**
      - The training will now be offered online through the year so all merchant employees will have access to it.
      - Current PCI security training may be found on the PCI Compliance website at http://security.tennessee.edu/pci-dss-compliance-information/.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

- 10.2: Are automated audit trails implemented for all system components to reconstruct the following events:
  - 10.2.2: All actions taken by any individual with root or administrative privileges?
    - Be able to show verification of processes and configurations.
  - 10.2.4: Invalid logical access attempts?
    - Be able to show verification of processes and configurations.
  - 10.2.5: Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges?
    - Be able to show verification of processes and configurations.
- 10.3: Are the following audit trail entries recorded for all system components for each event:
  - 10.3.1: User identification?
    - Be able to show verification of processes and configurations.
  - 10.3.2: Type of event?
    - Be able to show verification of processes and configurations.
  - 10.3.3: Date and time?
    - Be able to show verification of processes and configurations.
  - 10.3.4: Success or failure indication?
    - Be able to show verification of processes and configurations.
  - 10.3.5: Origination of event?
    - Be able to show verification of processes and configurations.
  - 10.3.6: Identity or name of affected data, system component, or resource?
    - Be able to show verification of processes and configurations.
- 10.6: Are logs and security events for all system components reviewed to identify anomalies or suspicious activity as follows?
  - 10.6.1 (b): Are the following logs and security events reviewed at least daily, either manually or via log tools?
    - All security events
    - Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD
    - Logs of all critical system components
    - Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)
      - Be able to show verification of processes and configurations.
  - 10.6.2 (b): Are logs of all other system components periodically reviewed—either manually or via log tools—based on the organization's policies and risk management strategy?
    - Be able to show verification of processes and configurations.

  - 10.6.3 (b): Is follow up to exceptions and anomalies identified during the review process performed?
    - Be able to show verification of processes and configurations.
- 10.7 (b): Are audit logs retained for at least one year?
  - Be able to show verification of processes and configurations.
- 10.7 (c): Are at least the last three months' logs immediately available for analysis?
  - Be able to show verification of processes and configurations.

Requirement 11: Regularly test security systems and processes

- 11.1 (a): Are processes implemented for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis?
  - **Note that Requirement 11.1 (use of a process to identify unauthorized wireless access points) must still be answered even if wireless is not in your network, since the process detects any rogue or unauthorized devices that may have been added without your knowledge.**
  - PCI DSS requires documentation defining these methods and processes.
- 11.1 (b): Does the methodology detect and identify any unauthorized wireless access points, including at least the following?
  - WLAN cards inserted into system components;
  - Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.); and
  - Wireless devices attached to a network port or network device.
    - **You may answer "Yes" to this question.**
    - The UTSA ISO works with the campus network groups to verify this requirement is met and maintained.
- 11.1 (c): If wireless scanning is utilized to identify authorized and unauthorized wireless access points, is the scan performed at least quarterly for all system components and facilities?
  - **You may answer "Yes" to this question.**
  - The UTSA ISO works with the campus network groups to verify this requirement is met and maintained.
- 11.1 (d): If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), is monitoring configured to generate alerts to notify personnel?
  - **You may answer "Yes" to this question.**
  - The UTSA ISO works with the campus network groups to verify this requirement is met and maintained.
- 11.1.1: Is an inventory of authorized wireless access points maintained and a business justification documented for all authorized wireless access points?
- 11.1.2 (a): Does the incident response plan define and require a response in the event that an unauthorized wireless access point is detected?
  - **PCI DSS requires that the IRP includes response procedures for when unauthorized wireless devices are detected.**
  - The IRP is also needed for Requirement 12.10.

