

departments, colleges, or other units. In the latter case, the unit administrator is the System Sponsor.

- D. A "System Manager" is the person(s) authorized by a System Sponsor to grant, restrict or deny user privileges, maintain the system files, inform users of all applicable policies, and generally ensure the effective operation of a system. In some cases, the System Manager and the System Sponsor may be the same individual(s).
- E. "Facility Staff" are the individuals who are authorized to monitor, manage, or otherwise grant temporary access to computing facilities (such as microcomputer laboratories) in which one or more systems are used on an open access basis by either specific populations of faculty, staff, and students, or the entire campus community.
- F. A "User" is any individual who uses, logs in, attempts to use, or attempts to log in to a system (whether by direct connection or across one or more networks) or who attempts to connect to or traverse a network, whether via hardware, software, or both.
- G. An "Account" is a combination of username and password that provides an individual with access to an Information Technology Resource.
- H. "Content" is any and all text, images, multimedia elements, coding, and other such items posted, transmitted, and/or used by Information Technology Resources.

IV. Respect and Obligations

The MTSU Information Technology Resources Policy is intended to provide a framework for users to practice respectful use of Information Technology Resources. Failure to act responsibly can adversely affect the work of other users. The policy is intended to prevent abuse of equipment and services and to ensure that usage honors the public trust and supports the University's mission.

V. Who May Obtain Accounts

- A. No person is to be granted access to University Information Technology Resources without agreeing to abide by the provisions of this policy.
- B. The following persons may obtain an account at MTSU:
 - 1. Any current faculty, retired faculty, staff, retired staff, student, or alumnus of MTSU.
 - 2. Other persons may qualify for public service accounts on a particular system at the discretion of the Vice President for Information Technology and CIO.

VI. System Sponsors and Applicable Policy

- A. The Information Technology Resources at MTSU serve a diverse population. System Sponsors are given discretion to establish reasonable and appropriate policies applicable to the systems they oversee. (For example, on some campus systems, playing of computer games or use of

- chat programs may be permitted or even encouraged. On other systems, game-playing and chatting may be discouraged or even prohibited.)
- B. System Sponsors, and by their delegation System Managers and Facility Staff, have discretion to set and revise reasonable usage priorities and operational policies (such as hours of operation, usage time limits, populations to be served, etc.). They may also take such routine steps (e.g., troubleshooting, updating systems, backing up systems, etc.) as may be reasonably necessary for the operation of their systems or facilities.
 - C. In cases of conflict among Users of Information Technology Resources, resolution will follow the MTSU Infrastructure Administrative Hierarchy chart (Figure 1).

