I. Purpose

In order to protect customers' (as defined below) nonpublic personal financial information (as defined below) from disclosure and to comply with federal regulations mandated by the Gramm-Leach-Bliley Act (the "Act") and the Federal Trade Commission's *Standards for Safeguarding Customer Information* (the "Standards"), the University must establish and maintain a comprehensive information security program. This Policy describes the University's program for implementing the requirements of the Act and the Standards so as to meet the following objectives:

1. Ensure the security and confidentiality of customers' nonpublic personal financial information records;
2. Protect against any anticipated threats or hazards to the security or integrity of such records; and
3. Protect against the unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to customers.

II. Policy

It is the policy of IIT to manage nonpublic personal financial information collected from customers as confidential records. IIT has developed and will continue to develop appropriate procedures to protect such financial information against reasonable threats and hazards and unauthorized access or use of such records that could result in substantial harm or inconvenience to customers.

The University Bursar is IIT's Information Security Program Officer (the "Program Officer"). The Program Officer, in consultation and coordination with the Directors of Financial Aid, Chief Information Officer and Controller, is responsible for overseeing the implementation of IIT's Information Security Program, as set forth in this Policy (the "Program") and for ensuring the overall security of electronic systems and infrastructure for the University, including undertaking risk assessment, security awareness, data security, threat detection and monitoring and controlling systems activities that are reasonable given the size and complexity of the University, the nature and scope of its activities and the sensitivity of the nonpublic personal financial information at issue. The Program Officer may designate, as necessary, other representatives of the University to oversee and coordinate additional elements of the Program.

III. Definitions

"Customer" means students, parents or other third parties who have disclosed nonpublic personal financial information when applying for and/or obtaining from IIT a financial service or product, including, but not limited to, the application and administration of student loans, scholarships and grants, the payment of tuition and fees or processing of tuition deferment agreements, the admission application process, collection activities and employee background checks.

"Nonpublic Personal Financial Information" means any paper or electronic record containing nonpublic personal financial information provided by students or others in order to obtain a financial product or service from the University, including, without limitation, loan applications, bank and credit card numbers, account histories, Social Security numbers, income tax returns, credit reports and other related customer information.

IV. No Third Party Rights

While this Policy is intended to promote the security of information, it does not create any consumer, customer or other third-party rights or remedies or establish or increase any standards of care that would otherwise not be applicable.

V. Procedures

A. General

Consistent with the Act and the Standards, all Offices of Financial Aid, the Office of the Bursar and any other department that collects nonpublic personal financial information must, at reasonable intervals, evaluate and update their risk assessment and related information safeguards in light of testing and monitoring results, material changes to their operations or any other known circumstance that may have a material impact on the security of nonpublic personal financial information. .

B. Securing Information

Departments should periodically assess the safeguards they have in place to protect not only nonpublic personal financial information, but also all confidential University data. Specific safeguarding practices that departments must assess, and if necessary, implement and include in employee training, include:

1. Maintaining physical security by locking rooms and file cabinets where nonpublic personal financial information and other sensitive information is stored or electronic storage is housed. Procedures should include ensuring that windows and doors are locked when areas are unoccupied and restricting access to areas where sensitive data exists.

2. Maintaining adequate key control and limiting access to sensitive areas to those individuals with appropriate clearance which require access to the area to carry out their assigned job duties.

3. Using authentication processes (such as secure passwords) and granting access privileges only to authorized personnel with legitimate business need to authorize and enforce a user's access to and actions towards specified resources.

4. Using firewalls and encrypting information when feasible.

5. Referring calls and mail requesting customer information to those individuals who have been trained in safeguarding information.

6. Shredding and erasing customer information when they no longer need to be maintained under IIT's *Record and E-mail Retention Policy* (Procedure No. Q.4).

7. Encouraging employees to report suspicious activity to supervisors.

8. Ensuring that agreements with third-party contractors who have access to nonpublic personal financial information collected by the University contain safeguarding provisions and monitoring those agreements to oversee compliance with the privacy and safeguarding provisions of the Act and the Standards.

9. Ensuring that electronic hardware, electronic operating systems, software upgrades and other electronic means of storing and manipulating data are installed and configured to maintain adequate security of nonpublic personal financial information.

C. Training

Departments that collect nonpublic personal financial information should ensure that all new and existing employees who are involved in activities covered under the Act and the Standards receive periodic safeguarding training. Training should, at a minimum, encompass the nine "Securing Information" items listed above in Section
B. The Program Officer should establish a training program and designate person(s) to conduct training sessions.

D. Monitoring and Detection

Department heads and responsible departmental personnel, in consultation with the Office of Technology Services, must on an on-going basis periodically assess the vulnerabilities of their electronic as well as paper-based systems and propose improvements as needed.

E. Managing System Failures

If despite the reasonable precautions taken to secure and protect University systems and data a security breach occurs, immediate steps should be taken to correct such breach. Anyone who has reason to suspect a deliberate or significant

breach of established security policy or procedure should promptly report it to their supervisor and the Program Officer. Affected customers may also need to be notified after the department consults with the appropriate areas within the University. Examples of significant failures would include a successful hacking effort, a burglary or impersonations leading to the defrauding of customers.

VI. Related Policies

The University is deemed to be in compliance with the privacy provisions of the Act and the Standards because it complies with the Family Educational Records and Privacy Act ("FERPA"). See https://www.iit.edu/registrar/students-and-alumni/ferpa for information on IIT's FERPA obligations. As with student records under FERPA, nonpublic personal financial information should not be released to outside parties, except in the following circumstances:

1. When a customer makes a written request for such disclosure
2. In furtherance of a transaction or services requested by the student;
3. As permitted or required by law or court order; or
4. To authorized third-party affiliates of IIT, but only to the extent necessary to further the transaction or service, such as a collection agency, credit bureau, loan processor or background checking entity.

In addition, the following Policies and laws supplement and help to create a comprehensive information security plan are incorporated by reference into the Program:

- Use of Computer Resources (Procedure No. Q.3)
- Records and E-Mail Retention Policy (Procedure No. Q.4)
- Illinois Personal Information Protection Act (815 ILCS 530/1 et seq.)
- Family Educational Records and Privacy Act (20 U.S.C. 1232g)