

South Dakota Board of Regents

Policy Manual

SUBJECT: Information Technology Appropriate Use Policy

VERSION NUMBER 3 revised 03/20/03

1. Background and Purpose

Information Technology ("IT") Systems are provided at State expense. Therefore, all the laws of the State and all the normal rules of courtesy regarding impact on other Users apply. To help you understand how the State laws apply to you, and how your usage can diminish services to others, we provide the following Acceptable Use Policy ("AUP") as an explanation.

Information technology, the vast and growing array of computing and electronic data communications facilities and services, is used daily to create, access, examine, store, and distribute material in multiple media and formats. Information technology at the South Dakota Board of Regents and its Regental Institutions plays an integral part in the fulfillment of education, research, clinical, administrative, and other roles. Users of IT resources have a responsibility not to abuse those resources and to respect the rights of the user community as well as the BOR itself. This South Dakota Board of Regents IT Appropriate Use Policy (the "Policy" or "AUP") provides guidelines for the appropriate use of all BOR IT resources as well as for the BOR access to information about and oversight of these resources. BOR institutions may create their own AUP which augments this BOR AUP but may not create an AUP that supercedes this BOR AUP.

Most IT use parallels familiar activity in other media and formats, making existing BOR policies important in determining what use is appropriate. Using electronic mail ("email") instead of standard written correspondence, for example, does not fundamentally alter the nature of the communication, nor does it alter the guiding policies. BOR policies that already govern freedom of expression and related matters in the context of standard written expression govern electronic expression as well. This Policy addresses circumstances that are particular to the IT arena and is intended to augment but not to supersede other relevant BOR policies.

The purpose of this Policy is to ensure an information technology infrastructure that promotes the basic missions of the Universities in teaching, learning, research, extension and administration. In particular, this Policy aims to promote the following goals:

- To ensure that IT Systems support the basic missions of the BOR;
- To ensure the integrity, reliability, availability, and superior performance of IT Systems;
- To ensure that use of IT Systems is consistent with the principles and values that govern use of other BOR facilities and services;
- To ensure that IT Systems are used for their intended purposes; and
- To establish processes for addressing policy violations and sanctions for violators.

2. Scope

This Policy applies to all Users of IT Systems, including but not limited to students, faculty, staff, affiliated campus organizations or non-profit groups, and other individuals, groups and organizations relying on the BOR as a host through contractual relationships. It applies to the use of all IT Systems. These include but are not limited to IT Systems, and facilities administered by the BOR, as well as those administered by other BOR-based entities.

All use of IT Systems, even when carried out on a privately owned computer that is not managed or maintained by the BOR, is governed by this policy. That is, Users that connect privately owned IT Systems to BOR networks (for example, connecting a privately owned laptop in an office, classroom, lab or library) are subject to this BOR AUP.

3. Definitions

For purposes of this policy:

