POLICY & PROCEDURE DOCUMENT

NUMBER: 3.3101

DIVISION: Finance & Administration

TITLE: Policy & Procedures for Credit Card Merchants

DATE: April 10, 2017

Authorized by: VP for Finance & Administration
Issued by: Office of the Bursar in association with the PCI Committee

I. Purpose and Scope

In order to ensure that credit card activities are consistent, efficient and secure, the University has adopted the following policy and supporting procedures for all types of credit card activity transacted, whether in-person, over the phone, via fax, mail or the Internet. This policy provides guidance so that credit card acceptance complies with Payment Card Industry Data Security Standards (PCI DSS), which can be found at: https://www.pcisecuritystandards.org/
Users of this policy should also refer to the PCI Policy 3.3201 for further details regarding PCI compliance at the University.

II. Policy

A. Applicability

Any University employee, contractor or agent who, in the course of doing business on behalf of the University, is involved in the acceptance of credit card payments for the University, is subject to adherence to this policy. Failure to comply may result in disciplinary actions for any involved employee (in accordance with Human Resources Policies and Procedures), termination of a contract with a contractor or agent, or limitation of a department's credit card acceptance privileges.

B. Merchant Department

Any department accepting credit card payments on behalf of the University for gifts, goods or services, (the "Merchant Department"), shall designate an individual within that department who shall have primary authority and responsibility for credit card transaction processing. This individual shall be referred to as the Department Contact and shall ensure that all credit card data collected by the Merchant Department in the course of performing University business, regardless of how the payment card data is stored, is secured. Data may be physical or electronic, and includes, but is not limited to, card imprints and account numbers.

No University employee, contractor or agent who obtains access to payment card or other personal payment information in the course of conducting business on behalf of the University may sell, purchase, provide or exchange said information in any form to any third party other than to the University's merchant card processor, depository bank, VISA, MasterCard or other credit card company, or pursuant to a government request. This includes, but is not limited to, imprinted sales slips, photo or carbon copies of imprinted sales slips, mailing lists, tapes, or other media obtained by reason of a card transaction. All requests to provide information to a party outside of the department shall be coordinated with the Cashier's Office in the Office of the Bursar.

C. Card Industry Data Security Standards (PCI DSS) Compliance

1. All University Merchant Departments must comply with PCI DSS. These standards may be found at the PCI Security Council website.
2. Annually, every merchant of the University must submit to the Office of the Bursar a completed PCI DSS Self-Assessment Questionnaire, also known as an "SAQ." Additionally, the merchant departments will be subject to remote vulnerability network scans, server scans and application scans performed by the WKU IT Department and/or approved third parties.
3. All University Merchant Departments should refer to the University's PCI Policy 3.3201 for further details regarding PCI compliance.

III. Procedure

A. Implementation

1. The Department shall take the following steps to implement payment card processing at the University.

   a) Read these procedures thoroughly.

   b) Complete and sign the Application for a Credit Card Merchant Number.
   Application

2. After verifying all information is correct and signing the application, it shall be submitted to the Office of the Bursar.

3. The Bursar's Office is responsible for final review. After the application has been approved, the applicant will be given the appropriate SAQ to complete.

B. Equipment and Supplies

1. Equipment (i.e., swipe terminals or manual imprint machines) for processing credit cards shall be PCI compliant and will be acquired by coordinating with the Bursar Specialist in the Office of the Bursar.
2. Installation of equipment should be coordinated with the University's IT Security personnel.

3. Any equipment no longer being used to process credit card transactions must be returned to the Cashier's Office and signed in by Bursar Office personnel.

4. All departments must notify the Office of the Bursar prior to a change in location of credit card terminal(s).

C. Software and e-Commerce

1. Any department with a need to accept credit cards through the internet via a web application (e-Commerce) must contact the Bursar Specialist within the Office of the Bursar to coordinate web-based payment solutions with the payment processor under contract with the University.

2. Server-based software applications and point-of-sale (POS) systems (i.e. cash registers, event ticket distribution) that collect and transmit credit card data for payment must be certified as PCI DSS compliant. Any department interested in implementing a server-based software application or POS system in order to accept credit card payments must notify the Bursar and the IT Department (IT Security team) to ensure PCI DSS compliance.

D. Card Association Rules and Regulations

Visa, MasterCard, Discover and American Express are the only credit cards that may be accepted. Merchant Departments are expected to comply with the rules and regulations set forth by each of the card associations in the processing of credit card payments. Each card association's rules and regulations can be found on their company websites.

VISA

MasterCard

Discover

American Express

The card associations may impose fines or revoke the privilege of accepting credit cards for not complying with their rules and regulations.

E. Associated Costs

Merchant Departments are responsible for all costs associated with the acceptance of credit cards including costs associated with installation, supplies and equipment, as well as processing fees. For additional information regarding costs and fees, refer to the application form. Departments are also responsible for any credit card transactions that are disputed and charged back to the University.

F. Review of Merchants

Periodic reviews of Merchant Departments will be coordinated by the Cashier's Office. Additionally, credit card handling procedures are subject to audit by Internal Audit. Merchant Departments not complying with approved safeguarding and processing procedures may lose the privilege to serve as a credit card merchant.

G. Security

1. Security breaches can result in serious consequences for the University, including release of confidential information, damage to reputation, added compliance costs, substantial fines, possible legal liability and the potential loss of the ability to accept credit card payments.

2. Departments that accept credit cards are responsible for ensuring all credit card information is received and maintained in a secure manner in accordance with the payment card industry standards. Individual departments will be held accountable if monetary sanctions and/or card acceptance restrictions are imposed as a result of a breach in PCI compliance.

