Information Access Policy

I. Policy Statement
Information is a valuable asset of the University; we must provide appropriate access to information needed by students, faculty, and staff while protecting the privacy, confidentiality, and integrity of this University resource. Anyone with access to University information for the purpose of performing their work has a responsibility to protect that information.

II. Reason for Policy
This policy establishes the basic use and protection of all information, in any form, which is generated by, owned by or otherwise in the possession of the University, including all administrative and academic data (research data are excluded from this policy).
Note: Access to University systems or data is subject to all federal, state, local and University policy and regulations.

III. Entities Affected By This Policy
This policy applies to anyone who needs access to administrative or academic data, and is specifically enacted by data stewards and department heads.
This policy applies to:
- All data supporting the business and operational needs of the University
- Information and data in all forms including information kept on servers or personal workstations, manually maintained files, and mobile devices and removable media
- All application, network, and operating system software used for computerized management of this data

IV. Website Address for this Policy
http://www.scranton.edu/pir/policies.shtml

V. Related Documents, Forms, and Tools
Most policies and procedures in this section are located on the Information Resources Policy web site or the University of Scranton policy web site:

University of Scranton Information Management Model

Computer Security Incident Response Team (CSIRT) Operations Manual
IT Policy
Policy Name: Information Access Policy

Acceptable Use of Computing Resources Policy

Information Classification & Protection Policy

Records Management & Retention Policy

Information Resources Account Provisioning Procedures

Employee Separation Procedures: Information Resources

Family Educational Rights and Privacy Act (FERPA):

Health Insurance Portability and Accountability Act of 1996 (HIPAA):
http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

VI. Contacts
For policy clarification and interpretation contact the Information Security Office at 570-941-4226 or email security@scranton.edu

VII. Definitions
Data: Factual information including measurements, statements, and statistics

Information: Data that are organized in a meaningful manner

Access: Permission, privilege or ability to read, enter, update, manage or administer access to the University of Scranton’s information assets. Authorized by the data steward or department head, access is dependent upon the sensitivity of the data. “Sensitivity” is determined by the legal responsibility of the University and the specific job responsibilities of the individual(s) for whom access is requested. (see also the Information Classification & Protection Policy)

Data Steward: University officials or their designated representatives responsible for data handling practices in their divisions. Collectively, University data stewards form the Information Management Advisory Committee which is responsible for guiding the development and maintenance of policies and programs designed to establish standards for information management and to ensure the confidentiality, integrity, and availability of the University’s information assets.

Data User/Custodian: Any individual in possession of University data.

VIII. Responsibilities
Data custodianship is a shared responsibility to protect access to University data following the controls specified by the data stewards; non-university entities should be bound contractually to this same responsibility. More specific roles are described below.
IT Policy
Policy Name: Information Access Policy

Data User/Custodian:
- Accesses data as authorized by the appropriate department head or data steward
- Obtains appropriate authorization before disclosing University data
- Assures that proper physical and electronic safeguards are in place to protect data
- Complies with all applicable data access practices, standards, and guidelines as defined by data stewards
- Informs the department head or data steward when he/she no longer needs access to information or an element of data
- Reports suspected access breaches to the data in their custody (see Procedures for Improper Access or Use)

Data Provider:
- Accesses data, as authorized by the appropriate department head or data steward, when performing information-processing tasks in support of Data Users
- Obtains appropriate authorization before disclosing University data
- Assures that proper physical and electronic safeguards are in place to protect data

Data Steward:
- Determines the classification of the information
- Specifies access security requirements
- Determines and implements appropriate information security controls in collaboration with Information Resources
- Authorizes access to the information
- Reports suspected access breaches and works with Information Resources through the incident response process (refer to the CSIRT Operations Manual)

Planning & Information Resources Division (or IT Service Provider)
- Access data, as authorized by stewards, when performing the tasks necessary to assure its integrity and availability
- Implements data access security as specified by the data steward and relevant information policies
- Implements adequate controls to protect data from unauthorized access
- Assures that proper physical safeguards are in place to protect data
- Provides and supports the systems and application code required to meet steward specifications for maintenance and dissemination of data
- Monitors the effectiveness of physical, procedural, and data access controls against unauthorized attempts at intrusion
- Protects data from unauthorized destruction, modification, or access during the electronic or physical transfer of the data from one location to another
- Periodically assesses the global and functional area information access policies to ensure that they are current

Information Management Advisory Committee:
- Charged with stewardship of the University’s information
- Reviews and recommends policies and procedures relating to the use and access of University of Scranton information