MONTANA BOARD OF REGENTS OF HIGHER EDUCATION
Policy and Procedures Manual

SUBJECT: INFORMATION TECHNOLOGY
Policy 1306 - Logging On and Off Computer Resources
Adopted: May 24, 2002; Revised: May 23, 2014

Board Policy

A. SCOPE
This policy applies to all MUS-owned or managed computer systems. Unless otherwise indicated, the term "user" here refers to both employee and student users.

B. REQUIREMENTS
MUS entities must provide for the security of their data and information resources. For employee and student users, access to these resources must be controlled by having users properly log onto and off of computer systems and by prohibiting users from using other users' accounts. Employee and student users must be positively identified prior to being able to use any authentication controlled MUS computer resource. Positive identification involves both a user ID and a password which are unique to the individual. For patron users, management of the patron-accessible systems must prohibit users from engaging in activities that result in security problems.

All MUS-operated computer systems to which a user can connect interactively must display an informational banner at user-connection time explaining what are considered acceptable uses of MUS information technology resources; this information may be in the form of references to MUS policies on security and monitoring, acceptable use, or other pertinent topics.

> SAMPLE WARNING BANNER
>
> This system is the property of the Montana University System and is subject to the MUS security, monitoring, and appropriate-use policies located at: http://www.mus.edu/borpol/bor1300/bor1300.asp. Unauthorized use is a violation of 45-6-311, MCA and Montana University System policies. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use. **Log off immediately** if you do not agree to the conditions stated in this warning.

C. GUIDELINES – RECOMMENDATIONS, NOT REQUIREMENTS
For a computer dedicated for use by a single employee user, at the end of each workday the user should disconnect from network-accessible resources if possible. The user should power off his/her computer(s), or use password-protected screen savers or "sleep modes" to prevent unauthorized access. The user should also release network-accessible resources (i.e., through log-off of connection to that resource) whenever those resources are not in use. Users who plan to leave their computers unattended for 30 minutes or longer should either log off network-accessible resources or use password-protected screen savers or sleep modes to prevent unauthorized access.

For a computer shared by multiple employee and/or student users, each user should disconnect from network-accessible resources, log-off the computer, and make it available for another user immediately upon completion of his/her "computer session." Users of shared computer systems should generally not leave their computer sessions unattended – they should log-off if they must leave the immediate vicinity of the computer, then log in again upon return.

History:
Item 114-104-R0102, Logging On and Off Computer Resources, approved by the Board of Regents on May 24, 2002. Item 163-106-R0514, revised May 23, 2014.