DATE

PCI Credit Card Payment Security Policy & Procedures
OR
Payment Security Policy & Procedures (if cash/checks are included)

FOR: DEPARTMENT NAME
MERCHANT NAME if different
MID#'s and/or include MID #'s in Service Provider/Terminal section.

Name: *unless noted, the person listed is the owner of this document.*
Should anyone else be listed? Is anyone else mentioned in Reconciliation section?
Address:
City, State, Zip
Telephone 502-852-
Fax: 502-852-
Email address

Our policy and procedures are reviewed annually by (insert title) and reviewed with applicable personnel in (July or when??).

WEBSITE: Does your department have a website? Do you accept online payments?

SERVICE TYPE: list the methods accepted. Online payments, telephone payments, mail payments, faxed payments. *Note: email is not acceptable, so, should not be listed as an accepted method.*

Add a paragraph or two explaining what and why your department/school accepts credit card payments. Are they buying a tangible item? Are they registering for a camp or class? Think about how the registrant/payee/student even knows when to make contact? Will they receive a letter? Will they receive an email? What if they didn't attend the event previously, how will they find out about the current year's event? etc.…

CASH

- If you prefer, include cash procedures. Perhaps, the only item to note is that cash is not accepted.
- Is there a petty cash?
- Can anyone accept cash, or does it need to be a manager level?
- Is a receipt given?
- Where is the cash kept?

CHECKS/EFT/ACH

- If you prefer, include check/EFT procedures. Perhaps, the only item to note is that checks are not accepted.
- Who is check made out to?
- Is a Student ID needed? If so, what do you put on the check?
- Is a receipt given?
- Where is the check kept?

CREDIT CARDS

Payments:

- Insert accordingly here based on how you accept credit card payments. Subsection for each way your accept payments (online, in-person, etc.).
- Be sure to include which card brands are accepted. Keep in mind, Visa, MasterCard, Discover are automatic. American Express is optional.
- List how you do NOT accept credit card payments. For instance, if you only have online payments, then you don't accept In-Person, mail, telephone, fax, or email.
- No one should copy, move or store any cardholder data onto local hard drives or removable electronic media.
- Do you save any documentation with full credit card data, short-term or long-term? If so, how do you protect this information during this timeframe?
- How is full credit card data destroyed?

Refunds:

- How are refunds handled?
- What do you need to issue a refund?
- Is a receipt sent?

TERMINAL SUPPORT ….OR……SERVICE PROVIDERS

- List any software application vendors, gateway vendors, contact information, date of agreement. Is this an annual agreement?

…OR….

- List the name and phone number for terminal support.
- List Merchant ID (MID) numbers. Elavon/US Bank; if applicable, American Express

TERMINAL INFORMATION …… OR ….. WEB SITE FLOW

- Credit Card terminal make (Ingenico or VeriFone)
- Terminal model (iCT250, iWL250, Vx520)
- Serial number (Listed on back of terminal)
- Wall jack information, color and number of (port where terminal is plugged into the wall.

…OR….

- Document the website flow from beginning website to end, so, exactly how the registrant/payee will log on, maneuver through the site to register/pay. Think about

how the payee even knows when/where to go? Will they receive a letter? Will they receive an Email? What if you didn't attend the event previously, how will they find out about the event?

For Example:

- Previous year registrants receive email with link to: http://louisville.edu/finance/controller/treasurymgmt/
- Choose Events tab *(did website address change/redirect? If so, copy & paste)*
- Choose specific Event *(did website address change/redirect? If so, copy & paste)*
- Registrant completes form and clicks 'Pay Now', and redirected to: https://crdtcrd.louisville.edu/CC/.....
- Credit card information is entered and clicks 'Submit.
- Registrant receives pop-up confirmation.
- Registrant is automatically redirected back to: http://louisville.edu/finance/controller/trasurymgmt/

TERMINAL TAMPERING VERIFICATION

If applicable, indicate who will be periodically (weekly?) checking for terminal tampering, such as checking serial number, no additional cords, no scratches, on back of terminal.

RECONCILIATION

Daily

- Show the daily reconciliation procedures.
- Show the separation of duties from accepting payments and reconciling.

Monthly

- Show the monthly reconciliation procedures by comparing the monthly US Bank/Elavon statement (American Express statement also if applicable) to the University Reports.
- Show the separation of duties from accepting payments and reconciling

INCIDENT RESPONSE PLAN

- Any suspicious activity should be reported to the **(insert Contact Name and Title)** immediately.
- Who will contact me? Jill Riede, Merchant Services Manager, 502-852-0892. jmried02@louisville.edu
- Who else will you contact internally? Who would you contact if your website is down, not necessarily credit card payments?
- Any Service Providers for Third party vendors to contact?

BACKGROUND: The Payment Card Industry Data Security Standard (PCI DSS) is an industry regulated compliance initiative that dictates security standards for merchants and service providers for the safe handling of credit card information. As a merchant, the University of Louisville has an obligation to protect the sensitive financial information, such as credit card data, of its customers.

PROCEDURE: Per the Payment Card Industry Security Standards Council (PCI SSC), each department that handles credit/debit card information must have documented procedures for complying with the current version of the PCI DSS.

PURPOSE: In order to ensure that credit card activities are consistent, efficient and secure, the **INSERT DEPARTMENT NAME** has adopted the University's Credit Card (PCI) Policy and supporting Procedures which apply to all types of credit card activity, whether in-person, telephone, mail, fax and/or the internet. The PCI Policy provides guidance so that credit card acceptance complies with PCI DSS and must be implemented and strictly enforced in order for our department to continue accepting credit cards for payment. The university's reputation would be seriously damaged by the exposure of card numbers.

COMPLIANCE: Negligent or fraudulent activity by any employee will adversely affect our department and users; therefore, it is the responsibility of each employee to become familiar with and adhere to the University and Department's PCI Policy and Procedures. Any person found to be involved in fraudulent activity will be terminated with possible criminal charges filed.

ACKNOWLEDGEMENT: I hereby acknowledge that I have read the payment policy and procedures and understand my responsibilities as they relate to PCI DSS and the protection of credit card information.

Employee Name: (PRINT) _____

Employee Signature: _____

Date: _____

Department Head Name: (PRINT) _____

Department Head Signature: _____

Date: _____