MSU Information Security Incident Response Plan

PURPOSE

Information security incidents are receiving enormous attention with the increasing number of leaks of protected information and cases of identity theft. Major universities are in a unique position with large amounts of educational, medical, financial, and other critical information. MSU is subject to numerous federal and state laws and regulations regarding the protection of data. The risk associated with an information security breach or significant information loss requires that the institution respond to such incidents in a timely and decisive manner.

The effective resolution of computer security incidents such as virus or spyware infected computers, denial of service attacks, unauthorized access or inappropriate usage of resources are all critical to the usability of the campus information technology infrastructure. The breach of protected information is fundamentally different and more troublesome. The university risks its reputation as well as possible financial penalties, while the consequences of identity theft to an individual can linger for years.

Incidents that involve threats to personal safety, physical property or other illegal activities should be immediately reported to the University Police department.

DEFINITIONS

Protected Information:

1. Per **Mississippi Code Annotated § 75-24-29:**
    - Breach of security means the unauthorized acquisition of electronic files, media, databases or computerized data containing personal information that has not been secured via encryption or any other method or technology that renders the personal information unreadable or unusable.
    - "Personal information" is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements:
        i. Social security number;
        ii. Driver's license number or state identification card number; or
        iii. An account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account; "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media;
    - Requires the University to disclose any breach of security to all affected individuals without unreasonable delay.

2. The Family Educational Rights and Privacy Act of 1974, (FERPA) commonly referred to as the Buckley Amendment, protects the rights of students by controlling the creation, maintenance, and access of educational records. It guarantees students' access to their academic records while prohibiting unauthorized access by others.

3. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes significant privacy requirements by creating national standards to protect personal health information.
4. The Gramm-Leach-Bliley Act (GLBA), while targeted at financial institutions, requires universities to maintain an information security program for the protection of financial information.
5. The Payment Card Industry (PCI) Data Security Requirements apply to all members, merchants, and service providers that capture, store, process, or transmit credit card data.

Information Security Incident: MSU becomes aware that protected information has been compromised or is at risk. In most cases this will be electronic information but includes information in all forms.

Incident Classification: The following table will serve as a guide in classifying incidents and their required response.

Classification	Characteristics	Examples
Low Priority	- annoyance - inconvenience for an individual user	- Spyware - minimal impact virus
High Priority	- compromised individual access - results of internal risk analysis cause concern - multiple systems exhibit similar problem	- user account hacked - unpatched server at risk due to new exploit - new virus starts to spread on campus
Emergency	- compromised critical system - protected information exposed on the internet - external report of breach	- Banner hacked - SSN data exposed - Credit card account numbers captured (PCI) - media or user report of ongoing incident to ITS

PROCEDURE

Any MSU employee who becomes aware of an information security incident shall immediately report the incident. The University may become aware of suspected security incidents in a number of ways:

- An intrusion detection sensor reports suspicious network traffic
- Log files show a suspicious pattern of activity
- Internal or external user report
- Media report
- Police report
- Internal Audit

Once Information Technology Services (ITS) is made aware of a potential incident, the Security and Compliance Officer or designee will direct an initial investigation to collect and understand the basic facts of the incident. Based upon the investigation the incident will be classified and the following actions taken:

Low Priority Incidents will typically be resolved between ITS and the affected user/department and should require no further action.

High Priority Incidents will require interaction between ITS and the affected user/department and may require the involvement of other campus units such as audit, legal, financial, etc. Resolution of these incidents may involve changes to systems or procedures as well as user awareness training. Multiple incidents may result in the user/department being referred to the Information Technology Council (ITC).

Emergency Incidents demand an institutional response and will bring to bear campus resources and leadership to manage the overall response, recovery, and communication to stakeholders. Importantly, lessons learned will be used to improve the overall information security environment and mitigate the risk of future incidents.

