

Michigan Technological University Computer Use Policy

Developed by Michigan Tech Computer Advisory Committee

Approved by Provost on August 8, 2001

MTU considers access to computer resources to be a privilege granted on the condition that each member of the University Community uses these resources responsibly, and in accord with professional and university standards. This document describes MTU's computer resources, the responsibilities assumed by users of the system, the services provided to support and assist users, and professional and university standards that must be observed.

Use of Computers and Networks

Computer and network facilities are provided for educational, research and administrative use. All access and use of University computing resources and services is presumed to be consistent with University rules and regulations, including University personnel policies, faculty and student codes of conduct and departmental policies and procedures. All use is also subject to the University's Conflict of Interest and Intellectual Property policy and procedure. Use of Michigan Technological University's computers and networks for non-MTU-related business purposes or personal gain without authorization is prohibited.

Individuals who are provided access to MTU's computer facilities and to the campus-wide communication network assume responsibility for appropriate use of these resources. The University expects individuals to be responsible in the use of computers and networks. Those who use wide-area networks (such as the Internet) to communicate with others or to connect to computers at other institutions are expected to abide by the rules of the remote systems and networks as well as those for MTU's systems. In addition to being a violation of University rules, certain computer misconduct is prohibited under Michigan Laws. Act 53 of the Public Acts of 1979 of the State of Michigan (as amended by Act 326 of 1996), states "An act to prohibit access to computers, computer systems, and computer networks for certain fraudulent purposes; to prohibit intentional and unauthorized access, alteration, damage, and destruction of computers, computer systems, computer networks, computer software programs, and data; and to prescribe penalties." In addition, individuals may be held responsible for misuse which occurs by allowing their account to be accessed by a third party.

Individuals must consult their department System Administrator or other designated individual prior to any activity that might threaten the security or performance of University computers and networks. Failure to do so may result in disciplinary action. An individual who may have unintentionally or inadvertently participated in or caused such an event, must notify the System Administrator as soon as possible.

Use of Facilities

MTU computer and network facilities have tangible value. Consequently, attempts to circumvent accounting systems or to use the computer accounts of others will be treated as forms of attempted theft.

Individuals may not

- attempt to damage or to degrade the performance of MTU's computers and networks,
- disrupt the work of other users,
- attempt to circumvent security systems or to exploit or probe for security holes in any MTU network or system, or attempt any such activity against other systems accessed through MTU's facilities,
- execute or compile programs designed to breach system security,
- disclose their passwords or otherwise make MTU's facilities available to anyone else,
- possess or collect passwords, personal identification numbers (PINs), private digital certificates, or other secure identification information other than their own,
- use University resources for commercial gain or solicitation, except within the boundaries of standard University policies. Individuals shall not run a private business on the MTU network, or
- engage in unauthorized conduct to place MTU in the position of being considered a service provider for third parties.

Occasionally, course assignments, independent studies or research activities may involve testing the integrity of implemented system security. Individuals who plan to assign, will be overseeing, or engaging in such activity must, at a minimum, discuss their plans with their departmental system administrator, and, if requested, a member of the University's System Administration Council prior to the start of any such activity.

Protection of Information

Computer systems and networks provide mechanisms for the protection of private information from examination. Any unauthorized attempt to circumvent them or to gain unauthorized access to private information (including both stored computer files and messages transmitted over a network) is a violation of privacy and will result in disciplinary action.

In general, information that the owner would reasonably regard as private must be treated as private by other users. Examples include the contents of electronic mail boxes, the private file storage areas of individual users, and information stored in other areas that are not public. In other words, an individual may not engage in unauthorized viewing or accessing private files or databases.

On shared and networked computer systems some kinds of information about users and their activities is visible to others. Users are cautioned that information is readily accessible, including user accounting and directory information (for example, user

names and electronic mail addresses), certain records of file names and executed commands, and information stored in public areas. Such unsecured information about other users must not be manipulated in unauthorized ways; for example, eavesdropping by computer and systematically monitoring the behavior of others will result in disciplinary action. The compilation or redistribution of information from University directories (printed or electronic) to third parties, especially those outside the University, is forbidden. Access to University information does not confer the right to read, transmit or distribute to others that information, or to make use of it except as part of official University business. Reasonable steps must be taken to ensure security of such electronic data. Computer resources must be used in a manner that does not violate the Family Education Rights and Privacy Act that MTU is bound to follow.

Users are also cautioned to familiarize themselves with applicable copyrights, licenses, and copyright laws when reproducing or providing access to information created by someone other than themselves. This includes, but is not limited to, reuse of material (text, graphics, sound, video, or other) in printed or electronic form. Unauthorized use of such information is strictly prohibited under this policy.

Individuals authorized by MTU may monitor users' data, programs, or any computer activities to

- perform routine maintenance,
- prevent damage to systems,
- ensure compliance with University procedures, rules, or regulations or
- ensure compliance with State and Federal regulations and laws.

No Expectation of Privacy

Users should be aware that due to the complexity of current software and computer networks, it is not possible for MTU to ensure privacy and fully protect systems, files, and email. Users are advised that they may not have an expectation of privacy in computer usage or contents, including email.

Electronic Communication

MTU neither sanctions nor censors opinions expressed on its systems; however, the same standards of behavior are expected in the use of electronic communication as in the use of other systems of communications at MTU. Electronic communications, for instance,

- must not threaten or endanger the safety of a member of the University Community,
- must not be obscene,
- must not violate the MTU Policy on Discrimination and Harassment,
- must not misrepresent the identity of the sender,
- must not be defamatory, and
- should not be sent as chain letters.

Generally, email on a given topic that is sent to large numbers of recipients should be directed only to those who have indicated a willingness to receive such email. University procedures define specific situations in which mass electronic mailings are acceptable.

Discipline

MTU specifically reserves the right to review messages, files, data, and other activity for legitimate purposes, during ordinary business operations, emergencies or if misconduct or abuse is suspected.

Using MTU resources in a manner that violates the provisions set forth in this policy can lead to revocation of all computer privileges as well as other disciplinary action, up to and including dismissal from the University. If required under prevailing law and to the extent required under the prevailing law, MTU will comply with due process rights. Due process and disciplinary procedures appropriate to the individual(s) involved will be followed as set forth in applicable University handbooks and/or tenure process. However, MTU reserves the right to immediately suspend any account to protect the integrity of the system and to curtail abuse.

To the extent computer usage is believed to be a violation of federal, state, or local laws, MTU will turn the matter over to the appropriate authorities.

Anyone who suspects a violation of the computing policy should report the occurrence to the staff or faculty member responsible for the facility.