TO: Andrew Leavitt, Chancellor
FROM: John Koker, Provost and Vice Chancellor
DATE: December 9, 2019
RE: UWS Payment Card Compliance Policy (PCC-DSS) - 350

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 UWS Payment Card Compliance (PCC-DSS) – 350 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

12/16/2019

Date
Payment Card Compliance Policy 350

1. PURPOSE

The purpose of this policy is to protect and prevent loss or disclosure of cardholder data (CHD).

2. RESPONSIBLE OFFICER

Assistant Vice President for Financial Administration

3. SCOPE

This policy governs payment card handling, processing, transmission, storage, and disposal of cardholder data transactions at all UW System institutions including UW System Administration and at all locations that process credit card payments on behalf of UW System and UW System institutions.

Third-parties who have access to cardholder data through relationships with the UW system and UW System institutions are responsible for complying with PCI Standards to ensure the protection of such data.

This policy does not pertain to the University Purchasing Card or Travel Card Program or non-branded loadable institution debit cards.

4. BACKGROUND

UW System institutions can reduce the risk of compromised cardholder data by meeting all applicable Payment Card Industry (PCI) compliance requirements. 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. Protection of cardholder data reduces the risk of this data from being released to anyone other than the acquirer or other approved third-party applications 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
UW System institutions must comply with these security standards to continue to accept payment cards. Non-compliance with these standards put UW System at risk for:

- Large monetary fines assessed to a department and/or to UW System institutions
- Loss of merchant status for a dependent
- Possible loss of merchant status for all UW System institutions
- Potential damage to the institution’s reputation

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.

**Institution:** All research and comprehensive UW System universities and branch campuses, UW-Shared Services, and UW System Administration.

**NACHA:** A non-profit association charged with overseeing the Automated Clearing House (ACH) system, which operates the largest electronic payment network in the world.

**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:** For purposes of PCI DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or VISA, Inc.

**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.

Qualified Security Assessor (QSA): A QSA is an independent security organization that has been qualified by the PCI Security Standards Council to validate an entity’s adherence to PCI DSS. QSA Employees are individuals who are employed by a QSA Company and have satisfied and continue to satisfy all QSA Requirements.

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

UW System institutions may accept payment cards as a form of payment. UW System institutions that accept payment cards must do so in compliance with the PCI Standards and in accordance with this policy document, institutional payment card procedures, and state and federal law. UW System institutions shall attest compliance with PCI standards on an annual basis.

Service Providers and other entities that have access to cardholder data through relationships with the UW system or UW System institutions are responsible for adhering to PCI Standards to ensure the protection of cardholder data. UW System institutions shall verify the compliance of those entities with the current PCI standards continuously by reviewing and obtaining relevant compliance documentation (Attestations of Compliance) from Service Providers or third-party entities.

A. Accepting Payments via Payment Cards

Institutions must accept only payment cards authorized by the UW System Office of Financial Administration and agree to operate in accordance with the contract(s) that UW System or UW System institutions hold with their service provider(s) and the Card Brands. This is to ensure that all transactions comply with the Payment Card Industry Standards, federal regulations, NACHA rules, service provider contracts, and UW System’s policies regarding security and privacy that pertain to electronic transactions.

A UW System institution must not process, store or transmit payment card transactions for related foundations, affiliated organizations or other related third parties, unless that institution adheres to the Service Provider recommendations defined by the PCI DSS in relation to those entities. An institution engaging in these activities should then consult a QSA or the acquirer to ensure PCI compliance is properly reported. Institutions must document the ownership of cardholder data and risk assumptions associated with processing cardholder data with their respective foundations.
Institutions should have procedures for engaging and approving hardware, software, and third-party service providers that process credit card transactions. Select approved PCI-PTS devices, PA-DSS software, P2PE Solutions, or service providers validated on VISA website. In the process the institution should have policies and procedures for ensuring contracts with these entities address PCI Compliance and credit card security. After a solution is implemented compliance is to be validated using the correct PCI Self-Assessment Questionnaire.

All purchased payment card applications must be obtained through appropriate UW System institutions’ purchasing processes and must be PCI compliant. Validation of PCI compliance must be obtained prior to purchase and annually thereafter, by verifying that the payment application is listed on the PCI Security Standards Council’s List of Validated Payment Applications.

All point-to-point encryption solutions (P2PE) must be PCI compliant. Validation of PCI compliance must be obtained prior to implementation and annually thereafter, by verifying that the P2PE solution is listed on the PCI Security Standards Council’s PCI Point-to-Point Encryption (P2PE)™ Solutions list.

Cardholder data (CHD) received through end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.) is never to be used to process a payment. UW System institutions must follow the institutionally approved procedures for the appropriate method of responding to and securely destroying the cardholder data.

Cardholder data cannot be stored on any personal computer, server, or within any software application not validated by the PCI Council. Storage of cardholder data in applications such as Microsoft Excel will bring the entire network into scope and is a violation of PCI DSS.

All payments received must be directed into a UW System Bank Account that is set up to accept electronic transactions (e.g., ACH, Credit Card, Point of Purchase, wire, etc.).

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

B. Cardholder Data Security

Sensitive authentication data must not be stored. Keep storage of card data 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:

- Limitations for data storage amount and retention time to that which is the minimum required for legal, regulatory, and/or business requirements.
- Retention requirements specific to cardholder data. Data that is not necessary to conduct business shall not be retained in any format. All data shall be treated as confidential.
- Specific retention requirements for cardholder data.
• Processes for secure deletion of data when no longer needed
• Quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention time requirements.
• Restrictions to data records. Physical access to data records restricted to staff with a need to know.

C. Incident Response

UW System Institutions shall report and/or respond to potential incidents of compromised cardholder data according to UW System Administrative Policy 1033, Information Security: Incident Response, or an UW System institution-developed incident reporting mechanism that meets or exceeds the requirements of UW System Administrative Policy 1033.

D. Potential Sanctions for Non-Compliance

UW System institutions are responsible for any fees, fines, penalties or other costs resulting from acceptance of payment cards or non-compliance with PCI Standards.

E. Exceptions

Exceptions to this policy require a business plan (including reason why the available processing systems will not work) to be submitted and approved by the institution’s controller in advance of any equipment or system purchase.

F. Procedure

Each institution, including UW System Administration and UW-Shared Services, is responsible for developing procedures that ensure compliance with this policy. Institutions may use the SYS 350 Procedure Templatedocx as a starting point and guide for developing procedures. At a minimum, procedures must include:
• Card acceptance and handling
• Payment card data security
  o Processing and collection
  o Storage and destruction
• Risk assessment
• Incident response
• Policy and training
• Sanctions for non-compliance

7. RELATED DOCUMENTS

Regent Policy Document 25-5, Information Security
UW System Administrative Policy 1030, Information Technology Acquisitions Approval
UW System Administrative Policy 1030, Information Security: Authentication
8. HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/13/2018</td>
<td>Original Issuance Date</td>
</tr>
<tr>
<td>03/29/2019</td>
<td>Revision 1</td>
</tr>
<tr>
<td>05/14/2019</td>
<td>Faculty Senate</td>
</tr>
<tr>
<td>05/16/2019</td>
<td>Senate of Academic Staff</td>
</tr>
<tr>
<td>10/16/2019</td>
<td>University Staff Senate</td>
</tr>
<tr>
<td>06/12/2019</td>
<td>Oshkosh Student Association Senate</td>
</tr>
<tr>
<td></td>
<td>Chancellor</td>
</tr>
</tbody>
</table>

9. CHANCELLOR'S APPROVAL

Chancellor's Signature

Date: 12/16/2019