- The **BOR** is The South Dakota Board of Regents and its Regental Institutions including the six South Dakota State universities and two special schools and the combined facility in Sioux Falls as follows: Black Hills State University, Dakota State University, Northern State University, South Dakota School of Mines and Technology, South Dakota State University, the University of South Dakota, South Dakota School for the Blind and Visually Impaired, South Dakota School for the Deaf, USDSU in Sioux Falls, and all facilities associated with the above.
- The term “**IT Systems**” means the computers, terminals, printers, networks, modem banks, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by the BOR. For example, IT Systems include but are not limited to Universities and departmental information systems, faculty research systems, desktop computers, the campus network, and BOR general access computer clusters.
- The term “**Public IT Systems**” means IT Systems that are intended to be freely open to the entire campus community and guests. For example, Public IT Systems include but are not limited to public labs, public terminals in libraries (e.g. SDLN), and public terminals in the student centers for checking email. Contrasted with non Public IT Systems which, for example, include but are not limited to, IT Systems in private offices, departmental offices, secure locations (e.g. restricted access computer rooms), restricted access labs (e.g. Law School and Medical School), non public applications (e.g. Colleague, FIS, departmental file/print shares), and others not intended to be freely open to the entire campus community and guests.
- The term “**User**” is any person, whether authorized or not, who makes any use of any IT System from any location. For example, Users include a person who accesses IT Systems in a BOR computer lab or cluster, or via an electronic network.
- The term “**Systems Authority**” used in this policy means, while BOR is the legal owner or operator of all IT Systems, it may delegate oversight of particular IT systems to personnel designated by the BOR for that function.
- The term “**Systems Administrator**” means a person designated by System Authorities as "Systems Administrator" to manage the particular IT system assigned to him or her. Systems Administrators oversee the day-to-day operation of the IT systems.
- The term “**Security Administrator**” means a person designated by Systems Authority as Security Administrator which has been designated by the BOR and who has received Specific Authorization to access all IT Systems for the purpose of administering university policy and investigating IT policy violations. The Security Administrator may be the IT Security Officer or other IT Staff as designated by the Systems Authority.
- The term “**Certifying Authority**” means the Systems Authority or other BOR authority who certifies the appropriateness of an official document for electronic publication in the course of BOR business.
- The term “**Specific Authorization**” means documented permission provided by the applicable Systems Authority or Certifying Authority either directly in writing or indirectly through job descriptions and the like.
- The term “**IT Staff**” means those employees (including consultants) of the BOR that provide support services to the BOR (including but not limited to software installation, hardware installation, troubleshooting of IT Systems, administration of IT Systems, monitoring of IT Systems and programming of IT Systems). IT Staff typically have more privileged access to IT Systems than other Users.
- An **Incident** is a suspected, observed or reported breach of the BOR AUP whether observed directly, observed through monitoring of systems or networks, alleged by any person or suspected through analysis of logs or emails or other documents.
- **Point of Contact.** Systems authorities may designate another person or facility such as a help desk as a Point of Contact for receiving incident reports.
- A **Chief Information Officer (CIO)** and a **Chief Information and Technology Officer (CITO)** are interchangeable for purposes of this document.

4. Appropriate Use of IT Systems

Although this Policy sets forth the general parameters of appropriate use of IT Systems, faculty, students, and staff should consult their respective governing policy manuals for more detailed statements on permitted use and the extent of use that the BOR considers appropriate in light of their varying roles within the community. In the event of conflict between IT policies, this Appropriate Use Policy will prevail.

A. Appropriate Use. IT Systems may be used only for their authorized purposes -- that is, to support the research, education, administrative, and other functions of the BOR. The particular purposes of any IT System as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the User. In addition, Users must respect the rights of other Users.

B. Proper Authorization. Users are entitled to access only those elements of IT Systems that are consistent with their authorization.

C. Specific Proscriptions on Use. The following categories of use are inappropriate and prohibited:

1. Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others. Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including by "resource hogging" (such as peer-to-peer file sharing), excessive file downloading, excessive file uploading, excessive game playing, excessive printing, misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages). Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.

2. Use that is inconsistent with BOR missions. The BOR is tax-exempt and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of IT Systems for non-BOR purposes is generally prohibited, except if specifically authorized and permitted under BOR and other related policies. Prohibited commercial use does not include communications and exchange of data that furthers the BOR educational, administrative, research, and other roles, regardless of whether it has an incidental financial or other benefit to an external organization.

3. Harassing or threatening use. This category includes, for example, display of offensive, sexual material in the workplace and repeated unwelcome contacts with other Users.

4. Use damaging the integrity of University or other IT Systems. This category includes, but is not limited to, the following six activities:

a. Attempts to defeat system security. Users must not defeat or attempt to defeat any IT System's security (physically, digitally or by other means)-- for example, by "cracking" or guessing and applying the identification or password of another User, sharing passwords, sharing User account IDs, using another User's access to violate this AUP or compromising room locks or alarm systems. (This provision does not prohibit, however, System or Security Administrators from using traffic monitoring, traffic capture and security scan programs within the scope of their Systems Authority.)

b. Unauthorized access or use. The BOR recognizes the importance of preserving the privacy of Users and data stored in IT systems. Users must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. For example, a non BOR organization or individual may not use non Public IT Systems without specific authorization. Privately owned computers may be used to provide public information resources, but such computers may not host sites or services for non-BOR organizations or individuals across the BOR networks

without specific authorization. Similarly, Users are prohibited from accessing or attempting to access data on IT Systems that they are not authorized to access. Furthermore, Users must not make or attempt to make any deliberate, unauthorized changes to data on IT Systems. Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, network monitoring or otherwise tapping phone or network lines or other communication systems (except for System or Security Administrators as in the above 4.C.4.a).

