PROCEDURES RELATED TO PCI-DSS FOR:

(please fill in the name of your department here)

Purpose: To comply with Payment Card Industry Data Security Standards (PCI-DSS) as well as good business practices related to the handling of our customers' credit card information.

Credit Card Data Handling

- Cardholder data will be treated as confidential. At a minimum, cardholder data consists of the full PAN (primary account number). 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.

- We will not store any card-validation code (i.e., the three- or four-digit code) used to validate a card-not-present transaction, personal identification number (PIN) or encrypted PIN block.

- Account numbers will be masked if and when displayed (i.e., no more than last four digits of credit card number).

- All employees handling cardholder data must have annual PCI DSS compliance training.

- Perform routine visual inspections of every device, looking for potential signs of tampering. Keep track of any operational difficulties that begin happening on a regular basis. If you notice these or anything out of the ordinary, stop using the device immediately and disconnect it from the POS device or network, but do not power it down. Immediately contact the campus central business office and campus central IT office. Some examples of things to look for include:
    - Damaged or altered tamper seals
    - Missing manufacturer labels
    - Missing screws or screws with damaged heads
    - Incorrect keyboard overlays
    - External wires
    - Holes in the device housing
    - An electronic serial number that does not match the number printed on the bottom of the device
    - A high number of mag-stripe read failures or debit card declines
    - Difficulty inserting a chip and PIN card into the EMV slot

- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.

- Do not install, replace, or return devices without verification.

- Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).

- Report suspicious behavior and indications of device tampering or substitutions to appropriate personnel (for example, to a manager or security officer).

- When employees have access to payment card data, whether accepted via telephone, in person, or through other non-electronic methods, the data must be secured before employees leave their workstations for any purpose.

- If possible, at the end of each business day, all POS devices will be locked up in a secure place that can only be accessed by those who need to access the devices.

- Data that is not absolutely necessary in order to conduct business will *not* be retained in any format (e.g., paper or electronic).

- If data must be written down, use the standard credit card authorization form found on the campus central business office website under PCI. Print this form out on bright paper, so that staff will know what it is by color.

- We will not accept, request, or retain such data via e-mail (or similar messaging system), fax, voice mail or other electronic means.

- Physical access to records will be restricted to staff with a "business-need-to-know". Means such as locked file cabinets and restricted file rooms as well as restricted distribution of such records will be used. Secure storage containers, if any, used for materials that are to be destroyed.

- If external media or couriers are used to transmit or transfer such data, we will use means that enable tracking of the data. Any transfer using these or similar means will be approved by appropriate levels of management before the fact.

- We will cross cut shred any data.

- If such data is shared with any external service provider, we will ensure that:
    - A list of providers is maintained and any changes sent to the campus central business office;
    - A written agreement is executed and retained which defines the provider's responsibility related to the security of this information, with a copy sent to the campus central business office;
    - Any new service provider will be thoroughly vetted by departmental management, the campus central business office and others as appropriate, before engagement to ensure that the provider can meet these requirements.
    - Every service provider's PCI-DSS compliance status is reviewed on an annual basis, with a copy sent to the campus central business office. Instances of non-compliance are reported to the campus central business office personnel for assistance in determining appropriate follow-up actions.

<u>System Configuration at the Department Level</u>

We will ensure, through working with our campus central IT office and others as needed, that:

- Anti-virus software will be implemented, updated, and run at regular intervals.

- Vendor patches will be installed on a timely basis.

- Access will be granted to systems only on a "business-need-to-know" basis.

- Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:
    - Generic user IDs are disabled or removed.
    - Shared user IDs do not exist for system administration and other critical functions.
    - Shared and generic user IDs are not used to administer any system components.

- If external vendors need remote access to service our third-party software, their access will be granted only for the time needed to do the necessary task(s) and then immediately disabled.

Note: These procedures apply to all technologies, processes, and personnel that relate to the processing of this information. We will ensure that all personnel affected by these procedures are aware of these responsibilities on at least an annual basis. System and device functionalities established for credit card data activities of the university may be used only for credit card data activities of the university, not for personal use. This document will be reviewed on an annual basis and modified as necessary to reflect current business practices and new legal or regulatory requirements. In the event a breach of this information is suspected or confirmed, we will call the campus central business office and the campus central IT office to ensure that the appropriate disclosure protocols are followed.

Date last reviewed: _____