PCI Standards

Last Revision Date: April 26, 2019

Purpose: This document is designated to give further clarification and specifics to the PCI policies and procedures outlined in the UWSP Payment Card Processing and Compliance Policy document. The PCI Standards is meant to be a living document to be updated as new issues are identified in the payment card processing procedure. Many aspects of this document are very similar to its parent document, but in more explicit detail. Both documents should be used to create merchant level policy and procedure documents and assist the merchant in processing payment cards in compliance of the current PCI DSS version. PCI DSS v3.2.1

1. Merchants/Merchant Coordinators

1.1. **Merchants must designate a primary and a backup/secondary authority over the merchant account that will be responsible for the oversight of payment card transactions.** This designation is referred to as Merchant Coordinator and responsibilities include, but are not limited to, keeping an accurate list of employees and devices used in the payment card transaction, ensuring training of all employees using the device, reconciliation of account activity, and facilitating activities between the department and the PCI team. While not recommended, student employees may be appointed as a secondary authority if there are no other full-time employees available or able to be assigned additional responsibilities. Generally, the department/merchant coordinator or a seasoned full-time employee should be assigned primary authority over payment card transactions.

The Merchant Coordinator and backup/secondary authority must also sign annually the Payment Card Merchant Compliance Statement after reviewing the UWSP Payment Card Processing and Compliance Policy.

1.2. **Merchants must have a written policies and procedures document specific to their merchant account**. The document should be reviewed, and revised if needed, annually and sent to the PCI Team for review and approval. The merchant should upload the document into the PCI Merchants Microsoft Teams site for the PCI team (and other merchants) to review and to retain an archive.

1.3. **Self-assessment questionnaires must be completed annually**. The PCI Team along with Information Security will be involved to help merchants correctly assess what SAQ forms need to be filled out and will assist in answering questions within the SAQ that may not pertain to the merchant. The PCI Team will also assist in determining who will be responsible to fill out the SAQ forms and will make sure there is a separation of duties to prevent error or the perception of fraud.

1.4. **Departments who wish to become a payment card accepting merchant must first fill out the PCI Questionnaire – New Merchants document**. Submit the completed document to the PCI Team for review and approval. Consideration will be given to determine the scope (business process and IT functionality) of procuring a new merchant account. A similar questionnaire will also be used to assess merchant accounts annually and is located here: PCI Questionnaire. It may be helpful to review this document, so you know what to expect during the review and to help create a merchant level policy and procedure document.

2. Employee Training

2.1. **Employees who MAY have access to cardholder data must be trained upon hire and will be assigned training annually.** Even if an employee is not designated to handle cardholder data there might be a situation where they are exposed to it and should undergo training as a precautionary measure. A record of completion must be retained for documentation and record retention purposes.

The PCI Team will determine what training is acceptable and training will be assigned annually by the Information Security Office.

3. Processing and Collection

3.1. **Fax machines used to transmit payment card information to a merchant department must be standalone machines with appropriate physical security**; receipt or transmission of payment card data using a multi-function fax machine (copy/scan/fax) is not permitted. Approval to use fax machines must be received from the PCI Compliance Team. The fax machine must be kept in a locked room with limited access (only by employees who received PCI training). This includes limiting access to non-department employees like custodial staff.

3.2. **Email must never be used to transmit payment card or personal payment information**, nor should it be accepted as a method to supply such information. If payment card data is received in an email:

- The email should be replied to immediately with the payment card number deleted stating that “UWSP does not accept payment card data via email as it is not a secure method of transmitting data.”
- Provide alternate, compliant option(s) for payment.
- Delete the email from your inbox and delete the email from the ‘Trash’ folder.
- Contact the Information Security Office for further instructions.

3.3. **Merchants who wish to procure new device(s) for processing payment cards** must first reach out the PCI Team to get a list of approved devices supported by our payment processor.

