

Administration and Department Procedures Payment Card Procedures:

Appendix 2 – Application for

New Payment Card Merchants

Payment Card Industry

Data Security Standard (PCI DSS)

Version 1.0

**Contents**

[Revisions/Approvals 2](#_Toc400615895)

[Purpose 3](#_Toc400615896)

[Best Practices for Offices Accepting Payments Cards 3](#_Toc400615897)

# Revisions/Approvals

| Ver. # | Changes By | Ver. date | Reason |
| --- | --- | --- | --- |
| 1.0 | D. Lewis and R. Grose | 08/01/2018 | Adopted and modified template from CampusGuard |
| Ver. # | Changes By | Ver. date | Reason |
| 2.0 | S. Anderson | 10/10/2022 | Updated form due to staffing changes |

# Purpose

To be completed by departments that would like to accept payment cards (Visa, Master Card, American Express, Discover cards and debit cards) as a form of payment for goods and/or services, receipt of donations, non-tuition courses, conferences, seminars, tickets and other approved University of Wisconsin Oshkosh (UW Oshkosh) related products.

Please read Payment Card Handling Procedure and Payment Card Procedures prior to completing this application to make sure that your department will be able to comply with all the requirements listed in this Procedure.

Application must be submitted to the PCI Team. Once the application has been approved, please contact the PCI team and your vendor to determine the timeline for installation and set-up. The information provided on this application will be used to create an “Merchant Profile” that will be submitted to our bank, American Express, and Discover Business Services to request merchant numbers. For assistance or questions regarding this form, please contact the PCI Compliance Coordinator at pci@uwosh.edu.

# Best Practices for Offices Accepting Payments Cards

We understand that complying with the PCI DSS may be difficult and confusing for some departments. If you have identified a business need that requires you to accept credit and/or debit card payments, we recommend that you review this set of high-level best practices before you complete this application.

1. If you don’t need it, don’t store it!

* Many offices retain cardholder data (CHD) “just because.” If you keep the transaction number and date, you can always ask the acquiring bank for the CHD if you need it.
* This includes paper and forms. Once the transaction has been processed, destroy the CHD on the form. This may require a redesign of the form to move the CHD to the bottom where it can be properly removed and cross-cut shredded.

1. Proper destruction

* All forms or paper with CHD should be shredded in a “cross-cut” type shredder.
* Third-party shredding services may be used, providing the bins that they provide are secure and cannot be removed from the area. Tracking chain of custody with the CHD and receiving a certificate of secure destruction is also recommended.

1. Online Payment Card Systems

* Many departments employ the use of third-party payment systems to outsource card processing to an online process. Many times it is considered good customer service to take phone calls, emails or some other form of communication to process a credit card transaction.
  1. Never accept cardholder data that is sent via email; refer to the *Payment Procedure* for the approved method of response for this type of situation.
  2. It is not recommended to act as the customer and input their data for them. It would be better to verbally walk them through the flow as they enter in their data on the website themselves.
  3. If you choose to accept payment data over the telephone, transactions should be conducted on a separate (isolated) computer or via a dial-up payment terminal. Do not type credit card data in to your workstation computer.

1. Maintain clean desk policy

* CHD should not be left out on desks or in open areas when not needed. Even if leaving the desk for a short period, staff should keep material in a folder and lock the folder in the desk when they leave temporarily. At the end of the day, all CHD should be stored in a secure file cabinet or safe.

1. Electronic storage of CHD

* Do not copy or type CHD into spreadsheets or documents on general use workstations even for temporary use. Even if you don’t save the document, an image or file of the data is stored on the hard drive.

1. Never email Credit Card information

* Staff should never use email as a manner of transmitting Cardholder data
* Should a customer email their credit card information:
  1. Reply to the sender, deleting the credit card information from the reply and inform them that “for their protection and UW Oshkosh’s, policies dictate that credit card information shall not be accepted via email. Please use one of our accepted methods of processing your information: (in-person, online, fax, form, etc.).”

1. Do not allow unauthorized persons unaccompanied access to areas where credit card data is stored or processed

* This includes other UW Oshkosh staff. As an example, maintenance and janitorial staff should not be permitted in secure areas unaccompanied. This sometimes requires a change in service times.

