HOWARD UNIVERSITY
The Gramm-Leach-Bliley Act

Jonathan F. Piersol
Associate Vice President & Chief Information Officer

Table of Contents

Document Control Table

Version	Date	Author	Rationale
1.0	October 2019	Oreoluwa Onatemowo	Original Draft
1.0	November 2019	Jonathan F. Piersol	Approval

1. Introduction

Gramm-Leach-Bliley Act, (GLBA) effective May 23, 2003, addresses the safeguarding and confidentiality of customer information held in the possession of financial institutions such as banks and investment companies. GLBA contains no exemption for colleges or universities. As a result, educational entities that engage in financial activities, such as processing student loans, are 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, the University has adopted a Customer Compliance Program for certain highly critical and private financial and related information. This Compliance Program applies to customer financial information (covered data) the University receives in the course of business as required by GLBA as well as other confidential financial information included within its scope.

1.1 Purpose

In order 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, the University has adopted this Compliance Program for certain highly critical and private financial and related information. The Compliance Program forms part of the overall strategic information security program of the University. This program applies to customer financial information (covered data) the University receives during business as required by GLBA as well as other confidential financial information the University has voluntarily chosen as a matter of policy to include within its scope. This page describes many of the activities undertaken by the University to maintain the security and privacy of the covered data according to GLBA requirements.

1.2 Scope

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).

1.3 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.

1.4 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.
- IT with the collaboration of HR shall develop appropriate training programs to ensure staff is aware of protocols for protecting customer information.
- The Coordinator shall work with the Office of the General Counsel and Procurement Office, 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.

1.5 Departments Covered Under the GLBA

GLBA Safeguard Rules for Title IV Schools

Financial assets under the GLBA Safeguarding Rule	**Departments that handle these types of information assets**
• Student loans (Howard loans, bank loans, and federal loans) • Private Student loans	• Financial Aid • Bursar • Office of Admission

Financial assets under the GLBA Safeguarding Rule	Departments that handle these types of information assets
• 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	• Office of the Registrar • International Student Service Office • Human Resources • The School of Law • Dean's Offices
• Personal Identifiable Information - SSN, Billing Information, Credit Card, Account Balance, Passport Information, Tax Return Information, Bank Account Information, Driver's License and Date of Birth	• Office of the General Counsel
• 403(b) loans • Emergency faculty loans • Emergency staff loans • Payroll W2s	• Human Resources (HR)
• G5 drawdown of federal funds • Refunds and T & E payments • Reconciliations • Coordination of Audits • 1099	• Office of the CFO & Treasury

2. GLBA Compliance Program

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

- The results of the required testing/monitoring,
- Any material changes to Howard's operations or business arrangements and
- Any other circumstances that may have a material impact on Howard's information security program.

2.1 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

2.2 Risk Assessment and Implementation of Safeguard

The Compliance Program:

- 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 compromise of such information; and

- 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.

2.3 Design and Implement of 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. Howard implements the following policies and procedures that guides the security and privacy of data covered by GLBA:

700-002 Acceptable Use Policy

600-002 Student Privacy Rights Policy (FERPA)

400-003 Record Retention and Destruction

2.4 Provide Awareness, Training and Education

The following shall guide the training and management of employees:

- IT with the collaboration of HR 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 St. John'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).

2.5 Program Maintenance

The Coordinator, working with responsible units and offices, monitors, evaluates and adjusts the Compliance Program in light of 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.

2.6 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:

Jonathan F. Piersol,
Associate Vice President & Chief Information Officer
Wonder Plaza
2301 Georgia Avenue NW, Suite 334
Washington DC, 20059
Email: jonathan.piersol@howard.edu
Telephone: (202) 806-2973

Oreoluwa Onatemowo
Acting Information Security Manger
Compliance Coordinator
Wonder Plaza
2301 Georgia Avenue NW, Suite 220
Washington DC, 20059
Email: oreoluwa.onatemowo@howard.edu
Telephone: (202) 806-2478

The complete Gramm Leach Bliley Information Security Program is available on the ETS webpage at www.howard.edu/technology

The Compliance Program:

- 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 compromise of such information; and

- 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.

3. Service Provider Oversight

Whenever the University retains a service provider that will maintain, process or have access to student or employee information, the University will ensure that the provider has in place an information security program sufficient to protect sensitive data. The University will include in the contracts with service providers having access to non-public information a provision requiring the providers to have in place security measures consistent with the requirements of federal regulations and to assure that such information is used only for the purposes set forth in the contract.

4. Definitions

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

Customer Information –
means any record containing nonpublic personal information, about a faculty, staff and student of Howard University, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of Howard or its 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 in the course of business by the University, whether or not such financial information is covered by GLBA. Covered data and information include 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 Howard that is subject to this part.