University of Central Arkansas

CREDIT CARD PROCESSING & SECURITY POLICY

TABLE OF CONTENTS

I. PURPOSE

The purpose of this policy is to establish guidelines for processing charges/credits on Credit Cards to protect against exposure and possible theft of account and personal cardholder information that has been provided to the University of Central Arkansas (UCA); and to comply with the Payment Card Industry's Data Security Standards (PCI) requirements for transferring, handling and storage of credit card information. UCA will follow the current PCI guidelines in selection of our merchant level to meet PCI compliance including the requirement of a quarterly network scan. For other forms of electronic payment methods, please refer to UCA's Cash Handling Procedures manual.

II. DEFINITIONS

A. *Cardholder Information Security Program (CISP):* CISP is designed to ensure that all merchants that store, process, or transmit cardholder data, protect it properly. To achieve CISP compliance, merchants and service providers must adhere to the PCI Data Security Standard.

B. *PCI:* The PCI Standard is the result of collaboration between the four major credit card brands to develop a single approach to safeguarding sensitive data. The PCI standard defines a series of best practices for handling, transmitting and storing sensitive data.

C. *Cardholder Data:* Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, Card Validation Code CVC 2 (MasterCard), Card Verification Value CVV2 (VISA), Cardmember ID (Discover) or CID - Card Identification Number (American Express) (e.g., three- or four-digit value printed on the front or back of a payment card).

D. System Administrator Data Custodian: An individual who performs network/system administration duties and/or technical support of network/systems that are accessed by other people, systems, or services. Only full-time and permanent part-time employees of the University and/or third party vendors approved by Informational Technology (IT) and/or Financial Services may function as system/network administrators and/or data custodians.

III. SCOPE

This policy applies to all UCA employees, contractors, consultants, temporaries, and other workers. This policy is applicable to any unit that processes, transmits, or handles cardholder information in a physical or electronic format.

IV. POLICY

All transactions (including electronic-based) that involve the transfer of credit card information must be performed on systems approved by the Division of Financial Services, after a prior compliance and security review from Information Technology. All specialized servers approved for this activity must be housed within the Department of Information Technology and administered in accordance with the requirements of all UCA policies and the CISP. UCA is involved in PCI DSS compliance and is subject to examination of system security and configuration to ensure cardholder information is securely maintained. The Division of Financial Services will be responsible for verifying compliance with industry best practices for conducting electronic payment transactions through Data Capture / Point of Sale machines (Credit Card Terminals), while web-based procurement of credit cards will be monitored by the Department of Information Technology. In addition:

A No electronic credit card numbers should be transmitted or stored in any other system, personal computer, or e-mail account.

B Physical cardholder data must be locked in a secure area and limited to only those individuals that require access to that data. In addition, restrict access to data on a "need to know" basis.

C Store only essential information. Do not store the Card Validation Code, or the PIN. Do not store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.)

D All credit card receipts must be kept in accordance with the University's records retention policy. Credit card numbers must be rendered unreadable, except the last four digits, immediately after processing and no more than 60 days after receipt. All media used for credit cards must be destroyed when retired from use. All hardcopy must be shredded prior to disposal.

E Departments must comply with the PCI Data Security Standard Payment Card Industry Data Security Standard.

F Exceptions to this policy may be granted only after a written request from the unit has been reviewed and approved by the Division of Financial Services.

V. PROCEDURES

Confidentiality and Security of Account Information

UCA employees are governed by various policies that include the Code of Conduct, Acceptable Use, Information Security policies, the Family Educational Rights and Privacy Act (FERPA), and the Gramm Leach Bliley Act (GLBA). These policies include the responsibility to protect the confidentiality of individual's personal information.

All credit card and debit card transactions, including web based procurement of the same, must be initiated and controlled through the Division of the Financial Services. Because the sale of goods and services to entities outside the university community may raise special considerations (e.g. unrelated business tax, accounting, legal, etc.) all sales should be reviewed by the Controller's Office, and/or General Counsel.

Departments that need to accept credit/debit cards and obtain a physical terminal to either swipe or key transactions through that Data Capture machine need to contact the Controller's office to execute the required paper work, obtain a Merchant Number and receive training on proper accounting methods. The University of Central Arkansas, through the Student Accounts Office, is pursuing alternative means to manage all credit card activity through the CORE Cashiering system. CORE Cashiering system will provide a method for departments to use a "call center" where it will be possible to accept credit card payments via the web. This preferred method will serve to reduce the risks associated with retaining credit card information, including the risk of inadvertent exposure of credit card numbers. Until this technology is available, please adhere to the following guidelines in order to safeguard credit card information:

The practice of least privilege will be utilized to restrict access to sensitive data. This practice involves assigning individual access on a "need-to-know" basis. Positions requiring specific levels of data access will be provided with approval by the department head and IT. For employees without a "need to know", credit card account numbers will be masked to protect account information. The last four digits are the maximum number of digits to be displayed.

Under no circumstances will it be permissible to request or transmit credit card information by e-mail.

Under no circumstances will any other payment mechanism other than the CORE Cashiering system be permissible for electronic commerce on the web once it is fully implemented and operational. Exceptions to this procedure must be submitted in writing to the Division of Financial Services and the Department of Informational Technology for approval.

Any changes to systems housing account information must only be performed when:

- Thorough testing has taken place to ensure adequacies of controls;
- Functionality testing with clients has taken place;
- Required client training is completed; and
- Change control processes have been followed.

Enforcement by Finance & Administration and Information Technology

Information Technology Personnel

- Responsible for approving installation, modifications, and removal of all network hardware devices throughout UCA.
- Responsible for monitoring the enforcement of this policy

System Administrators:

- Responsible for granting permission to sensitive areas based on the principle of least privilege.
- Responsible for configuring the masking of account numbers based on a user's access.

Data Storage and Destruction

The following processes must be followed for all data storage and destruction:

- Hardcopy containing cardholder data will be destroyed immediately after processing.
- All electronic media containing cardholder information should be labeled and identified as confidential.
- An inventory of media containing cardholder information should be performed monthly.
- Audit logs for systems housing cardholder data will be available for a period of five (5) years.
- Electronic backup media containing cardholder data will be maintained for a maximum period of six (6) months. Decommissioned media will be properly destroyed.

VI. SANCTIONS

Failure to meet the requirements outlined in this policy will result in suspension of physical and/or electronic payment capability for affected units. Additionally, fines may be imposed by the affected credit card company, beginning at $50,000 for the first violation.

Persons in violation of this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary action, suspension, termination of employment and legal action. Some violations may constitute criminal offenses under local, state, and federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

Violations of the policy will be addressed by the individual's respective disciplinary policies and procedures**.** All known and/or suspected violations must be reported to the Internal Audit office.

The appropriate University administrative office will investigate all such allegations of misuse with the assistance of the Department of Information Technology, Financial Services, General Counsel, and the Department of Human Resources.