JSU GLBA TRAINING 2022

Training for All 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:

1. What is the GLBA ACT
2. Key Terms under GLBA regulations
3. What actions are required or permitted under GLBA
4. New Required GLBA data protection safeguards
5. How to Avoid GLBA Violation
6. How/When to Report an incident with GLBA Data

WHAT IS GLBA?

- The Gramm-Leach-Bliley Act (GLBA) is a US law passed in 1999 that requires financial institutions to take steps to ensure the privacy, security and confidentiality of customer records
- GLBA also requires financial institutions to notify its customers about (1) how their non-public personal information (NPI) is shared, (2) what data they collect, and (3) who they share this data with

GLBA KEY TERMS

- **Financial Institutions-** companies that are “significantly engaged” in providing financial products or services (ex. loans, financial or investment advice, insurance, etc.)
- **Customers**-any student or individual who obtains or has obtained a financial product or service from a Financial Institution (ex. JSU)
- **Nonpublic Personal Information (NPI)**- any personally identifiable financial information: (ex. SSN, income, marital status, loan or deposit balances)
- **Safeguards**- rules that require colleges and universities to apply administrative, technical, and physical safeguarding of customer information they collect and/or store

GLBA KEY TERMS

- **Multi Factor Authentication (MFA)-**authentication through verification of at least two of the following types of authentication factors: (1) a password; (2) a token; or (3) fingerprint
- **Encryption**-a way of translating data from plaintext (unencrypted) to a format that is unreadable (encrypted) by a human or computer
- **Authorized User-** is any employee, contractor, agent or vendor that participates in JSU business operations and is authorized to access and use JSU's information systems and data
- **Pretexting**-the impersonation of a student to request private information by phone, email, or other media

WHO DOES GLBA APPLY TO?

- Colleges or Universities such as JSU that engage in financial activities, like processing or making Federal Perkins Loans
- Therefore the Federal Trade Commission (FTC) considers Colleges and Universities such as JSU to be financial institutions under Gramm-Leach-Bliley Act

PENALTIES FOR NON-COMPLIANCE

- A financial institution like JSU can be fined $100,000 for each violation
- A JSU employee found in violation of GLBA compliance may be fined $10,000 per violation
- An employee found violating the GLBA can also face up to 5 years of imprisonment

HOW GLBA PROTECTS DATA

- GLBA outlines several specific requirements JSU must follow to ensure data privacy and security:

  1) Inform customers about their information sharing practices

  2) Explain to customers their right to "**opt out**" of sharing their non public information with 3rd parties

  3) Assess current customer information protection practices, identify vulnerabilities, and apply safeguards

GLBA SAFEGUARD OBJECTIVES

- (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

JSU EMPLOYEES' ROLE UNDER GLBA

- Become aware of GLBA responsibilities and roles needed to protect sensitive data in your department
- Complete quarterly or annual GLBA Awareness Training
- Conduct quarterly assessments of information practices to identify vulnerabilities
- Report incidents, threats and attacks against GLBA data immediately to the proper parties in JSU's IT department

TIPS TO AVOID VIOLATING GLBA

- Dispose of customer information in a secure way ; don't toss paperwork with NPI data on it in trash bins
- Shred papers containing NPI data or private information so that it cannot be read or reconstructed
- Properly dispose of hard drives containing non public or private information by contacting the appropriate IT personnel

TIPS TO AVOID VIOLATING GLBA

- Always check to make sure student information is being secured using the JSU Workplace Vulnerability Checklist (WISP)
- Contact JSU IT Department to help address issues with unprotected Non public Information data in your department
- Avoid sending unencrypted Non public information through email to external third parties and internally to JSU employees

TIPS TO AVOID VIOLATING GLBA

- Practice a clean desk policy by removing any paperwork containing sensitive data from desks while unattended
- Store records containing student private data in a locked room or locked cabinet when unattended
- Turn on screen savers that are password activated to lock computers after a period of inactivity

TIPS TO AVOID VIOLATING GLBA

- Ensure that the computer where customer information is stored is accessible only with a “strong” password that is not easy to guess
- Do not share or openly post passwords in work areas that store NPI data
- Only access sensitive customer information if you are (1) an authorized user of this data and (2) it is needed to conduct your job duties or 3) for a “legitimate educational interest“

TIPS TO AVOID VIOLATING GLBA

New Mandatory GLBA Safeguards

- Authorized users (ex. JSU employees, vendors) must enable Multi Factor Authentication (ex. Google DUO) for any account(s) used to access NPI data
- All data sets containing customer NPI information must be encrypted while at rest and when in transit on internal and external networks

TIPS TO AVOID VIOLATING GLBA

- Report suspicious attempts to obtain customer information to designated personnel
- Refer calls or pretexting requests for customer information to designated individuals if you are unsure about how to safeguard personal data
- Beware of phishing scams and social engineering attempts to obtain NPI data by participating in phishing exercises and trainings

JSU GLBA VIOLATION DISCLAIMER

- Compliance with these data protection policies and safeguards under the GLBA is the responsibility of all members of the Jackson State 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 Division of Information Technology

Chief Information Security Officer : Dameion Brown

Cyber Security Awareness Training Coordinator: Shayron Nichols, PhD

Email Administrator: Josiah Dosunmu

Report Cyber Incidents or Questions to: cybersecurity@jsums.edu

GLBA REFERENCES

- https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm
- 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