B5009 - Cardholder Data Security – Incident Response Procedures

Background

These procedures address any security incidents that involve the unauthorized disclosure or modification of cardholder information (as defined by the Payment Card Industry Data Security Standard (PCI DSS)) – https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

1. Any malicious attempt, either successful or unsuccessful, by an unauthorized party to negatively impact the confidentiality or integrity of cardholder data is within scope of these procedures.

2. All departments that handle cardholder data must be familiar with the Incident Response Procedures and ensure that departmental staff who process credit cards payments as part of their job are aware of the Procedures.

3. Any suspected security incident must be reported immediately as set out below.

4. Financial Services is responsible for reviewing the procedures annually.

Procedures

The primary reporter/discoverer of the incident will:

1. Contain or limit the exposure. Some steps to limit exposure include:
- Stop taking further payments until cleared to do so by Organizational Risk Assessment.
- Contact IT to disconnect the compromised system from the network. Do not alter or access the computer system until IT security has had an opportunity to examine the IT system.
- Lock any paper records in a secure location.

2. The primary reporter/discoverer Template (see below).

3. Contact Financial Services, Organizational Risk Assessment and IT immediately. The primary contacts are:
- Financial Services – Director, Financial Services
- Organizational Risk Assessment - Director, Organizational Risk and Internal Controls
- IT – CIO or Associate Director

4. Wait until Financial Services, in consultation with IT and Organizational Risk Assessment, provide the department with approval to restart payment processing.

Financial Services, Organizational Risk Assessment and IT:

1. In consultation with Organizational Risk Assessment and IT, Financial Services will:
   - Validate and assess the incident:
     - Establish how the compromise occurred
     - Document the type of cardholder data breached (PAN, mag stripe, expiration date, etc.)
     - Identify the source of the compromise
     - Identify the timeframe of the compromise
     - Approximate # of cardholders affected
     - Review the technology environment
     - Confirm that the incident has been contained
   - Keep senior management informed

2. Financial Services will report the incident to the College's acquirer (Moneris), and the applicable card brands (Visa, Mastercard, etc.). Each card brand will have specific processes and requirements to follow.

3. Organizational Risk Assessment will obtain legal advice regarding the requirements for reporting compromises.

4. Financial Services will advise the Director of Communications and Marketing of the incident and engage Communications and Marketing for communications support as required.

5. Financial Services will advise the Privacy Officer of the incident.

6. Once the root cause of the incident has been identified, Financial Services and IT will implement security controls (either physical, procedural, or technical) to prevent future incidents.

7. Financial Services, in consultation with IT and Organizational Risk Assessment, will provide the department (primary reporter) with approval to restart payment processing.

Following two pages: **Incident Assessment Template**. Each department that is involved in credit card processing transactions will complete the contact information in the following template and make these available to all staff that are involved in handling any card holder information. These forms, procedures, and their use should be reviewed at a minimum annually with all staff within each department that handle card holder information.

Incident Assessment Template (page 1 of 2)

Originating Department: ____ Date: ____________________

- Ensure all facts about the incident are properly documented, verified and validated before reporting the incident to Financial Services, Organizational Risk Assessment, and IT.

- Who should initially be informed or notified about the incident within the department?
    - Follow the chain of command within your department before reporting an incident

Primary contact	{Name of Person}	{Contact number}
Alternate contact	{Name of Person}	{Contact number}

- Who should report the incident to Financial Services, Organizational Risk Assessment, and IT?
    - The designated person responsible for contacting these groups should have all the pertinent facts and information about the incident

Primary	{Name of Person}	{Contact number}
Alternate	{Name of Person}	{Contact number}

- When do you contact Campus Security and/or the Police?
    - You may initially contact Campus Security and/or the police if the incident involves an imminent danger or physical threat

Langara Security	For Langara Security “emergencies”	• Internal Phone: 4444 • External Phone: 604.374.2373
Vancouver Police	Emergency	• Internal Phone: 9 911 • External Phone: 911

- Business Recovery and Continuity Procedures – Physical input devices

o POS/PIN pad	o Discontinue the use of the POS device (PIN pad/parking machine) and disconnect from network or telephone line – Contact IT
o Electronic application systems	o Where possible, immediately discontinue the use of the affected application system

- Any contact with the Acquirer/Card Companies (regarding an incident) is coordinated through the Finance Department and Organizational Risk Assessment and not by the Department or Merchant

- As the Senior Administrator of this department, I attest that these procedures have been shared and reviewed annually with all staff in this department involved in handling card holder data.

Name: ____________________________________ Signature:_________________________________

Date: _______________________________________

Fill in the name of the contact person and number and distribute this information to all of the staff involved in credit card processing. The Incident Assessment Template outlines the gathering of information that will easily facilitate the communication of the incident to Finance, Organizational Risk Assessment, and IT.

Incident Assessment Template (page 2 of 2)

Question	Response/Comments
When was the incident discovered?	
When did the incident occur (if different from date of discovery)?	
Who discovered the incident?	
What type of incident occurred?	□ System/Data Compromise □ Network Attack/Malware/Virus □ Lost/Stolen Equipment □ Lost/Stolen Data □ Physical Compromise of POS (e.g. damage/tampering) □ Langara Policy Violation □ Other – please describe ___________________
Was cardholder data involved? □ No □ Yes – select what type of data is involved	□ Credit Card Number □ Cardholder Name □ Expiration Date □ None
Was sensitive authentication data involved?	□ Full Magnetic Stripe Data □ CVV □ PIN □ None
What is the estimated number of people or records impacted?	□ None □ 1-499 □ 500 or above
Does the incident compromise business operation continuity (availability)?	□ No □ Potentially □ Yes □ Unknown
Is there a need for client/customer notification?	□ No □ Potentially □ Yes
What steps have been taken to resolve or rectify the incident?	

Last Revised: June 2019