- 11.1.2 (b): Is action taken when unauthorized wireless access points are found?
  - **PCI DSS requires documentation detailing this action.**
- 11.2: Are internal and external network vulnerability scans run at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), as follows:
- 11.2.1 (a): Are quarterly internal vulnerability scans performed?
  - **You may answer "Yes" to this question.**
  - Scanning details are documented in the UTSA ISO's *Vulnerability Scanning Standards*.
- 11.2.1 (b): Does the quarterly internal scan process include rescans as needed until all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved?
  - **You may answer "Yes" to this question.**
  - Scanning details are documented in the UTSA ISO's *Vulnerability Scanning Standards*.
- 11.2.1 (c): Are quarterly internal scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?
  - **You may answer "Yes" to this question.**
  - Scanning details are documented in the UTSA ISO's *Vulnerability Scanning Standards*.
- 11.2.2 (a): Are quarterly external vulnerability scans performed?
  - **You may answer "Yes" to this question.**
  - Scanning details are documented in the UTSA ISO's *Vulnerability Scanning Standards*.
- 11.2.2 (b): Do external quarterly scan results satisfy the *ASV Program Guide* requirements for a passing scan (for example, no vulnerabilities rated 4.0 or higher by the CVSS, and no automatic failures)?
  - **You may answer "Yes" to this question.**
  - Scanning details are documented in the UTSA ISO's *Vulnerability Scanning Standards*.
- 11.2.2 (c): Are quarterly external vulnerability scans performed by a PCI SSC Approved Scanning Vendor (ASV)?
  - **You may answer "Yes" to this question.**
  - Scanning details are documented in the UTSA ISO's *Vulnerability Scanning Standards*.
- 11.2.3 (a): Are internal and external scans, and rescans as needed, performed after any significant change?
  - **You may answer "Yes" to this question.**
  - Scanning details are documented in the UTSA ISO's *Vulnerability Scanning Standards*.
- 11.2.3 (b): Does the scan process include rescans until:
  - For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS,

    - For internal scans, a passing result is obtained or all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved?
        - **You may answer “Yes” to this question.**
        - Scanning details are documented in the UTSA ISO’s *Vulnerability Scanning Standards*.
- 11.2.3 (c): Are scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?
    - **You may answer “Yes” to this question.**
    - These details are documented in the UTSA ISO’s *Vulnerability Scanning Standards*.
- 11.3.4: If segmentation is used to isolate the CDE from other networks:
    - 11.3.4 (a): Are penetration-testing procedures defined to test all segmentation methods, to confirm they are operational and effective, and isolate all out-of-scope systems from in-scope systems in the CDE?
        - ♦ Penetration testing procedures are documented in the UTSA ISO’s *Penetration Testing Standards*.
    - 11.3.4 (b): Does penetration testing to verify segmentation controls meet the following?
        - Performed at least annually and after any changes to segmentation controls/methods
        - Covers all segmentation controls/methods in use
        - Verifies that segmentation methods are operational and effective, and isolate all our-of-scope systems from in-scope systems in the CDE.
        - ♦ Penetration testing details are documented in the UTSA ISO’s *Penetration Testing Standards*.
- 11.5 (a): Is a change-detection mechanism (for example, file-integrity monitoring tools) deployed within the cardholder data environment to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files?
    - Be able to show verification of system configurations and file-integrity monitoring tools configurations.
- 11.5 (b) Is the change-detection mechanism configured to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files, and do the tools perform critical file comparisons at least weekly?
    - Be able to show verification of system configurations and file-integrity monitoring tools configurations.
- 11.5.1: Is a process in place to respond to any alerts generated by the change-detection solution?
    - Be able to show verification of how alerts are investigated and resolved.

Maintain an Information Security Policy

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

- 12.1: Is a security policy established, published, maintained, and disseminated to all relevant personnel?
  - **PCI DSS requires an information security policy be in place and disseminated to relevant personnel, as well as relevant vendors and business partners.**
  - “Personnel” refers to any employee who has access to the company’s cardholder data environment.
  - Personnel should know these UT policies at a minimum:
    - FI0311 – *Credit Card Processing*;
    - IT0110 – *Acceptable Use of Information Technology Resources (AUP)*;
    - FI0115 – *Reconciling and Reviewing Departmental Ledgers*;
    - IT0115 – *Information and Computer System Classification*;
    - FI0120 – *Records Management*;
    - IT0121 – *Information Security Plan Creation and Data Breach Notification Procedures*; and
    - All internal policies you may have.
- 12.1.1: Is the security policy reviewed at least annually and updated when the environment changes?
  - **Your internal policies should include the requirement that the information security policy be reviewed at least annually and updated to reflect any change to business objectives and/or the risk environment.**
  - This will be in the merchant’s internal documentation.
  - This policy should detail how the information security policy is to be reviewed and updated as needed.
  - Please add “Reviewed” and “Updated” dates somewhere on the policy to show verification that you have done these things.
- 12.3: Are usage policies for critical technologies developed to define proper use of these technologies and require the following:
  - 12.3.1: Explicit approval by authorized parties to use the technologies?
    - Examples of critical technologies may include remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants [PDAs], email, and Internet usage.
    - **PCI DSS says you must have a written policy that requires users to have explicit approval from authorized parties to process credit card transactions.**
    - This will be in the merchant’s internal documentation.
    - UT does not allow the use of personally-owned devices for credit card processing.
  - 12.3.2: Authentication for use of the technology?
    - **PCI DSS states that your usage policy must include the requirement that all technology use be authenticated with user ID and password or other authentication item, such as two-factor authentication.**

