THE UNIVERSITY OF ALABAMA | Division of Financial Affairs

Policy Name: OHPW Credit Card Security Policy		
Effective Date: 12/10/2015	**Revision Date:**	**Department/Area/Division:** OHPW
Department/ Area Policy #:	**Departmental Contact:** Heather Clayton, Manager	

Purpose:

The credit card security policy is to address the security of cardholder data related to credit card payments taken by the Office of Health Promotion and Wellness (OHPW). 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 Office of Health Promotion and Wellness. 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:

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 Office of Health Promotion and Wellness (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 via an online account.

> Credit card information processed via the 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: Refunds of online transactions are conducted via the secure, third party hosted gateway. No PII is accessible or necessary to the staff.

Customer Reported Suspected Credit Card Misuse: 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.

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

Credit Card Security Policy - http://fawp.ua.edu/policies/wp-content/uploads/sites/4/2015/08/PCI-Compliance-Policy-for-Credit-Card-Security.pdf

Office of the Vice President of Financial Affairs:

Approved by: Dana S Keith

Date: January 6, 2016

THE UNIVERSITY OF ALABAMA | Division of Financial Affairs

Policy Name: OHPW Credit Card Security Policy		
Effective Date: 12/10/2015	**Revision Date:**	**Department/Area/Division:** OHPW
Department/ Area Policy #:	**Departmental Contact:** Heather Clayton, Manager	

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

Employee Name:	
Position:	
Employee Signature:	
Date:	