INDIANA UNIVERSITY OF PENNSYLVANIA

INFORMATION PROTECTION POLICY

December 1, 2005

Approved for implementation by Dr. Tony Atwater and President's Cabinet
October 31, 2005

POLICY STATEMENT

Subject: Information Protection Policy

Date: 12-DEC-1994
Revision Date: 31-OCT-2005

Distribution Code: A

Reference Number:

Addition X
Deletion ____
New Item ____

Originating Office: ACOC
Administrative Computing
Oversight Committee

President's Approval [redacted] 12/1/05

1. PURPOSE:

To develop among the University community an appreciation for the value, and often vulnerable nature, of information, and to reduce the danger of misuse, destruction, or loss of information especially that of a critical or confidential nature, without restricting academic freedom or complicating access to information to which the University community has a legitimate and specific need.

2. SCOPE:

This policy applies to all employees and affiliates of the University.

3. OBJECTIVE:

The objective of this policy is to establish a framework for the use, access, and maintenance of information.

4. POLICY:

It is the policy of Indiana University of Pennsylvania that all information be used in a manner that maintains an appropriate and relevant level of confidentiality and that provides sufficient assurance of its integrity in compliance with existing laws and PASSHE and University Policies. [Examples would include (but are not limited to) Copyright Law, US Code Title 18, the Family Educational Rights and Privacy Act of 1974 (FERPA), the Pennsylvania Library Theft law (Act 1982-95), and the Gramm-Leach-Bliley Act (GLBA)]. While the elimination of all risk is impossible, the goal of the policy is to minimize the possibility of information misuse, corruption, and loss through the adoption of reasonable procedures for the University community to follow. While this policy is especially pertinent to information stored electronically, it is also intended to guide users of all information, including what is stored in other formats such as paper, microform, and video, as well as the content of confidential meetings and conversations.

5. DEFINITIONS:

University community - All employees and affiliates of the University.

Information - Data, in all its forms, collected, maintained, accessed, modified, or synthesized by and for members of the University community. The various forms of data include but are not limited to computer files, paper files, books, microfilm and fiche, video, conversations and oral presentations, and pictures or images.

Public Information - Information to which the University community has unrestricted access and for which there are no requirements of confidentiality. The vast majority of information at the University is of a public nature, for example: telephone directories, calendars, schedules, library books in general circulation, most conversations and meetings, and information bulletins.

Restricted Information - Information which is sensitive and confidential in nature or legally constrained, and requires access only by that part of the University community with the specific need to do so. Restricted University information includes, for example, individual student class schedules, grades, bills, financial aid applications, health records, personally identifiable financial information, and confidential personnel actions, whether the information is in paper, electronic, micrographic, or conversational form.

6. RESPONSIBILITIES:

Access

1. Access to public information is limited only by such restrictions as circulation policies, copyright restrictions, license and contractual agreements, University policies (such as the Computer Software Policy), and procedures for use.

2. Restricted information may only be accessed by those authorized members of the University community with a specific and legitimate need to know. Legitimate access does not include the freedom to "fish" (out of curiosity or other motives) for information which is restricted, if it is not specifically required to perform a job-related task or legitimate research.

Use

1. Responsibility will vary from member to member of the University community, and each user will be accountable for appropriate use.

2. Each member of the University community is responsible for using information appropriately. Appropriate use is wise and prudent use of information so that information resources are not wasted, damaged, or misused. Inappropriate use includes releasing restricted information, erasing or modifying information without proper authorization, defacing or removing pages from books, using information to embarrass, intimidate, or harass, or attempting to subvert the flow of information, such as purposefully attempting to crash or slow down computer systems, modifying or removing posted information without authority, and other such actions.

7. PROCEDURES:

Maintenance

1. Each office responsible for University information shall identify the information it maintains, determine whether it is of a restricted nature, and implement reasonable and clear procedures for granting access only to employees with a legal, specific, and legitimate need to know. Employees must be aware of applicable restrictions on the use of information to which they have access. Specific offices with responsibility for the University's electronic data are listed on-line in the University's Administrative Computing Oversight Committee (ACOC) Web Site. Information on accessing this list may be obtained from the Technology Services Center.

2. Each member of the University community with access to restricted information is responsible for maintaining the confidentiality of that information whether it has been obtained or created through electronic, paper, or conversational means. Each such person will read and sign the IUP Confidentiality Statement. The Confidentiality Statement will be maintained in the employee's official personnel file in the Office of Human Resources. Maintenance of Confidentiality Statements for student employees will be maintained in Student Payroll. Each such person shall take appropriate action to ensure that the information is being used properly and appropriately. For example, confidential files should be locked

when not in use. Sensitive or confidential information should be destroyed when discarded. It is particularly important that passwords to computer accounts with access to restricted information not be shared.

3. Members of the University community charged with maintaining restricted information are responsible for maintaining the accuracy and integrity of that information and for determining who requires access to it. Critical information on the University and University-related information systems is automatically backed up on a regular basis to maintain its integrity and retrievability should it be accidentally or otherwise destroyed or lost. Individual users with critical information maintained locally, i.e., on a personal computer, on paper, or in other media, shall also take appropriate steps to ensure that valuable and confidential information not be lost, damaged, or otherwise compromised.

Oversight

The Administrative Computing Oversight Committee (ACOC) is responsible for the procedures and programs to support the Maintenance (Section 7) of the Information Protection Policy, including the creation and maintenance of any specific programs required by law [example, GLBA Safeguards Rule]. Copies of this policy and all associated procedures shall be maintained on the IUP Policy web site.

Questions regarding the applicability or violation of the policy, or appropriate access to information should be referred to the Chair of the Administrative Computing Oversight Committee (ACOC).

Violations of this policy will be reported to the Associate Vice President for Human Resources. Violations of the policy may result in disciplinary action up to and including separation from employment or expulsion from school in accordance with the student handbook, applicable collective bargaining agreements, and/or University and PASSHE personnel policies.

A violation of this agreement may result in criminal action if it is determined that any local, state, or federal law has been violated.

8. RECISION: Alumni/Development Information System Confidentiality Policy.

9. PUBLICATIONS STATEMENT:

This policy should be published in the following publications:

Administrative Manual

10. DISTRIBUTION:

Distribution Code	Description
A	All Employees