Policy Statement

This Credit/Debit Card and PCI Compliance Policy provides requirements and guidance for all credit card activities for the College of Charleston.

This policy is in compliance with the credit card industry’s PCI-DSS (Payment Card Industry Data Security Standard) as set by Visa and the other major credit cards (https://www.pcisecuritystandards.org/).

The Credit/Debit Card and PCI Compliance Policy deals with access to the College of Charleston’s computing and network resources with regard to credit card processing as well as any free standing credit card processing unit or Point of Sale system. The Credit/Debit Card and PCI Compliance Policy supersedes and replaces all other campus policies and procedures for all issues related to the scope of this policy.

Policy Manager and Responsible Department or Office

Treasurer’s Office

Purpose/Reason for the Policy

This policy exists to provide the steps needed, and resources available, to safely accept credit card payments at College of Charleston. The College has an obligation to protect
our constituency’s credit and debit card accounts and does so by adhering to Payment Card Industry standards.

_______________________________________________________________

Departments/Offices Affected by the Policy

All entities on the campus, or affiliated with College of Charleston, who accept credit and/or debit cards as a form of payment.

_______________________________________________________________

Procedures Related to the Policy

A. Scope

1. The Credit/Debit Card and PCI Compliance Policy applies to:

   a) All departments, affiliates, and employees of the College of Charleston who accept and process credit card payments in the conduct of College business.

   b) All external organizations contracted by the aforementioned parties to provide outsourced services for credit card processing for College business.

   c) All departments, affiliates and employees of the College of Charleston who provide credit card processing services for third parties.

B. Definitions

1. Account Number (Credit Card Account Number): The unique number identifying the credit card and the person authorized to use the card when processing financial transactions.

2. Cardholder data: Cardholder data is any personally identifiable data associated with a cardholder. Examples include but are not limited to an account number, expiration date, name, address, social security number, etc.

3. PCI-DSS (Payment Card Industry Data Security Standard): The Standard was
created by the major card brands (Visa, MasterCard, Discover, American Express, JCB) to increase controls around cardholder data to reduce credit card fraud and exposure. PCI-DSS originally began as five different programs: Visa’s Cardholder Information Security Program, MasterCard’s Site Data Protection, American Express’ Data Security Operating Policy, Discover’s Information Security and Compliance, and the JCB’s Data Security Program. Each company’s intentions were roughly similar: to create an additional level of protection for card issuers by ensuring that merchants meet minimum levels of security when they store, process and transmit cardholder data. The Payment Card Industry Security Standards Council (PCI SSC) was formed, and on December 15, 2004, these companies aligned their individual policies and released version 1.0 of the Payment Card Industry Data Security Standard (PCI-DSS).

4. Sensitive Cardholder data: Sensitive Cardholder data is defined as the account number, expiration date, CVC2/CVV2/CID (a three or four digit number displayed on the signature panel of the card or in the case of American Express on the face of the card), and data stored on track 1 and track 2 of the magnetic stripe of the card.

5. Credit Card Processing: Act of storing, processing, or transmitting credit card data.


8. POS Device: Point of Sale (POS) computer or credit card terminals either running as stand-alone systems or connecting to a server either at the College of Charleston or at a remote off site location.

9. Web Development: The design, development, implementation and management of the user interface of the e-commerce application

C. Statement of Policy

1. Responsibility of College Departments

   a) All departments that manage credit card transactions must adhere to strict procedures for ensuring that data is secure at all times. Regardless of which credit card vendor is used, the College of Charleston faces steep penalties, including fines and lost business, or revocation of card processing privileges if credit card data is stolen.

   b) All College of Charleston divisions and departments desiring to accept payment for financial transactions electronically via the Internet using e-commerce are required to process all transactions through gateways approved by the Treasurer’s Office. The College provides PCI ready solutions, such as TouchNet’s MarketPlace, to appropriately handle these transactions. All requests for access to credit card acceptance must be made to the Treasurer’s Office.
2. Types of E-commerce:
   a) Web Sites: The College provides secure and PCI compliant transactions through TouchNet’s MarketPlace product. The MarketPlace (https://secure.touchnet.com/C20590_ustores/web/) is available to all departments at CofC. To find out more please contact the Treasurer’s Office at treasurer@cofc.edu.

   b) E-Mail: Credit card information should never be solicited or accepted by email. This presents a risk to both the credit card holder and the College.

   c) Products or services provided by e-commerce sites are limited to those that support the College of Charleston mission.

