SOUTH DAKOTA BOARD OF REGENTS

Policy Manual

SUBJECT: Acceptable Use of Information Technology Systems

NUMBER: 7:1

---

1. Purpose

The Board acquires, maintains and operates information technology systems to support administrative, research, instructional and service functions of the universities and special schools. This policy serves to assure the optimum functioning of these information technology systems and to protect them from abuse and from unlawful or other misuse. By using the electronic information and communications systems, users agree to abide by all relevant policies and procedures, as well as all current federal, state, and local laws.

2. Information Technology Devices and Systems Subject to this Policy

Information technology systems include any and all electronic means used to create, store, access, transmit and use data, information or communications in the conduct of administrative, instructional, research or service activities. These systems include, devices now in existence, or to be invented, that serve such purposes.

A. Privately owned information technology devices will be subject to all policies governing system use, including those involving administrative access to system components, while actively connected to the system.

1. Persons wishing to use privately owned information technology devices to access Board information technology services may be required to demonstrate to the satisfaction of the Chief Information Officer that their devices and software conform to the specifications of the information technology systems.

3. Selection and Operation of Information Technology Systems

Information technology systems can only achieve their intended purposes if they operate in an integrated fashion. Therefore, the selection, purchasing, allocation, installation, maintenance, replacement and governance of electronic information and communications systems necessarily involve the governmental policy-making responsibilities of the Board.

A. In its sole discretion, the Board shall select, purchase, allocate, install, maintain, replace and regulate the hardware, software or support services that comprise its information technology systems.
   1. The Board will make reasonable effort to support specialized information systems needed for research.

2. The Board will determine the extent of the authority granted to each user to access its information technology systems.

3. The Board will regulate uses that affect system performance or availability of system resources.

4. Administrative Monitoring, Access and Disclosure of Information Technology Systems Data or Contents

A. The Board safeguards the privacy and confidentiality of information and communications systems in accordance with relevant laws, regulations, and policies. While the Board permits limited personal use of the communications components within its information technology systems, persons availing themselves of this privilege do not acquire a right of ownership or privacy in communications transmitted or stored on university information technology resources,

B. The Board routinely monitors aggregate information technology system usage to assure proper system operation, but it does not routinely monitor use of information technology systems. Nevertheless, the Board will access components of information technology systems to conduct routine operation, troubleshooting, audit, maintenance or security activities; to investigate activities that disturb optimum information technology system operations; to recover documents or files needed for instructional, research, service or business activities; to respond to health or safety emergencies; to investigate violations of law, policy or rule; or to respond to inquiries properly initiated under law.

1. Routine maintenance may include remote access to components of information technology systems to install anti-virus programs, software updates or for other purposes designed to assure the integrity and optimal functioning of the information technology systems.

2. In the event that administrative monitoring of system operation or investigating apparent policy violation necessitates the inspection of a privately owned information technology device, the owner will be deemed to have consented to its inspection at all times when the device is actively connected to the information technology systems.

C. Individual users with access to communications components within the Board's information technology systems may access or disclose the content of communications in which they are intended correspondents; provided that the disclosure does not involve an unacceptable use under this policy or otherwise involve a violation of law, regulation or policy.

D. Reasonable administrative access to information technology and communication systems for purposes other than routine operation, troubleshooting, audit, maintenance

or security activities, will be authorized by the Board's Chief Information Officer (or such subordinates as that officer may designate), for good cause shown. The following circumstances illustrate, but do not limit, situations where access may be provided, with or without notice in accordance with law:

1. When requested by the Board of Regents General Counsel, or an attorney designated by the General Counsel for such purposes, in order to respond to a court order, subpoena, search warrant or other such duly issued mandate;

2. When requested for necessary business purposes by an appropriate system or institutional official, including, but not limited to, the Board of Regents General Counsel, or an attorney designated by the General Counsel to represent the institution, Chief Human Resources Officer, or the Vice President with administrative responsibility and supervision over the administrative unit, functions and staff that use the components of information technology systems for which access is sought;

3. When requested in furtherance of the legal, regulatory, or other applicable duties of the institution or the system;

4. When requested in the course of investigating potential violations of policy, rule or law; or

5. When requested in the course of responding to a health or safety matter.

5. Acceptable Use of Information Technology Systems

Use of the Board's information technology systems is a privilege and requires that individual users act responsibly. Individual users must respect the rights of other users, respect the integrity of the systems, and observe all relevant laws, regulations, and contractual obligations. Since electronic information is volatile and easily reproduced, users must exercise care in acknowledging and respecting the work of others through strict adherence to software licensing agreements, copyright, patent, trademark and trade secret laws. When accessing remote resources from Board or institutional facilities, users are responsible for following the policies of Board:

A. Authorization to access the information technology systems is granted only to support the administrative, research, instructional and service functions of the universities and special schools.

