LONG ISLAND UNIVERSITY

INFORMATION SECURITY RISK ASSESSMENT POLICY

PURPOSE

To assess and manage University information security risks that result from threats to the confidentiality, integrity and availability of University data and information systems.

The purpose of this policy is to facilitate compliance with applicable federal and state laws and regulations, protect the confidentiality and integrity of the University's Information Technology resources, and enable informed decisions regarding Risk Management.

Applicable regulations include the Family Educational Rights and Privacy Act ("FERPA"), Gramm–Leach–Bliley Act ("GLBA"), Health Insurance Portability and Accountability Act ("HIPAA")) and other relevant regulations.

STATEMENT OF POLICY

Data responsibility in the age of information systems is shared between data custodians and Information Technology. At every level of the institution, all LIU employees are considered data custodians. The University completes an information security risk assessment used to identify potential threats to information systems and data and analyze the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction if a threat were to be realized. Specifically, the risk assessment aims to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of student financial information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information.

Long Island University manages four types of data classifications:

1. Restricted/Confidential Data: Potential significant level of risk based on government, compliance, litigation. Examples: HIPAA; FERPA, PCI-DSS; U.S. Export Controlled information (some programs are not allowed to be taught to international students from specific countries); Gramm-Leach-Bliley, etc. (restricted)
2. Intellectual Property: Potential moderate level of risk. The result of university, staff and faculty research and innovation. (restricted)
3. Private Data: Potential moderate level of risk. Any data not classified as restricted or public data. Example: home address, ethnicity, salary information. Private data can cross over into restricted/confidential data classification when it becomes identifiable to a specific person. (restricted)
4. Public Data: Potential little or no risk. Examples: press release, course information, research publication. (non-restricted)

In accordance with GLBA regulation 314.4(b), the University documents its risk assessment to ensure the following are addressed:

(i) Criteria for the evaluation and categorization of identified security risks or threats considered;
(ii) Criteria for the assessment of the confidentiality, integrity, and availability of information systems and student information, including the adequacy of the existing controls in the context of the identified risks or threats faced; and
(iii) Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.

Information systems containing privileged and/or confidential data must be assessed for risk to the University that results from threats to the integrity, availability, and confidentiality of LIU data. Evaluations and Assessments should be completed prior to purchase of, or significant changes to, an Information System; and periodically for systems that store, process, or transmit Restricted Data. Restricted data includes data in any format collected, developed, maintained or managed by or on behalf of the University, or within the scope of University activities that are subject to specific protections under federal or state law or regulations or under applicable contracts. Examples include, but are not limited to, social security numbers, credit card numbers, certain student records, and research protocols.

- The University's Enterprise Risk Management (ERM) Team is responsible for the overall business classifications of data risks. The ERM Team must identify, quantify, and prioritize risk acceptance and objectives relevant to the University. The results are to guide and determine the appropriate management action and priorities for managing information security risks and for implementing Controls to protect against these risks.
- The Chief Information Officer (or designee) is authorized by the ERM to perform periodic information security risk assessments to determine vulnerabilities and initiate appropriate remediation.
- The University, with the guidance of the ERM, implements formal Information Security Risk Management (ISRM) programs that identify risks as well as plans to address and manage them.
- The Information Security Officer manages the ISRM program and coordinates the development and maintenance of program policies, procedures, standards, and reports, in coordination with ERM governance.
- Reports are published about the ISRM findings and presented to the ERM Team for determining risk remediation.

POLICY TYPE: OPERATIONS