UNIVERSITY of WISCONSIN
LA CROSSE

Business Services

Accepting and Processing Payment Cards for University Business

Revision: 02		**Effective: 4/01/17**
		Last Updated: 09/30/2019

PURPOSE

The University of Wisconsin-La Crosse requires all departments involved with payment card handling to be in compliance with Payment Card Industry Data Security Standards (PCI DSS, Version 3.2.1), and in accordance with the procedure outlined in this document. The standards are designed to protect cardholder information of any individual or entity who utilizes a payment card to transact business with the University. This policy is intended to be used in conjunction with the complete PCI DSS requirements as established and revised by the PCI Security Standards Council (PCI SSC).

SCOPE

This policy applies to all individuals with access to payment card information, including:

- Any employee who accesses, handles, or maintains payment card information. UWL employees include full-time, part-time, and hourly staff members as well as student workers who access, handle or, maintain records.
- Employees who contract with service providers (third party vendors) who process card payments' on behalf of UWL.
- Employees responsible for developing and maintaining a University website to conduct business transactions using payment cards.

POLICY

PCI DSS are technical and operational requirements set by the PCI SSC to protect cardholder data. These standards are a set of mandated requirements agreed upon by the five major payment card companies: VISA, MasterCard, Discover, American Express, and JCB. The PCI DSS applies to all entities who store, process, and/or transmit cardholder data. The security controls and processes required by PCI DSS are vital to protecting cardholder account data (both electronic and paper handling), including the primary account number (PAN) printed on the front of a payment card. Merchants and any other service providers involved with payment card processing must never store sensitive authentication data after authorization. This includes sensitive data printed on a card or stored on a cards magnetic stripe or chip.

All departments considering accepting payment cards must receive prior approval from the PCI Compliance Team by completing the Request to Process Payment Cards Form.

All users authorized to process payment cards must complete annual PCI DSS training.

All departments must submit their Payment Card Processing Procedures to the PCI Compliance Team for review and approval annually. In addition, an annual Self-Assessment Questionnaire(s) (SAQ) must be completed. The SAQ is a validation tool for eligible organizations who self-assess their PCI DSS compliance. Each section of the questionnaire focuses on a specific area of security based on the PCI DSS requirements. The PCI Compliance Team will work with each Department directly to complete the SAQ.

Department Procedures
PCI requires certain procedures be maintained and documented.

- The PCI Compliance Team must approve the storage, transmission, or processing of payment card data in an electronic format. All network locations and devices must be specifically approved for processing payment cards. (PCI DSS 12.3)
- The PCI Compliance Team must approve any third party vendors which process card payments on behalf of the University. (PCI DSS 12.8)
- The PCI Compliance Team must establish, publish, and maintain a security policy that is disseminated to all relevant personnel (PCI DSS 12.1)
- The University must approve and provide any device that is allowed to process payment cards. The costs of acquiring or implementing those devices will be charged to the department. (PCI DSS 12.3)
- Departments are responsible for the physical security and inventory of all devices which process payment cards. (PCI DSS 9.9.a, PCI DSS 9.9.1)
- Departments are responsible for periodic inspections of devices to look for tampering or substitution (PCI DSS 9.9.b, PCI DSS 9.9.2)
- Departments are responsible for requiring personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices (PCI DSS 9.9.c, PCI DSS 9.9.3)
- Payment card information via any end user technology such as email, instant messaging, text message, or via the campus voicemail system cannot be accepted as a form of payment. Emails containing payment card information should be immediately deleted and purged from the system. (PCI DSS 4.2)
- All merchants are required to include a refund policy. Departments are responsible for establishing and communicating this policy to customers. Refunds must be processed with the same payment card account which was used in the original transaction.

Consequences for Non-Compliance
Failure to comply with this policy can result in your department losing the privilege of accepting payment cards as form of payment.

Settlement
Terminals must be settled no less than daily. A transaction will not be processed and charged to the cardholder until the batch is settled. The department must maintain all signed receipts and payment card terminal batch total settlement reports.

Payment Card Fees
The University is charged a variable rate and other fixed fees for all payment card transactions. The variable rate and fixed fees may be different based on payment card type and/or transaction type. .

A ‘card present’ transaction is face-to-face interaction when the card is inserted in the terminal to capture the payment card transmittal data.

A ‘card not present’ transaction occurs when the payment card data is obtained by mail, telephone, or fax and is manually keyed by an authorized operator of the payment card terminal. These transactions may be subject to additional fees.

Fees (e.g., credit and debit card fees) for each department’s merchant account will be posted to the department’s designated WISDM account on a monthly basis.

Cardholder Disputes and Chargebacks
The bank will notify the University of disputed charges. Business Services is the primary contact. All disputes are reviewed by Business Services, and the department is contacted to receive written authorization/documentation of the transaction. Failure to respond to these requests will result in a chargeback to the department’s account.

