THE UNIVERSITY OF ALABAMA | Division of Finance and Operations

Boone Cabin Credit Card Transaction and Security Policy

Unit: Shared Administrative Services
Effective Date: 9/1/2017
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 University employees who handle payments by credit card for use of the Boone Cabin facility. 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, department 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 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. Payment will not be processed using this information. 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 the University's Boone Cabin facility, do not contain the full credit card number, the University does not have a policy to address the Transfer of Custody of Credit Card Information for this facility. Receipts only show the last four digits of the credit card number. These receipts are sent to the Logistics and Support Services Assistant for scanning.

Securing and Storing Customers' Personal Credit Card Information

The University's policy applicable to the Boone Cabin Facility is to not maintain any personal financial information such as credit card number, expiration date, or security code once the transaction has occurred.

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 in a locked drawer in the Special Property Management Director's office and submitted to the Logistics and Support Services Administrative Specialist on a daily basis. Receipts received are reconciled to the daily settlement reports. These receipts and reports should not contain the full card number as the University's policy applicable to Boone Cabin transactions is to not maintain this information.

Credit Card Information Received by Telephone

It is the preferred method that credit cards are swiped in person for payment on any Boone Cabin facility use. If personal credit card data is taken over the phone including the credit card number, expiration date, and security code, it

must be recorded on the Charge Card Authorization Form provided by Student Account Services and taken by Boone Cabin personnel only. Under no circumstances should any Charge Card Authorization Form containing customers' credit card information be removed from Special Property Management Director's office where Boone Cabin Facility information is stored. The Charge Card Authorization Forms are destroyed immediately after the transaction is completed.

Securely Processing Customer Refunds to a Credit Card

If a refund to a credit card is necessary, the refund must be credited to the same credit card account from which the purchase was made. Before a refund may occur, all documentation relating to the original rental of Boone Cabin must be made available. Security deposit refunds may be performed by the Senior Executive Director of Logistics and Support Services, Special Property Management Director, Special Property Management Coordinator or Logistics and Support Services Assistant. Refunds made for any other reason may only be performed by the Senior Executive Director of Logistics and Support Services or Special Property Management Director.

If a staff member charges the incorrect amount to the customer's credit or debit card, a void will need to be submitted the same day. Only the Senior Executive Director of Logistics and Support Services or Special Property Management Director may submit a void.

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.

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 Logistics and Support Assistant in order to detect possible tampering or substitution. An inspection report is then sent to the System Support Coordinator for filing. In addition, department personnel will be trained as to signs of tampering and substitution and will informally inspect terminals as they are used during day-to-day operations. Due to the limited volume of transactions performed for Boone Cabin, the terminal should be stored in the locked safe until needed to process transactions.

Credit Card Data Retention and Disposal

Because of the nature of Boone Cabin 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 Special Property Management Director.

Customer Reported Suspected Credit Card Misuse

If any University staff member who handles Boone Cabin facility transactions is contacted by a customer or employee from another department to report suspected fraudulent use of their credit card, the customer should be referred to Student Account Services. Student Account Services will assist and involve other University authorities as needed.

The University will not handle any disputes related to Boone Cabin transactions between the customer and the financial institution. All disputes will be handled by Student Account Services.

If any University staff member who handles Boone Cabin Facility transactions knows or suspects that their credit card receipts or other stored credit card data has been breached, they should contact the OIT Information Security Officer as

quickly as possible. Do not turn device(s) off, but unplug only the network cable. UA has an incident response team which will determine the appropriate course of action needed.

Information Security Policy

Special Property Management, System Support and Administrative Services, and Process Review and Financial Compliance 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 who have access to credit card data will be provided annually. 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. All employees must also complete the University required online training through Skillport (PCI DSS Compliance Awareness Training). A certificate of completion will be issued and a copy must be sent to the Senior Director of System Support and Administrative Services. The signed acknowledgments and certificate of completions will be kept 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.

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 University employees who handle Boone Cabin payments by credit card.

Office of the Vice President of Finance and Operations

Signed: DocuSigned by: Cheryl Mowdy 1/9/2019
DC7FC10D2304E0...
Cheryl Mowdy
Assistant Vice President for Finance and Operations