1. Document Desk Procedures

* To insure continuity when office personnel are out, have all individuals document their daily procedures for their role in the handling of confidential data. Include such items as receipt and processing procedures, disposition and destruction of CHD, and storage and transfer of forms within the office.

**1. DEPARTMENT INFORMATION:**

|  |  |
| --- | --- |
| DEPARTMENT NAME: |  |
| MERCHANT (LOCATION) NAME: |  |
| Note: The merchant (location) name will appear on your customer’s monthly statements and on the bank statements sent to the Controller’s Office | |
| INTERNET ADDRESS: |  |
| Note: The merchant (location) name will appear on your customer’s monthly statements and on the bank statements sent to the Controller’s Office | |
| MERCHANT (LOCATION) ADDRESS: |  |
| Note: Merchant address must include Building & Room number. Statements will be mailed to this address.  Device Location: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Note: Please provide a map of your location, including where the device is location and any security measures (locked doors, cameras) | |

**2. PRIMARY CONTACT INFORMATION:**

|  |  |  |  |
| --- | --- | --- | --- |
| CONTACT NAME: |  | MAIN TELEPHONE #: |  |
| CONTACT TITLE: |  | ALT. TELEPHONE #: |  |
| EMAIL ADDRESS: |  | FAX NUMBER: |  |
| Note: Primary contact will be responsible for the overall process of accepting payment cards at this location and must be a full time employee. (Work Study employees are not allowed). | | | |

**3. MERCHANT INFORMATION:**

GIVE A BRIEF DESCRIPTION OF YOUR PAYMENT CARD BUSINESS:

|  |
| --- |
| (What is the main purpose of this merchant account? For example, registration fees, tuition for non-credit courses, tickets for events) |

|  |  |  |  |
| --- | --- | --- | --- |
| DATE SUBMITTED: |  | DESIRED “LIVE” DATE: |  |

TRANSACTION TYPE TO BE ACCEPTED (Mark with an X):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ( ) | VISA | ( ) | AMERICAN EXPRESS | ( ) | DEBIT |
| ( ) | MASTERCARD | ( ) | DISCOVER |  |  |

ESTIMATED ANNUAL CREDIT CARD VOLUME:

|  |  |
| --- | --- |
| Total Annual Dollar Amount: | $ |
| Average Amount per Transaction: | $ |
| Annual Number of transactions: |  |

DEPARTMENT ACCEPTS PAYMENT CARDS (Check all that apply):

|  |  |  |
| --- | --- | --- |
| ( ) | IN PERSON |  |
| ( ) | BY PHONE |  |
| ( ) | BY MAIL (submit form design to PCI Team) |  |
| ( ) | ONLINE VIA UNIVERISTY’S APPROVED INTERNET PROCESSOR |  |
| ( ) | OTHER, NAME: |  |

PROCESSING SYSTEMS (Check the types of system currently being used or will be used):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ( ) | POS Terminals | ( ) | Internet (Online) | | ( ) | Other |
| If Other, describe in detail: | | | |  | | |
| Current Third Party Vendor, if applicable: | | | |  | | |

IF PROCESSING USING A POINT OF SALE (POS) ELECTRONIC TERMINAL, PLEASE PROVIDE:

|  |  |  |
| --- | --- | --- |
| MODEL | FIRMWARE/SOFTWARE VER. | SERIAL NUMBER |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**4. PROCESSING INFORMATION**

These items will be required before implementation…

* Yourself, or your employees, have received training on how to handle cardholder data in a compliant manner.
* Your department has written instructions on how handle cardholder data in a compliant manner for all employees to review.
* All documents that contain sensitive payment card information are destroyed using a crosscut shredder immediately after the transaction is processed.
* Payment card numbers are truncated on the receipt.
* The {technology used} is kept in a secured and restricted area, away from public access.
* The {technology used} is inspected on a regular, periodic basis for tampering and/or substitution.
* A “unique code” is assigned to each person with access to payment card processing and is this code not shared with another person.
* Is the {technology used} connected to an analog line?

