THE UNIVERSITY OF ALABAMA® | Division of Finance and Operations

Credit Card Security Policy

Unit: Student Account Services
Effective Date: 1/19/2015
Revision Date: 7/24/2019

Contact: Kristy Pritchett
Title: Director, Student Account Services

Purpose

The credit card security policy is designed to address security of cardholder data related to credit card payments taken by the Department of Student Account Services (hereafter the Department). This policy is reviewed annually and updated as necessary to ensure compliance with Payment Card Industry (PCI) standards.

This policy applies to all employees within the Department. Each employee should read, understand, and ensure compliance with this policy 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 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. 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. Any media containing cardholder data is destroyed immediately once the transaction has been authorized. As such, the Department has no need to develop a policy to address Transfer of Custody of Credit Card Information.

Securing and Storing Customers' Personal Credit Card Information

No media containing personal credit card is stored after transaction authorization. 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

In person terminal credit card payments are processed through the Department's point-of-sale system via a secure, hosted payment gateway. Staff members do not have access to Personally Identifiable Information (PII) related to these payments.

Credit Card information received by telephone

Credit card information taken from a customer by telephone is recorded by the staff member on a Charge Card Authorization Form. The credit card transaction is processed immediately via a terminal 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. The Charge Card Authorization Form is destroyed via cross-cut shredder immediately after the transaction has been authorized.

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 PII related to these payments.

Securely Processing Customer Refunds to a Credit Card

All refunds 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 E-Commerce Manager. 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 daily by appropriate personnel to detect possible tampering or substitution. Logs of these daily inspections will be reviewed monthly by the Associate Director, Operations. 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

Charge Card Authorization Forms are destroyed via a cross-cut shredder immediately after a transaction is authorized. No media, paper or electronic, is stored after transaction authorization.

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, Accounting. 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 Associate Director, Accounting.

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, terminal security, 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.

Scope

This policy applies to all employees within Student Account Services.

Office of the Vice President of Finance and Operations

DocuSigned by:

Signed: Cheryl Mowdy 7/24/2019

DC7FC10D23404E0...

Cheryl Mowdy
Assistant Vice President for Finance and Operations