

IMMACULATA GRAMM LEACH BLILEY ACT REQUIRED INFORMATION SECURITY POLICY

Effective Date:

- Authority** This Program was approved by the President of Immaculata University (hereinafter "IU").
- Policy Statement** The Gramm-Leach-Bliley Act ("GLBA") regulates the security and confidentiality of customer information collected or maintained by or on behalf of financial institutions or their affiliates. Because IU is classified as a "financial institution" under GLBA, by virtue of processing or servicing student loans, or offering other financial products or services, IU has established this IU GLBA Required Information Security Policy to ensure compliance with GLBA.
- Policy Purpose** This Policy reflects the intention of IU to implement an information security program ("Program") that (i) ensures the security and confidentiality of covered records, (ii) protects against any anticipated threats or hazards to the security of such records, and (iii) protects against the unauthorized access or use of such records or information in ways that could result in substantial harm to students, faculty and staff. This policy incorporates by reference any other IU policies and procedures that deal with obligations to maintain the security of confidential information or the implementation of security plans, such as the IU Administrative Data Security Plan and the IU Confidentiality of Student Records Plan.
- Summary** This Program outlines the responsibilities of the Program Officer and IU's commitment to maintaining physical, technical and administrative safeguards for Non-Public Customer Information.

Section headings are:

1. DESIGNATION OF REPRESENTATIVE
2. DEFINITIONS
3. ELEMENTS OF THE PROGRAM

I. DESIGNATION OF REPRESENTATIVE

Vice President for Finance and Administration is designated as the "**Program Officer**" who shall be responsible for coordinating the implementation of this policy, the IU Red Flag Rule Policy and the IU IT Security Incident Response Plan. The Program Officer may designate other representatives of IU to oversee and coordinate particular elements of the Policy.

II. DEFINITIONS

“Institutional Data” means any information relating to IU. This includes Non-Public Customer Information as defined below and any information that can be linked to any individual, including but not limited to, students, faculty, staff, patients or contractors.

“Non-Public Customer Information” means any information (i) a student or other third party provides in order to obtain a financial service from the University, (ii) about a student or other third party resulting from any transaction with IU involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person. Non-Public Customer Information may be in paper, electronic or other form.

III. ELEMENTS OF THE PROGRAM

A. Risk Identification and Assessment

IU shall undertake to identify and assess external and internal risks to the security, confidentiality, and integrity of Non-Public Customer Information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. The Program Officer will establish procedures for identifying and assessing such risks, including the evaluation of the effectiveness of IU’s procedures, policies and practices relating to access to and use of Non-Public Customer Information.

B. Information Systems and Information Processing and Disposal

The Program Officer will coordinate with representatives of IU and outside auditors to assess and monitor the risks of unintentional disclosure of Non-Public Customer Information arising from the IU’s information systems, including network and software design, information processing and the storage, transmission and disposal of Non-Public Customer Information.

C. Detecting, Preventing and Responding to Attacks

The Program Officer, in conjunction with the IU Incident Response Plan and the IU Red Flag Rules Program, will evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks.

D. Designing and Implementing Safeguards

The Program Officer will design and implement safeguards to control the risks identified through such assessments and to test or monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through

are in addition to the physical, technical and administrative safeguards outlined and mandated by the IU Administrative Data Security Policy.

1. Physical Safeguards

IU uses direct personal control or direct supervision to control access to and handling of all Non-Public Customer Information. Whether the information is stored in paper form or any electronically accessible format, Non-Public Customer Information is maintained, stored, transmitted and otherwise handled under the direct personal control of an authorized employee of IU.

Non-Public Customer Information is collected, processed, transmitted, distributed and ultimately disposed of with constant attention to its privacy and security. Conversations concerning Non-Public Customer Information are held in private. Papers with Non-Public Customer Information are mailed via official campus mail, U.S. mail, or private mail carrier. When best practices permit the disposal of Non-Public Customer Information, it is shredded or destroyed.

Confidential material is kept secure. Most offices have locked windows and locked doors with restricted access. For those that do not, materials are kept in locked filing cabinets or other locked storage areas. Non-Public Customer Information that is stored off campus by remote hosting and systems administrators is locked and secured by 24-hour security.

2. Technical Safeguards

The Office of Technology Services ("OTS") provides network security and administrative software password access security according to industry standards and pursuant to the IU Administrative Data Security Policy. All information, including Institutional Data and Non-Public Customer Information is stored on secured servers. In addition, Non-Public Customer Information is encrypted when transmitted electronically over networks or when stored online. Additional technical safeguards such as firewalls, anti-virus software and all applicable updates and patches are utilized to secure the IU network.

3. Administrative Safeguards

Pursuant to the IU Administrative Data Security Policy all IU employees, including part-time and temporary employees, are given specific training by their supervisors about issues of security of sensitive and confidential materials, including Non-Public Customer Information, used in their respective offices. Employees are held accountable to know that although they have access to Non-Public Customer Information in order to perform their duties for IU, they are not permitted to access or disclose such information to unauthorized persons. The Employee Handbook, which is provided to all employees, states that violation of

security policies could result in termination of employment or legal action, or both.

All outside service providers that work with IU are contractually obligated to maintain appropriate safeguards of Non-Public Customer Information and provide the same standards of information security followed by IU in handling such information. Contractual provisions with outside service providers govern the storage, disclosure and transmittal of all Non-Public Customer Information and Institutional Data. In addition, these contracts provide for the return or destruction of all Institutional Data received upon completion of the contract; allow for the entry of injunctive relief in order to prevent or remedy breach of confidentiality obligations of the contract; provide that any violation of the contract's protective conditions amounts to a material breach of the contract and entitles IU to immediately terminate the contract without penalty; provide for auditing of the service provider's compliance with the contract safeguard requirements; and ensure that the contract's protective requirements survive any termination agreement.

E. Overseeing Service Providers

The Program Officer is responsible for assuring that IU retains only those service providers that are capable of maintaining appropriate safeguards for Non-Public Customer Information of students and other third parties to which they will have access. IU, through the assistance of its legal counsel, will develop and incorporate standard, contractual protections applicable to third party service providers that will require such providers to implement and maintain appropriate safeguards. These standards shall apply to all existing and future contracts entered into with such third party service providers.

F. Employee Training and Management

The Program Officer shall designate other representatives of IU to provide training to employees regarding security initiatives to minimize the disclosure of Non-Public Customer Information.

G. Adjustments to Program

The Program Officer shall adjust IU's security initiatives based on the risk identification and assessment activities as well as any material changes to IU's operations or other circumstances that may have a material impact on IU's security initiatives.