Gramm-Leach-Bliley Information Security Plan
For Indiana University of Pennsylvania

Gramm-Leach-Bliley Act (FTC)

A. The Program Officer for the coordination and execution of the information security plan will be designated by the President. The designated Program Officer is the Associate Vice President for Finance of Indiana University of Pennsylvania. All correspondence and inquiries should be directed to the Program Officer.

B. This plan is applicable to any employee or affiliate of the university with access to customer financial information as defined by the Federal Trade Commission. Customer information is defined as non-public, personally identifiable information that the University handles or maintains about an individual in the process of offering a financial product or service, or such information provided to the University by a financial institution. Such customer information is covered whether it is in paper, electronic, or other form. Examples of customer information include bank and credit card information, tax, income, and credit histories, addresses, phone numbers, and social security numbers. The following have been identified as the most relevant areas to be considered when assessing the risks to customer information:

1. Admissions Offices (Undergraduate, Graduate, Continuing Education and Distance Education)
2. Alumni Relations
3. Athletics
4. Bursar
5. Financial Aid
6. Human Resources
7. Institutional Research
8. Internal Review
9. Office of Housing and Residence Life
10. Office of the Registrar
11. Purchasing Services
12. Student ID Card Office
13. Student Health Services
14. Information Technology Services

C. The Program Officer will work with the university community to implement all aspects of the Gramm-Leach-Bliley Information Security Plan. Each relevant area is responsible to secure customer information in accordance with the University's Information Protection Policy. The Program Officer will work with associated division Vice Presidents and department directors to develop and maintain information protection procedures for all University and University-related information systems. In addition, consistent with the University's Information Assurance Guidelines, all Information Technology units (Information Technology Services, Colleges Technology Managers and Affiliates) will implement and maintain procedures that protect against any anticipated threats to the security

or integrity of central electronic customer information and that guard against the unauthorized use of such information.

D. Indiana University of Pennsylvania will select appropriate service providers that are given access to customer information in the normal course of business and will contract with them to provide adequate safeguards. In the process of choosing a service provider that will have access to customer information, the evaluation process shall include the ability of the service provider to safeguard customer information. Contracts with service providers shall include the following provisions:

    1. An explicit acknowledgement that the contract allows the contract partner access to confidential information;
    2. A specific definition of the confidential information being provided; a stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract; a guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract; a guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information;
    3. A provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract;
    4. A stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract;
    5. A stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles Indiana University of Pennsylvania to immediately terminate the contract without penalty;
    6. A provision allowing auditing of the contract partners' compliance with the contract safeguard requirements; and
    7. A provision ensuring that the contract's protective requirements shall survive any termination agreement.

E. This information security plan shall be evaluated and adjusted in light of relevant circumstances, including changes in the University's business arrangements or operations, or as a result of testing and monitoring the safeguards. Periodic auditing of each relevant area's compliance shall be coordinated through the Program Officer and the internal auditor's office. Annual risk assessment will be done through the Program Officer and division Vice Presidents and associated department directors.