Policy Title: BF4023 - Payment Card Industry (PCI) Compliance

Subject Area: Finance

Responsible Official(s): Executive Vice President and Chief Operating and Financial Officer

Responsible Office(s): University and Student Business Services

Policy Statement

In order to accept Payment Cards, the University of Memphis is required to comply with the Payment Card Industry Data Security Standard (PCI-DSS), which is a mandatory set of requirements for protecting Cardholder Data that was developed by the Payment Card Industry Security Standards Council (PCI-SSC). The University has established a compliance program that consists of the requirements contained within this policy.

This policy formally establishes the Payment Card Data Industry Security Standard (PCI-DSS) compliance program at the University of Memphis, grants authority for approval and oversight of payment card acceptance activities and defines broad roles and responsibilities for PCI-DSS compliance activities. The policy applies to all departments, units, and personnel ("Entities") that accept payment cards as payment for goods or services or in any way engage in payment card handling in support of the mission of the University of Memphis. Payment card handling includes transmission, storage, and/or processing of payment card data (electronic or hard copy) on behalf of the University or affecting the security of cardholder data.

Definitions

Acquirer – An Acquirer may also be referred to as "merchant bank", "acquiring bank", or "acquiring financial institution". Entity, typically a financial institution, which processes payment card transactions for merchants and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding merchant compliance.

University – The University of Memphis which is all encompassing and includes all units.

Cardholder Data/Information – A cardholder data or information would be the personal account number (or credit card number), name on the card, expiration date, and Card Validation Code. This information can also be considered any information stored on the magnetic stripe or chip of a payment card that could potentially be used for fraudulent

activities.

Cardholder Data Includes:	Sensitive Authentication Data Includes:
Primary Account Number (PAN)	Full magnetic stripe data or equivalent on a chip
Cardholder Name	
Expiration Date	CAV2/CVC2/CVV2/CID
Service Code	PINs/PIN blocks

Payment Brands – An organization with branded payment cards or other payment card form factors. Payment brands regulate where and how the payment cards or other form factors carrying its brand or logo are used. A payment brand may be a PCI-SSC Participating Payment Brand or other global or regional payment brand, scheme, or network. Five members of the PCI-SSC, but not limited to: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and VISA Inc.

Payment Card – For purposes of PCIDSS, any card form factor that bears the logo of a Payment Brand that is used for payment. Examples include credit and debit cards.

Merchant – Any University entity that accepts payment cards via any means as payment of goods and/or services. Examples of merchants may include, but are not limited to: academic departments, business units.

Primary Account Number – Unique payment card number (credit, debit, or prepaid cards, etc.) that identifies the Payment Card issuer and the cardholder account.

PCI Committee – The PCI Committee is composed of representatives appointed by the Executive Vice President and Chief Operating and Financial Officer, charged with overseeing the implementation of this policy.

PCI-DSS – An acronym for “Payment Card Industry Data Security Standards.” This is a security standard consisting of 12 overarching requirements established by the PCI-SSC that all Merchants and Service Providers must follow in order to secure credit card transactions.

PCI-SSC – An acronym for "Payment Card Industry Security Standards Council." The PCI-SSC is led by a policy setting Executive Committee, composed of representatives from the five founding global payment brands and strategic members. The council provides a variety of tools, questionnaires, guidance, FAQ's, training resources and other materials and information to assist organizations seeking to achieve compliance with its standards.

SAQ –An acronym for “Self-Assessment Questionnaire.” This would be the tool used by any entity to validate its own compliance with PCI-DSS.

PCI Scope – All people, technology, and processes that support payment card handling.

Service Provider – A business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data.

Policy

Cardholder data may never be stored, transmitted, or processed via any means without review and approval by the PCI Committee. Any Entity that wishes to begin accepting payment cards as payment for goods or services, or already accepts payment cards but wishes to add new payment acceptance methods or service providers, must initiate a compliance review with the PCI Committee and obtain approval from the Executive Vice President and Chief Operating and Financial Officer prior to commencing new payment card acceptance activities. Following approval, custody and life cycle activities of any physical equipment and associated merchant accounts used for processing payment card information must be authorized, tracked, and monitored by representatives of the PCI Committee.

This policy is intended to be used in conjunction with the Payment Card Information Classification and Control requirements in Section 6.2.3.5 of the State of Tennessee's Enterprise Information Security Policy. Failure to comply with this policy may jeopardize the University of Memphis's ability to accept payment cards and could result in fraudulent transactions, as well as significant financial and reputational damage to the University of Memphis.

