Cardholder Data Security Incident Response Plan

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).

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.

All merchants are expected to be familiar with the Incident Response Plan and ensure that departmental staff who process credit cards payments as part of their job are aware of the Incident Response Plan.

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 CCS IT security has had an opportunity to examine the IT system.

Step 2: Merchants should contact Business Operations and CCS IT Security. The primary contact points in each office are:

<table>
<thead>
<tr>
<th></th>
<th>Business Operations</th>
<th>Computing and Communications Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary Contact</strong></td>
<td>Valerie Evans</td>
<td>Jamie Campbell</td>
</tr>
<tr>
<td></td>
<td>Manager, Business Office</td>
<td>Assistant Director, Information Security and Operating Platforms</td>
</tr>
<tr>
<td></td>
<td>301N Robertson Hall</td>
<td>401C Robertson Hall</td>
</tr>
<tr>
<td></td>
<td>(613) 520-2600 x1330</td>
<td>(613) 520-2600 x2116</td>
</tr>
<tr>
<td></td>
<td>[<a href="mailto:Valerie.Evans@Carleton.ca">Valerie.Evans@Carleton.ca</a>]</td>
<td>[<a href="mailto:Jamie.Campbell@Carleton.ca">Jamie.Campbell@Carleton.ca</a>]</td>
</tr>
<tr>
<td><strong>Alternate Contact</strong></td>
<td>Kristine Simmons</td>
<td>Geoff Leboldus</td>
</tr>
<tr>
<td></td>
<td>Assistant Manager, Business Operations</td>
<td>Senior IT Security Analyst</td>
</tr>
<tr>
<td></td>
<td>301J Robertson Hall</td>
<td>402N Robertson Hall</td>
</tr>
<tr>
<td></td>
<td>(613) 520-2600 x2070</td>
<td>(613) 520-2600 x6725</td>
</tr>
</tbody>
</table>

In the event that a security incident is detected outside of normal business hours, please contact the CCS 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 CCS.

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

**Step 4:** Validate and assess the incident. CCS IT security will investigate the incident in accordance with CCS Incident Handling Procedures. As part of the investigation, Business Operations and CCS 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 CCS 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 CCS IT Security, will provide the merchant with approval to restart payment processing.

**Awareness and Updating of the Incident Response Plan**

Business Operations and CCS 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](http://www.chasepaymentech.com/data_security.html)