Date of Last Revision: September 2024
Responsible Department: Information Technology

Grand Valley State University Payment Card Industry (PCI) Security Incident Response Plan

Payment Card Industry Data Security Standard (PCI DSS) Version 4.0

Contents

I. Background / Purpose

The Payment Card Industry Data Security Standard (PCI DSS) is a mandatory set of requirements developed by the PCI Security Standards Council (PCI SSC) and enforced by the major credit card companies. These security requirements apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as forms of payment. Further details about PCI can be found at the PCI Security Standards Council website (https://www.pcisecuritystandards.org).

To accept credit or debit card payments, Grand Valley State University (GVSU) must establish and maintain compliance with the PCI DSS. The PCI DSS contains requirements for detecting and responding to suspected or confirmed security incidents that impact payment card data. These requirements address the security risks inherent in the acceptance and handling of payment card data.

This document defines those responsible for, the classification and handling of, and the reporting/notification requirements for the incident response plan at GVSU.

II. Scope

Responsibility for following this Incident Response Plan (IRP) falls to all GVSU staff that store, process, or transmit payment card data on behalf of GVSU, or affect the security of such payment card data.

III. Policy Statement

Incident Response Team

GVSU has formed an Incident Response Team (IRT) chaired by Luke DeMott and comprised of GVSU staff. The names and contact information for IRT members are listed in Appendix A.

The IRT is responsible for leading all incident investigation and response activities, and at least one IRT member must always be available to ensure 24/7 response capability. The IRT has the authority to confiscate or disconnect equipment, monitor suspicious activity, and obtain copies of data or records in support of its incident response efforts. IRT members shall participate in training on their incident response responsibilities as defined in the organization's targeted risk analysis.

Payment Card Incident

In the event of a suspected or confirmed payment card incident, the personnel/department identifying the incident shall notify the IRT at security@gvsu.edu and always cooperate with the IRT and in accordance with the procedures described in section IV below.

A payment card incident is an incident which impacts:

1. Systems, devices, or networks that store, process, or transmit payment card data;
2. Systems or devices that could affect the security of the systems, devices, or networks described in (1) above; or
3. Account data in any form, whether paper or electronic, encrypted, or unencrypted.

A payment card incident includes but is not limited to:

- Any situation where there has been unauthorized access to a system, device, or network described under (1) or (2) above; and
- The loss or theft of any material or records that contain account data.

Additionally, a "suspected" payment card incident includes but is not limited to:

- Any situation where security protections for account data have failed (e.g., payment card data accessible to unauthorized personnel); or
- Any situation where account data is discovered where it is not expected, regardless of whether there is any evidence of unauthorized access to such data.

Incident Response Plan Review and Testing

This IRP shall be reviewed at least annually, and updated as needed (e.g., due to organizational changes, new PCI DSS requirements, or industry developments). The plan shall also be tested at least annually.

IV. Incident Response Plan

The IRP needs to consider 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 the Incident Response Plan.

The GVSU IRP is summarized as follows:

1. All suspected incidents must be reported to the Incident Response Team (IRT) immediately.
2. All actions taken must be documented.
3. The IRT will confirm receipt of the incident notification.
4. The IRT will investigate the incident and determine if a breach has occurred.
5. If a breach is confirmed, the IRT will assist the compromised department in limiting the exposure of account data.
6. The IRT will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card brands, credit card processors, etc.) as necessary.
7. The IRT will determine if policies and/or processes need to be updated to avoid a similar incident in the future.

Preparation

Adequate preparation is a critical component to incident response because incidents are typically unanticipated and can take many forms. Additionally, severe incidents can pose the challenge of service interruptions that can impact the tools and communication methods that

would typically be used by the IRT. Thus, it is important that procedures and fallback plans exist to ensure that the IRT can still function in the event of a severe incident.

GVSU maintains a central email address security@gvsu.edu, which is monitored at all times by at least one IRT member. The IRT also maintains contact lists for IRT members (see Appendix A) and critical internal and external resources that the IRT may need for assistance with incident response activities.

The IRT will use the GVSU Service Portal https://services.gvsu.edu for tracking incident response activities. In the event it is unavailable at the time of an incident, the IRT will use the payment card incident log included in Appendix D.

Detection and Notification of IRT

Detecting data breaches is a difficult task that requires planning, diligence, and participation of staff from multiple departments across the organization. While GVSU has configured automatic alerting for some indicators of a potential incident, other indicators may be detected by personnel during the course of their normal, daily activities.

