University of Scranton
Information Technology Policy

May 17, 2012

Privacy and Confidentiality

Executive Sponsor: AVP Information Resources

Responsible Office: Information Security

Originally Issued: 5/17/2012[1]
Revised: n/a

I. Policy Statement

All University divisions and constituent organizational support units will work to ensure that information privacy and confidentiality is preserved throughout their procedures and information systems. Where appropriate, information privacy and confidentiality will be mandated further by policy and/or enforced contractually.

II. Reason for Policy

This policy establishes the principles to guide the practices of divisions and units in protecting the privacy and confidentiality of the information entrusted to us. This policy also helps to fulfill the requirements of federal and state information security regulations; specific examples of these can be found in Section V.

III. Entities Affected By This Policy

This policy impacts all units of the University, and is specifically enacted by data stewards, department heads, and other responsible parties.

IV. Website Address for this Policy

http://matrix.scranton.edu/pir/policies.shtml

V. Related Documents, Forms, and Tools

Information Classification & Protection Policy; Information Access Policy:

http://matrix.scranton.edu/pir/policies.shtml

Records Management and Retention Policy:

http://matrix.scranton.edu/Governance/university-policies%20.shtml

Computer Security Incident Response Team Operational Standards Manual:

http://www.scranton.edu/pir/documents/CSIRT%20Operational%20Standards%20Manual.pdf

[1] Approved May 17, 2012 by Jerome DeSanto, Vice President for Planning & CIO.

Related Required Disclosure Statements

Student Rights & Confidentiality of Information Statement (FERPA):

http://catalog.scranton.edu/content.php?catoid=6&navoid=109&print#Academic_Policies_and_Regulations

Health Insurance Portability and Accountability Act Privacy Policy:

http://www.scranton.edu/humanresources/hipaa_privacy_policy.doc

Weinberg Memorial Library Borrowing and Lending Policies Confidentiality Statement (PA Law 24 CSA Section 4428):

http://www.scranton.edu/academics/wml/about/policies/borrowing-lending.shtml

Information Resources Privacy & Confidentiality Statement

https://royaldrive.scranton.edu/Groups/Planningandinformationsystems/PAIRO/Governance/Policy%20Analysis/Technology%20Policies/Policies/Privacy%20and%20Confidentiality/PIR%20Division%20Privacy%20Statement%20final%202012.pdf?ticket=t_j4mkMKgS

Finance Information Security Policy – in development for Treasurer's web page

Website Tracking Disclosure Statement – in development with PR

VI. Contacts

For policy clarification and interpretation, or consulting on maintaining the privacy and confidentiality of information, please contact the Information Security Office at 570-941-4226 or email security@scranton.edu

For information on privacy and confidentiality legal requirements, or consulting on the interpretation of federal and state regulations, contact the General Counsel's Office at 570-941-6213.

VII. Definitions

Privacy is the state in which only intended recipients can access information

Confidentiality is the preservation of the privacy of information entrusted with confidences

VIII. Responsibilities

Employees, as data custodians, are expected to handle all information in a manner consistent with the Information Classification & Protection Policy, the controls prescribed by data stewards, and in a manner consistent with the following guiding principles for protecting privacy and confidentiality.

IX. Procedures - Guiding Principles

At all times, employee collection of, access to, and care of electronic information shall be guided by the following principles:

Accountability: Information systems should be architected in such a way that all data access is attributable to the responsible party.

Availability: Information systems should be architected to support continuity of operations to the extent possible.

Disclosure: Individuals will be notified if their personally identifiable information is being collected and informed of their rights.

Integrity: Information systems should be architected in such a way that data cannot be modified without authorization.

Legitimate Educational Interest: Access to information shall be restricted to those individuals having legitimate educational interest, as defined by the Family Educational Rights and Privacy Act (FERPA).

Limited Scope: Information should only be used for the stated purposes for which it was collected.

Minimization: Only the essential information should be collected that is necessary for enabling a business process.

Nondisclosure: Confidential or restricted information shall not be further shared or released to third parties outside the University and contracted business partners without prior consent unless compelled to do so by law.

Retention: Data should only be retained for the period specified in the University Records Management and Retention Policy and Records Retention Schedule, for the duration of the business process that it enables, or as required by law.

X. Appendix – None