FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Payment Card Processing # 1110.025

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
April 8, 2010	January 4, 2024	Office of the Controller Information Security Office

POLICY STATEMENT

All Florida International University (FIU) departments/units that collect, process, transmit and/or store cardholder data must comply with all the requirements of the latest version of the Payment Card Industry Data Security Standard (PCI DSS).

Departments that anticipate payment card (i.e. debit or credit card) acceptance for goods and/or services must be approved by the FIU PCI Compliance team which is comprised of members from the Controller's Office and the Division of IT. The provisions of this policy also apply to all existing University departments that have previously been approved for payment card processing. Departments that use third party vendors to accept payment cards are also subject to compliance requirements of this policy, this includes vendors providing goods/or and services on campus, other entities or organizations that process payment cards at, with, or for FIU.

SCOPE

This policy applies to all faculty, staff, students, organizations, third-party vendors, individuals, systems, and networks involved with payment card handling. This includes transmission, storage, and/or processing of payment card data, in any form (electronic or paper).

REASON FOR POLICY

The University has a fiduciary responsibility to protect our customers' payment card information. Cardholder data is of high value to malicious individuals because the information can be used for fraudulent purposes. Therefore, we must ensure that appropriate safeguarding measures are in place to protect cardholder data and continuously demonstrate PCI DSS compliance.

The PCI DSS is a set of comprehensive requirements for enhancing cardholder data security, which is intended to help organizations proactively protect cardholder data and was developed by the founding payment brands (i.e. Visa, Mastercard, Discover, American Express, and JCB) of the Payment Card Industry Security Standards Council. All payment card activity on behalf of FIU, at the University, or using FIU resources must comply with the PCI DSS. Failure to comply may result in fines, legal liability, reputation damage and loss of business.

DEFINITIONS	
TERM	**DEFINITIONS**
Acquirer	Also referred to as "acquiring bank" or "acquiring financial institution". Entity that initiates and maintains relationships with merchants for acceptance of payment cards.
Approved Scanning Vendor (ASV)	Company approved by the PCI Security Standards Council to conduct scanning services to identify common weaknesses in system configuration.
Business Need-to-Know	When an employee's access rights are granted to only the least amount of data and privileges needed to perform a job.
Cardholder Data	At a minimum, cardholder data contains the full primary account number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, service code, and/or other sensitive authentication data.
Cardholder Data Environment (CDE)	Area of computer system network that processes cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.
Data Breach	A data breach is an incident in which sensitive data may have potentially been viewed, stolen, or used by an unauthorized party.
FIU Network	The FIU Network is a high-performance series of interconnections which connects the FIU community, providing access to departmental computing resources, FIU system resources, as well as Internet connectivity. The network enables any person and/or device with network connectivity access to any FIU service both on-and off-campus. The network is designed to be highly reliable and operational 24 hours a day, 365 days a year.
Malware	Malicious software designed to infiltrate a computer system with the intent of stealing data, or damaging applications or the operating system. Such software typically enters a network during

	many business approved activities such as via email or browsing websites.
Merchant	A University department approved to accept payment cards at a given location as payment for goods and/or services or receipt of donations.
Merchant ID Number (MID)	A unique number that identifies the University department approved to accept payment cards.
Payment Card Application	Any hardware, software, or combination of hardware and software that aid in the processing, transmitting or storing of cardholder data as part of authorization or settlement. Examples include: point of sale (POS) devices, e-commerce shopping carts, web-based payment applications and third party (vendor) provided systems.
Payment Card Industry Data Security Standard (PCI DSS)	PCI DSS is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands. The PCI DSS includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. The PCI DSS may be accessed at: https://www.pcisecuritystandards.org/.
Self-Assessment Questionnaire (SAQ)	A validation tool intended to assist merchants and service providers in self-evaluating their compliance with the PCI DSS. There are multiple types of the PCI DSS SAQ to meet various payment card processing scenarios. Each unique version of the PCI DSS SAQ includes a Self-Assessment Questionnaire and Attestation of Compliance, which must be completed annually by the merchant and/or service provider as appropriate. The FIU PCI Compliance Team will assist you in the selection and completion of the SAQ for your merchant location.
Payment Card Processing	The processing, transmitting and/or storing of cardholder data, i.e. acceptance of credit or debit cards.
Primary Account Number (PAN)	Unique number for credit and debit cards that identifies the cardholder account.
Qualified Security Assessor (QSA)	A company approved by the PCI Security Standards Council to validate an entity's adherence to PCI DSS requirements.

