PAYMENT CARD PROCESSING

Policy Statement
Payment Card Processing (the processing, transmitting and/or storing of cardholder data, i.e. acceptance of credit or debit cards) by University departments shall comply with the Payment Card Industry Data Security Standard (PCI DSS). All University departments or units that will accept payment via debit or credit card in support of their operations or activities must be approved through the Office of the Controller. The provisions of this policy also apply to all University departments which support payment card processing. Departments that use third party vendors to accept these credit or debit card payments are also subject to this policy.

Reason for Policy
Cardholder data is of high value to malicious individuals because the information could be used to generate fake payment cards and create fraudulent transactions. Therefore, a merchant must ensure that appropriate safeguarding measures are in place to protect cardholder data.

The PCI DSS is a set of comprehensive requirements for enhancing cardholder data security (intended to help organizations proactively protect cardholder data) that was developed by the founding payment brands of the Payment Card Industry Security Standards Council. All merchants and service providers are required to comply with the PCI DSS. Failure to comply with the PCI DSS may result in fines, legal liability, reputation damage and loss of business.

Related Information
FIU Policies
Gramm-Leach-Bliley Act – Safeguards to Protect Confidential Financial Information (Information Technology Policy No. 1930.015)
Information Technology Security (Policy No. 1930.020) (if AFSCME, PBA or SEIU see appropriate policy)
Cash Control Policy (Finance and Administration Policy No. 1110.010)
Preventing Identity Theft on Covered Accounts Offered or Maintained by FIU (Finance and Administration Policy No. 1110.032)
Address Validation Requirements in Connection with Covered Accounts Offered or Maintained by FIU (Finance and Administration Policy No. 1110.002)
Pre-Employment Requirements (Human Resources Policy No. 1710.257)

FIU Procedures
Data Stewardship (Information Technology Procedure No. 1930.020a)
Payment Card Processing Procedures

Definitions
Account Number – The unique payment card number (credit or debit card) that identifies the issuer and the particular cardholder account. Also referred to as “PAN” or “Account Number”.

Acquirer – Also referred to as “acquiring bank” or “acquiring financial institution”. Entity that initiates and maintains relationships with merchants for acceptance of payment cards.
**Cardholder** – Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.

**Cardholder Data** – At a minimum, cardholder data contains the full 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.

**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 Number** – A unique number that identifies the University department approved to accept payment cards.

**Payment Card** – Any credit, debit or private label card accepted as a form of payment for goods and/or services or receipt of donations.

**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 standard is maintained by the Payment Card Industry Security Standards Council, which maintains both the PCI DSS and a number of other standards, such as the Payment Card Industry PIN Entry Device security requirements (PCI PED) and the Payment Application Data Security Standard (PA-DSS).

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/](https://www.pcisecuritystandards.org/).

**Payment Card Industry Data Security Standard Self-Assessment Questionnaire (PCI DSS SAQ)** – The PCI DSS SAQ is a validation tool intended to assist merchants and service providers in self-evaluating their compliance with the PCI DSS. There are multiple versions of the PCI DSS SAQ to meet various 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.

**Payment Card Processing** – The processing, transmitting and/or storing of cardholder data, i.e. acceptance of credit or debit cards.

**Primary Account Number (PAN)** – The unique payment card number (credit or debit card) that identifies the issuer and the particular cardholder account. Also referred to as “PAN” or “Account Number”.

---

**PROCEDURES (O*)**

**MERCHAND REQUIREMENTS**

**Becoming a Merchant to Accept Credit Cards or Debit Cards at FIU**

Arrangements must be made through the Controller’s Office to obtain a merchant number and approval to accept payment cards for payment of goods and/or services, or receipt of donations. The appropriate Controller’s Office forms and PCI DSS Self Assessment Questionnaire (PCI DSS SAQ) must be completed. This applies to a new merchant as well as any existing merchant who is planning to make changes from the original application (i.e., significant changes to the business process used by a department to accept payment cards, changes in products and/or services being sold, changes in third party vendor, etc.).

