

**GRAMM-LEACH-BLILEY ACT
AND THE FTC SAFEGUARDS RULE**

**GEORGIA STATE UNIVERSITY
INFORMATION SECURITY PLAN
MAY 2003**

Prepared by Tammy L. Clark, University Information Security Officer

Reviewed by:

*Roberta Byrum, Assistant Vice President Finance
Kerry Heyward, Associate Legal Advisor, Legal Affairs
Mary Jane Casto, Interim Associate Provost*

Adopted by:

Carl V. Patton, President

Date

TABLE OF CONTENTS

I.	Executive Overview	1
	A. What is the Gramm-Leach-Bliley Act (GLBA)?	1
	B. What is the FTC Safeguards Rule?	1
	C. Why does the GLBA Apply to Georgia State University?	1
	D. What is the Scope of the Security Plan?	1
	E. What are the Primary Goals of this Security Plan?	1
II.	Compliance Measures	2
	A. Designating Employees to Coordinate the Safeguards	2
	B. Identifying and Assessing the Risks to Customer Information in Relevant Areas of the University	2
	C. Evaluating the Effectiveness of the Current Safeguards in Place	2
	D. Implementing Supplemental Measures	4
	E. Safeguards Reviews and Updates	4
III.	Employee Education and Training	4
	A. Brochure – Information Security Guidelines	4
	B. Departmental Procedures	4
IV.	Overseeing Service Providers	5
V.	Information Systems	5
	A. Storage of Physical and Electronic Records	5
	B. Secure Data Transmission	5
	C. Disposal of Sensitive Information	5
	D. Oversight and Audit Procedures	5
	E. Inventory and Security Reviews of Computer Systems	6
VI.	Managing Systems Failures	6
	A. Prevention, Detection and Response to Attacks, Intrusions or Other System Failures	6
	B. Preservation of Security and Integrity of Sensitive Data in the Event of System Failures	6
	C. Prevention of Unauthorized Access to Sensitive Data	6
	D. Notification and Reporting in the Event of Sensitive Data Compromises or Loss	6

I. EXECUTIVE OVERVIEW

A. What is the Gramm-Leach-Bliley Act?

The Gramm-Leach-Bliley Act (GLBA) requires “financial institutions” as defined by the Federal Trade Commission (FTC), to protect and secure customer information such as names, social security numbers, addresses, account and credit card information. The GLBA sets forth extensive privacy rules which the University is deemed to be in compliance with because of its adherence to the provisions of the Family Education Rights and Privacy Act (FERPA). The GLBA also establishes a Safeguards Rule, from which the University is not exempt, that requires the University to protect and safeguard customer information.

B. What is the FTC Safeguards Rule?

The Safeguards Rule requires financial institutions to secure customer information. It requires the University, as a financial institution, to develop a written information security plan that describes its program to protect customer information.

C. Why does the GLBA apply to Georgia State University?

The GLBA applies to the University because the University is considered a “financial institution” due to the financial activities in which it engages, such as processing student loans.

D. What is the Scope of this Security Plan?

This Plan applies to all “customer information” which is defined as any personally identifiable, nonpublic information that the University handles or maintains about an individual in the process of offering a financial product or service, or such information provided to the University by another financial institution. Such customer information is covered whether it is in paper, electronic or other form. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package and other miscellaneous financial services. Examples of customer information include addresses, phone numbers, bank and credit card information, income and credit histories and social security numbers.

E. What are the Primary Goals of this Security Plan?

The primary goals of this Security Plan are to:

- Designate one or more employees to coordinate the Security Plan
- Identify and assess the risks to customer information and evaluate the effectiveness of current procedures in place
- Design and implement a safeguards program

- Review and update the safeguards to ensure continued compliance with current federal requirements

II. COMPLIANCE MEASURES

A. Designating Employees to Coordinate the Security Plan

The University has designated the Director of Student Accounts, the Director of Financial Aid and the Registrar as the individuals responsible for coordinating this Plan. In addition, every University department that handles or maintains customer information is responsible for designating an individual who is responsible for coordinating safeguard measures and monitoring security risks within their department.

B. Identifying and Assessing the Risks to Customer Information in Relevant Areas of the University

Every University department that handles or maintains customer information is responsible for identifying the type of information, the form of the information and the security risks within their department and taking appropriate measures to mitigate those risks.

Potential security risks to customer information include the following:

Description
Computer systems vulnerable to electronic break-ins
Paper forms vulnerable to office break-ins after hours
Paper forms and computer systems left unattended or accessible during business hours
Paper forms containing customer information that are accessible to all employees

C. Evaluating the Effectiveness of the Current Safeguards in Place

Current safeguards taken to protect customer information include the following:

Description
Computer access limited by system ID's and passwords
Paper reports in file cabinets accessible only to staff in office who need access
Offices that are locked after hours
File cabinets that are locked
Data backed up nightly
Passwords that expire periodically and employees must then reset them
Passwords not posted in publicly viewable places
Intrusion detection systems that monitor the University network to allow the prompt detection of attacks and intrusions
Vulnerability scanning of systems containing customer information
Antivirus protection maintained on computer systems

