SIU CARBONDALE SOUTHERN ILLINOIS UNIVERSITY OFFICE OF INFORMATION TECHNOLOGY

Data Classification Policy

Document Number:	ISP-007	**Version:**	1.3
Document Owner:	Director of Information Security	**Effective Date:**	09/01/2014
Responsible Office:	Information Technology		

TABLE OF CONTENTS

PURPOSE [TOP]

The purpose of this policy is to establish a framework for classifying University data based on its level of sensitivity, value and criticality to the University as required by the University's Information Security Plan. Classification of data will aid in determining minimum security controls for the protection of data, proper utilization of resources, and for compliance with regulations, laws, and auditors' recommendations.

SCOPE [TOP]

This policy applies to any system that contains or processes institutional data related to Southern Illinois University (SIU). In the context of this document, system includes software, hardware, processes, and printouts and copies of electronic data, whether on SIU premises or not, related to SIU business, whether owned by SIU or not.

POLICY

[TOP]

All members of the University community (See Roles and Responsibilities) have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by the University, irrespective of the medium on which the data resides and regardless of format (e.g., in electronic, paper, or other physical form).

Pursuant to this responsibility, all institutional data and systems related to SIU shall be classified (See Appendix A) into one of the following three data classification levels according to its sensitivity and inventoried to assist in designating the proper security controls of this data for the business continuity and efficiency of the University and to enable compliance with laws, regulations, policies, requirements, standards, and other appropriate criteria. It is the direct responsibility of all data custodians, owners, users, and administrators to assure that data inventories are reported in a timely fashion. Information Technology will determine procedures for reporting data inventories in accordance with this policy which may include by manual or automated means.

Level 1 - Public Data

Data should be classified as ***Level 1 - Public*** when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

Public data is not considered sensitive; therefore, access to Public data may be granted to any requester or published with no restrictions. The integrity of Public data should be protected. Where possible, the appropriate Data Owner must authorize replication or copying of the data in order to ensure it remains accurate over time. The impact on the institution should Public data not be available is typically low, (inconvenient but not debilitating). Examples of Public data include directory information, course information, job postings, and non-copyright research publications.

Level 2 – Internal Data

Data should be classified as ***Level 2 - Internal*** when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the University or its affiliates. By default, all institutional data that is not explicitly classified as ***Level 4 - Highly Restricted***, ***Level 3 – Restricted,*** or ***Level 1 - Public*** data should be

treated as ***Level 2 - Internal***. A reasonable level of security controls should be applied to this level of data.

Access to Internal data must be requested from, and authorized by, the Data Owner who is responsible for the data. Access to Internal data may be authorized to groups of persons by their job classification or responsibilities ("role-based" access), and may also be limited by one's department.

Internal data is moderately sensitive in nature. Often, Internal data is used for making decisions, and therefore it's important that this information remain timely and accurate. The risk for negative impact on the University should this information not be available when needed is typically moderate. Examples of Internal data include official university records such as financial reports, organization charts, planning documents, memorandums, some research data, and budget information.

Level 3 – Restricted Data

Data should be classified as ***Level 3 - Restricted*** when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the University or its affiliates. The highest level of security controls should be applied.

Access to Restricted data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the University who require such access in order to perform their job ("need-to-know"). Access to Restricted data must be individually requested and then authorized by the Data Owner who is responsible for the data.

Restricted data is highly sensitive and may have personal privacy considerations, or may be restricted by federal or state law. In addition, the negative impact on the institution should this data be incorrect, improperly disclosed, or not available when needed is typically very high. Examples of Restricted data include data protected by state or federal privacy regulations, data protected by confidentiality agreements, official student records (non-directory information), and employment information.

Level 4 – Highly Restricted Data

Data should be classified as ***Level 4 - Highly Restricted*** when the unauthorized disclosure, alteration or destruction of that data could cause an extreme level of risk to the University or its affiliates. The highest level of security controls should be applied.

The primary difference between ***Level 3 - Restricted*** and ***Level 4 - Highly Restricted*** data is that ***Level 4 - Highly Restricted*** data carries a direct financial liability to the University in the case of improper disclosure.

Access to Highly Restricted data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the University who require such access in order to perform their job ("need-to-know"). Access to Highly Restricted data must be individually requested and then authorized by the Data Owner who is responsible for the data.

Highly Restricted data is extremely sensitive and may have personal privacy considerations, or may be restricted by federal or state law. In addition, the negative impact on the institution should this data be incorrect, improperly disclosed, or not available when needed is typically very high and may have significant **financial impact to the University**. Examples of Highly Restricted data include data protected by state or federal privacy regulations, data protected by confidentiality agreements, Payment Card Industry (PCI) data, social security and credit card numbers, and individuals' health information.

ROLES AND RESPONSIBILITIES

[TOP]

All SIU personnel including, but not necessarily limited to, faculty, staff, Civil Service, Administrative Professional, outsourced contractual workers, volunteers, temporary extra help, students, student workers, graduate assistants, and undergraduate assistants are required to abide by the requirements and standards established within this policy.

