University of Wisconsin Stevens Point

UWSP Merchant Services Policy and Procedures

Payment Card Processing and Compliance Policy

Effective Date: May 13, 2019
Last Revision Date: March 26, 2024

1. PURPOSE

University of Wisconsin-Stevens Point (UWSP) departments processing credit and debit card payments must take appropriate measures to prevent loss or disclosure of customer information including card numbers. Failure to comply with requirements imposed by the Payment Card Industry Security Standards Council (PCI SSC) may result in financial loss for many customers, fines imposed on the university, suspension of card processing privileges, and damage to the reputation of the unit and university. The purpose of this policy is to provide requirements and guidance for all credit and debit card processing activities for UWSP.

2. RESPONSIBLE CAMPUS DIRECTOR

Controller
Chief Information Officer

3. DEFINITIONS

Cardholder: The person to whom a payment card is issued, or any individual authorized to use the payment card.

Cardholder Data (CHD): At a minimum, cardholder data consists of the full Primary Account Number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, and/or service code. See Sensitive Authentication Data for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.

Cardholder Data Environment (CDE): A computer system or networked group of IT systems that processes, stores and/or transmits cardholder data or sensitive payment authentication data. A CDE also includes any component that directly connects to or supports this network.

High Risk Data: Any data where the unauthorized disclosure, alteration, loss, or destruction may: cause personal or institutional financial loss, or the unauthorized release of which would be a violation of a statute, act or law; constitute a violation of confidentiality agreed to as a condition of possessing or producing or transmitting data; cause significant reputational harm to the University; or require UWSP [UW System] to self-report to the government and/or provide public notice if the data is inappropriately accessed.

Merchant Account: A bank account that enables the holder to accept credit cards for payment.

Merchant Department: Any department or unit (can be a group of departments or a subset of a department) which has been approved to accept payment cards.

Payment Card: A financial transaction card (credit, debit, etc.) issued by a financial institution; also called Bankcard/Payment Card/Charge Card/Credit Card/Debit Card.

Payment Card Industry Data Security Standards (PCI DSS): A multifaceted security standard developed and owned by the major payment card companies that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. PCI DSS represents a common set of tools and measurements to help ensure the safe handling of sensitive information. The standard is comprised of 12 requirements that are organized in 6 logically related groups or "control objectives." Failure to conform to these standards can result in losing the ability to process payment card payments and being audited and/or fined.

Point-to-Point Encryption (P2PE): A comprehensive set of security requirements for point-to-point encryption solution providers, this PCI standard helps those solution providers validate their work. Using an approved point-to-point encryption solution will help merchants to reduce the value of stolen cardholder data because it will be unreadable to an unauthorized party. Solutions based on this standard also may help reduce the scope of their cardholder data environment – and make compliance easier.

Sensitive Authentication Data: Security-related information (including but not limited to card validation codes/values, full track data from the magnetic stripe or equivalent on a chip, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

Service Provider: A business entity that is not a payment brand but is directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This includes companies that provide services that control or could impact the security of cardholder data. Examples include service providers that provide managed firewalls, intrusion detection systems (IDS), and other services.

4. POLICY

UW Stevens Point departments that accept credit and debit cards as a form of payment are required to do so in accordance with state and federal laws, PCI Standards, UW System policy and in compliance with this policy and related cash handling procedural documents.

This policy will ensure ongoing compliance with PCI DSS and other applicable policies and standards; establish the governance structure for payment card processing and compliance activities; define responsibilities for payment card services at various process phases; and provide general guidelines regarding the handling of cardholder data.

Responsibilities

The Vice Chancellor for Business Affairs, Chief Financial Officer, has overall PCI DSS compliance authority for UW Stevens Point. The CFO hereby delegates to the Controller oversight of the PCI program in collaboration with the Chief Information Officer (CIO) and the authority to define responsibilities for payment card services at various process phases.

UW Stevens Point's PCI DSS compliance is a consolidated attestation of compliance. Consequently, one merchant who fails to meet PCI DSS requirements causes the entire institution to be out of compliance. Therefore, failure of any single merchant to maintain continuous compliance will result in cancellation of the merchant account to preserve and allow continuous operation for other critical business functions dependent on payment cards.

