Office/Contact: Division of Technology and Security
Source: SDBOR Policy 7:1, SDBOR Policy 7:4
Link: https://www.sdbor.edu/policy/documents/7-1.pdf; https://www.sdbor.edu/policy/documents/7-4.pdf

SOUTH DAKOTA STATE UNIVERSITY
Policy and Procedure Manual

SUBJECT: Acceptable Use of Information Technology Systems
NUMBER: 7:5

1. Purpose

   This policy implements SDBOR Policy 7:1 and serves to assure the optimum functioning of the information technology systems that support University's administrative, research, instructional and service functions, and to protect them from abuse and from unlawful or other misuse.

2. Definitions

   a. Information technology system(s): technology that includes 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, including devices provided or supported by University such as desktops, laptops, iPads, cell phones, or any other electronic device used to access technology systems.

   b. User(s): any person or entity that accesses or utilizes computing resources, including, but not limited to, students, employees, faculty, staff, agents, vendors, consultants, visitors, contractors or subcontractors of the University.

3. Policy

   a. By using the SDBOR and University's information technology systems, users agree to abide by all relevant policies and procedures, as well as all current federal, state, and local laws.

   b. All information technology systems of the SDBOR and University are subject to this policy. 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. Persons wishing to use privately owned information technology devices to access SDBOR and University information technology services may be required to demonstrate to the satisfaction of the Vice President for Technology & Security, successor, or designee that their devices and software conform to the specifications of the information technology systems. The University does not provide technical support for technology, including computer systems or smartphones, purchased privately by users, regardless of whether University work is conducted on these systems.

c. Information technology systems can only achieve their intended purposes if they operate in an integrated fashion. Therefore, the SDBOR, and as delegated the University, is responsible for and at its sole discretion will select, purchase, allocate, install, maintain, replace, and regulate the hardware, software, or support services that comprise the University's information technology systems.

    i. Specialized information technology systems needed for research are subject to SDBOR and as delegated University approval, and the SDBOR and as delegated the University will make reasonable effort to support such systems.

    ii. The SDBOR, and as delegated the University, will determine the extent of the authority granted to each user to access the SDBOR and University's information technology systems and will regulate uses that affect system performance or availability of system resources.

d. The University, under the direction of the SDBOR, safeguards the privacy and confidentiality of information and communications systems in accordance with relevant laws, regulations, and policies. While limited personal use of the communications components within the SDBOR and University information technology systems is permitted, users availing themselves of this privilege will not acquire a right of ownership or privacy in communications transmitted or stored on the SDBOR or University's information technology systems.

e. The University, under the direction of the SDBOR, monitors aggregate information technology system usage to assure proper system operation, but it does not routinely monitor use of information technology systems. Nevertheless, the University and the SDBOR 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.

    i. 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.

    ii. 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 SDBOR and University's information technology systems.

f. Users with access to communications components within the SDBOR and University'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.

g. Reasonable administrative access to information technology and communications systems for purposes other than routine operation, troubleshooting, audit, maintenance, or security activities will be authorized by the Vice President for Technology & Security, successor, or designee, 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:

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

    ii. When requested for necessary business purposes by an appropriate system or University officer, including, but not limited to, the University Office of General Counsel, SDBOR General Counsel, or an attorney designated by the University Office of General Counsel or SDBOR General Counsel to represent the University, the Assistant Vice President for Human Resources, or designee, 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;

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

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

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

h. Use of the SDBOR or University's information technology systems is a privilege and requires that users act responsibly. 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 the University, users are responsible for abiding by the following principles:

    i. Authorization to access the information technology systems is granted only to support the administrative, research, instructional, and service functions of the University; and

    ii. Authorized users may use the information technology systems for incidental purposes provided that such use does not directly or indirectly interfere with the University's operation of such systems, interfere with the user's employment or other obligations to the University, burden the University with noticeable incremental costs, or violate law or University or SDBOR policies.

i. 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 the University's information technology systems definitively and referred for disciplinary

action. Unacceptable use includes, but is not limited to, the following attempted or completed actions:

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

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

iii. Violating intellectual property licensing agreements;

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

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

2. 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;

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

4. 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 review and approval of the Provost, or successor, and the Vice President for Technology & Security, or successor, as to matters involving the compatibility of such research with the proper functioning of information and communications systems;

5. Installing or attaching any equipment to the electronic information and communications system without prior approval from the Vice President for Technology & Security, or successor;

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

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

action.

2. 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.

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

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

1. Using electronic information or communications systems for criminal purposes, including, without limitation, SDCL §§ 22-19A-1 (stalking); 22-24A-3 (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);

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

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

4. Harassing individuals in violation of University or SDBOR policies proscribing harassment;

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

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

x. 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 University itself;

xi. Using the information and communications system for the purpose of benefitting any sectarian or religious society or institution in violation of Article 6, § 3 of the South Dakota Constitution;

xii. Using the information and communications system for advertising, solicitations, or promotions or other private commercial purposes, including personal purposes, except as permitted under University or SDBOR policies or with the appropriate approval;

1. Using email or other communication resources for broadcast or third party commercial advertising of meetings, events, and activities or to make announcements is prohibited. Email can be directed to specific individuals when this information comes from recognized University entities and organizations.

2. Broadcast advertising and announcement-making using email or other communication resources is permitted only in instances in which the University President or applicable Vice President considers the information to be critical to supporting the business activities of the University. Failure by individuals to distribute non-critical information in a timely matter via other communication means will not be relayed via broadcast email.

3. Advertising for events, meetings, or activities which are not officially sponsored by the University or its recognized groups or organizations is prohibited.

xiii. Using University created mailing lists without specific prior authorization, which may be granted solely for purposes of communication University messages to recipients.

xiv. Encryption or any other means taken by users to obfuscate communication not authorized by the University may be construed as purposefully evading this policy.

j. Authorized users will be subject to discipline or corrective action for violation of this policy, consistent with the rules applicable to their status with the University. Alleged violations of this policy should be directed to the Vice President for Technology & Security, successor, or designee, who is responsible for investigating 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.

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

k. When requested, users will cooperate with the University in the investigation of suspected violations of this policy. Failure to cooperate may result in suspension of access to the systems or disciplinary action.

l. If the investigation establishes reasonable grounds to believe that a user has violated this policy, the Vice President for Technology & Security, successor, or designee, is responsible for initiating disciplinary proceedings.

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

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

m. 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.

4. Responsible Administrator

   The Vice President for Technology & Security, successor, or designee, is responsible for the annual and ad hoc review of this policy. The University President is responsible for approval of modifications to this policy.

SOURCE: Approved by President on 11/17/2015. Revised, Approved by President on 01/30/2019. Revised; Approved by President on 02/22/2022.