University of South Alabama
Payment Card Industry (PCI) Compliance Policy

Policy

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all companies that process, store or transmit payment card information maintain a secure environment. The Payment Card Industry Security Standards Council (PCI SSC) was created in September 2006 by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB) to manage the evolution of the Payment Card Industry (PCI) security standards with focus on improving payment account security throughout the transaction process. The PCI DSS is administered by the PCI SSC.

The University of South Alabama (USA) adheres to the highest standards related to the security of payment card data and must follow the guidelines set by the PCI SSC. Debit cards and credit cards are hereinafter referred to as payment cards.

The following procedures will assist us in being compliant with the standards set forth by the PCI SSC. The policy shall apply to any University-related entity, hereinafter referred to as department/unit that accepts payment cards to conduct business.

A copy of this policy and procedures must be read and signed by the appropriate individuals annually.

Signed copies of this policy will be maintained by the department/unit and the Investment Manager.

Procedures

I. MERCHANTS:
   A. A USA Merchant is any University division, college, department, or business unit that accepts payment cards as a form of legal tender, including retail and Web-based operations.
B. All Merchants must be authorized by the Executive Director of Student Financial Services and the Investment Manager.

C. Any Merchant accepting payment cards on behalf of the University must designate an individual within the department who will have primary authority and responsibility within that department for payment card transactions. This employee shall be referred to as the Merchant Department Responsible Person (MDRP). The Merchant should also specify a back-up, or person of secondary responsibility, should matters arise when the primary person of responsibility is not available.

D. All University employees who have access to payment card data must read and sign the PCI Compliance Policy prior to the handling of payment card information. All personnel who are involved, in any way, with payment cards must acknowledge annually that they have read and understand the University’s PCI Compliance Policy.

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 (CDE) network change, the merchant should notify the Investment Manager so roles and security privileges within the CDE network can be modified if necessary.
   4. When an employee with access to the CDE network leaves employment with the University or transfers out of the Merchant’s department, the merchant must notify the Investment Manager immediately so all user accounts and roles within the cardholder environment that are associated with the employee can be disabled or modified.

B. Payment card data must be kept confidential and secure at all times during the sales process.

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), and fax machines that are not in a secure area.

D. Saving of Cardholder Data (credit card number, cvc code 3 digit code) on electronic media devices is PROHIBITED. Unallowed storage includes, but is not limited to, the following: desktop computers, laptop computers, network server shares (this includes in text files, databases, spreadsheets, word documents, etc.), compact disks, USB flash drives, personal digital assistants, cellphones, tablets and portable external hard drives.

E. Payment card data shall not be stored in paper form, including payment forms, camp registrations, ticket orders, word documents, excel documents, etc. Once the transaction has been processed, destroy payment card information in a crosscut shredder or place in locked containers designated for shredding, incineration or other forms of destruction so that information cannot be reconstructed. Payment card data must be removed from paper forms after authorization is obtained if the paper/form is retained by the Merchant. This data must be removed before it is scanned or stored. Simply obscuring or blacking out the number is not acceptable. Cut the payment card data (at a minimum the card number, PIN, and card verification code) out of the form/paper and destroy the payment card data in the manner noted above.

F. The University will not accept payment card information via email and will not send payment card information via email. In the event an email is received with payment card data for payment, as quickly as possible reply to the email with the message shown below. Before sending the e-mail reply, delete the Cardholder’s Data. Delete the original message after replying.

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 a very unsecure process of providing cardholder information and any other vital information, therefore the email with your cardholder data has been deleted and YOUR PAYMENT HAS NOT BEEN PROCESSED. You may make a payment on our website at _______________. If it is not convenient to make your payment online, we will be happy to take your information over the phone at ________.

G. Payment card payments via phones are strongly discouraged. If in some cases it is necessary to accept payment by telephone, immediately enter payment card data at payment card input device. Do not write down the payment card data.