PCI Compliance Team

The PCI Compliance Team consists of representatives from Financial Operations, Information Technology, and merchant departments. This team reviews department requests to become new merchants and evaluates changes in merchant activities that impact PCI DSS compliance.

The PCI Compliance Team provides guidance for initial technical implementation of card payment processing for requesting merchants, as well as technical changes requested by merchants.

The team also coordinates all compliance activities related to PCI DSS including:

- Overseeing annual PCI DSS validation
- Coordinating remediation activities as required by PCI DSS or other applicable policies and standards
- Assisting with the completion of annual SAQ
- Making appropriate revisions to this policy, as needed

Financial Operations – Student Financial Services

The Financial Operations unit is responsible for initiating and maintaining the individual merchant accounts, assisting merchants with department business processes for payment card processing and compliance, and maintaining the institutional policy and procedures related to payment card processing and compliance. The Financial Operations - Student Financial Services unit is responsible for disbursing all revenue for merchant sales and processing all chargeback entries for applicable merchant fees.

Information Technology

The Department of Information Technology (IT) is responsible for maintaining and disseminating security policies and procedures that address PCI DSS requirements, establishing and testing UWSP's infrastructure and network environment, administering the annual PCI merchant training provided by UWS, and assisting merchants in completing the technical sections of the annual SAQ. IT will work closely with the contracted QSA to interpret PCI DSS requirements and to communicate and facilitate overall security and technical compliance with merchants.

IT is responsible for configuration and maintenance of centralized IT systems, facilitating merchant hardware and software configurations, and providing oversight of all computer systems and other IT resources to support compliance with PCI DSS and UW security requirements. IT will manage and provide training and tools to limit access to IT resources and cardholder data.

IT procurement and related contracts should include appropriate PCI DSS requirement clauses in all vendor and external entity contracts to ensure assignment of accountability for these policy requirements where PCI DSS applies for goods or services being acquired by UWSP.

Merchant Coordinators

Merchant Coordinators are responsible for ensuring that all business processes, IT environments and associated systems for accepting, processing, retaining, and disposing of cardholder data comply with PCI DSS.

Merchant Coordinators are responsible for developing and documenting the department's card handling procedures (review Section 5. Procedures – B. Payment Card Data Security for required components).

Merchant Coordinators are responsible for the reconciliation of the daily merchant account activity, ensuring the activity is reconciled to not only the settled processed report, but also the general ledger WISER activity no less than monthly. Any questionable or suspicious activity must be reported to the Bursar or the University Information Security Office immediately.

Merchant Coordinators are responsible for completing the annual SAQ in partnership with the PCI Compliance Team and IT. Merchant Coordinators, and their designated back-up, must attend a UWSP annual PCI merchant training. Merchant Coordinators are also responsible for ensuring all departmental employees who handle cardholder data receive the mandatory training offered online via Canvas by IT and Financial Operations.

Merchant account holders who fail to comply with established policies and procedures are subject to:

- Any fines imposed by the payment card industry;
- Any additional monetary costs associated with remediation, assessment, forensic analysis, or legal fees; and
- Suspension of the merchant account.

5. PROCEDURES

A. Payment Card Acceptance and Handling

A request for opening a new merchant account for accepting and processing payment cards is considered by the PCI Team. Any fees associated with the acceptance of cards as a form of payment will be charged to the merchant department which processed the card transaction.

Departments accepting payment cards on behalf of the institution must designate an individual within the department who will have primary authority and responsibility within the department for oversight of payment card transactions – the Merchant Coordinator. The department should also specify a back-up, or a person of secondary responsibility, should matters arise when the primary is unavailable.

Specific details regarding processing and reconciliation will depend on the method of payment card acceptance and type of merchant account. Detailed instructions will be provided when the merchant account is established and are also available by contacting the Student Financial Services office.

All service providers and third-party vendors providing payment card services must be PCI DSS compliant. Departments who contract with third-party service providers must maintain a list that documents all services provided and:

- Ensure contracts include language stating that the service provider or third-party vendor is PCI DSS compliant and will undergo a security review by the IT Security Office.
- Annually verify the PCI DSS compliance status of all service providers and third-party vendors. A lapse in PCI DSS compliance could result in the termination of the relationship.

