

Information Technology: Acceptable Use

Section I: Access to Information Technology Facilities

A.

To protect the integrity of the University's information technology facilities and the users thereof against unauthorized or improper use of those facilities, MSU reserves the right, without notice, to temporarily limit or restrict any individual's use and to inspect, copy, remove, or otherwise alter any data, file, or system resource which may undermine the authorized use of any information technology facility.

B. Investigation and Review of Policy Infractions

1. University sanctions are imposed by the appropriate university authority and may include, but are not limited to, limitation or revocation of access rights and/or reimbursement to the university for all costs incurred in detecting and proving the violation of these rules, as well as from the violation itself.
2. Users must use only those information technology resources which the University has authorized for their individual use. The unauthorized use of information technology resources or providing false or misleading information for the purpose of obtaining access to information technology facilities is prohibited and may be regarded as a criminal act and will be treated accordingly. Users may not use university information technology facilities to gain unauthorized access to other institutions, organizations, or individuals.
3. Failure to comply with one or more of the specific requirements of this policy may jeopardize access to or use of Murray State facilities and services and could result in a review and investigation into the identified violation.
4. Supervisors of systems and facilities have the authority to immediately terminate any program or access that is suspected to be inappropriate or detrimental to operations.

C. Control and Licensing of Software

1. All users are expected to comply with all intellectual property laws including copyright law.
2. Users may not copy, distribute, display, or disclose third party proprietary software without prior authorization from the licensor. 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 is the personal responsibility of the user. The University assumes no liability for such acts.
3. 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 Information T

- a. Leaving confidential or protected information on a screen where it could be viewed by unauthorized individuals
- b. Giving a personal password to someone else
- c. Leaving a personal password where it can easily be found
- d. Allowing someone to use a system signed on under a personal password
- e. Knowingly failing to report a personal password that has been used by another person, with or without permission
- f. Leaving a system signed on and accessible while unattended

E. Confidentiality

1. The unauthorized release of any personal or confidential information may violate state and federal law and will not be tolerated. Failure to protect confidential information is unacceptable.
 - a. Users are responsible for their information technology accounts they should maintain secure passwords and take precautions against unauthorized access to their information technology resources. Users may be charged with a violation if someone uses their accounts inappropriately.

F. General Security

1. General security infractions include, but are not limited to:
 - a. Using information technology resources for unauthorized remote activities
 - b. Deliberately causing system failure, disruption, or compromising system security
 - c. Intentionally obscuring, changing, or forging of the date, time, physical source, logical source, or other label or header information on data or electronic communications
 - d. Unauthorized interception of electronically transmitted information without prior written authorization from the Chief Information Officer or designee
 - e. 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

Section III: Copyright and the Use of MSU s Information Technology Resources

A. General Copyright Principles

1. The nature and purpose of copyright in general.
 - a. Copyright protections are intended to promote progress in science and the arts and to stimulate the production and publication of enlightening and creative matter.
 - b. Books, periodicals, musical works, motion pictures, sound recordings, computer programs, and photographs are examples of materials or works which may be protected by copyright.
 - c. The rights afforded to the holder of a copyright include the exclusive rights to copy and distribute the work to which the copyright applies.
 - d. It is not the purpose of this policy to discuss copyright principles in detail. Helpful

contains relevant materials such as “Copyright Basics” and “Frequently Asked Questions” as well as links to various publications which cover a wide array of topics.

infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit MSU to locate the material or reference or link.

IV. Information reasonably sufficient to permit MSU to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

V.

