

# The University of Georgia Credit/Debit Card Processing Policy

**The following are responsible for the accuracy of the information contained in this document:**

**Responsible University Officers**

Senior Vice President for Finance and Administration (SVPFA)  
Chief Information Officer (CIO)

**Responsible Coordinating Offices**

Bursar's Division  
Chief Information Security Officer  
Internal Auditing Division

## 1. Executive Summary and Purpose

This policy provides requirements and guidance for all credit and debit card processing activities for the University of Georgia.

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

This policy deals with access to the University of Georgia's computing and network resources. All relevant provisions in the Computer Security and Ethics Policy<sup>1</sup> are applicable and included by reference in this document. This policy pre-empts all other campus policies and procedures for **ALL** issues within the scope of this policy.

## 2. Scope

This policy applies to:

- All units, affiliates, and employees of the University of Georgia who accept credit/debit card payments for University business.
- All external organizations contracted by the aforementioned parties to provide outsourced services for credit/debit card processing for University business.
- All units, affiliates and employees of the University of Georgia who provide credit/debit card processing services for third parties.

## 3. Definitions

**Account Number:** The unique number identifying the cardholder's account which

is used in financial transactions.

**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.

**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.

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

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

**Data Security Standard (DSS):** Data security standards mandated by American Express.

**e-Commerce Application:** Any internet-enabled financial transaction application.

**Employee:** Any employee as defined by the UGA Human Resource Policy & Procedure, <http://www.busfin.uga.edu/manual/>

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

**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 Georgia or at a remote off site location.

**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.

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

## **4. Statement of Policy**

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

- The SVPFA, CIO or delegate(s) must approve all credit/debit card processing activities at the University of Georgia 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). Approved units must register their credit/debit card processing information with the Bursar's Office.
- 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 SVPFA, CIO or delegate(s) prior to entering into any contracts or purchasing of software and/or equipment.
- Sensitive cardholder data should not be stored in any fashion on UGA computers or networks. Exemptions to this must come from both the SVPFA and CIO.

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

- All employees (business managers, operations personnel, and technical staff) involved in e-Commerce or POS transactions must attend appropriate training.
- All units should create, maintain and test annually, business continuity and disaster recovery plans as well as incident response capabilities.
- All servers and POS devices will be administered in accordance with the requirements of the *Credit/Debit Card Processing Procedures*.
- Access to credit/debit card processing systems and related information must be restricted to appropriate personnel.
- Each unit responsible for credit/debit card processing must complete a self assessment annually on all systems processing cardholder data to ensure compliance with this policy and the associated procedures. The Chief Information Security Officer and the Bursar's Office will, at the request of the unit, assist in the initial self assessment. Audits will be performed periodically by the Internal Auditing Division to confirm the results of the self assessments. On a quarterly basis, the Office of Information Security will conduct a vulnerability assessment on machines processing credit/debit cards.

c. On a regular basis, the Chief Information Security Officer, Bursar's Office and Internal Auditing will provide appropriate training to all employees associated with credit/debit card processing.

|

## 5. Procedures

The *Credit/Debit Card Processing Procedures* document 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.

## 6. Revisions and Exceptions

This policy may be revised only with approval of the SVPFA of the University of Georgia.

The SVPFA and the CIO may grant exceptions to this policy or revise the *Credit/Debit Card Processing Procedures* document by mutual agreement.

## 7. Compliance

Failure to comply with this policy and the associated required procedures will be deemed a violation of University policy and subject to disciplinary action up to and including termination as noted in the Guide to Progressive Discipline. Technology that does not comply with this policy and the associated required procedures is subject to disconnection of network services.

## 8. Communication

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

- Associate Vice Provosts
- Deans, Directors and Department Heads
- Associate Vice Presidents

---

<sup>i</sup> Computer Security and ethics policy <http://www.infosec.uga.edu/compsec>