University of Wisconsin Whitewater

PCI Management Practice Directive

	Division: Administrative Affairs
	Department: Financial Services
	Contact Information: Director of Financial Services, Controller/ Todd Carothers/ (262) 472-1331/ carothet@uww.edu
	Effective Date: MM/DD/2019
	Revised Date:

Authority:

Regent Policy Document 25-5, Information Security
UW System Administrative Policy 350, Payment Card Compliance Policy
UW System Administrative Policy 1010, Information Technology Acquisitions Approval
UW System Administrative Policy 1030, Information Security: Authentication
UW System Administrative Procedure 1030.A, Information Security: Authentication
UW System Administrative Policy 1031, Information Security: Data Classification and Protection
UW System Administrative Procedure 1031.A, Information Security: Data Classification
UW System Administrative Procedure 1031.B, Information Security: Data Protections
UW System Administrative Policy 1032, Information Security: Awareness
UW System Administrative Policy 1033, Information Security: Incident Response
PCI DSS Quick Reference Guide v3.2
University of Wisconsin System Fiscal & Accounting General Records Schedule

Objective:

The purpose of this procedure is to highlight Payment Card best practices and to prevent disclosure of cardholder data (CHD) in accordance with University of Wisconsin System Administrative Policy 350, Payment Card Policy.

Statement:

UW System Administrative Policy 350, Payment Card policy, requires that all UW System institutions develop procedures to prevent loss or discloser of cardholder data. 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.* In order to ensure this information is properly handled please consult the corresponding procedure for appropriate card acceptance and handling requirements, data security prevention measures as well as basic incident protocols.

Procedures:

PCI Management Procedure

Searchable Words:

Service Provider, Payment Card Industry data security standards (PCI DSS), Cardholder, Cardholder Data, High Risk Data, Institution, Merchant Account, Merchant department, Payment Card, Payment Card Industry data security standards (PCI DSS), Sensitive authentication Data, Service Provider.

University of Wisconsin Whitewater

PCI Management Procedure

Intent:

The purpose of this document is to ensure appropriate management of Payment Card Industry (PCI) best practices at UW – Whitewater.

Scope:

This Procedure document, along with the corresponding Payment Card Practice Directive, provide a framework for ensuring PCI best practices are consistently followed to protect cardholder information and put in place clear expectations around merchants' role in this process .

Definitions:

PCI Security Incident. A violation or imminent threat of violation of PCI data confidentiality. Examples include exposure or a hack of cardholder data to unauthorized organizations or persons. The exposure could happen internal to the University or with a third-party processor.

Institutions. All four-year UW System campuses, UW Colleges, the University of Wisconsin- Extension, and UW System Administration.

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 all 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 a part of a payment transaction.

Merchant Account: A bank account that enables the holder to accept credit cards for payment.

Merchant department: any department or unit (can be a group of department or a subset of a department) which has been approved by a UW System institution to accept payment cards.

Payment Card: a financial transaction card (Credit, Debit, etc.) issued by a financial institution: also called bankcard/payment card/charge card/ credit card/ debit card.

Table of Contents:

Best Practices:

Best practices involve the implementation of preventative measures to secure systems and reduce the risk of incidents occurring.

Specific Responsibilities

Step	Action
1.	The UW-Whitewater Instructional, Communication and Information Technology Department (iCIT) will evaluate current methodologies used to monitor systems for indicators of compromise. They will also review and evaluate tools and processes to improve threat prevention and detection. iCIT will leverage the Information Security Incident Response Procedure to implement improvements in vulnerability management, and incorporate improvements based on lessons learned from incident handling.
2.	The Merchant Department is expected to: • maintain a list of third-party processors used as part of its PCI transactions and document their procedures. • ensure contact information is up to date with the third-party processor for proper communications. • monitor business and vendor information to identify potential risks. • notify the Director of Financial Services of the potential incident.

General Milestones for Prioritizing PCI Compliance Efforts

	Goal
1.	**Remove sensitive authentication data and limit data retention.** This milestone targets a key area of risk for entities that have been compromised. Remember – if sensitive authentication data and other cardholder data are not stored, the effects of a compromise will be greatly reduced. If you don't need it, don't store it.
2.	**Protect systems and networks, and be prepared to respond to a system breach.** This milestone targets controls for points of access to most compromises, and the processes for responding.
3.	**Secure payment card applications.** This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas offer easy prey for compromising systems and obtaining access to cardholder data.
4.	**Monitor and control access to your systems.** Controls for this milestone allow you to detect the who, what, when, and how concerning who is accessing your network and cardholder data environment.
5.	**Protect stored cardholder data.** For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protection mechanisms for that stored data.
6.	**Finalize remaining compliance efforts, and ensure all controls are in place.** The intent of Milestone Six is to complete PCI DSS requirements, and to finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment.

Information Security Incident Response:

Contact the iCIT Help Desk in the event of an information security incident and refer to the steps below for additional information.

1.	The Merchant Department and/or iCIT Help Desk will alert the Director of Financial Services of a potential incident.
2.	The Director of Financial Services will notify the Associate Vice Chancellor for iCIT and the Vice Chancellor for Administrative Affairs of the potential incident. Consultation of the Information Security Incident Response Procedure will occur to manage the preparation, detection and analysis, containment, eradication and recovery, as well as necessary post-incident activity.
3.	UW-W iCIT, Director of Financial Services, and the Merchant Department will discuss the appropriate response to the potential incident including further confirmation with third-party processors, additional internal testing, and communication with UW System AVP for Information Security.
4.	The Merchant Department will: • collect all information received or available publicly related to a third-party processor's potential incident and store PDFs of this information related to the potential incident. This includes email notifications. • collect all related communications. • collect any subsequent testing and/or analysis related to the potential incident. • maintain all information for a three-year period.
5.	The iCIT Department will test the incident response procedure annually to evaluate and enhance response capabilities, as well as ensure this procedure stays in alignment with the Information Security Incident Response Procedure and the Payment Card Procedure.

Resources:

PCI Management Practice Directive

Administration:

Approval Details

Approval Authority:	Regent Policy Document(s): Regent Policy Document 25-5, Information Security UW System Policy: UW System Administrative Policy 1033 Information Security: Incident Response, UW System Administrative Policy 1031, Information Security: Data Classification and Protection
Approval date:	MM/DD/2019
Version no:	V1.0
Date for next review:	MM/DD/2022

Revision History

Version	Revision date	Description of changes	Author
1.0	MM/DD/2019	Procedure established	Quality Assurance Improvement Manager

Contact Person/Unit

Contact Person/Unit:	Director of Financial Services, Controller

Keywords

Keywords:	Service Provider, Payment Card Industry data security standards (PCI DSS), Cardholder, Cardholder Data, High Risk Data, Institution, Merchant Account, Merchant department, Payment Card, Payment Card Industry data security standards (PCI DSS), Sensitive authentication Data, Service Provider.