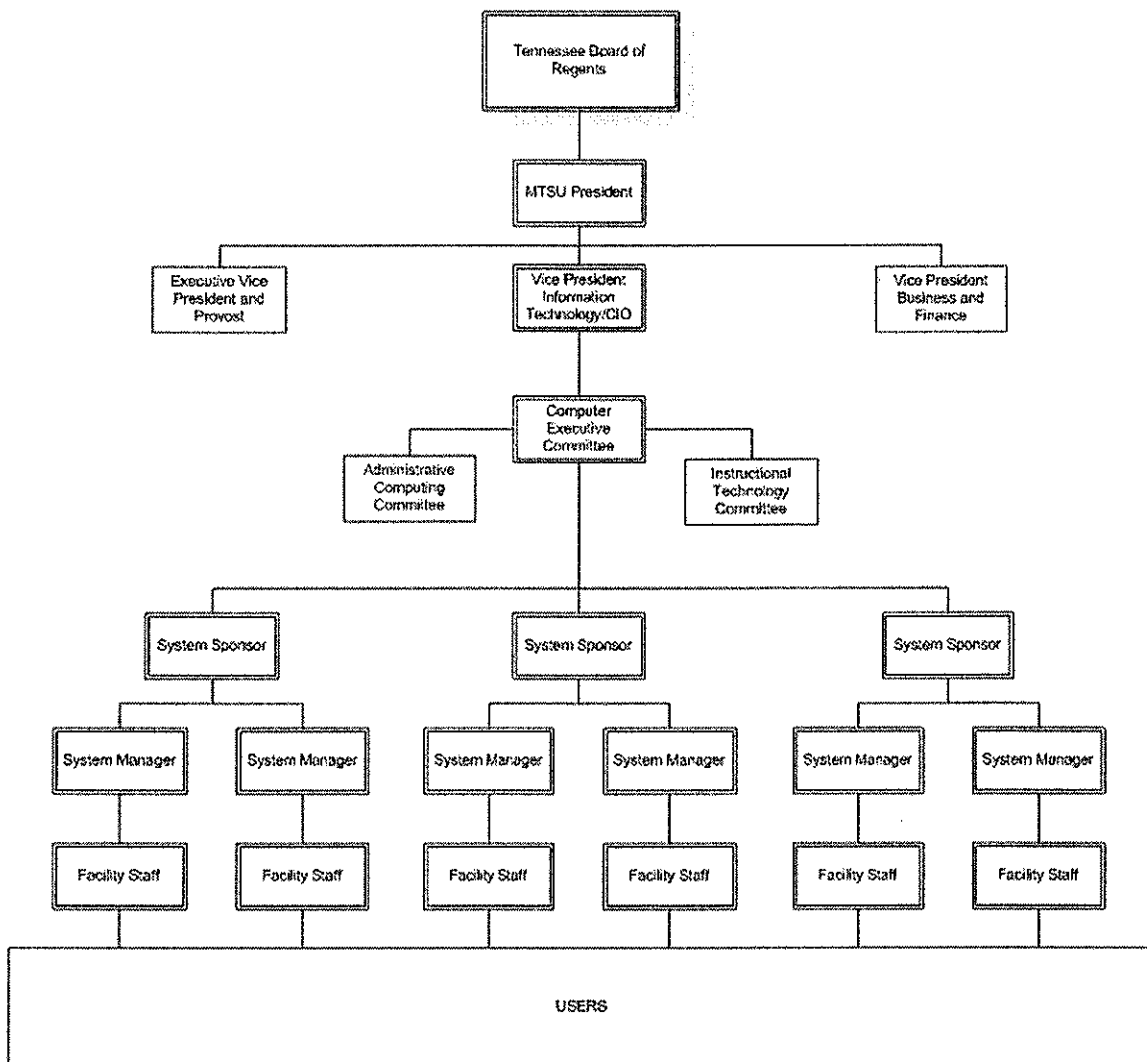


Figure 1: MTSU Infrastructure Administrative Hierarchy

VII. Cyber-Citizenship

A. Responsibility

1. Use of MTSU Information Technology Resources must comply with TBR and institutional policies, procedures, standards, and all applicable laws and not be used for any personal for-profit or any unauthorized not-for-profit purpose.
 2. Users must expect variation in what constitutes acceptable use from system to system on campus, and must make reasonable efforts to inform themselves about the particular policies applicable to each system they use. In cases of doubt, it is the responsibility of the User to inquire concerning the permissibility of an action or use, prior to execution.
 3. Users should protect their systems from misuse and attack by being up to date on security patch installations, maintaining the latest version of antivirus pattern/definitions, and running only necessary services.
 4. Questions concerning acceptable use should be directed as outlined by the MTSU Infrastructure Administrative Hierarchy chart (Figure 1).
- B. Privacy and Privilege
1. Users must respect the privacy and usage privileges of others, both on the MTSU campus and at all sites reachable via MTSU's external network connections.
 2. Users will not intentionally seek information on passwords. Users will not modify files, data, or passwords belonging to other Users. Users will not develop or retain programs for these purposes.
 3. Users will preserve and protect the privacy, dignity, well being, and informed consent of all participants.
- C. System Integrity
1. Users must respect the integrity of computing systems and networks, both on the MTSU campus and at all sites reachable via MTSU's external network connections.
 2. Users will not by any means attempt to gain access to a computing system or network without proper authorization, either on the MTSU campus or elsewhere.
 3. Users will not attempt to damage, or alter without proper authorization from the System Sponsor, either the hardware or the software components of a computing system or network, either on the MTSU campus or elsewhere.
 4. Users will not attempt to disable any hardware or software components of a computing system or network via network attacks and/or scans.
- D. Knowledge of External Network Policy
1. Users of MTSU's external network connections will comply with the evolving acceptable use policies established by the external networks' governing bodies. A link to the current relevant policy from the Tennessee Board of Regents is given at the end of this policy.

