SIU CARBONDALE SOUTHERN ILLINOIS UNIVERSITY OFFICE OF INFORMATION TECHNOLOGY

Safe Handling of Sensitive Information Standard

Document Number:	ISP-008	**Version:**	1.0
Document Owner:	Director of Information Security	**Effective Date:**	11/01/2014
Responsible Office:	Information Technology Library Affairs		

TABLE OF CONTENTS

PURPOSE [TOP]

This standard defines the usage and security requirements of Level 4 – Highly Restricted data (herein referred to as "sensitive" or "confidential") at Southern Illinois University (SIU or the University). The purpose of this standard is to establish specific requirements for the proper handling of sensitive data in order to ensure that the University maintains strict confidentiality in compliance with applicable requirements and regulations of the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Personal Information Protection Act (PIPA), and other applicable federal and state privacy laws. This standard sets forth this institution's requirements with regard to the handling of sensitive institutional data and serves as the consumer data and privacy standard for the University.

SCOPE [TOP]

The scope of this standard applies to all University personnel (see Roles and Responsibilities) having access to, or who may come in contact with, sensitive information. This standard

pertains to the security and privacy of sensitive information including financial information, health information, personally identifiable information and other appropriately identified University information whether it is in hard copy or electronic form. Accordingly, documents that include sensitive and confidential information such as social security numbers, credit card information, and medical information must be secured during printing, transmission (including by fax), copying, storage and disposal. The information covered in this standard includes, but is not limited to, information that is stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as by telephone and video conferencing).

For the purposes of this document sponsored University research information is considered out of scope. Policies and guidelines established by the granting authority shall be used for proper care and use of research information. Additionally, while Family Educational Rights and Privacy Act (FERPA) data is not specifically covered under the requirements of this standard University policy and guidelines should be used to dictate proper handling of FERPA protected information.

STANDARD

[TOP]

The data user understands and agrees that all information, records, files, documents, and discussions involving sensitive data, as defined in this standard, shall be handled as STRICTLY CONFIDENTIAL. Except in pursuit of his/her role at the university, the data user agrees not to disclose or publish--verbally, in writing, or otherwise—to any person or entity any confidential data.

The data user must manage the creation, storage, amendment, transmission, copying and deletion or destruction of data in a manner which safeguards and protects the confidentiality, integrity and availability of such data. Access to sensitive information is restricted to those who have a need to know as defined by job duties. Access is subject to University-authorized approval. Anyone who receives sensitive information has a responsibility to maintain and safeguard that information and to use it with consideration of that regard for others.

In general, SIU personnel are expected to use common sense and to handle data categorized as sensitive in an appropriate manner. If an employee is uncertain of the sensitivity of a particular piece of information, he or she should consider it sensitive by default and contact their Vice Chancellor, Dean or their designee, or direct supervisor for clarification before taking any action with regard to the information in question.

The requirements that follow provide details on how to properly handle and/or distribute sensitive information, including acceptable electronic transfer and storage methods. Where applicable, disposal standards are given. Please note that these standards represent the most common use cases for the handling and distribution of University data and should be used as a reference only. Information in each category may necessitate more or less stringent measures of protection depending upon the specific circumstances and the nature of the information in question.

Note: If a suspected security event (e.g., compromised system, unauthorized access, etc.) occurs, the data user must follow the University's published incident response procedures.

A. General

1) Sensitive information must not be transferred by any method to persons who are not authorized to access that information.
2) Users must seek to ensure that adequate security measures are in place at each destination when sensitive data is transferred from one location to another.
3) Sensitive information should only be stored, transferred or copied when the confidentiality and integrity of the data can be reasonably assured throughout the process.
4) Sensitive information must be encrypted and or secured while at rest and while in transit.
5) Sensitive information must not be taken off campus unless the user is authorized to do so and only if encryption or approved security precautions have been applied to protect that information.
6) Only University employees who have authorization from the relevant data custodian(s) may have access to confidential data. Supervisor approval is also required.
7) The archiving of digital information must consider legal, regulatory and business requirements and support the University's Retention Policy and guidance from the Records Management Office.
8) Sensitive information and outputs from systems handling sensitive data must be appropriately labelled as "confidential".

9) Destruction or disposal of digital storage devices must be in accordance with standards and guidelines specified by Information Technology.

10) Employees should receive annual training on their responsibilities regarding appropriate use and steps they can take to protect sensitive information. University training regarding safe handling of Social Security Number (SSN) can be found here. Additional training may be found on the Information Security website.

11) Employees must not discuss or display sensitive information in conditions where it may be overheard or viewed by unauthorized individuals.

12) Employees must not leave keys or access badges for rooms or file cabinets containing sensitive information in areas accessible to unauthorized personnel.

13) Once sensitive information no longer serves an active administrative or historical function, it should be disposed of in a timely manner to mitigate the risk of exposure.

14) Sensitive information collected and stored as part of an approved business process must have a designated retention schedule in compliance with the University Records Retention Schedules.

