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 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 whether kept on servers or personal workstations and manually maintained files
- All application, network, and operating system software used for computerized management of this data

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

V. Related Documents, Forms, and Tools
Information Management Model
Information Classification & Protection Policy
Computer Security Incident Response Team (CSIRT) Operations Manual
Code of Responsible Computing for Faculty and Staff
Records Management & Retention Policy
IT Policy
Policy Name: Information Access Policy

Employee Separation Procedures: Information Resources

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.

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
IT Policy

Policy Name: Information Access Policy

- 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
IT Policy
Policy Name: Information Access Policy

IX. Procedures

Account Creation
Faculty and staff receive access to services and information required to perform their roles by the following processes:

University employees with an active Human Resources record have the appropriate account(s) automatically created for them providing access to groupware products. Groupware products include but are not limited to e-mail, calendar, campus portal, Royal Drive, and courseware. Account information is communicated to employees by his/her immediate supervisor or by contacting the Technology Support Center. New employees should allow three days to receive an account.

Employees who need to access the corporate database and the Banner System, will be given a Banner account based on requests made by the divisional Banner User Coordinator or the Department Supervisor to the Technology Support Center. Each individual will receive a unique account. Accounts must not be shared. For a list of Banner Coordinators see: http://matrix.scranton.edu/pir/banner-support/support-contacts.shtml

Students receive access to services and information by the following processes:

When a student is accepted by the Undergraduate Admissions Office a portal account is created with limited access to relevant information, such as public information and their own Financial Aid information through self-service. They claim their account, set up challenge questions, and establish their account password. Once their deposit is entered into Banner to confirm their acceptance and the May 1 deposit date has passed, they gain access to all student services in the portal including e-mail, library, and other self-service.

Undergraduate transfer students and on-campus graduate students gain access to the campus portal services by claiming their account after their deposit is entered into Banner. Graduate students in online programs are considered confirmed at the time of their acceptance, so they have full portal access when they are accepted.

Student workers are also given an employee role in the my.scranton portal and are provided with Banner and Royal Drive accounts when requested by their supervisor.

Employee accounts are retired upon separation, refer to Employee Separation Procedures: Information Resources for more information. Student accounts are retired after graduation or after they are not enrolled for 2 consecutive semesters. See the Account & Data Policy (2004) for more information.

Improper Access or Use
Employees, contract employees, students, or other data users who intentionally and without proper authorization 1) access or disclose restricted or confidential University information or 2) modify or destroy University information, are in direct violation of the University of Scranton Information Access Policy. Such violations may lead to disciplinary action by the University up to
IT Policy
Policy Name: Information Access Policy

and including dismissal from the University. Under certain circumstances, such violations may give rise to legal actions.

All faculty, staff, and students shall immediately report inappropriate disclosure or suspected loss of Confidential or Restricted information to the Computer Security Incident Response Team (CSIRT) via abuse@scranton.edu or 570-941-4226.