COMPLIANCE WITH GRAMM LEACH BLILEY ACT

Harding University

Jun 1, 2023

Compliance with Gramm-Leach-Bliley Act (GLBA)

Introduction..... 2
GLBA Compliance Program..... 2
Categories of Information under the Plan..... 2
Purpose..... 3
Key Points..... 3
Departments Covered Under the GLBA..... 4
Roles and Responsibilities..... 5
GLBA Compliance Program Coordinator..... 6
Compliance Program Plan..... 6
- Defined Policy and Standards..... 7
- Data Mapping..... 7
- Risk Assessment and Implementation of Safeguard..... 7
- Conduct Risk Assessment..... 7
- Design and Implement Safeguards..... 8
- Testing and Monitoring of Systems..... 8
- Vulnerability Assessment..... 8
- Access Control..... 8
- Encryption..... 8
- Data Retention and Disposal..... 8
- Provide Awareness, Training and Education..... 8
- Incident Response Plan and Procedures..... 9
- Evaluate Service Providers' Agreements and Processes..... 9
- Program Maintenance..... 9

Contact Information..... 9
Definitions..... 10
Acknowledgement..... 11

Compliance with Gramm-Leach-Bliley Act (GLBA)

Introduction

The Gramm-Leach-Bliley Act, (GLBA) came into effect on May 23, 2003. It addresses the safeguarding and confidentiality of customer information held in the possession of financial institutions such as banks and investment companies.

However, GLBA contains no exemption for colleges or universities. Since Harding University engages in financial activities, such as processing student loans, it is required to comply. GLBA and other emerging legislation could result in standards of care for information security across all areas of data management practices both electronic and physical (employee, student, customer, alumni, donor, etc.). Therefore, this policy will be in effect for other highly critical and private financial and related information.

GLBA Compliance Program

The GLBA Compliance Program covers the entirety of the activities and practices of the following offices and individuals:

- Academic and administrative offices that handle electronic or printed personnel records, financial records, transactional records, or student records.
- Academic and administrative offices that transmit confidential information (protected data) to off-site locations as part of a periodic review or submission requirement.
- Centers and Institutes that provide services and acquire personal or financial information from participants or constituents.
- Faculty serving as directors, coordinators, principal investigators, or program directors for programs collecting protected data.
- Faculty, staff, and administrators with contracts to use, access, or provide protected data to or receive from a non-campus entity (e.g., government databases, science databases).

Categories of Information under the Plan

Information covered under the plan is defined by three categories:

- Personal Identifiable Information (PII)– Also known as protected data, PII includes first and last name, social security number, date of birth, home address, home telephone number, academic performance record, physical description, medical history, disciplinary history, gender, and ethnicity.
- Financial Information – Information that the University has obtained from faculty, staff, students, alumni, auxiliary agencies, and patrons in the process of offering financial aid or conducting a program. Examples include bank and credit card account numbers, and income and credit histories.
- Student Financial Information – Information that the University has obtained from a student in the process of offering a financial product or service, or such information provided to the University by another financial institution. Examples include student loans, income tax information received from a student's parent when offering a financial aid package, bank and credit card account numbers, and income and credit histories.

Compliance with Gramm-Leach-Bliley Act (GLBA)

Purpose

To continue to protect private information and data and to comply with the provisions of the Federal Trade Commission's safeguard rules implementing applicable provisions of the GLBA, Harding has adopted this compliance policy for certain highly critical and private financial and related information. This program applies to customer financial information (covered data) that Harding receives during business as required by GLBA as well as other confidential financial information that Harding has voluntarily chosen as a matter of policy to include within its scope.

Key Points

The Compliance Program is a continuous process that is undertaken at periodic intervals.

The GLBA Compliance Program Coordinator is responsible for implementing this Compliance Program.

Information Systems & Technology (IS&T) with the collaboration of Human Resources and the Finance departments shall develop appropriate training programs to ensure staff are aware of protocols for protecting customer information.

The Coordinator shall work with the CFO, and other offices as appropriate to make certain that service provider contracts contain appropriate terms to protect the security of covered data.

The Coordinator, working with responsible units and offices, shall monitor, evaluate and adjust the Compliance Program in light of the results of the risk management process.

Departments Covered Under the GLBA

The following table illustrates mapping of the departments that fall under the scope of the GLBA Safeguard Rules.

