PCI
Incident Response Plan

Payment Card Industry
Data Security Standard (PCI DSS)
Contents

Revisions/Approvals .......................................................................................................................... i
Purpose ........................................................................................................................................... 2
Scope/Applicability .......................................................................................................................... 2
   PCI Incident Response Team .................................................................................................. 2
Procedures ....................................................................................................................................... 2
   PCI Incident Response Plan (IRP) ....................................................................................... 2
   PCI Incident Response Team Procedures ............................................................................. 3
   Bank Breach Response Plans ............................................................................................... 4
Flow Chart for Suspected Breach ............................................................................................... 5
PCI Incident Response Team (PCIRT) Tool Kit .......................................................................... 6
Card Association Breach Response Plans .................................................................................... 6
   Visa – Responding to a Breach .......................................................................................... 6
   MasterCard – Responding to a Breach ............................................................................... 6
   American Express – Responding to a Breach .................................................................... 6
Procedures and Other Supporting Documents .......................................................................... 8
   PCI Incident Response and Management Process Flow .................................................... 9
Interpretations .............................................................................................................................. 10
Definitions ..................................................................................................................................... 10

Revisions/Approvals

<table>
<thead>
<tr>
<th>Ver. #</th>
<th>Changes By</th>
<th>Ver. date</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>S. Wilson</td>
<td>12/20/2017</td>
<td>Updates to Cornell’s version</td>
</tr>
<tr>
<td>0.2</td>
<td>S. Wilson</td>
<td>1/5/2018</td>
<td>Updated with changes per D. Federation</td>
</tr>
<tr>
<td>0.3</td>
<td>S. Wilson</td>
<td>2/12/2018</td>
<td>Updated from 2/12/meeting</td>
</tr>
<tr>
<td>1.0</td>
<td>S. Wilson</td>
<td>4/12/2018</td>
<td>Document finalized</td>
</tr>
</tbody>
</table>
Purpose
The PCI Incident Response Plan supplements the University Incident Response Plan.

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 PCI 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 PCI incident response plan at Cornell University.

Scope/Applicability
For all units that accept credit cards as a method of payment for goods or services in relation to university business/operations, Cornell University requires compliance with Payment Card Industry – Data Security Standards (PCI-DSS) protocols, and in accordance with the procedures outlined in this document.

PCI Incident Response Team
The Cornell University PCI Incident Response Team is comprised of Data Privacy Incident Response Team (DPIRT) and Credit Card advisory Group (C-CAG).

Communication for the PCI Incident Response Team can be sent to pci-help@cornell.edu. Off hours contact ITSO operations: 1-607-255-6664.

Procedures

PCI Incident Response Plan (IRP)
The PCI Incident Response Plan needs to take into account that incidents may be reported/identified through a variety of different channels but the PCI Incident Response Team will be the central point of contact and responsible for executing Cornell University’s PCI Incident Response Plan.

The Cornell University’s PCI incident response plan is summarized as follows:
1. All incidents must be reported to the PCI Incident Response Team.
2. All actions taken must be documented on the Payment Card Incident Log (appendix A)
3. The PCI Incident Response Team will confirm receipt of the incident notification.
4. The PCI Incident Response Team will investigate the incident and assist the compromised department in limiting the exposure of cardholder data.
5. The PCI Incident 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.
6. The PCI Incident 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 cardholder data is collected, processed, stored or transmitted. 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. Do NOT touch or compromise any possible evidence. Do not shut off any computer or POS system.
2. Contact the PCI Incident Response Team by sending an email documenting the incident to:
   
   pci-help@cornell.edu or for after hours supports contact the ITSO operations team at 607-255-6664

   a. Overview of incident, including date, time, and location of incident
   b. Incident Type
      i. Computer Abuse
      ii. Malicious Code
      iii. Spam
      iv. Unauthorized Access/Use
      v. Breach of Physical Security (unlocked file cabinet, storage room, etc.)
      vi. Possible tampering of POS device
      vii. Other
   c. Intrusion Method
      i. Virus
      ii. Spyware/Malware
      iii. Stolen Password
      iv. Other
   d. Overview of data on the system?
   e. Explanation of discovery
   f. Action taken upon discovery
   g. Explanation of impact and impact on daily activities
   h. Any additional information

3. The PCI Incident 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 PCI Incident Response Team has arrived. Include the date, time, person/persons involved and action taken for each step.

