MONTGOMERY COLLEGE

Office of Information Technology

IT Process

Credit Card Account Security Incident Response

Process:	IT16001A
Original Effective Date:	09/15/2015
Last Revised:	10/11/2019
Last Reviewed:	03/10/2021
Next Scheduled Review Date:	04/01/2022
Version No.:	2.1
Administrative Owner:	Information Security & Privacy Director

Purpose

The major card brands (Visa, MasterCard, Discover, American Express and JCB) have jointly established the Payment Card Industry (PCI) Security Standards Council ("Council") for the purpose of developing and implementing security standards for credit card account data protection. One of the Council's specific responsibilities is to administer the Payment Card Industry Data Security Standard (PCI DSS) that provide detailed requirements for safeguarding credit card account data. Among the PCI DSS requirements is the requirement for each merchant company such as Montgomery College ("College") to document an incident response plan for the purposes of handling data security incidents involving credit card account data.

The purpose of this plan is to provide the foundation for an appropriate response to incidents that threaten the confidentiality, integrity, and availability of College credit card account data and system processing. The document provides specific direction that must be followed in the event of a credit card account data security incident. This direction is in addition to direction noted in the *IT Standard Information Security Incident Response and Management IT160001*. This incident response plan will be reviewed annually and revised as appropriate.

Scope

This process applies to the handling of any security incident involving credit card account data at Montgomery College whether taken via College technology or by a Third Party Vendor working on behalf of a College Merchant Unit.

Definitions

Term	Definition
College Merchant Unit	Administrative office or academic department approved by the Office of Business Services to process credit cards in payment for products or services.
Credit Card Account Security Incident	A credit card account security incident is defined as any event that results in the loss of confidentiality, availability, or integrity (unauthorized modification) of a credit card processing system, technology asset or data. Examples of possible events include but are not limited to the following: • Unauthorized access to a credit card processing system or data. • Theft or damage to physical credit card processing device. • Denial of service attack involving a credit card processing system, technology or data. • Misuse of a credit card processing system by College employee or student. • Malicious software infection of a credit card processing system.

	• Theft or accidental disclosure of credit card data. • Report of unusual system behavior involving credit card processing system or data.
Payment Card Industry (PCI)	The Payment Card Industry is MasterCard, Visa, American Express, Discover and JCB.
PCI Incident Response Team (IRT)	The PCI Incident Response Team ("IRT") is a team of personnel who are responsible for the administration of an incident response to any event that may threaten College credit card account data. This includes the procedural management, approval, and coordination of: • Incident confirmation • Forensic investigations • Internal and external communications • Contact with law enforcement, banking, regulatory, and credit card associations • Evidence preservation • Incident documentation and reporting • Post incident evaluation.
Third Party Vendor	A vendor contracted by a College Merchant Unit to take credit card payments for goods or services on behalf of a College Merchant Unit.

PROCESS

A. General

1. The following College roles or designated representatives are members of the IRT and as required will support an IRT response to a security incident involving credit card account data. See *Appendix A* for a current listing of College personnel in these roles.

   - IT Security Manager serving as the IRT Coordinator
   - IT Policy Administrator (ITPA)
   - Vice President of Instructional and Information Technology / CIO
   - General Counsel
   - Associate Sr. Vice President for Administrative and Fiscal Services
   - Vice President of Finance / Chief Financial Officer (CFO)
   - Director of Accounts Receivable / Treasurer
   - Director of Infrastructure and Engineering Services/ Chief Technical Officer (CTO)
   - Information Security and Privacy Director
   - Senior Administrator from impacted area
   - Vice President of Communications
   - Chief Compliance Officer

2. The following personnel or functions, and others not listed, may be added to the IRT as appropriate.

   - Chief Government Relations Officer
   - Office of Information Technology personnel

- Office of Human Resources and Strategic Talent Management
- Office of Safety and Security and other law enforcement, including FBI, as appropriate
- Records Management
- Internal Audit
- Other personnel, as appropriate

3. This incident response plan will be reviewed and tested annually.

B. Process

The following process is to be followed by the respective groups below in response to a suspected or confirmed Credit Card Account Security Incident.