2. In cases of doubt, it is the responsibility of the User to inquire concerning the permissibility of external network uses prior to execution. Where no policy is evident, such questions should be directed as outlined by the MTSU Infrastructure Administrative Hierarchy chart (Figure 1).
- E. Resource Management
1. To effectively manage Information Technology Resources, priority is given to applications that support the University mission. The System Sponsor has the responsibility to manage resources so as to make them available for mission related applications.
 2. Users are expected to comply fully with the instructions of Facility Staff, System Managers, System Sponsors, and the Infrastructure Sponsor. In particular, Users will vacate workstations or the facility and will surrender other resources promptly when asked to do so.

VIII. Examples of What Users Are Encouraged to do with MTSU Information Technology Resources (Not an Exclusive List):

- A. Use Information Technology Resources as tools for obtaining and promulgating knowledge.
- B. Use Information Technology Resources for research and information gathering in support of advisory, analysis, and professional development activities related to the User's University duties.
- C. Use Information Technology Resources as an aid to the development of surveys and targeted demographic research.
- D. Use Information Technology Resources to communicate with other University agencies and research partners of University agencies providing document delivery or transferring working documents/drafts for comment.
- E. Use Information Technology Resources to communicate and exchange information relating directly to the mission and work tasks of the University including email in direct support of work-related functions or collaborative projects.
- F. Use Information Technology Resources as tools for the preparation of course materials.
- G. Use Information Technology Resources to enhance educational approaches and teaching methods.
- H. Use Information Technology Resources to enhance coursework submissions.
- I. Use Information Technology Resources to increase multi-cultural awareness and to develop practices of observation and reading through exposure and exploration of scientific knowledge, cultural heritage, and the changing contemporary world.
- J. Use Information Technology Resources for professional development or to maintain job knowledge or skills.

- K. Use Information Technology Resources for administering grants or contracts for University research programs or work-related applications.
- L. Use Information Technology Resources to announce University regulations, procedures, policies, services, or activities.

IX. Examples of What Users Are Not Permitted to do with MTSU Information Technology Resources (Not an Exclusive List):

- A. Violate Laws. For example:
 - 1. Use Information Technology Resources in a manner that violates MTSU policy and/or other applicable policy and laws. Note:
 - a) Users will comply with State and Federal regulations concerning obscenity and the distribution, collection or practice of child pornography; State prohibitions of gambling and restrictions on gaming; and the Federal regulations prohibiting chain letters.
 - b) Faculty Users will comply with the current Ethics Guidelines for Faculty set forth in the MTSU Faculty Handbook.
 - c) Student Users must abide by the current MTSU Student Handbook Resources and Rules.
 - 2. Transfer or use copyrighted materials without the explicit consent of the owner.
 - a) The unauthorized downloading, copying, or distribution of materials (i.e. proprietary music, video, software, or database information) via Information Technology Resources is prohibited.
 - b) Student Users should be aware that course instructors have primary responsibility for the maintenance of academic integrity. Cases involving academic dishonesty (i.e. plagiarism, cheating, etc. and/or facilitating such an act) should be reported to the dean of the college concerned.
- B. Commit Offenses Against Others. For example:
 - 1. Harass another using Information Technology Resources.
 - 2. Impersonate another.
 - 3. Take or alter another's work without permission.
 - 4. Assume credit for the work of another.
 - 5. Interfere in another's legitimate use of Information Technology Resources.
 - 6. Display obscene material in a public area. (Note: Any direct attachment, linkage, or anchoring of such materials to documents viewable by the public is prohibited).
- C. Abuse Information Technology Resources. For example:
 - 1. Attempt to gain another User's password or to log on as another User.
 - 2. Permit unsupervised use of an assigned account by any other person.