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| * YES | * ( ) | * NO | * ( ) | * If NO, please explain |  |

* UW Oshkosh’s *“Payment Card Processing Procedures”* is being followed by employees involved in payment card handling?
* Employees are educated on practices for accepting and processing payment cards and closing out batches?
* All transactions and settle batches are audited by yourself or an employee daily.
* There is a back-up to process transactions daily in your absence.
* You, or your employees, are taking every measure possible to prevent duplicate entries.
* All employees are educated on common types of payment card fraud and how to counteract them.
* All employees are educated on common types of merchant mistakes and how to avoid them.
* Background checks are required for employees involved in payment card processing, or employees that have access to such data.
* Employees are required to acknowledge, at least annually, that they have read, understood, and agreed to abide by the UW Oshkosh’s policies and procedures on payment card processing by completing the Employee Statement of Understanding.
* You have the ability to process payment cards if normal modes of processing are down.
* The number of employees who process payment cards are limited to appropriate employees based on their job duties.
* The PCI Team is aware of any changes in your payment card program.
* Access to stored cardholder data is restricted to users on a need to know basis
* When an employee leaves the Department, his/her access to payment card processing is immediately revoked?
* The storage of cardholder data and other sensitive information is prohibited.
* Storage of the full contents of any track from the magnetic stripe (on the back of the card) in a database, log files, or point of sale products is prohibited.
* The storage of the card validation code (3 digit value printed on the signature panel of a card) in a database, log files, or point of sale products is prohibited.
* The transmission of CHD via insecure mediums, e.g. fax, email, or chat is prohibited.
* The “Privacy Policy” is updated to reflect changes and keep it current.
* The “Refund Policy” is updated to reflect changes and keep it current.

**5. TECHNICAL INFORMATION:**

* All staff members who process payment cards aware of the “Emergency Contact Plan” in case the system has been breached or compromised.
* All staff members are trained and tested on the Emergency Contact Plan, at least annually? (same as #1)
* Default security settings, accounts, and passwords are changed on production systems before taking the system into production?
* Transmission of cardholder data and other sensitive information across public networks is encrypted using PCI-approved methods?
* On all systems that are commonly affected by malware, anti-malware software is installed on all servers and workstations involved in payment processing, and is it regularly updated?

**6. THIRD PARTY PROCESSORS OR GATEWAYS INFORMATION:**

If you are not using a Third Party Processor or Gateway, please go to PART 7.

* A list of service providers (vendors) is maintained, including a description of the service(s) provided.
* Your department has written agreement with an acknowledgment that indicates that the service provider (vendor) is responsible for the security of cardholder data.
* The written agreement has been reviewed and approved by our Purchasing Department.
* The written agreement has been reviewed and approved by Information Technology.
* A program is in place to validate the service provider's (vendor's) PCI DSS compliance status before engaging in a new relationship.
* A program is in place to validate the service provider's (vendor's) PCI DSS compliance on at least an annual basis.
* Information is maintained about which PCI DSS requirements are managed by the service provider (vendor), and which are managed by the merchant.

**7. EMPLOYEE ATTESTATION STATEMENT**

I attest that the information in this merchant questionnaire has been completed to the best of my knowledge and belief. I understand the intent of this merchant questionnaire and that the information I have provided is an important element of UW Oshkosh’s Payment Card Handling Procedure.

I attest that I have read UW Oshkosh’s policies, procedures and guidelines listed under the “Related Information” section of the UW Oshkosh Payment Card Handling Procedure.

I understand that payment card processing information is to be kept in the strictest of confidence to protect cardholder information and that failure to comply with UW Oshkosh’s Payment Card Handling Procedure may result in disciplinary action, up to and including termination.

I further understand that accepting card holder data via insecure methods (fax, email, chat…etc) is prohibited by UW Oshkosh procedure.

I confirm that I have read, understood, and agree to abide by the policies and procedures associated with accepting and handling payment cards on behalf of UW Oshkosh.

|  |  |  |  |
| --- | --- | --- | --- |
| *Authorized Signature:* |  | *Date:* |  |
|  |  |  |  |
| *Printed Name:* |  | *Telephone #:* |  |
|  |  |  |  |
| *Title:* |  | UW Oshkosh *ID:* |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Authorized UW Oshkosh Signature Date*

*UW Oshkosh Controller*