Credit Card Security Incident Response Plan
Payment Card Industry
Data Security Standard (PCI DSS)
Eastern Kentucky University

Contents

Revision History

Version	Change	Date
1.1	Added Revision History	4/7/2020
1.2	Spring 2020 Additions	5/31/2020
1.3	Changed Footprints to Asana for incident tracking	7/1/2024

1. 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 the roles and responsibilities, handling of, reporting/notification, and communication requirements for incidence response plan at Eastern Kentucky University (EKU).

For the purpose of this Plan, an incident is an event in which cardholder data in any format—physical or digital media (**truncated card numbers are not card holder data**)—has been or is believed to be lost, stolen, or accessed by an individual unauthorized to do so.

This Incident Response Plan is dependent upon the merchant and/or cardholder data environment (CDE) Resource and Data Owners being compliant with the Payment Card Industry Data Security Standard (PCI DSS) and all applicable EKU IT Security policies.

This Incident Response Plan will be reviewed and tested annually by the PCI Response Team to account for changes to/updates in the environment and/or industry trends.

2. Scope

The PCI DSS Incident Response Plan applies to all Eastern Kentucky University owned merchants.

3. Authority

PCI Response Team

The Eastern Kentucky University Computer Emergency Response Team (ECERT) is listed in EKU Policy 11.2.3. The ECERT team will determine who needs to be brought into conversations to gather all needed information.

4. Incident Response Roles and Responsibilities

A. Merchant/Business Unit

- Report a known or suspected data breach or compromise of a system to the IT Service Desk and ask to speak with someone in IT Security or the CIO.
- Do not access or alter a suspected or confirmed compromised system.
- Do not turn off the suspected or confirmed compromised systems.
- Unplug only the network cable from the system to isolate a suspected or confirmed compromised system.

B. University Counsel

- The University Counsel Office will be responsible for determining any obligation to the University to report a breach to the State of Kentucky for compliance with the State of Kentucky Data Breach Laws.

C. Information Technology

- Monitors cardholder data environment systems for suspicious activity.
- If an unauthorized wireless access point is found connected to the cardholder data environment, it should be unplugged from the network immediately, but left on. Notify IT Networking and/or IT Security.
- Coordinates incident response and notification efforts.
- Documents actions taken, individuals involved, and dates.
- Maintains the PCI DSS Incident Response Plan
- Follows the EKU Information Security Incident Response Policy once given appropriate notification from the Acquiring Bank.
- Provides PFI Reports to all appropriate parties.

D. The EKU PCI Incident Response Team

- The EKU PCI Incident Response Team will consist of, at a minimum, those listed on the ECERT in University Policy 11.2.3. The team can bring others into discussions as necessary.
- Determine whether breach notification to the card brands and/or the card holders is required or warranted and will approve and direct any notification and/or reporting required by the responsible department.

E. Student Accounting Office

- Initiates and maintains contact with the acquiring bank.
- Coordinates communications with the acquiring bank and EKU Information Technology.
- Determines the official line of notification.

F. Acquiring Bank

- Assess the information supplied by the Student Accounting Office.
- Determines if a Payment Card Industry Forensic Investigator must be called in.

G. Payment Card Industry Forensic Investigator

- Initiates and performs all aspects of the forensic investigation.
- Does investigation report in a secure and timely manner.

5. Incident Response Plan (IRP)

A. Incident Discovery

Anytime an employee reasonably believes University customer credit card information may be at risk, the employee should report it in accordance with the established policies and/or procedures of the Merchant/Business Unit where the potential risk is identified. The follow are examples of incidents or events or observations that should be reported.

- The loss or theft of any form of media or hardware used as a point of interaction with credit card data. (Thefts should also be reported to the proper law enforcement agency at the time of the incident, and the Merchant and/or Business Unit must maintain a record of the report in accordance with the University record retention policies.)
- Any signs of tampering with hardware used as a point of interaction with credit card data.
- Any observed activity outside that of normal operation; for example, a login or credit card transaction activity occurring after normal business hours.
- Virus or malware detection on any system that stores, transmits, processes, or accesses credit card data.
- Any system event or alert indicating a possible compromise or unauthorized access to a system that stores, transmits, processes, or access credit card data.
- Any violation of PCI standards.

In the event of a suspected or confirmed incident (Symptoms of Data Breaches in APPENDIX A):

1. Do NOT touch or compromise any possible evidence. Do not shut off any computer or POS system.
2. Unplug only the network cable from the system to isolate the system.
3. Contact the PCI Response Team. Make verbal contact with a team member, DO NOT LEAVE A VOICE MAIL. During business hours contact the IT Service Desk and ask to speak with someone in IT Security or the CIO. After hours, contact Public Safety at their non-emergency number and ask for the IT Person on call.
    a. Overview of incident, including date, time, and the 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

4. The PCI Response Team will immediately coordinate a response and reply to this initial notification/communication to confirm they are aware of the incident.
5. If the incident involves a payment station (PC use to process credit cards):
    a. Do NOT turn off the PC
    b. Disconnect the network cable from 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.
6. Document any steps taken until the PCI Response Team has arrived, include the date, time, person/persons involved, and action taken for each step.
7. Assist the PCI Response Team as they investigate the incident.