3. Under no circumstance shall credit card information be obtained or transmitted via email. Credit card information shall not be stored on individual PCs or servers that have not been deemed PCI compliant. All hard-copy credit card information must be stored in a manner that would protect the individual cardholder information from misuse.

4. Credit/debit card payment information should be kept secured and confidential at all times.

    a. Credit/debit card information should be secured in a locked area (room or closet).
    b. The area designated to store credit/debit card information should be restricted to the department designee responsible for processing or researching a transaction.
    c. Any credit/debit card point of sale terminal should be placed in a secure area to prevent access to data within the terminal.
    d. If the secured location is within an office, where other employees have access, it is recommended to store the information in a locked file cabinet or desk.
    e. Access to credit/debit card data should be restricted to those individuals whose job requires such access.
    f. A privileged user access form will be maintained by the department and reviewed or updated annually or as needed.

5. All but the last four digits of the account number should be marked through (redact) when displaying a cardholder data receipt that includes the merchant and customer copy and any other form that may contain credit/debit card information.

6. Pin pads or any magnetic strip readers should not be attached to a credit/debit card terminal or computer. Credit/debit card information may not be stored in any device used for credit/debit card processing.

    a. Security data/track is defined as the data elements stored within the magnetic stripe on the back of a card, as well as the cardholder validation code (the three or four digit value printed on the signature panel of the card).
    b. The information includes all the data required to commit fraud on a cardholder's account.
    c. The only data a merchant may store is the cardholder's name, account number, expiration data and authorization code. Once authorization has been received the data must be deleted.

7. Credit/debit card payment information cannot be stored on computers or networks, regardless of encryption.

8. Credit/debit card information must be transmitted and received in a secure manner.

a. If your department received credit/debit card payment information by fax and/or mail, all digits of the card number except the last four, must be marked through before retaining for your records.
b. Credit/debit card information should not be sent to a fax application with an IP address.
c. Fax machines should be in secured area (room with a locking door) with no through traffic and with limited access.
d. Credit/debit information should not be received by email.
e. Credit/debit card information should never be sent via text message.

9. Credit/debit card receipts should be stored according to WKU's record retention schedule. All receipts must be shredded after that time.

10. All credit card terminals should be regularly inspected for signs of tampering or substitution. If tampering is discovered, contact the Office of the Bursar immediately.

H. Process for Responding to a Security Incident

In the event that a merchant knows or suspects that credit card data, including card number and card holder name, has been disclosed to an unauthorized person or stolen, the Merchant Department shall immediately take the following steps.

1. The department contact or any individual suspecting a security breach shall immediately report the issue by completing the IT Security Form.

2. If an actual breach of credit card data is confirmed, the IT Department shall alert the Western Kentucky University Police Department, the Director of IT and any relevant regulatory agencies of the breach.

IV. Related Policies

See also:

3.3011 - Cash Operations
3.3201 – PCI Policy

WKU

WESTERN KENTUCKY UNIVERSITY
APPLICATION FOR CREDIT CARD MERCHANT NUMBER

Name: ____________________________________ Title:_____________________

Dept. Name: ________________________________ Banner Index: ______________

College/Division: ____

Mailing Address: ____

Email: ____________________ Phone #: _____________ Fax #: _______________

Describe the goods, services and/or gifts for which you will receive payments. Please be specific:

Is this an existing or new source of revenue?

Explain why your department wants to accept credit card payments.

Describe the frequency of credit card payments. Is this a one-time event? Are payments for seasonal or year-round activity? Provide detailed timeframes.

Will credit card be the sole method of payment? If not, what other methods of payment do you anticipate accepting for this specific purpose?

How do you plan to process these payments? (check all that apply)

□ In-person (card present) □ Mail/phone/fax order* □ Internet

**Note: Credit card data should never be transmitted via e-mail correspondence. Faxes must be secure.*

Which equipment do you need to process credit cards?

□ Credit Card Terminal (VX520 or ICT220 – $269-$299 plus $100 set up fee)
Usage fees: 1.84% of total charges

□ None* **Note:When processing credit cards via the internet, no equipment is required.*

If you are planning to accept credit card payments via the Internet, please provide the following information:

3rd Party Online Payment Gateway Processor (i.e., Authorize.net): ____________________
Authorize.net Usage fees: $99 license setup fee, $24.95 monthly charge plus 1.84% of total charges plus $0.06 per transaction, $0.06 per batch.
Note: all costs and fees subject to change

Please indicate the estimated annual dollar volume and number of transactions for each applicable credit card acceptance process:

In-person $__________________ # of transactions __________________
Mail/phone/fax $__________________ # of transactions __________________
Internet $__________________ # of transactions __________________

Who will be the Department Contact who is responsible for managing credit card transaction processing?

Name: ____ Title:____________________
Phone Number: ____________________ Email: ______________________________

Will any other departments, software packages or outside vendors be involved in the processing of credit card payments? If so, please identify all parties and describe their roles and responsibilities.

By signing this form, the Department Contact acknowledges that he/she understands his/her role as outlined in the University's Procedures for Credit Card Merchants and accepts the responsibility of that role. Additionally, the Department Contact recognizes that the liability for a breach is accepted by the Merchant Department should a breach occur due to negligence of the department to adhere to the University's Procedures for Credit Card Merchants.

By signing this form, Supervisor approves of the business case presented for the department to become a Merchant Department, the Departmental information provided, and the designated Department Contact.

Signatures: ______________________ ____________________________
Department Contact Supervisor

Date: ______________________________

Please submit completed form to:
Bursar Specialist
Office of the Bursar
208 Potter Hall
Western Kentucky University
1906 College Heights Blvd #11022
Bowling Green KY 42101-1022

For Office of the Bursar use only

Date application received: __________________________________
Merchant Account Number: _________________________________
Date merchant number received from BB&T: ____________________
Processed by: ____