3. Use Information Technology Resources for commercial purposes, except as authorized by appropriate University administrative officials.
 - a) Use MTSU web pages for commercial, private or personal for-profit activities such as the use of web pages for advertising services for private purposes such as marketing or business transactions, private advertising of products or services, and any activity meant to foster personal gain.
 - b) Use commercial logos / icons unless that vendor provides a University service, such as dining services. Those pages must contain a notice that the vendor provides the service under contract to the University.
4. Use Information Technology Resources in support of agencies or groups outside the University when such use is not in compliance with the mission of the University.
 - a) Use MTSU web pages for unauthorized not-for-profit business activities. This includes the conducting of any non-University related fundraising or public relations activities, such as solicitation for religious or political causes.
5. Use Information Technology Resources for activities unrelated to the mission of the University when such use prevents or seriously restricts resource usage by persons fulfilling the mission.
6. Use Information Technology Resources to give access to persons who have not and/or could not obtain access to University resources through official MTSU channels.
7. Use any access not specifically assigned to the User and not provided for training or public use.
8. Deliberately alter the account structure assigned to the User so as to increase system permissions.
9. Attempt to render the system or equipment inoperative.
10. Participate in activities that have the intent of tying up Information Technology Resources.
11. Physically abuse Information Technology Resources.
12. Install wireless network transmitters.

X. Copyright Provisions

A. Default Access

1. The default access to Information Technology Resources (such as files) is to be set to allow the owner read, write, delete, and execute access and to give access to no other person. If the owner of such resources modifies this access to grant others access, such access by another, in itself, is not considered an ethical infraction. However, it is prohibited to use such access to copy another's work and assume credit for it, modify the file of another without explicit verbal or written permission to do so,

and/or embarrass the owner of a file by publicizing its contents without authorization or by modifying the file's contents in a manner unauthorized by the file's owner.

B. Software

1. MTSU utilizes a wide variety of software, with an equally wide range of license and copyright provisions. Users are responsible for informing themselves of, and complying with, the license and copyright provisions of the software that they use.
2. No software copy is to be made by any User without a prior, good faith determination that such copying is in fact permissible. All Users must respect the legal protection provided by copyright and license to programs and data.

C. Content Issues

1. With regard to intellectual property, MTSU reserves the right to protect copyrights, patents, trademarks, trade secrets, and other rights obtained legally that prohibit copying, trading, displaying, or using without permission. Many of these items may be found by searching networks including the Internet, but their presence does not imply that they are free to use without permission.
2. All content must comply with copyright laws, policies and regulations detailed in the Federal Copyright Law (Title 17 of the United States Code), and Digital Millennium Copyright Act (DMCA), the Technology, Education and Copyright Harmonization (TEACH) Act, and the Ethics Guidelines for Faculty in the MTSU Faculty Handbook and the current MTSU Student Handbook Resources and Rules.
3. Logos
 - a) The use of the MTSU logo is acceptable on University hosted web pages.
 - b) Authorization to use the MTSU Blue Raider logo is granted only by the MTSU Athletic Department.

XI. Rights

A. Rights to Access

1. Access to MTSU Information Technology Resources is granted contingent on that access not being misused. If that access is misused it can be withdrawn at any time. Further action may be taken as a result of serious offenses.