Service Provider	A business entity that provides various services to merchants. Typically, these entities store, process, or transmit card data on behalf of another entity (such as a merchant) OR are managed service providers that provide managed firewalls, intrusion detection, hosting, and other IT-related services.
Vulnerability Scan	A software tool that detects and classifies potential weak points (vulnerabilities) on a computer network.

ROLES AND RESPONSIBILITIES

Compliance with PCI DSS is a continuous process involving three steps:

- Assess –the process of assessing the business processes and information technology assets for payment card processing and analyzing them for vulnerabilities that could expose cardholder data.
- Remediate –the process of fixing those vulnerabilities, including unsafe practices in payment card processing and technical flaws in software, hardware, and network configurations. , .
- Report –the process that entails the compilation of records required by PCI DSS to validate remediation and submission of compliance reports as required by acquirer.

Office of the Controller – responsibilities include:

- Assist merchants with assessing their business process for payment card processing, remediation of vulnerabilities, and compliance reporting related thereto
- Verifying that merchants comply with this policy, PCI DSS, and University policies defined in "Related Sources" regarding business process for payment card processing
- Overseeing the policies and procedures on payment card processing including issuance of merchant number and revocation of merchant number if merchant fails to comply with this policy
- Review and approve third party vendor contracts that are related to the University handling cardholder data and/or when FIU acts as a service provider

Division of Human Resources – responsibilities include:

- Conduct appropriate level of background checks for employees who will have access to, or otherwise handle, cardholder information upon the department's request consistent with applicable law and University policies.

Division of Information Technology – responsibilities include:

- Assist merchants with assessing information technology assets for payment card processing, remediation of vulnerabilities, and compliance reporting related thereto
- Verifying that merchants comply with this policy, PCI DSS, and University policies defined in "Related Sources" regarding information technology assets for payment card processing
- Operations and maintenance of the FIU data networks and the establishment of information technology security policies and standards
- Perform applicable vulnerability scans and penetration testing
- Review vendor contracts which deal with credit card data and PCI
- Assist with the selection of validated P2PE devices
- Provide security awareness training reports
- Overseeing the conduct of internal and external cardholder data environment controls at the appropriate intervals
- Work with QSA and Controllers Office to review SAQs for attestation of PCI compliance

Office of the General Counsel (OGC) – responsibilities include:

- Review merchant related contracts that exceed $75k
- Review e-commerce refund and privacy policies

Office of Business Services - responsibilities include:

- Ensure that vendors that are connected to the FIU network are PCI DSS compliant
- Oversight of new and existing vendors/tenants that process payment cards
- Engage the PCI Compliance Team for review and approval of new or existing vendor contracts from a PCIDSS compliance perspective
- In conjunction with the PCI Compliance Team conduct an annual assessment of existing contracts to verify they are compliant with the latest PCI DSS, this policy, and University policies defined in "Related Sources"
- Annually obtain the Attestation of Compliance (AOC) from third-party vendor s and communicate information to the PCI Compliance Team

Merchants (University Department) – responsibilities include:

- Analyzing your business process and technical components for improvements
- Timely remediation of vulnerabilities
- Compliance reporting related thereto including completion of annual forms, questionnaires, on-site reviews, third-party vendor verification, on-boarding employee verification, timely removal of any employee access, etc.