Exemplars of Data	Departments
○ Student loans (Harding and Federal ○ Private Student Loans ○ Personal Identifiable Information- SSN, Billing information, credit card, account balance, citizenship, passport information, tax return information, bank account information, driver's license, and date of birth ○ Disbursement of Financial Aid ○ Payment plans ○ 1098	● Financial Aid ● Business Office ● Admissions Office ● Office of the Registrar ● International Student Office ● International Programs Office ● Legal counsel
○ Loans ○ Payroll W2s	● Human Resources ● Payroll
○ Refunds ○ Drawdown of federal funds ○ Reconciliations ○ Audits ○ 1099	● Finance

Roles and Responsibilities

Role	Responsibility
Chief Information Officer	● Designates and serves as the GLBA Compliance Plan Coordinator ● Responsible for the system wide compliance with GLBA safeguarding rule through appropriate communication with and coordination among applicable groups ● Designates individuals who have the responsibility for Information Systems and Technology resources
IS&T Security Team	● Establishes and disseminates enforceable rules regarding access to and acceptable use of IS&T resources ● Establishes reasonable security policies and measures to protect data and systems ● Monitors and manages system resource usage ● Investigates problems and alleged violations of university information systems and technology policies and reports violations to appropriate university offices
Deans, Department Heads and other Managers	● Keep employees informed about policies and programs that pertain to their work, including those that govern GLBA compliance and ensure that they successfully complete the required training.
Employees with access to covered data	● Abide by University policies and procedures governing covered data as well as any additional practices or procedures established by their unit head or directors ● Report concerns to their supervisor
CFO	● Assist units with setting risk evaluation schedules and processes as requested
University auditors and cross-department GLBA working team	● Review conformance to the GLBA Compliance Plan as part of routine internal audits

GLBA Compliance Program Coordinator

The GLBA Compliance Program Coordinator (Coordinator) is responsible for implementing this Compliance Program. The Coordinator is appointed by the Executive Vice President.

The Coordinator:

- Works closely with the University Registrar, Human Resources, the General Counsel, the Business Office, the Office of Financial Aid, and such other offices and units as they have an interface with or control over covered data.
- Consults with responsible offices to identify units and areas of the University with access to covered data. As part of this Compliance Program, the Coordinator has identified units and areas of the University with access to covered data.
- Conducts surveys, or utilizes other reasonable measures, to confirm that all areas with covered information are included within the scope of this Compliance Program. The Coordinator maintains a list of areas and units of the University with access to covered data.
- Ensures that risk assessments and monitoring are carried out for each unit or area that has covered data and that appropriate controls are in place for the identified risks.
- Works to ensure adequate training and education are developed and delivered for all employees with access to covered data.
- Verifies existing policies, standards, and guidelines that provide for the security of covered data are reviewed and adequate.
- Makes recommendations for revisions to policy, or the development of new policy, as appropriate.
- Updates this Compliance Program, including this and related documents, from time to time.
- Ensures the written security plan is maintained and makes the plan available to the University community.

Compliance Program Plan

Compliance means following the laws, regulations and University policies that govern our everyday activities as members of the Harding community. This Compliance Program is a continuous process that is evaluated and adjusted, considering the following:

- The results of the required testing/monitoring
- Any material changes to Harding's operations or business arrangements
- Any other circumstances that may have a material impact on Harding's information security
- Data Mapping
- Risk assessment and implementation of safeguards
- Access control
- Encryption
- Awareness, training, and education
- Incident response plan and procedures
- Evaluate service provider's agreements and processes

- Continuous program maintenance
- Defined policies and standards

Defined Policy and Standards

Keeping security risks at a minimum is a priority. Harding's structure for maintaining confidentiality with information security ensures that risks of any kind are minimized. There is the quality assurance that comprehensive processes are in place for best practices and information protection. The areas are listed below:

- Risk assessments
- Third party risk management
- Vulnerability assessment and penetration testing
- Vulnerability and patch management
- Access Control
- Acceptable use
- Cryptography
- Security awareness, training, and education
- Incident response

Data Mapping

The Compliance program identifies the flow of the data processed throughout the university to assist in the identification of risks to privacy and security. This activity includes determining:

- The types of data being processed by the various business units
- The format of the data processed, and the location of the data being used and stored
- The purpose of the data being processed

Risk Assessment and Implementation of Safeguard

- Identifies reasonably foreseeable external and internal risks to the security, confidentiality and integrity of covered data that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromises of such information
- Assesses the sufficiency of any safeguards in place to control these risks
- The Coordinator works with all relevant departments to carry out comprehensive risk assessments.

Conduct Risk Assessment

This process includes system-wide risks as well as risks unique to each area with covered data and the effectiveness of management practices currently in place to ensure compliance and security enhancement. Risk assessments shall include a consideration of risks in each relevant area of operations and cover processes for handling, storing and disposing of paper records, processes for detecting, preventing, and responding to security failures and employee training and management, including the appropriateness and frequency of staff and management security awareness training.

