LSU | Information Technology Services

GLBA INFORMATION SECURITY PROGRAM

Overview

The Gramm-Leach-Bliley Act (GLBA) reformed the financial services industry, addressed the privacy of non-public customer information, and described the necessity for the administrative, technical, and physical safeguarding of customer information. The Act broadly defines “financial institution” as any institution engaging in the financial activities enumerated under the Bank Holding Company Act of 1956, including “making, acquiring, brokering, or servicing loans” and “collection agency services.” A Federal Trade Commission rule enacted on November 12, 1999, extends GLBA compliance to colleges and universities. Because higher education institutions participate in financial activities such as making Federal Perkins Loans, FTC regulations consider them financial institutions for purposes of compliance with the Act.

Purpose and Scope

This document describes the measures taken by Louisiana State University A&M (“LSUAM” or “University”) that will ensure the security and confidentiality of covered data, protect against any anticipated threats or hazards to the security of such data, and protect against the unauthorized access or use of such data in ways that could result in substantial harm or inconvenience to customers. The practices described in this document are in addition to any University policies and procedures that may be required pursuant to other federal and state laws and regulations, including the Family Educational Rights and Privacy Act (“FERPA”).

For purposes of GLBA, covered data is limited to nonpublic personal information (NPI) in connection with student and parent finances, such as student and parent loans, bank account information, and income tax information for financial aid packages.

The following system and university offices (“functional units”) have GLBA responsibilities: Bursar Operations, Enrollment Management and Student Success (including Financial Aid & Scholarships and Registrar), and LSUAM Information Technology Services.

Program Requirements

1. Qualified Individual

LSUAM's Chief Information Security Officer (CISO) shall act as the designated Qualified Individual responsible for the GLBA Information Security Program. As Qualified Individual, the CISO shall oversee, implement, and maintain the GLBA Information Security Program. Although the ultimate responsibility for compliance lies with the Qualified Individual, the individual functional units are responsible for developing, implementing, and overseeing the University's compliance with the policies and procedures required by the Gramm Leach Bliley Act (GLBA).

2. Risk Identification and Assessment

The Information Security and Policy Team ("ITSP") has developed and maintained a risk management framework specific to information security. This framework, which includes a comprehensive risk register and mitigation approval process, is reviewed regularly with functional units, the GLBA Committee, and University leadership to document and prioritize all relevant information security risks. The risk management framework is based on the EDUCAUSE Risk Management Maturity Model.

The risks identified and prioritized in the register inform the regularly occurring security assessments of the functional units performed by ITSP. At the conclusion of each security assessment, functional units are provided with a comprehensive report detailing progress, deficiencies, and suggested mitigation strategies.

3. Safeguards

The following is a current list of safeguards implemented which are maintained through regular testing and monitoring for effectiveness, to ensure the security, confidentiality, and integrity of covered data:

I. Policies and Standards

LSUAM has implemented and published revised IT Policies and Standards as of Fall 2023. The policies and standards can be found at https://www.lsu.edu/its/units/it-security/it-policies.php.

These policies and standards support internal and external compliance and legal requirements and will be updated as necessary. University IT Policies and Standards are designed to reduce the inherent risk of handling sensitive data.

Functional units are responsible for facilitating and enforcing compliance with all information security policies and standards applicable to their unit.

II. Information Systems

Access to covered data through university information systems is limited to employees with a legitimate business need to access such data. Access to these information systems is restricted through access controls such as role-based

accounts, group policy, and network segmentation. Physical security perimeters are established through the use of gates, cameras, guards, card access, and biometrics.

Single Sign On (SSO) is available to all departments and units for authentication of University IT assets and applications. Enhanced security controls such as Multifactor Authentication (MFA) is leveraged for all enterprise applications.

All University-owned user endpoints must be encrypted using whole-disk encryption. Any data classified as sensitive is stored on encrypted servers, storage systems, databases, etc. Any system, application, and/or database that stores passwords/credentials must implement the appropriate encryption methodologies. Any transmission of sensitive data must be performed using approved, encrypted methods.

Change management procedures apply to all assets classified as enterprise assets. Departments and functional units are encouraged to maintain their own change management processes and procedures for assets under their purview.

LSUAM application developers shall incorporate security considerations within all phases of the software development lifecycle (SDLC). Custom applications are classified based on the data stored, processed, accessed, and/or presented through the application. Custom applications are required to comply with baselines that define the security parameters.

