The University of Scranton

Division of Information Technology

Executive Sponsor:
Associate Vice President for Information Technology/CIO

Information Classification & Protection Policy

Responsible Office:
Information Security

Issued: 4/2011
Revised: 1/2021
Reviewed: 12/2021

I. Policy Statement

The University of Scranton is committed to protecting the confidentiality, integrity, and availability of its information and technology assets. This policy defines how University information is to be classified and protected. All University information will be classified as Restricted, Confidential, or Public, and protected in accordance with this policy.

II. Reason for Policy

Students, faculty, staff, and alumni trust that the University protects their personal information, both electronic and physical records. The purpose of this policy is to define the University's information classification levels, determine who is responsible for classifying information, and establish how information is to be protected based on the classification level.

III. Entities Affected By This Policy

All individuals who access information maintained by the University are responsible for complying with this policy. This includes students, faculty, staff, graduate teaching assistants, work study students, and all third parties.

IV. Website Address for this Policy

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

V. Related Documents, Forms, and Tools

IT Equipment Disposal Procedure
https://www.scranton.edu/information-technology/policies.shtml

Records Management and Retention Policy:
https://www.scranton.edu/Governance/university-policies%20.shtml

University FERPA Policy:
https://catalog.scranton.edu/content.php?catoid=51&navoid=6294&hl=%22FERPA%22&returnto=search

Securely Sharing Files with Restricted Data:
https://www.scranton.edu/information-technology/policies.shtml

VI. Contacts

For policy clarification and interpretation, contact the Associate Vice President for Information Technology/CIO at 570-941-6185. For legal advice and interpretation of law, please contact the Office of General Counsel at 570-941-6213.

VII. Definitions

Electronic Records: Information in a digital format which requires an electronic device to read.

Physical Records: Information in paper records and documents.

Restricted information: University information that is protected by legal or regulatory requirements, contractual requirements, or specific University policies. The unauthorized disclosure, modification, or destruction of restricted information would present the highest level of risk to the University and could result in legal or financial liability to the University. Restricted information should only be accessed on a need to know basis and external distribution should be authorized by the appropriate Data Steward.

Common examples of restricted information are:

- Healthcare information protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Graham Leach Bliley (GLB) Act, the Federal Trade Commission Red Flag Rules, the Pennsylvania Senate Bill 712, or any other federal, state, industry, or local law.
- Credit card information protected by the Payment Card Industry Data Security Standard (PCI DSS).
- Personal information protected by the Graham Leach Bliley Act (GLBA), the Federal Trade Commission Red Flag Rules, the Pennsylvania Breach of Personal Information Notification Act, or any other federal, state, industry, or local law.
- Financial account information
- Authentication secrets (passwords, private keys)

See Appendix A for more detail.

Confidential information: University information that is used primarily to conduct official University business with limited internal distribution. The unauthorized disclosure, modification, or destruction of confidential information would present a moderate level of risk to the University and could result in damage to the University's reputation or level of confidence in the University. Confidential information should have limited internal distribution and external distribution should be authorized by the appropriate Data Steward.

Common examples of confidential information are:

- Student records that are covered by the Family Educational Rights and Privacy Act (FERPA)
- Employee information
- Donor records
- University proprietary information

See Appendix A for more detail.

Public information: University information that is not classified as restricted or confidential. The unauthorized disclosure, modification, or destruction of public information would present a low, or no, level of risk to the University.

See Appendix A for more detail.

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.

VIII. Responsibilities

Information Security is responsible for maintaining a matrix of applicable controls by process and information type for use by Data Stewards and Information Technology staff. This matrix shall be considered Appendix B of this policy.

University Data Stewards are responsible for performing an annual inventory of all information their division acquires, communicates, transmits, processes, or stores and assign to that information one of the information classifications defined in this policy. Data Stewards shall then apply and document the appropriate controls from Appendix B for each set of records based on the highest classification of data contained in those records. Any information that does not receive a classification shall default to a classification of confidential.

Users who are authorized to use or modify information are responsible for adhering to the controls applied by the Data Stewards.

IX. Procedures

Controls

The appropriate control shall be applied to every process used to handle restricted and/or confidential information, according to the classification of that information.

- Acquisition

  Restricted and Confidential information shall only be requested from an individual, or acquired from other sources, when there is a legal and active business use for the information.

- Access

  For Restricted and Confidential information, in any medium, University Data Stewards shall apply appropriate physical and electronic controls to limit access to this information to persons who need to use it to perform their University assigned duties and for whom it is legally appropriate to have access to this information. Only the minimum level of access necessary should be granted.

  For Restricted information, it is required that those given access have University duties that require access and for whom it is legally appropriate to have access. In addition, all student employees given access to Restricted information must have executed a confidentiality agreement that covers this information.

- Network Transmission

Restricted information may be transmitted over University or external networks only if the data or the entire transmission is encrypted. Questions regarding encryption of data for external transmission should be directed to Information Security prior to transmission.

Confidential information may be transmitted over the University or external networks as required, provided that access to the information is restricted to those who must use it to perform University assigned duties.

- Processing of Information

  The University and its employees shall employ information processing systems and procedures with appropriate safeguards to ensure that Restricted and Confidential information is not lost or disclosed to unauthorized persons during or after processing.

- Communication

  Confidential and Restricted information communicated by voice, mail, fax, or other methods must use reasonable safeguards against disclosure to unauthorized persons, as appropriate to the method of communication.

