I. Policy Statement
All University departments will classify and protect all information that is entrusted to us.

II. Reason for Policy
This policy defines how University information is classified and how it is to be protected. Students, faculty, staff, and alumni trust that the University protects their personal information as it exists in any medium — electronic, as well as all forms of paper record.

This policy also helps to fulfill the requirements of federal and state information security regulations; specific examples of these regulations can be found on page 2.

III. Entities Affected By This Policy
This policy impacts all units of the University, and is specifically enacted by data stewards and department heads.

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

V. Related Documents, Forms, and Tools
Computer Security Incident Response Team Operational Standards Manual:

Records Management and Retention Policy:
http://www.scranton.edu/general-counsel/docs/records_policy.pdf

University FERPA Policy:
http://catalog.scranton.edu/content.php?coid=24&navoid=2109#Academic_Policies_and_Regulations

Information Management Model: http://www.scranton.edu/pir/policies.shtml
VI. Contacts
For policy clarification and interpretation, or consulting on classification and control of electronic information, contact the Information Security Office at 570-941-4226 or email security@scranton.edu

For information on the classification and control of physical records, or consulting on the interpretation of federal and state regulations, contact the General Counsel’s Office at 570-941-6213.

VII. Definitions
University information is contained in physical and electronic records. Physical records (which include all forms of paper records and documents) contain information directly readable by humans. Electronic records contain information that requires an electronic device to read the information.

Information classification categories:
Restricted information is University information that:
- Makes the University liable for costs or damages due to unauthorized disclosure under laws, government regulations, or contract.
- Includes authentication secrets (passwords, private keys, see Appendix A/B for further examples)

Confidential information is University information that:
- Is used primarily to conduct official University business with limited internal distribution
- Contains proprietary information, pertains to student records that are covered by the Family Educational Rights and Privacy Act (FERPA), or pertains to donor records. See Appendix A/B for further information.

Public information is University information that:
- Is not classified as restricted or confidential

Known confidential and restricted data fields are contained in Appendix A/B.

VIII. Responsibilities
University department heads or designates are responsible to inventory all information their offices acquire, communicate, transmit, process, or store and assign it to one of the information classifications defined in this policy. This includes information stored and processed in applications provided by any third-party service used by the department. Department heads
IT Policy
Policy Name: Information Classification & Protection Policy

shall then apply and document the appropriate controls for each set of records (e.g. forms, electronic documents, database, etc.) based on the highest classification of data contained in those records (see currently supported controls in Appendix D and classification/documentation examples in Appendix C). Department heads should confer with their division’s data steward throughout this process. Departments’ inventory, information classification, and controls should be reviewed annually.

The Information Security Office shall maintain a matrix of applicable controls by process and information type for use by department heads and Information Resources staff. This matrix shall be considered Appendix C of this policy. A list of technical procedures for implementing encryption and access controls will be maintained by Information Resources and published by the Information Security Office, considered Appendix D of this policy.

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 department heads shall use 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. For restricted information, it is required that those given access have a need to know and have executed a non-disclosure/confidentiality agreement that covers this information.

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

  Restricted information shall not be transmitted over University or external networks, outside a data center, a firewalled network so designated by Information Resources, unless the data or the entire transmission is encrypted. Questions regarding encryption of data for external transmission should be directed to the Information Security Office prior to transmission.

- Data Processing
  The University and its employees shall employ data 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.

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

Storage
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 information in electronic records shall be secured with strong encryption 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. Mobile devices that store restricted data should also be protected with a PIN.

Retention, Disposal and Transfer
Confidential and Restricted information must be retained and disposed of in accordance with the University’s Records Management Policy. Computers and other electronic devices must be transferred or disposed of in accordance with the Desktop Computer Disposa l 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 Computer Security Incident Response Team (CSIRT) via abuse@scranton.edu or 570-941-4226.

The responsible division head or dean will sign any legally mandated information breach notification letters for information lost or disclosed by their employees. For more information see the CSIRT Operational Standards Manual.

