AMERICAN UNIVERSITY
WASHINGTON, DC

**University Policy: Gramm-Leach-Bliley Policy**

**Policy Category:** Information Technology

**Subject:** Compliance with certain safeguards and regulatory obligations to protect the security and confidentiality of an individual's sensitive, non-public, personal information ("Covered Information").

**Responsible Executive:** Vice President & Chief Information Officer

**Offices Responsible for Review of this Policy:** Office of Information Technology and Office of Finance and the Treasurer

**Supplemental Documents:** Supplemental information contained on the OIT Security & Privacy dedicated webpage

**Related University Policies:** Data Breach Notification Policy, Data Classification Policy, Confidentiality of Student Records Policy (FERPA)

---

## I. SCOPE

This policy applies to all offices, departments, or units that collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Covered Information. These offices include, but are not limited to, IT, financial aid offices (undergraduate, graduate, and law school), student accounts, financial operations, auxiliary services, admissions (undergraduate, graduate, and law school), housing and residence life, and human resources ("Covered Offices").

## II. POLICY STATEMENT

This policy outlines American University's ("University" and/or "AU") compliance with the Gramm-Leach-Bliley Act (GLBA) and its implementing regulation called the Safeguards Rule ("the Rule") (16 CFR Part 314 as amended) which requires the University to develop, implement, and maintain a comprehensive written Information Security Program to safeguard customer financial information.

Information Security Program objectives include:

**A.** Ensuring the security and confidentiality of customer financial information in compliance with applicable GLBA rules as published by the Federal Trade Commission;

**B.** Protecting against any anticipated threats to the security or integrity of such information; and

**C.** Guarding against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

## III. DEFINITIONS

*Customer:* any individual (student, parent, faculty, staff, or other third party) with whom the University interacts, who receives a financial service from the University and who, in the course of receiving that service, provides the University with sensitive, non-public, personal information about themselves.

**A.** ***Financial services:*** examples include offering or servicing student and employee loans; receiving income tax information from a student's parent when offering a financial aid package, engaging in debt collection activities, and leasing real or personal property to individuals for their benefit.

**B.** ***Covered Information:*** sensitive, non-public, personally identifiable information including, but may not be limited to, an individual's name in conjunction with any of the following: social security number, credit card information, income and credit history, bank account information, tax return, asset statement. Covered Information includes both paper and electronic records.

## IV. POLICY

The Gramm-Leach-Bliley Act requires financial institutions – companies and organizations that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. Academic institutions, including American University, are considered financial institutions and must adhere to the GLBA Financial Privacy and Safeguards Rules when handling student financial records.

American University will take the following steps to comply with GBLA:

### A. Appointment of Qualified Individual

American University has appointed the Chief Information Security Officer (CISO, ciso@american.edu), supported by the Director of Cyber Policy, to serve as the Qualified Individual to oversee, implement, and enforce the information security program.

### B. Risk Assessments and Safeguards

American University has a robust information security program that includes identifying areas of risk and maintaining appropriate safeguards. Safeguards are designed to reduce risk inherent in handling protected information and include safeguards for information systems and the storage of paper.

More information about the University's GLBA related information security program can be found here on the OIT Security & Privacy dedicated webpage.

The program includes regular testing and monitoring of the effectiveness of key safeguards, including those to detect actual and attempted attacks on, or intrusions into, AU information systems.

In the case Covered Information exists outside an enterprise system, such as department managed database: Each Covered Office is responsible for assessing the security of Covered Information in accordance with this policy. Covered Offices must develop and document their own information safeguards for Covered Information. This documentation must be shared with the Chief Information Security Officer (ciso@american.edu) and updated or reviewed on an annual basis.

### C. Policies and Procedures

The University has adopted comprehensive policies, standards, and guidelines relating to information security. Where appropriate, Covered Offices may adopt procedures consistent with this and other University policies. Unit leaders are responsible for facilitating and enforcing compliance with all GLBA information security policies and practices applicable to their unit.

Paper records: Covered Offices should develop and maintain procedures that reasonably assure the security of paper records and include guidelines which comply with the University's Records Retention and Disposal Policy. Periodic evaluation of these procedures regarding physical paper records should be conducted.

### D. Oversight of Service Providers and Contracts

AU will take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. Vendors who will have access to covered data must undergo a security risk assessment to identify and document risks associated with the vendors transmitting and/or storing Covered Information. The Office of Information Technology (OIT) works closely with Procurement and Contracts to ensure appropriate data security provisions are included in contracts with such vendors.

### E. Evaluation and Revision of the Information Security Program

In light of the results of regular testing and monitoring described above, the OIT security team review and adjusts the information security program following established governance practices. OIT will make recommendations to Covered Offices as it deems necessary to ensure the continued security of Covered Information.

### F. Establish an Incident Response Plan

American University has established the Data Breach Notification Policy that requires the implementation of safeguards for Covered Information and encourages reporting of potential data breaches. Additionally, Office of Information Technology's Critical Incident Management Process (AU login required) provides an internal process for the management of critical data incidents should one occur.

### G. Report Regularly to Governing Body

AU's Qualified Individual will provide a written report, at least annually, to the Board of Trustees via the Vice President and CIO.

### H. Employee Training and Education

Each Covered Office trains and educates its employees on relevant policies and procedures for safeguarding Covered Information. The Qualified Individual or designee can assist Covered Offices in evaluating the effectiveness of procedures, practices, and employee training. Covered Offices are responsible for updating and maintaining documentation of required employee training.

## V. EFFECTIVE DATE AND REVISIONS:

This Policy is effective September 27, 2024.

This Policy was approved February 2009 and reviewed December 2010 and January 2015.