AMERICAN UNIVERSITY WASHINGTON, D.C.

University Policy: Gramm-Leach-Bliley Policy

Policy Category: Operational Policies: Ethics, Integrity and Legal Compliance Policies: Information Technology Policies

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").

Office Responsible for Review of this Policy: Office of Finance and Treasurer

Procedures: Guidance for Implementing AU's Information Security Plan: Thresholds for Notification—Deciding Whether or Not to Notify

Related University Policies: Data Breach Notification Policy: American University Information Technology Security Policies: Identity Theft Prevention Policy: Records Retention and Disposal Policy

---

I. SCOPE

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

II. POLICY STATEMENT

This policy encompasses the information security plan that is intended to comply with the Gramm-Leach-Bliley Act ("GLBA") in protecting the security and privacy of sensitive, non-public, personal information. In addition, to the information required to be protected by GLBA, the university has voluntarily chosen to protect other sensitive personal information. Collectively, this information will be referred to as "Covered Information."

The information security plan is designed to: 1) ensure the security and confidentiality of Covered Information, 2) protect against anticipated threats to the security or integrity of Covered Information, and 3) protect against unauthorized access to or

use of Covered 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.
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.
Covered Information—sensitive, non-public, personally identifiable information includes, but may not be limited to, and 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

1. Information Security Plan Coordinator
   The designated employee for the coordination and oversight of this policy is the Executive Director of Risk Management and Safety Services or his/her designee ("Information Security Plan Coordinator" or "coordinator"). The coordinator must work with all relevant areas of the university: 1) to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Covered Information, 2) to evaluate the effectiveness of the current safeguards for controlling these risks, 3) design and implement a safeguards program, 4) to implement a training program for employees who have access to Covered Information, 5) to oversee service provider and contract compliance, and 6) to evaluate and adjust the security plan periodically.

   The coordinator, with guidance from the vice president of finance and treasurer and the provost, may establish a Gramm-Leach-Bliley working committee to work with the coordinator to carry out elements of the policy. The coordinator may also designate other university officials to oversee and

coordinate particular elements of the policy. All comments and inquiries about the university's Gramm-Leach-Bliley Policy should be sent by e-mail to the coordinator at pat@american.edu.

2. Risk Assessment

   The coordinator provides guidance to Covered Offices to identify and assess internal and external risks to the security, confidentiality, and integrity of Covered Information that could result in unauthorized access, disclosure, misuse, alteration, destruction or other compromise of such information.

   Each Covered Office is responsible for securing Covered Information in accordance with this policy. Covered Offices must develop and document their own information safeguards for Covered Information. The scope of such assessment and evaluation may include but is not limited to management and training of employees (including student employees) and volunteers; information systems (including network and software design, as well as information processing, storage, transmission and disposal for both paper and electronic records); procedures for detecting, preventing and responding to attacks, intrusions, or other system failures (including data processing, and telephone communication), and contingency planning and business continuity.

3. Employee Training and Management

   Each Covered Office trains and educates its employees on relevant policies and procedures for safeguarding Covered Information. The coordinator helps each Covered Office develop procedures to evaluate the effectiveness of its procedures and practices regarding employee training.

4. Information Systems

   The coordinator, or his/her designee, develops procedures to assess the risks to Covered Information associated with the university's information systems including network and software design, as well as information processing, storage, transmission, retrieval, and disposal of Covered Information. This assessment includes a review of the university's information technology practices and procedures. In addition, the coordinator assesses the procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with security flaws.

5. Physical Security of Paper Records

   Covered Offices should develop and maintain procedures that reasonably assure the security of paper records and include guidelines relating to the university's records retention and disposal policy. Periodic evaluation of these procedures regarding physical paper records should be conducted.

6. Managing System Failures
   The university maintains systems to prevent, detect, and respond to attacks, intrusions, and other system failures. The coordinator, or his/her designee, develops a plan for detecting, preventing and responding to attacks or other system failures; and reviews network access an security policies and procedures, and protocols for responding to network attacks and intrusions.

7. Designing and Implementing Safeguards
   The risk assessment and analysis described in section 2 shall apply to all methods of handling or disposing of Covered Information, whether in electronic, paper, or other forms. On a regular basis, the coordinator shall implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. The level of monitoring will be appropriate based upon the potential impact and probability of the risks identified, as well as the sensitivity of the information provided.

8. Service Providers and Contracts
   From time to time, the university may share Covered Information with third parties in the normal course of business. These activities may include debt collection activities, transmission of documents, destruction of documents or equipment, or other similar services. All contracts must include provisions that address third-party Gramm-Leach Bliley compliance.

   The coordinator works with those responsible for the third-party service procurement activities and Covered Offices to raise awareness of, and to institute methods for selecting and retaining only those providers that are capable of maintaining appropriate safeguards for Covered Information.

9. Roles and Responsibilities
   Deans, Directors, Department Heads and other Managers—individuals responsible for managing employees with access to "Cover Information" will designate a responsible contact person to work with the coordinator to assist in implementing this policy. The designated contact will ensure that risk assessment questionnaires are completed for that unit and that monitoring based upon identified risks takes place.

   Employees with Access to Covered Information—must abide by university policies and procedures governing Covered Information, as well as any additional practices or procedures established in their units.

   Information Security Plan Coordinator—is responsible for implementing the provisions of this policy.

Chief Information Officer—will designate individuals who have the responsibility and authority for information technology resources; establish and disseminate enforceable rules regarding access to and acceptable use of information technology resources, establish reasonable security policies and measures to protect information and systems; monitor and manage system resource usage; investigate problems and alleged violations of university information technology policies; and refer violations to appropriate university offices such as human resources, the office of general counsel and university public safety department for resolution or disciplinary action.

10. ***Policies, Standards and Guidelines***—the university has adopted comprehensive policies, standards, and guidelines relating to information security. These policies are incorporated by reference into this policy.

V. EFFECTIVE DATE:

Revised format February 2009; Reviewed December 2010; January 2015

VI. Approval

This document was approved and signed by

Donald Myers
Vice President and Treasurer

on February 4, 2009