H. Payment card data is discouraged from being received via Fax. Sending of
payment card data via fax is prohibited. If payment card data is required to be received via fax it is imperative that USA’s receiving fax machine be located in a secure environment where payment information cannot be viewed or accessed by the general public or by University staff and employees who do not have a need to know. Once the payment is processed the cardholder’s data must be destroyed immediately using a crosscut shredder or placed in locked containers designated for shredding, incineration or other forms of destruction so that information cannot be reconstructed.

I. If your office must deliver forms or other correspondence containing cardholder numbers to another office or processing site, 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 from the desk with sensitive information visible. If you must leave, secure cardholder and other sensitive data by locking work papers in your desk or a file cabinet. If payments need to be left in a staff member’s office, do not leave them on a desk; they should be placed in a secure lock box. Limit access to the box.

K. Always close payment card batches daily.

L. Only the last four digits of the cardholder’s data will be displayed on all receipts.

M. Picture ID’s are required for all transactions where the cards are not signed.

N. Manual swipe machines or card imprinters cannot be used.

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 Computer Services Center and the Investment Manager before implementation.

B. All PCs, laptops, and workstations that are involved in any way in the processing of payment card transactions or have access to the Cardholder Data Environment network 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. General purpose computers are defined as any computer for which its use includes: checking email, browsing the web, etc.

2. All payment card processing and interaction with the Cardholder Data Environment network must take place from specifically purposed and properly secured computers and/or equipment.

3. In those instances where a point of sale terminal has the ability to access e-mail and browsing the web and the need to access is vital for business purposes, contact the University’s Computer Center to provide the optimal set-up to secure the connection between the two functions.

D. The University requires management approval for the use or change of any technology (for example remote access technology or the use of Bluetooth or Wireless to connect system components used in processing transactions) connected to the Cardholder Data Environment. Management approval procedures shall be determined by the Investment Manager, in consultation with the Computer Services Center. Users wishing to connect any new device to the CDE environment must first obtain approval from the Investment Manager.

E. Merchants must review hardware and software technologies at least annually to confirm that they continue to be supported by the point of sale vendor and can meet the entity’s security requirements, including PCI DSS. If it is discovered that technologies are no longer supported by the vendor or cannot meet the entity’s security needs, the Merchant should prepare a remediation plan, up to and including replacement of the hardware and software technology, as necessary.

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

G. Devices that capture card data via direct physical interaction with the card (such as card swipe and card dip devices):

1. Merchant must obtain card swipe devices or card dip devices from the Executive Director Student Financial Services (Student Accounting)
2. Merchant must notify the Investment Manager when a card swipe device or card dip device is removed from service. Decommissioned devices must be returned to the Investment Manager for disposal.
3. Merchant must maintain a list of such devices used.
   a. The list must include a description of the device sufficient to identify and locate the device and must include: Make and Model, location within the unit or department, and device serial number. If there is no serial number then some other method of unique identification must be determined.
b. The list must be updated when such devices are added, relocated, or decommissioned.

4. Merchants must develop and document procedures to periodically inspect such devices to detect tampering (for example, the addition of card skimmers to the devices) or substitution (for example, by checking the serial number or other device characteristics to verify that it has not been swapped for a fraudulent device. Note: The majority of terminals will also have a method of displaying the serial number electronically. As part of your regular checks, note the serial number on the back of the terminal and check this against the electronic serial number). 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 or other external markings. Additional skimming prevention information is available on the PCI website at www.pcisecuritystandards.org.

a. Tampering and/or substitution of devices must be immediately reported to the Investment Manager.

H. Personnel within each Merchant’s department must be trained to be aware of attempted tampering or replacement of devices. Training must include the following:

1. 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-- for example, by checking with management or phoning the POS maintenance company (such as the vendor or acquirer) for verification.

2. Do not allow installation, replacement, or the return of devices without verification, and without approval from the department/unit’s management. (One means of gaining access to Cardholder Data is through the unauthorized swapping of equipment).

3. Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).

4. Immediately report suspicious behavior and indications of device tampering or substitution to appropriate personnel (see page 9 and appendix for appropriate personnel).

