

Georgia Institute of Technology

Credit Card Processing Policy

Policy Number: 03.GIT.120 Rev. 1.71

Effective Date: 7/31/2003 until approval of final version

Lat Review Date: N/A Next Review Date:

Status

Draft

Under Review

Approved

Obsolete

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

Responsible University Officer

Associate Vice President of Financial Services

Responsible Coordinating Office

Financial Services

1. Executive Summary and Purpose

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

At the initial publication of this policy the following sources were consulted and provided the basis for this program: ISO 17799, Visa CISP, MasterCard SDP.

This policy deals with access to Georgia Tech computing and network resources. All relevant provisions in the [Computing and Network Usage Policy \(CNUP\)](#)^[1] 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.

REVIEW Comment: This policy will be considered effective July 31st, 2003 based on the provisional approval of the Associate Vice President of Financial Services and the Associate Vice President of the Office of Information Technology. Final approval of this policy will be by the President of the Georgia Institute of Technology based on a review by the Information Security Policy Committee.

Georgia Institute of Technology Credit Card Processing Policy

Version 1.71 – Last revised 7/30/2003

2. Definitions

Application Server: The computer hosting the application that the general end-user or the point-of-sale (POS) terminal connects

Category III Data – Sensitive: This information is considered private and should be guarded from disclosure. However, public disclosure of this information due to a system compromise generally does not result in financial fraud or violation of State and/or Federal law. Examples include intellectual property information, private directory listings, and contract negotiations.

Category IV Data – Highly Sensitive: Any disclosure of this information, intentional or otherwise, may contribute to financial fraud and/or violate State and/or Federal law. Examples include Social Security numbers, credit card numbers, financial institution account numbers, and employee and student health records.

Cardholder Information Security Program (CISP): The formal data protection program mandated by Visa

Credit Card Number: Any part or all of the unique number identifying the account for a financial transaction

Database Servers: The computer storing the sales and/or credit card numbers

eCommerce Application: Any internet-enabled financial transaction application, whether a buying application or selling application.

Employee: Any employee (as defined by the *Employee Handbook*), faculty, student employee, or contractor employed by a third party and providing services to the Georgia Institute of Technology

ISO 17799: The International Standards Organization document defining computer security standards. The credit card vendors may have based their policies on this standard.

POS Terminal: Point-of-sale (POS) computer terminals either running as standalone systems or connecting to a server either at the Georgia Institute of Technology or remotely off site

Purchase Cards (P-Cards): Credit cards obtained by Georgia Tech through a customer agreement with a bank for procurement purposes

Site Data Protection Program (SDP): The formal data protection program mandated by MasterCard

Swipe Terminal: POS credit card terminals

Web Development: The design, development, implementation and management of the “front-end” of the eCommerce application

Georgia Institute of Technology Credit Card Processing Policy

Version 1.71 – Last revised 7/30/2003

3. Scope

All academic units, administrative units, organizations, and employees of the Georgia Institute of Technology or that use systems or networks supported Georgia Institute of Technology must abide by this policy.

This policy specifically addresses all credit card processing by the Georgia Institute of Technology. All POS terminals handling credit card numbers (in full or truncated) and all servers receiving, storing, or transmitting credit card numbers (in full or truncated) are subject to this policy. An exemption is provided for P-card numbers provided the credit card number are functionally truncated to four digits or less.