B. Event Assessment

A member of the EKU IT Security Team will open an Asana task to document when the incident is reported, by whom, and what is being reported. The PCI Response Team will start a PCI Incident Report utilizing the PCI Incident Report Template (see #3 in section A, above). No other information related to the incident, or its investigation, will be included in Asana due to privacy concerns. All documentation related to the incident must be maintained on secure University resources.

In response to the system compromise, the PCI Response Team 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 Response Team, depending on the nature of the data compromise, must notify the appropriate organizations that may include the following:
    a. EKU VP for Finance and Chief Information Officer
    b. EKU Acquiring Bank(s), the Acquiring Bank will be responsible for communicating with card brands (VISA, MasterCard)
        -Card Association Breach Response Plans (APPENDIX B)

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

   A reported incident will be assessed by the PCI Response Team with the reporting Merchant/Business Unit. The PCI Response Team will make a determination regarding whether the event put cardholder data at risk and should be elevated to a possible breach.

   An event involving loss or theft of media containing full card numbers (whether encrypted or not) will automatically be elevated to possible breach status.

   If the PCI Response Team determines that no cardholder data was put at risk by the reported incident, the PCI Response Team will close the incident, but it may also require the Business Unit or Merchant involved to put corrective measures in place. If the PCI Response Team determines that cardholder data was put at risk by the reported incident, the PCI Response Team will elevate the incident to a possible breach status.

C. Breach Assessment

Once an incident has been elevated, isolation, or containment processes for the affected cardholder data environment will be determined and implemented by the Merchant/Business Unit responsible for the resource, and the PCI Response Team will begin a formal investigation.

After the investigation, the PCI Response Team will make a probability of breach determination.

The PCI Response Team will determine what the University's reporting obligations are and will make a reporting decision regarding notice to the merchant provider, card brands, and/or cardholders.

The PCI Response Team, working with the Merchant/Business unit, will identify the potential quantity of affected card numbers.

D. Reporting

All notices and reports to the State, payment card processor, global payment brands, and acquiring banks; law enforcement, and cardholders, will be submitted to the PCI Response Team for review and approval prior to distribution in accordance with University Policy 11.2.3.

1. The campus accounting office will make any necessary reports to the payment card processor, global payment brands, and acquiring banks, as required by each entity.

2. The Merchant/Business Unit affected will perform any needed internal, law enforcement, and cardholder breach notifications as directed by the PCI Incident Response Team.

E. Post Breach Determination Activities

The Merchant/Business Unit affected will perform and document a root cause remediation. The PCI Response Team may help with this process if needed.

