

Credit Card Processing and Security Policy**Purpose**

The purpose of this policy is to establish guidelines for processing credit card transactions and working with related data and reports, so that the University of Arkansas can ensure cardholders that sensitive account and personal cardholder information they provide is protected against theft and/or improper usage. This policy also ensures that the University complies with all credit and banking industry security regulations related to credit card processing and reporting, including PCIDSS (*see Definitions, below*).

Definitions

PCIDSS: The Payment Card Industry Data Security Standard (hereafter referred to as the “PCI Standard”) is the result of collaboration between the major credit card brands to develop a single approach to safeguarding sensitive data. The PCI standard defines a series of requirements for handling, transmitting and storing sensitive data. All entities engaged in any form of credit card processing must comply with these standards by June 30, 2005 or face substantial fines and penalties. A copy of the PCI Standard can be obtained on the Visa website or from Credit Card Operations.

Cardholder data: Cardholder data is any personally-identifiable data associated with a cardholder. Examples include but are not limited to: account number, expiration date, card type, name, address, social security number, and Card Validation Code (e.g., three-digit or four-digit value printed on the front or back of a payment card referred to as CVV2 or CVC2). Final responsibility for determination of what constitutes cardholder data rests with Credit Card Operations.

E-commerce: E-commerce transactions are those where the card is not present, the customer is often offsite with respect to the merchant, and the authorization and settlement are processed through a computer over the Internet.

Scope

This policy applies to all University of Arkansas departments, employees (including temporary), contractors and consultants. This policy is applicable to any unit that processes, transmits, handles or stores cardholder information in any physical or electronic format. Affiliated entities are encouraged to comply.

Policy

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

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

All departments engaged in any form of credit card processing must comply with the Procedures below in List A. In addition, departments engaged in e-commerce or otherwise utilizing a computer to transmit or store ANY cardholder or transaction information must also comply with the Procedures in List B.

Procedures

List A

All campus departments must:

- Maintain a written list of operational procedures, approved by Credit Card Operations, that demonstrates how compliance with this policy and the PCI Standard will be achieved
- Never store ANY cardholder data (in any physical form) that is not required for business operations, and then only in a locked, secured environment whose access is limited to employees who need such data to perform their jobs
- Ensure that all employees who process or access cardholder data complete the Human Resources Credit Card Security training and sign an acknowledgement, provided to Credit Card Operations, that they understand their responsibility to protect the data
- Shred any physical documents containing cardholder information before disposal
- Perform any background checks required by Credit Card Operations on all employees who will have access to cardholder data prior to hiring them or assigning them the responsibility of working with card data
- Require all personnel involved in credit card handling to attend the Human Resources Credit Card Security training at least every two years
- Establish segregation of duties between credit card processing, the processing of refunds, and reconciliation
- Require supervisory approval for any refund transactions
- Never store full account numbers or the full contents of any track on the magnetic stripe
- Never transmit cardholder data, especially account numbers, via any insecure method, especially e-mail, fax, cell phone or vocally in a public location
- Never store ANY cardholder data on portable devices, including laptops, external hard disks, memory keys, etc.
- Perform an annual security self-assessment and report the results to Credit Card Operations
- Comply fully with the PCI Standard, including any new provisions added to it.

List B

In addition to the above requirements, departments using computers to transmit or store cardholder data must also:

- Use the centralized Q-Pay e-commerce system for any e-commerce applications. Exceptions due to unique business needs may be requested through Credit Card Operations. If the waiver to utilize another e-commerce processing method is approved, the department requesting the waiver must demonstrate full compliance with the PCI Standard and submit written documentation of adherence to the PCI Standard to Credit

Card Operations. The department is liable for all processing fees, support and maintenance costs, etc. related to the alternate processing method, including the quarterly external security scans required by the PCI Standard. Any alternate e-commerce processing method must also include a written security policy, a written disaster recovery plan, and documented and utilized methods for monitoring all activity on the commerce system.

- Use Secure Sockets Layer encryption, or any alternate industry standard certified by Credit Card Operations, to protect the transmission of any cardholder data over any network (Internet or Intranet)
- Use an encryption method approved by Credit Card Operations to protect any stored data and databases
- Provide to Credit Card Operations the IP addresses of any computer equipment used in the processing of credit card transactions or other transmission or storage of cardholder data
- Immediately inform Credit Card Operations of any infrastructure changes that affect credit card processing and/or reporting
- Cooperate with Credit Card Operations in obtaining the quarterly external security scans (required by the PCI Standard) of the equipment engaged in processing, transmitting or storing cardholder data
- Remediate in a time deemed reasonable by Credit Card Operations any failure to adhere to the PCI Standard that is revealed by routine security scans, audit, breach, annual self-assessment or other means, or become subject to the *Sanctions* below
- Never store ANY cardholder data in any electronic format which has not been certified by Credit Card Operations
- Never store ANY data related to credit card transactions that is not required for reconciliation, chargeback research and reporting, and then never for a period longer than 6 months (the processing vendor and Credit Card Operations should be the source for most reporting data rather than local copies which increase our risk and exposure)
- Use disk wiping software approved by Computing Services to render unreadable any hard disk or other media which has ever stored cardholder data before retiring from service.

Migration of existing e-commerce applications

Any e-commerce applications not using the centralized Q-Pay system at the time this policy is effected must work with Credit Card Operations to migrate to and integrate with Q-Pay, unless a waiver is granted as described above. The timeframe for each migration will be decided upon by Credit Card Operations in consultation with the affected department.

Reporting and Monitoring Responsibilities

Credit Card Operations will assist departments with arranging their quarterly security scans as well as the annual self-assessment questionnaire. CCO staff will also perform regular internal assessment of systems, security, policies and controls in place related to credit card processing and will provide an annual report on compliance to the Vice Chancellor for Finance and Administration. Because those attempting to compromise our data continually develop new threats, each processing department performing e-commerce transactions is expected to follow that part of the PCI Standard which mandates regular monitoring of the network and systems involved with card processing, as well as regular monitoring of system and event logs. If any

breach is found or suspected the department must immediately notify the Vice Chancellor for Finance and Administration, Cash Management and Credit Card Operations.

Fees

Each department will pay for the actual costs incurred by the University to process their transactions, plus setup and monthly fees for any e-commerce merchant account. These fees will be deducted from a BASIS company cost center each month. 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 it incurs, as well as the cost of the quarterly security scans. Departments must also pay for training and background checks required by this policy.

Sanctions

Departments not complying with approved safeguarding, storage, processing and administrative procedures will lose the privilege of serving as a credit card merchant if compliance is not achieved in a time deemed reasonable by Credit Card Operations. In addition, each department engaged in credit card processing will be responsible for any financial losses due to poor internal or inadequate controls or negligence/neglect in adhering to the PCI Standard. Any appeals of the decisions made by Credit Card Operations will be considered by the Vice Chancellor for Finance and Administration.

January 4, 2007