THE CITADEL
The Military College of South Carolina
171 Moultrie Street
Charleston, SC 29409

MEMORANDUM 23 April 2015
NUMBER 5-004

ELECTRONIC COMMERCE POLICY

1. PURPOSE

The purpose of this policy is to establish guidelines and minimum requirements to be followed when accepting e-Commerce payments, specifically credit and debit card payments.

The Vice President for Finance will have oversight responsibility for institutional provisions that define electronic commerce, e-Commerce standards and procedures, and enforcement of payment card industry data security standards at The Citadel.

2. REFERENCE

www.pcisecuritystandards.org

3. DEFINITIONS

A. Electronic-Commerce: Business transactions over electronic means. This normally means the internet, but can include any electronic interaction – including automated phone banks, touch screen kiosks, or even ATMs. Transactions can include debit/credit cards (historically the primary method of e-Commerce payment), but also include any electronic transfer of funds via automated clearing house (ACH).

B. Payment Card Industry Data Security Standard [PCI DSS]: A consolidated standard from the major credit card issuers detailing merchant requirements when accepting credit/debit cards. The requirements include network, security (physical/logical), and monitoring components, among others.

C. Cardholder Data: Cardholder data is any personally identifiable information associated with a user of a credit/debit. Primary account number [PAN], name, expiry date, and card verification value 2 [CVV2] are included in this definition.

D. Self-Assessment Questionnaire-A (SAQ-A): Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Not applicable to face-to-face channels.

E. Self-Assessment Questionnaire-A-Electronic Publication (SAQ-A-EP): E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that does not directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Applicable only to e-commerce channels. This is new under PCI DSS v3.

F. Self-Assessment Questionnaire-B (SAQ-B): Merchants using only: imprint machines with no electronic cardholder data storage; and/or standalone, dial-out terminals with no electronic cardholder data storage. Not applicable to e-commerce channels.

G. Self-Assessment Questionnaire-B-Internet Protocol (SAQ-B-IP): Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. Not applicable to e-commerce channels. This is new under PCI DSS v3.

H. Self-Assessment Questionnaire-C (SAQ-C): Developed to address requirements applicable to merchants where payment application systems (for example, point of sales (POS) systems) are connected to the Internet (for example Digital Subscriber Line (DSL), cable modem, etc.). Not applicable to e-commerce channels.

I. Self-Assessment Questionnaire-C-Virtual Terminal (SAQ-C-VT): Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. Not applicable to e-commerce channels.

J. Self-Assessment Questionnaire-Point-to-Point Encryption-Hardware (SAQ-P2PE-HW): Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. Not applicable to e-commerce channels.

K. Self-Assessment Questionnaire-D (SAQ-D): applies to SAQ-eligible merchants not meeting the criteria for any other SAQ type. Examples of merchant environments that would use SAQ D <u>may include but are not limited to</u>: E-commerce merchants who accept cardholder data on their website, merchants with electronic storage of cardholder data, merchants that don't store cardholder data electronically but that do not meet the criteria of another SAQ type, or merchants with environments that might meet the criteria of another SAQ type, but that have additional PCI DSS requirements applicable to their environment.

4. POLICY

This policy applies to all College departments, employees, approved vendors, consultants, and other persons associated with the College wishing to conduct e-Commerce via any and all media and delivery mechanisms.

Departments or individual units with Point of Sale (POS) equipment will develop procedures to cover requirements outlined by PCI DSS for the safeguarding of hardware and operations of POS systems. This will include any physical security requirements for computer, and credit card devices. Procedures will be forwarded to the Treasurer for approval. If appropriate, the Treasurer will forward procedures to Information Security Coordinator in Information Technology Services (ITS) for review.

Information Technology Services (ITS) is responsible for maintaining requisite PCI DSS campus network infrastructure to PCI DSS standards. This includes network topology and physical (closet) diagrams. ITS will coordinate physical security requirements with Facilities and Engineering and Public Safety. Unfunded requirements will be forwarded through appropriate funding channels for consideration and prioritization.

The Citadel views electronic commerce as an additional outlet for contact with future alumni, faculty, staff, and the public. The Citadel encourages College and auxiliary departments to utilize electronic commerce as a component of current business functions and interactions.

The use of credit cards or debit cards is a common and widely accepted practice of conducting payment transactions. The Citadel allows departments within the College to establish themselves as credit card merchants to more fully participate in e-commerce at The Citadel.

Departments or individual units within the College must define 'conditions of use' for information resources under their control. These statements must be consistent with this overall policy, but may provide more stringent detail, guidelines, and/or restrictions. Such procedures may not relax or subtract from this policy. Where such 'conditions of use' exist, enforcement mechanisms defined therein shall apply. These additional procedures are subject to review and approval by the Vice President for Finance and the Chief Comptroller’s Office, Internal Auditor or Policy Coordinator.

Any electronic commerce associated with The Citadel must have a basis in the College’s mission. Unrelated e-Commerce activity must not utilize the College network or associated systems.

Any transaction, system, application, or process associated with e-Commerce (including credit/debit card transactions) will be performed in compliance with the PCI DSS, Citadel standards and procedures for e-Commerce, and retain ongoing approval of the Vice President for Finance.

E-Commerce activity will be performed within the centralized solution provided by The Citadel administration unless a written exception is granted by the Vice President for Finance.

Departments with PCI DSS requirements are required to complete PCI DSS self-assessment questionnaires (SAQs) on an annual basis and forward them to PCI@citadel.edu. Contracted campus merchants will forward completed questionnaires to their respective department and to PCI@citadel.edu.

The merchants grandfathered in as SAQ-C and SAQ-D levels will hire external assessors to validate compliance with PCI DSS and forward the results to PCI@citadel.edu. The department responsible for the merchant will be required to pay for the assessor's report unless prior arrangements are made for the merchant to pay for the report.

Following The Citadel's Policies and Procedures, South Carolina laws and applicable federal laws, The Citadel strives to protect personal privacy and the confidentiality of information. Departments engaging in e-Commerce are responsible for safeguarding confidential information used in the processing of e-Commerce activity.

Cardholder information can never be transmitted across a network unsecured. Secure Socket Layer [SSL] at the very minimum is required to transmit cardholder data. Emailing unencrypted credit card numbers is never acceptable.

As a part of The Citadel's network, wireless connectivity is available for use in the same manner as a wired network jack. However, special considerations and additional security requirements from a PCI DSS standpoint are necessary when connecting to a wireless network for e-Commerce activities. For these reasons, The Citadel has not authorized the use of any wireless network for e-Commerce activities.

The major regulatory body associated with credit card transactions is the PCI security Standards Council (www.pcisecuritystandards.org) and promulgates the rules and regulations The Citadel adheres to in the credit card environment.

For procedural or technical questions related to this policy, send an e-mail to PCI@citadel.edu.

5. COMPLIANCE

Failure to comply with this policy may have the following consequences: revocation of credit card acceptance for the affected unit, fines (up to $500,000.00) assessed to the responsible branch or department, legal action by injured parties, prosecution for criminal violations. Citadel employees may face disciplinary action or termination of employment for negligent behavior.

6. NOTES

A. Dates of Official Enactment and Amendments:

Approved by the Vice President for Finance on 23 April 2015.

B. Responsible Department:

Treasurer

C. Responsible Official:

Treasurer

D. Cross References:

N/A

7. RESCISSION

N/A

8. REVIEW

Review this policy on an as needed basis or on a biennial basis.

FOR THE PRESIDENT:

OFFICIAL

//signed, JG, 23 April 2015//
JOSEPH GARCIA
Colonel, UMSC
Vice President for Finance