UNIVERSITY OF WISCONSIN OSHKOSH

University of Wisconsin Oshkosh
Payment Card Procedure

Payment Card Industry
Data Security Standard (PCI DSS)
Version 1.0

Contents

Revisions/Approvals

Ver. #	Changes By	Ver. date	Reason
1.0	R. Sitzberger D. Lewis	8/01/2018	Adopted and modified template from CampusGuard v 3.2.2

Purpose

This document and additional supporting documents represents University of Wisconsin Oshkosh's (UW Oshkosh) Procedure to prevent loss or disclosure of sensitive customer information including payment card data. Failure to protect customer information may result in financial loss for customers, suspension of credit card processing privileges, and fines imposed on and damage to the reputation of the unit and the institution.

PCI DSS

The PCI DSS is a mandated set of requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express and JCB. These security requirements apply to all transactions surrounding the payment card industry and the merchants/ organizations that accept these cards as forms of payment. Further details about PCI can be found at the PCI Security Standards Council Web site (https://www.pcisecuritystandards.org)

In order to accept credit card payments, UW Oshkosh must prove and maintain compliance with the Payment Card Industry Data Security Standards. The UW Oshkosh Payment Card Procedure and additional supporting documents provide the requirements for processing, transmission, storage, and disposal of cardholder data transactions. This is done in order to reduce the institutional risk associated with the administration of credit card payments by individual departments and to ensure proper internal control and compliance with the Payment Card Industry Data Security Standard (PCI DSS).

Visa Cardholder Information Security Plan (CISP)

Visa Inc. instituted the Cardholder Information Security Program (CISP) in June 2001. CISP is intended to protect Visa cardholder data - wherever it resides - ensuring that members, merchants, and service providers maintain the highest information security standard. In 2004, the CISP requirements were incorporated into the Payment Card Industry Data Security Standard (PCI DSS).

MasterCard Site Data Protection Program (SDP)

The SDP Program, with the PCI DSS as its foundation, details the data security and compliance validation requirements in place to protect stored and transmitted MasterCard payment account data.

Scope/Applicability

The UW Oshkosh Payment Cards Procedure applies to all faculty, staff, students, organizations, third-party vendors using UW Oshkosh's network, individuals, systems, and networks involved with payment card handling. This includes transmission, storage, and/or processing of payment card data, in any form (electronic or paper), on behalf of UW Oshkosh.

Authority

UW Oshkosh policies fall within a greater hierarchy of laws, statutes, and regulations. The Board has been authorized by the State to govern UW Oshkosh. The Board has delegated the authority

to manage the institution to the Chancellor. As a part of that management, the Chancellor will direct the development and implementation of UW Oshkosh's policies and procedures.

Procedure

It is the Procedure of UW Oshkosh to allow acceptance of payment cards as a form of payment for goods and services upon written approval from the Controller. UW Oshkosh requires all departments that accept payment cards to do so only in compliance with the PCI DSS and in accordance with this Procedure document, the UW Oshkosh payment card procedures, and other supporting documents.

All entities of UW Oshkosh that receive or expect to receive payments electronically must comply with the guidelines and procedures issued by the Controller. All entities who wish to take payments via payment cards must be reviewed by the PCI Team. Once approved, the request should be forwarded to the Controller for final approval and implementation. All merchants should submit their requests for approval to the appropriate University Business Officer and then, once approved, forward the signed form to the PCI Team.

Entities accepting payment cards will sign an agreement with the Controller that details their responsibilities, as well as the security requirements (Payment Card Industry Data Security Standard and institutional Data Security Policies) that must be followed. This agreement may be updated from time to time as requirements change. Failure to follow the requirements of the agreement may result in the revocation of your ability to accept card payments.

