COLLEGE of CHARLESTON

OFFICIAL POLICY

2.2.3.2	Credit/Debit Card and PCI Compliance Policy	10/17/2016

Policy Statement

This Credit Card Acceptance and Processing Policy provides requirements and guidance for all credit card activities for the College of Charleston. Employees approved as merchants and their respective departments are responsible for being aware of and complying with all terms and conditions included in the full policy and not just those outlined in this executive summary.

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 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

Policy

1. Scope

The Credit/Debit Card Policy encompasses people, processes, and systems and as such applies to:
-All computing and network resources with regard to credit card processing. -Any free-standing credit card processing unit or Point of Sale system. -All departments, affiliates, and employees of the College of Charleston who accept and process credit card payments in the conduct of College business.
-All approved external organizations contracted by the aforementioned parties to provide outsourced services for credit card processing for College business.
-All approved departments, affiliates and employees of the College of Charleston who provide credit card processing services for third parties.

2. Definitions

Account Number: The unique number identifying the cardholder's account which is used in processing financial transactions.

Breach Notification Laws: Governing laws that require a merchant to notify customers of a data breach that results in loss or theft of that customer's personally identifiable information (PII).

Business Continuity Plan (BCP): A documented plan for maintaining business operations in the event of a disaster or breach. A supplemental document will be provided by the Treasurer's Office, IT Information Security and IT Network Engineering to detail the required elements of a Business Continuity Plan.

Cardholder data: Cardholder data is any personally identifiable data associated with a cardholder. Examples include but are not limited to the primary account number, cardholder name, expiration date, and the service code

Cardholder Data Environment: Any and all people, places and technologies used to store or process or transmit cardholder data.

Commerce Server Data Environment: The location of a physical or virtual server machine used in the processing, transmitting or storing of cardholder data.

Data Compromise: The exposure of sensitive or personally identifiable information (PII) resulting from either intentional security breach (an "attack")

or human error.

Data Security Breach: The act of circumventing security controls on a system, thus allowing unauthorized access to data via an attack on the system. Data may or may not be compromised during a security breach.

Disaster Recovery Plan: A documented plan for information technology continuity in light of a disaster, emergency or breach that details incident response testing procedures and data back-up procedures. A supplemental document will be provided by the Treasurer's Office and Information Technology to detail the required elements of a disaster recovery plan as it relates the conduct of credit and/or debit card activity.

ISO 27002: The International Standards Organization document defining computer security standards.

Payment Application Data Security Standard (PA DSS): A set of requirements derived from and closely related to the PCI DSS, but intended to illustrate for payment software vendors what is required for their payment software applications to facilitate and not prevent their customers' PCI DSS compliance.

Payment Card: Any credit, debit or pre-paid credit/debit card. Payment cards are those branded with the Visa, MasterCard, Discover and American Express logos. All payment card activity for College of Charleston is monitored by the Treasurer's Office.

Payment Channel: The hardware/software used to conduct a payment transaction.

Personally Identifiable Information (PII): Information that can be used to uniquely identify, contact or locate an individual, or information that can be used in conjunction with other sources to uniquely identify an individual. In the case of payment card data, PII can be all printed and non-printed information contained on a payment card that identifies the customer. The Treasurer's Office and General Counsel will identify and periodically update PII applicable to the Policies and Procedures found at http://pci.cofc.edu as revisions to industry regulations and other security factors require.

In the context of payment card operations, it is strictly prohibited for a College of Charleston entity to retain the following elements of PII: credit/debit card number, card security code, customer's PIN or contents of the magnetic stripe of a payment card.

Payment Card Industry Data Security Standard (PCI DSS): The Payment Card Industry Data Security Standard is the result of collaboration between the major credit card brands to develop a single approach to safeguarding

sensitive data. The PCI DSS defines a series of requirements for handling, transmitting and storing sensitive data. Entities engaged in any form of payment card processing must comply with these standards as a condition of their payment card processing contracts. A copy of the PCI DSS can be obtained at https://www.pcisecuritystandards.org/

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.

Processing Method: The means by which authorized departments accept payment cards. Payment card transactions can only be accepted via walk-in (face-to-face) payment, telephone (in authorized locations only. Telephone calls cannot be recorded) or customer-initiated online payment. Tuition/fee payments are accepted only as customer-initiated through the MyCharleston or in person. No department may accept a payment card transaction or payment card information via mail, email, fax, any end-user messaging technology or on a website that collects payment card information unless the site is authorized by the Treasurer's Office via a system usage waiver.

Risk Assessment: A documented process used to identify and qualitatively and/or quantitatively evaluate risks and their potential effects, including brand damage and monetary effects. A supplemental document will be provided by the Treasurer's Office and Information Technology to detail the required elements of a Risk Assessment. \

Sensitive Cardholder Data: Sensitive Cardholder data is defined as the full track data (mag stripe or chip), the card security code (CAV2/CVC2/CVV2/CID), and PINs or PIN blocks

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

3. Statement of Policy

Responsibility of College Departments

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.

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.

Types of E-commerce:

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.

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.

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

Approved Process:

The approval process for all credit card activities will be as follows:

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). An inventory of all credit card processing units, including model and serial numbers, should be provided to the Treasurer's Office and all personnel processing credit cards must receive PCI training.

All technology implementations (including approval of authorized payment gateways) associated with the credit card processing must be in accordance with the Credit/Debit Card Policy and approved by the Treasurer, VP of Fiscal Services, Procurement, and Information Technology Dept. if considering a legitimate business need for credit card processing.

Sensitive cardholder data (see the definition above) 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 or fax documents.

All unsolicited credit card information must be destroyed using a cross cut

shredder.

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

Maintaining Standards:

Departments and events approved for credit card processing activities must maintain the following standards:

All approved employees including students involved in e-commerce or POS transactions must understand all requirements as outlined in the Credit/Debit Card Policy. The Treasurer's Office must be provided a list of all individuals handling payment transactions per the Cash Receipts Policy (http://treasurer.cofc.edu/policies/cash-receipts.php) and the list must be kept current noting any changes in personnel and business processes. All employees involved in credit card processing, including Information Technology, Public Safety, Physical Plant and MarketPlace users, must complete PCI training prior to credit card acceptance or gaining access to network access areas on campus.

All servers and POS devices will be administered in accordance with the requirement of the PCI DSS standards.

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.

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 Technology department. All systems processing cardholder data must comply with the Credit/Debit Card Policy and the associated procedures. The College's 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/PCI_DSS_v3-2.pdf?agreement=true&time=1468259004464 and https://www.pcisecuritystandards.org/documents/PA-DSS_v3-2.pdf?agreement=true&time=1468259087326).

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

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 or PA-DSS compliance, such as inclusion on a card brand's global registry or by providing an Attestation of Compliance, annually. These documents must be provided to the Treasurer's Office each year.

All third party vendors 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.

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

4. Revisions and Exceptions

The Credit/Debit Card 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.

5. Compliance

Failure to comply with the Credit/Debit Card Policy and the above referenced procedures will be deemed a violation of College policy and may 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.

6. Communication

Upon approval, the Credit/Debit Card Policy shall be published on http://pci.cofc.edu. The Treasurer, Chief Information Security Officer and Internal Auditor will recommend subsequent revisions to the Credit/Debit Card Policy for approval by the Vice President of Fiscal Services and Executive Vice President for Business Affairs.

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

See pci.cofc.edu for additional information.

Related Policies, Documents or Forms

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

Issue Date: 7/11/2016 **Date of Policy Revision:10/17/2016**	**Next Review Date: 10/17/2020**

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 Glenn F. McConnell Date: 10-27-16