Payment Card Security Incident Response Plan

The Payment Card Security Incident Response Plan supplements the Virginia Tech Guide for Cyber Security Incident Response (the Guide). A copy of the Guide is available through the Information Technology Security Office (ITSO). A list of the merchants and operations with payment card acceptance and IP addresses has been provided to the ITSO to identify the areas accepting payment cards.

Accepting payment cards on behalf of Virginia Tech requires merchants to adhere to the Payment Card Industry Data Security Standard (PCI DSS). The standard was created by the five largest credit card brands: Visa, MasterCard, American Express, Discover, and Japan Credit Bureau. The PCI DSS is a set of guidelines that is designed to enhance security regarding payment card transactions. One of the guidelines requires merchants to create a security incident response team and document an incident response plan. The members of the University Payment Card Incident Response Team (PCIRT) are listed below.

**Virginia Tech Payment Card Incident Response Team**

<table>
<thead>
<tr>
<th>Department</th>
<th>Position</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of University Bursar</td>
<td>University Bursar</td>
<td>Melinda West</td>
</tr>
<tr>
<td>Office of University Bursar</td>
<td>E-commerce Operations Manager</td>
<td>Becky Ford</td>
</tr>
<tr>
<td>Office of University Bursar</td>
<td>Cash Receipts and Disbursements Manager</td>
<td>Rosa Lucas</td>
</tr>
<tr>
<td>IT Security Office</td>
<td>University IT Security Officer</td>
<td>Randy Marchany</td>
</tr>
<tr>
<td>IT Security Office</td>
<td>IT Security Analyst</td>
<td>Beth Lancaster</td>
</tr>
</tbody>
</table>

*Department IT Contact*

<table>
<thead>
<tr>
<th>Department</th>
<th>Position</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outreach Information Services</td>
<td>IT Security and Compliance Specialist</td>
<td>Joseph Goodman</td>
</tr>
<tr>
<td>Athletics Information Technology</td>
<td>Director of Information Technology</td>
<td>Tommy Regan</td>
</tr>
</tbody>
</table>

<For merchant department, include merchant location personnel and third party vendor contact if applicable.>

* Merchant/Department IT contact will be involved depending on the area affected in the incident.

**Payment Card Incident Response Team Notification**

A payment card incident may be discovered and reported through several channels. First, the Information Technology Security Office is the central point of contact for reporting cyber incidents. Merchant or department must report all cyber security incidents to the ITSO in accordance with the Guide. If the ITSO detects or receives a report of a cyber-incident in a predetermined list of IP addresses in the cardholder

---

1 Reference: “Incident Response Plan, Template for Breach of Personal Information”, American Institute of Certified Public Accountants, Inc.

Last revised: 10/14/2016
data environment (CDE), the ITSO will notify the Office of the University Bursar (OUB) and the affected department.

Second, a suspected breach may be reported to the OUB by the processing bank, the card association, or a third party vendor. In that case, the OUB will notify the campus merchant(s) involved in the suspected breach and the ITSO.

Finally, all physical breaches to the CDE such as office break-in, loss of payment card devices, or loss of paper forms which may contain cardholder data must be reported to the OUB and the university police.

Once the OUB receives notification of a suspected payment card data breach, the OUB will work with the ITSO to conduct an initial investigation/analysis to determine the potential scope of the incident and whether cardholder data may have been compromised. The university bursar or its designee will then determine whether the Payment Card Incident Response Team (PCIRT) activation is appropriate. The PCIRT will only be activated if a payment card security incident has been identified and cardholder data may have been compromised.

The OUB will notify Internal Audit, General Counsel, the Vice President for Finance, the merchant bank, and the payment card associations if appropriate.

The next section discusses the detailed steps that merchants and the university would follow should a suspected payment card breach was discovered. Appendix E shows a flow chart for electronic incident response procedures.

Payment Card Security Incident Response Procedures

**Merchant Response Procedures**

Each merchant should maintain a detailed incident response plan by identifying responsible employees and contact information at a minimum. The merchant’s incident response plan shall be in accordance with the University’s Payment Card Security Incident Response Plan and the parameters set forth by the Card Brands.

Merchant should refer to the Guide for guidelines on incident response preparation and detection. Once a payment card security incident or a suspected breach of cardholder data environment has been detected, the merchant must immediately execute the following three steps:

1. a) In the event of a physical breach to the cardholder data environment, contact the Virginia Tech 4Help line at (540) 231-4357 and the university police at (540) 232-8477 immediately.

   b) In the event of an electronic incident, contact the Virginia Tech 4Help line at (540) 231-4357 to report a payment card security incident. The merchant should execute the following steps to ensure preservation of electronic data:
• Disconnect the computer/devices(s) from the network. To disconnect the device from the network, simply unplug the network cable, or if the computer uses a wireless connection, disconnect from the wireless network.

