IUP Information Protection Procedures

A. Introduction

1. The IUP Information Protection Policy includes the following directive:

"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 Pennsylvania State System of Higher Education (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 [FERPA], the Pennsylvania Library Theft law [Act 1982-95], and the Gramm-Leach-Bliley Act [GLBA])."

2. The policy also details responsibilities for the access, use, and maintenance of restricted information and defines restricted information as follows:

"**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 information, health records, personally identifiable financial information, and confidential personnel actions, whether the information is in paper, electronic, micrographic, or conversational form."

3. There are a variety of potential internal and external risks related to the security, integrity, access, and use of restricted information. These potential risks include but are not limited to actions with:

(a) Physical or electronic access (storage, transmission, disposal)
(b) Physical loss due to disaster
(c) Compromised computer systems (including computer viruses)
(d) Lack of training and education of employees pertaining to protection policies that can lead to unauthorized use, disclosure, alteration or destruction of restricted information.

The IUP Information Protection Procedures defined herein are intended to support compliance with the Information Protection Policy and provide a framework that outlines procedures and controls to mitigate these risks.

BETBT1[illegible]ter

(b) Division Vice President access control procedures are as follows:

(1) For University and University-related information systems, division VPs will designate Security Officers who are responsible for defining and managing access to the information systems.

(2) For Administrative Network File Services, division VPs will designate Administrative Network User Group members who are responsible for defining and managing access to administrative network files services (O: Drive and any related shared drives such as the X: drive).

(3) Requests for access to information system must be submitted to the appropriate Security Officer. The Security Officer will work with Information Technology Services (IT Services) to add, change, or delete access for a given UserID.

(c) IT Services is responsible for managing the centralized University and University-related information systems and network file services. Any unit maintaining information systems and related services beyond the centralized scope is responsible for implementing data security and access controls consistent with these procedures and the IUP Information Assurance Guidelines

(d) All IUP computer systems are subject to the IUP Information Assurance Guidelines. Designated system administrators are responsible for full compliance with the guidelines including the provisions for the physical and logical

D. Non-Compliance

1. Questions regarding the applicability or violation of the policy, or appropriate access to information should be referred to the Information Protection Program Officer