c. **Disguised use.** Users must not conceal their identity when using IT Systems, except when the option of anonymous access is explicitly authorized such as anonymous FTP. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity (such as another User's account ID).

d. **Distributing computer viruses.** Users must not knowingly distribute or launch computer viruses, worms, or other malicious programs.

e. **Modification or removal of data or equipment.** Without specific authorization, Users may not remove or modify any BOR-owned or administered equipment or data from IT Systems.

f. **Use of unauthorized devices.** Without Specific Authorization, Users must not attach any device to IT Systems (such as but not limited to an external disks, printers, switches, hubs, routers, wireless access points, web servers, email servers, network "sniffers", keystroke monitors, network traffic capture programs or video systems).

g. **Violation of Copyright Laws.** Users are prohibited from using, making, distributing, helping others use, make or distribute unauthorized copies of copyrighted material. This includes but is not limited to forms of copyrighted material such as printed, electronic music files, electronic pictures, software, or electronic video files. Users should be aware of their responsibilities under regulations such as the Digital Millennium Copyright Act (DMCA).

h. **Violation of License Agreements.** Users must follow their license agreements. Users must not install, request installation of, copy or distribute software in violation of software license agreements.

i. **Family Educational Rights and Privacy Act (FERPA).** Users should be aware of the data protection responsibilities placed on the BOR and Users by federal regulations such as FERPA governing disclosure of data such as student information.

5. **Use in violation of law.** Illegal use of IT Systems -- that is, use in violation of civil or criminal law at the federal, state, or local levels -- is prohibited. Examples of such uses, but not limited to, are: promoting a pyramid scheme; distributing illegal obscenity; receiving, transmitting, or possessing child pornography; infringing copyrights; and making bomb threats. South Dakota has enacted legislation that defines illegal activities associated with IT Systems. Users should be aware of laws such as S.D.C.L. 43-43B-1 and 43-43B-7 and changes to these laws legislated by S.B. 184.

With respect to copyright infringement, Users should be aware that copyright law governs (among other activities) the copying, displaying, and using of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

6. **Use in violation of BOR contracts.** All use of IT Systems must be consistent with the BOR contractual obligations, including limitations defined in software and other licensing agreements.

7. **Use in violation of BOR policy.** Use in violation of BOR policies also violates this AUP. Relevant BOR policies include, but are not limited to, those regarding sexual harassment and racial and ethnic harassment, as well as BOR, BOR departmental, and work-unit policies and guidelines regarding incidental personal use of IT Systems.

8. **Use in violation of external data network policies.** Users must observe all applicable policies of external data networks when using such networks.

9. **Use in violation of IT Staff Agreements.** IT Staff have special privileges with regard to IT Systems. IT Staff must adhere to terms of their confidentiality agreements and not knowingly violate or cause other Users to violate their agreements or this AUP.

D. Free Inquiry and Expression. Users of IT Systems may exercise rights of free inquiry and expression consistent with the principles of the BOR and within the limits of the law.

E. Personal Account Responsibility. Users are responsible for maintaining the security of their own IT Systems accounts and passwords. Any User changes of password must follow published guidelines for passwords. Accounts and passwords are normally assigned to single Users and are not to be shared with any other person without authorization by the applicable Systems Administrator. Users are presumed to be responsible for any activity carried out under their IT Systems accounts or posted on their personal web pages. Therefore, Users are not to divulge (and should not be asked by their supervisors to divulge) their passwords to anyone.

F. Encryption of Sensitive Data. Users are encouraged to encrypt sensitive files, documents, and messages for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks. Software and protocols used ~~must~~ should be endorsed by Information Security personnel ~~that~~ and provide robust encryption, as well as the capability for properly designated BOR personnel to decrypt the information, when required and authorized under this policy. Users who elect not to use endorsed encryption software and protocols on IT Systems are expected to decrypt information upon official, authorized request. Users should be aware that encrypted files in storage may not be recoverable by support personnel if they become corrupt or the User loses the encryption key.

G. Responsibility for Content. Official BOR information may be published in a variety of electronic forms. The Certifying Authority under whose auspices the information is published is responsible for the content of the published document.

