

Georgia Institute of Technology

Credit Card Processing Procedures

Procedures No. 03.GIT.120-A Rev. 1.71

Effective Date: 7/31/2003 until approval of final version
Lat Review Date: N/A Next Review Date:

Directly in support of the following Policy Document(s):
Credit Card Processing Policy No. 03.GIT.120

Status	The following are responsible for the accuracy of the information contained in this document
<input type="checkbox"/> Draft	Responsible University Officer
<input checked="" type="checkbox"/> Under Review	Associate Vice President of Information Technology
<input type="checkbox"/> Approved	Responsible Coordinating Office
<input type="checkbox"/> Obsolete	Office of Information Technology – Information Security

1. Executive Summary and Purpose

These procedures are required in direct support of the *Georgia Institute of Technology Credit Card Processing Policy* and were included in the original approval of the policy. This document sets forth the technical details and procedural requirements for implementing credit card processing at the Georgia Institute of Technology or outsourcing that processing to a third party.

The procedures' scope, revisions, exceptions, and compliance are noted in the *Credit Card Processing Policy*.

2. Definitions

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

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

Card Verification Value 2 (CVV2): An additional verification code used in transaction processing

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

Encryption: Scrambling data in a recoverable format

Firewall: A network device or host-based software implementation designed to restrict network access to a computer

Hashing: Scrambling data in an unrecoverable but verifiable format

Intrusion Detection System (IDS): A network monitoring device for recognition of attempts to compromise monitored systems

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

Two-factor Authentication: Authentication requiring two different methods confirming identity typically based on something the user has (e.g. a card, a key, a fingerprint) and something the user knows (e.g. a password)

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

3. Required Procedures

The procedures are separated into the following general areas of interest:

3.1. Computer system security requirements

All computers handling credit card numbers must have the following in place:

- a. A host-based firewall technology preventing connections from all ports except a specific subset (e.g. 443 for secure web transactions, IP restricted port 22 for

- system administration). All firewall rules must be documented and modifications approved in keeping with the *Service Certification Process*.
- b. All Microsoft Windows computers must run anti-virus software.
 - c. File integrity monitoring to an external system for critical system and application files for inappropriate/unauthorized modifications. Reviews for potential changes must occur daily.
 - d. System logging or auditing to an external server for all critical operating system modifications (e.g. all logins, unauthorized file access attempts) and maintain the log for at least 6 months
 - e. A single function (e.g. application or database) is implemented per server.
 - f. Security patches must be tested and, if possible, applied within one week of vendor release. All patches must be applied or documentation explaining the implementation problem within 30 days. A change log must be maintained for all servers.
 - g. Passwords must be at least 8 characters long and require complex passwords (inclusion of a number or special character), expire after 90 days or less, not reuse the last 4 passwords, and stored in an encrypted or hashed format.
 - h. All accounts must be disabled after 30 days of inactivity and, if not re-enabled and actively used, removed after an additional 60 days. The only exception is emergency accounts used for system recovery and not used regularly.
 - i. All system patches must be applied to a new computer before connecting to the network. All default account names and default passwords must be changed before connecting to the network. All computer security configurations and services/daemons must be reviewed before connecting to the network.
 - j. Perform vulnerability testing on associated computers every 30 days with penetration testing at least annually.
 - k. Only allow computer access by uniquely assigned and auditable IDs.

3.2. Connectivity security requirements

All computers handling credit card numbers must have the following provisions in place for network and modem connectivity:

- a. A network-based firewall preventing inappropriate/unauthorized access from outside the academic/business unit or specific authorized computers.
- b. An intrusion detection system monitoring for unauthorized access attempts.
- c. 24/7 monitoring for network-based firewall and IDS systems for potential penetrations and 24/7 on-call expertise for potential security incidents.
- d. Two-factor authentication for routers servicing all computers connecting to, handling, processing, or storing credit card numbers.
- e. Specific authorization for modem connections. All modem connection must be outbound only.
- f. All data transfers and administrative access must be in an encrypted format (e.g. SSL, SSH, IPSEC).

3.3. Credit card number storage requirements

Credit card numbers must be protected by encryption, hashing, or truncation. No complete credit card numbers will be stored on computers owned by the Georgia Institute of Technology in an unprotected manner. Standard encryption algorithms must use at least 128bit key. Minimum key lengths will be increased as computing

processing power improves. Minimum key lengths for new encryption technologies must be provided with these guidelines prior to implementation. Keys must be in a single accessible location with back-ups. Keys must be changed every 90 days and old keys must be deleted/destroyed after an additional 30 days.

The following additional requirements apply to computers storing credit card numbers and network connectivity beyond those noted in sections 3.1 and 3.2:

- a. Accounts must lock-out after six or fewer invalid login attempts and require manual re-enabling.
- b. Sessions must time-out after 15 minutes.
- c. All accesses to credit card numbers must be logged.
- d. All root access activities must be logged to an external server.
- e. The system must not be openly accessible from any public network.
- f. The computer's IP address must not be available outside the local subnet.
- g. A dedicated firewall must be in place specifically for computers storing credit card numbers to preventing any public access to protected systems. Access is only permitted by exception by both IP and port.
- h. Credit card numbers must not be stored in multiple locations with the exception of backups.
- i. CVV2 information must not be stored beyond the transaction authorization point.
- j. Two-factor authentication is *recommended*.

3.4. Physical security requirements

All servers storing credit card numbers must have the following provisions in place:

- a. The servers must be in the Network Operations Center (NOC) for the Office of Information Technology. Servers placed in a separate locked room within the NOC or within locked racks. Video surveillance must be maintained on the servers. All access to servers by anyone except employees specifically approved for access to the credit card numbers must be escorted continuously.
- b. The NOC must log all room access (maintained for at least 90 days), maintain video surveillance of room ingress and egress, and provide identification for easily distinguishing employees, visitors, and inappropriate access. Visitors must be issued a NOC ID that must be returned or issued a temporary ID and continuously escorted.
- c. All backup media must be secured on site, off site, and in transit. All transportation must be handled by approved Institute employees or bonded couriers.

3.5. Outsource requirements

Any unit may select to outsource their credit card transaction processing. This option transfers the risk to the outsourced service. Approval for credit card transaction processing must follow the standard approval process. Contracts must address these elements:

- a. Compliance with all appropriate credit card company security requirements.
- b. Service level agreements.
- c. Defining data retention and destruction requirements.

3.6. Review process for credit card transaction processing requests

- a. Document the business need for accepting credit card transactions in a new unit or location.
- b. Meet with Financial Services for justification and approval of business case.
- c. Meet with Information Security to evaluate options and costs for implementation (using existing facilities, implementing separate facilities, or outsourcing transaction processing).
- d. Meet with the Associate Vice President of Information Technology or Executive Director for the Office of Information Technology for technical approval of implementation.
- e. Meet with Georgia Institute of Technology Legal Affairs to ensure all contracts meet federal, state, and contractual requirements.

4. References

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

^[2] Data Access Policy

^[3] Credit Card Processing Policy