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 -46 25 () -95

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.

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,J E5 3 (p) 3 [H4.48 (