Users also are able to publish information on IT Systems or over BOR networks. Neither BOR, nor individual IT staff, systems administrators nor security administrators will screen such privately published material (except in accordance with Conditions of BOR Access) nor can they ensure its accuracy or assume any responsibility for its content. The BOR will treat any electronic publication provided on or over IT Systems that lacks a Certifying Authority as the private speech of an individual user.

H. Personal Identification. Upon request by a Systems Administrator or Security Administrator or other BOR administrator, Users must produce valid BOR identification.

5. Conditions of BOR Access

The BOR places a high value on privacy and recognizes its critical importance in an academic setting. There are nonetheless circumstances in which, following carefully prescribed processes, the BOR may determine that certain broad concerns outweigh the value of a User's expectation of privacy and warrant BOR access to relevant IT Systems without the consent of the User. Those circumstances are discussed below, together with the procedural safeguards established to ensure access is gained only when appropriate.

A. Conditions. In accordance with state and federal law, BOR authorized personnel may access all aspects of IT systems, without the consent of the User, in the following circumstances:

1. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT Systems;
2. When required by federal, state, or local law or administrative rules;
3. When there are reasonable grounds to believe that a violation of law or a significant breach of BOR policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct;
4. When such access to IT Systems is required to carry out essential business functions of the BOR;
or
5. When required to preserve public health and safety.

B. Process. Consistent with the privacy interests of Users, BOR access without the consent of the User will occur only with the approval of the BOR or their respective delegates, except when an emergency entry is necessary to preserve the integrity of facilities or to preserve public health and safety. The BOR, through the Security and Systems Administrators, will log all instances of access without consent. Security and Systems Administrators will also log any emergency entry within their control for subsequent review by the appropriate BOR Systems Authority. A User will be notified of BOR access to relevant IT Systems without consent, pursuant to Section 5. A. (1-5).-Depending on the circumstances, such notification may occur before, during, or after the access, at the discretion of the BOR.

C. User access deactivations. In addition to accessing the IT Systems, the BOR, through the appropriate Security or Systems Administrator, may deactivate a User's IT privileges, whether or not the User is suspected of any violation of this policy, when necessary to preserve the integrity of facilities, user services, or data. The Security or Systems Administrator will attempt to notify the User of any such action.

D. Use of security scanning systems. By attaching privately owned personal computers or other IT resources to BOR networks, Users consent to BOR use of scanning programs by Security Administrators for security purposes on those resources while attached to the network.

E. Logs. Most IT systems routinely log user actions in order to facilitate recovery from system malfunctions and for other management purposes. All Systems Administrators are required to establish and post policies and procedures concerning logging of User actions, including the extent of individually identifiable data collection, data security, and data retention.

F. Encrypted material. Encrypted files, documents, and messages may be accessed by the BOR under the above guidelines. See Section 5 A, above.

6. Incident Handling and Reporting

This Policy sets forth the general parameters of Incident handling for IT Systems. Faculty, students, and staff should consult their respective governing policy manuals for more detailed statements on permitted use and the extent of use that the BOR considers appropriate in light of their varying roles within the community. In the event of conflict between IT policies, the BOR CIO will decide which applies.

- A. **Warnings and alerts.** Users are not authorized to issue or forward warnings regarding IT systems without Specific Authorization from a Systems Authority or IT Staff. The designated IT Staff are to subscribe to the appropriate services for receiving alerts and warnings. IT staff will verify the authenticity of alerts in warnings before forwarding them to Users.
- B. **Reporting Incidents.** If an individual has observed or otherwise is aware of a violation of this AUP or other BOR IT policy whether or not they've been harmed by the alleged violation, he or she should report it promptly. Incidents are to be reported to the Systems Authority overseeing the facility most directly involved, or to the local Security Administrator, or to the BOR Security Officer or other designated BOR authority (such as campus security/police), which must investigate the allegation. When appropriate, persons investigating incidents are to refer the matter to BOR disciplinary and/or law enforcement authorities.

Security Administrators must report Incidents to the registered Point of Contact when sites other than BOR IT Systems are involved.

When Users are reporting an Incident which they feel should involve law enforcement they should refer to local policy for contacting the appropriate law enforcement agency starting with local campus security/police. Users should also be encouraged to contact the local Point of Contact, Systems Authority, or IT Security Administrator.

