UNIVERSITY OF WISCONSIN OSHKOSH

Appendix 1 - Credit Card Security Incident Response Plan

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

Contents

Revisions/Approvals

Ver. #	Changes By	Ver. date	Reason
1.0	R. Sitzberger D. Lewis	08/01/2018	Adopted and modified template from CampusGuard

Purpose

The Payment Card Security Incident Response Plan supplements the University Incident Response Plan.

To address credit cardholder security, the major card brands (Visa, MasterCard, Discover, and American Express) jointly established the PCI Security Standards Council to administer the Payment Card Industry Data Security Standards (PCI DSS) that provide specific guidelines for safeguarding cardholder information. One of these guidelines requires that merchants create a Security Incident Response Team (Response Team) and document an Incident Response Plan (IRP).

This document defines those responsible, the classification and handling of, and the reporting/notification requirements for incident response plan at the University of Wisconsin Oshkosh (UW Oshkosh).

Scope/Applicability

A list of the merchants and operations with payment card acceptance and IP addresses has been provided to the Information Technology Security Office to identify the areas of accepting payment cards. This procedure is in effect for all departments or persons receive or have access to cardholder data.

Authority

Security Incident Response Team

The University of Wisconsin Oshkosh credit card Response Team is comprised of Financial Services and Information Technology. See below for names and contact information.

University of Wisconsin Oshkosh Credit Card Security Incident Response Team
Communication for the Response Team can be sent to helpdesk@uwosh.edu.

Name	**Department/Title**	**Role**	**Telephone**	**Email**
Jeanne Schneider	AVC/Controller	PCI Committee Chairperson	(920) 424-0717	schneiderj@uwosh.edu
Deborah Matulle	Assistant Controller	PCI Team Member	(920) 424-3318	matulle@uwosh.edu
Daphne Lewis	Senior Business Analyst	PCI Team Member	(920) 424-2174	lewisdc@uwosh.edu
Jean Wolfgang	Bursar	PCI Team Member	(920) 424-1442	wolfganj@uwosh.edu
Rachel Grose	Bursar Generalist	PCI Team Member	(920)424-1336	groser@uwosh.edu
Mark Clements	Director of Information Services	PCI Security Lead	(920)424-3020	clementsm@uwosh.edu
Richard Montano	IT Specialist	PCI IT Specialist	(920)424-3020	montanor@uwosh.edu

Procedures

Incident Response Plan (IRP)

The Incident Response Plan needs to take into account that incidents may be reported/identified through a variety of different channels but the Incident Response Team will be the central point of contact and responsible for executing UW Oshkosh Incident Response Plan.

The UW Oshkosh security incident response plan is summarized as follows:

1. All incidents must be reported to the Response Team.
2. All actions taken must be documented on the Payment Card Incident Log (appendix A)
3. The Response Team will confirm receipt of the incident notification.
4. The Response Team will investigate the incident and assist the compromised department in limiting the exposure of cardholder data.
5. The Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
6. The Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future.

An 'incident' is defined as a suspected or confirmed 'data compromise'. A 'data compromise' is any situation where there has been unauthorized access to a system or network where prohibited, confidential or restricted data is collected, processed, stored or transmitted; Payment Card data is prohibited data. A 'data compromise' can also involve the suspected or confirmed loss or theft of any material or records that contain cardholder data.

In the event of a suspected or confirmed incident:

1. Do NOT touch or compromise any possible evidence. Do not shut off any computer or POS system.
2. Contact the Response Team. Make *verbal* contact with a team member, DO NOT LEAVE A VOICE MAIL. (During business hours contact the HelpDesk at (920)424-3020. After hours, contact University Police)
    a. Overview of incident, including date, time, and location of incident
    b. Incident Type
        i. Computer Abuse
        ii. Malicious Code
        iii. Spam
        iv. Unauthorized Access/Use
        v. Breach of Physical Security (unlocked file cabinet, storage room, etc.)
        vi. Possible tampering of POS device
        vii. Other
    c. Intrusion Method
        i. Virus
        ii. Spyware/Malware
        iii. Stolen Password
        iv. Other
    d. Overview of data on the system? Was it sensitive?
    e. Explanation of discovery

