POLICY TITLE

Information Security Policy Plan

POLICY NUMBER

8-002

Responsible Unit: *Division of Information Technology*	**Effective Date:** *03/12/2021*
Responsible Official: *Associate Vice President for Information Technology*	**Last Reviewed Date:** *03/01/2021*
Policy Classification: *Information Technology*	**Origination Date:** *01/01/2021*

I. POLICY STATEMENT AND RATIONALE

This Southern University System Information Security Policy ("Plan") describes safeguards implemented by the Southern University System to protect covered data and information in compliance with the Federal Trade Commission's (FTC's) Safeguards Rule promulgated under the Gramm Leach Bliley Act (GLBA), Family Educational Rights and Privacy Act (FERPA), Louisiana House Bill No.633 Act No.155, and the Payment Card Industry Data Security Standard (PCI-DSS).

These safeguards are provided to:

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

This Information Security Program also identifies mechanisms to:

- Identify and assess the risks that may threaten covered data and information maintained by the Southern University System
- Develop written policies and procedures to manage and control these risks
- Implement and review the program
- Adjust the program to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security

II. POLICY SCOPE AND AUDIENCE

The scope of this policy includes all information assets governed by the Southern University System. All personnel and service providers who have access to or utilize information assets of the Southern University System, including data at rest, in transit or in process shall be subject to these requirements. This Policy applies to all information assets operated by the Southern University System; all information assets provided by Southern University System through contracts, subject to the provisions and restrictions of the contracts; and all authenticated users of the Southern University System's information assets.

All third parties with access to the Southern University System's non-public information must operate in accordance with a service provider contract containing security provisions consistent with the requirements promulgated under, but not limited to the Gramm-Leach-Bliley Act (GLBA), Family Educational Rights and Privacy Act (FERPA), Louisiana House Bill No.633 Act No.155, and the Payment Card Industry Data Security Standard (PCI-DSS).

This policy applies to all non-public personal information of the Southern University System's "customers" such as students, alumni and donors that the Southern University System is privy to, or maintains.

III. POLICY COMPLIANCE

Violations of this policy may result in loss of Southern University system and network usage privileges, and/or disciplinary action, up to and including termination or expulsion as outlined in the applicable user policies.

IV. POLICY DEFINITIONS

- Covered data and information: For the purpose of this program, this includes customer financial information (defined below) that is protected under the GLBA and other regulations listed above. In addition to this coverage, which is required under federal law, the Southern University System chooses as a matter of policy to include in this definition any and all sensitive data, including credit card information and checking/banking account information received in the course of business by the organization, whether or not such information is covered. Covered data and information includes both paper and electronic records.
- Pretext calling: This occurs when an individual attempts to improperly obtain personal information of Southern University System's customers so as to be able to commit identity theft. It is accomplished by contacting the organization, posing as a customer or someone authorized to have the customer's information, and through the use of trickery and deceit (sometimes referred to as 'social engineering'), convincing an employee of the organization to release customer-identifying information.
- Student financial information: This is information that the Southern University System has obtained from a student or customer in the process of offering a financial product or service, or such information provided to the organization 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 addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

V. POLICY IMPLEMENTATION PROCEDURES

GLBA mandates that the Southern University System appoint an Information Security Program Coordinator, conduct a risk assessment of likely security and privacy risks, organize 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) and Committee

The Deputy CIO of Security & Risk Management and the Information Security Officer have been appointed as the coordinators for the Southern University System. They are responsible forming a committee, the Cybersecurity Committee, for assessing the risks associated with unauthorized transfers of covered data and information, and implementing procedures to minimize those risks to the organization. The Cybersecurity Committee, together with risk management, accounting and other personnel will also conduct reviews of areas that have access to covered data and information to assess the internal control structure put in place by the administration and to verify that all departments comply with the requirements of the security policies and practices delineated in this program.

Identification and Assessment of Risks to Customer Information

The Southern University System recognizes that it is exposed to both internal and external risks, including, but not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties

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 Southern University System Cybersecurity Team will actively participate and monitor appropriate cybersecurity advisory groups for identification of new and emerging risks.