• DO NOT turn the computer device off or reboot. Leave the device powered on and disconnected from the network.

• Be on high alert and monitor traffic on all systems with cardholder data.

• Prevent any further access to or alteration of the compromised system(s) (i.e., do not log on to the machine and/or change passwords; do not log in as ROOT; do not run a virus scan). Do not use the compromised system(s) to avoid losing critical, volatile data.

• In short, leave the system(s) alone, disconnected from the network, and wait to hear from the ITSO or the OUB.

Upon receiving the call, the Network Operations Center will email the person reporting the incident the above instructions for preserving electronic data and a template for documentation (see details in 2 below).

2. The merchant should document every action you taken from detection of the suspected breach forward, preserving any logs or electronic evidence available (i.e. original evidence, security events, web, database, firewall, etc.). The Payment Card Incident Documentation Template (see Appendix A) may be used to report actions taken or the merchant’s own form which should include the following at a minimum:

• Date and time
• Action taken
• Location
• Person performing action
• Person performing documentation
• All personnel involved

3. Notify the dean, director or department head of the unit experiencing the breach or suspecting a cardholder data breach. No one should communicate with anyone outside of their supervisor(s) or the Payment Card Incident Response Team about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated through University Relations by the PCIRT.

University Response Procedures

1. In the event an incident has been reported to the 4Help line, the Network Operations Center will email members of the PCIRT with the information collected from the merchant reporting a suspected incident and call the members of the PCIRT in the provided order until one member
has been contacted. Members of the PCIRT should send an email response to VTOC-OC-DL@exchange.vt.edu acknowledging receipt of information relating to the suspected incident.

2. The OUB and the ITSO will work with the affected merchant to quickly analyze and validate the incident and perform an initial assessment to determine the scope of the incident, the possible cause of the incident and whether cardholder data has been compromised. The initial analysis should provide adequate information for the university bursar to determine if the PCIRT needs to be activated and for the PCIRT to prioritize subsequent activities.

3. If a payment card security incident has been confirmed, the PCIRT will alert Internal Audit, General Counsel, University Relations, the Vice President for Finance, the merchant bank, and the payment card associations as appropriate (see step 4).

4. The PCIRT will notify the applicable acquirer(s) and the payment card association(s) in the event of a confirmed payment card security incident. The university will follow procedures required by the payment card associations in responding to payment card security incident and cardholder data compromise.

- Within 24 hours alert all necessary parties immediately
  - Notify the applicable acquirer(s) and/or merchant bank(s)
  - Notify the applicable payment card association(s)
  - Visa Incident Response Manager at 1-650-432-2978 or usfraudcontrol@visa.com
  - MasterCard Compromised Account Team by phone at 1-636-722-4100 or by email at compromised_account_team@mastercard.com. The email should provide a detailed written statement of fact about the payment card compromise (including the contributing circumstances; and provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers and information.
  - Discover Fraud Prevention at 1-800-347-3102
  - American Express Merchant Services at 1-800-528-5200
- Within three (3) business days of the reported compromise
  - Provide written documentation to the Visa client or to Visa
  - Engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation)
Within ten (10) business days

- Provide all compromised Visa, Interlink, and Plus accounts to the Visa acquiring bank or to Visa. Acquiring entities must provide all compromised Visa Account numbers regardless if the transaction went through another regional or national network. The account information must indicate if the transaction was Visa, Interlink, Plus or other network ID. All potentially compromised accounts must be provided and transmitted as instructed by the Visa acquiring bank and Visa. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information.

- Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.

- Provide forensic reports and findings of all audits and investigations to the MasterCard Merchant Fraud Control Department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

For additional activities that must be performed see Visa’s “What To Do If Compromised“:


MasterCard’s “Merchant Rules Manual“:


Obtain additional, specific requirements from Discover Card and American Express.

