UNIVERSITY OF SOUTH ALABAMA

# USA Payment Card Industry (PCI) General Merchant Procedures

| | |
|---|---|
| Approved by: | G. Scott Weldon, Vice President for Finance and Administration |
| Effective Date: | September 15, 2015 |
| History: | Approval Date: November 4, 2019<br>Revisions: October 15, 2019 |
| Responsible Officials: | Investment Manager<br>Director of Information Security |

The USA Payment Card Industry (PCI) General Merchant Procedures has been approved by G. Scott Weldon, Vice President for Finance and Administration.

Signature: _____

Date: November 4, 2019

B. Any Merchant accepting payment cards on behalf of USA must designate an individual within the department who will have primary authority and responsibility within that department for payment card transactions and PCI Compliance. This individual will be referred to as the Merchant Department Responsible Person (MDRP).

## II. CARDHOLDER DATA PROTECTION

A. Access to payment card data and system components will be limited to those employees whose jobs require such access.

1. Access privileges assigned to user IDs shall be limited to the least privileges necessary to perform job responsibilities.
2. Access privileges should be assigned based on the individual's job classification and functions.
3. When the job responsibilities and functions of an employee with access to the cardholder data environment changes, the merchant will need to notify the PCI Coordinator and the Investment Manager. The MDRP will also need to modify roles and security privileges within the cardholder data environment as necessary.
4. When an employee with access to the cardholder data environment leaves employment with USA or transfers out of the merchant's department, the merchant will notify the PCI Coordinator and the Investment Manager. The user accounts and roles within the cardholder data environment will also need to be disabled or modified by the MDRP so that the former employee has no access to the cardholder data environment or to cardholder data.

B. Payment card data must be kept confidential and secure at all times.

C. Payment card data must not be transmitted in an unsecure manner such as, but not limited to, inter-office mail, text messaging, copy machines, other electronic messaging (including email), or fax machines.

D. Storage of cardholder data in any way is prohibited and in violation of the PCI DSS. Storage includes, but is not limited to: desktop computers, laptop computers, network servers (this includes in text files, databases, spreadsheets, word documents, etc.), compact disks, USB flash drives, personal digital assistants, cellphones, tablets, portable external hard drives, etc.

E. Cardholder data will not be stored in paper form, including payment forms, camp registration forms, ticket orders, etc. Once the credit card transaction has been processed, payment card information must be destroyed in a crosscut shredder so that information cannot be reconstructed. Payment card data must be removed from paper forms after authorization is obtained if the paper form is to be retained by the merchant. Cardholder data must be removed completely and left unreadable before the form is scanned or stored. Simply obscuring or blacking out cardholder data is not compliant.

F. Accepting/sending payment card information via email is strictly prohibited. In the event an email is received with cardholder data for payment, the recipient should immediately reply to the email with the message below. Before sending the e-mail reply, delete the cardholder data and after replying, delete the original message.

> *Thank you for providing the information necessary to process your payment for _____. The University of South Alabama strives to protect all vital information of our customers and email is an unsecure process of providing cardholder data, therefore the email with your cardholder data has been deleted and your payment has not been processed. Please reach out to _____ to make a secure credit card payment.*

G. Payment card payments made via telephone is strongly discouraged. If in some cases it is necessary to accept payment by telephone, directly enter the payment card data into the credit card device. Do not write down the payment card data, if possible.

H. Sending or receiving payment card data via fax is prohibited.

I. If your office must deliver forms or other correspondence containing cardholder data to another office, special care should be taken to ensure the safety of the documents. Such documents should be hand-carried by a courier and documents should be placed in a locked bag/case during transport.

J. Safeguard your desk area by not walking away when cardholder data is visible. If you must leave, secure cardholder data by locking it in your desk or file cabinet. If payments need to be left in a staff member's office, do not leave them on a desk. Cardholder data should be placed in a secure and lockable space.

K. Be sure only the last four digits of the payment card number is displayed on receipts.

L. Picture ID's are required for all transactions where the payment cards are not signed.

## III. HARDWARE, SOFTWARE, AND TECHNOLOGY

A. Changes to hardware, software, or other payment card systems that process payment card transactions must be approved by the Department of Information Security, the PCI Coordinator, and the Investment Manager before implementation.

