F.27 Use of Data Communications and Computers

Date
10/23

I. **Purpose**

The University of Southern Indiana Information Technology (IT) Department provides computer access and capabilities for the University. The University relies heavily on various systems to meet educational, operational, and informational needs. It is essential that USI's computer systems, computer networks, and the data they store and process be operated and maintained in a secure environment and in a responsible manner. These computer systems, networks and data must be protected from misuse and unauthorized access.

This policy applies to all University computer users and systems regardless of type of hardware. In particular, this policy covers computer systems ranging from desktop and laptop personal computers, servers, tablets, and smartphones, whether hardwired to the network or connected via wireless.

In addition to this data communications and computer use policy, users of these computer systems are subject to applicable state and federal laws as well as the rules and regulations of the University.

Computing resources are valuable and their abuse can have a far-reaching negative impact. Computer abuse affects everyone who uses computer systems and computer networks The same moral and ethical behavior that applies in the non-computing environment applies in the computing environment.

The University will ensure that all users are aware of the policy by publishing it on the web and by making copies available at the IT Help Desk.

II. **Definition of Terms**

A. Computer Systems
Computer systems include any type of device, such as desktop or laptop computers, tablets, smartphones, or servers, used on this campus either on wired or wireless networks.

B. Computer Networks
Computer networks include any wired or wireless local or wide-area communication system connecting computer systems as defined above.

C. Computer Users, referred to here-in as Users
Computer users are defined as students, employees, alumni, retirees, guests, and recognized organizations.

III. **Computer Use Guidelines**

Each user is provided an individual university account with a user name and password. This account is intended for the specific user only and this user is responsible for activities with the account. Most users are also provided an email account, licensed access to business software, and centralized file storage.

In general inactive accounts lose access to email, licensed business software and centralized file storage. Alumni and retirees are eligible to retain email only. Upon request, retirees with emeritus status may retain access to licensed business software and centralized file storage.

An account is considered inactive when:

- Account owner is no longer an active employee

- Account owner is deceased
- Retiree does not use email for 12 months
- Alumni does not use email for 12 months
- Student account is not enrolled for 2 consecutive academic terms
- Account owner is no longer an active guest

An account may also be disabled upon request from Human Resources or Dean of Students.

Users are to have valid passwords for computers systems, network systems, and software applications. It is the responsibility of all users to safeguard their passwords. Passwords must be changed as needed to ensure security; a good practice is to change your password every 90 days.

Employees must log off of their computer, or lock the screen with a password protected screen saver, when the employee will be away from their computer for any extended amount of time. When a business reason exists to bypass screen locking, a waiver must be requested from the Information Technology Chief Information Security Officer.

Users may not change, copy, delete, read, or otherwise access files or software without permission of the owner of the files or the system administrator. Users may not bypass accounting or security mechanisms to circumvent data protection schemes. Users may not attempt to modify software except when intended to be user customized (i.e., user's data files).

Users must not use the computer systems to violate any rules in the University Handbook, University codes of conduct, or any local, state, or federal law.

Legitimate use of resources does not extend to whatever one is capable of doing with them. Although information security controls may permit access, a person may not access confidential information unless they have some legitimate reason for doing so. For example, employees with access to confidential student records have no right to access them absent an approved legitimate business purpose.

A user shall disclose to the appropriate authorities misuses of computing resources or potential loopholes in computer systems security, and cooperate with the Chief Information Officer (CIO) in the investigation of abuses. Anyone who discovers or suspects an information security breach of the University has a duty to report the suspected breach to IT Security by e-mail at it@usi.edu or by phone at 812-465-1080. Reporting must not be delayed in order to collect more information or to make a determination if a breach has actually occurred.

In connection with inquiries into possible abuses, the University reserves the right to examine network data traffic, files, programs, passwords, accounting information, printouts, email, or other computing material without notice.

The University reserves the right to limit bandwidth on a per connection basis, monitor traffic, and log communications to ensure proper usage of network resources.

The University reserves the right to charge fees for data communications access, data, and networked applications.

Without specific authorization, users of University Computer Systems must not cause, permit, or attempt any destruction or modification of data or computing or communications equipment. This rule protects data, computing, and communications equipment owned by USI, or any other person or entity. 'Specific authorization' refers to permission by the owner of the equipment or data to be destroyed or modified.

Unacceptable Activities

1. Attempting to access another user's computer files without permission.

2. Supplying or attempting to supply false or misleading information or identification in order to access another user's account.
3. Deliberate, unauthorized attempts to access or use University computer systems, , programs, or data. Users must not defeat or attempt to defeat any University system security, for example, by "cracking" or guessing user identification or passwords.
4. The unauthorized capturing of computer network data directly from the computer networks, including wireless transmissions.
5. Attempting unauthorized access to computers outside the University using the University Computer Systems or Computer Networks.
6. Intentionally sending either e-mail or a program that replicates itself (i.e., a virus or worm) or damages another user's account, computer, or operating system.
7. Recreational game-playing and/or audio/video file sharing that interferes with instructional or work-related use of university-owned computers.
8. Using computer accounts for work not authorized for that account.
9. Sending chain letters or unauthorized mass mailings.
10. Using the computer for commercial purposes not supporting USI.
11. Using the computer for illegal purposes (e.g. using email to instigate phishing or hacking attacks).
12. Sending of abusive, harassing, or obscene messages via electronic devices.
13. Mass emailing for selling, soliciting, or spamming other users.
14. Running unauthorized servers or daemons, i.e., SMTP, DNS, DHCP, etc., on the network.
15. Denying service through any action.
16. Running any unauthorized data packet collection program on the network.
17. Attaching any devices to the network without registration or prior approval from the IT Department.
18. Unreasonably slowing down the University Computer Systems or Computer Networks through the excessive use of system resources (network bandwidth, disk space, CPU time, and printer queues).

