NUMBER: BUSF 4.11
SECTION: Business and Finance

SUBJECT: Credit/Debit Card Processing Policy

DATE: November 1, 2006

Policy for: All Campuses
Procedures for: All Campuses
Authorized by: Rick Kelly
Issued by: Financial Services

I. Executive Summary and Purpose

This policy provides requirements and guidance for all credit and debit card processing activities for The University of South Carolina.

At the initial publication of this policy the following sources were consulted and provide the basis for this program: ISO 17799, Visa CISP, MasterCard and Discover Merchant Operating Regulations.

This policy deals with access to The University of South Carolina's computing and network resources. This policy pre-empts all other campus policies and procedures for all issues within the scope of this policy.

II. Scope

This policy applies to:

A. All units, affiliates, and employees of The University of South Carolina who accept credit/debit card payments for University business.

B. All external organizations contracted by the aforementioned parties to provide outsourced services for credit/debit card processing for University business.

C. All units, affiliates and employees of The University of South Carolina who provide credit/debit card processing services for third parties.

III. Definitions

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

B. Cardholder data: Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, etc.

C. Sensitive Cardholder data: This is defined as the account number, expiration date, CVC2/CVV2 (a three-digit number imprinted on the signature panel of the card), and data stored on track 1 and track 2 of the magnetic stripe of the card.

D. Cardholder Information Security Program (CISP): CISP defines a standard of due care for securing cardholder data, wherever it is located. CISP compliance has been required of all entities storing, processing, or transmitting cardholder data.

E. Credit/Debit Card Processing: Act of storing, processing, or transmitting credit/debit cardholder data.

F. E-Commerce Application: Any internet-enabled financial transaction application.

G. Employee: Any employee as defined by the University of South Carolina Human Resource Policy & Procedure Manual.

H. ISO 17799: The International Standards Organization document defining computer security standards.

I. POS Device: Point-of-sale (POS) computer or credit card terminals either running as standalone systems or connecting to a server either at The University of South Carolina or at a remote off site location.

J. Site Data Protection Program (SDP): The formal data protection program mandated by MasterCard. The SDP Program provides acquiring members with the ability to deploy security compliance programs, ensuring that online merchants and member service providers are adequately protected against hacker intrusions and account data compromises.

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

IV. Statement of Policy

A. Responsibilities of University Departments

1. All departments that manage credit card holder data must adhere to strict procedures for ensuring that data is secure at all times. Regardless which

credit card vendor is used, the University of South Carolina face steep penalties, including fines and lost business, if credit card data is stolen.

2. All University of South Carolina divisions, departments, and campuses desiring to accept payment for financial transactions electronically via the Internet using e-commerce are required to process all transactions through approved gateways. All gateways must ensure that all data and personal information related to credit card sales passes through specific, approved hardware and software that meets all criteria specified by the Cardholder Information Security Program (CISP). These requirements are for all credit card transactions.

B. Types of E-Commerce

1. Web display only: Under this type, departments, selling approved goods and services create an individual Web site to display product and service information. However, the ordering, transfer or payment, and shipping information is performed elsewhere such as, through use of phone or mail, traditional methods for securing and providing for the safety and the retention of personal and financial information on written records would apply.

2. E-Mail Transactions: Web sites developed by departments may display product and service information. However, visitors have the option of submitting order information to the seller via e-mail. This method is acceptable for exchanging quantitative information and for communicating an interest to purchase. E-mail must not be used to transfer confidential data/information such as credit card numbers, social security numbers, purchaser identification, or other sensitive information related to the purchaser.

3. Secured Restricted Gateway: This type combines a Web site to display products and services developed by the selling department and an electronic link to the approved Gateway software. This is the required methodology for all University of South Carolina e-commerce involving the acceptance of payments by credit card via the internet.

Products or services provided by e-commerce site are limited to those that support the University of South Carolina's academic mission.

C. Approval Process

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

1. The Bursar and Vice President for Financial Services or delegate(s) must approve all credit/debit card processing activities at the University of South

Carolina before a unit enters into any contracts or purchases 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[1]). Approved units must register their credit/debit card processing information with the Bursar's Office and the University Technology Services Network and Security Operations Group.

2. All technology implementation (including approval of authorized payment gateways) associated with the credit/debit card processing must be in accordance with the Credit Card Processing Procedures and approved by the Bursar and University Technology Services Network and Security Operations Group prior to entering into any contracts or purchasing of software and/or equipment.

3. Sensitive cardholder data should not be stored in any fashion on the University of South Carolina computers or networks. Exemptions to this must come from the Bursar.

D. Maintaining Standards

Units approved for credit card processing activities must maintain the following standards:

1. All employees (business managers, operations personnel, and technical staff) involved in e-Commerce or POS transactions must understand all requirements as outlined in the Credit/Debit Card Processing Procedures.

2. All units should create, maintain and test (as required by CISP); business continuity and disaster recovery plans as well as incident response capabilities.

3. All servers and POS devices will be administered in accordance with the requirements of the Credit/Debit Card Processing Procedures.

4. Access to credit/debit card processing systems and related information must be restricted to appropriate personnel.

5. Each unit responsible for credit/debit card processing must complete an Annual Self-Assessment Questionnaire and a Quarterly Network Scan by an approved independent scan vendor. All systems processing cardholder data must comply with this policy and the associated procedures. The University Technology Services Network and Security Operations Group and the Bursar's Office will, at the request of the unit, 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 Credit Card Processing Procedures to achieve certification. Self-assessment and certification forms will be sent to the Bursar.

[1] Third party vendors must suppress the use of mechanisms that collect or track customer information (e.g., web bugs, cookies).Third party source code (HTML or script) should be provided to authorize individuals at the University of South Carolina upon request. A third party vendor must provide evidence of adequate liability insurance.

Only approved University of South Carolina logos may be used on e-commerce sites on University of South Carolina's domain. (See BUSA 3.06)

V. Procedures

The Credit/Debit Card Processing Procedures provides details for implementation of this policy. This separate document carries the full force of this policy. This separation allows for easier modifications to the procedures due to the changing nature of business, technology and security.

VI. Revisions and Exceptions

This policy may be revised only with approval of the Vice President for Business and Finance of the University of South Carolina. The Vice President for Business and Finance may grant exceptions to this policy or revise the Credit/Debit Card Processing Procedures document by mutual agreement.

VII. Compliance

Failure to comply with this policy and the associated required procedures will be deemed a violation of University policy and will result in suspension of electronic payment capability for affected units. Additionally, fines may be imposed by the affected credit card company, beginning at $50,000 for the first violation. Technology that does not comply with this policy and the associated required procedures is subject to disconnection of network services.

VIII. Communication

Upon approval, this policy shall be published on the appropriate University of South Carolina web site(s). The following offices and individuals shall be notified in writing with any subsequent revisions or amendments made to this policy:

A. Bursar
B. Vice President and Chief Information Officer
C. University Internal Auditor

D. Associate Vice Provosts
E. Deans, Directors and Department Heads
F. Chancellors

IX. Reason for policy
Establish policy for credit card business activities.

Send Comments to Joe Taylor