15) Retention schedules must have a plan to destroy or archive the sensitive data with the University archives.

B. Physical

1) Papers and forms containing sensitive information must be kept in a physically secured location such as a locked cabinet and/or office in accordance with their records retention schedule.

2) Sensitive data should only be printed when there is a legitimate need.

3) Hardcopies of sensitive data must be limited to the minimum number required.

4) When printing, photocopying or faxing, employees must ensure that only authorized personnel will be able to see the output. Output should not be left unattended on a printer/fax. Sensitive information should not be transmitted to network-connected printing/scanning devices unless on a closed or securely encrypted network.

5) When sensitive information is not required on an ongoing basis:

a. The sensitive information must be redacted with a black permanent marker or whiteout such that the sensitive information is completely unintelligible. The original document must then be photocopied, and the copy retained while the original is securely shredded.

b. Paper records that are not required on an ongoing or historical basis must be securely shredded by use of a crosscut shredder.

6) Sensitive information stored on removable media such as USB removable drives ("thumb drives"), CDs, and DVDs is typically discouraged. In cases where such media is required sensitive data must be stored in an encrypted form as individual files or encrypted volumes. Alternatively, sensitive information may be stored on encrypted media with password, key, or pin protection.

7) When not in use, removable media must be kept in a physically-secured location such as a locked cabinet and/or office.

8) When sending sensitive information in non-electronic form to off-campus locations (e.g. via United States Postal Service, UPS or Federal Express), measures must be taken to secure the information. Consult with the appropriate data owner for specific handling restrictions.

9) When sending sensitive information to on-campus locations, in non-electronic form, the sender must consult with the appropriate data owner for proper handling procedures. Such handling procedures might include using a security envelope with sealed flap inside a second envelope, stamping "Sensitive" or "Confidential" on the inner and/or outer envelope seal or signing the envelope seal. If possible, the University transit service should be utilized unless another secure means of transportation has been identified.

10) When carrying sensitive information or devices containing such information, employees must ensure that it is physically secure at all times.

11) Employees must not remove sensitive information from an approved secure location without prior approval of the data owner.

C. Electronic records

1) Electronic records containing sensitive information must be stored on University owned equipment or on a remote site such as a cloud storage provider that is under contract with the University and has been approved for storage of sensitive

information. Regardless of physical storage location, files containing sensitive information must be stored in an encrypted format. Unencrypted local drives may not be used for storage of sensitive information.

2) Employees must encrypt sensitive information using an approved University encryption tool when (1) placing it on removable media; (2) placing it on a mobile computer (i.e., laptops); or (3) sending it via electronic mail.
3) Desktops, laptops, etc. must be locked or logged out when unattended and require password authentication to regain access.
4) Access to electronic records containing sensitive information must be restricted to only those users with a business need to access the data. Such access must be periodically reviewed and updated to ensure that access is still required by the user. Users with authorized access should only store sensitive information if there is a legitimate business reason or process that requires it.
5) Access to systems housing sensitive information is restricted to the local campus network or via remote access (i.e., off-campus) utilizing the University's secure Virtual Private Network (VPN). Unsupervised remote access by a third party for technical support is not permitted.
6) Electronic records containing sensitive information must be securely erased when disposed of using a University approved secure erase tool. Deleting files or reformatting electronic media is not sufficient.
7) Servers hosting sensitive information:
    a. Must be protected with a network firewall using a "default deny" rule set. The firewall rule set should be reviewed every 365 days.
    b. Must not be visible to the entire Internet, nor unprotected subnets like the residence halls or guest wireless network.
    c. Must be hosted in the Wham Data Center. Physical access must be monitored, logged, and limited to authorized personnel 24x7.
    d. Must utilize a host-based firewall, where appropriate, to limit access to only required systems, processes, and users.
8) Electronic transmission of sensitive information must be done in an encrypted form, using encryption methods on the University's list of approved encryption methods.

9) Email or file transfer must be performed with the sensitive data encrypted using the University's approved encryption service. If using email, required passwords must be transferred under separate cover/email.

ROLES AND RESPONSIBILITIES

[TOP]

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

DEFINITIONS

[TOP]

Confidential Data - Generalized term that represents data classified as Level 4 - Highly Restricted according to the data classification standard of the University.

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

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.

Data User - Data users are individuals who need and use University information as part of their assigned duties or in fulfillment of assigned roles or functions within the University community.

Level 4 Highly Restricted Data - Refer to the University Data Classification Standard.

Sensitive Data - Generalized term that represents data classified as Level 4 - Highly Restricted according to the data classification standard of the University.

COMPLIANCE

[TOP]

Violations of this standard 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]

ISP-007 Data Classification Standard
NIST SP 800-118

AUTHORITY [TOP]

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

REVISION HISTORY [TOP]

Version	Description	Revision Date	Author
1.0	Standard was approved by CIO and Dean of Library Affairs.	10/17/2014	Director of Information Security