LONG ISLAND UNIVERSITY

INFORMATION SECURITY POLICY- GRAMM-LEACH-BLILEY ACT (GLBA)

PURPOSE

This policy sets forth parameters and protocols for the University's compliance with the Gramm-Leach-Bliley Act (GLBA).

The GLBA Safeguards Rule addresses the safeguarding and confidentiality of customer information held in the possession of financial institutions such as banks and investment companies. GLBA does not contain an exemption for colleges or universities; therefore, education entities that engage in financial activities, such as processing student loans, are required to comply.

Therefore, the University has adopted an Information Security Program (ISP) for certain critical and private financial and related information. This program applies to customer financial information (covered data) the University receives in the course of business as required by GLBA and other confidential financial information included within its scope.

Compliance with GLBA is based on the following objectives:

- Ensuring the security and confidentiality of customer information;
- Protecting against threats to the security or integrity of such information; and
- Guarding against unauthorized access to or use of such information.

STATEMENT OF POLICY

Key Elements of ISP

The University's ISP is coordinated by the Office of Information Technology. Key elements of the ISP include the following:

- **Appointment of a qualified individual as coordinator:** The University shall designate a specific, qualified individual to coordinate the GLBA ISP.

- **Written risk assessment:** At least annually, the GLBA ISP Coordinator shall prepare a written report, identifying reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of covered data that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, along with the sufficiency of any safeguards in place to control these risks.

- **Safeguards to protect against risks identified in the risk assessment:** The GLBA ISP Coordinator shall work with heads of units to oversee their individual safeguarding programs. Specific safeguarding practices include, but are not limited to, the following:

    - Conducting periodic inventory of where covered data is collected, stored, and transmitted and designing safeguards to respond accordingly, including periodic review of access controls.
    - Establishing access controls that limit access only to authorized users and only to the information needed to perform their duties and functions;
    - Maintaining a written Records Retention Policy that outlines the secure disposal of data no longer needed to conduct business;
    - Maintaining user and activities logs through security information and event management platforms, and monitoring for unauthorized access.
    - Logging and monitoring to detect unauthorized access or use of, or tampering with, information.
    - Maintaining physical security by locking rooms and file cabinets where customer and sensitive information is stored.
    - Maintaining and reviewing adequate key control and limiting access to sensitive areas to those individuals with appropriate clearance who require access to those areas as a result of their job.
    - Using and frequently changing passwords to access automated systems that process sensitive information, requiring multi-factor authentication for access to systems, and requiring identification before processing in-person transactions.
    - Using firewalls and encrypting information when feasible and using authentication and passwords when creating new accounts.
    - Ensuring that agreements with third-party contractors contain safeguarding provisions and monitoring those agreements to oversee compliance. Periodically reviewing changes in vendor applications to ensure continued safeguards are still in place.
    - Discouraging the use of social security numbers where feasible and using social security numbers only in accordance with university policy.

- **Testing:** The University shall continually monitor systems for potential penetration and periodically conduct penetration testing and publicly-known security vulnerabilities scans in the event of a material change to operations or systems.

- **Training**: The University shall ensure all new and existing employees who are involved in activities covered under this plan receive safeguarding and compliance training.

- **Vendor selection:** The University shall select service providers, that are given access to covered data in the normal course of business, that have the skills and experience to maintain appropriate safeguards. Agreements shall include security expectations and service providers' work shall be monitored and periodically assessed for suitability.

- **ISP maintenance:** The University shall review and periodically update the ISP through the Office of the Chief Information Officer (CIO), the Office of University Counsel, and representatives from Finance, Enrollment Services, Financial Aid, Admissions, Human Resources and Risk Management.

- **Written incident response plan:** The University's ISP shall include a written incident response plan that will be held in the office of the CIO.

- **Reporting to the Board of Trustees:** The University's ISP shall periodically be reported to the University's Board of Trustees.

Definitions

Covered data under the plan is defined by three categories:

- **Personal Identifiable Information** (**PII**) – Also known as non-public personal information or protected data, PII includes social security numbers, academic performance record, physical description, medical history, disciplinary history, gender, and ethnicity.

- **Financial Information** – Information that the University has obtained from faculty, staff, students, alumni, auxiliary services and patrons in the process of offering financial aid or conducting a program. Examples include direct deposit banking information, making, servicing, and collecting loans, including payment plans, income, and credit histories.

- **Student Financial Information** – Information that the University has obtained from a student in the process of offering a financial product or service, or such information provided to the University by another financial institution. Examples include student loans, income tax information received from a student's parent when offering a financial aid package (FAFSA), bank and credit card account numbers, and income and credit histories.

POLICY TYPE: OPERATIONS