University of Louisville's Credit Card
Payment Card Industry Data Security Standard
(PCI DSS) INCIDENT RESPONSE PLAN

Background:

The PCI Data Security Standard, published in January 2005, was the result of a joint initiative by VISA, MasterCard, American Express, Discover, Diners Club, and JCB to create a single security standard for storing and transmitting sensitive customer information.

Requirements

The PCI Data Security Standard applies to all members, merchants, and service providers that store, process or transmit cardholder data.

Steps and Requirements for the University and Compromised Merchant(s)

If a compromise is known or suspected to have occurred:

1. Immediately contain and limit the exposure. Contact your Tier 1 or Help Desk Support 502-852-7997 should you have any questions.

To prevent further loss of data, conduct a thorough investigation of the suspected or confirmed loss or theft of account information within 24 hours of the compromise. To facilitate the investigation:

- Do not access or alter compromised systems (i.e., don't log on to the machine and change passwords).
- Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable).
- Preserve logs and electronic evidence.
- Log all actions taken.
- If using a wireless network, change Service Set Identifier (SSID) on the access point and other machines that may be using this connection (with the exception of any systems believed to be compromised).
- Be on HIGH alert and monitor all Visa systems.

2. Immediately contact Merchant Services and/or the Information Security Office (treasury@louisville.edu; isopol@louisville.edu) **AND call a number below to leave voice mail.**

Contact Information:

Merchant Services:

- Brian Soverns, Asst. Treasurer, 502-852-8253
- Bev Santamouris, Controller, 502-852-6272

Information Security:

- Office, 502-852-8305
- Kim Adams, Chief Information Security Officer, 502-852-6692