Training, Access and Guidance
Access to cardholder data is restricted to only those individuals who are authorized. All personnel

who utilize or support the processing of payment cards must have completed UWL security training and PCI DSS training prior to receiving access. It is the responsibility of the manager to notify Business Services any time there is a new employee or a termination. PCI DSS training is required on an annual basis. Departments authorized to accept payment cards must have written operational procedures that include restricting access to cardholder data.

Reporting a Breach
In the event of a breach or suspected breach of security, immediately notify Business Services at 608-785-8730. Follow the instructions below:

- Document every action you take from the point of suspected breach forward, preserving any logs or electronic evidence available. Include in the documentation the date and time, action taken, location, person performing action, person performing documentation, and all personnel involved.
- Notify Business Services and the Dean/Director/Department Head of the unit experiencing the breach. No one should communicate with anyone outside of their supervisors, IT, or Business Services.
- Prevent any further access to or alteration of the compromised system.
- If a suspected or confirmed intrusion/breach of a system has occurred, the Controller, along with the PCI Compliance Team, will alert the bank, payment card processor, and other respective authorities as required.
- Securing payment card data is everyone's responsibility. Should there be a data security breach, the department responsible for the merchant account will be responsible for the costs of the breach.

PROCEDURES

Departments may accept payment cards with the prior approval of the manager and the PCI Compliance Team. This includes any third party vendors which process payment cards on behalf of the University and submit payment via ACH or paper check. All revenue must be deposited into a UWL bank account which posts to UWL General Ledger.

Authorization to Establish Payment Card Business: Complete a Request to Process Payment Cards Form and submit to Business Services. The PCI Compliance Team will review and approve the request and communicate with the department approval and the next steps required.

Payment Card Terminals: The use, purchase, or rental of payment card terminals must be coordinated through Business Services. All devices must meet PCI DSS standards. Business Services personnel will provide on-site training at initial setup to the authorized department. The department is responsible to ensure that only authorized staff have access to the terminal and are properly trained. Devices that capture payment card data must be protected. This protection must include preventing the device from being tampered with or substituted. Terminals will be inventoried with Business Services and must be maintained in a secure location by the department.

Protecting Your Swipe Devices from Illegal Tampering
The threat of Point of Sale (POS) terminal tampering is serious and worldwide. Every day criminals install skimmers, keyKatchers, and other devices which grab cardholder data. The cardholder data is used to create cloned cards or to break into bank accounts to steal money.

To help UW-La Cross Merchants anticipate threats and to keep your POS devices safe from criminals, Business Services has provided the following information and tips.

Watch your POS Equipment

- Examine your POS device that accepts credit and debit cards, look for anything abnormal. Examples-Skimmers, Keykatchers, missing or broken seals, damage to the device, damage to external cable or broken port or other materials that could mask damage or tampering.
- Business Services requires that you inspect your POS device and PIN-entry devices (PED) on a regular basis. Check for the following:
  - Is the POS device and PED in its designated location?
  - Is the POS device's manufacturer name, model and serial number correct? Each merchant must maintain a record of the model and serial numbers for reference.

Business Services maintains a record of all POS devices we well.
    - Is the color and condition of the POS device as expected with no additional marks, or scratches, especially around the seams of the terminal window display?
    - Are the manufacturer's security seals and labels present with no signs of peeling or tampering?
    - Is the number of connections to the POS device as expected, with the same type of color of cables, and with no loose wires or broken connector?

Physical Security Safeguard Your POS Equipment and Surrounding Areas

- All POS devices will be locked up in a secure area at the end of each business day to prevent any unauthorized removal attempts from your merchant location.
- Check your POS environment for hidden cameras or recording devices. Merchants should:
    - Verify there are no additional or unauthorized displays where a camera could be hidden. Examples-adjacent walls, plaques or signs, brochure containers or personal items.
    - Inspect the ceiling area above the POS device.

Staff Communication and Education

- As part of card acceptance all staff will be trained annually on how to recognize noticeable signs of equipment tampering by Business Services. It will be the responsibility of the POS custodian to train any new employees in their area to recognize signs of equipment tampering before they can process credit or debit cards.
- Control POS device and PED access by service support representatives. Allow only validated and authorized service personnel to access POS devices and PED's. Unauthorized or unexpected individuals should not be allowed access to the POS device.
    - Business Services is the only area who will provide support for your POS equipment. The PCI Compliance Team will work directly with the POS custodian in your department on all equipment issues.
    - Any third-party persons claiming to be repair or maintenance personnel are prohibited from gaining access to your POS device. Report any personnel attempting to gain access to your POS device to the PCI Compliance Team within Business Services. Do not accept any replacement POS devices from third-party personnel or company.
    - Ensure that only authorized support personnel are escorted and monitored at all times while attending the equipment.

What to Do In the Event of POS Tampering

If you believe your merchant operation has been subject to device tampering, contact the PCI Compliance Team within Business Services.

