Information Security Management

Policy Statement

It is the goal of Slippery Rock (SRU) to ensure the security, availability, privacy, and integrity of its information technology systems and institutional data and to comply with applicable federal and state statutes and regulations. The purpose of this policy is to support that goal by providing standards for protecting institutional data and defining user and custodial responsibilities for that data. This policy should be used as the basis for any related standards, procedures, and guidelines.

The University will protect the confidentiality, integrity, and availability of university information as well as reduce the risk of information exposure that would damage the reputation of the University.

Procedures

Definitions

The following terms are found within this policy and its associated procedures and guidelines.

Availability –Assurance that a computer system is accessible by authorized users whenever needed.

Confidentiality – An attribute of information; confidential information is sensitive or private information, or information whose unauthorized disclosure could be harmful or prejudicial.

Data Custodian – Individuals officially designated by the President whose position is accountable for the oversight and general operation of data systems that serve the university community.

Encrypt – The process of turning readable text into unreadable cipher text.

Institutional Data – Data created, collected, maintained, recorded or managed by SRU, its staff, and agents working on its behalf. It includes extracts of institutional data, feeds of these data from enterprise systems, and data maintained within so-called shadow or secondary database systems whether derived from enterprise systems or collected or assembled directly by university units.

Integrity – Data or a system remains intact, unaltered, reliable, and available.

Portable Computing Device – Any device used for computing and/or storage of electronic information. This includes portable computers (i.e. laptops and notebooks), smartphones, PDAs, etc, as well as storage devices and media such as flash drives, removable hard drives, CDs, disks, etc.

Principle of Least Privilege – Access privileges for any user should be limited to only what is necessary to complete their assigned duties or functions, and nothing more.

Privacy – An individual's right to be left alone; to be secluded and not intruded on; to be protected against the misuse or abuse of something legally owned by the individual or normally considered by society to be his or her property.

Security – An attribute of information systems that includes specific policy-based mechanisms and assurances for protecting the confidentiality and integrity of information, the availability and functionality of critical services, and the privacy of individuals.

Sensitive Data – Sensitive Data includes information that is protected from disclosure under the law. Sensitive information is often personal in nature but many other types of information such as legal or financial data are also protected.

User – An individual who has been granted privileges and access to institutional computing, network, and data systems, services, applications, resources, and information.

Roles and Responsibilities

Data Custodian

Data Custodians play a critical role in protecting the University's systems and data. Data Custodians are accountable for the oversight and general operation of institutional data systems. They provide direct authority and control over the management and use of institutional data regardless of where the data resides.

Data Custodians' responsibilities include, but are not limited to:

- Ensure compliance with all Slippery Rock University's policies, as well as state and federal statutory and regulatory requirements
- Provide institutional requirements for access to and protection of institutional data in all test, development, and production institutional data systems
- Assign, monitor, and review privileges for access to institutional data
- Ensure appropriate security measures for transmission of institutional data
- Review and recommend changes for procedures surrounding the assignment of access to institutional data
- Coordinate staff and faculty training and development for the proper use of institutional data
- Audit and maintain institutional data
- Delegating object custodianship (authority and responsibility for specific data fields) as necessary to effectively manage use of data systems

- Ensure the accuracy of data reporting; collaborates, when necessary, with other departments in provision of data reports

Data Custodians are as follows:

- Student Data – Registrar
- Financial Aid Data – Director, Financial Aid
- Finance Data – Chief Financial Officer
- Staff and Faculty Employment, Personnel and Workload Data – Director, Human Resources

Object Custodian

An Object Custodian is a university official with delegated operational authority and responsibility for defining, managing, and maintaining the integrity, security, and accuracy of one or more specific data fields (objects) found within SRU's data systems.

Data User

A Data User is any individual (staff, faculty, students, and agents working on the university's behalf) using institutional information technology systems, networks, or data in the conduct of university business.

As a condition of access, institutional data users agree to adhere to the Data User Responsibilities described in appendix A, when they access or are in possession of institutional data of any kind. Data users are required to acknowledge they will adhere to these requirements to the best of their ability for the system(s) to which they require access.

Information Security Standards

General

SRU regards the security and confidentiality of its business data and information to be of significant importance. Each user granted access to institutional data holds a position of trust and must preserve the security and confidentiality of that information.

Access

a. Access Requirements. Access to institutional data:

(1) Is restricted to individuals whose job duties require it;

(2) Is granted only to fulfill the specific functions required to perform a specific job;

(3) Must be approved by both the user's department head and the Data Custodian or designee before requested access is provided.

Data and Object Custodians are expected to use the principle of least privilege when authorizing access to data for which they are responsible. In some cases, Data and Object Custodians may require users to attend formal training before access is granted.

Use of Institutional Data

All institutional data are the property of Slippery Rock University and may only be used by individuals for university business which they are authorized to conduct. Use of this data as it relates to the role or responsibilities of one's position are considered to be routine, and therefore considered an acceptable use.