DEFINITIONS

[TOP]

Data Custodian - Employee of the University who has administrative and/or operational responsibility over institutional data.

Data Owner - An individual or group of people who have been officially designated as accountable for specific data that is transmitted, used, and stored on a system or systems within a department, college, school, or administrative unit of the University.

FERPA - The Family Educational Rights and Privacy Act.

Institutional Data - Institutional Data is defined as any information (in any form, location, or unit) that satisfies at least one of the following criteria:

- It is created, received, maintained, or transmitted as a result of educational, clinical, research, or other scholarly activities.
- It is substantive, reliable, and relevant to the planning, managing, operating, documenting, staffing, or auditing of one or more major administrative functions of the university.
- It is used to derive any data element that meets the above criteria.

Non-public Information - Any information that is classified as ***Level 2* - Internal Data** according to the data classification scheme defined in this document.

Sensitive Data - Generalized term that typically represents data classified as ***Level 4 - Highly Restricted*** according to the data classification scheme defined in this document.

COMPLIANCE [TOP]

Violations of this Policy may result in suspension or loss of the violator's use privileges, with respect to Institutional Data and University owned Information Systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with the University. Civil, criminal and equitable remedies may apply.

REFERENCES [TOP]

NIST SP 800-60

AUTHORITY [TOP]

Southern Illinois University Board of Trustees Policy, SIU System Information Security Plan.

REVISION HISTORY [TOP]

Version	Description	Revision Date	Author
1.0	Policy was approved by CIO.	09/01/2014	Director of Information Security
1.1	A fourth classification level (Highly Restricted) was added.	10/27/2014	Director of Information Security
1.2	Added intellectual property to Highly Restricted examples in Appendix B.	10/31/2014	Director of Information Security

1.3	Data classification examples were adjusted to rectify ambiguities primarily within the Restricted classification.	11/18/2014	Director of Information Security

APPENDIX A – DETERMINING CLASSIFICATION

[TOP]

The data classification scheme in this document is based on National Institute of Standards and Technology (NIST) Special Publication 800-60 Volume 1 Revision 1, August, 2008, Guide for Mapping Types of Information and Information Systems to Security Categories, U.S. Department of Commerce. This scheme refers to FISMA and FIPS. FISMA is the Federal Information Security Management Act. FIPS is the Federal Information Processing Standard.

Security Objectives

The goal of information security, as stated in the University's Information Security Plan, is to protect the confidentiality, integrity and availability of information assets and systems. Proper data classification and handling reflects the level of impact to the University if confidentiality, integrity or availability of the data is compromised.

Determining Classification

Refer to Appendix B for specific examples before applying the logic in this section. If the specific data classification level cannot be determined based on the examples in Appendix B, potential impact can be used to properly classify the data. When determining Data Classification, the appropriate level can be derived by cross referencing the potential impact using only the Confidentiality security objective in the table below. Using the Confidentiality security objective; **Low** equals ***Level 1 – Public,*** **Moderate** equals ***Level 2 – Internal,*** and **High** equals either ***Level 3 – Restricted or Level 4 – Highly Retstricted***. To determine if data should be classified as ***Level 3 – Restricted*** or ***Level 4 – Highly Restricted*** assess the financial impact to the University should the data be lost or improperly disclosed. Data should be classified as ***Level 4 – Highly Restricted*** if the improper disclosure of loss of data would have a direct and substantial financial impact to the University. If a system, then, has data with an impact level of moderate, the data classification level would be ***Level 2 - Internal***. The Integrity and Availability security objectives are extremely important in mapping data types but for the purposes of data classification in this document are not used to calculate data classification level.

Data Owners may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of a student's name, address and social security number, the data collection should be classified as Level 3 - Restricted even though the student's name and address may be considered Public information.

The aggregate data classification for a system is the highest of the individual impact levels for the data on that system. For example, if a system has data with an impact level of low, additional data with an impact level of low, and additional data with an impact level of high, the aggregate impact level for the system containing or processing all of this data is high (because high is the highest value of the individual values of low, low, and high). A high impact level translates into a ***Level 3 - Restricted*** data classification.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality - *Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity - *Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.*	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability - *Ensuring timely and reliable access to and use of information.*	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

APPENDIX B – EXAMPLES OF DATA CLASSIFICATION LEVELS

[TOP]

The following list is not exhaustive or comprehensive. If you have a question about a specific data type and/or are uncertain how it should be classified, please contact the Information Security Team (security@siu.edu).

Public

Academic Information

- Course catalog
- Schedule of classes

Employment Information

- Directory information such as name, job title, business address, business telephone number, etc.
- Previous work experience
- Education & Training background
- Dates of first and last employment

General

- Advertising
- Job Postings
- Press releases
- Published maps, newsletters, newspapers, and magazines
- Published research
- Training manuals
- Websites

Student Information

- Directory information such as name, mailing address, preferred telephone listing, e-mail address, major, etc. Refer to specific FERPA information for details about directory information.