Alerts are configured to notify IT personnel in the case of events from:

- Intrusion detection/intrusion prevention systems
- Firewalls and routers
- System file integrity monitoring
- File integrity monitoring on payment webpages
- Detection mechanisms for unauthorized wireless access points

Additional signs of a potential incident can include:

- 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 logs, or 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-malware software 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 use of software or a sniffer device used to capture network traffic
- Use of port scanners, remote requests for information about systems and/or users, or social engineering attempts

- Unusual time of usage
- Unexpected/unauthorized removable media present
- Missing/stolen device

Upon detecting a potential incident, the person or department detecting the incident should immediately follow the steps below:

1. Contact the Incident Response Team either in person or via email at security@gvsu.edu Include the following details:
    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. Discovery of account data in unexpected location
        viii. Other
    c. Intrusion Method (if applicable)
        i. Virus
        ii. Spyware/Malware
        iii. Stolen Password
        iv. Other
    d. Overview of data impacted (i.e. type of data, etc.)
        i. Is PAN (card numbers) impacted?
        ii. Is sensitive authentication data impacted?
    e. Explanation of how the incident was discovered
    f. Actions taken upon discovery
    g. Anticipated impact on daily activities and customers
    h. Any additional information
2. The Incident Response Team will immediately coordinate a response and reply to this initial notification/communication to confirm they are aware of the incident.
3. Document any steps taken until the Incident Response Team has begun investigating the incident. Include the date, time, person/persons involved, and action taken for each step.
4. Assist the Incident Response Team as they investigate the incident.

IRT Response

In response to a potential incident, the IRT will:

1. Ensure any compromised systems are isolated from other devices on the network.
2. Classify and prioritize the incident in accordance with Section VII below.
3. Coordinate the backup of impacted data, where applicable.
4. Gather, review, correlate, and analyze all centrally maintained logs and alerts.
5. Assist department in analysis of locally maintained logs, as needed.
6. Conduct appropriate forensic analysis of any compromised systems.
7. Notify the appropriate personnel/organizations that may include the following:

a. Chief Financial Officer and the Chief Information Officer
b. Internal Audit group
c. Law enforcement
d. PCI Committee
e. Acquiring Bank(s) (see Section V below)*
f. If American Express payment cards are potentially impacted, American Express must be notified within 72 hours. More details on the AmEx requirements can be found in Section VI below.
g. If Discover Network payment cards are potentially impacted, Discover must be notified within 48 hours by calling (800) 347-3083.
h. Other external entities as required by law or contractual obligations.

8. Oversee eradication efforts, including identification and mitigation of any exploited vulnerabilities and removal of malware, compromised accounts, etc.
9. Coordinate the restoration of business operations in accordance with Grand Valley State University's comprehensive emergency response plan. (https://www.gvsu.edu/cms4/asset/45587EC7-FE4C-BB4F-80A05E76DBCD3970/2020_final_update.pdf).
10. Coordinate the long-term preservation of data where appropriate (e.g., for potential litigation)
11. Determine whether any additional external reporting is required.
12. Complete an incident report form (See Appendix B).
13. Where needed, conduct a lessons-learned meeting to identify changes to configurations or processes to better prevent or detect future incidents.

* The acquiring bank will be responsible for communicating with Visa and MasterCard
    a. More details on the Visa requirements can be found in Section VI below
    b. More details on the MasterCard requirements can be found in Section VI below

V. Bank Breach Response Procedures

Elavon
Notification of a suspected breach should go to the acquiring bank, Elavon, immediately following discovery of a Data Incident. To notify Elavon, contact Beverly Baker, the Incident Response Representative at 502.933.8406 or Elavon Customer Support Service at 888.292.5934.

Stripe – https://stripe.com

NetBank – https://netbank.ph

VI. Card Brand Breach Response Plans

Visa

While the initial notification of a suspected breach should go to the acquiring bank, Visa does require notification of a breach within three (3) calendar days of discovery of the event, as well as a completed "Incident Report" within three (3) calendar days of the initial notification. This report can be found in Visa's "What to do if compromised" guide (links below).

US: http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf

Australia: https://www.visa.com.au/content/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

MasterCard

The MasterCard Security Rules and Procedures set forth instructions for MasterCard members, merchants, and agents (including but not limited to service providers, data storage entities, and terminal servicers) regarding processes and procedures relating to the administration of the MasterCard Account Data Compromise (ADC) program.

Online Resources – PCI 360 page:
https://www.mastercard.com/globalrisk/en/resources/pci360.html

Security Rules and Procedures – Merchant Edition

US: https://www.mastercard.us/content/dam/public/mastercardcom/na/global-site/documents/SPME-Manual.pdf

Australia: https://www.mastercard.com.au/content/dam/public/mastercardcom/na/global-site/documents/SPME-Manual.pdf

American Express

Merchants must notify American Express immediately and in no case later than seventy-two (72) hours after discovery of a Data Incident.

To notify American Express, contact the American Express Enterprise Incident Response Program (EIRP) toll free at 1.888.732.3750/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.