B. All PCs, laptops, and workstations that are involved in the processing of payment cards or have access to the cardholder data environment must have security logging capabilities and must have basic OS level auditing turned on to facilitate tracking of user accounts in the event of a security breach or other unauthorized access.

C. Use of General Purpose PCs, Laptops, and Workstations:

1. Merchants are prohibited from processing payment card transactions using general purpose computers, or point-of-sale equipment and any other card processing equipment that is connected to general purpose computers without proper configuration (i.e. Virtual terminals, hardening, etc.). General purpose computers are defined as any computer that has access to email, general web access, etc.
2. If a point of sale terminal is connected to a general purpose computer, contact the Department of Information Security and the PCI Coordinator to provide a secure setup.
3. All payment card processing and interaction with the cardholder data environment must take place from specifically purposed and properly secured computers and/or equipment.

D. USA requires management approval for the use or change of any technology. Users wishing to connect any new device to the cardholder data environment must first obtain approval from the Director of Information Security and the PCI Coordinator or Investment Manager.

E. Each Merchant shall maintain a list of all hardware, software, technologies, and any equipment/devices used in the department for transmitting and processing cardholder data. The list shall also include the names of personnel with access to the hardware, software, technologies, and equipment/devices.

F. Guidance for devices that capture cardholder data via direct physical interaction with the card (such as card swipe and card dip devices):
1. Merchants must obtain card swipe devices or card dip devices from the PCI Coordinator.
2. Merchants must notify the PCI Coordinator or the Investment Manager when a card swipe device or card dip device is removed from service or when relocated. For decommissioned devices please reach out to the PCI Coordinator for disposal instructions.
3. Merchants must maintain a list of credit card devices used in their department area.
    a. The list must include the following: make and model, location within the department, serial number, and USA ID tag number.
    b. The list must be updated when credit card devices are added, relocated, or decommissioned.
4. Merchants must develop and document local procedures and must periodically inspect credit card devices for tampering (e.g. the addition of a card skimmer) or substitution (e.g., by checking the serial number or other device characteristics to verify that it has not been swapped with a fraudulent device).
    a. Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or

changed security labels, broken or differently colored casing, or changes to the serial number.

b. Tampering and/or substitution of credit card devices must immediately be reported to the PCI Coordinator, Investment Manager, and the Director of Information Security.

G. Personnel within each merchant department must be trained to identify attempted tampering or replacement of devices. The following rules should be in place:

1. Verify the identity of any third-party persons (this could be someone claiming to be repair/maintenance personnel) prior to granting them access to the credit card device. Check with the PCI Coordinator, Investment Manager, Computer Services Center, or the Director of Information Security for verification.
2. Do not allow installation, replacement, or the return of credit card devices without the approval of the PCI Coordinator.
3. Be aware of suspicious behavior around credit card devices (e.g. attempts to unplug or open credit card devices by unknown persons).
4. Immediately report suspicious behavior and device tampering/substitution to the department supervisor, PCI Coordinator, Investment Manager, and Director of Information Security.

H. The appropriate PCI firewall set up is required for any computer and/or credit card device that accepts and processes payment cards. Contact the Department of Information Security for more information.

I. The use of anti-virus software is required on all computers that accepts and processes payment cards. If anti-virus software is not currently installed on the necessary computers, please contact the Department of Information Security.

J. Operating systems on all computers used in the processing of payment cards must be set to auto update security patches. Contact the Department of Information Security for more information.

K. Use of computers, workstations, point-of-sale terminals, and devices used in the acceptance and processing of payment card transactions and/or connected to the cardholder data environment must require each user to log in using a unique user identifier and password. Sharing of user accounts is prohibited.

L. Point of Sale System Passwords:

1. A minimum length of at least seven characters, containing both numeric and alphabetic characters.
2. Passwords must be changed every 90 days.
3. Do not allow an individual to submit a new password that is the same as any of the last four passwords he/she has used.

4. Passwords for first-time use should be changed immediately after logging in (i.e. do not use vendor default provided passwords).

M. Auditing (automated audit trails) must be enabled on all cardholder data environment system components. If you have any questions regarding this requirement, please contact the Department of Information Security.

N. Physical Security:

1. All equipment used to accept or process payment card transactions must be secured against unauthorized use in accordance with the PCI DSS. Each merchant should have security controls in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or areas where such equipment is located. If credit card devices accept credit card payments in an open or unsecured space, then it is recommended that a credit card security stand be installed on the credit card device and fixed to the physical structure of the payment location.

