Policy Title: IT6003 - Acceptable Use of Information Technology Resources

Subject Area: Information Technology

Responsible Official(s): Chief Information Officer

Responsible Office(s): Information Technology Services

Policy Statement

In keeping with the spirit of free intellectual inquiry that is fundamental to our mission, the principles of academic freedom and individual privacy will be respected by the University as outlined in this policy. In turn, all users of the University's information technology resources are expected to demonstrate the highest respect for the rights of others in their use of these resources. **Access to the University's information technology (IT) resources is a privilege. This privilege may be limited or revoked if an individual violates University policies or state or federal laws.**

This policy applies to all information technology resources provided by the University and to all users of these resources. All members of the University community are given notice of this policy by virtue of its publication and are subject to it on the same basis. Ignorance of this policy does not relieve any user of his or her responsibilities under the policy. **All users are expected to familiarize themselves with the contents of this policy and act in conformance with the following principles regarding any use of the University's IT resources.**

Definitions

Users – All University faculty, staff, students, contractors, vendors, guests, and volunteers who access any University information technology systems or resources.

Hack - An unauthorized access to a computer or service. This access may include modifications to programs or other unauthorized activities.

Malware **-** Software designed to negatively impact or impair performance of computers or networks. May include intrusive pop-up ads, malicious and/or damaging software, virus programs, worms, Trojans, scareware, ransomware, etc. May result in loss or theft of data.

Eradication may require use of specialized tools or complete erasure and rebuilding of computer operating system. May be introduced by opening dubious email attachments, visiting dubious websites, or installing infected software.

Peer-to-Peer File Sharing **-** A software program that automatically discovers and/or shares files with peers on a network. Although there are legitimate peer-to-peer file sharing programs, some of these programs are used for unlawful activities, such as sharing music and videos that are protected by copyright.

Policy

User Access - Principle I

User access to information technology resources is granted to an individual by the University solely for the grantee's own use. User access privileges must not be transferred or shared, except as expressly authorized by an appropriate University official.

This principle is intended to help protect the integrity, security, and privacy of user accounts. Sharing access with another individual undermines the security of an account, leaving it vulnerable to abuse by others. Sharing or transferring access may also jeopardize the security of the University's entire information technology system. Keeping passwords secure and attending to an account while logged on are fundamental to the security of an account.

Not sharing access privileges also helps protect against unauthorized activities on an account for which an individual could be held personally responsible. For example, if someone else uses an account **with the account holder's permission** and violates University policy, including the Student Code of Rights and Responsibilities, the account holder can be charged with the violation and made subject to the same student or employment disciplinary action as the actual user.

Students **should not** share account information and/or passwords with any other users. University employees should not share passwords with any other employee unless expressly authorized to do so by the appropriate University authority with responsibility for the account.

For information and assistance about obtaining and/or maintaining a University IT account, contact the University's IT Service Desk at 901-678-8888.

User Privacy, Integrity and Operational Security - Principle II

The privacy of all users and the integrity and operational security of the University's information technology system must be respected by all. University IT resources must not be used to attempt unauthorized access to information maintained by users or by the University.

This principle is intended to apply to all aspects of the University's information technology system, and to all Users. The University's IT resources must not be used to gain unauthorized access to information, even if that information is not securely protected or is otherwise available. The fact that an individual account and its data may be unprotected does not confer either an ethical or legal right to access it.

Users have no reasonable expectation of privacy in the use of University's resources. However, restricted data as defined in the University's Data Classification shall be protected in accordance with federal guidelines and regulations requiring reasonable and appropriate protections.

The University does not routinely monitor electronic communications, electronic activity, or electronic data for specific users. The University may monitor electronic communications or electronic activity while protecting University information. Investigations of misuse, unauthorized use or illegal activity, as well as routine or emergency maintenance of the University's IT system, may require observation of communications or information by appropriate and authorized university officials, employees, or their authorized agents.

Electronic records sent, received, or stored on computers owned, leased, or administered by the University are the property of the University. As the property of the University, the content of such records, including electronic mail, is subject to inspection by University personnel. The University is able and reserves the right to monitor and/or log all network activity of users without notice, including all email and Internet communications. Such activities are not in violation of this principle so long as these activities are conducted by authorized individuals on behalf of the University. University employees conducting these activities sign a Confidentiality Agreement as part of their new hire orientation. Other authorized agents of the University are subject to contractual language requiring protection of University data.

Unauthorized access to information constitutes a violation of this principle, and may result in serious disciplinary charges under the Academic Misconduct up to and including expulsion, and/or employment discipline, up to and including termination. Violation of this principle may also constitute a violation of state or federal law.

Examples of activities that may violate this principle.

