Bemidji State University Policies

Policy Name: Acceptable Use of Computers and Information Technology Policy	**Effective Date:** 6/1/2015
Policy Owner: Chief Information Officer	Last Review: 4/1/2018
	Next Review: 9/1/2021

Policy Statement

Bemidji State University policy on acceptable use of computers and technology states computer and information technology resources are essential tools in accomplishing the university's mission. These resources must be used and managed responsibly to ensure their availability for the competing demands of teaching, scholarship, administration and other mission related uses.

This policy further states that as responsible members of the university community, individuals using information technology resources are expected to act in accord with general principles based on the acceptable law as well as common sense, common decency and civility applied to the networked computing environment. The university encourages the use of information technology as an effective and efficient tool within the framework of applicable state and federal laws, policies and rules and other necessary restrictions.

Scope and Purpose of Policy

The scope of this policy applies to university information technology resources, wherever located, provided for use by currently enrolled university students, administrators, faculty, other employees, and other authorized users. Access to and the responsible use of modern information resources is a privilege and is essential to the pursuit and achievement of excellence at BSU.

The university encourages appropriate use of technology to enhance productivity through the efficient exchange of information for intended uses of the university mission. Nothing in this policy shall be interpreted to expand, diminish or alter academic freedom, articulated under MnSCU Board Policy and university collective bargaining units. Use of these resources must be consistent with these goals.

Bemidji State University and Minnesota State are not responsible for any personal or unauthorized use of resources. Security of data transmitted on its information technology resources cannot be guaranteed.

Definitions

Security measures means processes, software, and hardware used by university and network administrators to protect the confidentiality, integrity, and availability of the computer resources and data owned by the university or its authorized users. Security measures may include, but are not limited to, monitoring or reviewing individual user accounts for suspected policy violations and investigating security-related issues.

University information technology means all university facilities, technologies, and information resources used for information processing, transfer, storage and communications. This includes, but is not limited to, computer hardware and software, computer labs, classroom technologies such as computer-based instructional management systems, and computing and electronic communications devices and services, such as modems, e-mail, networks, telephones, voicemail, facsimile transmissions, video, mobile computing devices, and multimedia materials.

Transmit means to send, store, collect, transfer or otherwise alter or affect information technology resources or data contained therein.

User means any individual, including, but not limited to, students, administrators, faculty, other employees, volunteers, and other authorized individuals using university information technology in any manner, whether or not the user is affiliated with Bemidji State University and Minnesota State Colleges and Universities.

Procedures

The following information applies to all users:

1. Users must comply with laws and regulations, Minnesota State Board policies and university procedures, contracts, and licenses applicable to their particular uses. This includes, but is not limited to: the laws of libel, data privacy, copyright, trademark, gambling, obscenity, and child pornography; the federal Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit “hacking” and similar activities; state computer crime statutes; applicable conduct codes, including the Minnesota State System Procedure 1C.0.1, Employee Code of Conduct; applicable software licenses; and Board Policies 1B.1, prohibiting discrimination and harassment, 1C.2, prohibiting fraudulent or other dishonest acts; and 3.26, concerning intellectual property. Illegally downloading or distributing copyrighted material (including but not limited to software, data, music, and video) through any means, is a violation of Federal law. The University/College is obligated to take immediate action upon receipt of "cease and desist" notices, or upon discovery of any activities concerning copyright infringement. In some instances, *streaming* content may be considered “downloading.”

2. Users are responsible for the content of their personal use of university information technology and may be subject to liability resulting from that use.

3. Users must use only university information technology they are authorized to use and use them only in the manner and to the extent authorized. Ability to access information technology resources does not, by itself, imply authorization to do so. Wired or wireless routers and access points that are not managed or maintained by BSU or NTC Information Technology Services are not allowed on the University/College network. Students are allowed to use unmanaged “simple” switches only.

4. Users must abide by the security restrictions on all information technology systems and information to which access is authorized.

5. Users must not allow others who are not authorized to:
   a. use any account or password assigned by the university to anyone else;
   b. share any account or password, assigned to the user by the university, with any other individual, including family members;
   c. allow others to use university information technology under the user’s control.

6. Users must not circumvent, attempt to circumvent, or assist another in circumventing security controls in place to protect the privacy and integrity of data stored on university information technology.

