1901.2 – Use of Computer and Network Facilities

Purpose:

This procedure is to operationalize BSC Policy 1901.2 Use of Computer and Network Facilities. These procedure details are intended to assist individuals to ensure appropriate use of computing and network services and resources.

Procedure:

This policy procedure identifies unacceptable use of BSC computing and network resources.

Examples of misuse which are considered to be *inappropriate and unauthorized 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 unauthorized automated or mass postings, or other types of unauthorized large-scale distributions;
- Providing others with access to one's assigned NDUS and BSC account(s);
- Gaining or attempting to gain access to 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;
- Setting up rogue networks (e.g. routers, wireless access points, switches);
- 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 online gambling;

- Use of BSC managed devices for online gaming is prohibited unless under the supervision of an instructor or coach;
- 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);
- 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.

References:
North Dakota University System (NDUS) Procedure 1901.2, Computer and Network Usage, contains specific policies, procedures, rights, and responsibilities which also apply to BSC. This policy is in addition to NDUS Procedure 1901.2, Computer and Network Usage, and references the definitions of "Authorized Use" and "Authorized Users" from section 1 of NDUS Procedure 1901.2, Computer and Network Usage:

History of This Policy Procedure:
First policy: 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; July 30, 2013.

First policy reviewed and approved by Campus Council on September 9, 2023. Reviewed by the Executive Council on September 9th, 2023 and approved by the President on October 5th, 2023.