6. Assist the PCI Incident Response Team as they investigate the incident.

**PCI Incident Response Team Procedures**

The Cornell University’s PCI 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 PCI Incident Response Team, along with other designated university staff from Computers and Information Technology, will implement their PCI incident response plan to assist and augment departments’ response plans.

In response to a system compromise, the PCI Incident Response Team 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:
   a. DPIRT & C-CAG
   b. Cornell University’s 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
   c. 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
   d. 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
   e. Campus police and local law enforcement

6. If applicable, assist card industry security and law enforcement personnel in investigative process.

**Bank Breach Response Plans**

The credit card companies have specific requirements the PCI Incident 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.

— Responding to a Breach
Flow Chart for Suspected Breach

1. **Banking Partner, Card Association, 3rd-party Security Firm**
   - Central IT
   - Department/Merchant

   **SUSPICIOUS ACTIVITY REPORTED**

2. **BREACH SUSPECTED**

   - Do NOT turn off the PC/server
   - Disconnect PC/server from network
   - Document
     - Suspicious activity
     - Steps taken to-date
     - Personnel involved

3. **Notify Response Team**

4. **Incident Response Team**

   - Confirm/research breach
     - Ensure system(s) are isolated
     - Gather/log central evidence
       (firewalls, file integrity, IDS, AV, etc)
     - Analyze local machines/logs
     - Forensic analysis on breached PC
   - Prepare INITIAL incident report and notify
     - pci-help@cornell.edu
     - University Police & Law Enforcement
     - Acquiring Bank and Card Brands
     - Continue/assist with on-going investigation

5. **Issue FINAL incident report**
   - Prioritize/complete any remediation items
PCI Incident Response Team (PCIRT) Tool Kit

Preparing a tool kit for the PCIRT to use will enable them to respond promptly to any reported breaches.

- The kit should leverage existing ITSO IR tools
- Contact ITSO to obtain information for this tool kit.
  - Email pci-help@cornell.edu
  - Call - (607) 255-842

Card Association Breach Response Plans

Visa – Responding to a Breach


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.

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

- American Express Data Security Operating Policy – U.S.
Procedures and Other Supporting Documents

Cornell University Policy 3.17 – Accepting Credit Cards to Conduct University Business
Cornell University Policy 5.4.2 – Reporting Electronic Security Incidents
## PCI Incident Response and Management Process Flow

**Cornell University PCI Incident Response and Management Process**

<table>
<thead>
<tr>
<th>Incident Occurs</th>
<th>Notification of Incident</th>
<th>Response Team</th>
<th>Triage &amp; Investigations</th>
<th>Detailed Analysis / Communication</th>
<th>Remediation</th>
<th>Incident Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Compromise or Suspected System Compromise</td>
<td>Email <a href="mailto:help@cornell.edu">help@cornell.edu</a>. After hours contact ITSO Ops. 607-255-6094</td>
<td>ITSO &amp; Treasurer’s office</td>
<td>Identify Scope</td>
<td>Ensure compromised system is isolated off the network</td>
<td>ITSO &amp; Treasurer’s office</td>
<td>Notify compromised customers (if necessary)</td>
</tr>
<tr>
<td>Suspected or Confirmed breaches of cardholder data</td>
<td>Contact Department IT</td>
<td>Department IT</td>
<td>suspend Processing</td>
<td>Gather, review, and analyze centrally maintained system, firewall, file integrity and intrusion detection/protection system logs and alerts</td>
<td></td>
<td>Resume processing if appropriate</td>
</tr>
<tr>
<td></td>
<td>Document incident in the PCI Log</td>
<td></td>
<td>Contain the breach</td>
<td>Assist department in analysis of locally maintained systems and other logs, as needed</td>
<td></td>
<td>Lessons learned</td>
</tr>
<tr>
<td></td>
<td>Assemble Response Team Members as needed</td>
<td>University Counsel, Risk Management, University Communications, Audit, CIO</td>
<td>Begin triage—look at environment &amp; determine validity of claim</td>
<td>Conduct appropriate forensic analysis of compromised system.</td>
<td></td>
<td>Closeout report</td>
</tr>
<tr>
<td></td>
<td>Contact CUPD as needed</td>
<td>Cornell University Police</td>
<td></td>
<td>If an incident is confirmed, follow procedures in the Incident Response Plan for outreach and communication.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Interpretations**
For clarification or questions on this plan please contact pci-help@cornell.edu

