THE UNIVERSITY OF ALABAMA®

Gramm-Leach-Bliley Act Information Security Program

Unit: Office of Information Technology (OIT)
Effective Date: 8/6/2003
Revision Date: 9/30/2019

Contact: J. Ashely Ewing
Title: Chief Information Security Officer

Purpose

Gramm-Leach-Bliley Act (15 U.S. Code § 6801 *et seq.*, hereinafter "GLBA"), along with agreements between the University and the United States Department of Education (Federal Student Aid Program Participation Agreement – PPA, and the Student Aid Internet Gateway Enrollment Agreement – SAIG), require the University to ensure the security, integrity, and confidentiality of covered information and data, which includes student financial aid records and Information. The University is in compliance with the privacy provision of GLBA by its compliance with the Family Education Right and Priviacy Act (FERPA).

Policy

This Information Security Program ("Program") ensures that administrative, technical and physical safeguards are implemented by The University of Alabama to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle covered data and information in compliance with the FTC's Safeguards Rule (16 C.F.R. Part 314) promulgated under the GLBA. These safeguards are provided to:

- Ensure the security and confidentiality of covered data and information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any customer.

In compliance with GLBA and FTC final Safeguards Rule, the University shall appoint an Information Security Program Coordinator(s), conduct risk assessments of likely security and privacy risks, maintain a training program for all employees who have access to covered data and information, oversee service providers and contracts, and evaluate and adjust the Information Security Program periodically.

Information Security Program Coordinator(s)

The Director of Student Financial Aid, the Director of Student Account Services and the Chief Information Security Officer (CISO) are the co-coordinators of this Program. The Director of Student Financial Aid and the Director of Student Account Services are responsible for maintaining a program for the periodic training and awareness related to the handling and protection of information covered by this Program, and oversee service providers and contractors. The CISO will assist the Director of Student Financial Aid and the Director of Student Account Services with a periodic risk assessment that will identify likely security and privacy risk to the covered data, and provide a remediation plan for the identified risk. The Director of Student Financial Aid and the Director of Student Account Services will maintain the

artifacts related to periodic risk assessment and remediation, and maintain training and awareness data provided to each relevant business unit.

Director of Student Finanical Aid and the Director of Student Account Services are responsible for maintaining a data map, coordinating with each relevant business unit handling covered data, and ensuring training and awareness. Each relevant business unit may also assist with periodic risk assessments and implementation of certain risk assessment remediation, and may assist with periodic review and input to this Program.

The Director of Student Financial Aid, the Director of Student Account Services, and the CISO will evaluate this Program periodically to make appropriate adjustments.

Identification and Assessment of Risks to Customer Information

The Director of Student Financial Aid, the the Director of Student Account Services assisted by the CISO, shall periodically conduct and document risk analysis consisting of, but not limited to the following:

- Asset Inventory –servers, desktops, and applications that contain covered data
- Data criticality analysis
- Threat assessments including but not limited to the following:
    - Compromised system security as a result of system access by an unauthorized person
    - Deliberate network-based attacks or malicious software upload
    - Ransomware, rendering covered data unreadable or unusable
    - Interception of covered data during transmission
    - Loss of covered data integrity
    - Lack of a clean desk policy
    - Inadvertent data entry
    - Physical loss of covered data in a disaster (floods, earthquakes, tornados, electrical storms, etc.)
    - Inaccessibility of covered data due to environmental factors (long-term power failure, pollution, chemicals, and liquid leakage)
    - Errors introduced into the system
    - Corruption of data or systems
    - Unauthorized access (intentional and unintentional) to electronic or hardcopy covered data and information by employees or others
    - Unauthorized requests for covered data and information
    - Unauthorized transfer of covered data and information through third parties
    - Third party vendors who process covered data and information not appropriately safeguarding covered data
    - Unsecure storage of covered data and information
    - Failure to dispose of covered data and information in a secure manner
- Design, implementation, and development of a risk mitigation strategy
- Maintain a written record of risk assessments and remediation

Recognizing that this may not represent a complete list of the risks associated with the protection of covered data and information, and that new risks are created regularly, The University of Alabama Office of Information Technology (OIT) Security Team will actively participate and monitor appropriate cybersecurity advisory groups for identification of additional risks.

