Office of the President
University Policy

SUBJECT: PAYMENT CARD SECURITY	**Effective Date:** 8-21-17	**Policy Number:** 12.8	
	Supersedes: New	**Page** 1	**Of** 2
	Responsible Authority: Associate Provost and Chief Information Officer		

APPLICABILITY/ACCOUNTABILITY:

This policy is applicable to all users and systems that accept or process payment cards on behalf of the University.

POLICY STATEMENT:

This policy sets basic controls and responsibilities for the handling of payment cards including credit cards to comply with the Payment Card Industry Data Security Standard and additional safeguards as determined by the University.

I. POLICY

a. Responsibility for the information security of payment card operations is assigned to the Director of Information Security including, but not limited to, the following:
   a. Establishing, documenting, and distributing security policies and procedures
   b. Monitoring and analyzing security alerts and information and distributing to appropriate personnel
   c. Establishing, documenting, and distributing security incident response procedures as appropriate

b. Acceptance of payment cards including credit cards and debit cards must be approved through the Controller's Office. The Controller's Office will work with the Director of Information Security to ensure that appropriate security measures are in place to secure payment card transactions.

c. All contracting of third parties to accept or process payment card transactions on behalf of the University must be approved by the Controller's Office and the Director of Information Security.

d. An inventory list of devices and services utilized for the acceptance or processing of payment cards will be maintained by the Controller's Office. It is the responsibility of departmental staff to ensure that the Controller's Office has a current inventory of devices in its department.

e. The Director of Information Security will maintain documented minimum safeguards for protecting payment card data handled by the University.
f. All devices that accept or process payment cards must adhere to the current minimum safeguards as documented and defined by the Director of Information Security.
g. Documented minimum safeguards are evaluated against systems for compliance prior to a system being approved for use.
h. If a documented set of safeguards changes, advance notice will be provided to system operators prior to the new safeguards becoming mandatory if feasible through consultation between the Director of Information Security and the Controller's Office.
i. All FAU employees who handle credit cards on behalf of the University are required to take applicable training on an annual basis. This training will cover, at a minimum, Security Awareness and PCI Training.

II. SANCTIONS

Violations of the policies and laws described herein by an employee are grounds for disciplinary action up to and including termination in accordance with applicable University and the Florida Board of Governors regulations and/or collective bargaining agreements. Such disciplinary actions may also include reprimand or suspension. Violations of these policies and laws by any users are grounds for terminating their use of University technology resources and other appropriate sanctions.

Disciplinary or other action taken by the University does not preclude the possibility of criminal charges, as appropriate. The filing of criminal charges similarly does not preclude action by the University.

III. INITIATING AUTHORITY: Associate Provost and Chief Information Officer

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: _12.8__

Initiating Authority
Signature: ____ Date: ___________
Name: Jason Ball

Policies and Procedures
Review Committee Chair
Signature: ____ Date: ____________
Name: Elizabeth F. Rubin

President
Signature: ____ Date: ____________
Name: Dr. John Kelly

Executed signature pages are available in the Office of the General Counsel