III. Data Management

University Data Management Policy is defined in Policy Statement 124. Standards regarding data classification, data handling, data storage, and data privacy are outlined.

Additionally, individual functional units are responsible for developing policies and procedures in accordance with applicable GLBA requirements such as data destruction, retention, and data asset mapping/inventory. Departments and functional units shall take reasonable measures to include processes for the disposal of covered information no later than two years after the last use date. A periodic review of data retention policies shall be conducted.

Functional units shall identify the flow of sensitive data processed throughout University systems. Data maps shall be developed detailing the types of data being processed, the data's location and format, and the data's purpose.

IV. Employee Management and Training

Background checks are performed on all employees before hire. When applicable, extended background checks may be performed. LSUAM only finalizes hires in Workday once all required background and reference checks have been completed. All employees are required to complete Cybersecurity Awareness training upon hire.

All LSUAM employees must complete mandatory annual training, which includes:

a) The Louisiana Code of Governmental Ethics
b) Power-based Violence Prevention & Response
c) Digital Resource and Content Accessibility Awareness

In addition to the University's annual training, functional units identified by the GLBA Committee require annual role-based training for employees interacting with covered data. Role-based training includes:

a) Family Educational Rights and Privacy Act (FERPA)
b) Gramm-Leach-Bliley Act (GLBA)
c) Payment Card Industry Data Security Standard (PCI-DSS)
d) Health Insurance Portability and Accountability Act (HIPAA)

Individual units are responsible for ensuring employees are adequately trained. This includes ongoing role-based training for IT personnel to effectively address relevant security risks and maintain current knowledge of changing information security threats and countermeasures.

ITSP maintains a comprehensive Security Awareness Program to educate and familiarize the university community with common threats they may encounter at work and home. This program features monthly phishing campaigns, social media, and hosted events such as interactive games and promotional item giveaways.

V. Oversight of Service Providers

GLBA requires the University to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. The Office of General Council has assisted with reviews, working with the offices of Procurement, Risk Management, and Information Security and Policy, ensuring that all relevant service provider contracts include specific language relating to governing laws, insurance needs, etc. Vendors who will have access to covered data must undergo a security risk assessment to identify and document risks associated with transmitting and/or storing covered data. Appropriate data security provisions are included in contracts with such vendors.

VI. Monitoring and Incident Response

Access to covered data is logged and monitored in accordance with the relevant IT Security Policy.

LSUAM maintains a comprehensive threat and vulnerability management program. Frequent, regularly occurring vulnerability scans are conducted on all systems containing sensitive data. Departments and units are responsible for leveraging available tools and addressing identified vulnerabilities. ITSP will address any high or critical vulnerabilities not remediated within the stated timeline by the individual unit. Penetration testing is conducted regularly.

LSU ITSP has developed a written Incident Management and Response Plan detailing processes and procedures that must be taken during and after a security incident. The plan identifies and details:

- The Cyber Incident Response Team members and their responsibilities
- Internal and external notification procedures
- Requirements for cyber incident response reporting and documentation
- Incident classification/severity
- Containment and eradication procedures
- Recovery and remediation procedures
- Post-recovery actions and monitoring
- Continuous plan evaluation

4. Program Evaluation and Adjustment

The information security program is required by GLBA to be periodically evaluated and adjusted based on the results of testing and the monitoring of any material changes to the operation, the results of the required risk assessments, or any other circumstances that are known to have, or that may have a material impact on the information security program. ITSP, in conjunction with the GLBA Committee, will evaluate and adjust the program at least annually.

5. GLBA Reporting

The CISO, acting as the designated Qualified Individual, shall deliver a report to the University Administration addressing the GLBA Information Security Program's overall status and related material matters. This report shall be delivered in writing, at least annually.

Contact Information

Designated Qualified Individual:

Sumit Jain, Director, IT Security and Policy (CISO)
E-mail: sjain@lsu.edu
Voice: 225-578-1362

Functional Leads:

Amy Marix, Director of Federal Aid & Scholarships
E-mail: amarix@lsu.edu
Voice: 225-578-3103

Elahe Russell, Associate Vice President for Accounting Services/Controller
E-mail: erussell@lsu.edu
Voice: 225-578-1639