

From: Leo Tran, Information Security Officer
Office: Technology Services
1555 Poydras St, Suite 1400
Phone: (504) 988-8514 Email: ldtran@tulane.edu

Date: June 15, 2006
Ver: 1.0

Re: Guidelines for all computer systems handling credit card numbers at Tulane University.

I. Introduction

To be in compliance with the Graham Leach Bliley (GLB) Act as well as maintain compliance with requirements imposed by the Visa Card Holder Information Security Plan (CISP), MasterCard Site Data Protection Program (SDP) and Payment Card Industry Data Security Standard (PCI-DSS), Tulane University entities processing credit card payments must take appropriate measures to prevent the loss or disclosure of customer information including credit card numbers. Failure to protect the privacy of our customers may result in financial loss for many customers, fines imposed on the unit, suspension of credit card processing privileges and damage to the reputation of the unit and the university.

This document provides guidelines for all computer systems handling credit card numbers at Tulane University.

II. Guidelines

1. System Security Requirement

- a. A host-based firewall technology preventing connections from all ports except a specific subset.
- b. All Microsoft Windows computers must run anti-virus software.
- c. Daily file integrity monitoring.
- d. Daily system log auditing.
- e. System must have the latest operating system, firewall, and virus protection patches.
- f. Login passwords must be complex and at least 8 characters long with 60 days expiration.
- g. 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.
- h. Perform vulnerability testing on associated computers every 30 days.
- i. Perform penetration testing at least annually.

2. Connectivity Security Requirement (*Network and Modem*)

- a. A network-based firewall preventing inappropriate/unauthorized access from outside the academic/business unit or specific authorized computers.

- b. An intrusion detection system (IDS) that monitors for unauthorized access attempts.
- c. Continuous monitoring for network-based firewall and IDS systems for potential penetrations.
- d. Specific authorization for modem connections. All modem connection must be outbound only.
- e. All data transfers and administrative access must be in an encrypted channel (e.g. SSL, SSH, IPSEC).

3. Credit card number storage requirement

- a. Storage of credit card data is strongly discouraged. If stored, credit card numbers must be protected by encryption, hashing, or truncation. Advanced Encryption Standard (AES) algorithm is recommended. Triple Data Encryption Standard (3DES) algorithm is acceptable. In either case, the encryption keys must be stored in a single accessible location with backup.
- b. Access to credit card numbers shall be strictly limited to those with a legitimate business need.
- c. All media used for credit card numbers must be destroyed when retired from use.
- d. All paper records containing credit card numbers shall be shredded locally at the end of their required retention period.

4. Physical Security Requirement

- a. The server must be in one of Technology Services secured data centers.
- b. All access to servers by anyone except employees specifically approved for access to the cardholder systems must be escorted continuously.
- c. All backup media must be secured on site, off site, and in transit. All transportation must be handled by Institute employees or bonded couriers.

III. Definitions

Cardholder Data: Credit card numbers (in full or in part)

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

Encryption: Scrambling data in a recoverable format.

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

Graham Leach Bliley (GLB) Act: A US law containing provisions that require all financial institutions including our university to disclose to consumers and customers their policies and practices for protecting the privacy of nonpublic personal information. This law is also known as the Financial Modernization Act of 1999.

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.

Payment Card Industry Data Security Standard (PCI-DSS) : The unified standard data protection program mandated by VISA, MasterCard, American Express, Diners Club, Discover and JCB.

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

IV. References

- Payment Card Industry Data Security Standard (PCI-DSS)
- Visa CardHolder Information Security Plan (CISP)
- MasterCard Site Data Protection Program (SDP)
- Graham Leach Bliley (GLB) Act

V. Attachments

- Payment Card Industry Self-Assessment Questionnaires
- Payment Card Industry Security Standard