   f. Action taken upon discovery
   g. Explanation of impact and impact on daily activities
   h. Any additional information
3. The Response Team will immediately coordinate a response and reply to this initial notification/communication to confirm they are aware of the incident.
4. If the incident involves a payment station (PC used to process credit cards):
   a. Do NOT turn off the PC.
   b. Disconnect the network cable connecting the PC to the network jack. If the cable is secured and you do not have the key to the network jack, simply cut the network cable.
5. Document any steps taken until the Response Team has arrived. Include the date, time, person/persons involved and action taken for each step.
6. Assist the Response Team as they investigate the incident.

Incident Response Team Procedures

The UW Oshkosh Credit Card Security Incident Response Team must be contacted by a department in the event of a system compromise or a suspected system compromise. After being notified of a compromise, the Response Team, along with other designated university staff from Computers and Information Technology, will implement their incident response plan to assist and augment departments' response plans.

In response to a system compromise, the Response Team and Computers and Information Technology will:

1. Ensure compromised system is isolated on/from the network.
2. Gather, review and analyze all centrally maintained system, firewall, file integrity and intrusion detection/protection system logs and alerts.
3. Assist department in analysis of locally maintained system and other logs, as needed.
4. Conduct appropriate forensic analysis of compromised system.
5. If an incident of unauthorized access is confirmed and card holder data was potentially compromised, the PCI Committee, depending on the nature of the data compromise, must notify the appropriate organizations that may include the following:
   a. UW Oshkosh Chief Financial Officer and the Chief Information Officer
   b. UW Oshkosh Internal Audit group
   c. UW Oshkosh Acquiring Bank(s), the Acquiring Bank will be responsible for communicating with the card brands (VISA, MasterCard)
      i. see Bank Breach Response Plan
      ii. see Visa – Responding to a Breach
      iii. see MasterCard – Responding to a Breach
   d. If American Express payment cards are potentially included in the breach the University is responsible for notifying and working with American Express
      i. For incidents involving American Express cards, contact American Express Enterprise Incident Response Program (EIRP) within 24 hours after the reported incident.
         1. Phone number: (888) 732-3750
         2. Email: EIRP@aexp.com.
      ii. For more detail see American Express – Responding to a Breach