4. Statement of Policy

4. The approval process for all credit card processing activities:
 - 4.1.1. The Associate Vice President of Financial Services or delegate must approve all credit card processing activities at the Georgia Institute of Technology prior to entering into any contracts or purchasing equipment. This requirement applies regardless of the transaction method used (e.g. online processing at Georgia Tech, outsourced to a third party, or swipe terminals).
 - 4.1.2. All technology implementation associated with the credit card processing must be in accordance with the *Credit Card Processing Procedures* and approved by the Associate Vice President of Information Technology prior to entering into any contracts or purchasing equipment.
 - 4.1.3. All credit card numbers must be handled in accordance with the *Data Access Policy* requirements for category 4 data. Please contact OIT Information Security for assistance with interpretation and implementation. However, instances of P-card numbers or corporate cards where 4 or fewer numbers are functionally present may be handled as category 3 data. Any conflicts between the requirements of the *Data Access Policy* and the *Credit Card Processing Procedures* will be resolved in favor of the *Credit Card Processing Procedures*.
- 4.2. Units approved for credit card processing activities must maintain the following standards:
 - 4.2.1. Provide appropriate training to all employees handling systems with credit card numbers including both personnel within the unit handling the credit card transactions and appropriate personnel in the Office of Information Technology

Georgia Institute of Technology Credit Card Processing Policy

Version 1.71 – Last revised 7/30/2003

- 4.2.2. Create, maintain and test annually business continuity/disaster recovery plans and system compromise response plans.
- 4.2.3. All outsourcing agreements must meet the standards set forth in the *Credit Card Processing Procedures*.
- 4.2.4. All servers storing or processing credit card numbers will be housed with the Office of Information Technology. All servers and POS Terminals will be administered in accordance with the requirements of the *Credit Card Processing Procedures*.
- 4.2.5. Credit card numbers will be retained for a maximum of 90 days. The only exception is transactions for future events, which may be retained up to 180 days from the transaction date. All media used for credit card numbers must be destroyed when retired from this use. All hardcopy must be shredded by at least a cross-cut shredder prior to disposal.
- 4.2.6. Access to credit card numbers must be restricted to the minimum number of people possible. No employee may have access to credit card numbers until he or she has attended the Credit Card Processing Policy Training and has tendered written acknowledgement of receipt of a copy of this policy, the *Credit Card Processing Procedures* and other appropriate policies (e.g., CNUP, Data Access Policy, Service Certification Process and Procedure, and unit level security policy). After completion of these requirements, the unit head may issue, in writing, authorization for the employee's access. No employee will have access to credit card numbers without such written authorization.
- 4.2.7. Each unit responsible for credit card processing must complete audits quarterly on all systems storing or processing credit card numbers to ensure compliance with this policy and the associated procedures. The Office of Information Technology will participate in these audits. Annual audits must be performed by Office of Information Technology Information Security to confirm the results of the quarterly audits.
- 4.2.8. All computers handling, processing, or storing credit card numbers must be registered in accordance with the revised Computer and Network Usage Policy.

5. Procedures

The *Credit Card Processing Procedures* document provides the technical 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 technology and security.

Georgia Institute of Technology Credit Card Processing Policy

Version 1.71 – Last revised 7/30/2003

6. Revisions and Exceptions

This policy may be revised only by signature by the President of the Georgia Institute of Technology.

The Associate Vice President of Financial Services and the Associate Vice President of Information Technology may grant exceptions to this policy or revise the *Credit Card Processing Procedures* document by mutual agreement. Either the Associate Vice President of Financial Services or the Associate Vice President of Information Technology may grant exceptions to the *Credit Card Processing Procedures*.

7. Compliance

Failure to comply with this policy and the associated required procedures by employees will be deemed a violation of Institute policy and subject to personnel action up to and including termination as noted in the Employee Handbook and/or the Faculty Handbook. Technology that does not comply with this policy and the associated required procedures is subject to disconnection of network services or confiscation of equipment pending review and approval of processes, procedures, and/or equipment.

8. Communication

Upon approval, this policy shall be published on the Georgia Tech Office of Information Technology website under policies and the Business Office web site. The following offices and individuals shall be notified in writing with any subsequent revisions or amendments made to this policy:

- Associate Vice Provosts
- Deans
- Associate Vice Presidents
- Chairs
- Internal Auditing

9. References

[1] Georgia Tech [Computing and Network Usage Policy \(CNUP\)](#)

[2] Data Access Policy

[3] Credit Card Processing Procedures