ENTERPRISE IT STANDARDS AND PROCEDURES: ACCEPTABLE USE STANDARDS

Policy: Information Technology Security
Document: Acceptable Use Standards
Campus: MSU-Northern
Revised Date: April 2023
Review Date: April 2025
Contact: Chief Information Officer

These Standards establish minimum guidelines for acceptable use of information technology as outlined in the Montana State University Enterprise Acceptable Use Policy.

Access to computer systems and networks owned or operated by MSU-Northern imposes certain responsibilities and obligations. Acceptable use always is ethical and demonstrates respect for intellectual property, ownership of data, system security mechanisms, individuals' rights to privacy and to freedom from intimidation and harassment.

The purpose of this standard is to define acceptable use requirements, but is not an exhaustive list of appropriate or inappropriate uses.

Appropriate Use of Facilities and Accounts

Users shall:

- Use resources only for authorized purposes.
- Protect your user id, password, and system from unauthorized use. You are responsible for all activities on your NetID or that originated from your system. Any user feeling pressured to reveal a password or suspect that their account has been compromised should contact the ITS Help Desk. Non-reported cases of unauthorized access may be classified as intentional and subject to enforcement procedures.
- Access only information that is your own, that is publicly available, or to which you have been granted authorized access, and only in the manner, and to the extent authorized. Ability to access University resources does not, by itself, imply authorization to do so.
- Users granted access to data in which individuals are identifiable must respect the confidentiality of the data as well as any applicable Federal or State law. Confidential and restricted data should be stored according to Data Stewardship Standards
- Users of University resources are responsible for the content of their communications and may be subject to liability resulting from that use.
- Use only legal and supported versions of software that are in compliance with vendor license or open source requirements.
- Comply with all University and MUS Board of Regents policies and applicable laws.

Users must not:

- Use another person's NetID, password or user profile (eg accessing files and data on an unlocked computer).
- Attempt to circumvent or subvert system or network security measures. Implementing methods that mask network traffic for unauthorized or unlawful purposes is prohibited. Any defects discovered in system security should be reported to the Chief Information Officer.
- Engage in any activity that might be purposefully harmful to systems or to any information stored thereon.
- Use university systems for commercial or political purposes, such as using electronic mail to circulate advertising for products or for political candidates.

- Make or use illegal copies of copyrighted materials or software, store such copies on university systems, or transmit them over university networks.
- Use email or messaging services to harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or NetID.
- Use the university's systems or networks for personal gain; for example, by selling access to your NetID or to university systems or networks, or by performing work for profit with university resources in a manner not authorized by the university.
- Users must avoid excessive use of University resources, including but not limited to network capacity. Excessive use means use that is disproportionate to that of other users, or is unrelated to academic or employment-related needs.
- Any use that interferes with other authorized uses.

The university reserves the right to copy and examine any files or information residing on university systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten or degrade operations.

Misuse of computing, networking, and information resources may result in suspension or loss of the violator's use privileges, with respect to institutional data and University owned information systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with the University. Civil, criminal and equitable remedies may apply. If the matter involves illegal action, law enforcement agencies may become involved, as they would for campus actions that do not involve information technologies or the Internet.

MSU-Northern reserves the right to update or revise these standards or implement additional policies and procedures in the future. Users are responsible for staying informed about and compliance with University policies and procedures regarding the use of computing and communication technology.