UNIVERSITY OF WISCONSIN – SUPERIOR

Policy: **Information Security Policy for Payment Card Industry Data Security Standards (PCI-DSS)**

Policy Subject: **Security Controls and Processes for PCI- DSS Requirements**

Cabinet Division: **Administration & Finance**

Date Revised: **February 18, 2019**

I. Background and Purpose

The payment card industry has developed technical and business standards that regulate the way credit card business is conducted. In order to accept credit card payments, UW-Superior must prove and maintain compliance with the Payment Card Industry Data Security Standards (PCI-DSS). The Business Office is responsible for providing guidance to departments accepting credit card payments. A security breach of credit card data attributable to UW-Superior jeopardizes the institution's ability to continue to accept credit card transactions. Additionally, a breach could result in significant fines to the institution.

This policy is intended to 1. Provide campus departments with compliant, consistent, and acceptable methods for securely processing credit card payments, and 2. Reduce institutional risk associated with the administration of credit card payments. This policy also requires the campus to build and maintain a secure network, to protect cardholder data, maintain a vulnerability management program, to implement strong access control measures and to regularly monitor and test systems in which credit card transactions are processed.

II. Constraints

1. PCI-DSS Security Standards Council
   https://www.pcisecuritystandards.org/security_standards/
2. Gramm-Leach-Bliley Act (GLBA) of 1999

III. Definitions

Access Control	Mechanisms that limit availability of information or information processing resources only to authorized persons or applications.
Account Data	Cardholder data plus sensitive authentication data. See *Cardholder Data* and *Sensitive Authentication Data*.
Account Number	See *Primary Account Number (PAN).*
Acquirer/Acquiring Bank	Entity that initiates and maintains relationships with merchants for the acceptance of payment card transactions.

Cardholder	Individual to whom a payment card is issued or any individual authorized to use the payment card.
Cardholder Data	Cardholder data consists of the full 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.
Card Verification Code or Value, or Card Security Code	Refers to either: (1) magnetic-stripe data, or (2) printed security features. (1) Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. (2) The second type of card verification value or code is the rightmost value printed in the signature panel area on the back of the card. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic.
Compromise	Also referred to as "data compromise" or "data breach". Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.
Encryption	Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Protects information against unauthorized disclosure.
Intrusion Detection System (IDS)	Software or hardware used to identify and alert on network or system intrusion attempts.
Information Security	Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction
Merchant	An entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services.
Primary Account Number (PAN)	Also referred to as "account number". A unique payment card number that identifies the issuer and the particular cardholder account.
Penetration Scan	Tests that attempt to exploit vulnerabilities to determine whether unauthorized access or other malicious activity is possible.
Remote Access	Access to computer networks from a remote location, typically originating from outside the network.

Self-Assessment Questionnaire (SAQ)	Validation tool for merchants and service providers to assist in self-evaluating compliance with the PCI DSS. Organizations may be required to share an SAQ with their acquiring bank.
Security Breach	An act from outside an organization that bypasses or contravenes security policies, practices, or procedures. A similar internal act is called security violation.
Service Provider	Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data.
Virtual Private Network (VPN)	Web-browser-based access to an acquirer, processor or third party service provider website to authorize payment card transactions, where the merchant manually enters payment card data via a securely connected web browser.
Vulnerability Scan	Tests performed by IT services on a quarterly basis to assess computers, computer systems, networks or applications for weaknesses

IV. Policy Statement

The University of Wisconsin - Superior requires all departments that accept credit card payment to do so in compliance with payment card industry standards and in accordance with the procedures outlined below.

V. Policy Procedures

5.1 Business Services:

- 5.1.1 Update the Information Security Policy on an annual basis to reflect changes to business objectives and the risk environment.
- 5.1.2 Publish and maintain the Information Security Policy on the IT website.
- 5.1.3 Apply for and secure all campus merchant ID numbers.
- 5.1.4 Establish and maintain a process for campus departments to accept credit cards.
- 5.1.5 Reconcile monthly statements from credit card companies to the Shared Financial System.
- 5.1.6 Ensure credit card processing fees are charged in accordance with State and University of Wisconsin System contracts.
- 5.1.7 Ensure credit card processing fees are charged back to the appropriate department.
- 5.1.8 Provide training to the campus on merchant card transactions.
- 5.1.9 Maintain a list of all service providers.
- 5.1.10 Request written acknowledgement that service providers are responsible for the security of cardholder data that the service providers possesses.