American Express Data Security Operating Policy

US: https://www.americanexpress.com/content/dam/amex/us/merchant/new-data-security/DSOP_United_States_EN.pdf

Australia: https://www.americanexpress.com/content/dam/amex/us/merchant/new-merchant-regulations/Regs_EN_AU.pdf

VII. 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, work-tickets created and prioritized, and identified vulnerabilities can be addressed.

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 action not completed in required time, Alert CIO and/or Senior Management of the affected area.	1 Hour
2	- If required, block direct Internet access. - Email sent to Response Team. - Phone call to IT Security and Risk Officer to notify of the problem.	- If action not completed in required time, escalate to Class 1 - Alert Service, System or Application Manager as appropriate.	2 Hours
3	- Email sent to Response Team. - Phone IT Security Officer for region.	- If action not completed in required time, escalate to Class 2	4 Hours
4	- Email sent to Response Team.	- If action not completed in required time, escalate to Class 3	1 Day
5	- Email sent to Response Team.	- If action not completed in required time, escalate to Class 4 - If a network device is compromised escalation is to Class 3	1 Week

	Security Problem Family				
Payment Card Security Problem	**Unlawful Activity**	**Violation of Appropriate Usage Policy**	**Data Disclosure**	**Network Device Compromises**	**Vulnerabilities**
Unauthorized access to data or systems in PCI environment	1		1		
Account data at risk of disclosure to the internet or unauthorized people (personnel or the public).			1		
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 e.g. Virus/Trojan. No User Interaction required for infection				1	
Port scanning		2		2	
Malicious Software e.g. Virus/Trojan. User interaction required for infection.				3	
Highly Insecure Configuration					4
Vulnerability less than one week old that allows arbitrary code to be run					5

VIII. Other Supporting Documents

GVSU PCI Policies: https://www.gvsu.edu/pci

IX. 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 major Credit Card Brands.
Cardholder	Someone who owns and benefits from the use of a membership card, particularly a payment card.
Account Data	Consists of Cardholder Data and/or Sensitive Authentication Data.
Cardholder 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.

Appendix A – Incident Response Team Contact Information

Report incidents to the monitored IRT mailbox at security@gvsu.edu				
Name	**Department/Title**	**Role**	**Telephone**	**Email**
DeMott, Luke	Information Technology/Associate Vice President of Information Technology and Chief Information Security Officer	PCI Committee Chairperson	(616) 331-8832	demottl@gvsu.edu
Van Sweden, David	Information Technology/Information Security Analyst	PCI Technical Lead	(616) 331-3107	vansweda@gvsu.edu
Vedders, Greg	Information Technology/ Security Principal Lead	PCI Technical Lead	(616) 331-9484	veddersg@gvsu.edu
Reynolds, Chad	Business & Finance/Director of Treasury	PCI Banking Liaison	(616) 331-9484	reynchad@gvsu.edu

Appendix B – Incident Report Form

For Incident Response Team Use Only

Report Date/Time:

Initial or Final Report: **Initial** ☐ **Final** ☐

Confidentiality

Distribution of this document is limited to Information Technology. Access should only be granted to those with a business-related need-to-know. If you have any questions pertaining to the distribution of this document, please contact Assistant Vice President and Chief Information Security Officer.

Reporting Party

Name:	
Title:	
Telephone/Email:	

Summary

The summary is at a high level, suitable for upper management. Elements include:

- Basic description of the incident
- Systems, services and/or user communities impacted by the incident
- Whether service was impacted, degraded, or interrupted
- Duration of the incident (start to finish)

Details of the Incident, Steps Taken To-date

Specifically, what caused the incident (who, what, where, when, how) and what steps have been taken by the reporting party to-date.

- Description of the incident
- Detail the flow of the incident response (i.e. John -> Suzanne -> Mike)

Systems

Steps Taken To-date:	
Network cable unplugged (time/date):	
Last time machine rebooted (time/date):	
When anomalous activity was noticed (time/date):	
IR Team notified (time/date):	
Additional Details:	

IRT Lead

- Identify the IR team member assigned to take the lead on this incident.

Name:	
Title:	
Telephone/Email:	

Incident Analysis

PCI Data Breach Yes/No:	
Justification:	

If PCI Data Breach is "Yes" complete the following steps.

