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.

B. Procedures

1. Electronic Access and Security Controls

(a) University Systems --
All users of University administrative data must be authorized to access the appropriate systems. Electronic Access Control procedures are governed by the division Vice Presidents (VPs) and associated department directors. Copies of data, regardless of location, have the same data security and access control requirements as the original data.

(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 (authentication, secured hosts, virus scanning, active monitoring, backup/recovery) security management of each computer system.

(e) For information system and network access, users will be issued a unique UserID to be used for all system access. UserID and password will be required for all information and system network access.

2. Users are responsible for all activity occurring under their UserID –

   Users are responsible for maintaining the security of their UserIDs and passwords. UserIDs and passwords are not to be shared or posted. Passwords should be changed on a regular basis. Passwords should include a combination of letters and numbers.

3. External/Third Party Systems --

   All users of external/third party administrative data must be authorized to access the appropriate systems. Electronic access control procedures are governed by both the Service Provider and the IUP administrative office. Such information systems include but are not limited to the following: loan guaranty agencies, state grant and scholarship agencies, U.S. Veterans' Administration, Selective Service Administration, U.S. Department of Education and its affiliates, contractors, and subsidiaries, federal Perkins loan collection and servicing agencies, proprietary loan software and internet sites, and student employment online information. Copies of

data, regardless of location, have the same data security and access control requirements as the original data.

4. Access control procedures --

   (a) Requests for access to information systems must be submitted to the appropriate IUP administrative office director and through the external/third party security system.

   (b) Users will be issued a unique UserID to obtain access to information systems and networks of the specific external/third party system. Users are responsible for maintaining the security of their User IDs and passwords. Users are responsible for all activity occurring under their User ID. User IDs and passwords are not to be shared.

5. Physical Access Controls --

   Physical access to restricted information regardless of form (paper, CD/Disk/external drives, PCs/Laptops, portable devices/smartphones/etc.) must be restricted to authorized personnel. Unit heads are responsible for ensuring the physical security including provisions for:

   (a) Organization of work areas to minimize security risks of physical exposure to personally identifiable information, including storage in locked file cabinets, rooms, or vaults.

   (b) Restriction of the distribution of keys which provide entry to secure areas in compliance with the University's Key Acquisition and Control Procedures.

   (c) Proper disposal of all materials containing personally identifiable information. This includes shredding of documents and destruction of microfilms, electronic and voice media (including the secure format or physical destruction of hard drives transferred between units or sent to surplus).

   (d) Proper location of fax machines and printers which receive and print documents containing personally identifiable information.

   (e) Proper archiving and disposal of all customer and Univeristy banking related information. (i.e. lock box payments, deposits, credit card receipts, direct deposit requests, any personally identifiable payment related information)

   (f) Requirements to enter a valid UserID and Password to access PCs (log off of PCs when not in use, use password-protected screen savers)

6. Information Usage Controls

   (a) Personal Identification -- An alternate identifier is utilized for the majority of the university processes. Social Security numbers will be utilized only by areas of necessity such as Financial Aid, Registrar, Human Resources and

Institutional Research. In addition, Social Security numbers are not provided to any outside agency except to those contracted to provide services to areas mentioned above.

(b) Service Provider Access --

Service providers accessing University related data which may include personally identifiable information, will be required to ensure compliance with Gramm-Leach-Bliley Act.

(c) Internet Applications –

University web sites that collect restricted information must implement technical and functional procedures to safeguard the secure storage and transmission of all data consistent with federal, state, and financial industry security standards.

7. Requests for Information --

(a) In cases where confidential or restricted information is sought by internal or external individuals or agencies, a written request may be required and submitted to the director of the department or security officer for that area.

(b) Requests will be reviewed on a case-by-case basis and a decision will be made as to whether or not the information can be released to the requestor. In situations where access is granted, in no case does this permit re-release of the information to any other entity or third party.

(c) Requests for System reporting, information needed by the U.S. Department of Education, Pennsylvania Higher Education Assistance Agency and other governmental funding agencies are not subject to this review process.

C. Training and Education

1. University management is responsible for instituting safeguard procedures relative to their specific areas in compliance with the Information Protection Policy and Procedures, and for educating and training all associates working within their area.

2. The Information Protection Policy and Procedures will be publicized on all related university websites, with notices of the approved policies and procedures sent to all university employees and students. Training information will also be available in the form of a brochure and formal training sessions will be conducted as requested.

3. The Office of Human Resources will ensure that all employees, (current, new hires and student) are provided a copy of the training brochure. All employees, including students, must sign a confidentiality statement, indicating that they understand the privacy policy and the ramifications of violation of the policy. The statements will be maintained in the official personnel file for employees; the Student Payroll Office will maintain the statements for student workers.

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.

2. Violations of these procedural guidelines will be reported to the Associate Vice President for Human Resources and 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 agreement, and/or University and PASSHE personnel policies.

3. Violations may result in criminal action if it is determined that any local, state, or federal law has been violated.