Under specific conditions, institutional data may also be used for purposes other than official university business. In such cases, use of institutional data may be authorized under other official university policy or related state and federal laws, or with written permission of the Data Custodian responsible for housing and maintaining the data.

It is the data user's responsibility to access and use institutional data in accordance with Slippery Rock University's policy and procedures and State and Federal Laws. If in doubt, data users should contact their supervisor or the appropriate Data Custodian.

Release of Institutional Data

The authority to release institutional data varies depending on the type of data involved and the person or agency to whom the data is released. In most cases, institutional data should only be released according to the guidelines contained in appendix B. Any release of data which does not conform to these guidelines must be authorized by the appropriate Data Custodian.

Protection of IT Systems and Institutional Data

Safeguarding institutional data and data systems requires a combination of personnel security, physical security, and technological security.

a. Personnel security includes restricting access, training users, and administering and complying with this policy.

b. Physical security means taking appropriate measures to secure IT equipment and storage media from unauthorized physical access, vandalism, and theft.

c. Technological security includes all IT equipment, applications, and technologies designed to protect systems and data from compromise.

d. User authentication systems and firewalls are used to restrict access.

e. Virus protection applications help protect systems from malicious software

f. Data encryption helps protect information from being compromised even when it has been accessed by unauthorized persons

Inadequate physical security and lack of data encryption pose a significant threat to the security of institutional data. Storing institutional and other sensitive data on laptop computers or portable storage devices/media significantly increases the potential for data to be fraudulently accessed or misused. Similarly, unattended / unsecured workstations create opportunities for IT equipment to be lost or misused and for the data they contain to be compromised. To protect against the compromise of institutional data, precautions must be taken to physically secure IT equipment and storage media containing institutional data and to encrypt such data when adequate physical security is impractical. Related security requirements are described in appendix A.

Sanctions

The privacy and confidentiality of all accessible data shall be maintained at all times. Individuals who violate this policy may be denied access to institutional information technology systems, networks, and data and may be subject to disciplinary, civil, and/or criminal actions. The university may temporarily suspend, block, or restrict access to institutional information technology systems, networks, and/or data at any time when it reasonably appears necessary to do so in order to protect the integrity, security, or availability of these resources or to protect the university from liability. Slippery Rock University will take any and all actions it deems necessary to resolve violations of this policy. Anyone who violates this policy is subject to disciplinary or legal action as set forth in the Student Conduct Code, SRU employee work rules or Pennsylvania statues.

Responsibility for Implementation

All members of the University Community are responsible for administering this policy.

Scope of the Policy

This policy pertains to all IT systems and networks, and all institutional data. It applies regardless of the environment, media, or device where the data resides or is used, the form or format the data may take, or how the data may be transmitted. This policy applies to all users of institutional IT systems, networks, and/or data including staff, faculty, students, agents working on the university's behalf, and others. his policy applies to all University employees, students, guests and contractors.

Appendix A – Data User Responsibilities

An individual given access to SRU institutional data in any format acknowledges an understanding of and agrees to adhere to the following:

a. Users shall comply with established policies, guidelines, standards, and procedures, including applicable federal and state statutes and regulations.

b. Users shall routinely evaluate their IT security practices based on the requirements of this policy and related guidance.

c. Users shall maintain the security of the systems they use. Users are responsible for all activity that occurs under their information system accounts. Further, users may only share institutional data, in any format, with other users who are authorized to use that data.

d. Users will not share their assigned security access credentials (username and password) for any institutional information technology systems with anyone (this includes supervisors, co-workers, or colleagues). If access to a user's system is required to support the operational needs of the University and the user is unavailable, unwilling, or unable to provide needed information or data, the Office of Information Technology will access the system. A supervisor or manager needing such access shall contact IATS for assistance. To meet the requirements for accessing a system under this section, the following provisions apply:

(1) there must be a need to access specific information or data in support of university operations;

(2) the information or data needed must be reasonably expected to be stored on or accessible through the system in question;

(3) the primary user of the computer or device in question is unavailable, unable, or unwilling to provide the information or data needed;

(4) the vice president or designated representative for the unit involved must approve the access in writing prior to OIT taking action (memo or email approval will suffice);

(5) the provisions of this section shall not be used as a subterfuge to access a system for any other reason; and,

(6) whenever possible, at least two persons shall be present when accessing a system under these circumstances.

Student access to institutional data is generally discouraged. Offices that need student employee access must request individual access for each student and must ensure that the student has received the appropriate training and oversight. Shared usernames for use by multiple student employees in an office will not be granted in any system or application.

Departments must inform the Office of Information Technology immediately when an individual student or employee no longer needs access.

Users and departments will ensure that workstations connected to SRU IT systems are properly maintained and managed to prevent problems that could affect the SRU computing environment.

Users will not leave a workstation unattended while logged into SRU IT systems.

Users will take precautions to protect the security and integrity of data to which they have access.

Users will take precautions to ensure the physical security of IT equipment and media, including:

- Lock offices and rooms containing IT equipment when unoccupied.
- Secure laptops, media, and other IT equipment when not in use.
- Maintain physical control of portable equipment and media.
- Do not leave equipment/media unattended in a vehicle.