1. Notification: Immediately upon an incident being classified as an emergency, the following individuals will be notified:
    - Chief Information Officer/Chair of the ITC
    - Unit head in which the incident occurred
    - Unit head's administrative chain-of-command up to and including the Vice President
    - Unit's IT security contact (if applicable)
    - Chief Communications Officer, Director of Internal Audit and General Counsel
    - Other university offices as appropriate

2. Response and Recovery: The ITS Security and Compliance Officer will take immediate action to secure any information or system which was breached. The preservation of evidence including relevant log entries and system backups will enable complete investigation and possible prosecution. Recovery and return to normal operations in a secure manner is the principal priority. PCI breaches have additional and specific card industry requirements that are documented in Appendix D.

3. Information Technology Council: The Chair of the ITC is responsible for overseeing the institutional response and has the authority to take immediate action or consult with the ITC as appropriate. The unit in which the data breach occurred will prepare a report to be submitted within one week to the Chair of the ITC. This report should follow the template provided in Appendix B. PCI breaches use Appendix E template. The ITC will review the report and recommend any additional actions that may be needed, including possible disciplinary action.

4. Communication: If it is determined that public notification of the incident is required, Office of Public Affairs will lead the development of a communications plan. Emphasis will be on accuracy and timeliness and may include press releases, response to media reports, notification letters and a website with ongoing information. See Appendix C for Educause Data Notification Template resources and components of a sample notification letter. Without undue delay notice will be given to affected individuals whose personal information has been breached subject to the provisions of Miss. Code § 75-24-29.

5. Forensic Analysis: A forensic analysis of the incident will be done internally with support from appropriate ITS and other university units such as the Center for Computer

Security Research. Engaging a company for external forensic investigation may be preferred or required in some circumstances such as Payment Card Industry incidents.

6. Post Mortem: The ITC will review all aspects of the incident and document lessons learned. The committee will prepare a final report to chronicle the incident and make recommendations to strengthen the University's information security posture.

Appendix A – Information Technology Services Contact Information

Department/User	Contact Information
ITS Helpdesk	Phone: 662-325-0631 Toll-Free: 888-398-6394 Email: helpdesk@msstate.edu Web: helpdesk.msstate.edu
ITS Security and Compliance Officer	Phone: 662-325-3709 Email: security@its.msstate.edu
Chief Information Officer	Phone: 662-325-9311 Email:office@its.mstate.edu

Appendix B – Emergency Incident Report Template

Departmental Security Contact Information:

Name:
Department:
Email:
Phone:
Location/Site Involved (Building/Room/Campus):

- Protected Information Disclosed (HIPPA,GLBA,PCI,FERPA)
- Unauthorized Access (System Hacked/Intrusion)
- MSU Website Defaced
- Malicious Virus or Worm
- Misuse of Computer System(s)
- Other

Classify Incident as above.

Incident Description: Please provide as much information about the incident as possible.

Date and Time of Discovery:

Computer Hardware and Operating System:

How was the incident detected?

How long was the compromise in place?

What measures were in place to protect the information or system? What failed? Why?

What employees are assigned to the security of the system or information? Any shared administration with other departments?

What was done in response to the incident? Please provide as much information about incident response as possible.

For example:

- Log files maintained
- Forensics investigation
- Physically secured system
- System restored from backup
- Patches/virus updates and system verified
- Exposed information removed from web and external search engine(s) cache cleared

Appendix C - Educause Data Notification Template

Template Location

https://library.educause.edu/resources/2013/1/data-incident-notification-toolkit

https://spaces.internet2.edu/display/2014infosecurityguide/Data+Incident+Notification+Toolkit

https://spaces.internet2.edu/display/2014infosecurityguide/Incident+Checklist

Appendix D - Credit Card Security Incident Response Plan
Payment Card Industry
Data Security Standard (PCI DSS)
PCI DSS Version 3.1

Purpose

The Payment Card Security Incident Response Plan supplements the University Incident Response Plan. PCI compliance requires the additional elements that are defined in this appendix.

To address credit cardholder security, the major card brands (Visa, MasterCard, Discover, American Express and JCB) 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 {institution name}.

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.

Authority

Security Incident Response Team

The Mississippi State University credit card Response Team is comprised of a cross-section of the campus. See below for names and contact information.

Mississippi State University Credit Card Security Incident Response Team
Communication for the Response Team can be sent to **creditcard@controller.msstate.edu**.