B. Payment Card Data Security

All merchant departments authorized to accept payment card transactions must have their card handling procedures documented and made available for periodic review. Departments must have in place the following components in their procedures and ensure these components are maintained on an ongoing basis.

Processing and Collection

Access to cardholder data (CHD) is restricted to only those users who need the data to perform their jobs. Each merchant department must maintain a current list of employees with access to CHD and review the list periodically to ensure the list reflects the most current access needed and granted.

Software and equipment used to collect CHD is secured against unauthorized use or tampering in accordance with PCI DSS. This includes the following:

- Maintaining a software inventory and list of devices with their location;
- Periodically inspecting the devices to check for tampering or substitution; and
- Training for all personnel to be aware of suspicious behavior and reporting procedures in the event of suspected tampering or substitution.

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. In the event that it does occur, disposal as outlined below is critical. If payment card data is received in an email, then:

- 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.

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.

Storage and Destruction

Cardholder data, whether collected on paper or electronically, is protected against unauthorized access.

Physical security controls are in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents, or electronic files containing cardholder data.

No database, electronic file, or other electronic repository of information will store the full contents of any track from the magnetic stripe or the card validation code.

Portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: laptops, compact disks, floppy disks, USB flash drives, personal digital assistants, and portable external hard drives.

Cardholder data should not be retained any longer than that defined by a legitimate business need. CHD must be destroyed immediately following the required retention period using a PCI DSS-approved method of destruction. The UW System defined maximum period of time that credit card receipts and/or deposit transaction documents may be retained is three years from the date of transaction unless a longer retention time period is required by contract or law. The maximum period of time that training forms and corresponding PCI Compliance Logs may be retained is three years from the date of creation. A regular schedule (recommended quarterly) of deleting or destroying data should be established in the merchant department to ensure that no cardholder data is kept beyond the required retention period. For more details regarding record retention, please see the University of Wisconsin System Fiscal and Accounting General Records Schedule.

C. Risk Assessment

Implement a formal risk assessment process in which current threats and vulnerabilities to the institution's network and processing environment, including staff, are analyzed. Risk assessments must be conducted annually and must commence no later than two years after the initial adoption of UW System Administrative Policy 350, Payment Card Policy. Information Technology should conduct the risk assessment of the infrastructure and threats; departments that accept payment cards should also conduct an assessment of their physical environments and assess risks to the payment environment. Address all threats with mitigation tasks, timelines, and/or acceptance statements. Prepare and maintain documented output from the risk assessment exercise(s).

D. Incident Response

In the event of a breach or suspected breach of security, the department or unit must immediately execute the UWSP Incident Response Plan. This plan must meet or exceed the requirements of UW System Administrative Policy 1033, Information Security: Incident Response and should be reviewed at least annually.

If the suspected activity involves computers (hacking, unauthorized access, etc.), immediately notify the Information Security Office.

Email: Information.Security.Office@uwsp.edu
Phone: 715.346.4408
Office: Albertson Hall, Room 026
Mail: Information Security Office
026 ALB, UWSP
900 Reserve Street
Stevens Point, WI 54481

E. Sanctions for Non-Compliance

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability for the affected merchant(s). In the event of a breach or a PCI violation, the payment card brands may assess penalties to the institution's bank which will likely then be passed on to the institution. Any fines and assessments imposed will be the responsibility of the impacted merchant. A one-time penalty of up to $500,000 per card brand per breach can be assessed as well as on-going monthly penalties thereafter until compliance is achieved.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension, and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state, or federal laws. The university will carry out its responsibility to report such violations to the appropriate authorities.

6. REFERENCES and RELATED DOCUMENTS

UWSP Payment Card Merchant [PCI] Questionnaire
UWSP Payment Card [PCI] Standards
UW System Administrative Policy 350, Payment Card Compliance Policy
UW System Administrative Policy 1033, Information Security: Incident Response
PCI DSS Quick Reference Guide v3.2

7. POLICY HISTORY

Effective Date: 05/13/2019

Revision Date: 03/26/2024

Approved: 05/10/2019

Approved by: Vice Chancellor for Business Affairs

8. SCHEDULED REVIEW

May 2024