PAYMENT AND CARD INDUSTRY COMPLIANCE POLICY

All transactions (including electronic-based) that involve the transfer of credit card information must be performed on systems approved by the Division of Finance and Administration, 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 Finance and Administration 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 may be transmitted or stored in any other system, personal computer, or e-mail account.

INITIAL HERE ____________

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, access must be restricted on a “need to know” basis.

INITIAL HERE ____________

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.)

INITIAL HERE ____________

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.

INITIAL HERE ____________

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

INITIAL HERE ____________

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 Finance and Administration.

INITIAL HERE ____________

I READ, UNDERSTAND, AND WILL FOLLOW THE PAYMENT AND CARD INDUSTRY COMPLIANCE POLICY.

User Name Printed __________________________ Signature __________________________ Date ____________

Supervisor’ Name __________________________ Signature __________________________ Date ____________