I. Policy Statement
The University of Scranton is committed to protecting the confidentiality, integrity, and availability of its information and technology assets. The Information Security Office, in partnership with University Data Stewards, is authorized to develop, implement, and maintain an Information Security Program, including the establishment of Information Security Standards, consistent with applicable legal and regulatory requirements and industry best practice.

II. Reason for Policy
This policy is established to protect the assets and interests of the University and to ensure a coordinated approach to creating and maintaining a secure environment, protecting our information and technology resources. This policy also helps to fulfill the requirements of the Higher Education Opportunity Act (HEOA), Gramm-Leach-Bliley Act, HIPAA, PCI-DSS, PA BPINA, and Federal Trade Commission Red Flag rules.

Security controls enacted under this policy will be consistent with the framework published by the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) 27002. These security standards address various security requirements including risk assessment, the organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development, and maintenance, incident management, business continuity, and compliance.

III. Entities Affected By This Policy
This policy is intended to guide the work of the Information Security Office and Data Stewards in the development of an Information Security Program and to inform members of the campus community about the purpose and scope of the program. All individuals who utilize University information or technology systems are responsible for complying with the Information Security Program established under this policy.

IV. Website Address for this Policy
http://www.scranton.edu/pir/policies.shtml
V. Related Documents, Forms, and Tools

Please see the following documents located at http://www.scranton.edu/pir/policies.shtml:

- Information Management Model
- Information Classification & Protection Policy
- Information Access Policy
- Acceptable Use of Computing Resources Policy
- Incidental Use of Computing Resources Policy
- CSIRT Operations Manual

On the General Counsel Policy page http://www.scranton.edu/general-counsel/policies.shtml

- Copyright Policy
- Records Management and Retention Policy


VI. Contacts

For policy clarification and interpretation, please contact the Information Security Office at 570-941-4226 or email security@scranton.edu or the Associate Vice President Information Technology & CIO’s office at 570-941-5816.

VII. Definitions


University Standards: Required specifications, regulations, or rules. Outline minimal degree of compliance. Create consistency and uniformity of a process or activity. Differ from guidelines, which are recommended best practices.

University Information and Technology Assets: Includes, but is not limited to, University owned, operated, or maintained workstations, servers, printers, telephones; network switches, routers, wiring, and hubs; wireless and cellular components; mobile devices; software and data systems or devices that store, process, or transmit information or data; and data collected or generated for purposes of University operations.

VIII. Responsibilities

Information Security Office: Responsible for the development and maintenance of an Information Security Program. An Information Security Program addresses the identification of Data Stewards; a review of information-related risks; the development of technical, physical, and administrative safeguards for information, including the establishment of information security awareness and training activities, data handling and system configuration standards; and coordination of incident response to compromises or breaches of University information. The program development will be guided by this and other related Information Management & Security Policies noted in Section V. above.

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: Anyone using technology not provided by the University, such as handheld mobile devices or home computers, that interfaces with restricted or confidential University information must also ensure that their device(s) comply with the Information Security Program established under this policy.

IX. Procedures

1. The University Information Security Office will develop, implement, and maintain a University-wide Information Security Program. Elements of the Information Security Program and services offered by the Office will be published on the University Information Security Office website: http://www.scranton.edu/pir/information-security/

2. Each division head will identify a Data Steward(s) responsible for overseeing data handling practices in their division. These individuals will serve on the Information Management Advisory Committee and act as a point of contact for the Information Security Office as needed.

3. The Information Security Office will engage the PIR Division Leadership Group and Data Stewards, as necessary, in risk assessment to identify reasonable foreseeable risks to University data and recommend technical, physical, or administrative controls to mitigate these risks.

4. Information Security Standards developed as part of the Information Security Program will be reviewed by the appropriate Data Steward(s), the PIR Division Leadership Group, and approved by the Associate Vice President Information Technology & CIO.

5. Exceptions to the published Information Security Program requirements must be approved by the appropriate Data Steward if University data is involved. The exception must be documented in writing, acknowledging acceptance of responsibility by the department head and data steward for any risks to University data.

6. The Information Security Office will work with the Office of General Counsel to insure that in the review of contracts, reasonable steps are taken by service providers to maintain appropriate safeguards for University information.

