ITEM 114-104-R0102 Board of Regents Policies and Procedures Manual: Information Technology; User Responsibilities (2) (New)

No. 2-A

SCOPE

This policy applies to all MUS employees using MUS-owned or managed computing and information resources where access to those resources is part of their employment. It also applies to visiting faculty, "adjuncts," other persons having officially sanctioned, unpaid affiliations with a MUS campus, and any other person that has authorized access to MUS-owned or managed computing and information resources through other than student or patron status, as defined in Policy 1. The term "user" in this policy refers to MUS employees and the other types of users described above.

Separate policies apply to MUS student and patron users of MUS computing and information resources, i.e., Policies 2-B and 2-C respectively.

REQUIREMENTS

Each user of the Montana University System's computing and information resources should realize the fundamental importance of information resources and recognize his/her responsibility for the safekeeping of those resources. Users and system administrators must guard against abuses that disrupt or threaten the viability of all systems, including those connected to the MUS telecommunication network, the State telecommunication network, and other telecommunication networks to which MUS systems are connected.

Each user is responsible for having knowledge of MUS policies concerning security, privacy, and acceptable computing practices. Each user of MUS computing and information resources must act responsibly. Each user is responsible for the integrity of these resources. Each user of MUS-owned or managed computing systems must be knowledgeable of and adhere to MUS policies, respect the rights of other users by minimizing unnecessary network traffic that might interfere with the ability of others to make effective use of shared resources, respect the integrity of the physical facilities and controls, and obey all pertinent federal, state, county, and local laws and ordinances. Each user must abide by these policies, laws, and contractual obligations, and adhere to appropriate ethical standards.

MUS information technology resources are to be used by an employee for the job-related activities to which the employee is assigned. An employee should not use MUS information technology resources for private, commercial purposes, except those covered under formal agreements with the MUS.

ENSURING COMPLIANCE

In the case of MUS staff, it is the responsibility of the supervisor to ensure that employees are aware of MUS policies and procedures concerning the use of MUS computing and information technology resources, understand them, and comply with them. In the case of visitors, adjuncts, or other affiliates who have authorized access to MUS computers and information resources, this responsibility falls to the head of the agency that sponsors or sanctions the individual in question.

REPORTING AND DISCIPLINARY ACTION

Users of MUS information technology resources must cooperate with requests from system administrators for information about computing activities; follow MUS procedures and guidelines in handling diskettes and external files in order to maintain a secure, virus-free computing environment; follow MUS procedures and guidelines for backing up data and making sure that critical data are saved to an appropriate location; and honor the Acceptable Use Policies of any MUS or non-MUS networks they access through MUS facilities.

Users must report acceptable use violations and other security violations to their immediate supervisors, to local personnel responsible for local network policy enforcement, or to personnel responsible for the enforcement of the policies pertinent to the violation.

Misuse of MUS computing or information resources may result in disciplinary action appropriate to the misuse, up to and including termination of an employee.

GUIDELINES: RECOMMENDATIONS, NOT REQUIREMENTS

Example Misuses of MUS Information Technology Resources

The following items represent, but do not fully define, misuse of information technology resources. Note that many of these examples may be considered appropriate uses of technology resources in specific academic or professional contexts; determination of appropriateness is the initial responsibility of the user's supervisor (e.g., manager, director, instructor, department chair, dean, or provost).

- Excessive personal use of MUS computer and network resources.
- Using resources for derogatory, racially offensive, sexually offensive, harassing, threatening, or discriminatory purposes.
- Downloading, installing, or running security programs or utilities that reveal weaknesses in the security of MUS computer resources, except by a MUS employee as specifically required by that employee's assigned job responsibilities.
- Unauthorized use of computers and User IDs, or use of User IDs for purpose(s) other than those for which they have been issued.
- Modifying, installing, or removing computer equipment, software, or peripherals, or attempting to do so, without proper authorization.
- Accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by the MUS. For example, using the networks to which the MUS has access to improperly access resources at other sites will be considered an abuse of a user's MUS computing privileges.
- Circumventing or attempting to circumvent normal resource limits, logon procedures, or security regulations.
- Sending fraudulent e-mail, breaking into another user's e-mail account, or reading someone else's e-mail without his or her permission, unless specifically authorized to do so.
- Sending any fraudulent electronic transmission, including but not limited to fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or journal vouchers, or fraudulent electronic authorization of purchase requisitions or journal vouchers.
- Violating any legal software license agreement or copyright, including copying or redistributing copyrighted computer software or data without proper, recorded authorization.
- Violating the property rights of those who hold copyright to computer-generated data, reports, or software.
- Taking advantage of another user's naiveté or negligence to gain access to any system account, data, software, or file which would not otherwise be accessible.
- Physically interfering with other users' access to MUS computing facilities, unless authorized to do so by the appropriate authority.
- Encroaching on or disrupting others' use of MUS network resources by creating unnecessary network traffic (for example, by playing games or sending excessive amounts of e-mail); wasting computer processing time, connect time, disk space, or other resources; modifying system facilities, operating systems, or disk partitions without authorization; attempting to crash or deny service to a MUS computer; damaging or vandalizing MUS computing facilities, equipment, software, or computer files.
- Disclosing proprietary information, software, printed output, or magnetic media without the explicit permission of the owner.
- Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission, except in the case of MUS employees authorized to do so in the performance of their jobs.
- Knowingly transferring or allowing to be transferred to, from, or within the MUS, textual or graphical material commonly considered to be child pornography or obscene as defined in 45-8-201(2), MCA.
- Any other activity involving use of MUS computing and information resources that violates established MUS policies, state laws, or federal laws, whether or not those policies or laws relate specifically to the use of computing or information resources.