7. Users must not change, conceal, or forge the identification of the person using university information technology, including, but not limited to, use of e-mail.

8. Users must not knowingly download or install software onto university information technology unless allowed under applicable procedures or prior authorization has been received.

9. Users must not engage in activities that interfere with or disrupt network users, equipment or service; intentionally distribute viruses, worms, Trojans, or other malicious code; or install software or hardware that permits unauthorized access to university information technology.

10. Users must not engage in inappropriate uses, including:
    a. Activities that violate state or federal law or regulation;
    b. Wagering or betting;
    c. Harassment, threats to or defamation of others, stalking, and/or illegal discrimination;
    d. Fund-raising, private business, or commercial activity, unless it is related to the mission of the university or its colleges and universities. Mission related activities are determined by the college, university, or university office, and include activities of authorized campus or university-sponsored organizations;
    e. Storage, display, transmission, or intentional or solicited receipt of material that is or may be reasonably regarded as obscene, sexually explicit, or pornographic, including

any depiction, photograph, audio recording, video or written word, except as such access relates to the academic pursuits of a university student or professional activities of a university employee; and

f. "Spamming" through widespread dissemination of unsolicited and unauthorized e-mail messages.

11. All users are expected to abide by the security restrictions on all university systems and information to which you have access. Activities that interfere with or disrupt network users, equipment or services are prohibited.

12. All users found abusing computer facilities, or using the equipment without permission, or using the equipment for non-academic, recreational purposes, or copying copyright protected software will be subject to disciplinary action.

Enforcement

1. Conduct that involves the use of university information technology resources to violate a university policy or procedure, or state or federal law, or to violate another's rights, is a serious abuse subject to limitation or termination of user privileges and appropriate disciplinary action, legal action, or both.
    a. Bemidji State University reserves the right to temporarily restrict or prohibit use of its university information technology by any user without notice, if it is determined necessary for business purposes.
    b. Repeat violations of copyright laws. Bemidji State University may permanently deny use of university information technology by any individual determined to be a repeat violator of copyright or other laws governing Internet use.
    c. Disciplinary proceedings for alleged violations shall be addressed through applicable university procedures, including but not limited to University Procedure 1B.1.1, to address allegations of illegal discrimination and harassment; student conduct code for other allegations against students; or the applicable collective bargaining agreement or personnel plan for other allegations involving employees. Continued use of university information technology is a privilege subject to limitation, modification, or termination.
    d. Sanctions-Willful or intentional violations of this procedure are considered to be misconduct under applicable student and employee conduct standards. Users who violate this procedure may be denied access to university information technology and may be subject to other penalties and disciplinary action, both within and outside of the university. Discipline for violations of this procedure may include any action up to and including termination or expulsion.
        i. First offense: Students will receive a warning that their activities may be in violation of this Technology Policy and/or the Student Code of Conduct, and made aware of potential future consequences or penalties should violation of the policy continue.

ii. Second offense: Network service will be disabled for forty-eight (48) hours, and the student will be referred to the Institution's conduct system. Students subsequently found in violation of the Code of Student Conduct may be subject to sanction, up to and including expulsion from the Institution.

iii. Network service will be disabled indefinitely, and the student will be referred to the Institution's conduct system. Students subsequently found in violation of the Code of Student Conduct may be subject to sanction, up to or including expulsion from the University/College.

e. Under appropriate circumstances, Bemidji State University may refer suspected violations of law to appropriate law enforcement authorities, and provide access to investigative or other data as permitted by law.

Rationale

Access to and the responsible use of modern information resources is essential to the pursuit and achievement of excellence at BSU. The university encourages appropriate use of technology to enhance productivity through the efficient exchange of information for research. Use of these resources must be consistent with these goals.

Supporting References

- Minnesota State Board Procedure: Acceptable Use of Computers and other Information Technology Resources Policy http://www.minnstate.edu/board/policy/522.html
- Minnesota State Board Policy 5.22.1: Acceptable Use of Computers and other Information Technology Resources Procedures http://www.minnstate.edu/board/procedure/522p1.html
- Minnesota State Board Policy: Employee Code of Conduct http://www.minnstate.edu/board/procedure/1c0p1.html