PCI DSS Incident Response Plan
for University of Tennessee Merchants

Revision: October 10, 2017

Purpose

The PCI DSS Incident Response Plan is to outline the key roles and responsibilities, requirements, and notification methods when any confirmed or suspected compromise or data breach has occurred with regards to hardware and/or software used for processing or transmitting credit card transactions.

Scope

This Incident Response Plan applies to all University of Tennessee system-wide merchants.

Key Roles and Responsibilities

Merchant

- In the event of any confirmed or suspected data breach or compromise, **immediately** contact local campus IT helpdesk.
- Does not access or alter confirmed or suspected compromised system(s).
- Does not turn off the confirmed or suspected compromised system(s).
- Isolates the confirmed or suspected system(s) from the network by unplugging the network cable only, or the phone cable if the POS appears to have been tampered with.
- Follows UT IT Policy IT0122 – *Security Incident Reporting and Response* once UTSA ISO has been given appropriate notification from PCI DSS.

Campus Chief Information Officer/Information Security Officer

- Is on high alert and monitors all systems within cardholder data environment.
- Notifies the UTSA ISO immediately of suspicious activity.
- Follows UT IT Policy IT0122 – *Security Incident Reporting and Response* once UTSA ISO has been given appropriate notification from PCI DSS.

University of Tennessee System Administration Information Security Office (UTSA ISO)

- Coordinates incident response and notification efforts—evidence gathering, forensics, evaluating the scope, and ensuring the communication between all the appropriate parties.
- Documents all actions taken, including dates and individuals involved.
- Maintains the *PCI DSS Incident Response Plan*.
- Provides PFI Reports, including the Final Incident Reports, to all appropriate parties.

Treasurer's Office

- Initiates and maintains contact with the acquiring bank.
- Coordinates communications with the acquiring bank and the UTSA ISO.
- Determines the official line of notification.

Acquiring Bank

- Assesses the information supplied by the Treasurer's Office.
- Determines if a Payment Card Industry Forensic Investigator must be called in.

Payment Card Industry Forensic Investigator

- Drives and performs all aspects of the forensic investigation.
- Does investigation report in a secure and timely manner.

Incident Response Plan Requirements for PCI v3.x

PCI DSS says that an incident response plan must be implemented. This incident response plan must contain procedures to verify that the university is prepared to appropriately respond to any confirmed or suspected breach.

It is critical to remember that any confirmed or suspected breach be reported immediately to the Treasurer's Office and/or the UTSA ISO. Do not allow access to the system and do not make any attempts to change the system until further notice has been given. PCI DSS has very strict rules governing who is to investigate confirmed or suspected PCI data breaches and will decide if it is to be done by a PCI Forensic Investigator. Any attempts by the university to investigate before being notified can result in substantial fines, as possible forensic data (i.e., what is stored in memory) can be lost.

Once PCI DSS has given official notification that the university can proceed with their own incident response plan, IT0122 – *Security Incident Reporting and Response* will be followed.

Definitions

- Acquiring Bank – The acquiring bank is the financial institution (i.e., Elavon) that provides merchants with payment card processing or merchant accounts.
- Compromise – A compromise, also known as a data breach, is an intrusion into a computer or system that can lead to an unauthorized disclosure or theft, modification, or destruction or cardholder data.
- Forensics – Forensics, as it relates to information security, is the application of investigative tools and analysis techniques to gather evidence from computer resources to determine the cause of data compromises.
- PCI Forensic Investigator (PFI) – A PFI is a company, organization, or other legal entity that is in compliance with all PFI company requirements and has been approved as a PFI by PCI SSC. Only those approved PFIs are permitted to perform PFI investigations and are listed on PCI SSC's website for the PFI Regions(s) for which they are permitted to work.
- POS – POS, or Point-of-Sale is the hardware and/or software used to process payment card transactions at merchant locations.