B. Rights to privacy

1. Privacy of Information is the subject of a separate MTSU policy that gives considerable guidance on privacy. Other laws, policies and regulations from MTSU, the TBR, the State of Tennessee, and the federal government address privacy issues also.
2. While MTSU recognizes the role of privacy in an institution of higher learning and every attempt will be made to honor that ideal, there should be no expectation of privacy in any message, file, image or data created, stored, sent, retrieved or received by

use of MTSU Information Technology Resources. MTSU recognizes the principles of academic freedom and free expression. In consideration of these principles, MTSU will not monitor or review the content of electronic communications or files of its Users in most instances. MTSU expects all Users to obey all applicable policies and laws in the use of Information Technology Resources.

3. Pursuant to the Tennessee Code Annotated, Title 10, Chapter 7, and subject to the exemptions contained therein, electronic files (including email correspondence) which are maintained using MTSU resources may be subject to public inspection upon request by a citizen of the State of Tennessee.
4. The University abides by the Family Educational Rights and Privacy Act, or FERPA, which requires the University to protect the confidentiality of student educational records.
5. When sources outside the University request an inspection and/or examination of any University owned or operated Information Technology Resource, and/or files or information contained therein, the University will treat information as confidential unless any one or more of the following conditions exist:
 - a) When approved by the appropriate University official(s) or the head of the department to which the request is directed
 - b) When authorized by the owner(s) of the information
 - c) When required by Federal, State, or local law
 - d) When required by a valid subpoena or court order

Note: When notice is required by law, court order, or subpoena, computer users will receive notice of such disclosures (viewing information in the course of normal system maintenance does not constitute disclosure).

6. Data on University computing systems may be copied to backup media periodically. The University makes reasonable efforts to maintain confidentiality, but if Users wish to ensure confidentiality, they are advised to encrypt their data. Although Users may use encryption software, they are responsible for remembering their encryption keys; once data is encrypted, the University will be unable to help recover it should the key used to encrypt the data be forgotten or lost. Additionally, any User of the University's email resources who makes use of an encryption device to restrict or inhibit access to his or her email must provide access to such encrypted communications when requested to do so via appropriate University authority.
7. In general, the contents of a User's files are considered private except when the owner has set the file permissions to grant others access to it and then it is with the restrictions noted above in Section IX.
 - a) The System Sponsor in charge of a system may instruct personnel to investigate the system suspected of being used by someone other than its rightful owner.

- b) The System Sponsor in charge of a system may instruct personnel to investigate the system suspected of being used in a manner that violates TBR or University policy or federal, state, or local law.
- c) The content of User files is not to be surreptitiously or otherwise examined, nor is the User generated message content of User network transactions to be monitored without the prior written permission of either the User involved or the appropriate System Sponsor. However, System Managers and others charged by them with forwarding misdirected or undeliverable email and/or delivering printouts and plots may examine such email, files, or hardcopy to the extent reasonably necessary for such purpose.
- d) Information traversing the data networks may be intercepted and/or analyzed in conjunction with investigations.

XII. In Cases of Violation of the MTSU Information Technology Resources Policy, the Following Actions are Prescribed:

- A. Immediate suspension of any or all of the following: the User's account, network access, and Internet access; followed by timely review of the charges by the appropriate person or persons.
- B. The User's computing privileges at MTSU may be permanently and totally removed. There will be no refund of any technology access fees.
- C. Use of the regular disciplinary processes and procedures of the University for students, staff, administrators, and faculty
- D. Students may be recommended for suspension or dismissal from MTSU. Employees may be recommended for termination from MTSU employment.
- E. Referral to appropriate law enforcement agencies in the case of suspected law violations for criminal and/or civil action.

XIII. Related Acceptable Use Policies:

- A. Tennessee Board of Regents Information Technology Resources Policy
- B. MTSU Privacy of Information Policy