College Merchant Unit

In the event that a College Merchant Unit either suspects or confirms that a security incident has occurred, the unit should:

1. Contact the IT Service Desk (ITSD) immediately to report the incident. The ITSD will contact the IRT to initiate an incident response.
2. If the incident involves a College TouchNet or Vendini payment station connected to the Internet (PC or server used to process credit cards):
   a. Do NOT turn off the PC.
   b. If possible at all, disconnect the network cable connecting the PC to the network jack. (This is an important step in containing impact to the College network) or,
   c. If you cannot disconnect the network cable, stop further use of the PC, server or any point of sales device connected to the PC.
3. If the incident involves a College analog payment device connected by telephone line to the College's acquirer stop further use of the POS device.
4. If the incident involves a College Third Party Vendor, the Third Party Vendor will take responsibility for managing the incident response according to their procedures. The College merchant will be responsible for updating IRT personnel on the status of the vendor's incident response and of any actions that might be required of the College.
5. Document any observations made about activities occurring prior/during the suspected/confirmed security incident.
6. Document any actions taken until members of the IRT have arrived. Include the date, time, person/persons involved and action taken for each step.
7. Assist IRT members as they investigate the incident.
8. Work with the IRT and review the unit's business continuity plan in light of the incident to determine actions to be taken relative to continued merchant operations.

OIT and ITSD

In response to a suspected or confirmed credit card security incident reported to the ITSD, the ITSD will contact the ITSD "PCI Incident Response Team" group to initiate an incident response. If a suspected incident is reported to OIT through any other channel, the incident must be reported to the ITSD in order to support this plan. Once an incident is reported to the ITSD, the ITSD will support the IRT as needed until the incident is closed.

Incident Response Team

Upon contact from the ITSD, the ITPA will initiate an incident response. The ITPA will initially work with designated IRT members to assess and confirm the incident. The IRT or assigned College personnel working on behalf of the IRT will:

1. Work with the College Merchant Unit to assess and confirm that a security incident did occur.

2. Notify appropriate College leadership that a potential security incident is being investigated.
3. If confirmed or as appropriate:
   a. Secure all technology resources involved in the suspected incident. Ensure that any compromised system is isolated on/from the network.
   b. Contact and work with the College's merchant bank, payment application third party vendor, partner credit card association, and acquirer as outlined in *Appendix B* if credit card account cardholder data is involved and may have been breached. The College's merchant bank and partner credit card association and acquirer will provide specific direction in all aspects of the investigation and client outreach.
   c. Gather, review and analyze all system logs. Logs may include device logs, local system logs, firewall, and file integrity and intrusion detection/protection system logs.
   d. Determine any impact to the unit's related business applications and identify the need and process required to backup or recover data. Work with third party vendor as necessary.
   e. Conduct a forensic analysis of any compromised system, as appropriate.
   f. Contact and work with law enforcement agencies as appropriate.
   g. Make forensic and log analysis available to appropriate law enforcement/card industry security personnel.
   h. Assist law enforcement/credit card association security personnel in investigative process.
   i. Develop and deliver a client notification strategy according to Federal, State and local regulations, merchant bank and partner credit card association and acquirer direction as noted in Section G: Notification Process.
4. Prepare an incident report.
5. In the event that the incident is within the operations of a College Third Party Vendor, the IRT will continue contact with the College Merchant Unit and vendor liaison and proceed as appropriate.

C. Forensic Investigation / Analysis

A forensic analysis is conducted to help identify, preserve, and recover facts related to an incident. If it is determined that a forensic analysis should be conducted, the IT Security manager will coordinate/conduct the analysis. Any analysis should be conducted in cooperation with law enforcement and credit card association security personnel as appropriate.

D. Notification Process

1. The IRT will draft timely notifications to cardholders impacted by a confirmed Credit Card Account Security Incident. This may be in the form of a letter, website statement, press release, or other appropriate notification. Delivery of the notice will be in a manner that will ensure that the majority of those impacted will receive it. Content and delivery may also be regulated by current Federal and State of Maryland laws as well as banking and credit card association direction.

2. The following components may be considered or addressed in the notification. The letter or statement must be written in plain language. Do not disclose anything that might hamper the investigation or give additional information to those who would do harm.

   a. What happened?
   b. When did the breach occur and/or when was it detected?
   c. How was it detected?
   d. What data was potentially compromised?
   e. How much data was compromised?
   f. Whose data was compromised, e.g., students, staff, faculty, etc.?
   g. Why are you being notified?
   h. What steps were taken, e.g., machine off the net, law enforcement notified (local, FBI), credit card associations notified (for cases where contact information is needed

about cardholders), etc.

i. Is any data known to be fraudulently used or is notification precautionary?
j. Was the notification delayed as a result of a law enforcement investigation?
k. What steps should individuals take? Example: Place a fraud alert with credit bureaus, contact credit card association, close accounts, change passwords, etc.
l. Closing statement apologizing for inconvenience or statement of commitment to security.
m. Anticipated next steps, if any, e.g., intention to notify if any additional information becomes available.
n. Any provisions to be made by the College for a paid service to monitor credit card activity.
o. Who to contact for additional information including contact name, number, hours of availability, web-site, hotline, e-mail address, phone number, etc.
p. Signature. Who makes the most sense: President or other contact familiar to the individual; consider multiple signatures for different constituent groups.
q. Letterhead. Decide which institutional letterhead to use.