X. Appendix (optional)
Appendix A – Information Protection Data Fields by Classification
Appendix B – Information Protection Data Fields Alphabetical
Appendix C — Information Protection Controls for Each Classification
Appendix D — Information Protection Approved Technological Procedures
Appendix E — Information Protection Examples of Information Classification and Controls
IT Policy
Policy Name: Information Classification & Protection Policy

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

SPECIFIC CONFIDENTIAL DATA FIELDS
This is not an exhaustive list; however, these are known confidential data fields:

FERPA – Protected Student Records: As defined by the U.S. Department of Education, “the Family Educational Rights and Privacy Act is a Federal law that protects the privacy of student education records.” The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Further explanation can be found at the U.S. Department of Education website (http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html)

- Grades / Transcripts
- Class lists or enrollment information
- Student Financial Services information
- Athletics or department recruiting information
- Payment History
- Financial Aid / Grant information / Loans
- Student Tuition Bills

Note that the following data may ordinarily be revealed by the University without student consent unless the student designates otherwise.

- Name
- Former name(s)
- 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

Employee Information

- Performance reviews
- Worker’s compensation or disability claims
- Name in association with:
  - Salary or payroll information
  - Date of birth
  - Home address or personal contact information
  - Benefits information
IT Policy
Policy Name: Information Classification & Protection Policy

Management data
- Detailed annual budget information
- University investment information
- Non-anonymous faculty course evaluations

General Information
- Confidential information shared with legal counsel
- Internal departmental memos and other correspondence for internal-use-only

SPECIFIC RESTRICTED DATA FIELDS
This is not an exhaustive list of data fields that are covered by non-FERPA laws and University Policy; however, these are known restricted data fields:

Sensitive Personal Information Controlled by Law, Contract or Policy
- Credit Card Numbers
- Debit Card Numbers
- Bank Account Numbers
- PIN Numbers
- Social Security Numbers
- Drivers License or State Identification Numbers
- Authentication Secrets: passwords, lists of passwords or private keys for certificate authentication

HIPAA – Protected Health Information: As defined by the U.S. Department of Health and Human Services, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects individuals from the “wrongful disclosure of individually identifiable health information”. In summary, HIPAA prohibits institutions from releasing patient information that can be traced back to a specific individual. Further information can be found at the official HIPAA website http://www.hhs.gov/ocr/hipaa/. The following data, in relation to one’s status as a patient, is considered restricted information.
- Patient Names
- Street address, city, county, zip code
- Dates (except year) for dates related to an individual
- Telephone/Facsimile numbers
- E-mail, URLs, & IP addresses
- Account/Medical record numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle identification’s & serial numbers
- Device identification’s & serial numbers
- Biometric identifiers
- Full face images
- Any other unique identifying number, characteristic, or code
- Payment Guarantor’s information
EXAMPLES OF PUBLIC DATA FIELDS
These are examples only:

- Campus maps
- Business contact data (e.g., directory information)
- Event and class schedules
IT Policy
Policy Name: Information Classification & Protection Policy

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

Department heads shall apply and document the appropriate controls for a set of records (e.g. forms, electronic documents, database, etc.) based on the highest classification of data contained in those records.

