Clemson University
PCI Breach Procedures

1. Purpose

These procedures outline the steps to take when there is a data breach of University maintained cardholder information according to Payment Card Industry Data Security Standards (PCI DSS) and the University Computer Security Incident Response Policy.

2. Roles & Responsibilities

This document applies to all University personnel and assets.

Office of Information Security and Privacy (OISP) – A unit within the Clemson Computing and Information Technology (CCIT) division that is responsible for policies, standards, programs, and services relating to cybersecurity and information systems.

Office of Cash and Treasury Services – A unit within the Finance division that provides accounts receivable, banking, cash receipting, and merchant card services to the University.

Cyber Security Operations Center (CSOC) – A unit within the OISP responsible for ensuring information systems are sufficiently monitored to detect attacks and/or signs of potential attacks, including unauthorized access to the University's network.

IT Customer Services – A unit within the CCIT division that provides hardware, software, printing, applications and classroom technology support along with other IT services.

Clemson University Police Department – Investigate events related to criminal activity and serves as the liaison with external law enforcement agencies

Incident Management Team (IMT) – Ad-hoc team that responds to incidents which may have legal and or reputational consequences to the University. Team representatives include, but are not limited to, General Counsel, Risk Management, Communications, HR, Finance, Emergency Management.

3. Definitions

Cardholder Data – At a minimum, cardholder data consists of the full Primary Account Number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

Sensitive Authentication Data - Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

PCI Breach – Any situation where there has been unauthorized access to a system or network where cardholder or sensitive authentication data is collected, processed, stored or transmitted. A PCI Breach can also involve the suspected or confirmed loss or theft of any material or records that contain cardholder data.

4. Detection & Analysis

Suspected PCI Breaches must be promptly reported. The report can be made to the CCIT Support Center, or by sending an email notice to security@clemson.edu. All suspected PCI Breaches will be considered

Tier 2 according to the University Computer Security Incident Response Policy and will be handled by the IMT. For PCI breaches, the OISP will include Cash and Treasury Services as part of the IMT who will triage the incident.

5. Containment, Eradication & Recovery

The CSOC will be engaged to support technical measures related to the incident response. As part of the response they will immediately contain and limit the exposure of cardholder data and preserve evidence by taking the following steps:

1. Ensure compromised system is isolated from the network.
    a. Do not turn the compromised machine off. Instead, isolate compromised systems by unplugging the Ethernet cable or disabling wireless if possible. If using a wireless network, immediately contact the Payment Card Coordinator in the Office of Cash and Treasury Services at 864-656-0530 or cdorfne@clemson.edu to deactivate the Wi-Fi.
    b. 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).
2. Preserve logs and electronic evidence and document all actions taken.
    a. Gather, review and analyze all centrally maintained system, firewall, file integrity and intrusion detection/protection logs.
    b. Assist department in analysis of locally maintained system and other logs, as needed.
    c. Conduct appropriate forensic analysis of compromised system.
3. Determine potential vectors and risks
    a. Attempt to determine the source of the breach. Identify vulnerabilities, patch status, and potentially compromised accounts.
    b. Work with the departments to establish corrective actions as part of the eradication and recovery process.

Once the incident is contained, the IMT will review collected data and determine if a breach occurred. If a PCI breach is confirmed the IMT will identify the scope and affected individuals. The Payment Card Coordinator with the Office of Cash and Treasury Services will then contact the issuing banks as follows:

1. For incidents involving Visa, MasterCard or Discover network cards:
    a. Contact FirstData Merchant Services Account Manager at 301-766-5789 or sc.gov@firstdata.com within 72 hours of the reported incident.
2. For incident's involving American Express cards:
    a. Contact American Express Enterprise Incident Response Program (EIRP) within 24 hours after the reported incident at (888)-732-3750 or email EIRP@aexp.com.

6. Post Incident Activity

As part of the recovery process for Tier 2 incidents, a root cause analysis should be completed by the IMT to determine if additional policy, software, or hardware changes are required. If corrective actions cannot be implemented, they should be documented as a risk and approved by the Chief Information Officer.