Name	**Department/Title**	**Role**	**Telephone**	**Email**
Edelblute, Kevin	Office of the Controller/Treasurer / Controller & Treasurer	PCI Committee Chairperson	(662)-325-2302	kedelblute@controller.msstate.edu

Name	Department/Title	Role	Telephone	Email
Ritter, Tom	Office of the CIO/Security and Compliance Officer	PCI Technical Lead	(662) 325-3709	ritter@its.msstate.edu
Gentry, Betty	Office of the Controller/ Director -Treasury Services	PCI Banking Liaison	(662)-325-1931	bgentry@controller.msstate.edu
Johnson, Terri	Office of the Controller /Treasury Services Manager	PCI Business Office Support	(662)-325-5940	tjohnson@controller.msstate.edu
Barnes, Oscar	Enterprise Information Systems/Associate Director, DIS	PCI Technical Support	(662) 325-0756	obarnes@its.msstate.edu

Procedures

PCI 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 Mississippi State University's PCI Incident Response Plan.

The Mississippi State University security incident response plan is summarized as follows:

1. All incidents must be reported to the Response Team.
2. The Response Team will confirm receipt of the incident notification.
3. The Response Team will investigate the incident and assist the compromised department in limiting the exposure of cardholder data.
4. 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.
5. 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. Contact the Response Team by sending an email documenting the incident to…
   pci.security@msstate.edu.
2. The Response Team will immediately coordinate a response and reply to this initial notification/communication to confirm they are aware of the incident.
3. 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.

4. Document any steps taken until the Response Team has arrived. Include the date, time, person/persons involved and action taken for each step.
5. Assist the Response Team as they investigate the incident.

Incident Response Team Procedures

The Mississippi State University 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, will implement their incident response plan to assist and augment departments' response plans.

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

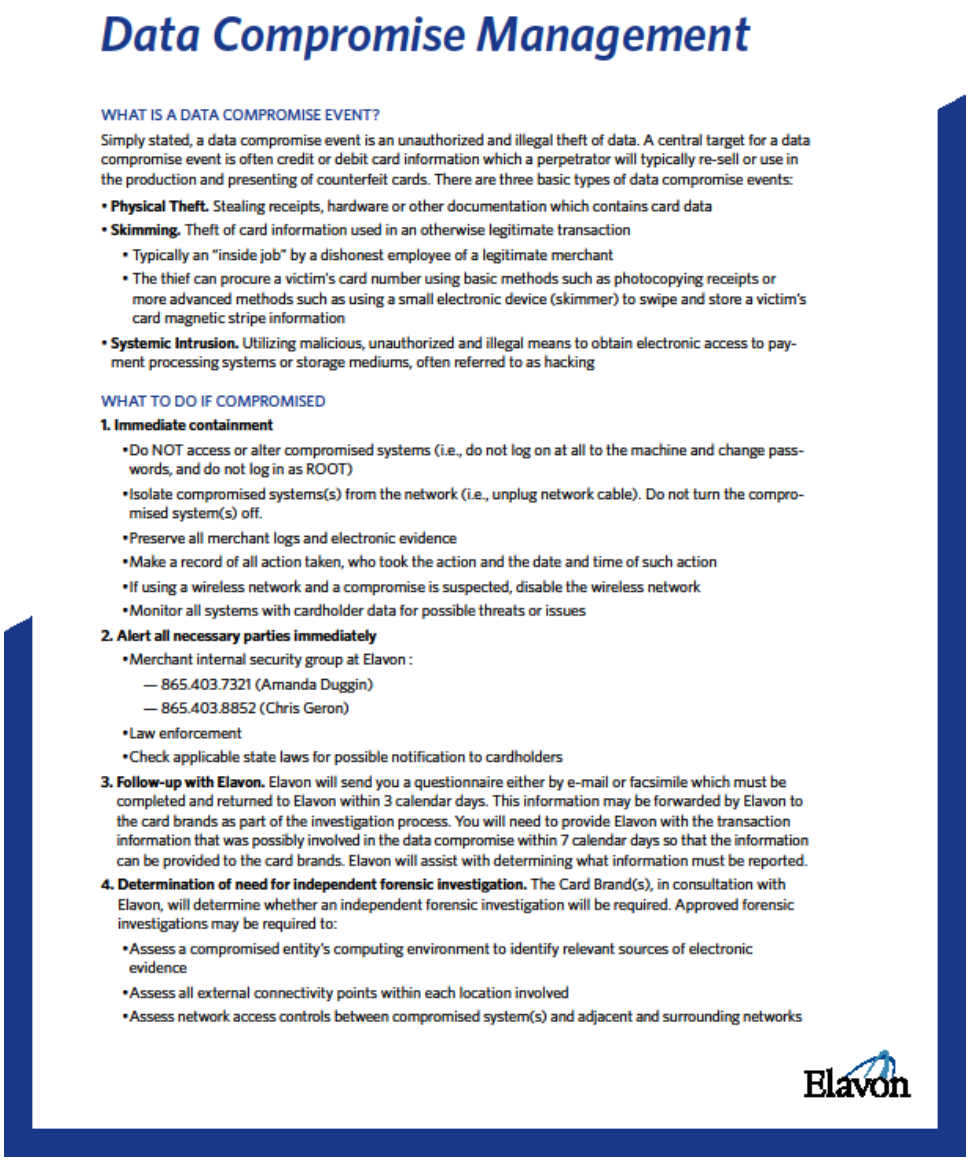
1. Ensure compromised system is isolated on/from the network.
2. Gather, review and analyze all centrally maintained system, firewall, file integrity and intrusion detection/protection system logs and alerts.
3. Assist department in analysis of locally maintained system and other logs, as needed.
4. 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 Mississippi State University staff:
    a. Chief Financial Officer and the Chief Information Officer
    b. Internal Audit group
    c. Mississippi State University 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.