Design and Implement Safeguards

As a result of the risk assessment, recommendations are made as necessary to change management practices to improve business controls and/or to implement information safeguards.

Harding has developed a set of policies and procedures to guide the security and privacy of data covered by GLBA.

Testing and Monitoring of Systems

Harding is diligent in its routine testing and monitoring of its systems, and the safeguards are a result of risk assessment outcomes.

Vulnerability Assessment

Harding ensures vulnerability assessment on systems that transmit, process, or store covered data.

Access Control

Access control is the university's ability to maintain, implement, and control its policies, standards, and procedures.

Encryption

To control the integrity and privacy of data that is processed, stored, and transmitted, Harding uses industry acceptable and approved encryption algorithms and solutions for access control.

Data Retention and Disposal

Harding is diligent in its data collection, retention, and disposal procedures. The record retention is in accord with the GLBA. This entails:

- Removing the maintenance of unnecessary documents from the onset of data collection to the end of the retention process.
- Supporting the maintenance of records filing systems to better facilitate retrieval and use.
- Protecting most important, up to date information while information of less value is disposed of or transferred to the appropriate secured storage area.
- Safeguarding information essential to Harding's daily business operations.

Provide Awareness, Training and Education

The following shall guide the training and management of employees:

- IS&T with the collaboration of HR will develop appropriate training programs to ensure staff is aware of protocols for protecting customer information.
- All training programs or materials incorporate concepts relevant to both electronic and paper-based customer information.
- Department managers and supervisors keep employees informed about policies and programs that pertain to their work, including those that govern GLBA compliance.

- Managers and supervisors ascertain which positions deal with customer information and assess whether these positions should be classified as “critical positions” requiring background checks, as provided for by Harding’s personnel policy.
- Department managers and supervisors ensure employees complete the mandatory core security training and specific GLBA training as assigned.
- All University employees that interact with the covered PII data during their daily activities are required to complete the GLBA Compliance training course describing their responsibilities while handling the personally identifiable information (PII).

Incident Response Plan and Procedures

Harding’s Incident Response Plan addresses possible threats that could arise concerning information privacy and cyber incidents. These steps are noted below:

- Formal and detailed documented responses for investigative purposes for resolving cyber issues
- Detection tools that readily identify cyber-attacks or system anomalies
- Official tabletop exercises to assist with preparation against common and known threats
- Incident response documentation that has additional information related to the incident such as status, impact, assessment, evidence gathered and next steps.

Evaluate Service Providers’ Agreements and Processes

Harding may share covered data with third parties. When this type of business is conducted, appropriate risk management steps are in place to minimize any corresponding potential risks. These steps include, but not limited to, reputational, financial, operational, strategic, and compliance risks. The decision to engage third parties will be consistent with Harding’s mission, values and vision.

Program Maintenance

The Coordinator, working with responsible units and offices, monitors, evaluates and adjusts the Compliance Program considering the results of testing and monitoring of the risks identified as well as in response to any material changes to operations or business arrangements and any other circumstances which may reasonably have an impact on the Compliance Program. This Program document will be reviewed, at a minimum, annually by the CIO and GLBA working committee.

Contact Information

Persons who may have questions regarding the security of any of the categories of information that is handled or maintained by or on behalf of the University may contact:

Office of the Chief Information Officer,
Ph 501 279 5700

Definitions

This section highlights some of the key terminologies used under the GLBA.

Customer Information - means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a faculty, staff, or student of Harding, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of Harding or its service providers.

The following are examples of data elements, but not limited, that fall under customer information, whether they are stored as paper records or electronically:

- Name
- Home address
- Home phone number
- Date/location of birth
- Driver's license number
- Name of spouse or other relatives
- Citizenship
- Bank and credit card number
- Income and credit histories
- Social Security numbers
- Students' performance evaluations or letters related to performance
- Other information within the definition of "customer information"

Non-public personal information - means any personally identifiable financial or other personal information, not otherwise publicly available, that the University has obtained from a customer in the process of offering a financial product or service; such information provided to the University by another financial institution; such information otherwise obtained by the University in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

Financial Information - includes student financial aid, student, faculty, and staff loans.

Covered data and information - for this program, this includes non-public personal information of customers required to be protected under GLBA. In addition to this required coverage, the University chooses as a matter of policy to also define covered data and information to include any bank and credit card account numbers, income and credit information, tax returns, asset statements, and social security numbers received during business by the University, whether or not such financial information is covered by GLBA. Covered data and information includes both paper and electronic records.

Service provider - means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to Harding that is subject to this part.

Acknowledgement

This document was prepared based heavily on the material that was discovered on the website of St John's University, 8000 Utopia Parkway Queens NY 11439.