Appendix 1 – Credit Card Security Incident Response Plan

(A) PURPOSE

The Credit Card Security Incident Response Plan supplements the University Credit Card Security Policy.

The University Credit Card Policy is designed to maintain secure financial transactions and comply with state law and contractual obligations. The University is responsible for responding to a breach or potential compromise of credit card data. This incident response plan provides guidance for identification, containment, notification, verification, investigation, and remediation of such incidents.

(B) RESPONSIBILITY

Any University employee, or any other person or entity accepting credit card payments on behalf of the University, who believes a breach or potential compromise (both electronic and non-electronic) of cardholder data has occurred is required to adhere to the steps outlined in this Incident Response plan.

(C) IDENTIFICATION

The first step in an incident response is to identify a breach or potential compromise of data that personally identifies information associated with a specific cardholder. Identification of a breach can occur through (but is not limited to) the following methods:

(1) A report from a third party (such as the cardholder),
(2) An anonymous complaint of unauthorized use or misuse of data,
(3) An alert from a security monitoring system such as intrusion-detection, intrusion prevention, firewalls, file-integrity monitoring systems, and network infrastructure devices that detect suspicious wireless access points that are physically connected to the network and used to intentionally circumvent University policy and security controls,
(4) The routine monitoring of activity and/or access logs,
(5) Vulnerability scans, or
(6) Suspicious circumstances beyond normal processes.

(D) CONTAINMENT

Containment is the next step to ensure limited exposure to the breached data, preserve potential evidence, and prepare for an investigation of the incident. Containment steps for an electronic device include:

(1) Not accessing or altering the compromised device,
(2) Not removing power to the device,
(3) Immediately terminate the network connection to the device or disabling the wireless adapter,
(4) Isolating access to the device by others,

(5) Documenting how the breach was detected and the state of the device at that point in time, and

(6) Documenting the steps taken to contain and isolate the device.

(E) INTERNAL NOTIFICATION

In the event of a breach or potential compromise of data, notification must be made immediately to the Accountant within the Controller's Office at 330-325-6369 and to the Information Technology (IT) Senior Systems Manager at 330-325-6233. An email should also be sent to acctg@neomed.edu. If it is after business hours, contact the NEOMED Police Department at 330-325-5911.

If the data breach involves the theft of physical property containing secure cardholder data, the NEOMED Police Department should be contacted at 330-325-5911. A copy of the police report should be given to the Accounting and IT Departments, and the NEOMED Police Department should be given contact information for the Accounting and IT Departments for follow up.

Upon verification of a breach of electronic data, the IT Department will be responsible for immediately assembling the response team. Upon verification of a breach of non-electronic data, the Accounting Department will be responsible for immediately assembling the response team.

Response Team

Accounting Department

Accountant, 330-325-6369
Controller, 330-325-6375
Assistant Controller, 330-325-6381

Information Technology Department

Senior Systems Manager, 330-325-6233
Information Technology Director, 330-325-6799
Project Manager, 330-325-6238

Risk Management

Chief Operating Officer, 330-325-6718

NEOMED Police Department

Chief of Police, 330-325-5911

General Counsel

General Counsel, 330-325-6356
Associate General Counsel, 330-325-6358

(F) VERIFICATION

The Information Technology Department will lead preliminary efforts in verifying a breach of electronic data. The Accounting Department will lead efforts in verifying a breach of non-electronic data. If upon discovering evidence of a criminal offense occurring, the NEOMED Police Department will be notified whereupon they may collaborate with other federal, state, and local law enforcement agencies as appropriate. A criminal investigation may be conducted in parallel to, may supersede, or may require further authorization for any additional actions to be taken by the University.

(G) INVESTIGATION

Breaches involving electronic data

For breaches of electronic data, the investigation will be the combined responsibility of the Information Technology Department and the NEOMED Police Department. The investigation will include (though not limited to) the following:

(1) Interviewing the person(s) who discovered the breach or potential compromise of data.
(2) Requiring the person who identified the breach fill out page 1 of an Incident Response Form (located at the end of this document).
(3) Collecting and preserving evidence such as:
  (a) Recording the scene, (either through photos or video)
  (b) Collect affected hardware,
  (c) Acquiring activity and/or access logs for the device,
  (d) Acquiring recent history of users of the device,
  (e) Retaining documentation of any associated alerts from security monitoring systems,
  (f) Obtaining video surveillance history and key swipe logs of area accessed without authorization, and
  (g) Maintaining chain of custody records for evidence collected.
(4) Determining the scope of the breach:
  (a) Determining if the breach is likely to be duplicated, or is beyond a single device,
  (b) Ceasing operation of certain hardware or physical areas where there is a reasonable belief the breach could be repeated, and
  (c) Providing alternatives to affected area to maintain business operations.
(5) Having the lead IT complete page 2 of the Incident Response Form.

Breaches involving non-electronic data

For breaches of non-electronic data, the investigation will be the combined responsibility of the Accounting Department and the NEOMED Police Department. The investigation will include (though not limited to) the following:

(1) Interviewing the person(s) who discovered the breach or potential compromise of data.

(2) Requiring the person who identified the breach fill out page 1 of an Incident Response Form (located at the end of this document).

(3) Collecting and preserving evidence such as:
   (a) Acquiring activity and/or access logs surrounding the breached data,
   (b) Acquiring recent history of users with access to the breached data,
   (c) Retaining documentation of any findings, and
   (d) Maintaining chain of custody records for evidence collected.

(4) Determining the scope of the breach:
   (a) Determining if the breach is likely to be duplicated,
   (b) Determining if there is a reasonable belief the breach could be repeated, and
   (c) Providing alternatives to affected area to maintain business operations.

(5) Having the lead accounting individual will fill out page 2 of the Incident Response Form.

(H) RECOVERY/EXTERNAL NOTIFICATION/REMEDIATION

The information gathered during the investigation will allow for assessment of functional impact, informational impact, and remediation.

(1) The Accounting Department will be responsible for the following:
   (a) Formally documenting of the event,
   (b) Consulting with Office of the General Counsel, Risk Management personnel, and Public Relations Department to determine notification procedures and credit reporting resources,
   (c) Coordinating a follow-up, and update, to the investigation within an appropriate time frame.

(2) The Information Technology Department will be responsible for the following:
   (a) Remediating any compromise to network or device security,
   (b) Documenting cardholder data including names and contact information of affected cardholders,
   (c) Providing backup and any necessary network, log, scan, and device data to any investigative body within the legal requirements,
   (d) Aiding in providing resources necessary for the University to coordinate communication to all entities listed within this plan.

(3) The University's Public Relations Department will be responsible for disseminating information to the media in consultation with the Office of General Counsel, the Accounting Department, and the Information Technology Department.

(I) EXTERNAL NOTIFICATIONS AND CARD ASSOCIATION BREACH RESPONSE PLANS

(1) Visa – Responding to a Breach

Initial Steps and Requirements for Visa Clients (Acquirers and Issuers)
https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

Notification

(a) 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.

(b) Within 48 hours, advise Visa whether the entity was in compliance with PCI DSS and, if applicable, provide appropriate proof of the PCI PA-DSS and PCI PIN Security requirements at the time of the incident..

Preliminary Investigation

(a) 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.

(2) 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.
http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf

(3) 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 two documents:

- American Express Data Security Operating Policy for Merchants
  - https://www209.americanexpress.com/merchant/singlevoice/pdfs/en_AU/DSOP%20AU%20for%20Merchants%204%2017_07%20.pdf
- American Express Data Security Operating Policy for Service Providers
  - https://www209.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Service_Provider_US.pdf