5.1.11 Verify annually that the service providers are compliant with applicable payment card requirements.

5.1.12 Ensure that each campus department that accepts credit cards annually completes the Self-Assessment Questionnaire required by applicable standards.

5.1.13 Follow the incident response plan for all security related incidents, as outlined in Section 5.5.

5.2 Technology Services:

5.2.1 Resolve exceptions pertaining to technology or electronic storage noted on the annual Self-Assessment Questionnaire and quarterly vulnerability scans.

5.2.2 Perform quarterly vulnerability scans of networks that are deemed in scope. The results of these scans will be reviewed by Technology Services staff and action will be taken in order to remediate threats to cardholder data.

5.2.3 Ensure annual penetration test is performed on in scope systems. Technology Services staff will review the results of these test and action will be taken to remediate threats to cardholder data.

- Ensure technologies used are in accordance with the University of Wisconsin Appropriate Use Policy and will require the following: Remote access to any systems used to store, process, or transmit cardholder data must be approved by Technology Services, the Business Office and the department that accepts the cardholder information for payment.
- Remote access must be initiated from a device that uses universally accepted encryption technologies to encrypt all digital storage devices local to that system.
- Universally accepted Virtual Private Network technologies must be used to connect to in scope systems using an encrypted tunnel.
- Mobile devices must be physically labeled in order to determine owner and contact information.
- The use of remote access shall be limited to locations determined by the campus department head seeking remote access to credit card processing. Locations' must be approved by Technology Services in order to make sure technical requirements are in place for secure remote access.
- Remote Access Technologies shall be configured with a timeout value where feasible and applicable.
- Vendors seeking remote access must contact Technologies Services to have remote access technologies activated and must immediately notify Technologies Services when they are done to have these technologies terminated.
- Copying, moving and storing cardholder data to local hard drives and remote electronic media is prohibited.

5.2.4 PCI-DSS Information security is formally assigned to the Chief Information Officer or their designee with the following responsibilities:

- Monitor and analyze security alerts from vulnerability scans, penetration tests, or other network monitoring systems and distribute to appropriate personnel for activating the incident response plan.

5.2.5 Follow the incident response plan for all security related incidents, as outlined in Section 5.5.

5.3 Credit Card Merchant (Department):

5.3.1 Establish credit card merchant sites through the Business Office. Departments are prohibited from obtaining merchant site status directly from the credit card companies.
5.3.2 Maintain a current contact person for Business Office and or Technology Services contact purposes.
5.3.3 Accept credit card information through a UWS authorized web application or by telephone, mail, or in person only.
5.3.4 Ensure that departmental procedures prohibit transmitting, processing, or storing credit card information on UWS computers, network systems, servers, fax machines, the Internet, e-mail or any removable electronic storage (USB memory stick, hard drive, zip disk, etc.); not even if encrypted.
5.3.5 Ensure that departmental procedures prohibit storing the Validation Code or Value, or Card Security Code electronically or on paper.
5.3.6 Ensure that departmental procedures establish that Paper credit card transaction records be stored in a locked room or file cabinet. Access to the storage area(s) must be limited to authorize personnel only.
5.3.7 Ensure that departmental procedures establish that if it is absolutely necessary to record the entire credit card number to process the transaction, all but the last four digits of the credit card number must be concealed.
5.3.8 Issue credit card receipts to customers that display only the last four digits of the credit card number.
5.3.9 Retain the original receipts, displaying only the last four digits of the credit card number, for all transactions in a secure location for a minimum of 12 months as required by the *University of Wisconsin System Fiscal and Accounting General Records Schedule.*
5.3.10 Ensure that departmental procedures establish an adequate separation of duty between any person authorized to issue a refund and the individual reconciling the merchant account.
5.3.11 Follow the incident response plan for all security related incidents, as outlined in Section 5.5.
5.3.12 Require all employees involved with credit card processing complete PCI training annually. Verify new employees complete PCI training prior to working with credit card information.

5.4 Incident Response Plan:

All employees must notify the Controller in the event of a compromise to customer credit card numbers or to a card processing device. The Controller will immediately notify the Vice Chancellor for

Administration and Finance and the Chief Information Officer to review the security incident and determine the appropriate response plan.

VI. Compliance

Those departments having a security breach and/or found to be in non-compliance with the responsibilities outlined above jeopardize their ability to accept credit card payments and/or may be subject to financial penalties.

Individuals found to be negligent within the scope of their employment responsibilities related to PCI-DSS compliance may be subject to disciplinary action.