B. Authorized users may use the systems for incidental personal purposes provided that such use does not:

1. Directly or indirectly interfere with the Board's operation of such systems;

2. Interfere with the user's employment or other obligations to the Board,

3. Burden the Board with noticeable incremental costs, or

4. Violate law or Board policy;

6. Unacceptable Use

Notwithstanding any other provision of policy, certain uses of information technology systems are unacceptable, and persons who engage in such uses may be denied access to information technology systems peremptorily and referred for disciplinary action. Unacceptable use includes, but is not limited to, the following attempted or completed actions:

1. Infringing intellectual properties, including copyrights, patents, and trademarks;

2. Disclosing trade secrets or other information resident in the systems that is private, confidential or privileged;

3. Violating intellectual property licensing agreements;

4. Interfering with the normal operation of electronic communications resources, including, without limitation:

    a. Modifying, damaging or removing, without proper authorization, electronic information or communications system components or private electronic information or communications resources belonging to other users;

    b. Encroaching upon others' access and use of the electronic information and communications system, as exemplified, without limitation, by sending excessive numbers of messages, printing excessive copies, running grossly inefficient programs when efficient alternatives are available, attempting to crash or tie up electronic communications resources;

    c. Intercepting, monitoring or otherwise conducting surveillance of communications, whether live or stored, of others;

    d. Developing or using programs such as, but not limited to, viruses, backdoors, logic bombs, Trojan horses, bacteria, and worms that disrupt other users, access private or restricted portions of the system, identify security vulnerabilities, decrypt secure data, or damage the software or hardware components of an electronic communications resource; provided that supervised academic research into such mechanism may be conducted upon the review and approval of the chief institutional

academic affairs officer and the Board's Chief Information Officer (or such subordinates as that officer may designate), as to matters involving the compatibility of such research with the proper functioning of the information and communications systems;

e. Installing or attaching any equipment to the electronic information and communications system without the prior approval of the Board's Chief Information Officer (or such subordinates as that officer may designate);

5. Accessing electronic information or communications systems without proper authorization, intentionally enabling others to do so, or exceeding authorization;

   a. Any superior who directs a subordinate to access electronic information systems under circumstances that exceed the authorized access of the institution or organizational unit will be deemed to have indirectly exceeded authorized access and will be subject to discipline.

   b. Subordinates who decline to exceed authorized access to electronic information systems or who report efforts to induce them to do so will not, for those reasons, be subject to adverse employment action.

6. Disclosing, without authorization, the password to a password-protected account;

7. Using the system in an unlawful or tortious manner, in ways involving obscene materials or in violation of Board policies, including, without limitation:

   a. Using electronic information or communications systems for criminal purposes, including, without limitation, SDCL §§ 22-19A-1 (stalking); 22-22-24.2 (possession, manufacture or distribution of child pornography); 43-43B-1 (unlawful uses of computer systems); Omnibus Crime Control and Safe Streets Act of 1968 (unlawful interception of communications); Computer Fraud and Abuse Act (unlawful access to computer systems); Protection of Children Against Sexual Exploitation Act of 1977 (trafficking in child pornography);

   b. Distributing fraudulent, libelous, slanderous, harassing, threatening, or other tortious communications;

   c. Creating, downloading, exchanging or possessing obscene material as defined by SDCL § 22-24-27, unless previously authorized for bona fide instructional or research purposes;

   d. Harassing individuals in violation of Board policies proscribing harassment;

8. Using the identity of another user without the explicit approval of that user, or masking the identity of an account or machine or person;

9. Creating the false impression that the user has authority to represent, give opinions, tender endorsements or otherwise make statements on behalf of the Board or the institution;

10. Using the information and communications system for partisan political purposes, in violation of SDBOR Policy 4:21, or where the message could be reasonably construed as expressing the position of the institution itself~~other than the expression of private political views by participants in otherwise permitted communications, so long as the user specifically disclaims any support, endorsement, or opposition by the Board for the views so expressed~~;

11. Using the information and communications system for the purpose of ~~sectarian purposes, to provide sectarian instruction or to~~ benefit~~ting of~~ any sectarian or religious society or institution in violation of Article 6, § 3 of the SD Constitution~~, other than the use of religion-based rationale or expression by participants in otherwise permitted communications, so long as the user specifically disclaims any support, endorsement, or opposition by the Board for the views so expressed;~~.

12. Using the information and communications system for advertising, solicitations or promotions or other private commercial purposes, including personal purposes, except as permitted under Board policy or with the appropriate approval.

13. Using institutionally created mailing lists without specific prior authorization which may be granted solely for purposes of communicating institutional messages to recipients.

7. Temporary Suspension of Privileges and Disciplinary Measures

Authorized users will be subject to discipline for violation of this policy.

A. When alleged violations of this policy come to the attention of the Board's Chief Information Officer (or such subordinates as that officer may designate), the Chief Information Officer shall investigate the allegations and may temporarily suspend access privileges if necessary or appropriate to maintain the integrity of the system or to comply with the system's legal obligations.

    1. Temporary suspension of access privileges is not a disciplinary action, but it will be deemed to be a grievable matter.

B. Users, when requested, will cooperate with institutions in the investigation of suspected

violations of this policy. Failure to cooperate may result in suspension of access to the systems or to discipline.

C. If the investigation establishes reasonable grounds to believe that a user has violated this policy, the Board's Chief Information Officer (or such subordinates as that officer may designate) shall initiate disciplinary proceedings.

    1. The procedural and appeal rights of users will be based upon rights provided to similarly situated employees or students.

    2. To the extent that any employee or student disciplinary code or procedure is inconsistent with the requirements of this policy, this policy shall control.

D. Where the facts that would trigger disciplinary action under this policy may also constitute a criminal infraction under any state or federal law it may be reported to responsible authorities, whether or not disciplinary action is initiated.

SOURCE: BOR, October 2008, October 2013.