Gramm-Leach-Bliley Act Information Security Plan
Florida National University

This Information Security Plan ("Plan") describes Florida National University's plan to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of non-public, personally identifiable information that the University handles or maintains about an individual in the process of offering a financial product or service ("Protected Information"), and to implement reasonable administrative, technical, and physical safeguards to control these risks, pursuant to the Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley ("GLB") Act, 15 U.S.C. Section 6801. These safeguards are intended to:

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

This Information Security Plan also provides mechanisms to:

- Identify and assess the risks that may result in the unauthorized disclosure, misuse, alteration, destruction or other compromises of Protected Information maintained by Florida National University;
- Design and implement a safeguards program to control these risks;
- Designate an employee(s) responsible for coordinating the program;
- Manage the selection of appropriate service providers; and
- Adjust the plan to reflect changes in technology, the sensitivity of Protected Information, and internal or external threats to information security.

When assessing risks and implementing safeguards on an initial and ongoing basis, particular attention is paid to information provided to the University by the U.S. Department of Education or otherwise obtained in support of the administration of the federal student financial assistance programs.

For additional information, please see the University's Privacy Statement (available at: https://www.fnu.edu/privacy-statement/) and Acceptable Use Policy Regarding Information Technology (available at: http://www.fnu.edu/Publications/FNU_Computer_Use_Policy.htm).

Identification and Assessment of Risks to Customer Information

Florida National University recognizes that it is exposed to both internal and external risks. These risks include, but are not limited to:

- Unauthorized access of Protected 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; and
- Unauthorized transfer of covered data and information through third parties.

Since technology growth is not static, new risks may be created regularly. Accordingly, the Coordinators (listed below) will actively work with and seek advice from University administration regarding the identification of new and evolving areas of risk. Florida National University believes the safeguards currently in place are reasonable and, in light of current risk assessments, are sufficient to provide security and confidentiality to Protected Information maintained by the University. Additionally, these safeguards reasonably protect against currently anticipated threats or hazards to the integrity of such information.

Information Security Plan Coordinators

Each Campus Dean is responsible for the overall maintenance of information security and privacy and the coordination of the University's information security program at their campus, and the System Administrator is responsible for coordination relating to the University's information technology systems. The Campus Deans and System Administrator are referred to in this plan as "Coordinators." Each department responsible for handling Protected Information will provide an annual update report to the appropriate Coordinator indicating the status of its safeguarding procedures. The Coordinators have overall responsibility for assessing the risks associated with unauthorized transfers of Protected Information and implementing procedures to minimize those risks that are appropriate based upon the University's size, complexity, and the nature and scope of its activities.

Design and Implementation of Safeguards Program

Employee Management and Training

In accordance with University policies, standards, and guidelines, reference checking and background reviews for new employees will be conducted when deemed appropriate depending on the position. During the employee orientation process, each new employee in departments that handle Protected Information will receive proper training, as appropriate for their role and responsibilities, on the University's policies and procedures for, and the importance of, maintaining the confidentiality of Protected Information. Each new employee will also be trained in the proper use of computer information and passwords relevant to their job functions. Further, in conjunction with the Coordinators, each department responsible for maintaining Protected Information will provide ongoing updates to its staff regarding any known new or heightened security risks. These training efforts are intended to help minimize risk and safeguard covered data and information security.

Physical Security

Florida National University has addressed the physical security of Protected Information by limiting access to only those employees who have a legitimate business reason to handle such information. All university employees are instructed to promptly report the loss or theft of Protected Information to the appropriate Coordinator. Offices and storage facilities that maintain Protected Information limit customer access and are appropriately secured.
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

Information systems include network equipment, hardware and software, as well as information processing, storage, transmission, retrieval, and disposal systems. Access to Protected Information via FNU's computer information systems is limited to those employees who have a legitimate business reason to access such information.

The University has policies, standards, and guidelines governing the use of electronic resources, as well as firewall and wireless policies. Florida National University will take reasonable and appropriate steps consistent with current technological developments to make sure that all Protected Information is secure and to safeguard the integrity of records in storage and transmission.

Social security numbers are considered Protected Information, and FNU has discontinued the use of social security numbers as student identifiers in favor of institution-issued identifiers. By necessity, student social security numbers will remain in the University's data systems, but access to social security numbers is restricted to those employees with a legitimate need for the information.

Detection and Prevention of Attacks, Intrusions and System Failures

The University will maintain effective systems to prevent, detect, and respond to attacks, intrusions and other system failures. Such systems may include maintaining and implementing current anti-virus software; checking with software vendors and others to regularly obtain and install patches to correct software vulnerabilities; maintaining appropriate filtering or firewall technologies; alerting those with access to covered data of threats to security; imaging documents and shredding paper copies; backing up data regularly and storing back-up information off-site, as well as other reasonable measures to protect the integrity and safety of information systems.

<u>Selection of Appropriate Service Providers</u>

The University will select appropriate service providers that are given access to Protected Information in the normal course of business and will contract with them to provide adequate safeguards. The University's process of choosing a service provider that will have access to Protected Information includes consideration of such provider's capability to maintain appropriate safeguards for such Protected Information. Contracts with service providers shall include appropriate provisions, such as a stipulation that the Protected Information will be held in confidence and accessed only for the purpose(s) specified in the contract, and an assurance from the contract partner that the partner will protect the Protected Information it receives.

Continuing Evaluation and Adjustment

This Information Security Plan will be subject to periodic review and adjustment, especially due to changing technology and evolving risks. The Coordinators, in consultation with University leadership, will review the standards set forth in this plan and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in the University's operations, technology, the sensitivity of student/customer data, and other circumstances that may have a material impact on information security.

Last Updated: April 2020