

ADMINISTRATIVE DIVISION FINA Finance		POLICY NUMBER FINA 48.11
POLICY TITLE Credit/-Debit Card Processing and Security		
SCOPE OF POLICY USC System		DATE OF REVISION XXX
RESPONSIBLE OFFICER Executive Vice President <u>of Administration and Finance</u> and Chief Financial Officer		ADMINISTRATIVE OFFICE <u>Administration and Finance University Bursar</u>

PURPOSE

The University of South Carolina ~~will follow~~maintains policies and procedures consistent with the requirements of Payment Card Industry Security Standards Council (PCI SSC), state and university policies, as well as contractual agreements regarding the acceptance of credit/debit card payment processing and security. This policy provides requirements and guidance for all credit and debit card processing activities for The University of South Carolina. ~~This document will serve as the cornerstone for the Vice President for Finance and Chief Financial Officer (CFO) and the University Bursar to develop, implement, and maintain the University wide plan to comply with the PCI Data Security Standard (PCI DSS).~~

DEFINITIONS

Payment Facility or Payment Facilities: refers to any department(s) or office(s) authorized to collect payments on the University’s behalf. The facility may be composed of the following: a physical location, a virtual “storefront” for conducting E-Commerce, any payment receiving method approved by the University Bursar or any combination of the above.

Payment Devices/Cards: this term, as used in this document, refers to credit cards, debit cards, purchasing cards, or other technologies that allow for a payment without the use of physical currency, personal check, wire transfer, or bank draft. Only cards or devices ~~that are~~ “backed” by one of the credit card issuing companies (Visa, MasterCard, Discover, American Express or JCB) are considered payment devices or payment cards. It can also refer to Point of Sale (POS) devices ~~that are~~ used to receive the cardholder data from cards or other technologies owned by the payee.

Client(s): refers to any person(s) making a payment to the University either remotely via internet interface or at Point of Sale (POS) with a Payment Device/Card. This group includes but is not limited to the following individuals: students, parents of students, faculty, staff, clients, invited guests and others purchasing goods and services from the university.

Payment Card Industry Security Standards Council (-PCI SSC): consortium body composed of the major credit card companies (American Express, Discover, JCB, MasterCard and Visa) and additional personnel who determine the best practices and security standards for processing Payment Device/Card transactions. While not a policing body, failure to meet or exceed the standards they set forth could lead to expensive fines, loss of the ability to accept payments from Payment Device/Cards, loss of reputation for The University of South Carolina, and increased

operational costs in the form of more extensive audits of our payment infrastructure by the PCI SSC.

Cardholder Data: consists of the full Primary Account Number (PAN), the number on the front of the payment card plus any of the following: cardholder name, expiration date and/or service code also known as a CVV or CVV2 code. Additional Personal Identifying Information (PII) may also be present during a credit card transaction and should also be secured.

E-Commerce: electronic commerce that incorporates using an electronic device at some point in the purchase of goods or services.

POLICY STATEMENT

The Executive Vice President for Administration and Finance and CFO and/or Associate Vice President and University Bursar will develop and administer the principles and framework for the University's approach to PCI DSS compliance to protect Cardholder Data. ~~This compliance process will be outlined by the Bursar's Office.~~ The Bursar's Office will develop and maintain the principles, standards, and procedures for PCI DSS compliance. ~~The Bursar's Office will and work with payment facilities in the various departments, schools, and campuses to ensure adherence to all policies and procedures contained in this document.~~

PROCEDURES

~~A. Procedure for All Campuses~~

1. All University of South Carolina divisions, departments, and campuses desiring to accept payment, by any method, for financial transactions on the University's behalf must have approval from the Associate Vice President and University Bursar. This process is fully defined in University Policy FINA 84.00 Academic Fees and Expenses. Those so approved are required to process all transactions through the Executive Vice President for Administration and Finance and CFO and University Bursar approved payment gateways.
2. The Executive Vice President for Administration and Finance and CFO via the Associate Vice President and University Bursar is responsible for ~~†~~
 - ~~i.~~ the development, implementation and maintenance of the University-wide payment card data security program.
3. ~~The Vice President for Finance and CFO via the University Bursar is responsible for~~
 - ~~i.~~ the development, implementation and maintenance of the University-wide response system to address any potential unauthorized access of Cardholder Data. The published response system is available in the Bursar's Office.
 - ~~ii.~~ ~~The Vice President for Finance and CFO via the University Bursar is responsible for~~ ensuring that all payment technology solutions meet PCI SSC compliance requirements.

5.4. Each payment facility is responsible for ensuring proper processing and disposal of cardholder data and other PII received in their office. This process will follow the outline presented in the PCI Compliance Program and associated policies, standards, and practices as developed by Procedure A.2 of this document.

6.5. Administrators or staff within the payment facility who are assigned the responsibility of maintaining or supporting PCI Compliance systems or assets will be responsible for implementing requirements outlined in this policy and established standards and procedures.

7.6. All levels of management are responsible for ensuring that all users within their area of accountability are aware of responsibilities as defined in this policy and for insuring a secure office environment. The head of each unit will authenticate the need for individual access to Payment Device/Card assets and must request and obtain authorization for access to said assets from the Associate Vice President and University Bursar.

8.7. Departments or organizations having locations on a university campus who do not receipt funds through the Bursar's Office (~~such as university affiliated 501c3 non-profits and auxiliary organizations that have locations on a university campus~~) but and do not collect funds on behalf of the University of South Carolina, ~~are still~~ must required to follow the PCI compliance process. An example of such an entity would include a university-affiliated 501c3 non-profits and auxiliary organization. Please note ~~that~~ the determination and attestation of compliance may differ substantially.

RELATED UNIVERSITY, STATE AND FEDERAL POLICIES

BTRU 1.24 Internal Control Policy

FINA 84.00 Academic Fees and Expenses

BUSFINA 84.10 Receipt and Handling of University Payments

FINABUSF 84.12 University Identity Theft and Detection Program

HR 1.39 Disciplinary Action and Termination for Cause

IT 3.00 Information Security

UNIV 1.50 Data Access

HISTORY OF REVISIONS

DATE OF REVISION	REASON FOR REVISION
November 1, 2006	New policy approval.
May 11, 2015	Policy revised to update the policies and procedures for University payment processing in response to the creation of the Payment Card Industry Security Standards Council (PCI SSC) and implementation of their standards, as well as departmental reorganization and name changes.

Xxxx

Policy updated to standard template. [Change in titles.](#)