Time/date of bank / card brand notification(s)

Notification time(s)/date(s):	

Steps taken during forensic investigation

ATTACHMENTS

Please attach any supporting documents. These documents may include:

- Logs or error messages
- Contents of trouble tickets
- Contents of e-mail

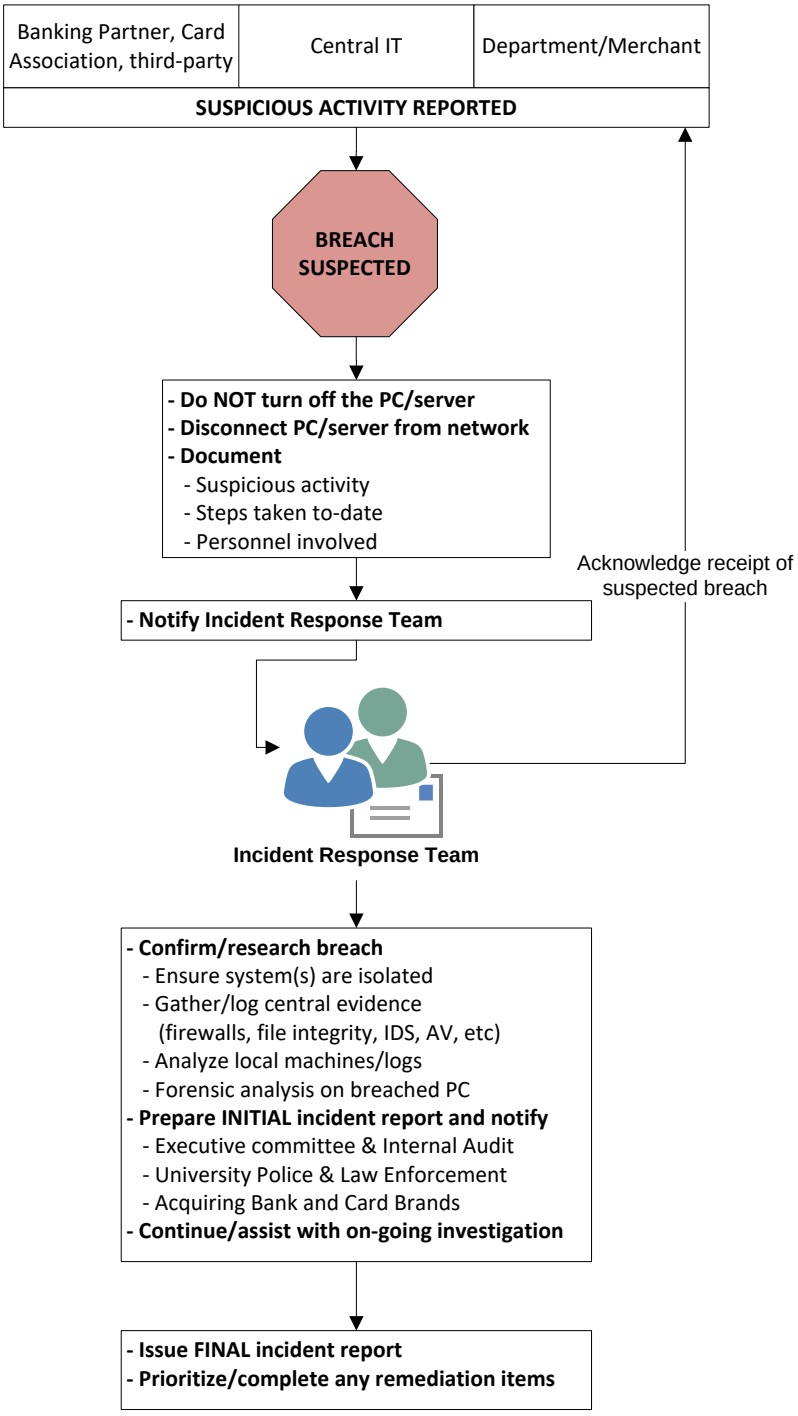
Conclusion, Findings and Recommendations

- What was the basic cause of the incident?
- What could have prevented this?
- Impact (e.g., degraded performance, downtime, data privacy breach/integrity loss)
- Business criticality (revenue producing, business critical, low)
  estimated cost (impact + business criticality)
- What prevents the incident from reoccurring?
- What additional actions or research need to happen?

_____ _____

Name: Title:

Appendix C – Example Flow Chart for Suspected Breach



Appendix D – Payment Card Incident Log for Merchants

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

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

1. Contact the Incident Response Team by sending an email documenting the incident to security@gvsu.edu.

2. The Incident Response Team will immediately coordinate a response and reply to this initial notification to confirm they are aware of the incident.

3. If the incident involves a workstation or POS machine used to process payment cards:
    a. Do NOT turn off the device.
    b. Remove network cable or contact Information Technology for additional help.

4. Document any steps taken until the Incident Response Team has arrived. Include the date, time, person/persons involved, and action taken for each step.

5. Assist the Incident Response Team as they investigate the incident.

6. If an incident of unauthorized access is confirmed and cardholder data was potentially compromised, the Incident Response Team will notify the PCI Committee Chairperson.