Entities must accept only payment cards authorized by Controller and agree to operate in accordance with the contract(s) the UW Oshkosh holds with its Service Provider(s) and the Card Brands. This is to ensure that all transactions are in compliance with the Payment Card Industry Data Security Standards (PCI DSS), Federal Regulations, NACHA rules, service provider contracts, and UW Oshkosh policies regarding security and privacy that pertain to electronic transactions. Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

- Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements
- Data that is not absolutely necessary in order to conduct business will not be retained in any format. All data will be treated as confidential.
- Specific retention requirements for cardholder data
- Processes for secure deletion of data when no longer needed
- A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.
- Physical access to data records is restricted to staff with a need to know.
- Never type credit card data into a workstation computer.

The controller must approve the use of Wi-Fi for credit card payments. All use of technology must follow the UW System Acceptable Use Policy (25-3 formerly 97-2).

Cardholder data (CHD) received via fax or end-user messaging technologies (for example, VoIP phone system, e-instant messaging, SMS, chat, etc.) is never to be used to process a payment. Follow approved departmental procedures for the appropriate method of responding to and securely destroying the cardholder data.

All proposed Processing Equipment is to be reviewed by IT Security by creating a HelpDesk ticket. Exceptions to this Procedure will be limited and will require a business plan (including reason why the available central processing systems will not work for your area) to be submitted and approved by IT Security in advance of any equipment or system purchase.

All payments received must be directed into a UW Oshkosh Approved Bank Account. The type and nature of the electronic transaction (e.g., ACH, Credit Card, Point of Purchase, wire, etc.) will dictate where the transaction will be deposited.

Accounting entries to record the receipt of the payment will be linked directly into the institution's Shared Financial System (SFS), whenever possible, to ensure timely recording of transactions and expedite the prompt reconcilement of general ledger and bank accounts.

Procedures and Other Supporting Documents

- UW Oshkosh - PCI Administration and Department Payment Card Procedures
- UW Oshkosh - Appendix 1 - PCI Payment Card Security Incident Response Plan
- UW Oshkosh - Appendix 2 - PCI Application for New Payment Card Merchants
- UW Oshkosh - Appendix 3 - PCI Annual Merchant Survey
- UW Oshkosh - Appendix 4 - PCI Payment Card Best Practices

Interpretations

The authority to interpret this Procedure rests with the Chancellor and the Financial Services Leadership Team.

Glossary

Term	Definition
Payment Card Industry Data Security Standards (PCI DSS)	The security requirements defined by the Payment Card Industry Security Standards Council and the 5 major Credit Card Brands: • Visa, MasterCard, American Express, Discover, JCB
Cardholder	Someone who owns and benefits from the use of a membership card, particularly a credit card.
Card Holder Data (CHD)	Those elements of credit card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date and the Service Code.
Primary Account Number (PAN)	Number code of 14 or 16 digits embossed on a bank or credit card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.
Cardholder Name	The name of the Cardholder to whom the card has been issued.
Expiration Date	The date on which a card expires and is no longer valid. The expiration date is embossed, encoded or printed on the card.
Service Code	The service code that permits where the card is used and for what.
Sensitive Authentication Data	Additional elements of credit card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data and PIN/PIN block.
Magnetic Stripe (i.e., track) data	Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.
CAV2, CVC2, CID, or CVV2 data	The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card- not-present transactions.
PIN/PIN block	Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.
Disposal	CHD must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, USB storage devices,(Before disposal or repurposing, computer drives should be sanitized in accordance with the (Institution's) Electronic Data Disposal

	Procedure). The approved disposal methods are: • Cross-cut shredding, Incineration, Approved shredding or disposal service
Merchant Department	Any department or unit (can be a group of departments or a subset of a department) which has been approved by the (institution) to accept credit cards and has been assigned a Merchant identification number.
Merchant Department Responsible Person (MDRP)	An individual within the department who has primary authority and responsibility within that department for credit card transactions.
Database	A structured electronic format for organizing and maintaining information that is accessible in various ways. Simple examples of databases are tables or spreadsheets