**Definitions**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Payment Card Industry Data Security Standards (PCI DSS)</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Cardholder</strong></td>
<td>Someone who owns and benefits from the use of a membership card, particularly a credit card.</td>
</tr>
<tr>
<td><strong>Card Holder Data (CHD)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Credit Card Advisory Group (C-CAG)</strong></td>
<td>The Credit Card Advisory Group (C-CAG) works with campus stakeholders to identify necessary compliance activities or technology solutions, recommend updates to this and other policies, and advise the Executive Vice President and Chief Financial Officer on PCI requirements.</td>
</tr>
<tr>
<td><strong>Data Privacy Incident Response Team (DPIRT)</strong></td>
<td>A committee that determines and guides the institution's response to the loss or exposure of university data. It is composed of representatives of University Counsel, Risk Management and Insurance, University Communications, Audit, IT Security, and the Cornell Police, and is chaired by the Chief Information Officer.</td>
</tr>
<tr>
<td><strong>Primary Account Number (PAN)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Cardholder Name</strong></td>
<td>The name of the Cardholder to whom the card has been issued.</td>
</tr>
<tr>
<td><strong>Expiration Date</strong></td>
<td>The date on which a card expires and is no longer valid. The expiration date is embossed, encoded or printed on the card.</td>
</tr>
<tr>
<td><strong>Service Code</strong></td>
<td>The service code that permits where the card is used and for what.</td>
</tr>
<tr>
<td><strong>Sensitive Authentication Data</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Magnetic Stripe (i.e., track) data</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>CAV2, CVC2, CID, or CVV2 data</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>PIN/PIN block</strong></td>
<td>Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disposal</td>
<td>CHD must be disposed of in a certain manner that renders all data unrecoverable. 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</td>
</tr>
<tr>
<td>Merchant Department</td>
<td>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.</td>
</tr>
<tr>
<td>Merchant Department</td>
<td>An individual within the department who has primary authority and responsibility within that department for credit card transactions.</td>
</tr>
<tr>
<td>Responsible Person (MDRP)</td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>A structured electronic format for organizing and maintaining information that is accessible in various ways. Simple examples of databases are tables or spreadsheets.</td>
</tr>
<tr>
<td>Wireless Access Point</td>
<td>Also referred to as “AP.” Device that allows wireless communication devices to connect to a wireless network. Usually connected to a wired network, it can relay data between wireless devices and wired devices on the network.</td>
</tr>
</tbody>
</table>
Appendix A. Payment Card Incident Log

In the event of a suspected or confirmed event, please follow the procedures below ensuring each step taken is documented using this incident log:

1. Contact the PCI Response Team by sending an email documenting the incident to pci-help@cornell.edu or for after hours supports contact the ITSO operations team at 607-255-6664

2. Unit Name and Contact Information

3. Date/Time and Incident description.

4. The PCI Incident Response Team will coordinate a response and reply to this initial notification/communication to confirm they are aware of the incident.

5. 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.

6. Document any steps taken until the PCI Incident Response Team has arrived. Include the date, time, person/persons involved and action taken for each step.

<table>
<thead>
<tr>
<th>Action</th>
<th>Date/Time</th>
<th>Location</th>
<th>Person(s) performing action</th>
<th>Person(s) documenting action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Additional notes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7. Assist the PCI Incident Response Team as they investigate the incident.

8. 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 Cornell University’s 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 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:

___________________________________________________________________________

___________________________________________________________________________