<table>
<thead>
<tr>
<th>Data Field</th>
<th>Classification</th>
<th>Special Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Athletics Information</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Alumni Information</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Authentication Secret such as:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passwords</td>
<td>Restricted</td>
<td></td>
</tr>
<tr>
<td>List of Passwords</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private Keys for Certificates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bank Account Number and/or PIN Number</td>
<td>Restricted</td>
<td></td>
</tr>
<tr>
<td>Budget Information</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Campus Map</td>
<td>Public</td>
<td></td>
</tr>
<tr>
<td>Course Enrollment Information</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Course Schedule</td>
<td>Public</td>
<td></td>
</tr>
<tr>
<td>Credit Card Number</td>
<td>Restricted</td>
<td></td>
</tr>
<tr>
<td>Debit Card Number</td>
<td>Restricted</td>
<td></td>
</tr>
<tr>
<td>Departmental Memo</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Directory Information</td>
<td>Public</td>
<td></td>
</tr>
<tr>
<td>Drivers License Number</td>
<td>Restricted</td>
<td></td>
</tr>
<tr>
<td>Employee Disability Claim</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Employee Name with:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Benefits Information</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Home Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Contact Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salary or Payroll Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee Performance Review</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Employee Social Security Number</td>
<td>Restricted</td>
<td></td>
</tr>
<tr>
<td>Employee Worker’s Compensation Claim</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Student Health Services Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>** See Notes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal Counsel Communication</td>
<td>Confidential</td>
<td>See “Patient Information” below.</td>
</tr>
<tr>
<td>Library Circulation Records</td>
<td>Restricted</td>
<td></td>
</tr>
<tr>
<td>Medical Records</td>
<td>** See Notes</td>
<td>See “Patient Information” below.</td>
</tr>
<tr>
<td>Password(s)</td>
<td>Restricted</td>
<td></td>
</tr>
<tr>
<td>Patient Information including</td>
<td>Restricted</td>
<td>HIPAA prohibits institutions</td>
</tr>
<tr>
<td>Information Category</td>
<td>Classification</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>----------------</td>
<td></td>
</tr>
<tr>
<td>Account Information, Beneficiary Information, Biometric Identifiers, Email Address, Guarantor’s Information, Health Plan Information, Identification Number(s), Medical Record(s), Name(s), Personal Contact Information, Photographs, Other Unique Identifying Information</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Royal Id</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Social Security Number</td>
<td>Restricted</td>
<td></td>
</tr>
<tr>
<td>Student Disciplinary Records</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Student Financial Aid Information</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Student Grades</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Student Grant Information</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Student Loan Information</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Student Name with Address, Telephone number, 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</td>
<td>** See Notes</td>
<td></td>
</tr>
<tr>
<td>Student Non-public Financial Information (such as income, assets, tax forms)</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Student Payment History</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>Student Social Security Number</td>
<td>Restricted</td>
<td></td>
</tr>
<tr>
<td>Student Tuition Bill Information</td>
<td>Confidential</td>
<td></td>
</tr>
</tbody>
</table>
## IT Policy
Policy Name: Information Classification & Protection Policy

<table>
<thead>
<tr>
<th>Information Type</th>
<th>Classification</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Transcripts</td>
<td>Confidential</td>
<td></td>
</tr>
<tr>
<td>University Counseling Center Records</td>
<td><strong>See Notes</strong></td>
<td>See “Patient Information”</td>
</tr>
<tr>
<td>University Investment Information</td>
<td>Confidential</td>
<td></td>
</tr>
</tbody>
</table>
## Appendix C — Information Protection
### Appropriate Controls for Each Information Classification by Handling Process

<table>
<thead>
<tr>
<th>Process</th>
<th>Restricted</th>
<th>Confidential</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Acquisition</strong></td>
<td>Must be:</td>
<td>Must be:</td>
<td>Must be:</td>
</tr>
<tr>
<td></td>
<td>• Legal to acquire</td>
<td>• Legal to acquire</td>
<td>• Legal to acquire</td>
</tr>
<tr>
<td></td>
<td>• Actively used</td>
<td>• Actively used</td>
<td></td>
</tr>
<tr>
<td><strong>Access</strong></td>
<td>Limited to those with University duties that</td>
<td>Limited to those with University duties that</td>
<td>Not restricted</td>
</tr>
<tr>
<td></td>
<td>require access</td>
<td>require access and for whom it is legally</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>appropriate to have access</td>
<td></td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>Data or entire transmission must be encrypted</td>
<td>As required on internal and external networks</td>
<td>As required on internal and external</td>
</tr>
<tr>
<td>Transmission</td>
<td>outside datacenter</td>
<td></td>
<td>networks</td>
</tr>
<tr>
<td><strong>Data Processing</strong></td>
<td>Systems must use appropriate safeguards to</td>
<td>Systems must use appropriate safeguards to</td>
<td>As required on any system</td>
</tr>
<tr>
<td></td>
<td>prevent loss/disclosure</td>
<td>prevent loss/disclosure</td>
<td></td>
</tr>
<tr>
<td><strong>Communication</strong></td>
<td>Methods must prevent disclosure to unauthorized</td>
<td>Requires appropriate safeguards against</td>
<td>As required to all persons</td>
</tr>
<tr>
<td></td>
<td>persons</td>
<td>disclosure</td>
<td></td>
</tr>
<tr>
<td><strong>Storage</strong></td>
<td>Must be one of:</td>
<td>Storage in a secure location with controls in</td>
<td>As required</td>
</tr>
<tr>
<td></td>
<td>• Strong encryption using strong password or</td>
<td>place to limit access to those with University</td>
<td></td>
</tr>
<tr>
<td></td>
<td>private key</td>
<td>duties that require access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• University central administrative database</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Securely locked</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Actively supervised in a private environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Retention, Disposal, Transfer</strong></td>
<td>According to Records Management Policy and Desktop Computer Disposal Procedure</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