1. Penalties under the law for copyright infringement.
 - a. Users may be sued for their infringing activities. Acts can be infringing and result in civil penalties even though there is no intent to violate a copyright. Under certain circumstances, the infringer may be responsible for the other party's attorney's fees. Statutory civil damages can be as high as \$150,000 for each work infringed if a violation is committed willfully.
 - b. Willful copyright infringement can also be a crime. Even a first time offense can carry a prison term of from 1 to 5 years plus fines depending upon the facts and circumstances.
2. Institutional penalties.
 - a. Procedures are discussed above with respect to notifying MSU of the presence of infringing materials on its website.
 - b. The procedure for handling complaints against any individual suspected of violating this policy regarding copyright and the use of MSU's Information Technology Resources is described in Section V.
 - c. Users of MSU Information Technology Resources who engage in activity contrary to this copyright policy, including unauthorized p2p file sharing, will be disciplined.
 - d. Complaints against students should be referred to the Vice President for Student Affairs.
 - i. Such referral may result in proceedings before the University Judicial Board.
 - ii. Sanctions which may be imposed against any student violating this policy include, depending upon the circumstances, referral to alternative services, warning, loss of privileges, probation, restitution, a program of self-improvement and education, recommendation of suspension, and recommendation of expulsion.
 - e. Complaints against faculty and staff who violate this policy will be handled in accordance with established university policy or practice.
 - i. Penalties assessed against faculty and staff who violate this policy may include written warning, loss of privileges, suspension of employment, and termination of employment depending upon the circumstances.
 - ii. Complaints against employees subject to receipt of employee disciplinary reports will be handled in accordance with provisions of the *Personnel Policies and Procedures Manual* regarding employee discipline. The severity of the violation will be taken into account in assessing any penalty.
 - iii. Established grievance procedures will be utilized to review any penalty imposed.
 - iv. Temporary or permanent loss of access to MSU's information technology resources may occur with a first violation of this policy. In appropriate circumstances, repeat offenders will permanently lose access.
 - f. In the event MSU becomes aware of a user's alleged violation of this policy, it may take advantage of the provisions regarding "Protection of Information Technology Resources and Institutional Data" and "Investigation and Review of Policy Infractions" found in Section II above.
 - g. As provided under Section II, under "Control and Licensing of Software," any user

D. Periodic Policy Review

1. This policy related to copyright and the use of MSU's Information Technology Resources will be reviewed periodically in order to assure that it addresses the changing needs and concerns of Murray State University and to remain compliant with law.
2. The Information Technology Advisory Committee will perform the periodic review stated in the preceding paragraph by applying assessment criteria it deems relevant.
 - a. It is authorized to revise and/or implement new policies under this Section III upon approval of the President of the University

A. Procedure for Reporting Violations

1. Violations should be reported to the faculty/immediate supervisor of the individual, the Chief Information Officer, or the administrator responsible for the system that was breached or misused. The notified party will inform the appropriate university official. Violations may result in one or more of the following actions:
 - a. Verbal or written warning with reference to appropriate policy
 - b. Suspend access either temporarily or permanently
 - c. File a formal Employee Disciplinary Report (EDR), if the individual is an employee
 - d. Formally submit student infractions to the Vice President for Student Affairs
 - e. Consult with the University Attorney and/or Public Safety, who may file civil or criminal charges.
 - f. Refer complaints of harassment or discrimination to the Office of Equal Opportunity
 - g. For any individuals outside of the immediate university community, send a written notice of the infraction to the employer, principal, or entity that initiated access for that person

B. Procedure for Appeal

1. Appeals may be filed using existing procedures for staff, faculty, and students. All other appeals will go to the Vice President for Administrative Services for disposition.

Section VI: Administration of Policy

A. Procedure for Development, Review and Modification of this Policy

1. The Policy Review Subcommittee of the Information Technology Advisory Committee will be a body comprised of at least four members of the larger committee in addition to the Chief Information Officer. The Policy Review Subcommittee will meet at the call of the Chief Information Officer.
2. Proposals for new policies and/or modifications to existing policies will be forwarded to the Chief Information Officer. The proposals and comments will be brought before the ITAC Policy Review Subcommittee by the Chief Information Officer.

B. Communication of Policy

1. Signature on an account application form, acceptance of a user ID, or online registration denotes that the applicant has read and understands the guidelines available and also denotes acceptance of the Information Technology Acceptable Use Policy.
2. The policy is available online at <http://campus.murraystate.edu/aup/> and in print form in Waterfield Library.

C. Other Information Technology Policies

1. Departments with their own information technology labs will adhere to the same general operating guidelines as established by this policy.

Glossary of Terms

T

•