3. Approved Process:
   a) The approval process for all credit card activities will be as follows:

      1) The Treasurer, or named delegate(s), must approve all requests to begin accepting credit cards at the College of Charleston before a unit enters into any contract or purchase of software and/or equipment. This requirement applies regardless of the transaction method used (e.g. e-commerce, POS device, or e-commerce outsourced to a third party). Approved units must register their credit card processing information with the Treasurer’s Office, and, in some cases, the College Information Technology Department.

      2) All technology implementations (including approval of authorized payment gateways) associated with the credit card processing must be in accordance with the Credit/Debit Card and PCI Compliance Policy and approved by the Treasurer, VP of Fiscal Services, Procurement, and Information Technology Dept. prior to entering into any contract or purchasing software and/or equipment.

      3) Sensitive cardholder data must not be stored in any way on the College of Charleston computers or networks. Credit card numbers should never be written down nor appear in emails.

      4) Third party vendors must not collect or track customer information (e.g., web bugs, cookies, software buffers).

4. Maintaining Standards
   a) Departments and events approved for credit card processing activities must maintain the following standards:

   b) All employees including students involved in e-commerce or POS transactions must understand all requirements as outlined in the Credit/Debit Card and PCI Compliance Policy. The Treasurer’s Office must be provided a list of all individuals handling payment transactions per the Cash Receipts Policy.
c) All servers and POS devices will be administered in accordance with the requirement of the PCI-DSS standards.

d) Access to credit card processing systems and related information must be restricted to appropriate personnel. In some cases personnel may be subject to background and credit checks prior to participating in the processing of credit card payments.

e) Each department responsible for credit card processing will be subject to an Annual Self-Assessment Questionnaire and a Quarterly Network Scan as scheduled by the Information Security department. All systems processing cardholder data must comply with the Credit/Debit Card and PCI Compliance Policy and the associated procedures. The College IT Department and the Treasurer’s Office will assist in the initial self-assessment. To combat the loss of payment card information to hackers, e-commerce sites must comply with all security requirements as outlined in the PCI-DSS standards (https://www.pcisecuritystandards.org/documents/PA-DSS_v3-1.pdf).

f) Third party source code (HTML, CGI or script) should be provided to the Treasurer’s Office and/or Information Technology at the College of Charleston upon request.

g) Third parties providing payment gateways or who interact in any way with credit cards as a form of payment must provide certification of PCI-DSS compliance annually.

h) A third party vendor must provide evidence of adequate liability insurance. The State of South Carolina regulations currently require coverage of $5 million per occurrence or $10 million aggregate.

i) Only approved College of Charleston logos may be used on e-commerce sites existing within the College of Charleston domain.

D. Revisions and Exceptions

1. The Credit/Debit Card and PCI Compliance Policy may be revised only with approval of the Vice President of Fiscal Services and Executive Vice President for Business Affairs. The Vice President of Fiscal Services may grant written exceptions to the policy in extreme circumstances and will notify the Executive Vice President for Business Affairs, Treasurer, Chief Information Security Officer and Internal Auditor.

E. Compliance

1. Failure to comply with the Credit/Debit Card and PCI Compliance Policy and the above referenced procedures will be deemed a violation of College policy and will result in suspension of electronic payment capability for the affected department. Additionally, fines
may be imposed by the affected credit card company, generally $50,000 for the first violation. Technology that does not comply with the Credit/Debit Card Policy and the associated PCI-DSS standards will be disconnected from network services.

F. Communication

1. Upon approval, the Credit/Debit Card and PCI Compliance Policy shall be published on the appropriate College of Charleston web site(s). The Treasurer, Chief Information Security Officer and Internal Auditor will recommend subsequent revisions to the Credit/Debit Card and PCI Compliance Policy for approval by the Vice President of Fiscal Services and Executive Vice President for Business Affairs.

Related Policies, Documents or Forms

Cash Receipts Policy (http://treasurer.cofc.edu/policies/cash-receipts.php)

---

Issue Date: 2/29/2016
Date of Policy Revision: 3/23/2016

Next Review Date: 10/23/2020

---

POLICY APPROVAL
(For use by the Office of the Board of Trustees or the Office of the President)

Policy Number: 2.2.3.2

President or Chairman, Board of Trustees

[Signature]

Date: 3/23/16