Shared Resources - Principle III

Information technology resources are *shared* resources that must be available to all users in an equitable manner. Users must not engage in any behavior or activity that unreasonably

interferes with the access privileges of other users or with the University's ability to provide access to these resources for its entire community of users.

Information technology resources are finite and must be shared. The University's commitment to the principle of fair and equitable access for all users requires that users refrain from activities that compromise its overall ability to deliver IT services or that interfere with its ability to make IT resources available for all qualified users. This principle involves every aspect of the University's IT services and infrastructure, ranging from such diverse activities as unauthorized network connections through disruptive behavior in University computer labs that interferes with the rights of other lab users. The University reserves the right to take all appropriate and reasonable measures, including the use of available technological measures (e.g., limiting the amount of available bandwidth) to ensure equitable access to IT resources for the benefit of all users.

Examples of activities that may violate this principle.

Misuse of IT Resources - Principle IV

Users must not use University information technology resources in the commission of any illegal or otherwise unauthorized act. Violation of state or federal laws, including anti-hacking provisions, copyright, and trademark laws, is inconsistent with the ethical and responsible use of University IT resources and is strictly prohibited.

Users agree to strict adherence to this principle through their use of University IT resources. In addition to possible civil and criminal penalties, illegal use can result in sanctions under University Policy GE2006 - Copyrighted Materials, Use of, and the Student Code of Rights and Responsibilities.

Examples of activities that may violate this principle.

Conduct and Behavior - Principle V

Users should observe the same standards of ethical conduct and courteous behavior that govern non-electronic vocal and written communications and other personal interactions whenever they use the University's IT resources.

Ethical and courteous use of information technology resources is the responsibility of every user. This principle is fundamental to the spirit of community and standards of civility that should govern interactions among all members of the University community.

While this principle applies to all users under any circumstances, it is particularly important that students using University owned computers in labs or other University controlled areas conform to this policy and all other applicable University policies or regulations, including Student Code of Rights and Responsibilities and the Computer and Lab Guidelines.

Employees of the University also have a special ethical duty to use their broad access to the University's information technology resources in conformance with this and all other principles of this policy. Use of information technology resources by University employees that is unrelated to their official position should be reasonable and limited in both time and resources and must not interfere with University's functions or the employee's performance of employment responsibilities.

Examples of activities that may violate this principle.

Unauthorized Commercial Use - Principle VI

Users may use University information technology resources for any authorized commercial purposes pursuant to University policy HR5011 – Extra Compensation and Outside Employment.

The University's IT resources are provided in support of the University's educational, research and service missions; therefore, uses that are consistent with this purpose must always receive the highest priority. Other uses, such as those that indirectly support this mission, including reasonable and limited personal use, while permissible, must necessarily receive a lower priority. Unauthorized commercial use of university resources is inappropriate and inconsistent with the University's mission.

Examples of activities that may violate this principle.

Peer-to-Peer File Sharing - Principle VII

Users may not install or use any unauthorized Peer-to-Peer File Sharing device to share or distribute:

- copyrighted material without authorization from the copyright owner.
- privileged, private, or strategic information determined by cognizant administrators as vital to the operation of the University.
- any malware, copyrighted software, or license keys.
- software that threatens or disrupts any University of Memphis computing services.

Peer-to-peer file sharing programs may pose opportunities for significant loss to owners of copyrighted material and significant liability to the University. Allowing non-authorized access to computers on the University network may provide access to privileged information. Peer to peer programs degrade the speed of the network, and they may contain malware or exploits that may allow unauthorized access to the machine hosting the program. These programs also contribute to network slowdowns and may provide backdoors to hackers with additional resources to launch attacks.

Use of Personally Licensed Software - Principle VIII

This principle ensures the protection of University data, in accordance with IT6005 – Data Security Policy, and maintain the security, compliance, and operational integrity of University-owned systems per IT6004 – Security and Protection of Electronic Information Resources. Users should not use software licensed to an individual on University-owned devices, including desktops, laptops, servers, and virtual machines, to conduct University business when University data will be stored or accessed, university electronic resources could be put at risk, or University processes could be negatively impacted.

Examples of activities that may violate this principle.

Response to Violations

Violation of this policy may result in action by the appropriate University official. Students who violate this policy may be referred to the University's Office of Student Accountability for disciplinary action under the Student Code of Rights and Responsibilities. Employees who violate this policy may be subject to disciplinary measures imposed by their appropriate supervisor in consultation with the University's Human Resources Office. Violations of state or federal laws regarding unlawful access or use may be referred to the appropriate law enforcement officials for investigation and/or prosecution.

University Sanctions

Sanctions may include, but are not limited to, limitation or revocation of access rights and/or other sanctions up to and including suspension or expulsion for students, and termination for employees. Sanctions may also include restitution to the University for charges incurred in detecting and substantiating violations of these rules, as well as any costs incurred because of the violation itself. Users should be aware such charges could be substantial. The process for the collection of violation charges can be found in Employee Debt and in Delinquent Accounts.