Engagement of Electronic Commerce (e-commerce): Departments or divisions of the University may engage in e-commerce only with the approval of the WISDM Manager and the PCI Compliance Team. When engaging in e-commerce activities, the department must be able to meet the following standards:

- Adhere to University financial and accounting policies and procedures.
- Satisfy security requirements defined by the University for secure connection and data management.
- Provide the University's privacy statement on their site.
- Keep abreast of University policies and procedures as they relate to e-commerce, as they may be periodically modified.

Standards for Business Process, Paper, and Electronic Processing: All departments must comply with these standards, based on PCI DSS, regardless of what method (i.e. terminal, online processing, paper acceptance, etc.) is used for processing cards. It is the department's responsibility to ensure all staff are trained and apprised of the proper policy and procedures for handling cardholder data.

- Keep storage of cardholder data to a minimum. This means only information necessary for processing should be retained. Mask the primary account number (PAN) showing only the last four digits wherever it is stored
- <u>Never</u> store the following payment card data:
    - Full contents from a magnetic stripe
    - CAV2/CVC2/CVV2/CID – card security code on the back of a payment card.
    - Personal Identification Number (PIN) – a numeric password used to authenticate a

user to a system.

- When absolutely necessary that cardholder information is to be collected on a form, locate that information on the bottom so that it may be cut off and destroyed properly.
- Develop a departmental disposal policy and adhere to it. Verify on a regular basis that the proper procedures are being followed.
- Maintain a regular process to review devices for tampering or substitution.
- Destroy cardholder data (CHD) properly. CHD must be disposed of in a certain manner that renders all data unrecoverable. This includes paper documents and any electronic media. Cross-shredding at the point of sale is recommend..
- Limit access of cardholder data only to those with a business need. Physically restrict payment card processing areas to those individuals with authority to be there. Maintain a list of those with access to payment card data. Assign access privileges based on job classifications and responsibilities. Separate duties to ensure proper controls (i.e. the individual responsible for card processing via terminals should not be the individual responsible for reconciliation).
- Ensure all personnel within their department understand that UWL prohibits anyone from accepting payment card information or processing card payments on behalf of the “customer.”

DEFINITIONS

Card Present

Payment card transaction (conducted face-to-face with a merchant) during which the cardholder is physically present and therefore his or her card is seen and swiped.

Card Not Present

Payment card transaction (conducted usually over internet or telephone) during which the cardholder is not physically present and therefore his or her card is not seen or swiped.

Cardholder Data (CHD)

At a minimum, cardholder data consists of the full PAN. Cardholder data may also include the full PAN plus any of the following: cardholder name, expiration date, and/or service code. In addition, any information on the magnetic strip or chip on the payment card is considered payment card data.

Electronic Commerce (e-commerce)

The buying and selling of goods and services, or the transmitting of funds or data, over an electronic network.

Merchant

Any person or entity that accepts payment cards bearing the logos of any of the five founding members of PCI SSC (American Express, Discover, JCB, MasterCard, or Visa) as payment for goods and/or services.

Payment Card

Any payment card, including debit cards, which is issued by one of the leading payment card brands or associations.

Payment Card Industry Data Security (PCI DSS)

A comprehensive set of requirements established by the PCI SSC for enhancing payment account data security. It is a multifaceted standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical safeguard measures.

Payment Card Industry Security Standards Council (PCI SSC)

The organization founded by American Express, Discover, MasterCard, JCB, and Visa that defines credentials and qualifications for assessors and vendors as well as maintaining the PCI DSS.

Point of Sale (POS)

Hardware and/or software used to process payment card transactions at merchant locations.

Primary Account Number (PAN)

The composite number code of 14 or 16 digits embossed on a bank or payment card and encoded in the card's magnetic strip. The PAN identifies the issuer of the card and the account including part of the account number and contains a check digit that verifies the authenticity of the embossed account number.

Self-Assessment Questionnaire (SAQ)

Tool used by UWL to validate its own compliance with the PCI DSS.

Sensitive Authentication Data

Security-related information including, but not limited to, card validation codes/values (e.g., three-digit or four-digit value printed on the front or back of a payment card, such as CVV2 and CVC2 data), full magnetic-stripe data PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions. Sensitive authentication data must not be stored after authorization.

FORMS

Request to Process Payment Cards Form

REFERENCES

PCI SSC website
www.pcisecuritystandards.org

UW System Administrative Policy 350
Payment Card Compliance Policy
https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/payment-card-compliance-policy/

UW System Administrative Policy 1030, Information Security: Authentication
https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-authentication/

UW System Administrative Procedure 1030.A, Information Security: Authentication
https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-authentication/information-security-authentication/

UW System Administrative Policy 1031 Information Security: Data Classification
https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification-and-protection/

UW System Administrative Procedure 1031.A Information Security: Data Classification
https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/information-security-data-classification/

UW System Administrative Policy 1032 Information Security: Awareness
https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-awareness/

UW System Administrative Policy 1033 Information Security: Incident Response https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-incident-response/

UW System Board of Regent Policy 21-4: Identity Theft Detection, Prevention, and Mitigation
https://www.wisconsin.edu/regents/policies/identity-theft-detection-prevention-and-mitigation/