FAYETTEVILLE POLICIES AND PROCEDURES 309.0

Payment Card Processing

Any office engaged in any form of payment card processing (e.g., POS/swipe or e-commerce) must have the approval of Financial Affairs Credit Card Operations and Cash Management prior to engaging in commerce activity. No University department may enter into any contracts or otherwise arrange for payment transaction processing, or obtain any related equipment, software or services without the involvement and approval of Credit Card Operations and Cash Management.

All payment activity must be established within the centralized University banking and accounting environment with receipts deposited into designated University of Arkansas bank accounts, unless an exception is approved by the Associate Vice Chancellor for Financial Affairs.

The University of Arkansas official online payment system is QPay. All departments wishing to accept online payment card transactions must use QPay, unless a waiver by Credit Card Operations is granted to that department (*See Payment Card Usage section below for additional information*).

The purpose of this policy is to outline the payment card acceptance methods suitable for university business and the usage restrictions for payment card transactions. Credit Card Operations is responsible for campus compliance with payment card processing and security regulations, and is granted authority to take appropriate action to ensure conformity with University policies and procedures. Appropriate action up to and including suspension or termination of payment card processing activities will be imposed for any University of Arkansas department that violates provisions outlined in the Fayetteville Policies and Procedures 309 series related to payment card processing, security and incident reporting.

Definitions

All terms mentioned in this policy are described in the Payment Card Policies Glossary for the 309 policy series. All campus users of payment card information are required to know and fully understand all terms associated with the 309 policy series.

Payment Card Usage

The University of Arkansas accepts Visa, MasterCard, Discover Card, and American Express payment cards for university business. In addition, departments that accept payments for activities that directly relate to the educational mission of the University may have the option to accept PINless debit transactions for Star, NYCE or Pulse branded cards. University of Arkansas accepts payment ONLY via telephone, walk-in traffic or an approved online portal.

If a department has a specific business operational need that QPay cannot meet, the department can apply for a System Usage Waiver. Departments initiate the waiver request by submitting written justification to Credit Card Operations that explains their need and why QPay cannot adequately support the operation. Waiver requests must be submitted annually to Credit Card Operations, and are evaluated on a case-by-case basis. As part of the waiver application process,

Credit Card Operations will conduct a full evaluation of proposed equipment, network structure and remote access privilege use.

In addition, departments applying for a System Usage Waiver must achieve and maintain full compliance with the Fayetteville Policies and Procedures 309 series, legal and industry regulations. A full list of requirements is available in the System Usage Waiver supplement document provided by Credit Card Operations. Any department granted a waiver is responsible for the fiscal costs associated with payment card security as detailed in the Fayetteville Policy and Procedure 309 series.

Acceptable Technology

Credit Card Operations does not publish a list of acceptable technology. Technology usage for each processing environment is evaluated on a case-by-case basis. University of Arkansas departments authorized to accept payment card transactions MUST supply Credit Card Operations with an inventory of all equipment to be used in the processing environment prior to authorization and assignment of merchant account. The inventory shall include –a description of the device, the model number, operating system or firmware information and a DNS/IP address, if applicable. Reports available in the University's Asset Inventory Management System (AIMS) are acceptable. Departments must notify Credit Card Operations within 7 days of any changes in processing equipment

The use of wireless or cellular technology for payment card processing is prohibited. Any wireless capable laptop used in the processing environment MUST have the wireless radio disabled while in use within the department processing environment. The use of mobile devices, other than a wired laptop, for payment card processing is prohibited.

As a convenience to customers, departments are permitted to maintain self-service kiosk stations, limited to accessing only the payment application, for customer use while in the department. Credit Card Operations must approve the kiosk technology and equipment prior to use within the payment processing environment. The kiosk is never to be used for web surfing, email use or any general university applications that do not directly relate to payment processing.

Departmental staff members are prohibited from using Remote Desktop Protocol (RDP) or any Terminal Services application to remote into their campus workstation from another computer to complete a payment card transaction. All terminal services must be disabled while the workstation is in used within the payment card processing environment.

User Access to Processing Environments

Departments authorized to accept payment card transactions will have one or more payment card merchant accounts established by Credit Card Operations. All payment card transactions for the department will flow through this account. As a condition of merchant account assignment, all requirements detailed in the Payment Card Security Policy of the 309 series MUST be met.

Access to the Cardholder Data Environment will be restricted by job duties of each individual. Every user must be assigned a unique User ID and password to access the Cardholder Data Environment. Passwords for users MUST be changed every 90 days. User accounts must also be

locked after at a maximum 3 failed login attempts. Accounts inactive for at least 90 days must be removed or locked.

Fees

Each department is responsible for the costs incurred by the University to process its transactions, plus setup fees for any new merchant account. Processing fees will be deducted monthly from a BASIS company cost center. A current fee schedule can be obtained from Credit Card Operations.

In addition, each department is responsible for any hardware, software, setup and/or maintenance costs to maintain the processing environment, including the cost of security scans. Departments may also be required to pay for training and background checks as required by Fayetteville Policies and Procedures.

November 19, 2010