JACKSON STATE UNIVERSITY'S

GRAMM-LEACH-BLILEY ACT

Training for All JSU Employees

GLBA TRAINING OVERVIEW

This JSU GLBA training course covers the basics of the Gramm-Leach-Bliley Act (GLBA) for all JSU Employees. After completing this training employees will be aware of the following:

- ❑ What is the GLBA ACT
- ❑ Key Terms under GLB Act regulations
- ❑ What actions are required or permitted under GLBA
- ❑ Required GLBA data protection safeguards
- ❑ How to Avoid GLBA Violation
- ❑ How/When to Report an incident with GLBA Data

GRAMM-LEACH-BLILEY DEFINITIONS

Customer: an individual/student who has obtained a financial product or service from the university to be used primarily for personal, family or household purposes and who has a continuing relationship with the university.

Customer Information: non-public personal information(ex. SSN, Bank or Credit Card Information) about an individual/student who has obtained a financial product or service from the university and who has a continuing relationship.

Information Security Program: A program developed, maintained and enforced by the JSU 's Department of Information Technology to ensure that the information assets of the university are maintained securely.

GRAMM-LEACH-BLILEY DEFINITIONS

Workplace Information Security & Protection (WISP) Checklist: A GLBA checklist designed to identify and correct weaknesses in the area of information security within a given department.

Student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and social security numbers, in both paper and electronic format.

3rd Party Service Provider: any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its direct provision of services to the university.

GRAMM-LEACH-BLILEY ACT (GLBA)

What is the GLBA Act?

The Gramm-Leach-Bliley Act is a law that mandates financial institutions to take steps to ensure the privacy, security and confidentiality of customer financial records.

How Does GLBA Apply to JSU?

Because higher education institutions engage in financial activities, such as making Federal Perkins Loans, the Federal Trade Commission (FTC) regulations consider them financial institutions for GLB Act purposes.

SECURING CUSTOMER INFORMATION

The GLBA Act outlines several specific requirements institutions must follow to ensure the privacy and security of customer financial information called Safeguards rules.

The Safeguards Rules require colleges/universities to apply administrative, technical, and physical safeguarding of customer information they collect.

To comply, JSU has created an information security plan and program that provides guidelines, safeguards, training, policies and best practices for its employees to protect critical data according to GLBA & FERPA laws.

JSU'S IT SECURITY PROGRAM

Jackson State University's Information Security program seeks to:

- (1) Ensure the security and confidentiality of customer/student records and information.
- (2) Protect against any anticipated threats or hazards to the security or integrity of such records.
- (3) Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any student/customer.

SECURING CUSTOMER INFORMATION

- Colleges/Universities must inform customers about their information-sharing practices.
- Colleges/Universities must explain to customers their right to "opt out" of sharing their non public information with 3rd party service providers.
- University units must assess their current customer information practices, identify vulnerabilities, and take appropriate measures to secure customer information.

JSU'S EMPLOYEES ROLE IN GLBA

Each JSU department head, supervisor, or manager is responsible for ensuring that all its employees do the following:

- Become aware of the responsibilities and roles of your department as it applies to the Gramm-Leach-Bliley Act Compliance.
- Complete quarterly/annual training on the Gramm-Leach-Bliley Act compliance guidelines.
- Conduct quarterly assessments of information security practices, and identify vulnerabilities in your area using the Workplace Information Vulnerabilities Checklist form
- Report incidents,threats and attacks in your area immediately to the proper JSU personnel (*Contact JSU information security officer or Email Administrator*).

TIPS TO AVOID VIOLATING GLBA

Don't toss sensitive paperwork in trash bins

- Dispose of customer information in a secure way and, where applicable, consistent with the FTC's disposal rules.
- Shred papers containing customer information so that the information cannot be read or reconstructed.
- Contact the appropriate IT personnel to dispose of hard drives containing non public student information.

TIPS TO AVOID VIOLATING GLBA

Review Vulnerability Check List Often

- Always check to make sure student information is being secured according to the JSU Workplace Vulnerability Checklist (WISP).
- Complete departmental assessment often; this should be done quarterly.
- Contact JSU Information Technology Department for help addressing any security vulnerabilities that can not be addressed within the department.

TIPS TO AVOID VIOLATING GLBA

Remove paperwork with non public info from desk

- Practice a clean desk policy by removing any paperwork containing sensitive data from desks while unattended.
- Store records in a room or cabinet when unattended.
- Lock rooms and file cabinets where records are kept.

TIPS TO AVOID VIOLATING GLBA

Use strong passwords & screen savers

- Ensure that the computer where student information is stored is accessible only with a “strong” password.
- Do not share or openly post employee passwords in work areas.
- Create strong passwords containing at least 10 characters that are difficult to guess.
- Turn on screen savers that are password protected to lock computers after a period of inactivity.

TIPS TO AVOID VIOLATING GLBA

Report any strange requests, emails, or vulnerabilities you encounter

- Report suspicious attempts to obtain customer information to designated personnel.
- Refer calls or other requests for customer information to designated individuals who have been trained in how to safeguard student data.
- Only access sensitive customer information if it is needed to conduct job duties or for a “legitimate educational interest“.

GLBA POLICY VIOLATIONS

Failure to Follow Policies

- Compliance with these data protection policies and safeguards under the GLBA is the responsibility of all members of the University community.
- Violations of these policies and laws will be dealt with seriously and will include sanctions, up to and including termination of employment.
- Employees suspected of violating these policies may be temporarily denied access to the data as well as University information technology resources during investigation of an alleged abuse.

CONTACT INFORMATION

JSU Department of Information Technology Incident Contacts:

- Shayron Nichols, PhD
  Cyber Security Awareness Training Coordinator

- Josiah Dosunmu
  Email Administrator

Report Cyber Incidents to:
cybersecurity@jsums.edu

**Feel free to contact us with questions or comments on information security or privacy at Jackson State University.*

REFERENCES FOR GLBA

Visit the Following Websites Below for More Resources on the GLB Act

- http://www.jsums.edu/cyberawareness
- https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-acty Rule?
- Https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information