11
ACCESS
Access to confidential and restricted information in electronic records shall be controlled as follows:
- Use appropriate system or network permissions for the individual or group to restrict access
- Authenticate each person accessing the information individually using one of the following:
  - University Network ID and Password
  - Other unique ID and a strong password that meets Information Resources’ Password Complexity Requirements
- Requests for access to restricted data must be made following Information Resources’ standard change request process and approved by the appropriate Data Steward.

All authentication must be encrypted.

TRANSMISSION
Public and Confidential Information may be transmitted as required on internal and external networks. Restricted information may NOT be transmitted on any network without encryption.

Acceptable encrypted network transmission methods include:
- Virtual Private Network (VPN) where systems on both ends of the transmission meet Security requirements. Examples:
  - Using a VPN connection to e-mail restricted information is NOT encrypted transmission because the e-mail will leave the VPN at some point on the way to its destination
  - Using a VPN to access reports from the central administrative system is secure transmission because the unencrypted reporting system is inside a data center
- Secure Sockets Layer (SSL) or Transport Layer Security (TLS) transport for network protocols such as Secure HyperText Transfer Protocol (HTTPS), Lightweight Directory Access Protocol (LDAP), etc.
- Secure Shell (SSH) and related protocols Secure File Transfer Protocol (SFTP) and Secure Copy (SCP)
- Remote Desktop Protocol (RDP) using encryption
- Secure email attachments server (Royal Drive)

STORAGE
Storage of restricted information outside the central administrative database requires strong encryption with a strong password.

Examples of storage encryption known to be strong include:
- Microsoft Encrypting File System (EFS) on Windows XP or later
- FileVault and disk image encryption on Macintosh OS/X
- Pretty Good Privacy (PGP) public/private key encryption, where the private key is secured
- Sophos Utimaco SafeGuard (whole disk encryption)
- Programs using standard protocols with at least a 128bit key protected by a strong password, examples include:
  - Triple DES/3DES
IT Policy
Policy Name: Information Classification & Protection Policy

- AES
- IDEA
- Blowfish

For consulting on access control, and encrypted transmission and storage methods, please contact the Information Security Office.
IT Policy
Policy Name: Information Classification & Protection Policy

Appendix E — Information Protection
Examples of Information Classification and Access Controls

NOTE: Each set of records should have controls applied according to the highest classification of data contained in those records; the procedures for implementing those controls by the department must be documented. The following examples are intended to assist with information classification. Applying the appropriate controls is the responsibility of the department head and data steward.

Example 1:
A physical form contains a restricted field, e.g. Social Security Number. Therefore, the entire form is handled under the restricted controls. Despite the presence of public and confidential information on the form, the entire form is classified as restricted and handled accordingly. If all of the data from the example form is entered into a single spreadsheet, that spreadsheet becomes restricted information and must have controls for restricted data applied and documented. If the SSN data from the example form is entered into one spreadsheet while the rest of the data is entered into a database (without the SSN), then the spreadsheet needs the restricted controls applied and documented, but the database does not. The department will document how the forms are obtained, handled and secured under the appropriate controls (e.g. which locked storage will be used when not being processed in a private area; what to do with the forms when they must be temporarily left unattended). The department will document how the spreadsheet containing the SSNs will be encrypted when transmitted (e.g. Secure Attachments server and stored on disk using PGP).

Example 2:
Someone calls into the Campus Operator asking for a student’s residence hall assignment. Unless the student has previously requested that his/her contact information not be disclosed, the student’s residence hall information can be disclosed without violated FERPA regulations. Information Classification and Protection Policy