UNIVERSITY OF SOUTH ALABAMA

USA Payment Card Industry (PCI) General Merchant Policy

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

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

Signature: _____

Date: November 4, 2019

Payment Card Acceptance Overview

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all entities that process**,** store, and 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.

During the normal course of business, many departments and organizations within the University, including its Hospitals and other affiliates of the University, process credit card transactions subject to the PCI DSS. Mishandling cardholder data associated with payment card transactions may result in the loss of customer data, leading to possible reputational damage or financial loss for the University.

Policy Statement

The University of South Alabama (USA) is required by the credit card associations to be compliant with the PCI DSS and is committed to providing a secure environment to protect cardholders and USA against both loss and fraud. This policy outlines USA's commitment to securely process, store, transmit and dispose of cardholder data by complying with the PCI DSS.

The PCI General Merchant Operating Procedures will provide further guidance on properly processing, storing, and transmitting payment cards while fulfilling the University's responsibility to comply with the PCI DSS.

Applicability

USA adheres to the highest standards related to the security of cardholder data and must follow the guidelines set by the PCI DSS. Compliance with this policy is mandatory for all USA faculty, staff, students, merchants, departments, organizations, third-party vendors, individuals, systems, and networks involved in accepting, processing, transmitting, storing, disposing, or have access to cardholder data. Adherence to this policy will help ensure that cardholder data is protected and kept secure from unauthorized access. A copy of this policy must be read and signed annually by all individuals involved in the payment card process. Signed copies of this policy will be maintained by the respective departments and USA's PCI Coordinator.

Definitions

For purposes of this Policy and the USA Payment Card Industry (PCI) General Merchant Procedures, the following terms and definitions apply:

USA: University of South Alabama and all affiliated organizations including USA Health University Hospital, USA Children's and Women's Hospital, USA Health Care Authority, and all USA clinics.

Cardholder: Someone who owns and benefits from the use of a membership card, particularly a credit card.

Cardholder Data (CHD): any personally identifiable information (PII) associated with a person who has a credit or debit card. Cardholder data includes the primary account number (PAN) along with any of the following data types: cardholder name, expiration date or service code. The term cardholder data is interchangeable with payment card data throughout this policy.

Cardholder Data Environment (CDE): is a computer system or networked group of IT systems that processes, stores and/or transmits cardholder data or sensitive payment authentication data. A CDE also includes any component that directory connect to or supports this network.

Disposal: CHD must be disposed of in a manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, and USB storage devices. The approved disposal methods are: Cross-cut shredding, incineration, or approved shredding or disposal services.

Merchant or Department: a USA department or operating unit that has applied for and been approved to accept credit/debit card payments for goods and/or services. A merchant is assigned a specific merchant account, which is used to process all credit/debit card transactions via a USA-approved payment card processor.

Payment card: refers to both credit and debit cards. Payment card processing is defined as using any application or device to process a credit/debit card transaction as payment for goods and/or services from a USA merchant.

Payment Card Industry Data Security Standard (*PCI DSS)*: a mandated set of requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express and JCB. These security requirements apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as forms of payment.

Self-Assessment Questionnaire (SAQ): a validation tool intended to assist merchants and service providers who are permitted by the payment brands to self-evaluate their compliance with the PCI DSS. This must be completed annually by the PCI Coordinator.

Responsibilities

Primary Guidance

- Payment Card Industry Data Security Standard: https://www.pcisecuritystandards.org
- USA PCI General Merchant Procedures: https://www.southalabama.edu/departments/csc/informationsecurity/pci_policy.html#collapse2
- USA PCI Individual Merchant Policies: https://www.southalabama.edu/departments/csc/informationsecurity/pci_policy.html#collapse3
- USA PCI Individual Technical Infrastructure Policies: https://www.southalabama.edu/departments/csc/informationsecurity/pci_policy.html#collapse4

Responsible University Office and Officer

- Tax Accounting Office: Investment Manager
- Department of Information Security: Director of Information Security

Sanctions

Non-compliance with the PCI DSS can mean that a merchant is vulnerable to breach. For this reason, banks and credit card institutions can apply additional monthly fees to non-compliant merchant accounts or even revoke their ability to accept payment cards.

Failure to meet the requirements outlined in this policy and its related procedures 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.

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.

Exclusions

None

Interpretation

This policy is subject to the interpretation of the Investment Manager, Director of Information Security, and the PCI Coordinator.

Policy Revision

This policy shall be reviewed annually by the PCI Coordinator, Investment Manager, and the Director of Information Security and shall be updated when the Cardholder Data Environment changes.

Policy Execution

This Policy shall be signed by all Merchant Department Responsible Persons (MDRPs) and all individuals that have access to cardholder data or are involved in any way with processing, storing, or transmitting payment card transactions (PCI Users).

I, the undersigned, have read and understand the University of South Alabama's PCI General Merchant Compliance Policy and will, to the best of my ability, abide by this policy.

DEPARTMENT NAME: _____

Merchant Department Responsible Person (MDRP):

Signature: _____

Printed Name: _____

Title: _____

Date: _____

PCI User Signatures:

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Please read, sign, scan and email to the PCI Coordinator:

Drew Underwood, PCI Coordinator and Cash/Investment Assistant

underwood@southalabama.edu

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