THE UNIVERSITY OF ALABAMA FINANCIAL AFFAIRS	Topic: Credit Card Security		
	Policy #: RC-2	Version:	Effective Date: January 19, 2015
	Submitted by: Kristy D. Pritchett	Title: Director	Dept./Area: Receivables and Collection

Purpose: The credit card security policy is designed to address security of card holder data related to credit card payments taken by the Receivables and Collection department. 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 Receivables and Collection department. 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 Receivables and Collections Department (hereafter the Department) 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.

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.

Because receipts for credit card transactions, generated by Student Receivables, are retained within the department and do not require transport to another area, Student Receivables has no need to develop a policy to address Transfer of Custody of Credit Card Information.

Securing And Storing Customers' Personal Credit Card Information: All documents containing personal credit card data are separated from general files and stored in the Department vault in order to limit access to only authorized staff members. The Department processes credit card transactions received over the telephone or in person via a stand-alone credit card terminal. Credit card transactions are also accepted via the student online account.

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 Director, Cashiering, 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 Department vault, which is locked at all times and armed during off hours.

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. During peak registration periods when these forms accumulate faster than they can be processed, they are securely stored during the day in a drawer at the staff member's work station. The forms should be processed as often as possible during the day and should never be stored at a staff member's desk over-night.

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 stand-alone terminal is required, only authorized personnel may access the Department vault to obtain the necessary information from the credit card receipt. The receipts are immediately re-filed in the Department vault by a Department cashier after the refund is processed. 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: A list of credit card terminals, including make and model of the device, physical location, and serial number, will be maintained by the Assistant Director, Credit Card Processing. The list will be reviewed monthly and updated as terminals are added, relocated, disposed, etc.

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

Terminal surfaces will be inspected monthly by the Assistant Director, Credit Card Processing in order to detect possible tampering or substitution. In addition, cashiers 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 Department'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 Department cashiers. Approval to remove the receipts and forms from the vault area and to shred them is given by the Department Assistant Director, Cashiering. The date that the documents are destroyed is entered on the Log of Secured Credit Cardholder Information as well as approval by the Assistant Director, Cashiering.

Customer Reported Suspected Credit Card Misuse
If a Department staff member is contacted by a customer to report suspected fraudulent use of his/her credit card, the customer should be referred to the Associate Director of Student Receivables Operations, Vicky Morrison. If a Department staff member is contacted by an employee from another department regarding possible fraudulent use of a credit card, that individual should be directed to the Assistant Director of Credit Card Processing, Mike Harris.

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.

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

Employee Name: _____

Position: _____

Employee Signature: _____

Date: _____

Definitions:

Payment Card Industry Data Security Standard (PCI DSS) - PCI DSS promotes cardholder data security. It establishes a foundation of technical and operational requirements designed to protect cardholder data and applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data and/or sensitive authentication data.

Other Department and/or Divisions:

All UA departments accepting credit card payments must establish a PCI policy for their employees and department to ensure the safety and protection of cardholder data.

References:

PCI Security Standards Council - https://www.pcisecuritystandards.org/index.php

Office of the Vice President of Financial Affairs:

Approved by: Dana S Keith

Digitally signed by Dana S Keith
DN: cn=Dana S Keith, o=The University of Alabama, ou=Associate Vice President for Financial Affairs, email=dkeith@fa.ua.edu, c=US
Date: 2015.06.24 14:10:33 -05'00'

Date: