

Policy Name: University of Alabama Equestrian Program PCI Compliance Policy		
Effective Date: 02/01/2016	Revision Date:	Department/Area/Division: BEQO/BA/FA
Department/ Area Policy #:	Departmental Contact: Diane Harrison, Assistant to the Vice President, FA	

Purpose:

The credit card security policy is designed to address security of card holder data related to credit card payments taken by the University of Alabama (UA) Equestrian Program in the division of Financial Affairs. This policy is reviewed annually and updated as necessary to ensure compliance with Payment Card Industry (PCI) standards.

Policy Statement:

This policy applies to all employees within the UA Equestrian Program. Each employee should read, understand, and ensure compliance with this policy at all times to ensure the protection of cardholder data. Each employee must acknowledge in writing at least once a year that they have read and understood the policy.

Policy:

Protecting Customers’ Personal Credit Card Information: All personal credit card information must be strictly controlled and protected. Failure to maintain strict controls over this information could result in unauthorized use of a credit card number and serious problems for the customer, our department and the University. Personal credit card data, including the credit card number, expiration date, and security code should never be removed from the UA Equestrian Program office (hereafter the UAEP office) for any reason. The security code may not be retained and must be destroyed in a manner consistent with current PCI guidance once the transaction has been authorized. This information should never be stored on a computer, any type of transportable USB drive, or other electronic media.

The policy applies to anyone who is involved in the processing of credit cards for the UA Equestrian Program. No employee should ever send or request cardholder information to be sent via e-mail, fax, instant messaging, chat, etc. If a staff member receives credit card information that has been transmitted in this manner, the staff member should fill out a credit card payment slip and take it immediately to a cashier to complete the transaction. Any other media containing the credit card information is to be destroyed immediately. The contacted staff member should remind the customer that alternative methods are in place for submitting credit card information that provide better security of personal data.

Transfer or Custody of Credit Card Information: Because receipts for credit card transactions will be generated when traveling to horse shows, the Assistant to the Vice President of Financial Affairs (Diane Harrison) or an employee from the UAEP will monitor the credit card terminal at all times, never leaving the machine unattended. All credit card transaction documentation as well as the credit card terminal will be in a locked box and monitored. When not under the direct control

Policy Name: University of Alabama Equestrian Program PCI Compliance Policy		
Effective Date: 02/01/2016	Revision Date:	Department/Area/Division: BEQO/BA/FA
Department/ Area Policy #:	Departmental Contact: Diane Harrison, Assistant to the Vice President, FA	

of an approved person, the locked box and terminal will be placed in the locked hotel room or locked car.

Securing And Storing Customers' Personal Credit Card Information: All documents containing personal credit card data are separated from general files and stored in the UAEP office locked box in order to ensure that access is limited to only authorized staff members. The UAEP office processes credit card transactions received over the telephone or in person via a credit card terminal.

Credit card transactions received in person – The merchant copies of credit card receipts generated from a terminal transaction are accumulated throughout the day by the responsible staff member. The credit card receipts are safely stored in a drawer at the staff member's work station. When the staff member leaves the work station, the drawer is locked. After the day's work is balanced by each staff member, all printed credit card receipts are submitted along with the daily work to the Assistant to the Vice President of Financial Affairs (Diane Harrison) who combines the receipts for all staff members. The receipts are placed in an envelope, labeled by date, and transferred to a filing cabinet inside the UAEP office locked box, which is locked at all times.

Credit Card information received by telephone – Credit card information taken from a customer by telephone is recorded by the staff member on a Telephone Charge Card Authorization Form. The credit card transaction is processed immediately or taken to a staff member responsible for processing credit card transactions. The forms should be processed as often as possible during the day and should never be stored at a staff member's desk overnight.

Credit card information processed via the student online account – Online credit card payments are made via a secure, hosted payment gateway. Staff members do not have access to any Personally Identifiable Information (PII) related to these payments.

Securely Processing Customer Refunds to a Credit Card: If a refund to a credit card processed via terminal is required, authorized personnel will contact the Assistant Director for Student Receivables (Mike Harris) to process. Refunds of online transactions are conducted via the secure, third party hosted gateway. No PII is accessible or necessary to the staff.

Credit Card Terminal Security: The credit card terminal's make and model as well as physical location, and serial number, will be maintained by the Assistant to the Vice President of Financial Affairs (Diane Harrison).

Any UAEP staff with access to the terminals will receive training so they are aware of procedures to detect and report attempted device tampering and substitution. Personnel will be trained to:

- verify the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices;
- not install, replace or return devices without verification;
- be aware of suspicious behavior around devices; and

Policy Name: University of Alabama Equestrian Program PCI Compliance Policy		
Effective Date: 02/01/2016	Revision Date:	Department/Area/Division: BEQO/BA/FA
Department/ Area Policy #:	Departmental Contact: Diane Harrison, Assistant to the Vice President, FA	

- report suspicious behavior and indications of device tampering or substitution to appropriate personnel.


Terminal surfaces will be inspected monthly by the Assistant to the Vice President of Financial Affairs (Diane Harrison) in order to detect possible tampering or substitution. In addition, UAEP staff will be trained as to signs of tampering and substitution and will informally inspect terminals as they are used during day-to-day operations.

Credit Card Data Retention and Disposal: Because of the nature of the UAEP office's business needs, credit card receipts generated from a terminal and completed Telephone Charge Card Authorization Forms are retained for a period of 12 months after the month of the transaction. There are twelve file folders—one for each month of the year—in the filing cabinet inside the Department vault which is locked at all times. A log of secured credit cardholder information is maintained listing all the folders and the specific dates of the content. At the end of each month, the credit card receipts and authorization forms in the oldest folder are shredded using a cross-cut shredder. Maintenance of the files and the monthly shredding is performed by the UAEP staff. Approval to remove the receipts and forms from the UAEP office locked box and to shred them is given by the Assistant to the Vice President of Financial Affairs (Diane Harrison). The date that the documents are destroyed is entered on the Log of Secured Credit Cardholder Information as well as approval by the Assistant to the Vice President of Financial Affairs (Diane Harrison).

Customer Reported Suspected Credit Card Misuse: If a UAEP staff member is contacted by a customer to report suspected fraudulent use of his/her credit card, the customer should be referred to the Assistant to the Vice President of Financial Affairs (Diane Harrison). The next step will be for the Assistant to the Vice President of Financial Affairs (Diane Harrison) to contact Associate Director for Student Receivables (Charles Poole) immediately.

Information Security Policy: The Department will review and update the credit card policy and associated procedures to address protection of credit card data on an annual basis. Mandatory training for all employees (permanent or temporary) who have access to credit card data will be provided annually. New employees will receive training when they begin work. Employees will acknowledge in writing that they have read and understood the department's security policy and procedures including data access limitation, data storage, data retention, and data disposal. This written acknowledgement must be reviewed and re-signed annually. The signed acknowledgments will be on file in the Department.

Office of the Vice President of Financial Affairs:

Approved by: 

Date: 2/9/16

Policy Name: University of Alabama Equestrian Program PCI Compliance Policy		
Effective Date: 02/01/2016	Revision Date:	Department/Area/Division: BEQO/BA/FA
Department/ Area Policy #:	Departmental Contact: Diane Harrison, Assistant to the Vice President, FA	

Employee Acknowledgement and Signature: I acknowledge that I have read, understand, and will abide by the preceding UAEP Credit Card Security Procedures.

Employee Name	
Employee Position	
Employee Signature	
Date Signed	