



Michigan Technological University
Information Technology Services and Security

Standards for the Acceptable Use of Information Technology Resources

The following standards apply to all uses of University information technology resources. These standards are not an exhaustive list of acceptable use, but are intended to illustrate what unlawful or malicious purposes are as defined by University Policy 2.1006 Acceptable Use of Information Technology Resources.

General Standards

- Responsible behavior with respect to all University information technology resources at all times.
- Behavior consistent with the mission of the University and with authorized activities of the University or members of the University community.
- Respect for the principles of open expression.
- Compliance with all applicable laws, regulations, and University policies.
- Truthfulness and honesty in personal and computer identification.
- Respect for the rights and property of others, including intellectual property rights.
- Behavior consistent with the privacy and integrity of all University information technology resources.

Identification of users

The following activities and behaviors are prohibited:

- Misrepresentation (including forgery) of the identity of the sender or source of an electronic communication.
- Acquiring or attempting to acquire passwords of others.
- Using or attempting to use the computer accounts of others.
- Alteration of the content of a message originating from another person or computer with intent to deceive.

Access to information technology resources

Users must respect the integrity of University information technology resources. Users must refrain from seeking to gain unauthorized access to information technology resources or enabling unauthorized access. The following activities and behaviors are prohibited:

- The use of restricted-access University information technology resources or electronic information without or beyond one's level of authorization.
- The interception or attempted interception of communications by parties not explicitly intended to receive them without approval of an authorized University official.
- Making University information technology resources available to individuals not affiliated with the University without approval of an authorized University official.
- Intentionally compromising the privacy or security of electronic information.

Copyrights and Licenses

The University complies with the [Digital Millennium Copyright Act \(1998\)](#). Users must respect copyrights and licenses to software and other on-line information.

- All software protected by copyright must not be copied except as specifically stipulated by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied except pursuant to a valid license or as otherwise permitted by copyright law.
- The number and distribution of copies must be handled in such a way that the number of simultaneous users does not exceed the number of original copies purchased, unless otherwise stipulated in the purchase contract.
- In addition to software, all other copyrighted information (text, images, icons, programs, videos, music, etc.) must be used in conformance with applicable law. Plagiarism of computer information is subject to the same sanctions as apply to plagiarism in any other media.

Operational integrity

The University complies with [Michigan Law: Act 53 of the Public Acts 1979](#) as well as the [Computer Fraud and Abuse Act](#). As such, the following activities and behaviors are prohibited:

- Interference with or disruption of the computer or network accounts, services, or equipment of others, including, but not limited to, the propagation of computer "worms" and "viruses", the sending of electronic chain mail, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts.
- Failure to comply with requests from appropriate University officials to discontinue activities that threaten the operation or integrity of computers, systems or networks, or otherwise violate this policy.
- Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access.
- Altering or attempting to alter files or systems without authorization.
- Unauthorized scanning of networks for security vulnerabilities.
- Attempting to alter any University computing or networking components (including, but not limited to, bridges, routers, and hubs) without authorization or beyond one's level of authorization.
- Intentionally damaging or destroying the integrity of electronic information.
- Intentionally disrupting the use of electronic networks or information systems.
- Negligence leading to the damage of University information technology resources.