Investigation and Review of Charges

When the Chief Information Officer, or designee, or the appropriate system administrator has reason to believe that a violation involving a security threat to the system or other users and/or illegal activity may have occurred, he or she may immediately suspend information technology privileges for the involved user(s).

If a user account is summarily suspended, the University will immediately attempt to notify the user. Users may check the status of reinstatement of access privileges by contacting the University's IT Service Desk at (901) 678-8888. If, upon further investigation by the appropriate University officials, the violation appears to have been willful and deliberate, the appropriate University official may refer the violation and the violator's identity to the appropriate University official for disciplinary action.

FAQs

What are activities that may violate Principle II - User Privacy, Integrity, and Operational Security?

Examples of activities that may violate this principle, include, but are not limited to the following:

- Hacking or attempted hacking activity of any kind, including but not limited to:
    - Altering, damaging or attempting to alter or damage files or systems without authorization
    - Intentionally damaging or destroying the integrity of electronic information
    - Attempting to access or control another computer network without authorization
    - Scanning of networks for security vulnerabilities
- Unauthorized access of another user's account in any manner
- Unauthorized viewing of information maintained on University systems
- Publishing, sharing, or disseminating information from University's systems without appropriate authorization

What are activities that may violate Principle III - Shared Resources?

Examples of activities that may violate this principle, include, but are not limited to the following:

- Intentional disruption of the IT system, including without limitation, installing, propagating, or otherwise running any malicious program that attempts to violate the operational integrity of the system (e.g. malware).
- Failure to comply with requests from appropriate University employees to discontinue activities that threaten the operational integrity of any component of the IT system
- Unauthorized connections to the system, its networks, as well as unauthorized extensions or re-transmissions of any system services.
- Continuing to download or upload large files during periods of peak usage after having received a request from the appropriate University IT official to defer such use until a later time
- Intentional physical damage to University's owned IT resources.

What are activities that may violate Principle IV - Misuse of IT Resources?

Examples of activities that may violate this principle, include, but are not limited to the following:

- Hacking activity of any kind.
- Unauthorized upload, download, or other digital reproduction of copyrighted materials, including documents, software, music, and films.
- Unauthorized storage of copyrighted materials, including documents, software, music and films, on University's owned or controlled IT resources.
- Misrepresentation of one's identity.
- Electronic distribution of threatening or illegally harassing communications.
- Unauthorized interception of electronically transmitted information.

What are activities that may violate Principle V - Conduct and Behavior?

Examples of activities that may violate this principle, include, but are not limited to the following:

- Repeated, unsolicited, or unwanted electronic communication with an individual after the sender has been asked to stop
- Misrepresentation of the identity of the sender of an electronic communication or web site host
- Obscuring or forging of the date, time, physical source, logical source, or other header information of a message or transaction
- Alteration of the content of a message originating from another person or computer with the intent to deceive
- Acquiring or attempting to acquire the passwords of other users
- The unauthorized deletion of another user's postings, files, etc.
- Using IT resources while on duty for the University in a manner that interferes with performance of employment responsibilities.
- Inappropriate use of University's authority or special access privileges to the University's system

What are activities that may violate Principle VI - Unauthorized Commercial Use?

Examples of activities that may violate this principle, include, but are not limited to the following:

- Using University hosted IT services to advertise, provide services to, and/or sell commercial products or services
- Using University IT resources to distribute unsolicited advertisements on behalf of commercial entities.

What are activities that may violate Principle VII--Peer-to-Peer File Sharing

Examples of activities that may violate peer-to-peer file sharing, include, but are not limited to the following:

- Downloading any copyrighted media without permission from the copyright owner.
- Creating a copy of electronic media that has been purchased and making it available online to others.
- Installing software that stores, downloads, uploads, advertises content, and distributes copyrighted media without permission from the copyright owner.
- Posting to personal web space licensed software that has been modified to run without a license.

What are activities that may violate Principle VIII – Use of Personally Licensed Software

Examples of activities that may violate use of personally licensed software, include, but are not limited to the following:

- Storing University data on personally licensed software, such that the University cannot access or recover the data.
- Using personal software in a way that exposes the University network and University data to security risks.

Last Revision Update Log: 08/14/2025

IT6003 – Revised March 29, 2018
IT6003 – Revised September 13, 2019
IT6003 – March 29, 2018 – supersedes policy number
UM1535 – April 4, 2016
UM1535 – March 16, 2014
UM1535 – Rev: April 17, 2013
UM1535 – Rev.1 - updated July 31, 2007
UM1535 – Issued: July 31, 2007 - supersedes policy number 1:2A:03:01
UM1535 – Issued: January 14, 2004