- 12.3.3: A list of all such devices and personnel with access?
    - **PCI DSS says you must have a policy that requires you to keep a list of these devices and authorized users.**
    - Please use the *PCI Inventory Log* found at http://security.tennessee.edu/pci-dss-compliance-information/.
    - Keep the list of devices and authorized personnel updated.
- 12.3.5: Acceptable uses of the technologies?
    - **PCI DSS requires that your documentation defines what is considered acceptable use of the technology.**
    - This will be in the merchant's internal documentation.
- 12.3.6: Acceptable network locations for the technologies?
    - **Verify that your local network group has documented policies for allowing network locations only where they are deemed acceptable.**
- 12.3.8: Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity?
    - **Verify with your local network group that the VPN has an automatic disconnect after a specific period of inactivity.**
- 12.3.9: Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use?
    - **PCI DSS requires that your policy includes specifics on activation of technologies and immediate deactivation after use for each remote access technology.**

- 12.4: Do security policy and procedures clearly define information security responsibilities for all personnel?
    - UT Policy FI0311 – *Credit Card Processing* defines this.
    - **Ensure all personnel are aware of this policy and review it regularly.**
- 12.5 (b): Are the following security management responsibilities formally assigned to an individual or team:
    - 12.5.3: Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?
        - This is covered in UT Policy FI0311 – *Credit Card Processing.*
        - **Ensure all personnel are aware of this policy and review it regularly.**
- 12.6 (a): Is a formal security awareness program in place to make all personnel aware of the importance of cardholder data security?
    - **You may answer "Yes" to this question.**
    - Campus Chief Business Officers disseminate emails to personnel detailing the importance of cardholder data security.
    - Other PCI security awareness information may be sent to merchants via the Treasurer's Office using the UT PCI listserv.
    - The UTSA ISO provides annual PCI security training.
        - **All UT and UTFI merchant employees who do any credit card processing are required to complete the training.**

        - The training will now be offered online through the year so all merchant employees will have access to it.
        - Current PCI security training may be found on the PCI Compliance website at http://security.tennessee.edu/pci-dss-compliance-information/.

- 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.

- 12.10.1 (a): Has an incident response plan been created to be implemented in the event of system breach?
  - **The *PCI DSS Incident Response Plan* is found at http://security.tennessee.edu/pci-dss-compliance-information/.**
  - Please note that the University's official incident response plan is IT0122 – *Security Incident, Reporting, and Response*, but it does not specifically address PCI DSS.
- 12.10.1 (b): Does the plan address the following, at a minimum:
  - Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum?
  - Specific incident response procedures?
  - Business recovery and continuity procedures?
  - Data backup processes?
  - Analysis of legal requirements for reporting compromises?
  - Coverage and responses of all critical system components?
  - Reference or inclusion of incident response procedures from the payment brands?
    - The UTSA ISO maintains the breach notification procedures that specifically address these items.

Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

- There is nothing to complete here for SAQ C.

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.

<u>Part 3a. Acknowledgement of Status</u>

- You must be able to check all <u>seven</u> 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.

<u>Part 3b. Merchant Attestation</u>

- 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.

<u>Part 3c. QSA Acknowledgement (if applicable)</u>

- You should leave this section blank.

<u>Part 3d. ISA Acknowledgement (if applicable)</u>

- You should leave this section blank.

<u>Part 4. Action Plan for Non-Compliant Requirements</u>

- **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 <u>must</u> 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.