7. The Information Security Office will work with IT Services and the IT Training Specialist to develop training and awareness materials and activities and disseminate them to the appropriate members of the University community.

8. The PIR Division utilizes technical controls to detect, prevent, and respond to attacks, intrusions, or other system failures. Any University information technology asset or personally owned technologies that pose a security threat may be disconnected from the University network or other systems. If a security breach is discovered in progress, immediate action, including but not limited to suspending access to University computing
and network resources, may be warranted pending further investigation if there is an imminent threat to University systems and data. Response to an information security breach is guided by the Computer Security Incident Response Team Operations Manual.

9. The Information Security Office, in collaboration with the PIR Division Leadership Group and Data Stewards, will regularly evaluate and review the controls implemented as part of the Information Security Program and will propose adjustments to the Program as needed.
Appendix A: Information Management Advisory Committee Charge and Membership (2014)

**Charge**
The Information Management Advisory Committee (IMAC) is charged with 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. Members will serve as data stewards for the area they represent. In this role, the group will:

- Guide the development of policies that preserve the security and privacy of data.
- Establish standards for data quality and consistent reporting, and monitor associated measures.
- Review and advise the records management program.
- Help to establish an environment where the University’s information assets can be used to improve operational efficiencies and enable business insight.

**Reporting Relationship**
Vice President for Planning & Chief Information Officer

**Membership**
Co-chairs: Helen Stager, Registrar  
Robyn Dickinson, Interim VP Planning & Chief Information Officer

Christian Kemmerer, Internal Auditor  
Nancy Dolan, Associate General Counsel  
Michael Knies, Library Special Collections  
Adam Edwards, Director Information Security

<table>
<thead>
<tr>
<th>Data Area</th>
<th>Steward</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student admissions</td>
<td>Mary Kay Aston, Asst. VP Admissions &amp; Enrollment</td>
</tr>
<tr>
<td>Student registration/Records</td>
<td>Lynn Pelick, Registrar’s Office</td>
</tr>
<tr>
<td>Student housing</td>
<td>Michelle Boughton, Asst. Director Housing</td>
</tr>
<tr>
<td>Student advising/Faculty data</td>
<td>Gina Butler, Asst. Dean CAS</td>
</tr>
<tr>
<td>Student advising/Faculty data</td>
<td>Meg Cullen-Brown, Asst. Dean CGCE</td>
</tr>
<tr>
<td>Student advising/Faculty data</td>
<td>Murli Rajan, PhD, Interim Associate Dean KSOM</td>
</tr>
<tr>
<td>Student advising/Faculty data</td>
<td>Victoria Castellanos, PhD, Associate Dean PCPS</td>
</tr>
<tr>
<td>CTLE Records</td>
<td>Eugeniu Grigorescu, Director</td>
</tr>
<tr>
<td>Health records</td>
<td>Pat Popeck, Director Wellness Center</td>
</tr>
<tr>
<td>Faculty/staff employment data</td>
<td>Patricia Tetreault, Interim Vice President Human Resources</td>
</tr>
<tr>
<td>Financial Aid</td>
<td>Margaret Hynosky, Assoc. Director Financial Aid</td>
</tr>
<tr>
<td>Finance data</td>
<td>Adrian Mihalko, Comptroller</td>
</tr>
<tr>
<td>Development/Alumni data</td>
<td>Carl O’Neil, Director of Development Operations</td>
</tr>
<tr>
<td>Institutional Research data</td>
<td>Valerie Taylor, Director of Institutional Research</td>
</tr>
<tr>
<td>Library records</td>
<td>Bonnie Strohl, Associate Dean</td>
</tr>
<tr>
<td>IT Applications</td>
<td>Connie Wisdo, Director of IT Development &amp; Applications</td>
</tr>
<tr>
<td>IT Infrastructure data/logs</td>
<td>Maureen Castaldi, Asst. Director Database Systems</td>
</tr>
<tr>
<td>Public Safety Records</td>
<td>TBD, Public Safety</td>
</tr>
<tr>
<td>Provost Office</td>
<td>Richard Walsh, Interim Asst. Provost Operations</td>
</tr>
</tbody>
</table>

Updated: 4/28/14