PRINCIPLES:
All individuals involved with payment card handling must:

- Comply with the requirements of the PCI-DSS.
- Comply with any payment card policies, procedures, and standards established by the University and the State of Tennessee.

Roles and Responsibilities

Executive Vice President and Chief Operating and Financial Officer

The Executive Vice President and Chief Operating and Financial Officer is responsible for this policy and for the PCI-DSS Compliance program at the University, including the appointing of the members of the PCI Committee, submission of PCI-DSS attestation documents to the University acquiring bank(s), and for overall enforcement of this policy.

PCI Committee

The PCI Committee consists of appointed representatives of Finance, USBS, Procurement, ITS, Internal Audit, Information Security, Advancement, and FedEx Institute. The PCI Committee is

responsible for reviewing all submitted documentation from Merchant areas to confirm that the PCI scope of the University is limited to only that which is needed to support the mission of the University of Memphis.

The PCI Committee will review the University's PCI scope, at a minimum annually and upon any credit card payment process change. The PCI Committee may engage the services of a PCI-DSS service provider to perform a PCI-DSS gap analysis and to identify any opportunities for reducing PCI scope.

The PCI Committee will review any new or updated procurement and implementation requests submitted by Merchants or University Procurement that support credit card transactions to determine any impacts to the University's PCI Scope and for compliance with the PCI-DSS prior to approval. The PCI Committee will provide PCI-DSS compliance tools for Merchant areas, including required annual and upon-hire awareness training, as well as and the appropriate PCI-DSS forms and tools to Merchant area leadership for completion annually.

Merchants

Merchant area leadership are responsible for local enforcement of this policy in their area(s). This includes:

- Ensuring that no cardholder data is retained following transaction authorization; and
- Performing an annual review/update of all payment card handling operating procedures; and
- Ensuring that all persons involved in payment card handling receive the PCI Committee provided training annually and at hire; and
- Ensuring that the access of all persons to cardholder data is strictly limited to business needs; and
- Annual submission of the following merchant area documentation to the PCI Committee:
    - Self-Assessment Questionnaire (SAQ) as assigned by the PCI Committee;
    - Current PCI DSS roles, responsibilities, and operating procedures;
    - List of persons involved in payment card handling;
    - Up-to-date inventory of technology in PCI-DSS scope;
    - Payment terminal inspection logs (if relevant).
- Submission of compliance documentation of service providers to the PCI Committee annually and prior to contract initiation; and
- Obtaining the required PCI DSS compliance documentation of service providers on an annual basis and prior to contract initiation. Documentation that must be obtained from the service provider includes, but is not limited to:
    1. PCI-DSS Attestation of Compliance that is less than 1 year old; and
    2. PCI-DSS Responsibilities Matrix for each service or solution to be provided by the service provider; and

3. Payment card data flow diagram of any transaction flows the service provider is supporting with the proposed solution or service.

Merchant area leadership are responsible for ensuring that all payment card handling activities are approved by the PCI Committee and compliant with this policy. Merchants are responsible for ensuring that all persons within their area(s) are properly trained prior to authorizing those persons to engage in payment card handling activities. Merchants are responsible for documenting current roles and responsibilities for all payment card activities in their areas. Merchants that wish to add/change their method of accepting payment cards or to engage any service provider to support payment card transactions must first contact the PCI Committee for review and approval.

Exceptions

Exceptions to this policy must be documented and submitted to the PCI Committee and approved by the Executive Vice President and Chief Operating and Financial Officer. Exceptions will be reviewed on a case-by-case basis, and will only be approved if a compelling business, legal, or regulatory need exists.

Related Tools/Policies

This policy should be used in conjunction with the State of Tennessee Enterprise Information Security Policy , the University Cash Handling Guide, Processing Payment Card Transactions, Cash Receipting Training, ITS Data Security Policy, and the BF4013 - Red Flag Policy . Failure to follow these policies and procedures could result in revoking the department's/activity's ability to accept payment cards and disciplinary action as deemed appropriate by University leadership.

Last Revision Update Log: 12/03/2024

BF4023 – Supersedes UM1762 March 31, 2018
UM1762 – Revised November 23, 2016
UM1762 – January 21, 2016
UM1762 – Issued: October 2, 2013
BF4023 – Revised March 31, 2018