Payment Card Security

Credit Card Operations has primary responsibility for campus compliance with payment card processing and security regulations, and is granted the authority to take appropriate sanctions to ensure conformity with University policies and procedures. Appropriate action up to and including suspension or termination of payment card processing privileges will be imposed for any University of Arkansas department that violates provisions outlined in Fayetteville Policies and Procedures 309 series related to payment card processing, security and incident reporting.

The purpose of this policy is to establish procedures for securing payment card transaction data, so that the University of Arkansas can seek to ensure that sensitive account and personally identifiable information customers provide is protected against theft and/or improper usage. Additionally the policy seeks to ensure that the University complies with credit and banking industry security regulations related to credit card processing and reporting, including PCI DSS. This policy applies to all University of Arkansas, Fayetteville departments, employees (including temporary), contractors and consultants. Affiliated entities are encouraged to comply.

Definitions

All terms mentioned in this policy are defined 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.

Reporting and Monitoring Responsibilities

Credit Card Operations staff will perform regular internal assessment of systems, security, policies and controls related to University payment card processing. Additionally, departments will complete a compliance questionnaire to be used by Credit Card Operations for preparation of the PCI DSS Self Assessment Questionnaire. The Associate Vice Chancellor for Financial Affairs will report annually to the Vice Chancellor for Finance and Administration on the status of campus compliance with Fayetteville Policies and Procedures and PCI DSS requirements.

Sanctions

Departments that do not comply with requirements of the Fayetteville Policies and Procedures 309 series, or other supplemental documents related to the policies, must take necessary action to become compliant or be subject to sanctions up to and including immediate suspension or termination of payment card processing privileges. Credit Card Operations will notify departments when remedial action is necessary to achieve compliance with campus and industry requirements. If compliance is not achieved in a time deemed reasonable by Credit Card Operations, payment processing privileges will be suspended and the department will no longer be an authorized payment card merchant. Within the institution, departments engaged in payment card processing are responsible for any financial loss incurred by the University resulting from inadequate controls or insufficient adherence to the PCI DSS and other industry security requirements. Any appeals of actions taken by Credit Card Operations regarding suspensions or cost recovery will be considered by the Vice Chancellor for Finance and Administration

Department Responsibilities
All departments engaged in any form of payment card processing must comply with the General Procedures listed below. Procedures for suspected or actual compromise of a card processing environment are detailed in the Payment Card Incident Response Policy in the 309 series. Additional procedures are required for departments that have been granted a System Usage Waiver (see Fayetteville Policy 309.0) to use an alternate processing system.

General Procedures.

- Each department engaged in payment card processing shall maintain formal, written operational procedures that demonstrate how compliance with the 309 policy series and the PCI DSS is achieved and maintained. Operational procedures must include transaction processing methods, refund policies, and reconciling procedures. Credit Card Operations will review the document and upon approval a copy will remain on file with Credit Card Operations. Departments must evaluate procedures annually and update with Credit Card Operations as necessary. [

- Each department engaged in payment card processing shall perform an annual risk assessment analysis and report the results to Credit Card Operations. Additional information regarding risk assessments can be found in the supplemental documentation to the 309 policy series provided by Credit Card Operations.

  Physical and electronic storage of sensitive PII associated with payment card transactions is prohibited. Credit Card Operations may revise the definition of PII for payment card policies as legal and industry regulations change. Examples of PII for which departmental retention is prohibited are: Primary Account Number (PAN), security code (CVV) or contents of magnetic track data from a payment card. Storage of the last 4 digits of the account number (PAN) is also prohibited.

- Each department engaged in payment card processing shall ensure that all employees who have access to customer PII associated with payment card transactions complete the annual Credit Card Operations Data Security Training course and sign an acknowledgement, provided by Credit Card Operations, stating that they understand their responsibility to protect customer PII. Additional training may be required, depending on the processing method used by the department. Only persons who have completed all required training will be permitted to handle payment card data on behalf of the University of Arkansas.

- Each department engaged in payment card processing must be in compliance with University policies regarding employee background checks.