The University of Alabama OIT Security Team works to monitor and maintain safeguards that are reasonable, and in light of current risk assessments, are sufficient to provide security and confidentiality to covered data and information maintained by the University. Additionally, the University of Alabama OIT Security Team strives to maintain safeguards that reasonably protect against currently anticipated threats or hazards to the integrity of such information.

Employee Management and Training

Background checks of new employees in areas that regularly work with covered data and information are required by Human Resource Policy. Employees in relevant business units receive proper training regarding the importance of safeguarding the confidentiality, security and integrity of covered data (e.g. student records, student financial information), including the University's Policy on Confidentiality of Student Records (FERPA), and regulations from the Department of Education. These employees are also trained on security measures, including the proper use of computer information and passwords, and incident response and breach notification procedures. Reports of these training efforts, which help minimize risk and safeguard covered data and information, are provided to Director of Student Financial Aid and the Director of Student Account Services.

Physical Security

The University of Alabama has addressed the physical security of covered data and information by limiting access to only those employees who have a legitimate business reason to handle such information. For example, federal financial aid applications, income and credit histories, accounts, balances and transactional information are available only to The University of Alabama employees with an appropriate business need for such information. Furthermore, each department responsible for maintaining covered data and information is instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures.

Information Systems

Access to covered data and information via The University of Alabama computer information system is limited to those employees and faculty who have a legitimate business reason to access such information. The University of Alabama has adopted comprehensive policies, standards, and guidelines relating to information security, which are incorporated by reference into this Information Security Program.

Social security numbers are considered protected information under both GLBA and the Family Educational Rights and Privacy Act (FERPA). As such, The University of Alabama has discontinued the use of social security numbers as student identifiers in favor of Campus Wide Identification (CWID) numbers as a matter of policy. By necessity, student social security numbers will remain in the information systems; however, access to social security numbers is granted only in cases where there is an approved, documented business need.

Management of Security Incidents

The University of Alabama OIT Security Team has developed written plans and procedures to detect any actual or attempted attacks on The University of Alabama information systems and has a Security Incident Response Plan, which outlines procedures for responding to an actual or attempted unauthorized access to covered data and information, including addressing university officials responsible for breach notification.

Oversight of Service Providers

GLBA requires the University take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. This Information Security Program ensures that such steps are taken by contractually requiring service providers to implement and maintain such safeguards. The Director of Student Financial Aid and the Director of Student Account Services will identify service providers who have or will have access to covered data, and work with Procurement and other offices as appropriate, to ensure that service provider contracts contain appropriate terms to protect the security of covered data. The section of the University's General Terms and Conditions, entitled "Safeguarding Rules of the Gramm-Leach-Bliley Act," is accessible on the Contract Management Office of Procurement Services website and sets forth the specific terms contractors of the University must comply with to maintain appropriate safeguards for covered data and information.

Continuing Evaluation and Adjustment

The Director of Student Financial Aid, the Director of Student Account Services, and the CISO will evaluate this Program periodically to make appropriate adjustments to the Program, to update risk assessment and remediaion, and review and update training material.

Scope

The GLBA Information Security Program should be observed by students, faculty, staff, and contractors/suppliers.

Definitions

Covered data and information Covered data and information for the purpose of this Program includes personal, non-public financial information (defined below) that is protected under the GLBA. Covered data and information includes both paper and electronic records.

Personal, non-public financial information Information that The University of Alabama has obtained from a student or customer in the process of offering a financial product or service, or such information provided to the University by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include the name of a student or student's family members and their addresses, phone numbers, bank and credit card account numbers, income and credit histories, and Social Security numbers, in both paper and electronic format.

Approved by

Kevin Whitaker, Executive Vice President and Provost