FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Gramm-Leach-Bliley Act: Safeguards to Protect Confidential Financial Information # 1930.015

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
June 12, 2006	June 2, 2021	Division of Information Technology/IT Security Office

POLICY STATEMENT

The University shall implement and maintain a written information security program that establishes the appropriate administrative, technical and physical safeguards the University has put in place in order to safeguard the privacy of customers' personally identifiable confidential financial information (hereinafter "Confidential Financial Information" or "CFI") as required by the Gramm-Leach-Bliley Act.

SCOPE

This policy applies to any recorded containing nonpublic financial information about a student or other third party who has a relationship with Florida International University, whether in paper, electronic or other form, which is handled or maintained by or on behalf of Florida International University or its affiliates.

REASON FOR POLICY

The Gramm-Leach-Bliley Act ("GLB" or "Act") requires "financial institutions" to protect the privacy of their customers, including the customers' personally identifiable financial information. Though institutions of higher education are not "financial institutions," they deal with a variety of financial records from students and their parents. The Act requires FIU to develop, implement and maintain a written information security program establishing the administrative, technical and physical safeguards that FIU has, or will put in place, in order to safeguard its customers' information. This information security program is written in one or more readily accessible parts and addresses administrative, technical and physical safeguards.

DEFINITIONS

TERM	DEFINITIONS
Confidential Financial Information (CFI)	For purposes of this policy, means information the University obtains in the process of offering a financial product or service, such as processing of tuition payments, financial aid and a faculty or staff loan. In addition, CFI includes any credit card or bank

	account information received in the course of business by the University, regardless of whether the transaction is covered by GLB
Consumer	An individual who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family or household purposes, or that individual's legal representative. Example: applying for a loan.
Customer	A consumer who has a continuing relationship with a financial institution.
Information Security Program	Is the administrative, technical, or physical safeguards the institution uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.
Personally Identifiable Financial Information	Any information that a consumer provides to the financial institution in order to obtain a financial product or service or that the financial institution obtains about a consumer in connection with providing a financial product or service. This includes information provided during any financial transaction. Example: processing of tuition payments and financial aid.

ROLES AND RESPONSIBILITIES

Chief Information Security Officer: Overall responsibility of overseeing information security and is responsible for coordinating and overseeing the information security program.

GLB Group: Committee designated by the President's Staff, and led by the Chief Information Security Officer.

RELATED RESOURCES

FIU 108 – FIU Board of Trustees Access to Student Education Records Regulation. Establishes the University's obligation to not release or permit access to education records and personally identifiable information kept on a student except as otherwise permitted by law and this rule.

IT Security Office Website: https://security.fiu.edu

CONTACTS

Division of Information Technology
Information Security Office
11200 SW 8 ST, PC534A
Miami, FL 33199

305-348-1366
security@fiu.edu
https://security.fiu.edu

HISTORY

Initial Effective Date: June 12, 2006
Review Dates (*review performed, no updates*): N/A
Revision Dates (*updates made to document*): June 2, 2021

FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY PROCEDURE

Gramm-Leach-Bliley Act: Safeguards to Protect Confidential Financial Information # 1930.015a

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
June 12, 2006	June 2, 2021	Division of Information Technology/IT Security Office

POLICY STATEMENT

The University shall maintain a written Information Security Program (hereinafter "Program") which:

1. Ensures the security and confidentiality of Customer Information;
2. Protects against anticipated threats or hazards to the security or integrity of such information; and
3. Protects against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

The Program shall serve to:

1. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.
2. Develop any necessary employee education and training.
3. Review information systems capabilities including network and software design, as well as information processing, storage, transmission and disposal.
4. Review capabilities for detecting, preventing and responding to attacks, intrusions, or other systems failures.
5. Design and implement information safeguards to control the risks identified through the risk assessment process.
6. Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
7. Ensure that there is a process in place to: select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue, and requiring that these safeguards be implemented and maintained through the contracts with such service providers.

Continuously evaluate and adjust the Program as may be necessary in order to address: the results of the risk testing and monitoring or any material change in the operations or business arrangements of the institution.