IV. Acceptable Personal Use

The University of Southern Indiana encourages Information Technology literacy for its computer users. As such, the University of Southern Indiana allows its electronic mail system and web server(s) to be used by computer users for reasonable and limited personal use. For example, occasionally sending electronic mail to family and friends is allowed. However, it is recommended that users maintain a personal email account. In all cases, "Personal Use" must conform to the guidelines established elsewhere in this document and must not interfere with the normal operation of the network.

The University provides individual web pages for faculty with active roles. These pages are for professional representation and must follow established Web Services and college guidelines. USI does not actively monitor or generally restrict the content of materials published on the faculty web pages. However, the use of USI resources is a privilege and not a public forum. Therefore, USI reserves the right to restrict or deny usage of the web server space when such usage does not support the mission of the University.

In order to avoid jeopardizing the University's tax-exempt status, computer facilities and services may not be used for personal financial gain or in connection with political activities, without prior written approval in each instance. Contact the vice president for Finance and Administration for detailed information.

V. Copyright Issues

The University owns licenses or leases to a number of proprietary programs. Users who redistribute software from the computing systems break agreements with software suppliers and violate applicable federal copyright, patent, and trade secret laws. Therefore, the redistribution of any software from computing systems is strictly prohibited except in the case of software that is clearly marked as being in the public domain. Leased software may be made available to faculty, staff, administrators, alumni, and retirees for work related purposes.

VI. Peer-to-Peer File Sharing

In full compliance with the Higher Education Act on Copyright Infringement, the unauthorized distribution of copyrighted material, such as through peer-to-peer (P2P) networks, is not permitted. The University implements

several technologies to block or inhibit peer-to-peer file sharing of copyrighted material. Additionally, encrypted peer- to-peer file sharing is not permitted and is blocked. Peer-to-peer file sharing of copyrighted material may subject the violator to civil and criminal penalties.

- The U.S. Copyright Law (http://www.copyright.gov/title17/) provides for damages as follows: Actual damages and profits or
- $750-$30,000 for each copyrighted work (song, movie, game, etc.) or
- $750-$150,000 for each copyrighted work if the infringement was committed willfully
- Criminal penalties for certain copyright violations

Copyright infringement is unlawful and thus a violation of the Employee Code of Conduct and Student Code of Conduct. If the University receives a notice that the IP address assigned to an employee has been identified as one that is receiving or distributing unauthorized copies of copyrighted material, the employee will be subject to appropriate disciplinary action. The employee must certify that all unauthorized material has been removed from University resources.

If the University receives a notice that the IP address of a device that is registered by a student has been identified as one that is receiving or distributing unauthorized copies of copyrighted material, this device will be blocked from accessing the campus network and the student will be required to certify that all unauthorized material has been removed before that privilege is restored. Judicial procedures and sanctions will apply.

For both employees and students, financial penalties, fines, damages, or other legal fees assessed for the illegal activity by the patent holder will be charged to the employee or student.

Under the law, the University could also be required under subpoena to release your name to appropriate authorities.

When technology makes it easy to abuse the rights of others, it may be tempting to engage in such behavior. Resist the temptation and use only legal downloading sites. As an alternative to illegal downloading, there are now many online sources that provide free and fee-based legal access (i.e. Amazon, Netflix, Hulu, etc.).

VII. General Terms and Disclaimers of Liability

Responsibility for all information transmitted via the Computer Network at USI lies with the user or the information provider.

Neither USI nor the IT Department make any warranty, expressed or implied, concerning the accuracy or fitness for any purpose of any information distributed by the Computer Network. Such warranties may or may not be expressed by information providers. Programs provided for use on the Computer Network have been tested for proper Computer Network functionality; however, the IT Department cannot guarantee their suitability for any specific user's purposes.

VIII. Enforcement and Penalties

Abuse or misuse of computing resources may not only be a violation of this policy, but also may violate criminal statutes. Therefore, the University will take appropriate action in response to user abuse or misuse, of Computer Networks or Computer Systems. The University may refer enforcement issues to the appropriate dean, administrator, or the IT Advisory Committee.

When instances of improper use are identified, the University will investigate and may take action to prevent further occurrence.

During an investigation, the University reserves the right to copy and examine any files or information resident on University systems allegedly related to the improper use, including the contents of electronic mailboxes. Human Resources or the Dean of Students is responsible for identifying and requesting email eDiscovery or litigation hold placements. When Information Technology receives a hold notification, the data and email of the hold are quarantined. Investigations that discover improper use may cause the University to:

1. Limit the access of those found using Computer Networks or Computer Systems improperly.
2. Disclose information found during the investigation to other University offices and authorities, and to civil and law enforcement authorities.
3. Begin disciplinary actions as prescribed by University policies and procedures.
4. Install automatic measures to limit proper use.
5. Require reimbursement for resources consumed or damaged.
6. Require reimbursement of any financial penalties, fines, damages, or other legal fees assessed to the University.
7. Take other legal action including recovery of damages