University of Scranton

Division of Information Technology

Executive Sponsor:
Senior Vice President for
Finance & Administration

Information Security Policy

Responsible Office:
Information Security

Issued: 06/2014
Revised: 12/2019
Last Review: 12/2021

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 the Information Security Advisory Council, and supported by the University Data Stewards, is authorized to develop, implement, and maintain an Information Security Program, including the establishment of Information Security Policies and 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 interest of the University and to ensure a coordinated approach to creating and maintain a secure environment, protecting our information and technology resources. This policy also helps fulfill the requirements of the Higher Education Opportunity Act (HEOA), Gramm-Leach-Bliley Act, HIPAA, FERPA, PCI-DSS, PA BPINA, and Federal Trade Commission Red Flag rules.

The Information Security Program of the University of Scranton will be based upon best practices recommended in the ISO 27002:2013 framework published by the International Organization for Standardization (ISO) International Electrotechnical Commission (IEC), and the National Institute of Science and Technology (NIST) special publication 800-171, appropriately tailored to the specific circumstances of the University.

III. Entities Affected By This Policy

This policy is intended to guide the work of the Information Security Office and the Information Security Advisory Council in 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, or access data maintained by the University, are responsible for complying with the Information Security Program established under this policy.

IV. Website Address for this Policy

https://www.scranton.edu/information-technology/policies.shtml

V. Related Documents, Forms, and Tools

Human Resources Security Policy

Asset Management Policy

Access Control Policy

Physical and Environmental Security Policy

Operations Security Policy

System Acquisition, Development, and Maintenance, and Supplier Policy

Information Security Incident Management Policy

Compliance Policy

VI. Contacts

For policy clarification and interpretation, please contact the Information Security Office at 570-941-4226 or email infosec@scranton.edu or the Associate Vice President Information Technology & CIO's office at 570-941-6185.

VII. Definitions

ISO/IEC 27002:2013: is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC) entitled *Information technology – Security techniques – Code of practice for information security management*.

NIST Special Publication 800-171: is an information security standard published by the National Institute of Standards and Technology (NIST) entitled *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.*

University Standards: are the required specifications, regulations, or rules that govern behavior at the University. University standards define what is necessary to attain a minimal degree of compliance, and are meant to create consistency and uniformity across processes and activities. Standards and guidelines differ in that standards are required best practices, whereas guidelines 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; the development of technical, physical, and administrative safeguards for information, including the establishment of information security policies and standards, 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.

Chief Information Officer: Responsible for general oversight of the Information Security Program, review of Information Security Standards, interpretation of policy, and determination of a data breach disclosure.

Data Steward: University officials, or their designated representatives with decision-making authority, responsible for data handling practice in their divisions. University data stewards will work in conjunction with the Information Security Office and the Information Security Advisory Council to ensure the confidentiality, integrity, and availability of the University's information assets.

Information Security Advisory Council: The Information Security Advisory Council provides guidance and oversight of the Information Security program with an emphasis on strategy and policy issues, risk management, and compliance to applicable laws and regulations ensuring compliance to applicable laws, regulations. In addition, the Council serves as an advocate of the University Information Security Program.

Data User: Anyone that accesses the University's information assets. Data users must also ensure that they comply with the requirements of the Information Security Program established under this policy.

Data Custodian: A person who has technical control over the University's information assets. Data custodians usually have administrator, system administrator or other equivalent level of access. Data custodians must also ensure that they comply with the requirements of 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 based on aforementioned industry best practices. 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/infosec
2. Information Security Program Governance:

    a. All new Information Security Policies will be drafted by the Information Security Office and presented to the Information Security Advisory Council for review and approval.
    b. New Information Security Standards will be developed by the Information Security Office, in coordination with specific departments and divisions. Information Security Standards that would affect the University community will be presented to the Information Security Advisory Council for review and approval. If broader

governance review is deemed necessary, that review will occur prior to presentation to the Information Security Advisory Council.

c. Updates to all Information Security Policies will be presented to the Information Security Advisory Council for review and approval.

d. Updates to Information Security Standards that change the basic intent of the standard will be submitted to the Information Security Advisory Council for review and approval.

e. The elimination of an Information Security Policy or Standard will be presented to the Information Security Advisory Council for review and approval.

f. Each division head will identify a Data Steward(s) responsible for overseeing data handling practices in their division. These individuals will work with the Information Security Office and the Information Security Advisory Council to maintain compliance with the information security policies and standards defined by the Information Security Program.

g. Violations of policies or standards established as part of the Information Security Program may result in suspension or loss of the violator's use privileges, with respect to Institutional Data and University owned Information Systems. Violators shall be subject to the regular disciplinary processes and procedures of the University that apply to students, faculty, staff, graduate teaching assistants, work study students, and all third parties.

h. Exceptions to the published Information Security Program requirements must be reviewed and 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. Once an exception request has been approved, the exception should be communicated to the Information Security Office.

3. The Information Security Office, in collaboration with the Information Technology Leadership Group and Data Stewards, will annually review the policies and standards implemented as part of the Information Security Program and will propose adjustments to the Program as needed.