Acceptable Use Standard

Document Number:	ISP-013	**Version:**	1.2
Document Owner:	Director of Information Security	**Effective Date:**	06/18/2018
Responsible Office:	Office of Information Technology	**Last Update:**	04/07/2023

TABLE OF CONTENTS

PURPOSE [TOP]

The purpose of this standard is to establish acceptable and unacceptable use of electronic devices, information systems, and network resources. The University provides computer devices, networks, and other electronic information systems to meet its mission, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This standard is in place to safeguard the electronic information system user and the University; comply with legal and contractual requirements; and protect the University against damaging legal consequences. Inappropriate use exposes the University to risks including viruses, compromise of network systems and services, and legal issues. This standard requires the users of information assets to comply with University policies, standards, and procedures and protects the University.

SCOPE [TOP]

The scope of this standard applies to all University personnel (see Roles and Responsibilities). This standard applies to all systems that contain or process information related to Southern Illinois University Carbondale (SIUC). In the context of this document, systems include software, hardware, network including the internet, processes, and electronic data, whether on SIUC premises or not, related to SIUC business, whether owned by SIUC or not. Personal devices used to access/interact with University resources are also covered. This standard applies to all activity originating from, directed to, existing on, or traversing the system. 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). It is the responsibility of the University Chief Information Officer, or designee, to determine whether a particular use of computing and network resources conforms to University policy, standards, and guidelines.

STANDARD [TOP]

All members of the University community have a responsibility to use information and information resources in an approved, ethical, and lawful manner to avoid loss or damage to University operations, image, or financial interests and to comply with all official acceptable use policies, standards, and procedures.

Pursuant to this responsibility, users of institutional data and systems related to SIUC shall abide by the standards in this document, in letter and spirit, to establish the appropriate and acceptable use of these data and systems for the purposes of protecting the University and to enable compliance with laws, regulations, policies, requirements, standards, and other appropriate criteria.

The University, and the Office of Information Technology, reserves the right to modify, add, or delete portions of this standard without notice, to protect students, staff, and the University from potential unknown or future security threats and regulations.

Acceptable Use

Acceptable use includes, but is not limited to, respecting the rights of other users, avoiding actions that jeopardize the integrity and security of University resources, and complying with all pertinent licensing and legal requirements.

- Users must comply with applicable laws and regulations, contractual agreements, SIU Board of Trustees and Administrative policies, and license agreements.
- Users must use only University resources that they are authorized to use, only in the manner, and to the extent authorized. Ability to access University resources does not, by itself, imply authorization to do so.
- Users are responsible for protecting their University-assigned accounts and authentication (e.g., password) from unauthorized use.
- Users must abide by the security controls on all University resources used for University business, including but not limited to mobile and computing devices, whether University or personally owned.
- Users of University resources are responsible for the content of their personal communications and may be subject to liability resulting from that use. The University accepts no responsibility or liability for any individual or unauthorized use of its resources by users

Unacceptable Use

Unacceptable use includes, but is not limited to, disrespecting the rights of other users, engaging in actions that jeopardize the integrity and security of University resources, and non-compliance with all pertinent licensing and legal requirements.

- Users are not permitted to share authentication details or provide access to their University accounts to anyone else.
- Users must not circumvent, attempt to circumvent, or assist another in bypassing the security controls in place to protect University resources and data.
- Users must not knowingly download or install software onto University resources which may interfere or disrupt service, or does not have a clear business or academic use.

- Users are prohibited from willingly engaging in activities that interfere with or disrupt network users, equipment, or service; intentionally distribute viruses or other malicious code; or install software, applications, or hardware that permits unauthorized access to University resources.
- Users must avoid excessive use of University resources, including but not limited to network capacity. Excessive use means use that is disproportionate to that of other users or is unrelated to academic or employment-related needs, or that interferes with other authorized uses. Units may require users to limit or refrain from certain activities by this provision. Some exceptions may apply including students residing on campus.
- Users are prohibited from using software for University business that is not licensed by the University and approved by the University Chief Information Officer.
- Users must not engage in inappropriate use, including but not limited to:
  - Activities that violate state or federal laws, regulations, or University policies.
  - Harassment by any means.
  - Widespread dissemination of unsolicited and unauthorized electronic communications including email.
  - Using University resources for unauthorized remote activities.
  - Deliberately causing system failure, disruption, or compromising system security.
  - Intentionally obscuring, changing, or forging of the date, time, physical source, logical source, or other label or header information on data or electronic communications.
  - Unauthorized interception of electronically transmitted information without prior written authorization from the Chief Information Officer or designee.
  - Performing an act which will adversely impact the operation of computers, terminals, peripherals, or networks. This includes, but is not limited to, tampering with components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer.

Control and Licensing of Software

1. All software used on University resources and to conduct University business shall be procured in accordance with official University policies and procedures, and shall be licensed, and registered in the name of the University.