3.4. **Merchants who wish to procure software for processing payment cards** must first reach out the PCI Team to see if there is already a vendor in place to serve the merchants needs. If the merchant wishes to use another vendor, they will be asked to complete and submit a PCI Questionnaire-New Merchants to the PCI Team to review.

3.5. **Systems not explicitly approved by the Information Security Office to accept cardholder data are NOT permitted**. This includes, but is not limited to, student projects (specifically CNMT 480 projects). A system that is unable to support a complaint method of taking payment cards will not be approved. However, this does not include in-house or student projects to create an online store or a shopping cart as part of the payment card transaction. The Information Security Office must conduct a security review and approve the project before the system can be used in production.

4. Device Protection

4.1. **Point of sale devices must be inspected for tampering periodically**. An inspection should consist of examining the device for anything abnormal such as skimmers, missing or broken seals, damage to the device, damage to external cable or broken port, or other materials that could mask damage or tampering. Compare the device to a picture of it and compare serial numbers (if possible). Contact the PCI Team with the make and model of the device and they will be able to assist you in identifying common tampering methods for the device if you are unsure.

4.1.1. **If the device is customer facing** (customer swipes the card) it must be inspected during opening and closing procedures. The employee should sign off that the device was inspected, and records should be kept to retain an audit trail.

4.1.2. **If the device is merchant facing** (employee swipes the card) it must be inspected weekly. Once again, the device must be signed off by the inspecting employee and records should be kept to retain an audit trial.

4.2. **Controls should also be put in place to protect the device for theft and prevent tampering**. Depending on the device, it can be locked down on a stand to make it immobile or kept behind a desk or teller window to limit access until it is needed. Staff need to be aware of suspicious behavior and reporting procedures in the event of suspected tampering or substitution.

4.3. **A device list must be kept up to date and should include the make/model, serial number, location, and status**. The list needs to be reviewed annually by the Merchant Coordinator and maintained within the merchant folder on the Microsoft Team site.

5. Mail and Order Forms

5.1 **The mail is not a secure method to transmit cardholder data.** Any business processes that require the use of mail services require special handling, delivery, and pickup from the campus central mail office.

5.2 **Cardholder data obtained using order forms must conform to storage and disposal standards provided in section 6: Storage and section 7: Disposal.** Forms must always be physically secured and disposed of as soon as business requirement for the data expire.

6. Storage

6.1. **Physical cardholder data must be stored in a locked cabinet with limited access**. The storage of cardholder data must be documented and approved with a legal or business need.

6.2. **Electronic cardholder data storage is not permitted**.

6.3. **The storage of sensitive authentication data** (Magnetic strip, CVV code, PIN) **is not permitted**.

7. Disposal

7.1. **Physical cardholder data must be destroyed with a cross-cut shredder** (confetti not strips).

7.2. **Electronic cardholder data must be destroyed by a PCI approved method**. Contact the Information Security Office for assistance.

7.3. **Cardholder data must be reviewed quarterly** to determine what should be destroyed or kept in storage.

8. Notifications

8.1. **In the event of a notification of non-compliance**, merchants must reach out the Information Security Office and the Controller's Office immediately to verify the claim and initiate necessary action steps.

8.2. **In the event of a suspected breach**, merchants must notify the Information Security Office immediately.

8.3. **Third party vendors should have the Information Security Office as a contact in the event of a security incident or a data breach**.

9. Reconciliation Standards

9.1. **Batch reports should be run on the merchant terminal daily.** Confirm the transactions ran on the terminal were also processed through the department cash register used to record sales.

9.2. **Reconcile the daily batch reports to the settlement reports saved in the Credit Card Merchants team site.** There are separate channels for Fifth Third and Official Payments daily batch reports. The daily files can be opened in Excel and saved to your own files to be sorted and or filtered as needed.

9.3. **Reconcile settlement reports to WISDM.** Verify the amounts from the settlement reports post correctly to the department ID the merchant terminal is programmed to. If revenue should be recorded to another department ID, request a transfer from the General Ledger Office.