Elavon – The merchant internal security group at Elavon provides their Data Compromise Management documentation below embedded as a PDF: (Double Click to open)



Data Compromise Management

WHAT IS A DATA COMPROMISE EVENT?

Simply stated, a data compromise event is an unauthorized and illegal theft of data. A central target for a data compromise event is often credit or debit card information which a perpetrator will typically re-sell or use in the production and presenting of counterfeit cards. There are three basic types of data compromise events:

- **Physical Theft.** Stealing receipts, hardware or other documentation which contains card data
- **Skimming.** Theft of card information used in an otherwise legitimate transaction
  - Typically an "inside job" by a dishonest employee of a legitimate merchant
  - The thief can procure a victim's card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store a victim's card magnetic stripe information
- **Systemic Intrusion.** Utilizing malicious, unauthorized and illegal means to obtain electronic access to payment processing systems or storage mediums, often referred to as hacking

WHAT TO DO IF COMPROMISED

1. Immediate containment

- Do NOT access or alter compromised systems (i.e., do not log on at all to the machine and change passwords, and do not log in as ROOT)
- Isolate compromised systems(s) from the network (i.e., unplug network cable). Do not turn the compromised system(s) off.
- Preserve all merchant logs and electronic evidence
- Make a record of all action taken, who took the action and the date and time of such action
- If using a wireless network and a compromise is suspected, disable the wireless network
- Monitor all systems with cardholder data for possible threats or issues

2. Alert all necessary parties immediately

- Merchant internal security group at Elavon :
  - 865.403.7321 (Amanda Duggin)
  - 865.403.8852 (Chris Geron)
- Law enforcement
- Check applicable state laws for possible notification to cardholders

