POLICY & PROCEDURE DOCUMENT

NUMBER: 3.3201

DIVISION: Finance & Administration

TITLE: Payment Card Industry (PCI) Data Security Standard (DSS) Compliance

DATE: April 10, 2017

REVISED: N/A

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

I. Purpose and Scope

The purpose of this policy is to educate all Western Kentucky University related members of the payment chain about the importance of ongoing security of cardholder data and how the ongoing security assists in the compliance with the current PCI DSS standard. The PCI DSS is a global security standard assembled by the Payment Card Industry Security Standards Council. The security standard applies to all organizations that store, process or transmit cardholder data. Compliance is enforced by the founding members of the Council: Visa, Inc. MasterCard Worldwide, JCB International, Discover Financial Services and American Express.

The primary function of the PCI DSS is to protect everyone in the payment chain, including: merchants, service providers and consumers. The standard focuses on protecting the members of the payment chain from damages resulting from theft or loss of cardholder data.

Any University employee, student, department, third party vendor, contractor or agent who, in the course of doing business on behalf of the University, is involved in the acceptance of, the handling of or the receiving of credit card information, is subject to adherence to this policy. Failure to comply may result in disciplinary actions for any person involved (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 (See also Section III Procedures, Part C. Sanctions).

II. Policy

<u>A. Merchant Responsibilities</u>

1. Departments that accept and process of credit cards for payment of goods or services must design adequate processes to ensure the following are maintained:

a. Approval of the Bursar and the IT Department before entering into any contracts or purchases of software and/or equipment related to credit card processing. This requirement applies regardless of the transaction method/technology used (e.g. POS device). Departments should review the University's current policy regarding hardware and software acquisitions (See Policy 5.5044)

b. Compliance with the Payment Card Industry Data Security Standard, which includes completing the appropriate type of Self-Assessment Questionnaire ("SAQ") on an annual basis.

c. Establishment of departmental procedures for safeguarding cardholder information and secure storage of data, if applicable.

d. Transmission of credit card data NOT in an unsecure manner such as by e-mail, email attachments, text, unsecured or stored fax, or through campus mail.

e. Storage of sensitive cardholder data NOT in any University system, personal computer, or e-mail account.

f. Performance of background checks prior to hiring any positions with access to cardholder information.

g. Requirement for all personnel involved in credit card handling attend card security training annually in conjunction with PCI assessments.

h. Requirement for all personnel involved in credit card handling to annually review and acknowledge the University's policies related to PCI DSS compliance, cash operations and credit card merchants.

i. Update the Office of the Bursar when new individuals are given authority to process credit card transactions and when an individual's authority is taken away (e.g. when an individual leaves the department or University).

2. Third Party Vendors that accept and process of credit cards for payment of goods or services must ensure the following when doing business on campus:

a. Adherence to PCI security requirements and provide proof of PCI certification to the merchant department it's associated with or directly to the PCI committee.

III. Procedure

A. Obtaining and Maintaining Merchant Status

1. All credit/debit card processing contracts and renewals, including web based procurement, must be initiated through the Office of the Bursar.

a. An Application for Credit Card Merchant Number form should be completed and submitted for approval.

b. Once approved, the Department contact (the individual in the department designated with primary authority and responsibility for credit card transaction processing) and all other individuals with delegated authority to process transactions shall complete all relevant training courses prior to accepting credit card payments.

2. All departments approved to accept credit cards for payment ("merchant department") will be subject to an annual inspection by the University's PCI Committee, which includes a representative from the University's IT Department.

3. All merchant departments will be required to complete the appropriate SAQ in a timely manner. The SAQ document and PCI Compliance affirmation documentation shall be retained at the department level for audit purposes.

B. Training

1. The Department contact shall be responsible for maintaining records of all training completed by all individuals in the department with authority to process credit card transactions.

2. The Department contact shall notify the Office of the Bursar when any new individuals are given the authority to process credit card transactions within the department or when an individual leaves the department or University.

3. All documentation related to any training performed and completed by the Department Contact and other individuals shall be maintained by the Department Contact for audit purposes. The retention period should match the University's record retention policy.

4. The frequency of all training related to credit card transaction processing shall be required based on the PCI DSS standards.

C. Sanctions

1. Departments not complying with this policy may lose the privilege to serve as a merchant department.

2. Violations carry fines of $10,000 to over $500,000 per incident potentially imposed by the affected credit card company, which will be the department's responsibility.

3. Persons in violation of this policy are subject to a range of consequences, including loss of computer or network access, disciplinary action, suspension, termination of employment and legal action.

IV. Related Policies

See also:

Policy 3.3101 – Credit Card Merchants