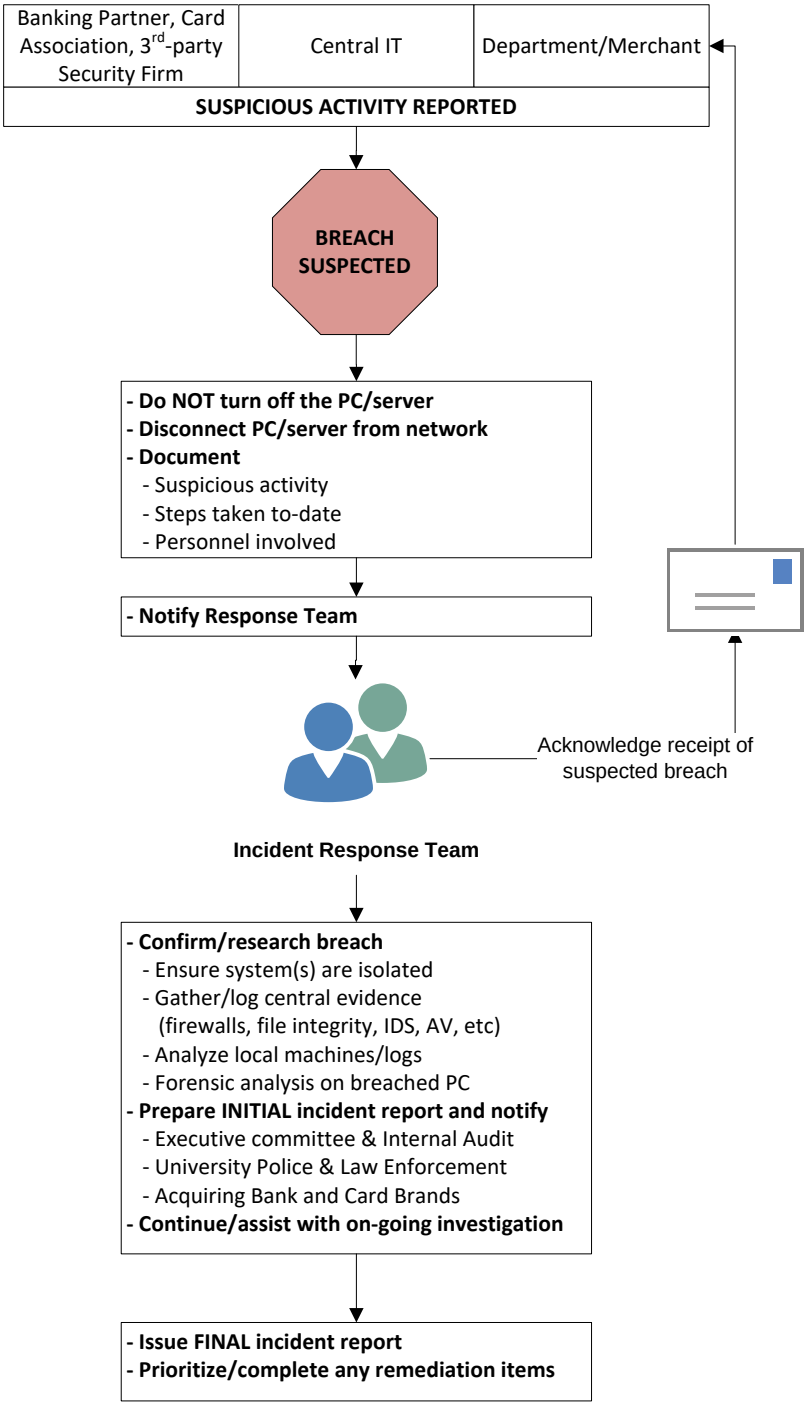
e. If Discover Network payment cards are potentially included in the breach the University is responsible for notifying and working with Discover Network.
    i. If there is a breach in your system, notify Discover Security within 48 hours.
        1. Phone Number: (800) 347-3083
    ii. For more details see Discover Network – Fraud Prevention FAQ
f. Campus police and local law enforcement

6. Assist card industry security and law enforcement personnel in investigative process.

Bank Breach Response Plans

The credit card companies have specific requirements the Response Team must address in reporting suspected or confirmed breaches of cardholder data. For Visa and MasterCard it is the University's responsibility to notify their own bank (the financial institution(s) that issues merchant accounts to the university) and the University's bank will be responsible for notifying Visa and MasterCard, were applicable.

Flow Chart for Suspected Breach



Symptoms of Data Breaches

Detecting date breaches is a difficult task that requires planning, diligence and participation from staff from multiple departments across the institution. While there are systems that can be implemented to provide automated monitoring to look for symptoms of breaches there are also some symptoms that may be detected by staff during the course of their normal, daily activities.

- A system alarm or similar indication from an intrusion detection tool
- Unknown or unexpected outgoing Internet network traffic from the payment card environment
- Presence of unexpected IP addresses or routing
- Suspicious entries in system or network accounting
- Accounting discrepancies (e.g. gaps in log-files)
- Unsuccessful logon attempts
- Unexplained, new user accounts
- Unknown or unexpected services and applications configured to launch automatically on system boot
- Anti-virus programs malfunctioning or becoming disabled for unknown reasons
- Unexplained, new files or unfamiliar file names
- Unexplained modifications to file lengths and/or dates, especially in system executable files
- Unexplained attempts to write to system files or changes in system files
- Unexplained modification or deletion of data
- Denial of service or inability of one or more users to log in to an account
- System crashes
- Poor system performance
- Unauthorized operation of a program or sniffer device to capture network traffic
- Use of attack scanners, remote requests for information about systems and/or users, or social engineering attempts
- Unusual time of usage
- Unauthorized wireless access point detected

Card Association Breach Response Plans

Visa – Responding to a Breach

Follow the steps set forth in the resource:
http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf

Initial Steps and Requirements for Visa Clients (Acquirers and Issuers)

(A full description of the steps is available at the link listed above)

Notification

1. Immediately report to Visa the suspected or confirmed loss or theft of Visa cardholder data. Clients must contact the Visa Risk Management group immediately at the appropriate Visa region.
2. Within 48 hours, advise Visa whether the entity was in compliance with PCI DSS and, if applicable, PCI PA-DSS and PCI PIN Security requirements at the time of the incident. If so, provide appropriate proof.

