February 27, 2002

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

No. 2-C

SCOPE

This policy applies to all MUS “patrons” using MUS-owned or managed computing and information resources that are made freely available to the public. In this policy "user" refers to a patron user, as distinct from any role the individual may also have as an employee (Policy 2-A) or student user (2-B).

REQUIREMENTS

Each campus of the Montana University System’s that provides patron access to computing and information resources should realize the fundamental importance of information resources and recognize its responsibility for the safekeeping of those resources. The designers and administrators of patron access facilities 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.

By definition, patron access systems do not require prior identification of the user or pre-created user accounts. Generally, patron systems should neither request nor save personal information. Thus any logging of patron activity should be done at the level of the generic patron, not at the level of the specific individual patron. If personal information is requested, the patron should provide it at his/her option, and it should be collected only if the patron has been made aware of it and has been informed of and has agreed with any other potential uses to which the personal information may be put. In addition, nothing herein shall be deemed to prevent a campus from requiring patrons from registering and agreeing to monitoring and record keeping of system usage as a condition of patron access to the system.

Access points to patron-accessible systems should clearly identify the allowable uses of such systems. However, patron users cannot be presumed to be knowledgeable of or bound to adhere to MUS policies concerning security, privacy, and acceptable computing practices. Hence, patron access systems must be designed and maintained so that the system prevents inappropriate actions by the user.

Patrons shall not be able to install, update, or modify in any way the software installed on a patron-accessible system. The system shall make available only software that is acceptable for use on that system. Patrons may require the ability to create temporary files for the duration of their session, but they should not be allowed to save personal data or files on the system between sessions, and system administrators shall take care to prevent the use of patron systems for illegal copying or duplication activities.

Patron-accessible network access programs (e.g., browsers) shall support only those features necessary to the mission of the patron access system. Site blocking or physical monitoring may be used to assure that network access activity is consistent with state and federal laws, other MUS policy, and the purpose of the patron system.

If provided at all, e-mail and/or messaging systems on patron-accessible systems shall be highly restricted. In general patrons shall not be permitted to use patron-accessible systems to send e-mail or messages to other users or addresses through MUS systems. Exception: e-mail or messages to appropriate accounts associated with the patron system are permissible (e.g., to system administrators to report problems, to other administrators to comment on service). Site blocking may be used when appropriate to restrict patron’s ability to use network-based e-mail and messaging systems.

Use of general purpose productivity tools (e.g., word processing and spreadsheet software) on patron systems is permissible, as long as this use is complementary to the primary use of the patron system, not its primary use, and is legal with respect to licensing of that software.

ENSURING COMPLIANCE

It is the responsibility of the campus offering patron services to ensure that its systems are designed and used appropriately.

REPORTING AND DISCIPLINARY ACTION

Units operating patron systems must cooperate with requests from central system and network administrators for information about the design and operation of these systems, and follow MUS procedures and guidelines to maintain a secure, virus-free computing environment.

Failure to conform to these requirements will result in a patron system being disconnected from the campus network, and may result in appropriate disciplinary action against those charged to oversee operation of that system.