MONTANA BOARD OF REGENTS OF HIGHER EDUCATION
Policy and Procedures Manual

SUBJECT: INFORMATION TECHNOLOGY
Policy 1307 - Internet Reporting
Adopted: May 24, 2002; Revised May 23, 2014

Board Policy

A. SCOPE
This policy applies to all access to or use of MUS-provided Internet or Internet2 services made from any computer that resides on an MUS campus, is connected to the campus intranet, and is connected through the intranet to the outside Internet or Internet2, or from any computer that is connected to an MUS campus intranet, and through it to the Internet or Internet2 via dial-up or other externally provided network access service (e.g., a commercial ISP service).

B. PURPOSE
The MUS has the responsibility to insure that its telecommunications systems are used in the most effective and secure manner. Accessing certain Web sites, certain types of Web services, or certain other network resources may lead to ineffective use of university telecommunication systems or may jeopardize their security. Therefore, the MUS has adopted policies addressing security, monitoring, and privacy issues associated with its computing and information resources, including telecommunications systems.

From time to time, the MUS may receive requests for records or other information obtained as a result of monitoring activities. These requests may be of several types, as described below. This policy, describes the steps to be taken to respond to such requests. It will be used for all such requests for network reporting, regardless of the source of the request or whether the activity involves the (external) Internet or (internal) intranet.

C. DEFINITIONS
Network Reporting

1. An ongoing analysis of overall network usage by a campus of the MUS, prepared by authorized MUS staff; or
2. A report on the specific network resources accessed by an individual employee or student account or by a particular computer (IP address) over a specified period of time, prepared by authorized MUS staff.

D. REQUIREMENTS
Reporting of network access activity may be provided for the following reasons.

1. Network Management. Authorized MUS staff on each campus may periodically analyze network traffic to determine if the campus has adequate bandwidth, within budgeted costs, to meet user needs and provide adequate response times. The staff, during the course of their analysis, will report to their supervisors or other authority designated by the campus administration any access to a network resource or class of network resources that the staff involved in the analysis consider:
   - not to be related to university business or scholarship
   - to pose a security threat, or
   - to be of sufficient volume to have a potentially detrimental impact on network performance.

2. Follow-up on Possible Misuses. Upon receipt of a report of possible network misuse from network operations staff, the supervisor or other authority will forward all pertinent information to the chief security officer of the campus involved in the activity in question. The chief security officer is then responsible for initially determining if the information warrants a campus request for additional information, or other appropriate follow-up activity.

3. Campus Request. Within the constraints outlined in the MUS information technology policy on privacy, security, and monitoring (Policy 1302) and, when relevant, library policy, and within the provisions of applicable state and federal laws, a campus may request a report of network resources accessed by an employee of the campus or by a student taking courses at or within the campus when using MUS-owned and/or operated resources. Campus requests should be made in writing and approved by the chief executive officer of the campus. The request should then be directed to the campus personnel charged with overseeing network usage.

4. Law Enforcement Request. Requests for network access records from law-enforcement agencies must be made through an appropriate legal process (e.g., a legally valid court order or subpoena). (Note: this does not preclude the MUS or any campus from contacting law enforcement as part of an investigation initiated by the MUS or the unit.) MUS legal counsel should be consulted whenever contact with a law-enforcement agency is initiated or received.

5. Public Request. Consistent with the MUS information technology policy on privacy, security and monitoring (Policy 1302) and, when relevant, library policy, requests by members of the general public for the network access records of an individual employee or student will not be honored except through an appropriate legal process, as defined above.

History:
Item 114-104-R0102, Internet Reporting, approved by the Board of Regents on May 24, 2002. Item 163-107-R0514, revised May 23, 2014.