Credit Card Data Security Incident Response Plan

To address cardholder data security, the major card brands (Visa, MasterCard, Discover, and American Express) 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 UH System Credit Card Security Incident Response Team (Response Team) is comprised of the Executive Director of UIT Security, Senior UIT Security Analyst, Treasurer, Assistant Treasurer, and the College or Division Business Administrator for the merchant location reporting the cardholder data security incident. The UH System security incident response plan is summarized as follows:

1. All incidents must initially be reported to UIT Security via the Online Incident Reporting Form.
2. UIT Security will report the incident to the entire Response Team.
3. The Response Team, along with other university staff, 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.

UH System Cardholder Data Security Incident Response Team:

1. Mary Dickerson, Chief Information Security Officer and Executive Director of UIT Security, at 832-842-4679 or MEDickerson@central.uh.edu.
2. Jana Chvatal, Manager, IT Security Risk Management and Compliance, at 832-842-8496 or jchvatal@central.uh.edu.
3. Ricardo (Ric) Rodriguez, Senior UIT Security Analyst, at 832-842-8493 or arch2u@Central.uh.edu
4. Raymond Bartlett, Treasurer, at 713-743-8781 or rbartlett@central.uh.edu
5. Roberta Puryear, Assistant Treasurer, at 713-743-8780 or rdpuryea@central.uh.edu

Incident Response Plan

An incident, for purposes of this plan, is defined as a suspected or confirmed compromise of cardholder data. At a minimum, cardholder data consists of the full card number. Cardholder data may also appear in the form of the full card number plus any of the following: cardholder name, expiration date and/or sensitive authentication data. A cardholder data compromise is any situation where intrusion into a computer system occurs and unauthorized disclosure, theft, modification, or destruction of cardholder data is suspected or the suspected or confirmed loss or theft of any material or records that contain cardholder data.

In the event of a suspected or confirmed cardholder data incident, the following steps will be taken:

Department that suspects a cardholder data incident:

1. Contact UIT using the Online Incident Reporting Form**.**
2. Immediately contain and limit the exposure and preserve evidence by taking the following steps:
   a. Do not access or alter compromised systems (i.e., don't log on to the machine and change passwords, do not log in as ROOT).
   b. Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable).
   c. Preserve logs and electronic evidence.
   d. Log all actions taken.
   e. If using a wireless network, change the Service Set IDentifier (SSID) on any access point or any other devices that may be using this connection with the exception of any systems believed to be compromised.
   f. Be on "high alert" and monitor all systems with cardholder data.
3. Document any steps taken until UIT has contacted you. Include the date, time, person/persons involved and action taken for each step.
4. Assist UIT and any other personnel as they investigate the incident.

UIT:

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.
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 cardholder data was potentially compromised, the Executive Director of UIT Security will contact the Chief Information Officer, Internal Audit, University Police, and Treasurer.

6. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel as applicable.

Treasurer:

1. The Treasurer or Assistant Treasurer will contact the System's acquiring bank as follows:
    a. For incidents involving Visa, MasterCard or Discover network cards, contact Bank of America Merchant Services Merchant Incident Response Team at (800) 228-5882 within 72 hours of the reported incident. ***See Appendix A***
    b. For incidents 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***
2. If a cardholder data compromise is confirmed and cardholder data was potentially compromised, the Treasurer will coordinate with the Response Team to proceed as indicated in Appendix A, since the credit card companies have specific requirements that must be addressed in reporting suspected or confirmed breaches of cardholder data.

APPENDIX A

Bank of America – Responding to a Breach
Follow the steps set forth in the resource: Responding to a Breach: A guide provided by Bank of America Merchant Services

MasterCard – Responding to a Breach
Follow the steps set forth in the resource: Account Data Compromise User Guide

Visa – Responding to a Breach
Follow the steps set forth in the resource: What to do if Compromised Guide

American Express – Responding to a Breach
Follow the steps set forth in section 2 of: American Express Data Security Operating Policy – U.S.