Sanctions

University merchants failing to comply with the principles above may lose their authorization to process payment card transactions. Any fines and assessments which may be imposed by the affected credit card company will be the responsibility of the merchant department. Individuals in violation of this policy may be subject to disciplinary action and termination in addition to criminal and civil penalties imposed by law. Some violations may constitute criminal offenses under local, state or federal laws. Virginia Tech will carry out its responsibility to report such violations to the appropriate authorities.
Appendix A. Payment Card Incident Documentation Template

Location, IP Address and name of the compromised machine ________________________________

Is the machine hosting any payment redirect service for cardholder data?  ☐ YES  ☐ NO

Does the machine have cardholder data?  ☐ YES  ☐ NO

When was the problem noticed and who reported? _________________________________________

Has Payment Card Incident Response Team approved removal from network?  ☐ YES  ☐ NO

If YES, date and time systems were removed: ______________________________________________

Name of person(s) who disconnected the network: _________________________________________

If NO, state reason: ___________________________________________________________________

Who has logged into machine(s) and what has been done? __________________________________

Does the ITSO have any record of the machine sending data to another machine?  ☐ YES  ☐ NO

If yes, what is the IP address of the machine(s)? _________________________________________

If cardholder data has been compromised, complete the following table when information is available:

<table>
<thead>
<tr>
<th>Type of data exposed</th>
<th>☐ Cardholder name</th>
<th>☐ Cardholder address</th>
<th>☐ PAN</th>
<th>☐ Expiry date</th>
<th>☐ CID, CAV2, CVC2, CVV2</th>
<th>☐ Track data (track 1, 2, or both)</th>
<th>☐ Encrypted or clear-text PINs</th>
<th>☐ PIN Blocks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brand exposure</td>
<td>☐ Visa</td>
<td>☐ American Express</td>
<td>☐ JCB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>☐ MasterCard</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>☐ Discover</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number of cards exposed:
(both live system space and unallocated space)

Breakdown by payment card brand:
- American Express
- Discover
- JCB
- MasterCard
- Visa
Use this table to document actions performed

<table>
<thead>
<tr>
<th>Action</th>
<th>Date and 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></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix B

Escalation Members

- Escalation - First Level
  
  University IT Security Officer
  
  IT Security Analyst
  
  University Bursar
  
  E-Commerce Operations Manager
  
  Network Engineer / Analyst
  
  Merchant Staff / IT Support

- Escalation - Second Level

  Controller

  Vice President for IT and Chief Information Officer (CIO)

  Vice President for Finance and Chief Financial Officer (CFO)

  University Relations

  University Legal Counsel

  Internal Audit

  University Police Chief

External Contacts (as needed)

  Merchant Bank

  Payment Card Associations

  Internet Service Provider (if applicable)

  Internet Service Provider of Intruder (if applicable)

  Communications Carriers (local and long distance)

  Business Partners

  Insurance Carrier
External Response Teams as applicable (CERT Coordination Center\(^2\), etc.)

Law Enforcement

  Local Police Force (jurisdiction determined by crime)

  Federal Bureau of Investigation (FBI) (especially if a federal interest computer or a federal crime is involved)

  Secret Service

Notification Order

  Payment Card Incident Response Team

  System Administrator(s) of area affected by incident

  Manager of area affected by incident

  Communications Network Services

  Controller

  Campus Police

  Internal Audit

Notified when nature and impact of incident has been determined

  VP for IT and CIO

  VP for Finance and CFO

  University Legal Counsel

  University Relations

  Business Partners

  Human Resources

\(^2\) The CERT/CC is a major reporting center for Internet security problems. Staff members provide technical advice and coordinate responses to security compromises, identify trends in intruder activity, work with other security experts to identify solutions to security problems, and disseminate information to the broad community. The CERT/CC also analyzes product vulnerabilities, publishes technical documents, and presents training courses. For more detailed information about the CERT/CC, see http://www.cert.org.
### Appendix C. Payment Card Incident Response Team Contact List

<table>
<thead>
<tr>
<th>Office of University Bursar</th>
<th>University Bursar</th>
<th>Melinda West</th>
<th>540-231-6277</th>
<th><a href="mailto:mwest@vt.edu">mwest@vt.edu</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of University Bursar</td>
<td>E-commerce Operations Manager</td>
<td>Becky Ford</td>
<td>540-231-6277</td>
<td><a href="mailto:huffmanb@vt.edu">huffmanb@vt.edu</a></td>
</tr>
<tr>
<td>Office of University Bursar</td>
<td>Cash Receipts and Disbursements Manager</td>
<td>Rosa Lucas</td>
<td>540-231-6277</td>
<td><a href="mailto:rosall@vt.edu">rosall@vt.edu</a></td>
</tr>
<tr>
<td>IT Security Office</td>
<td>University IT Security Officer</td>
<td>Randy Marchany</td>
<td>540-231-1688</td>
<td><a href="mailto:marchany@vt.edu">marchany@vt.edu</a></td>
</tr>
<tr>
<td>IT Security Office</td>
<td>IT Security Analyst</td>
<td>Beth Lancaster</td>
<td>540-231-5105</td>
<td><a href="mailto:blanct@vt.edu">blanct@vt.edu</a></td>
</tr>
</tbody>
</table>

