Cardholder Data Security Incident Response Plan

Purpose

The purpose of this document is to document the process to be followed for responding to security incidents involving the unauthorized disclosure or modification of cardholder data (as defined by the Payment Card Industry (PCI) Data Security Standard).

The document includes the roles, responsibilities, and procedures for the involved personnel when reacting to an information security incident.

This plan focuses on:

- Containing the incident
- Analyzing the incident
- Responding to the incident

What constitutes a security incident involving cardholder data?

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 this incident response plan.

Merchant Responsibilities

All merchants are expected to:

- Be familiar with the Incident Response Plan.
- Ensure that departmental staff who process credit cards payments as part of their job are aware of the Incident Response Plan.

Procedures for Merchants to follow in the event of a Suspected or Confirmed Security Incident

Step 1: Contain or limit the exposure. Some steps that merchants can take to limit exposure include:

- Stop taking further payments until cleared to do so by Business Operations, Financial Services.
- Disconnect the compromised system from the network (Note: Do not turn off the computer – simply unplug the network cable)
- Lock paper records in a secure location

Note: Do not alter or access the system until ITS IT security has had an opportunity to examine the IT system
Step 2: Merchants should contact Business Operations and ITS IT Security. The primary contact points in each office are:

<table>
<thead>
<tr>
<th>Primary Contact</th>
<th>Business Operations</th>
<th>Computing and Communications Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valerie Evans</td>
<td>Director, Business Operations</td>
<td>Tim Lott</td>
</tr>
<tr>
<td>301N Robertson Hall</td>
<td>401 Robertson Hall</td>
<td>Director, Information Security</td>
</tr>
<tr>
<td>(613) 520-2600 x1330</td>
<td>(613) 520-2600 x5048</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td><a href="mailto:Valerie.Evans@Carleton.ca">Valerie.Evans@Carleton.ca</a></td>
<td></td>
<td>401 Robertson Hall</td>
</tr>
<tr>
<td>Kristine Simmons</td>
<td>Assistant Manager, Business Operations</td>
<td>Mani Nimalan</td>
</tr>
<tr>
<td>301J Robertson Hall</td>
<td></td>
<td>Information Security Manager</td>
</tr>
<tr>
<td>(613) 520-2600 x2070</td>
<td></td>
<td>401 Robertson Hall</td>
</tr>
<tr>
<td><a href="mailto:Kristine.Simmons@Carleton.ca">Kristine.Simmons@Carleton.ca</a></td>
<td></td>
<td>(613) 520-2600 x5245</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:tim.lott@carleton.ca">tim.lott@carleton.ca</a></td>
</tr>
</tbody>
</table>

In the event that a security incident is detected outside of normal business hours, please contact the ITS Service Desk and indicate that the issue must be escalated immediately.

Step 3: Document any actions taken prior to the arrival/engagement of representatives from Business Operations or ITS.

Procedures for Business Operations and ITS IT Security to follow in the event of a Suspected or Confirmed Security Incident

Step 4: Validate and assess the incident. ITS IT security will investigate the incident in accordance with ITS Incident Handling Procedures. As part of the investigation, Business Operations and ITS IT Security will:

- Establish how the compromise occurred
- Document the type of cardholder data breached (PAN, mag stripe, expiration date, etc.)
- Identify the source for the compromise
- Identify the timeframe for the compromise
- Approximate # of cardholders affected
- Review the technology environment in accordance with the ITS Incident Response Procedures
- Confirm that the incident has been contained
- Keep senior management informed

Step 5: Once the root cause of the incident has been identified, implement security controls (either physical, procedural, or technical) to prevent future incidents.

Step 6: Business Operations, in consultation with ITS IT Security, will provide the merchant with approval to restart payment processing.

Awareness and Updating of the Incident Response Plan

Business Operations and ITS IT Security will review the incident response plan as part of merchant briefings on PCI compliance. This plan will be reviewed on an annual basis for completeness and will be updated based on the results of the review.

Reporting Incidents to Acquirer

Business Operations will report the incident to the University’s acquirer, Chase Paymentech via the website at the following URL:

http://www.chasepaymentech.com/data_security.html