Firewalls installed on computer systems
Separation of customer information from recycling and shredding of those records
Referring calls or other requests for customer information to designated individuals and being alert to fraudulent attempts to obtain this information
Keeping customer information stored in appropriate filing cabinets and clear of areas with public access
Customer information accessible only by staff with “need to know”
Promissory notes locked in storage for safe keeping after data entry

The following University policies also address the safeguarding of information:

Antivirus Software Policy:

<http://www.gsu.edu/%7Ewwwist/antivirussoftware.htm>

Install and maintain antivirus software on university computer systems

Sensitive Information Protection Policy:

<http://www.gsu.edu/%7Ewwwist/sensitiveinformation.htm>

Employ security measures designed to protect sensitive information

Georgia State University Information Security Policy:

<http://www.gsu.edu/~wwwist/informationSecurity.html>

Employ security measures to protect University computers from unauthorized access, compromises and attacks

Georgia State University Data Stewardship and Access Policy For University Information:

<http://www.gsu.edu/~wwwist/data.stewardship.html>

Follow proper procedures for requesting and granting access to University data that is critical to the administration of the University

Remote Access Policy:

<http://www.gsu.edu/%7Ewwwist/remotearchive.htm>

Use approved methods of gaining remote access to University computer systems, applications and data

The effectiveness of the above safeguards is dependent upon

- Universal application throughout the University
- University employees being responsible for complying with the above safeguards
- Implementation of additional safeguards as described below

D. **Implementing Supplemental Measures**

Additional safeguard measures that are recommended to supplement current safeguards include the following:

Description
Lock file cabinets containing customer information
Designate a staff member to supervise the disposal of records containing customer information
Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information
Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain customer information
Have the University Information Security Officer conduct security reviews to identify whether additional security measures are required to protect customer information processed and stored on University computer systems
Maintain inventories of all computer systems
Reduce paper forms and documents through increased web access to this information
Centralized files
Off-site storage retention of critical files and documents
Implement measures to ensure unauthorized persons cannot access University computer systems when left unattended
Avoid using Social Security numbers as primary identification number

E. **Safeguards Reviews and Updates**

Individuals responsible for coordinating this Plan will conduct periodic reviews of this Plan to ensure federal compliance, review current safeguards, and incorporate new safeguards that are adopted for implementation.

III. **EMPLOYEE EDUCATION AND TRAINING**

A. **Brochure – Information Security Guidelines**

An electronic brochure entitled **The Gramm-Leach-Bliley Act: Information Security Awareness Training** has been produced by the University Information Security Officer to advise employees of their responsibility to protect customer information and university computer systems from unauthorized access and compromises.

B. **Departmental Procedures**

Departments that process or maintain customer information are responsible for conducting training for employees who handle such information in the course of their job duties. This training should include physical handling and disposition of non-electronic documents containing customer information as well as proper procedures to follow in processing and storing electronic information and documents.

IV. **OVERSEEING SERVICE PROVIDERS**

The University will take reasonable steps to select and retain service providers who maintain appropriate safeguards for customer information. The Office of Legal Affairs will take steps to ensure that all relevant contracts include a privacy clause and are in compliance with the GLBA.

V. **INFORMATION SYSTEMS**

The FTC defines information systems as including network and software design, and information processing, storage, transmission, retrieval and disposal. Guidelines on how to maintain security throughout the life cycle of customer information—from data entry to data disposal are as follows:

A. **Storage of Physical and Electronic Records**

- Store records in secure areas and make sure that only authorized employees have access to these areas
Current and proposed additional safeguards would meet these guidelines.

B. **Secure Data Transmission**

- Provide for secure data transmission when collecting or transmitting customer information
Current and proposed additional safeguards would meet these guidelines.

C. **Disposal of Sensitive Information**

- Dispose of customer information in a secure manner
Current and proposed additional safeguards would meet these guidelines.

D. **Oversight and Audit Procedures**

- Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information
Current and proposed additional safeguards would meet these guidelines.

E. **Inventory and Security Reviews of Computer Systems**

- Maintain inventories of all computer systems and conduct security reviews on annual basis
Current and proposed additional safeguards would meet these guidelines.

VI. MANAGING SYSTEMS FAILURES

A. Prevention, Detection and Response to Attacks, Intrusions or Other System Failures

- Maintain up-to-date and appropriate programs and controls through
 - Computer security incident response plans
 - Installing security patches on computer systems
 - Using anti virus software that updates automatically
 - Using firewalls where appropriate
 - Centrally managed intrusion detection systems

Current safeguards, as well as existing Georgia State University Information Security Department programs and procedures, meet these guidelines.

B. Preservation of Security and Integrity of Sensitive Data in the Event of System Failures

- Back up all customer and financial data regularly
Current and proposed additional safeguards meet this guideline.

C. Prevention of Unauthorized Access to Sensitive Data

- Maintain systems and procedures to ensure that access to nonpublic customer information and financial data is granted only to legitimate and valid users
Current and proposed additional safeguards meet this guideline.

D. Notification and Reporting in the Event of Sensitive Data Compromises or Loss

- Notify customers promptly if their nonpublic personal information is subject to loss, damage, or unauthorized access
University departments are responsible for notifying their customers in the event that inadvertent disclosures occur.