  External communication of Confidential and Restricted should be authorized by the appropriate Data Steward.

  Restricted information may not be communicated to third parties, except as specifically required by legal obligation or protected under contractual agreements.

  Please see Securely Sharing Files with Restricted Data for additional guidance.

- Storage

  Restricted information in electronic records shall be encrypted when stored outside the central University administrative database. Restricted information in all forms of physical records must either be security locked or actively supervised in a private environment at all times.

  Confidential information shall be stored in physical or electronic environments where access is limited to only those who need to use the information for University assigned duties and for whom it is legally appropriate to have access to the information.

  Restricted and Confidential information shall only be stored on approved cloud or on premises storage.

  Restricted and Confidential information shall not be stored on personal devices.

  Restricted information shall not be stored on local hard drives.

- Retention, Disposal and Transfer

  Confidential and Restricted information must be retained and disposed of in accordance with the University's Records Management and Retention Policy. Computers and other electronic devices must be transferred or disposed of in accordance with the IT Equipment Disposal Procedure.

Improper Disclosure or Loss

All faculty, staff, and students shall immediately report inappropriate disclosure or suspected loss of Confidential or Restricted information to the Information Security Office at 570-941-4226 or email infosec@scranton.edu

Compliance

Violations of any part of this policy will subject violators 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.

X. Appendix (optional)

Appendix A – Information Protection Data Fields Alphabetical

Appendix B — Information Protection Controls for Each Classification

Appendix A — Information Protection Alphabetical
Specific Confidential and Restricted Data Fields with Examples of Public Data

Data Field	Classification	Special Note
Athletics Information	Confidential	
Alumni Information	Confidential	
Authentication Secret such as: Passwords List of Passwords Private Keys for Certificates	**Restricted**	
Bank Account Number and/or PIN Number	**Restricted**	
Budget Information	Confidential	
Campus Map	Public	
Course Enrollment Information	Confidential	
Course Schedule	Public	
Credit Card Number	**Restricted**	
Debit Card Number	**Restricted**	
Departmental Memo	Confidential	
Directory Information	Public	
Drivers License Number	**Restricted**	
Employee Disability Claim	Confidential	
Employee Name with: Benefits Information Date of Birth Home Address Personal Contact Information Salary or Payroll Information	Confidential	
Employee Performance Review	Confidential	
Employee Social Security Number	**Restricted**	
Employee Worker's Compensation Claim	Confidential	
Student Health Services Information	** See Notes	See "Patient Information" below.
Legal Counsel Communication	Confidential	
Library Circulation Records	**Restricted**	
Medical Records	** See Notes	See "Patient Information" below.
Password(s)	**Restricted**	
Patient Information including Account Information Beneficiary Information Biometric Identifiers Email Address Guarantor's Information Health Plan Information	**Restricted**	HIPAA prohibits institutions from releasing patient information that can be traced back to a specific individual.

Identification Number(s) Medical Record(s) Name(s) Personal Contact Information Photographs Other Unique Identifying Information		
Royal Id	Confidential	
Social Security Number	**Restricted**	
Student Disciplinary Records	Confidential	
Student Financial Aid Information	Confidential	
Student Grades	Confidential	
Student Grant Information	Confidential	
Student Loan Information	Confidential	
Student Name with Address (local and permanent) Telephone number (campus/local and permanent) Date and place of birth Photograph Major field of study Participation in officially recognized activities and sports E-mail address Dates of attendance Enrollment status Campus employment Class level Expected/actual date of graduation Degrees, awards, academic honors Weight and height of members of athletic teams	** See Notes	These data fields may ordinarily be revealed by the University without student consent unless the student designates otherwise.
Student Non-public Financial Information (such as income, assets, tax forms)	Confidential	
Student Payment History	Confidential	
Student Social Security Number	**Restricted**	
Student Tuition Bill Information	Confidential	
Student Transcripts	Confidential	
University Counseling Center Records	**See Notes	See “Patient Information”
University Investment Information	Confidential	

Appendix B — Information Protection
Appropriate Controls for Each Information Classification by Handling Process

Classification	Restricted	Confidential	Public
Process:			
Acquisition	Must be: • Legal to acquire • Actively used	Must be: • Legal to acquire • Actively used	Must be: • Legal to acquire
Access	Limited to those with University duties that require access and for whom it is legally appropriate to have access. Minimum level of access necessary. Requires confidentiality for student employees	Limited to those with University duties that require access and for whom it is legally appropriate to have access. Minimum level of access necessary	Not restricted
Network Transmission	Data or entire transmission must be encrypted	Transmission as required on internal and external networks	As required on internal and external networks
Processing	Systems must use appropriate safeguards to prevent loss/disclosure	Systems must use appropriate safeguards to prevent loss/disclosure	As required on any system
Communication	Reasonable safeguards against disclosure to unauthorized persons. Must be authorized by Data Steward. Communication to third party requires legal obligation/contract	Reasonable safeguards against disclosure to unauthorized persons. Must be authorized by Data Steward	As required to all persons
Storage	Only on approved storage Not on personal devices Not on local hard drives Strong encryption or University central administrative database If physical records, securely locked or actively supervised in a private environment	Only on approved storage Not on personal devices Storage in a secure location with controls in place to limit access to those with University duties that require access	As required
Retention, Disposal, Transfer	According to Records Management Policy and IT Equipment Disposal Procedure		