University of Central Florida

Office of the President

SUBJECT: Credit Card Merchant Policy	Effective Date: 11/28/2016	Policy Number: 3-206.5	
	Supersedes: 3-206.4	Page 1	Of 2
	Responsible Authority: University Controller		

DATE OF INITIAL ADOPTION AND EFFECTIVE DATE 01/12/06

APPLICABILITY/ACCOUNTABILITY

This policy applies to any employee, contractor, agent, or third-party service provider who stores, processes, or transmits cardholder data on behalf of university merchants accepting credit or debit cards. This policy applies to all credit and debit card transactions.

POLICY STATEMENT

University merchants are required to comply with the procedures contained within the online UCF Credit Card Merchant Procedures Manual. These procedures are designed to protect cardholder data; maximize the university's compliance with its merchant services provider contract, which includes compliance with the Payment Card Industry's Data Security Standards (PCI DSS) and the various credit card brand standards; and to ensure appropriate integration with the university's financial and other systems.

Each university merchant's dean, director, or chair (DDC) or their appropriate designee is responsible for compliance with this policy and the related procedures in the "UCF Credit Card Merchant Procedures Manual." The person assigned as the appropriate designee must have a sufficient level of management authority within the department.

DEFINITIONS

Cardholder data. All information pertaining to credit and debit cards and their owners. Commonly used elements of cardholder data include the account number, cardholder's name, expiration date, and the security or validation (CVV) code displayed on the card. Cardholder data includes all of these elements and any other information digitally stored on the magnetic stripe on the back of the card.

Dean, Director, or Chair (DDC). This workflow term refers to the person primarily responsible for the operations of the business unit per the Departmental Authorization List (DAL).

Payment Card Industry's Data Security Standards (PCI DSS). These standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The Council is responsible for managing the security standards, while compliance is enforced by the payment card brands. These standards include controls for handling and restricting credit card information, computer and internet security, as well as the reporting of a credit card information breach.

University merchants. Any University of Central Florida business unit that accepts credit and debit cards as a form of legal tender, including retail and web-based operations. University merchants are responsible for compliance by their third-party service providers who accept debit and credit payments on their behalf.

PROCEDURES

Detailed procedural information is available in the online manual UCF Credit Card Merchant Procedures Manual.

RELATED INFORMATION

UCF Finance and Accounting, Merchant Services Web Site

Payment Card Industry Security Standards Council Data Security Standards

INITIATING AUTHORITY Vice President for Administration and Finance and Chief Financial Officer

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

Policy Number: 3-206.5

Initiating Authority: _____ Date: 11-23-16

University Policies and Procedures Committee Chair: _____ Date: 11/23/16

President or Designee: _____ Date: 11/28/16

History 3-206.1 1/19/07, 3-206.2 4/16/08, 3-206.3 7/24/08, 3-206.4 5/18/11