Internal

Employment Information

- Resume

General Information

- Budget information
- Employee gross salary
- Financial reports
- Internal memos, emails, faxes, reports, and agendas
- Network ID
- Organization charts
- Planning documents
- Policies and procedures
- System security plans

Research Information

- Animal research protocols
- Incomplete or unpublished research

Student Information

- Student ID (i.e., DAWG Tag) if used strictly for identification purposes or in combination with directory information. Circumstances may dictate that FERPA guidelines apply (and therefore a Restricted classification) if used in combination with non-directory educational records.

Restricted

The following represents types of data categories as determined by various laws and regulations:

- FERPA: The Family Educational Rights and Privacy Act protects the privacy of student education records.

In addition to the above data categories the following represents a list of specific data types that are considered Restricted.

Employment Information

- Home or mailing address

- Biometric information (e.g.: fingerprint, voice recording, palm print, iris scan, DNA)
- Birthplace (City, State, and if not USA, Country)
- Personal telephone numbers
- Personal email address
- Parents and other family members' names
- Emergency contact names and telephone numbers
- Payment history
- Employee evaluations
- Background investigations
- Electronic or digitized signatures
- Private key (digital certificate)
- Ethnicity
- Gender
- Marital status
- Personal characteristics (i.e., hobbies)
- Physical description
- Photograph (i.e., staff identification card)

Facilities Information

- Building plans and architectural drawings

Library

- Registration records related to an individual patron information
- Circulation records related to an individual borrowing particular books and material

Purchasing and Accounts Payable Information

- Sealed bids prior to award
- Identifiable information (purchase order) of the supplier/company

Student Information

- Educational records of individual students (Excludes directory information such as name, mailing address, preferred telephone listing, e-mail address, major, etc. Refer to specific FERPA information for details about directory information.) Non-directory student information may not be released except with Office of the Registrar's approval and only under certain prescribed conditions.
- Home or mailing address

- Personal telephone numbers
- Personal email address (excludes SIU username@siu.edu)
- Ethnicity
- Gender
- Birthplace
- Grades
- Courses taken
- Schedule
- Test Scores
- Advising records
- Educational services received
- Disciplinary actions
- Photograph (e.g., student identification card)

Highly Restricted

The following represents types of data categories as determined by various laws and regulations:

- GLBA: The Gramm-Leach-Bliley Act protects customer financial information.
- HIPAA: The Health Insurance Portability and Accountability Act protects personal health information. See that act for a definition of protected health information.
- PCI DSS: The Payment Card Industry Data Security Standards protect information related to credit card transactions.
- Illinois PIPA: The Illinois Personal Information Protection Act protects social security numbers, driver's license and state ID numbers, and bank and credit card account information.
- Red Flags Rule: Federal Trade Commission (FTC) Red Flags Rule protects identity theft. Identifying information is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, social security number, date of birth, and driver's license.

In addition to the above data categories the following represents a list specific data types that are considered Highly Restricted.

Personally Identifiable Information (PII)

- Unencrypted SIU login credentials including passwords, encryption keys, etc.

- PINs (Personal Identification Numbers)
- Birth date combined with last four digits of SSN
- Tax ID
- Driver's license number, state identification card number, and other forms of national or international identification
- Social Security number
- Mother's maiden name

Financial Information

- Credit card information including cardholder name, account numbers, PINs, and magnetic stripe data
- Bank account or debit card information

Health & Insurance Information

- Medical records related to an individual
- Psychological Counseling records related to an individual
- Speech and Hearing records

Law Enforcement Information

- Law Enforcement Records related to an individual
- Vulnerability/security information related to campus law enforcement operations

Legal Information

- Legal investigations conducted by the University
- Settlements and claims against the University
- Accident reports and investigations

University Donor Information

- Name
- Home or mailing address
- Personal telephone numbers
- Personal email address
- Donation if request is for anonymous gift/donation

University Research

- Research proposals, protocols, and disclosures
- Research data posing no financial, emotional, or criminal harm to participants, with no link to individual identities
- Classified research requiring facility security clearance oversight
- Human subjects research determined by the IRB to pose criminal, financial, or emotional harm
- Research data subject to a federally approved Certificate of Confidentiality
- Research involving vulnerable populations as determined by the IRB
- Vertebrate animal research with designated species
- Misconduct in Research investigations and Conflict of Interest questionnaires and disclosures
- Internal review records of the Office of Research Integrity and Assurance
- Coded private data with links to individual identities in research protocols and disclosures
- Confidential or sponsor-proprietary information
- Export controlled research information (ITAR or EAR), software, deemed exports and equipment
- Intellectual property including invention disclosures, patent-related documents, material transfer agreements, and other related intellectual property documents

APPENDIX C – USES OF DATA CLASSIFICATION LEVELS

[TOP]

Data and systems inventoried pursuant to this policy may be used for, but not limited to, the following:

- Locations of equipment
- Risk assessments of systems
- Security management
- Business impact analyses
- Capital planning and investment
- System design
- Contingency and disaster recovery planning
- Incident response
- Monitoring of systems
- Law enforcement issues
- Notification indications after security breaches