UNIVERSITY OF WISCONSIN OSHKOSH

Appendix 3 – Annual Merchant Survey

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

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?

□ (□ If NO,
□ ( ) please
□ YES) □ NO 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 annual 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:* ____________