THE UNIVERSITY OF ALABAMA | Division of Finance and Operations

Capstone Village Credit Card Transaction and Security Policy

Unit: Shared Administrative Services
Effective Date: 6/15/2015
Revision Date: 1/9/2019

Contact: Christina Mullis
Title: Senior Director of Process Review and Financial Compliance

Purpose

The purpose of this policy is to address the protection of credit card data including data access limitation, data storage, data retention, and data disposal.

This policy applies to all employees at Capstone Village who handle payments by credit card. It is intended that this policy be followed for the security and confidentiality of personally identifiable information and to comply with the Payment Card Industry Data Security Standard (PCI DSS) requirements.

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, Capstone Village and the University. Personal credit card data, including the credit card number, expiration date, and security code should never be removed from campus for any reason. This information should never be stored on a personal computer or any type of transportable USB drive.

No employee (The University of Alabama or Southern Foodservice) should ever send or request cardholder information to be sent via e-mail, fax, instant messaging, chat, etc. Credit card information transmitted in this manner should be destroyed immediately. The customer should be reminded that there are alternative methods in place for submitting credit card information that would provide better security of personal data.

Transport of Secured Credit Card Data to Another Area

Since printed receipts for credit card transactions, generated by Capstone Village, do not contain the full credit card number, Capstone Village does not have a policy to address the Transfer of Custody of Credit Card Information. Receipts only show the last four digits of the credit card number. These receipts are sent to the Administrative and Financial Specialist for scanning.

Securing and Storing Customer's Personal Credit Card Information

No documents should be stored which contain personal credit card data.

Credit Card Transactions Processed Through a Terminal

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 at the staff member's work station and submitted to the appropriate member of management on a daily basis. Terminal credit card receipts from the concierge, beauty salon, or dining services are submitted by the Capstone Village Director of Accounting to the Administrative and Financial Specialist. Receipts ready for scanning are placed in an envelope, labeled by date, and arranged for scanning into the On Base Imaging System. Once scanned, the physical documents are transferred to a storage box and held in a locked unit until they are scheduled to be destroyed.

Credit Card Information Received by Telephone

Credit card information that must be taken from a customer or resident over the telephone should be processed as quickly as possible by the appropriate staff member. Should the information be stored overnight, it must be kept by the Capstone Village Director of Accounting in a locked drawer or filing cabinet. Once processed, the card number information should be destroyed immediately.

Securely Processing Customer Refunds to a Credit Card

If a refund to a credit card is required due to an error or mistake, a voided ticket should be performed immediately following the sale by the responsible staff member. This will initiate a refund in the payment processing software. A manager login will be required in order to void any transaction in the point of sale system.

Credit Card Terminals

A list of credit card terminals, including make and model of the device, physical location, and serial number, will be maintained by the System Support Coordinator. 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 to install, replace or return devices without verification, to be aware of suspicious behavior around devices, and to report suspicious behavior and indications of device tampering or substitution to appropriate personnel.

Terminal surfaces will be inspected monthly by the System Support Coordinator 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 Capstone Village business needs, credit card receipts generated from a terminal are scanned and retained for a period of 3 years. Terminal receipts only contain the last four digits of the customer's credit card; therefore, scanning and retaining receipts does not affect compliance with PCI requirements. Any other information received containing the entire credit card number, expiration date, or security code should be destroyed using a cross-cut shredder. Maintenance of the terminal receipts is performed by the Administrative and Financial Specialist.

Customer Reported Suspected Credit Card Misuse

If any staff member is contacted by a customer or resident to report suspected fraudulent use of their credit card, the customer or resident should be referred to the Executive Director of Capstone Village.

Information Security Policy

Capstone Village Administration and Shared Administrative Services 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 or within three days from initial date of employment for all new employees. All new users will not be granted access to the point of sale system until training has been completed. 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 Shared Administrative Services office.

Definitions

Payment Card Industry Data Security Standard - mandated set of security standards created by the major credit card companies to offer merchants and service providers a complete, unified approach to safeguarding cardholder data for all credit card brands.

Personal Credit Card Information - personally identifiable information related to an individual's credit card including the full credit card number, the expiration date, and the security code.

Personally Identifiable Information - an individual's personal data that may be subject to misuse. Examples include full credit card number, credit card expiration date, credit card security code, etc.

Point of Sale System - a point of sale system refers to the computer hardware, software and checkout terminals used by staff to process in-person customer transactions, create and print receipts, and maintain and update the associated databases and reports. POS systems process and transmit card holder data but do not store card holder data on University equipment or systems.

Security Code - a three- or four-digit value printed on the card or signature strip on the back of the card, used to verify that the customer has the card in their possession or has a least physically seen the card.

Scope

This policy applies to all employees at Capstone Village who handle payments by credit card.

Office of the Vice President of Finance and Operations

Signed: DocuSigned by: Cheryl Mowdy DC7FC10D23404E0... 1/9/2019

Cheryl Mowdy
Assistant Vice President for Finance and Operations