2. All users are expected to comply with all intellectual property laws including copyright law.
3. Users may not copy, distribute, display, or disclose third party proprietary software without prior authorization from the licenser. Proprietary software may not be installed on systems not properly licensed for its use. The University does not condone or authorize the copying or possession of illegal software. University students and employees are prohibited from copying software illegally and possessing illegal copies of software, whether for course-related, job-related, or private use. Any violations of this policy are the personal responsibility of the user. The University assumes no liability for such acts.
4. Any user who suspects or has knowledge of copyright or intellectual property law violations, must immediately report this activity to the University Chief Information Officer. Failure to report such activity will be considered a violation of the Acceptable Use Standard.
5. Any new software proposed for adoption to fulfill a business need of the university or needing integration with other university systems must be vetted and authorized by the Chief Information Officer or designate.

Privacy and Security Measures

Users must not violate the privacy of other users. Technical ability to access others' accounts does not by itself imply authorization to do so.

The University takes reasonable measures to protect the privacy of its information technology resources and accounts assigned to individuals. However, the University does not guarantee absolute security and privacy. Users should be aware that any activity on information technology resources may be monitored, logged and reviewed by University-approved personnel or may be discovered in legal proceedings.

The University assigns responsibility for protecting its resources and data to the Chief Information Officer, Chief Information Security Officer, system administrators, and data custodians, who treat the contents of individually assigned accounts and personal communications as private and does not examine or disclose the content except:

1. As required for system maintenance, or trouble shooting, including security measures;

2. When there exists reason to believe an individual is violating the law or University policy; and
3. As permitted by applicable policy or law.

Individual Privacy

The University reserves the right to employ security measures. When it becomes aware of violations, either through routine system administration activities or from a complaint, it is the University's responsibility to investigate as needed or directed, and to take necessary actions to protect its resources and to provide information relevant to an investigation.

1. Users are authorized to access, use, copy, modify, delete or grant others access to their personal files or data, as specified in this policy. However, users are not authorized to perform any of these functions on another user's account or a university system unless specifically authorized by the account holder, job description, the Chief Information Officer or designee, or the appropriate system administrator.
2. Users may not monitor another user's data communications.
3. User privacy is not to be violated. However, user privacy is subject to all university policies. As such, authorized individuals may access and disseminate private information in performance of their official job duties. Unauthorized personal use of a user's private information is prohibited.
4. Failure to protect the privacy of others by intentionally or unintentionally permitting access to systems or data is unacceptable. Violations of this requirement include, but are not limited to:
    - Leaving confidential or protected information accessible where it could be viewed by unauthorized individuals.
    - Giving a password to an unauthorized user.
    - Leaving a password where it can easily be found.
    - Allowing someone to use a system signed on under another user's password.
    - Knowingly failing to report a password that has been used by an unauthorized user, with or without permission.
    - Leaving a system signed on and accessible while unattended.

ROLES AND RESPONSIBILITIES [TOP]

All SIU personnel including, but not necessarily limited to, students, faculty, staff, retirees, outsourced contractual workers, guests, volunteers, temporary extra help, student workers, graduate assistants, undergraduate assistants and vendors are required to abide with the requirements and standards established within this standard.

DEFINITIONS [TOP]

Access Rights – Permission to use an SIUC information technology resource according to appropriate limitations, controls, and guidelines.

Confidential Data – A 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 operational responsibility for information assets.

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.

Inappropriate Use of Authority or Special Privilege – Use of one's access right(s) or position in a manner that violates the rules of use of those privileges as specified by the Chief Information Officer, or designee, or the appropriate system administrator.

University Resource – Any information technology/network equipment, facility or service made available to users by Southern Illinois University Carbondale.

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

Password – A word or string of characters that a user must supply to prove identity or access approval in order to meet security requirements before gaining access to a particular information technology resource, which is to be kept secret from those not allowed access.

Remote Activity – Any information technology action or behavior that accesses remote site facilities via a University resource as well as any information technology action or behavior that remotely accesses University resources from a non-University resource.

System Administrator – Any individual authorized by the Chief Information Officer, the Provost/Vice President, or a designee to administer a particular information technology hardware system and its system software.

Unauthorized Act – Except information technology actions or behaviors permitted in this policy, any act performed without the explicit permission of the Chief Information Officer, or designee, or the appropriate system administrator.

User – Any individual whether student, staff or individual external to SIUC -- who uses SIUC information technology resources.

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

AUTHORITY [TOP]

Southern Illinois University Board of Trustees Policy, SIU System Information Security Plan.
Southern Illinois University Carbondale Information Security Program (ISP).

REVISION HISTORY

[TOP]

Version	Description	Revision Date	Reviewed By
1.0	Standard was approved by CIO.	06/15/2018	Director of Information Security
1.1	Reviewed. Fixed broken links.	06/21/2019	Director of Information Security
1.1	Reviewed. Updated links.	03/04/2020	Director of Information Security
1.2	Reviewed. Clarified Individual privacy, bullet 4 to be inclusive of personal and departmental accounts	03/30/2021	Director of Information Security
1.2	Reviewed. No changes.	04/12/2022	Acting Director of Information Security and Associate Director, PMO
1.2	Reviewed, no changes needed.	04/07/2023	Interim Director, Information Security