UF | UNIVERSITY of FLORIDA

Office of the Vice President and Chief Financial Officer
Finance and Accounting Division

Purpose:

To define a governance model that will ensure the privacy and security of payment card data stored, processed, or transmitted by the University of Florida, together with the approach to the development, approval and maintenance of resulting payment card policies and standards.

Scope:

This policy covers all payment card usage for the entire UF enterprise, including the University of Florida and Direct Support Organizations (DSOs), as defined in the UF Annual Financial Report.

Policy:

1) **Terms of Use**

   All credit card usage at the University of Florida must be approved by Treasury Management (TM). New credit card merchant applications must be signed by a Manager, Dean or Department Head and approved by Treasury Management.

   Departments must have acceptable infrastructure and resources in place, such as:

   ➢ Must use banking institutions and accounting processes approved by applicable governing board
   ➢ Must agree to meet Payment Card Industry (PCI) defined requirements, as noted in the UF Directives and Procedures (storage, processing and transmission of card holder information)
   ➢ Must preserve the confidentiality of cardholder information
   ➢ Must have acceptable internal controls (i.e. timely reconciling, dual controls, etc.)

2) **Credit Card Information Storage**

   It is permitted to store in paper format only the following elements of credit card information:

   ➢ The last four digits of the Primary Account Number (PAN)
   ➢ Cardholder's name
   ➢ Expiration Date

Policy Number:	Policy Family:	Category:	Effective Date:
PCC-01	Controller's Office	Policy Category	01/01/2014

Revised: **12/06/2013**   Page **1** of **3**

The storage of this information in electronic format is only allowed if approved by Treasury Management, and the Primary Account Number must be rendered unreadable."

3) **Processing Methods**

Allowable processing methods are:

- ➢ Online payments (E-Commerce)
- ➢ Swiping machines (face-to-face, mail order/telephone order)
- ➢ Mobile devices
- ➢ Approved third party vendors – Any contract with a third party vendor must include the vendor's obligation to provide an Attestation of Compliance on demand at all times.

4) **PCI Standards and Audit/Monitoring Requirements**

The University will establish a single Qualified Security Assessor (QSA) relationship for the entire UF enterprise. All UF merchants will use this relationship unless an alternative QSA is approved by Treasury Management. At minimum, UF unit/departments accepting payment cards must submit an annual PCI Self-Assessment Questionnaire and are subject to audit/review. Applicable IP addresses are subject to vulnerability scanning, to be performed no less than quarterly as per applicable PCI requirement. However, monthly scans are highly recommended.

5) **Training**

All UF enterprise employees, and student workers of entities defined in the scope of this policy, as well as personnel of third party vendors operating on university property who process, store or transmit credit card information must complete the appropriate on-line UF PCI training module at hire and annually.

Responsibilities:

1. Policies are recommended by the Payment Card Committee and approved by the Chief Financial Officer (CFO).

1. The University of Florida Treasury Management will establish standards to govern the secure processing of credit and debit cards at the University of Florida.

Policy Number:	**Policy Family:**	**Category:**	**Effective Date:**
PCC-01	Controller's Office	Policy Category	1/1/2014

Revised: **12/06/2013**   Page **2** of **3**

2. The University of Florida Office of the Vice President and Chief Financial Officer will provide guidance to assist units in complying with these requirements.

3. All members of the University of Florida constituency who are currently processing, storing, or transmitting payment card information are required to be compliant with the Payment Card Industry Data Security Standard (PCI DSS).

4. All members of the University of Florida constituency will report a suspected breach of payment card information to the University Privacy Office and Treasury Management immediately upon detection of such breach.

Authority:

The CFO provides oversight and authority for the payment card environment for the entire UF enterprise. The CFO chairs the Payment Card Committee who acts in a consultative and fact finding role to assist in the development of payment card policies.

References:

Directives and Procedures on the use of Payment Cards at the University of Florida

Policy Number:	Policy Family:	Category:	Effective Date:
PCC-01	Controller's Office	Policy Category	1/1/2014

Revised: **12/06/2013**

Page **3** of **3**