ACCEPTING CREDIT CARD AND ELECTRONIC PAYMENTS (CREDIT CARD MACHINES AND MERCHANT ID'S)

1. Standards

The following responsibilities are an important aspect of the University's compliance with the Payment Card Industry Data Security Standards (PCI DSS). Any department collecting revenue on behalf of the University is considered a Merchant Department. The Merchant Department must designate an individual who will have primary authority and responsibility for revenue collection within that department. This individual will be the designated Merchant Department Representative or "MDR".

All Merchant Departments must:

1. Complete the application to become a Merchant Department (see Additional Resources below).
2. Follow the Card Acceptance Guide (or similar rules) of the merchant processor/acquirer (e.g., Global Payments) and the operating regulations and rules of any card associations/networks that will be accepted by the Merchant Department (e.g., MasterCard, Visa, etc.). Links to Global Payments, MasterCard, Visa, and American Express are provided for reference:
   - Global Payments Card Acceptance
     https://www2.globalpaymentsinc.com/GPDB
   - MasterCard Worldwide Rules and Chargeback
     http://www.mastercard.com/us/merchant/support/rules.html
   - Visa Merchant Responsibility and Card Acceptance Guide
     http://usa.visa.com/merchants/new_acceptance/merchant_responsibility.html
   - American Express Card Acceptance Guide
     https://www.americanexpress.com/us/content/merchant/get-support/guidelines
3. Revenue collection arrangements that require payees to enter credit card numbers on preprinted order forms which are then mailed or faxed to a UT Tyler department must be locked in a secured area.
4. Fax Transmissions (both sending and receiving) of credit card and electronic payment information are limited to those fax machines whose access is in a restricted area and whose access is restricted to authorized users.

5. Ensure that all credit card data collected including but not limited to account numbers, card imprints, and Terminal Identification Numbers) is secured. Data is considered to be secured only if the following criteria are met:
    - Only those with a need-to-know are granted access to credit card payment data.
    - Email is not used to transmit credit card payment information. If the use of email is necessary, only the last four digits of the credit card number are displayed.
    - Credit card or electronic payment information is never downloaded onto any portable devices such as USB flash drives, compact disks, laptop computers or personal digital assistants.
    - The processing and storage of personally identifiable credit card or electronic payment information on University computers and servers is prohibited.
    - Only secure communication protocols and/or encrypted connections are used during the processing of electronic transactions. For compliance, credit cards must be connected to a telephone line or a third party that does not use The University's network. NOTE: The UT Tyler Information Security Department maintains a staff of security professionals who are available, as required, to provide consultative services on appropriate security practices. The Director of Information Security can be contacted for more information regarding these services.
    - The three-digit card-validation code printed on the signature panel of a credit card is never stored in any form.
    - The Primary Account Number (PAN) is masked when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only personnel with a legitimate business need can see the full PAN.
    - Unprotected PANs are not to be sent via end-user messaging technologies.
    - All credit card and physical copies of data that is no longer deemed necessary or appropriate to store is destroyed or rendered unreadable.
    - All computers accessing or providing support for the web based marketplace must be encrypted with University standard encryption product. All discovered instances of the full credit card number, bank account number, or social security number must be reported to the Department Head, Cash Manager, and the Information Security Office and remedied immediately.
    - No credit card receipt or other document referencing the transaction shall include more than the last four digits of the account number or the month and year of the expiration date.

No University employee, contractor, or agent who obtains access to credit card or other personal payment information may sell, purchase, provide, or exchange said information in any form to any third party other than to the University's acquiring bank, depository bank, Visa, MasterCard or other credit card company, or pursuant to a government request. All requests to provide information to any outside party must be reviewed and approved in advance by the Vice President for Administration or his delegates.

2. Process

The MDR must follow the steps below in order to request approval to become a Merchant Department:

1. Notify the Cash Manager in the Office of Financial Services of a need to accept credit card and/or electronic payments by completing an application to become a Merchant Department.
2. Obtain approval from the Department Head. It is the responsibility of the Department Head to approve business case and all other information provided in the application, and to approve the designation of the Merchant Department Representative.
3. Submit the signed application to the Vice President for Administration for review and approval.
4. If the application is approved, the Cash Manager will forward a request to University Web Services to coordinate designing a payment web page with the Merchant Department unique to the Merchant Department's needs. The Merchant Department should allow sufficient time for this process to be completed.
5. Departments may only use credit card processing solutions and/or devices to accept credit card payments approved by the Director of Information Security, Vice President for Administration, and Cash Management. Departments that want to use an outside approved third party card processing solution and/or device to accept credit card payments must annually obtain verification of the PCI DSS Compliance Certification.
6. The MDR must contact the Information Security Office to schedule installation of University standard encryption product on the computers that will access or support the web based payment webpage.
7. The Cash Manager will arrange the necessary training for The Merchant Department, as well as any additional information pertinent to the approved payment method.
8. The Cash Manager will retain Merchant Department applications, add location forms, and any other correspondence related to adding a Merchant ID as long the Merchant ID is active.

3. Training and Inspection

Upon final approval of an Application to Become a Merchant Department, the MDR's will receive training to be aware of suspicious behavior and to report tampering or substitution of devices.

Cash Management will maintain an inventory of credit card devices including location and responsible party. Policy and procedures require that devices maintained are periodically inspected to look for tampering or substitution.

4. Annual Assessment

The Information Security Officer will collaborate with the Cash Manager and MDR's to complete the annual assessment and improvement process required by PCI DSS Standards.

5. Exceptions

Any exception to this published policy or procedure will be considered on a case by case basis, by the Director of Information Security, Business Administration, and Cash Management.

6. Additional Resources

Application to Become a Merchant Department
PCI Data Security Standards
Cash Management and Banking Services- HOP 4.6.2
UT System Information Use and Security Policy- UTS165
Accepting Credit Card and Electronic Payments- HOP **(DRAFT)**