Current safeguards implemented, monitored and maintained by Southern University System Cybersecurity team are reasonable, and in light of current risk assessments are sufficient to provide security and confidentiality to covered data and information maintained by the organization. Additionally, these safeguards reasonably protect against currently anticipated threats or hazards to the integrity of such information.

Employee Management and Training

The Southern University System Office of Human Resources performs references and/or background checks (as appropriate, depending on position) of new employees and those working in areas that regularly work with covered data and information (e.g. Cashier's Office, Financial Aid). During employee orientation, each new employee in these departments receives proper training on the importance of confidentiality of student (customer) records, student (customer) financial information, and all other covered data and information. Each new employee is also trained in the proper use of computer information and passwords. Training includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, as well as how to properly dispose of documents that contain covered data and information. These training efforts should help minimize risk and safeguard covered data and information.

Physical Security

The Southern University System 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, financial aid applications, income and credit histories, accounts, balances and transactional information are available only to Southern University System 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.

All servers and data storage systems are physically secured behind a card access system and mechanical cypher lock with limited access.

Information Systems

Access to covered data and information via the Southern University System's computer information system is limited to those employees who have a legitimate business reason to access such information. The organization has policies and procedures in place to complement the physical and technical (IT) safeguards in order to provide security to

Southern University System's information systems. These policies and procedures are available upon request from the Information Security Officer.

Social security numbers are considered protected information under both GLBA and the Family Educational Rights and Privacy Act (FERPA). As such, the Southern University System does not use social security numbers as student identifiers in favor of the Student-ID# as a matter of policy. By necessity, student social security numbers will remain in the student information system; however, access to social security numbers is granted only in cases where there is an approved, documented business need.

Management of System Failures

The Division of Information Technology has developed written plans and procedures to detect any actual or attempted attacks on Southern University systems and has an Incident Response Plan formulated in coordination with the Deputy CIO of Security & Risk Management, which outlines procedures for responding to an actual or attempted unauthorized access to covered data and information. This document is available upon request from the Information Security Officer or the Division of Information Technology.

Oversight of Service Providers

GLBA requires the organization to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. This Information Security Program will ensure that such steps are taken by contractually requiring service providers to implement and maintain such safeguards. The Information Security Program Coordinator(s) will identify service providers who have or will have access to covered data, and will work with financial affairs office and legal counsel, and other offices as appropriate, to ensure that service provider contracts contain appropriate terms to protect the security of covered data.

Continuing Evaluation and Adjustment

This Information Security Program will be subject to periodic review and adjustment as needed. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the designated Information Security Program Coordinator(s), who will assign specific responsibility for technical (IT), logical, physical, and administrative safeguards implementation and administration as appropriate. The Information Security Program Coordinator(s) will review the standards set forth in this program and recommend updates and revisions as necessary; it may be necessary to adjust the program to reflect changes in technology, the sensitivity of student/customer data, and/or internal or external threats to information security.

VI. POLICY RELATED INFORMATION

- Southern University System Cybersecurity Policy
- Southern University System IT Incident Handling Procedure

- Family Educational Rights and Privacy Act (FERPA)
- Gramm Leach Bliley Act (GLBA)
- Louisiana House Bill No.633 Act No.155
- Payment Card Industry Data Security Standard (PCI-DSS)
- Southern University System Acceptable Use of Technology Resources
- Southern University System Email Communications Policy
- Southern University System Personal Computing Policy
- All other applicable Southern University System Polices

VII. POLICY HISTORY AND REVIEW CYCLE

This is a new policy. The effective date of this policy is determined by the approval dates of both the Chair of the Southern University System Board of Supervisors and the President-Chancellor of the Southern University and A&M College System. Additionally, the policy last review and origination dates are identified. This policy is subject to a five-year policy review cycle.

VIII. POLICY URL

The approved policy will be posted on the Southern University System website under Board Policies at *www.sus.edu.*

IX. POLICY APPROVAL

Ray L. Belton

Ray L. Belton, Ph.D.
President-Chancellor, Southern University and A&M College System

Effective Date of Policy

The Honorable Attorney Domoine D. Rutledge
Chair - Southern University System Board of Supervisors

Effective Date of Policy