E. Incident Reporting

At the conclusion of an incident, the IRT shall prepare an incident report. The incident report should include a detailed description of the incident, response taken by the IRT, and any recommendations to minimize the likelihood of a repeated incident. The ITPA shall be responsible for distributing the report as appropriate.

F. Business Continuity

In the event of a confirmed Credit Card Account Security Incident, it is possible that credit card processing in impacted units may need to be altered or shut down. Business continuity plans developed by units as part of the Montgomery College Continuity of Operations Plan should be invoked to continue adequate customer service. The plans must take into account the business continuity plan for any third-party vendor or processing host that is involved with the unit's credit card process. Unit management or IRT members will serve as liaisons between the College and the vendors coordinating or overseeing business continuity activity and ensuring that the activity does not interfere with any ongoing incident response or investigation.

G. Lessons Learned and Policy Review

A facilitated Lessons Learned meeting will be scheduled upon final closure of the Credit Card Account Security Incident response. Meeting results will be included in the final incident response report. The meeting will review actions taken to resolve the security incident in order to:

1. Determine if modifications are required to the Montgomery College Credit Card Account Incident Response Plan.
2. Determine if modifications are required to College policies and procedures, IT standards, or unit processes and procedures.
3. Determine if further training is required in OIT, the College Merchant Unit,or another College academic or administrative unit.
4. Determine if modifications are required to College credit card processing technology resources.
5. Determine if modifications are required to a College Third Party Vendor contract.
6. Determine if modifications are required to backup and recovery procedures.
7. Determine if modifications are required to unit business continuity plans.

RELATED DOCUMENTS

- Appendix A: Contact Information for IRT Membership
- Appendix B: Merchant Bank and Credit Card Association Specific Requirements
- IT Standard IT16001, Information Security Incident Response and Management Standard
- Acceptable Use Policy and the accompanying Procedure/Guidelines Statement
- Montgomery College Policy 66002, Confidential Data Management and Security
- Montgomery College Policy 62003, Public Information, Communications, and Marketing

APPROVALS / REVISION HISTORY

DATE	VERSION / REVISION / NOTES	APPROVER
September 15, 2015	Original roll-out of this Credit Card Account Security Incident Response document.	Patrick Feehan, Information Security and Privacy Director/ITPA
October 11, 2019	Revised.	Patrick Feehan, Information Security and Privacy Director/ITPA
March 10, 2021	Reviewed. (Removed reference to no longer in existence creditcardsecurity@montgomerycollege.edu mailbox.)	Tim Neill, IT Security Analyst
March 2021	Decided upon and added review cycle dates.	Nell Feldman / Keith Wilson

Appendix A:
Contact Information for IRT Membership
As of October 2019

IRT Role	***IRT Contact***	***Contact Phone #***	***Contact E-mail***
IT Policy Administrator (ITPA)	Patrick Feehan	240-567-3087	
VP Instructional and IT / CIO	Jane Ellen Miller (interim)	240-567- 9195	
Office of General Counsel	Tim Dietz	240-567-7998	
Associate Sr. VP for Administration & Fiscal Services	Donna Schena	240-567-3085	
VP Finance / CFO	Elizabeth Greaney	240-567-5326	
Manager of Accounts Receivable	Natalie Thompson	240-567-5038	
Chief Technical Officer (CTO)	Anwar Karim	240-567-3212	
IT Privacy and Cybersecurity Compliance Director	Patrick Feehan	240-567-3087	
IT Security Manager	Nell Feldman	240-567-3120	
Senior Administrator from impacted area	As defined by the incident	240-567-TBD	
VP Communications	Ray Gilmer	240-567-7970	
Chief Compliance Officer	Victoria Duggan	240-567-7291	

Appendix B:
Merchant Bank and Credit Card Association
Specific Requirements

The following provides direction to the College’s most current merchant bank, credit card association and credit card acquirer incident response procedures to be included in this incident response plan in the event of a Credit Card Account Security Incident.

PNC Bank:

Follow any direction provided by PNC upon contacting the College directed point of contact.

Elavon:

Follow any direction provided by Elavon upon contacting the College directed point of contact.

If necessary or directed by Elavon or PNC, contact with credit card brands can be made as follows:

MasterCard:

Refer to any direction provided by MasterCard at:

https://www.mastercard.us/en-us/merchants/safety-security/suspect-fraud.html)

Visa:

Refer to any direction provided by Visa at:

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

Discover:

Notify the Discover Merchant Fraud Prevention Department to report a data compromise or cardholder breach at **1-800-347-1111 Authorization Code 10.**

American Express:

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 (U.S. only), or at 1.602.537.3021 (International), or email at EIRP@aexp.com.