## IV. THIRD PARTY VENDORS AND SERVICE PROVIDERS

A. Third parties must be contractually required to adhere to the PCI DSS requirements. Contracts with third-party vendors and service providers must define each party's roles and responsibilities with respect to the PCI DSS. Any agreements with third parties must be approved by the PCI Coordinator, Investment Manager, Director of Information Security, and a University Contract Officer such as the University Treasurer. Only the minimum amount of data needed to complete the transaction will be shared with third parties. All interaction must be properly documented and logged.

B. A list of point of sale third party vendors and service providers will be maintained by each department and the PCI Coordinator.

C. The PCI Coordinator will maintain a program to monitor vendor and service providers' PCI DSS compliance status on an annual basis.

## V. SECURITY INCIDENT IDENTIFICATION

A. Employees must be aware of their responsibilities in detecting security incidents. All employees have a responsibility to assist in the incident response within their departments. Some examples of security incidents that an employee might recognize during day to day activities include, but are not limited to:

1. Theft, damage, or unauthorized access (e.g., papers missing from desks, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry).
2. Fraud – Inaccurate information within databases, logs, files or paper records.

3. POS terminals devices showing signs of tampering.
4. Key-logger found.
5. Card-skimming devices found.
6. Detection of unauthorized equipment being substituted.
7. Unauthorized devices discovered on the network.
8. Lost, stolen, or misplaced cardholder data.
9. Lost, stolen, or misplaced computers, laptops, hard drives, or other devices that contain cardholder data.
10. Files containing cardholder data mistakenly, or otherwise, transmitted to an unauthorized party.

## VI. REPORTING AND RESPONDING TO AN INCIDENT

A. Alert the PCI Coordinator immediately of any suspected security incidents involving cardholder data. The PCI Coordinator will contact the necessary parties and, if necessary, law enforcement.

1. Employee communication regarding any suspected or actual security incidents should be limited to the employee's supervisor(s), the PCI Coordinator, the Investment Manager, the Direct of Information Security, the Director of Risk Management, Internal Audit, and other authorized personnel as appropriate. All communications with law enforcement or the public will be coordinated by the Investment Manager, Director of Information Security, and the director of Risk Management.

B. Employees should document related information while waiting for the PCI Coordinator to respond to the incident including date, time, and the nature of the incident. Any information provided will aid in responding in an appropriate manner.

C. When suspecting a breach, immediately cease using the device and connected systems and only perform actions as directed by the PCI Coordinator, Investment Manager, or Director of Information Security. The Director of Information Security shall determine the best way to isolate the affected systems from the network.

1. Unless explicitly instructed otherwise:
   a. DO NOT turn the computer/device off or reboot the system.
   b. DO NOT change passwords.
   c. DO NOT run a virus scan.
2. Document all steps taken.

D. Upon notification of a suspected incident within the cardholder data environment the PCI Coordinator, Investment Manager, Director of Information Security, and the Computer Services Center must promptly log the incident using an approved Incident Report Form. Reporting individuals and/or systems administrators must document relevant actions taken from the point of the suspected breach forward. Included in this documentation should be:

1. Date and Time
2. Action Taken
3. Location
4. Person performing the action
5. Person performing documentation
6. All personnel involved

E. The card brands (Visa, MasterCard, American Express, Discover, and JCB), payment processer, and acquiring bank will be notified by the PCI Coordinator or the Investment Manager, if necessary. The card brands will determine whether or not an independent forensics investigation will be initiated on the compromised device(s) and location(s).

F. Affected systems will not be brought back online until consultation and approval from the PCI Coordinator, Investment Manager, Director of Information Security, and the Computer Services Center.

## VII. SECURITY AWARENESS

A. Employees with access to cardholder data or involved in any way with processing, storing, or transmitting cardholder data must acknowledge that they have read and understand the USA Payment Card Industry (PCI) Compliance Policy on an annual basis.

B. Additionally, employees with access to cardholder data or involved in any way with processing, storing, or transmitting cardholder data must complete PCI training on an annual basis.

**Contacts:**

1. PCI Coordinator and Cash/Investment Assistant: Drew Underwood 341-4998
2. Investment Manager: Terry Albano 460-6373
3. Director of Information Security: Mark Wilson 460-7767

Effective Date: September 15, 2015

Revised Date: October 15, 2019