PCI Security Incident Response Plan

OVERVIEW

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 security incident response team and document an incident response plan. The Virginia Highlands Community College PCI Security Incident Response Team (Response Team) is comprised of the following:

- IT Coordinator
- Information Security Officer * Also the Team Leader
- Finance Manager
- Database Administrator
- Campus Police Chief

Virginia Highlands Community College PCI Security Incident Response Team			
	Current Member	Phone	Email
IT Coordinator	Glen Johnson	276-739-2467	gjohnson@vhcc.edu
Information Security Officer	Leigh Anne Hutton	276-739-2443	lhutton@vhcc.edu
Finance Manager	Mary Snead	276-739-2403	msnead@vhcc.edu
Database Administrator	Tammy McCracken	276-739-2495	tmccracken@vhcc.edu
Campus Police Chief	Blake Andis	276-739-2582	bandis@vhcc.edu

The Virginia Highlands Community College PCI Security Incident Response plan is summarized as follows:

1. All incidents must be reported to a member of the Response Team.
2. That member of the team will report the incident to the entire Response Team.
3. The Response Team will investigate the incident and assist the compromised department in limiting the exposure of cardholder data.
4. The 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.
5. The Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future.

PCI Security Incident Response Plan

PLAN

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. Contact a member of the Response Team and send an email documenting the incident to VH-PCI-IncidentResponse@vhcc.edu
2. 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.
3. Document any steps taken until the Response Team has arrived. Include the date, time, person/persons involved and action taken for each step.
4. Assist the Response Team as they investigate the incident.
5. If an incident of **unauthorized access** is *confirmed* and card holder data was potentially compromised, the Virginia Highlands Community College PCI Security Incident Response Team Leader will make the following contacts with VHCC's acquiring bank(s) after informing the College President:
   - **a.** For incidents involving Visa, MasterCard or Discover network cards, contact Bank of America Merchant Services Merchant Incident Response Team, MIRT at (800)228-5882 within 72 hours or reported incident.
     See Appendix A – Bank of America – Responding to a Breach
   - **b.** For incident's involving American Express cards, contact American Express Enterprise Incident Response Program (EIRP) within 24 hours after the reported incident at (888)-732-3750 or email EIRP@aexp.com.
     See Appendix A – American Express – Responding to a Breach
6. If an incident of **unauthorized access** is confirmed and card holder data was potentially compromised, the Response Team will proceed as indicated in Appendix A.

PCI Security Incident Response Plan

PROCECURE

The Virginia Highlands Community College PCI Security 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 Response Team, will implement their incident response plan.

In response to a system compromise, the Response Team will:

1. Ensure compromised system is isolated from all other systems.
2. Gather, review and analyze all centrally maintained system logs.
3. Assist department in analysis of locally maintained system and other logs, as needed.
4. Conduct appropriate forensic analysis of compromised system.
5. Work with the PCI Committee Chairperson to contact Internal Audit, and other law enforcement agencies as appropriate.
6. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel.
7. 7. Assist law enforcement and card industry security personnel in investigative process.

The credit card companies have specific requirements the Response Team must address in reporting suspected or confirmed breaches of cardholder data. See Appendix A for these requirements.

PCI Security Incident Response Plan

APPENDIX A

Bank of America – Responding to a Breach
Follow the steps set forth in the resource:
http://merch.bankofamerica.com/documents/10162/12961/respondingbreach.pdf

MasterCard – Responding to a Breach
Follow the steps set forth in the resource:
http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf

Visa – Responding to a Breach
Follow the steps set forth in the resource:
https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

Discover – Responding to a Breach
Contact Discover at the number below:
Merchant Fraud Prevention Department at ***1-800-347-3083***.

American Express – Responding to a Breach
To notify American Express, please contact the American Express Enterprise Incident Response Program (EIRP) toll free at ***(888) 732-3750*** or email at EIRP@aexp.com.