### Department IT Contact

<table>
<thead>
<tr>
<th>Outreach Information Services</th>
<th>IT Security and Compliance Specialist</th>
<th>Joseph Goodman</th>
<th>540-231-6065</th>
<th><a href="mailto:jkgoodman@vt.edu">jkgoodman@vt.edu</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Athletics Information Technology</td>
<td>Director of Information Technology</td>
<td>Tommy Regan</td>
<td>540-231-7539</td>
<td><a href="mailto:tregan@vt.edu">tregan@vt.edu</a></td>
</tr>
</tbody>
</table>
## Report Templates and Aids for PFI Investigations

### Preliminary Incident Response Report

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of compromised entity</td>
<td></td>
</tr>
<tr>
<td>Date investigation started</td>
<td></td>
</tr>
<tr>
<td>Is forensic investigation being done onsite or remotely?</td>
<td>Onsite</td>
</tr>
<tr>
<td>Evidence of a breach?</td>
<td>Yes</td>
</tr>
<tr>
<td>First confirmed date that the intruder or malware entered the network</td>
<td></td>
</tr>
<tr>
<td>Scope of forensic investigation (e.g., single vs. numerous locations;</td>
<td></td>
</tr>
<tr>
<td>how systems/network were determined for acquisition, remote vs. onsite)</td>
<td></td>
</tr>
<tr>
<td>Type of data impacted (e.g., full track, CID, CAV2, CVC2, CVV2,</td>
<td></td>
</tr>
<tr>
<td>encrypted or clear-text PINs, PIN blocks)</td>
<td></td>
</tr>
<tr>
<td>Window of system vulnerability</td>
<td></td>
</tr>
<tr>
<td>Initial thoughts on attack vector</td>
<td></td>
</tr>
<tr>
<td>Is the security breach ongoing or has it been contained?</td>
<td>Ongoing</td>
</tr>
<tr>
<td>If contained, how has it been contained?</td>
<td></td>
</tr>
<tr>
<td>Estimated date of investigation completion</td>
<td></td>
</tr>
<tr>
<td>Other comments</td>
<td></td>
</tr>
</tbody>
</table>
Appendix E. Payment Card Security Incident Response Procedure

Discovery of Suspected Payment Card Security Incident

- Banking Partner, Card Association, 3rd-party Vendor
  - Notify OUB
  - Notify ITSO

- Central IT, ITSO
  - Notify OUB
  - Notify affected merchant

- Department, Merchant
  - Physical breach?
    - Yes: Report to 4HELP & Police
    - No: Notify OUB & ITSO

**Initial Discovery**

- Do not turn off the machine
  - Disconnect from network
  - Document
  - Initial investigation

**Investigation and Notification**

- Potential CHD exposure?
  - Yes: Activate PCIRT
    - Confirm/research breach
    - Prepare initial incident report and notify as necessary
    - Continue with investigation
    - Issue FINAL incident report
    - Prioritize/begin remediation
  - No

- Coordinate remediation plan
- Conduct/confirm remediation
- Incident Closure
Appendix F. Definitions

**Cardholder/Payment card data** - the Primary Account Number (PAN) alone or the PAN plus any of the following: cardholder name, expiration date, or service code – encoded number on the magnetic stripe that specifies acceptance requirements and limitations for a magnetic stripe read transaction.

**Cardholder data environment** – the people, processes and technology that store, process or transmit cardholder data or sensitive authentication data including any connected system components.

**Data Breach** – Includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, access for an unauthorized purpose, or other unauthorized access, to data, whether physical or electronic.

**Incident/Security Incident** - The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

**Log** – Also referred to as “audit log” or “audit trail.” Chronological record of system activities. Provides an independently verifiable trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results.

**Merchant** – a university entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services.

**PAN** – primary account number is the fifteen or sixteen-digit payment card number on the front of the card that identifies the issuer and the particular cardholder account.

**Payment Card** – a credit or debit card issued through one of the five members of the payment card industry – Visa, Master Card, American Express, Discover, or JCP.

**PCI DSS** – Payment Card Industry Data Security Standard, a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.