- Each department engaged in payment card processing must establish segregation of duties among payment card processing, the processing of refunds, and reconciliation of revenue to the extent possible. Each such department shall immediately notify Credit Card Operations of any staff changes related to payment card data-handling positions.

- Acceptable methods of payment card acceptance include: walk-in (face-to-face), telephone, or customer-initiated online payment (via QPay or an approved alternate payment system). Phone payments must be processed while the customer is on the line. Making note of a customer's payment card number to process at a later time is prohibited. Accepting payment card data via mail, email, fax or any end-user messaging technology is prohibited. Tuition/Fee payments are accepted only as customer-initiated through the ISIS Student Center or Parental Portal.

- All refund transactions MUST be performed by the University Cashier's Office unless otherwise authorized in writing by Financial Affairs. It is strictly prohibited to authorize a refund through BASIS. The department must provide the University Cashier's Office with sufficient documentation and/or explanation to support the refund. Excessive refund activity will be investigated by Credit Card Operations and may result in a mandatory change in business operations.

- Customer PII associated with payment card transactions, especially account numbers, shall not be transmitted via any insecure method, especially e-mail, fax, cell phone, vocally in a public location, or any end-user messaging technology.

- Visitors are not permitted to enter a Server Data Environment unless properly identified by a badge or token that is surrendered when the visitor leaves. Visitors MUST be accompanied by UA staff at all times and must have a legitimate reason for being in the Server Data Environment. Departments are required to maintain a Visitor Log that all visitors must sign when entering and leaving a Server Data Environment.

- All devices within a department's cardholder data environment should be secured to the extent possible. Machines that are left unattended must be locked or logged-off. Non-computer devices should never be left unattended in an area where customers or visitors may have access to the device. Credit Card Operations will provide additional guidance to departments based on their specific needs.

- All workstations used in processing must run any Anti-Malware programs required by Credit Card Operations and have the computer name registered with Credit Card Operations. In addition, each workstation will be subject to weekly PCI DSS compliance scans performed by Credit Card Operations. All departmental workstations used in processing must be turned-on during scanning. The scan schedule will be provided by Credit Card Operations.

- Each department engaged in payment card processing must complete all security enhancements to processing systems as required by Credit Card Operations. All vendor supplied security patches to systems must be applied within 3 weeks of issue date.

- Each department engaged in payment card processing must use disk wiping software approved by University IT Services to render unreadable any hard disk or other media which has ever stored or processed customer PII before retiring such disk or media from service.

- Each department engaged in payment card processing must cooperate with all reporting and audits required by Credit Card Operations, including full compliance with the PCI DSS and all other industry security requirements, or be subject to the Sanctions detailed above.

- Any changes to the departmental processing environment, including any software/hardware additions MUST be approved by Credit Card Operations *prior* to purchase. If this provision is violated, the department will be subject to the sanctions detailed above.

- All departments MUST use the centralized QPay system for all payment card acceptance activity. Exceptions due to unique business needs may be requested through Credit Card Operations. If a System Usage Waiver to utilize another processing method is approved, the department requesting the waiver must demonstrate full compliance with the PCI DSS and all other industry security requirements, and submit written documentation of adherence to the PCI DSS to Credit Card Operations. System Usage Waivers will be evaluated annually.

Additional Procedures for Departments Granted Usage Waiver:

Departments that have been granted a System Usage Waiver MUST abide by all regulations set forth in the 309 policy series, and additional requirements not detailed above. A supplemental document containing all requirements for System Usage Waiver departments can be obtained from Credit Card Operations. All requirements MUST be met or the System Usage Waiver will be denied and the department will not be permitted to process payment card transactions via any POS/swipe or e-commerce channels.

Approval by Credit Card Operations is required for all third party processing agreements/contracts. All contracts and contract renewals for payment card processing MUST be approved by Credit Card Operations prior to execution. All contracts MUST contain PCI DSS contract language determined by Credit Card Operations and General Counsel.

Revised November 19, 2010
January 4, 2007