I. The appropriate firewall set up is required for any computer that processes payment cards. Contact Computer Services for more information.

J. The use of anti-virus software is required on all computers that process payment cards. The anti-virus software must be approved by the Computer Services Center and must be updated daily. Antivirus software shall be installed such that end-users cannot disable or alter settings. Only specifically authorized
administrators may change running configurations of anti-virus software. If not currently installed on any computers within a Merchant’s department, anti-virus software is available through the University’s Computer Services Center and the Merchant’s department is responsible for having the anti-virus software installed on all computers within the Merchant’s department that are involved in processing payment cards.

K. Operating systems on all computers used in the processing of payment cards must be set to auto update security patches. Contact Computer Services for more information.

L. Use of computers, workstations, point-of-sale terminals, and devices used in the processing of payment card transactions and/or connected to the Cardholder Data Environment network must require each user to log-in using a unique user identifier and password.
   1. No group or sharing of user accounts is permitted.
   2. Vendor and service provider accounts shall be issued only to individual users.

M. Passwords:
   1. The passwords should include a combination of special symbols, numbers, and both lower case and upper case letters so that duplication is difficult.
   2. Do not use passwords that have been provided by vendors.
   3. User IDs and passwords must not be shared with others.

N. Auditing (automated audit trails) must be enabled on all CDE system components. If you have any questions regarding this requirement, you should consult with the Computer Services Center.

O. Physical Security:
   1. All equipment used to collect data or process payment card transactions must be secured against unauthorized use in accordance with 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 devices are accessible by the public such as point-of-sale equipment and card readers, consider securing, when possible, the devices to the physical structure of the payment location.

IV. THIRD PARTY VENDORS AND SERVICE PROVIDERS:

A. The Investment Manager with input from the Computer Services Center shall establish a process for engaging point of sale third party vendors and service providers, including proper due diligence prior to engagement.
B. Third parties with whom the University cardholder data is shared must be contractually required to adhere to the PCI DSS requirements and to acknowledge the third parties’ responsibility for Cardholder Data security. Contracts with third-party vendors and service providers must delineate each party’s roles and responsibilities with respect to PCI-DSS compliance. Any agreements with third parties, with whom cardholder data is/will be shared, must be approved by the Investment Manager 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 documented and logged.

C. A list of point of sale third party vendors and service providers shall be maintained by each department/unit and the Investment Manager.

D. The Investment Manager shall maintain a program to monitor vendors’ and service providers’ PCI DSS compliance status, at least annually.

V. SECURITY INCIDENT IDENTIFICATION:
A. Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in day to day activities include, but are not limited to:

1. Theft, damage, or unauthorized access (e.g., papers missing from their desk, 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 substitution of equipment used in processing payment card transactions
7. Unauthorized wireless devices are discovered on the network
8. Lost, stolen, or misplaced sales forms/receipts
9. Lost, stolen, or misplaced payment card data
10. Lost, stolen, or misplaced computers, laptops, hard drives, or other devices that contain payment card data
11. Files containing cardholder account data mistakenly transmitted to an unauthorized party
VI. REPORTING AND RESPONDING TO AN INCIDENT:

A. Alert the following parties immediately of any suspected or actual security incidents involving cardholder data. (See appendix for contact information)
   1. Investment Manager
   2. Executive Director Information Technology
   3. Director of Risk Management and Insurance
   4. Executive Director of Internal Audit and Chief Financial Compliance Officer
   5. Executive Director Student Financial Services (Bursar)

The Investment Manager will contact the bank, and if necessary law enforcement.

The office and cell phone numbers for the parties listed above should be well known to all employees and the phone system should page someone during non-business hours.

6. Employee Communication regarding any suspected or actual incidents should be limited to the employee’s supervisor(s), the Investment Manager, the Computer Services Center, 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 and the Director of Risk Management and Insurance.

B. Employees should document related information while waiting for the Investment Manager or the Computer Services Center 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 through consultation with the Computer Services Center network security group and the Investment Manager. The Computer Services Center network security group shall determine how best 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 any and all steps taken.

