# GLBA Information Security Program

This document outlines the University's **GLBA Information Security Program**.

Wayne State University is required by the Gramm-Leach-Bliley Act (GLBA) and its implementing regulation called the Safeguards Rule (the Rule) (16 CFR Part 314) to develop, implement, and maintain a comprehensive written Information Security Program (ISP) to safeguard customer information in the University's care.

The objectives of the ISP are:
1. To ensure the security and confidentiality of customer information;
2. To protect against anticipated threats or hazards to the security or integrity of such information; and
3. To protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to customers.

**Scope of Customer Information**

The ISP applies to any record containing nonpublic personal information (PII) in paper, electronic or other form about a student or other third party who has a continuing relationship with the University, where such information is obtained in connection with the provision of a financial service or product by the University, and that is maintained by the University or on the University's behalf.

Nonpublic personal information is information:

(i) A student or other third party provides in order to obtain a financial service or product from the University,
(ii) About a student or other third party resulting from any transaction with the University involving a financial service or product, or
(iii) Otherwise obtained about a student or other third party in connection with providing a financial service or product to that person.

For example, nonpublic personal information includes bank and credit card account numbers, income and credit histories as well as names, address and social security numbers associated with financial information. Customer information does not include records obtained in connection with single or isolated financial transactions such as ATM transactions or credit card purchases.

**Related Policies and Programs**

The University has adopted comprehensive policies and practices to protect the privacy and security of information in its care. The policies enumerated below, and other institutional policies and practices that may be required under federal and state laws and regulations must be followed.

- Family Educational Rights and Privacy Act Policies
- Confidential Information Policy
- Acceptable Use of Information Technology Resources Policy
- Data Governance Policies
- Information Security Policy and/or standards

**Elements of the Wayne State University Information Security Program**

*1. Information Security Program Coordinator(s)*

The University has designated the Chief Information Officer (CIO) or as its ISP Coordinator (Coordinator). The Coordinator may designate others to oversee particular elements of the ISP. Questions regarding the ISP should be directed to the CIO or the CIO's designees.

*2. Risk Identification and Assessment.*

Each school, college or division should identify and assess reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. Further, each unit should assess the sufficiency of any safeguards in place to control these risks. This applies to information in any format, whether electronic, paper, or other form.

The website maintained by the Information Security Office offers guidance materials to help managers evaluate current data protection practices and assess reasonably anticipated risks in day-to-day operations including:

- *Employee training and management*: evaluate the effectiveness of current employee training and management procedures relating to the access and use of covered records.

- *Information Systems, Information Processing and Disposal* : assess the risks to covered information associated with the University's information systems, including network and software design, as well as information processing, storage, transmission, and disposal.

- *Detecting, Preventing and Responding to Attacks and System Failures*: evaluate procedures for and methods of detecting, preventing and responding to attacks, intrusions or other system failures.

*3. Designing and Implementing Safeguards*.
Each school, college or division with customer data must design and implement safeguards to control the risks identified in assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Testing and monitoring may be accomplished through existing network monitoring, problem escalation procedures and other data management practices. The Information Security Office can be consulted at any time for help with the design and implementation of safeguards and/or determining what University wide safeguards may be leveraged.

*4. Overseeing Service Providers*.
Each school, college or division with customer data is responsible for ensuring external service providers maintain appropriate safeguards. University policies for technology purchases, including cloud and other service providers, should be followed to allow for review of any contractual documents by the information security office and Office of General Counsel.

*5. Annual review*
Each school, college or division is required to perform an annual review of all controls, including review of external

service providers by updating the GLBA Compliance template and providing a copy to the ISP Coordinator or designee.

**6. Adjustments to Program.**

The Coordinator will evaluate and adjust the ISP as needed, based on risk identification and assessment activities and when material changes to the University's operations or other circumstances may have a material impact on the ISP.