- Notify Controller's Office and Division of Information Technology immediately in the event of any suspected payment card processing security breach, including those of any vendor or tenant
- Users processing credit cards and users with access to cardholder data are required to complete the IT Security Awareness training and the PCI training annually
- Comply with this policy and PCI DSS

Initial Merchant Requirements

Arrangements must be made through the Controller's Office to obtain prior approval to process payment cards. The appropriate Controller's Office forms and annual PCI DSS Self-Assessment Questionnaire (PCI DSS SAQ) must be completed. This applies to a new merchant as well as any existing merchant that have a significant change from the original application (i.e., business purpose, change in software and/or payment application, etc.). Refer to the Merchant Services/PCI DSS Compliance Manual for approved methods of payment card processing, employee requirements, and consequences of non-compliance.

Applications will be reviewed to ensure that all data related to payment card processing meets, at a minimum, the following criteria:

1) University policies defined in "Related Sources" and
2) FIU's summary list of security requirements based on the PCI Data Security Standards (listed in below)

Build and Maintain a Secure Network
Requirement 1: Use validated point-to-point encryption devices or cellular enabled POS devices to process credit card transactions for all methods of payment except for customer-self driven e-commerce sites where a device is not applicable
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data
Requirement 3: Merchants should not store sensitive cardholder data
Requirement 4: Transmission of cardholder data across open, public networks is not permitted. FIU Merchants must use a validated point-to-point encryption device or cellular enabled POS device to process credit card payments

Maintain a Vulnerability Management Program
Requirement 5: Use and regularly update anti-virus software
Requirement 6: Update all operating systems and software applications regularly
Requirement 7: Restrict access to cardholder data by business-need-to-know
Implement Strong Access Control Measures

Requirement 8: User accounts and passwords must be maintained and reviewed on a quarterly basis.
Requirement 9: Maintain physical security of the cardholder data environment.
Requirement 10: Log and monitor access to system components
Requirement 11: Review internal and external scan reports to address any vulnerabilities

Adhere to the University Information Security Policy
Requirement 12: Comply with this policy

RELATED RESOURCES

FIU Policies

- Gramm-Leach-Bliley Act –Safeguards to Protect Confidential Financial Information (Information Technology Policy No. 1930.015)https://policies.fiu.edu/policy/129
- Information Technology Security (Policy No. 1930.020) (if AFSCME, PBA or SEIU see appropriate policy)https://policies.fiu.edu/policy/96
- Cash Control Policy (Finance and Administration Policy No. 1110.010)https://policies.fiu.edu/policy/576
- Preventing Identity Theft on Covered Accounts Offered or Maintained by FIU (Finance and Administration Policy No. 1110.032) https://policies.fiu.edu/policy/594
- Address Validation Requirements in Connection with Covered Accounts Offered or Maintained by FIU (Finance and Administration Policy No. 1110.002) https://policies.fiu.edu/policy/595
- Background Check Requirements (Policy No. 1710.257) https://policies.fiu.edu/policy/76

FIU Procedures

- Data Stewardship (Information Technology Procedure No. 1930.020a) https://policies.fiu.edu/procedure/560
- Merchant Services/PCI DSS Compliance Manual https://controller.fiu.edu/wp-content/uploads/sites/24/2020/06/MerchantServicesPCI-DSSComplianceManual.pdf

CONTACTS

Office of the Controller
Merchant Services
11200 SW 8th Street, CSC 410
Miami, FL 33199
Telephone: 305-348-2161

Information Security Office
11200 SW 8th Street, PC531
Miami, FL 33199
Telephone: 305-348-7807

HISTORY

Initial Effective Date: April 8, 2010
Review Dates (*review performed, no updates*): N/A
Revision Dates (*updates made to document*): January 24, 2012 to replace the reference to "FIU PantherCard" with "FIU One Card" July 20, 2018; November 17, 2020, January 4, 2024.