ITEM 114-104-R0102 Board of Regents Policies and Procedures Manual: Information Technology; Privacy, Security and Monitoring (1) (New)

No. 1

SCOPE

This policy applies to all MUS individuals using MUS-owned or managed computing and information resources (hereinafter "users").

PURPOSE

This policy outlines the general rules governing the MUS's rights and responsibilities to monitor the use of the computers and networks it operates, and the balance between those rights and responsibilities and the expectation of a reasonable degree of privacy in the use of those facilities by users.

REQUIREMENTS

Each campus will report semi-annually to the Office of the Commissioner of Higher Education on the specific implementation of these policies.

The MUS has the legal responsibility to ensure that the computers and networks it operates are used appropriately. The data contained on those computers and transmitted on those networks are presumed to be MUS property unless MUS's rights are otherwise limited by law, policy, or contract. In any case, the data contained on those computers and transmitted on those networks is subject to monitoring and/or copying by the MUS. That is, in order to meet its obligations, the MUS, through individuals operating within the course of their legitimate job duties, may periodically, routinely, or for a specific purpose monitor activity on its computers and network. These individuals may include IT personnel and appropriate administrators and supervisors on each campus.

The types of activities the MUS may monitor and on which it may maintain records include, but are not limited to:

1. e-mail sent from or received by e-mail systems operating on MUS sites;

2. accesses to external Web sites originating from MUS sites;

3. other significant external network activity originating from or received by MUS sites; and

4. the contents of permanent storage devices attached to MUS computers (including installed software and software version information, system data, and user data).

The MUS's general interests in these aspects stem from both its obligations to prevent misuse of its resources and its commitments to its users to provide certain services, such as backups of system and user data for use in case of system failures, reasonable and robust network performance, optimized access paths for frequently accessed Web sites, optimized network performance for other types of network activity (e.g., video conferencing, remote high speed computation), guarantees that system software is updated appropriately and efficiently, and blocking and/or detecting the sorts of disruptive activity characterized as hacking or system cracking, virus/worm infection, and denial of service. Routine network monitoring typically focuses on "general" patterns of use, but attempts to optimize performance, detect anomalies, or track down possible intrusions may lead to more specific monitoring. Activities such as routine system backups always involve collecting and copying user-specific data and the contents of e-mail systems. In copying data for these purposes the MUS gains the right to use such copies appropriately; it does not gain intellectual property rights to the information contained in the data.

Personal information gained through monitoring will be held in confidence by the MUS when required by law. Records obtained by monitoring may be used within the MUS by MUS officials, employees and agents for purposes appropriate to the management and administration of the MUS, including the investigation of possible misconduct by a user or a third party. In addition, records will be released if necessary to comply with a court order or other legal instrument binding upon the MUS or its officials. Requests for records by members of the public will be complied with in a fashion consistent with the law on public access to records and privacy. Persons requesting public disclosure of such records may be assessed the reasonable costs of time and material involved in meeting the request.

Except for the identification, investigation, and prevention of misconduct by a user, including violations of law, MUS officials, employees, and agents will not divulge personally identifiable information obtained through monitoring.

CLASSES OF RESOURCE USERS

The computing and information technology resources owned and managed by the MUS are used by three distinct classes of users, who gain access to information technology resources through very different relationships with the MUS, and hence to which different acceptable use policies must apply.

1. **Employees**. These include individuals who are regular MUS employees, as well as visiting faculty, "adjuncts," and other persons having officially sanctioned, unpaid affiliations with a MUS campus. These users gain access to MUS information technology resources by virtue of their employment or sanctioned affiliations.

2. **Students**. These include individuals registered as full- or part-time students at a MUS campus. These users gain access to MUS information technology resources as part of the service package the campus provides to registered students.

3. **Patrons**. These are casual users who use MUS information technology resources that are made available to the public at large, e.g., people who use public access terminals in MUS libraries.

Because there are dramatic differences in the relationships between the MUS and individuals in each of these three groups, care must be taken to clearly identify the specific rights and responsibilities that pertain to each group of users. Also, a given individual may fall into more than one of the user classes, and hence gain different rights by virtue of participation in different types of activities. For example, MUS employee "Smith" gains "employee user" rights by virtue of his/her employment, and exercises those rights while at work. If Smith also registers for a class he/she gains "student user" rights for use in his/her academic pursuits. Finally, Smith may at any time visit a campus library and exercise "patron user" rights by using a public access terminal. It is reasonable to expect that the rights and responsibilities of an individual such as Smith differ depending on the context of his/her access, and the policies that apply to a given incident will therefore depend on the specific context of use.