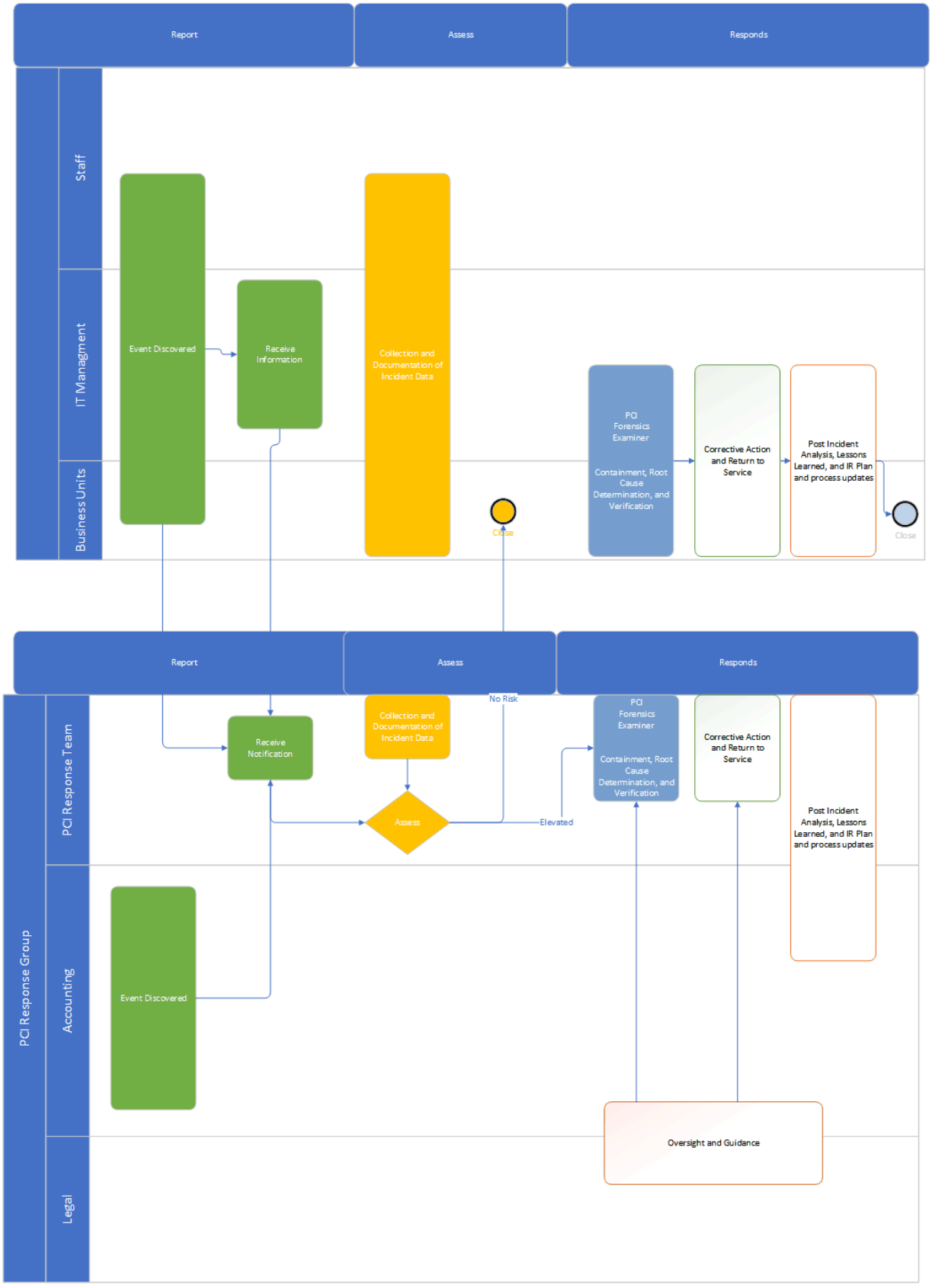
The PCI Response Team will conduct a recovery and compliance verification of the Merchant/Business Unit prior to returning the area's affected resource to service.

The PCI Response Team will conduct a post incident meeting to review the incident and determine that, if any, corrective adjustments to the cardholder data environment (CDE) and related policies and procedures are needed to help prevent a similar incident, as well as whether an adjustment to the Incident Response Plan itself is needed.

If adjustments are needed, the PCI Response Team will establish a corrective action plan and assign it to the entity responsible for the area needing adjustment.

The PCI Response Team will document the assessment and resolution in Asana and will close the incident.

PCI Incident Workflow



6. Definitions

- **Acquiring Bank** – A bank or financial institution that process cred or debit card payments on behalf of a merchant or provides merchant accounts.
- **Business Unit** – 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.
- **Business Department Responsible Person** – An individual within the department who has primary authority and responsibility within that department for credit card transactions.
- **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.
- **Cardholder Name** – The name of the Cardholder to whom the card has been issued.
- **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 the payment card used to verify card- not-present transactions.
- **Disposal** – CHD must be disposed of in a certain manner that renders all data unrecoverable. 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 DoD 5220.22-M standard. The approved disposal methods are: cross-cut shredding, incineration, approved shredding or disposal service.
- **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.
- **Incident**—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.
- **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.
- **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, and JCB
- **PCI Forensic Investigator (PFI)** - Companies, organizations or other legal entities that are in compliance with all PFI Company requirements or applicable terms of PFI Program remediation and have been qualified as PFI Companies by PCI SSC for purposes of performing PFI Investigations. Only PFI Companies and PFI Employees qualified by an Approving Organization and who are in PFI Good Standing are permitted to perform PFI

Investigations, and then only in the specific PFI Regions for which they have been qualified by PCI SSC.

- **PIN/PIN block** – Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.
- **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.
- **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.
- **Service Code** – The service code that permits where the card is used and for what.
- **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 devices and wired devices on the network.

APPENDIX A: Symptoms of Data Breaches

Detecting data 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 system files or changes in system files
- Unexplained modifications or deletion of data
- Denial of service or inability of one or more users to log in to an account
- Systems 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

APPENDIX B: Card Association Breach Response Plans

Visa – Responding to a Breach
Follow the steps set forth in the resource:
https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

Mastercard – Account Data Compromise Event Management Best Practices
Follow information in this resource:
https://globalrisk.mastercard.com/wp-content/uploads/2019/08/ADC-Best-Practice-Manual.pdf