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

1) University policies defined in “Related Information” and
2) PCI DSS 12 security requirements (grouped in six goals) including:

**Build and Maintain a Secure Network**
*Requirement 1:* Install and maintain a firewall configuration to protect cardholder data  
*Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters

**Protect Cardholder Data**  
*Requirement 3:* Protect stored cardholder data  
*Requirement 4:* Encrypt transmission of cardholder data across open, public networks

**Maintain a Vulnerability Management Program**  
*Requirement 5:* Use and regularly update anti-virus software  
*Requirement 6:* Develop and maintain secure systems and applications

**Implement Strong Access Control Measures**  
*Requirement 7:* Restrict access to cardholder data by business need-to-know  
*Requirement 8:* Assign a unique ID to each person for the use of the computer that contains cardholder data  
*Requirement 9:* Restrict physical access to cardholder data

**Regularly Monitor and Test Networks**  
*Requirement 10:* Track and monitor all access to network resources and cardholder data  
*Requirement 11:* Regularly test security systems and processes

**Maintain an Information Security Policy**  
*Requirement 12:* Comply with this policy

**Engaging Employees**  
Departments are responsible for ensuring that employees who will be involved in payment card processing, or have access to such data, have:

1. Reviewed the University’s Payment Card Processing Policy  
2. Completed a background check before being granted access to cardholder information. All background checks must be conducted by the Division of Human Resources in accordance with applicable law and University policies.  
3. Completed the Identity Theft Prevention Training (FTC Red Flags Rule)  
4. Obtained access to PeopleSoft through the proper channels  
5. Completed payment card processing training, according to the “method of payment” selected  
6. Completed training on how to create payment card processing journals  
7. Signed an Employee Statement of Understanding Regarding Payment Card Processing

**Approved Methods of Payment Card Processing**  
Merchants that want to provide payment card processing must utilize one or more of the following approved methods:

1. Point of sale terminal (electronic payment card terminal) procured through FIU’s payment card processor  
2. Internet payment card application recommended by FIU’s payment card processor and implemented through the Division of Information Technology Enterprise Web Services.  
3. Hosted solution by third-party vendor that is PCI DSS compliant and approved by the Division of Information Technology  
   (Note: only PCI DSS compliant vendors may be used; proof of compliance with PCI DSS must be in writing from a Qualified Security Assessor or other credible source, i.e. MasterCard, Visa, etc; and all software contracts and purchase orders must include non-disclosure and/or confidentiality statements.)

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

1. Assess – the process of assessing the information technology assets and business processes for payment card processing and analyzing them for vulnerabilities that could expose cardholder data.
2. Remediate – the process of fixing those vulnerabilities, including technical flaws in software code or unsafe practices in payment card processing.

3. 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.

**RESPONSIBILITIES (O*)**

Controller’s Office – responsibilities include:

1. Assist merchants with assessing business process for payment card processing, remediation of vulnerabilities, and compliance reporting related thereto
2. Verifying that all merchants are in compliance with this policy, PCI DSS, and University policies defined in “Related Information” regarding business process for payment card processing
3. 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 University policies regarding payment card processing

Division of Human Resources – responsibilities include:

1. Conduct 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:

1. Assist merchants with assessing information technology assets for payment card processing, remediation of vulnerabilities, and compliance reporting related thereto
2. Verifying that all merchants are in compliance with this policy, PCI DSS, and University policies defined in “Related Information” regarding information technology assets for payment card processing
3. Operations and maintenance of the FIU data networks and the establishment of information technology security policies and standards in compliance with PCI DSS, federal, state and local regulations
4. Overseeing the conduct of internal and external cardholder data environment controls at the appropriate intervals

Office of Business Services-responsibilities include:

1. Ensure that third party vendors for which Florida International University permits the FIU One Card (debit card) to be used as payment are PCI DSS compliant

University Department – responsibilities include:

1. Assessing business process and information technology assets for payment card processing, remediation of vulnerabilities, and compliance reporting related thereto including completion of annual forms, questionnaires, attestations, audits, etc.
2. Ensure that all University department merchants are in compliance with this policy, PCI DSS, University regulations, and University policies included in “Related Information”
3. Notify Controller’s Office and Division of Information Technology immediately in the event of any payment card processing security breach

**HISTORY (R*)**

Effective Date: April 8, 2010; Revised on January 24, 2012 to replace the reference to “FIU PantherCard” with “FIU One Card.”
**RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT (R*)**

Office of Finance and Administration  
Florida International University

**RESPONSIBLE ADMINISTRATIVE OVERSIGHT (R*)**

Office of the Controller  
11200 SW 8th Street - CSC 420  
Miami, FL 33199  
Telephone Number: (305) 348-2560

IT Security Office  
Division of Information Technology  
3000 N.E. 151st Street - LIB 328  
Miami, FL 33181  
Telephone Number: (305) 919-4299

* R = Required  * O = Optional

The University Policies and Procedures Library is updated regularly. In order to ensure a printed copy of this document is current, please access it online at [http://policies.fiu.edu/](http://policies.fiu.edu/).

For any questions or comments, the “Document Details” view for this policy online provides complete contact information.