UNIVERSITY OF WISCONSIN OSHKOSH

TO: Andrew Leavitt, Chancellor

FROM: John Koker, Provost and Vice Chancellor

DATE: December 9, 2019

RE: Payment Card Compliance Policy (PCC-DSS) – Data Security Standards

On the recommendations of the Faculty Senate, Senate of Academic Staff, University Staff Senate, and Oshkosh Student Association Senate, I am recommending your approval of the Payment Card Compliance Policy.

I have attached the policy for your review. Please contact me if you have questions regarding the proposal.

JK/eh

Attachment

✓ Approve

_____ Do not approve

Signature

12/17/19
Date

OFFICE OF THE PROVOST AND VICE CHANCELLOR
800 Algoma Blvd. | Oshkosh, WI 54901
PHONE (920) 424-0300 | FAX (920) 424-0247 | WEB uwosh.edu/provost

UNIVERSITY OF WISCONSIN OSHKOSH

Payment Card Compliance - Data Security Standards Policy (PCC-DSS)

1. PURPOSE

The purpose of this policy is to ensure that credit card payments and card data storage are executed according to UW System Policy 350.

2. RESPONSIBLE OFFICER

Chief Information Officer

3. SCOPE

This policy applies to all divisions and departments throughout the university that wish to take credit cards as a form of payment, including the Oshkosh, Fond du Lac, and Fox Valley campuses.

4. BACKGROUND

UW System institutions can reduce the risk of compromised cardholder data by meeting all applicable Payment Card Industry (PCI) compliance requirements by securing the network, hardware, applications, and processes. Payment Card Industry compliance requirements include the Data Security Standards (PCI DSS), Payment Application Standards (PCI PA-DSS) and Point-to-Point Encryption Standards (P2PE). PCI compliance means that all entities accepting credit or debit cards operate in a way that protects cardholder data such as card number, expiration date, name of cardholder, and security code. Protection of cardholder data reduces the risk of this data from being released to anyone other than the acquirer of the transactions going into the payment card processing network.

The Payment Card Industry Data Security Standard (PCI DSS) is the global data security standard adopted by the payment card brands for all entities that process, store, or transmit cardholder data. These security requirements apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as form of payment. The PCI DSS is comprised of twelve requirements grouped into six goals:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

Information protected from unauthorized disclosure by the PCI DSS is classified by the UW System as High Risk data, per UW System Administrative Procedure 1031.A, Information Security: Data Classification.

5. DEFINITIONS

Card Brands: Credit card networks including Visa, Mastercard, Discover, JCB International and American Express

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

Cardholder Data: 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.

Division/Department: Includes all UW Oshkosh campuses, departments, and units.

Payment Application Data Security Standard (PA-DSS): For software vendors and others who develop payment applications that store, process or transmit cardholder data and/or sensitive authentication data, for example as part of authorization or settlement when these applications are sold, distributed or licensed to third parties.

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 comprises 12 requirements that are organized in 6 logically related groups or "control objectives.".

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.

6. POLICY STATEMENT

A. Divisions and departments may accept credit cards as a form of payment. Each department must do so in compliance with UW System Policy 350 and UW Oshkosh procedures.

1. Workstation computers may not be used to enter any credit card data.
2. End-user messaging (for example, email, instant messaging, SMS, chat, etc...) is never to be used to process a payment.

B. If using a third party vendor to process credit card data, divisions/departments shall require an annual attestation of compliance from the vendor.

C. You shall not store any cardholder data past the minimum time required for legal, regulatory, and/or business requirements.

D. UW Oshkosh divisions and departments shall report and/or respond to potential incidents of compromised cardholder data in accordance with UW System Policy 350 and UW Oshkosh procedures.

E. UW Oshkosh departments shall pay any fees, fines, penalties, or other costs resulting from unauthorized acceptance of payment cards or non-compliance with PCI standards.

F. Exceptions to this policy require a business plan (including why the available processing systems will not work) that shall be submitted and approved by the UW Oshkosh controller in advance of any equipment or system purchase.

G. Each department shall create and maintain internal procedures for accepting credit cards as a form of payment.

7. REFERENCES

UW System Policy 350

8. PROCEDURES

UW Oshkosh Procedure

9. REVISION HISTORY

10/22/2019	Faculty Senate
10/24/2019	Senate of Academic Staff
10/30/2019	Oshkosh Student Association Senate
11/13/2019	University Staff Senate
	Chancellor

10. CHANCELLOR'S APPROVAL

Chancellor's Signature

12/17/2019
Date