Preliminary Investigation

3. Perform an initial investigation and provide written documentation to Visa within three (3) business days. The information provided will help Visa understand the potential exposure and assist entities in containing the incident. Documentation must include the steps taken to contain the incident.

MasterCard – Responding to a Breach

The MasterCard Account Data Compromise User Guide sets forth instructions for MasterCard members, merchants, and agents, including but not limited to member service providers and data storage entities regarding processes and procedures relating to the administration of the MasterCard Account Data Compromise (ADC) program.
http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf

American Express – Responding to a Breach

Merchants must notify American Express immediately and in no case later than twenty-four (24) hours after discovery of a Data Incident.

To notify American Express, please contact the American Express Enterprise Incident Response Program (EIRP) toll free at (888) 732-3750/US only, or at 1-(602) 537-3021/International, or email at EIRP@aexp.com. Merchants must designate an individual as their contact regarding such Data Incident.

For more complete language on the obligations of merchants and service providers see the following 2 documents:

- American Express® Data Security Operating Policy for Service Providers
  https://merchant-channel.americanexpress.com/merchant/en_US/data-security
- American Express Data Security Operating Policy – U.S.
  https://icm.aexp-static.com/Internet/NGMS/US_en/Images/DSOP_Merchant_US.pdf
- American Express Data Security Operating Policy – Australia
  https://icm.aexp-static.com/Internet/NGMS/alpha/webstatic/dashboard/pdf/au/en/datasecurity/DSOP_Merchant_Australia_Oct17.pdf

Incident Classification, Risk Analysis and Action Matrix

Each incident should be reviewed based on the risk and action matrix, which attempts to reflect the severity of the incident and its impact. Then, decisions on whether to develop further controls and processes can be made so work-tickets can be created and prioritized so that identified vulnerabilities are addressed.

	Security Problem Family				
Security Problem	**Unlawful Activity**	**Violation of Appropriate Usage Policy**	**Data Disclosure**	**Network Device Compromises**	**Vulnerabilities**
PCI-DSS Breach Distribution of Copyrighted Material Breach of HIPPA Breach of Telecommunications Act	1				
Confidential data at risk of disclosure to the Internet. Highly Confidential of a personal nature data at risk of disclosure to the network.			1		
Confidential data, of a personal nature at risk of disclosure to the network.			2		
Network resources providing un-authenticated access to data not intended for public distribution.			3		
Tools installed which present a significant risk to network stability				1	
Malicious Software eg. Virus/Trojan. No User Interaction required for infection				1	
Port scanning		2		2	
Unauthorised Publishing Service that can be used for content distribution. Eg. FTP Server.				2	
Malicious Software eg. Virus/Trojan. User interaction required for infection.				3	
Vulnerability more than one week old that allows arbitrary code to be run					4
Highly Insecure Configuration					4
Vulnerability less than one week old that allows arbitrary code to be run					5

Action Class	Actions to be taken by Response Team	Escalation Process	Default Action Period
1	- If required, completely block all network access. - Phone call to Response Team to notify of the problem, if IT Security and Risk Officer unavailable, call to CIO or Senior Manager - If required, duplicate disks - For network device compromise notify Regional CERT (US-CERT or AUS-CERT) of suspected source IP.	- If action not completed in required time, Alert CIO and/or Senior Management of the affected area.	1 Hour
2	- If required, block direct Internert access. - Verbal contact with Response Team. - Phone call to IT Security and Risk Officer to notify of the problem. - For network device compromise notify Regional CERT (US-CERT or AUS-CERT) of suspected source IP. - If required, duplicate disks	- If action not completed in required time, escalate to Class 1 - Alert Service, System or Application Manager as appropriate.	2 Hours
3	- Verbal contact with Response Team. - Phone IT Security Officer for region. - For network device compromise notify Regional CERT (US-CERT or AUS-CERT) of suspected source IP.	- If action not completed in required time, escalate to Class 2	4 Hours
4	- Verbal contact with Response Team.	- If action not completed in required time, escalate to Class 3	1 Day
5	- Verbal contact with Response Team.	- If action not completed in required time, escalate to Class 4 - If a network device is compromised escalation is to Class	1 Week