D. Upon notification of a suspected incident within the Cardholder Data Environment, 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 (MasterCard, Visa, Discover, American Express) and Payment Processor will be notified by the Investment Manager and the card brands shall determine whether or not an independent forensics investigation will be initiated on the compromised device(s).

F. Affected systems should be physically secured (and remain connected to a power supply) to prevent unauthorized tampering.

G. Affected systems will not be brought back on-line until consultation and approval from the card brands, the Computer Services Center, and the Investment Manager.

VII. SECURITY AWARENESS:
   A. Employees with access to Cardholder Data or involved in any way in the processing and transmission of payment card transactions must annually acknowledge that they have read and understand the University's Payment Card Industry (PCI) Compliance Policy.
   
   B. Additionally, each employee that has direct contact with the credit card process will need to review credit card security videos that pertain to their department. A user id and password will be provided by the Director of Information Security.

VIII. EFFECTIVE DATE
   A. September 15, 2015

IX. POLICY REVISION:
   A. This policy shall be reviewed annually by the Investment Manager and the Executive Director of Information Technology and shall be updated when the Cardholder Data Environment changes (for example, addition of new systems or processes, changes in system or network configurations).
X. **APPLICABILITY**
   A. This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers with access to the University's Cardholder Data Environment, including all personnel affiliated with point of sale third parties. This policy applies to all equipment connected to the University Cardholder Data Environment network.

XI. **POLICY MANAGEMENT**
   A. Responsible Offices: Office of Student Accounting, Investment Manager, and Computer Services Center
   B. Responsible Executives: Executive Director of Student Financial Services, Investment Manager, and Director of Information Security

XII. **DEFINITIONS:**
    See the latest Glossary of Terms, Abbreviations, and Acronyms at the PCI Security Standards Council website, [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org). If questions remain after viewing the PCI Security Standards Council’s latest Glossary of Terms, Abbreviations, and Acronyms, contact the Investment Manager.

XIII. **SANCTIONS:**
    A. Failure to meet the requirements outlined in this policy may result in suspension of the physical and, if appropriate, electronic payment capability with payment cards for affected departments/units. Additionally, if appropriate, any fines and assessments imposed by the affected payment card company will be the responsibility of the impacted departments/units.

    B. Employees in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, up to and including termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

XIV. **EXCLUSIONS:** None

XV. **INTERPRETATION:** This policy is subject to the interpretation of the Investment Manager.

XVI. **This Policy shall be signed by all Department/Unit Heads and all individuals that have access to Payment Card data or are involved in any way in the**
processing and transmission of payment card transactions.

I, the undersigned, have read and understand the University of South Alabama’s PCI Compliance Policy and will to the best of my ability abide by these guidelines.

DEPARTMENT NAME: ________________________________________________________________

Merchant Department Responsible Person (MDRP)

Signature: ______________________________________
Printed Name: ________________________________
Title: ________________________________
Date: ________________________________

Back-up Merchant Department Responsible Person (MDRP) if applicable

Signature: ______________________________________
Printed Name: ________________________________
Title: ________________________________
Date: ________________________________

Signature: ______________________________________
Printed Name: ________________________________
Title: ________________________________
Date: ________________________________

Signature: ______________________________________
Printed Name: ________________________________
Title: ________________________________
Date: ________________________________

Signature: ______________________________________
Printed Name: ________________________________
Title: ________________________________
Date: ________________________________
Please complete, sign, scan and email to the following:

talbano@southalabama.edu

The University of South Alabama

Terry Albano, Investment Manager

Phone: (251) 460-6373
APPENDIX:

1. Investment Manager: Terry Albano (251)460-6373 Cell: (251)709-3353
2. Director of Information Security: Mark Wilson (251)460-7767
3. Director of Risk Management: Connie Cook (251)460-6232
4. Executive Director of Internal Audit and Chief Financial Compliance Officer
5. Executive Director Student Financial Services (Bursar): Rick Schaffer (251)460-6584