General/Student Policy - Use of Computer and Network Facilities

Policy:

Individuals who use Bismarck State College (BSC) computing and networking resources assume the responsibility to use the resources in an appropriate manner. Misuse of computing and networking resources is considered a violation of the campus computing policy and regulations. It may also be a violation of law if data or individuals are disturbed or the privacy of the individuals is violated.

North Dakota University System (NDUS) Procedure 1901.2, Computer and Network Usage, contains specific policies, procedures, rights, and responsibilities which also apply to BSC. NDUS Procedure 1901.2, Computer and Network Usage, can be viewed at: http://www.ndus.edu/makers/procedures/ndus/default.asp?PID=301&SID=62.

This BSC Use of Computer and Network Facilities policy is in addition to NDUS Procedure 1901.2, Computer and Network Usage, and is based in large part on the definitions of "Authorized Use" and "Authorized Users" from section 1 of NDUS Procedure 1901.2, Computer and Network Usage:

"**Authorized use:**
Use of computing and networking resources shall be limited to those resources and purposes for which access is granted. Use for political purposes is prohibited (see Section 39-01-04 of the ND Century Code). Use for private gain or other personal use not related to job duties or academic pursuits is prohibited, unless such use is expressly authorized under governing institution or system procedures, or, when not expressly authorized, such use is incidental to job duties or limited in time and scope, and such use does not: (1) interfere with NDUS operation of information technologies or electronic mail services; (2) burden the NDUS with incremental costs; or (3) interfere with the user's obligations to the institution or NDUS."

"**Authorized user(s):**
Computing and networking resources are provided to support the academic research, instructional, outreach and administrative objectives of the NDUS and its institutions. These resources are extended to accomplish tasks related to the individual's status with NDUS or its institutions. Authorized users are (1) current faculty, staff and students of the North Dakota University System; (2) individuals connecting to a public information service (see section 5.3); and (3) other individuals or organizations specifically authorized by the

NDUS or an NDUS institution. For the purposes of this policy, no attempt is made to differentiate among users by the user's group. These policies treat all users similarly, whether student, faculty, staff or other authorized user, in terms of expectations of the user's conduct."

Limits and Regulations:

The use of the campus computer and networking service is a privilege that may be revoked at any time for inappropriate behavior. Examples of uses which BSC considers to be *unauthorized and unacceptable* include, but are not limited to:

- Stalking, fraud, misrepresentation, luring of minors or sending harassing, intimidating and/or threatening messages through electronic mail or other means;
- Intentionally intercepting, disclosing or using any electronic communication to which authorized access is not explicitly provided;
- Initiating or encouraging chain letters, unauthorized automated or mass postings, or other types of unauthorized large-scale distributions;
- Providing others with access to one's personal computer account(s);
- Gaining or attempting to gain access to the personal computer accounts, files, electronic information of others, or to accounts, files or systems to which authorized access has not been granted;
- Hacking or related behavior attempting to compromise BSC security or the security of remote systems accessed through BSC equipment or networks;
- Creating or releasing computer viruses or engaging in other destructive or potentially destructive programming activities;
- Browsing, viewing and/or sharing of pornographic material or Internet chat of a sexual nature;
- Disruption of network traffic by overloading the system or otherwise denying or restricting the access of others;
- Modifying, altering or otherwise tampering with systems hardware, software or networking infrastructure unless explicitly authorized to do so by the Chief Information Officer;
- Setting up a router and building a private subnet;
- Setting up wireless access points unless explicitly authorized to do so by the Chief Information Officer;
- Copying or distributing commercial or other copyrighted software or proprietary data which has not been placed in the public domain or been distributed as freeware;
- Use of BSC computers, systems, networks and/or services for political purposes, for commercial purposes or unauthorized financial gain;
- Use of BSC computers, systems, networks and/or services for on-line gaming or on-line gambling (playing games on BSC computers is prohibited unless done in a classroom situation under the supervision of an instructor);
- Use of BSC computers, systems, networks and/or services for peer-to-peer applications is prohibited unless explicitly authorized to do so by the Chief Information Officer;

- Use of BSC computers for mail spoofing (sending mail so as to appear to come from someone other than the actual sender) or for TCP spoofing (making your computer look like a different computer on the network);
- Use of BSC computers, systems, networks and/or services for packet sniffing (putting your network interface card in the promiscuous mode in order to see data destined for other machines) unless explicitly authorized to do so by the Chief Information Officer;
- Any act chargeable as a violation of local, state or federal law, whether or not charges are brought by civil authorities.

In order to protect the campus data networks, BSC Information Technology Solutions and Services department reserves the right to control network access. In the event of threats or network disruption, it may be necessary to temporarily block specific types of network traffic or isolate portions of the network. Devices may be removed from the network or have network access blocked without notice if they pose a threat to the network, the device itself or the user(s) of the device. Examples of reasons why a device might be removed or blocked from the network include, but are not limited to the following:

- A device is used for unauthorized use or by unauthorized users;
- Network addresses are unauthorized, misappropriated or have been modified to avoid restrictions;
- The provisioning of network services from user computers (e.g. BBS, IRC Server, DHCP Server, DNS Server, FTP, POP3, SMTP, WINS Server, Hotline, SNMP). Users who have a need to provide such services from their personal computers must have prior written authorization from the Chief Information Officer at BSC before running any such services.
- A device poses a threat to the network or the user because of vulnerabilities, compromises, incompatibilities with the network or other reasons.

Violation of this policy may be subject to discipline, which may include loss of computer and network privileges.

Portions of this policy are drawn from those developed by North Dakota State University and the University of North Dakota.

History of This Policy:

First policy draft December 1, 1994.

Revisions – January 12, 2004; approved by Computer Use Steering Committee February 27, 2006; approved by Infusing Technology Committee April 20, 2006; approved by Cabinet July 6, 2006; October 14, 2008; December 14, 2010; reviewed by the Operations Council on October 24, 2012 and approved by the Executive Council on October 30, 2012; reviewed by the Operations Council on December 12, 2012 and approved by the Executive Council on December 19, 2012; Revised July 30, 2013.