Users will take precautions to protect institutional data from being compromised even when IT equipment has been lost or stolen. This includes, but is not limited to:

- Users will store institutional data only on approved network file systems using security settings which prevent anyone other than approved users from accessing the data.

- Users will not store sensitive institutional data on the local hard drive of an office workstation of any type nor move such data to any external media unless approved by the appropriate authority and the file and file system are encrypted.

- Users will not store sensitive institutional data on portable computing devices. In the event there is no alternative to portable storage, data must be encrypted using approved encryption mechanisms provided by the Office of Information Technology. Such local storage on a portable computing device must also be approved by the appropriate Data Custodian.

Users will be held professionally accountable in the event of loss or disclosure of SRU data due to negligence in providing reasonable protection for the data.

Users will comply with institutional requirements, as described in this policy, for sharing and release of institutional data.

When finished working with institutional data that is not subject to records retention guidelines, users should delete and purge electronic files, regardless of format. Similarly, printed documents should be shredded or disposed of in a confidential shredding bin.

Appendix B – Release of Institutional Data

The authority to release institutional data varies depending on the type of data involved and the person or agency to whom the data is released. In most cases, institutional data should only be released according to the guidelines which follow. Any release of data which does not conform to these guidelines must be authorized by the appropriate Data Custodian.

a. To SRU employees: Within the institution, employees may share or disseminate institutional data to other employees who have a legitimate need to access or use the data

b. To external agencies: Employees may release appropriate data, if such activity is defined to be a part of their role and at the direction of their supervisor, to honor requests from appropriate state or federal agencies, legislative bodies, and other applicable agencies

c. Other: Due to the complex nature of laws governing the use of certain types of data, as well as the sometimes complex nature of the data themselves, release of institutional data to persons or agencies other than those described in paragraphs a and b above must be approved by an authorized individual and accomplished in accordance with applicable university policies and State and Federal laws. Authorized individuals, in these cases, may include designated Data Custodians, the Director of Institutional Research, Demography, and Assessment, and the Director of Records Management.

Specific requirements based on the type of data include:

(1) Restricted/Internal/Confidential Data:

Requests for these data must be referred to the appropriate Data Custodian. If necessary, the Data Custodian will work with the Director of Records Management and/or the Director of Institutional Research, Demography, and Assessment to facilitate the release of data. Such data are to be released only by authorized personnel in accordance with University policy. The use of much of the institution's data is covered by State and Federal statutes and regulations (Appendix C) and may be defined as personal, private, or confidential.

Employee personnel information, payroll data, etc. are considered high risk data due to the potential damage that could be caused through unauthorized disclosure, misuse, or modification.

Student data are also considered high risk and are protected under the Family Educational rights and Privacy Act (FERPA) as amended. Faculty and others who have access to student educational records may not release any information contained in a student's educational record to a third party without written consent from the student except as authorized by law. All requests for student information from outside the institution must be referred to Records and Registration Office.

(2) Public Data: To present and interpret institutional data correctly, disclosure of even public data should be done by an appropriate University Official. Although public data may be disseminated freely by such an official, officials should contact the appropriate Data Custodian, the Director of Records

Management, or other appropriate official if they have any doubts or concerns about the release of information.

(3) Electronic Data: Preservation and release of electronic data for litigation is highly confidential. All such activities should be coordinated through the PASSHE Legal Advisor or the designated head of the Lead Unit for the related litigation action.

Appendix C – References

Below are Federal Statutes and Regulations that directly or indirectly affect this policy and operational guidelines referenced within this document. These statutes and regulations are listed here for reference and to demonstrate the volume and complexity of the rules that relate to the use of computers, networks, applications, and data at SRU. There are continual changes and additions, so this list may not be an exhaustive review.

United States Code (USC)

- 5 USC Sec. 552 - Freedom of Information Act (FOIA)
- 5 USC Sec. 552a - Privacy Act
- 15 USC Sec. 6501 - Children's Online Privacy

Protection Act of 1998

- 15 USC Sec. 6801 - Protection of nonpublic personal information
- 18 USC Sec. 1029 - Fraud and Related Activity in

Connection with Access Devices

- 18 USC Sec. 1030 - Fraud and Related Activity in Connection with Computers
- 18 USC Sec. 1362 - Communications Lines, Stations, or Systems
- 18 USC Sec. 2701 - Electronic Communications

Privacy Act

- 18 USC Sec. 2703 - Requirements for Government Access
- 20 USC Sec. 1232g - Family Educational Rights and Privacy Act (FERPA)
- 29 USC Sec. 102 - Employee Retirement Income

Security Act

- 39 USC Sec. 3623 - Mail Privacy Statute
- 42 USC Sec. 200e - Equal Employment Opportunity Act
- 42 USC Sec. 1001 - Communications Assistance for Law Enforcement
- Pub. L. 107-056 - USA Patriot ActAll members and guests of the Slippery Rock University community are expected to comply with this policy and assist with its enforcement.