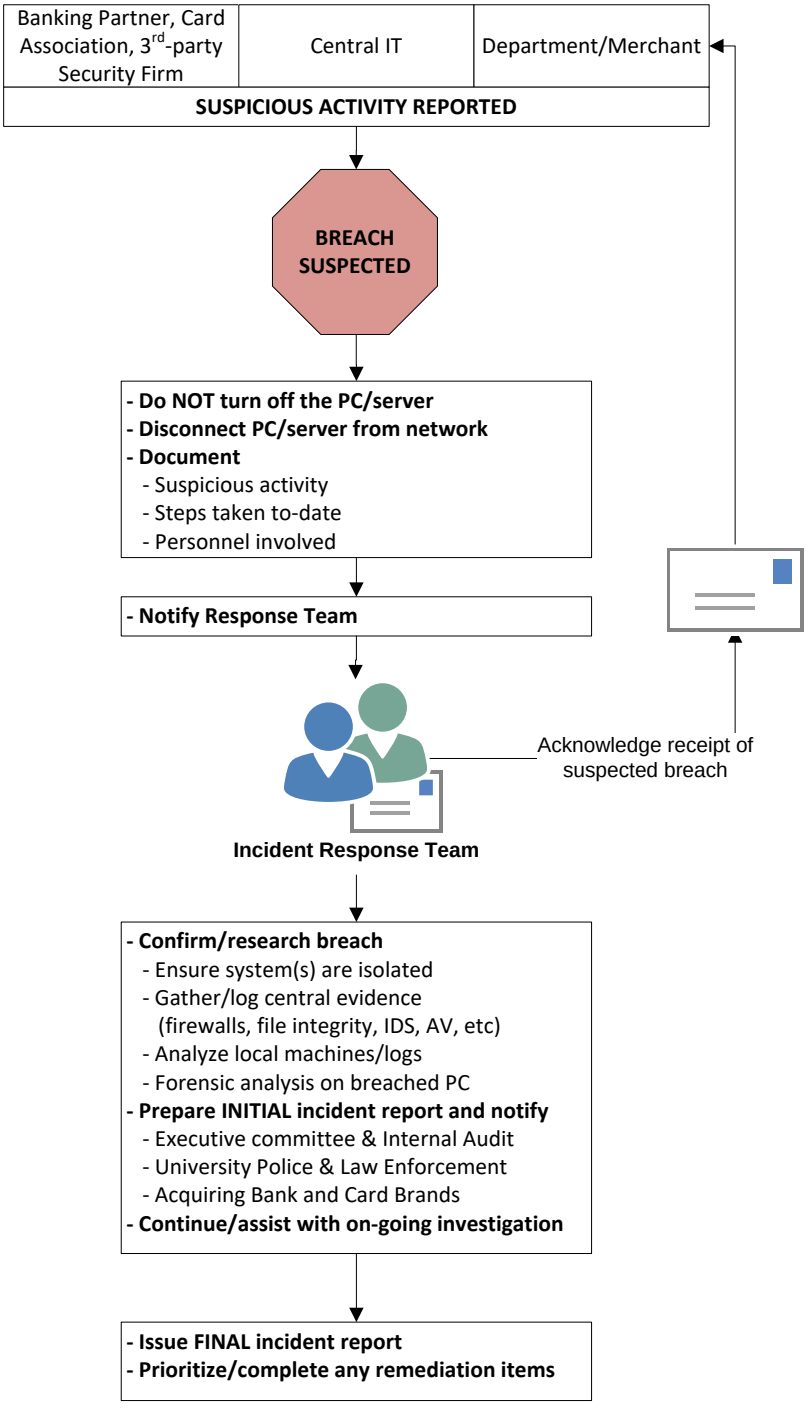
3. Follow-up with Elavon. Elavon will send you a questionnaire either by e-mail or facsimile which must be completed and returned to Elavon within 3 calendar days. This information may be forwarded by Elavon to the card brands as part of the investigation process. You will need to provide Elavon with the transaction information that was possibly involved in the data compromise within 7 calendar days so that the information can be provided to the card brands. Elavon will assist with determining what information must be reported.

4. Determination of need for independent forensic investigation. The Card Brand(s), in consultation with Elavon, will determine whether an independent forensic investigation will be required. Approved forensic investigations may be required to:

- Assess a compromised entity's computing environment to identify relevant sources of electronic evidence
- Assess all external connectivity points within each location involved
- Assess network access controls between compromised system(s) and adjacent and surrounding networks

Elavon

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://www209.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Service_Provider_US.pdf
- American Express Data Security Operating Policy – U.S.
  https://icm.aexp-static.com//Internet/NGMS/US_en/Images/DSOP_Merchant_US_Apr15.pdf

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 Policy). 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.

Appendix E. 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.

2. Contact the Response Team by sending an email documenting the incident to pci.security@msstate.edu.

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

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

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 Mississippi State University 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