Interpretations

The authority to interpret this procedure rests with the Chancellor and the Finance and Administration Leadership Team.

Definitions

Term	Definition
Payment Card Industry Data Security Standards (PCI DSS)	The security requirements defined by the Payment Card Industry Security Standards Council and the 5 major Credit Card Brands: • Visa, MasterCard, American Express, Discover, JCB
Cardholder	Someone who owns and benefits from the use of a membership card, particularly a credit card.
Card Holder Data (CHD)	Those elements of credit card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date and the Service Code.
Primary Account Number (PAN)	Number code of 14 or 16 digits embossed on a bank or credit card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.

Cardholder Name	The name of the Cardholder to whom the card has been issued.
Expiration Date	The date on which a card expires and is no longer valid. The expiration date is embossed, encoded or printed on the card.
Service Code	The service code that permits where the card is used and for what.
Sensitive Authentication Data	Additional elements of credit card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data and PIN/PIN block.
Magnetic Stripe (i.e., track) data	Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.
CAV2, CVC2, CID, or CVV2 data	The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card- not-present transactions.
PIN/PIN block	Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.
Disposal	CHD must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, USB storage devices,(Before disposal or repurposing, computer drives should be sanitized in accordance with the (Institution's) Electronic Data Disposal Procedure). The approved disposal methods are: • Cross-cut shredding, Incineration, Approved shredding or disposal service
Merchant Department	Any department or unit (can be a group of departments or a subset of a department) which has been approved by the (institution) to accept credit cards and has been assigned a Merchant identification number.
Merchant Department Responsible Person (MDRP)	An individual within the department who has primary authority and responsibility within that department for credit card transactions.
Database	A structured electronic format for organizing and maintaining information that is accessible in various ways. Simple examples of databases are tables or spreadsheets.

Wireless Access Point	Also referred to as "AP." Device that allows wireless communication devices to connect to a wireless network. Usually connected to a wired network, it can relay data between wireless devices and wired devices on the network.

Appendix A. Payment Card Incident Log

In the event of a suspected or confirmed, please follow the procedures below ensuring each step taken is documented using this incident log:

1. Start a new payment card incident log. Name and phone number of person reporting incident.

2. Contact the Response Team by sending an email documenting the incident to helpdesk@uwosh.edu or (920)424-3020

Action	Date/Time	Location	Person (s) performing action	Person(s) documenting action
Additional notes				

3. The Response Team will immediately coordinate a response and reply to this initial notification/communication to confirm they are aware of the incident.
4. If the incident involves a payment station (PC used to process credit cards):
    a. Do NOT turn off the PC.
    b. Disconnect the network cable connecting the PC to the network jack. If the cable is secured and you do not have the key to the network jack, simply cut the network cable.
5. Document any steps taken until the Response Team has arrived. Include the date, time, person/persons involved and action taken for each step.
6. Assist the Response Team as they investigate the incident.
7. If an incident of unauthorized access is confirmed and card holder data was potentially compromised, the PCI Committee Chairperson will make the following contacts with UW Oshkosh acquiring bank(s) after informing the Chief Financial Officer and the Chief Information Officer:
    a. For incidents involving Visa, MasterCard or Discover network cards, contact Elavon within 72 hours or reported incident.

YES ☐ NO ☐

If YES, date and time systems were removed:

_____

Name of person(s) who disconnected the network:

_____

If NO, state reason:

_____

_____

_____

Actions Performed

Action	Date and Time	Location	Person(s) performing action	Person(s) documenting action