- C. **Authorized Incident Investigation.** Confidentiality and proper investigation are important elements of an Incident investigation. It is important that only persons with Specific Authorization conduct these investigations as they might be exposed to private or confidential information. Some types of Incidents such as virus infections may be resolved by running virus cleaning utilities which can be done by Users or IT Staff. Other types of Incidents such as but not limited to unauthorized use, harassment, malicious code placement, and criminal offenses may require forensic investigation including accessing, monitoring, scanning or disconnecting IT Systems without Users permission. The circumstances for access without Users permission are covered in 5. A. (1-5). The CIO has authorized the Security Administrator to conduct these investigations. In addition, the CIO or the Security Administrator may designate others on a case by case basis to assist in these investigations because of their specialized skills or knowledge of IT Systems.
- D. **Unauthorized Incident Investigation.** Except as indicated in 6.C. above, Incident investigation by persons without Specific Authorization is prohibited. Departmental management must not request persons without Specific Authorization perform these investigations. Users with access to IT systems for purposes of technical support must neither seek nor assist others in obtaining unauthorized access to IT systems unless they are requested to do so, by the CIO or the Security Administrator.
- E. **Confidentiality.** The BOR recognizes the importance of preserving the privacy of Users and data stored on IT Systems. Some data may be protected by local, state or federal laws such as FERPA or HIPAA. Users, Systems Administrators, IT Staff and Security Administrators must honor this principle by neither disclosing nor discussing the contents of IT Systems, nor disclosing the identity of persons alleged to be involved in Incidents nor the actions or outcomes of investigations which information is not publicly disclosed by others with Specific Authorization to do so.
- F. **Incident Reporting by Investigator.** Incidents are to be logged by the person doing the investigation. The CIO will designate the Point of Contact to be notified according to the type and severity of the Incidents. For example, virus infections may not need to be reported to anyone outside the IT support organization while criminal activity may be required to be reported to the appropriate law enforcement agencies as required by local, state and federal laws. It is the responsibility of the investigator to follow the local notification policies and log these contacts.
- G. **Authority to Act.** During the investigation of an incident it may be necessary to shut down IT Systems in order to prevent further damage or compromise of IT Systems. The CIO may delegate this decision to Systems Administrators, Security Administrators or other IT Staff. It may also be necessary to monitor IT Systems traffic or use electronic scanning tools in order to either verify that an Incident is taking place or to obtain evidence to be used later in the investigation or after the investigation for legal purposes. Only Security Administrators are authorized to take these actions. Others must obtain Specific Authorization to act from either the CIO, or Security Administrator.
- H. **Goal of Operating Through Incidents.** The BOR recognizes the importance of keeping IT Systems running. While some Incidents are not harmful to IT Systems some Incidents are attacks on IT Systems specifically designed to damage or affect the performance of IT Systems if they are not promptly acted upon. When IT Systems are shut down because of an Incident the goal of the IT staff is to bring the IT Systems back on-line as soon as they reasonably can. The goal of the BOR is to maintain high availability of IT Systems rather than keep systems shut down in an effort to pursue prosecution of persons perpetrating attacks especially if in the opinion of the Security Administrator the person or persons cannot be identified promptly.

7. Enforcement Procedures

A. **Complaints of Alleged Violations.** An individual who believes that he or she has been harmed by an alleged violation of this Policy may file a complaint in accordance with established BOR Grievance Procedures (including, where relevant, those procedures for filing complaints of sexual harassment or of racial or ethnic harassment) for students, faculty, and staff. The individual is also encouraged to report the alleged violation to the Systems Authority overseeing the facility most directly involved, who must investigate the allegation and (if appropriate) refer the matter to BOR disciplinary and/or law enforcement authorities.

B. Disciplinary Procedures. Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the BOR Faculty Handbook, Staff Personnel Policies and Practices Manual, various student regulations (e.g., the Undergraduate Regulations for undergraduates, the relevant policy manuals for graduate and professional school students), and other applicable materials. Staff members who are members of BOR-recognized bargaining units will be disciplined for violations of this policy in accordance with the relevant disciplinary provisions set forth in the agreements covering their bargaining units.

Disciplinary action may include the loss of computing access and other disciplinary sanctions up to and including non-reappointment, discharge, dismissal and legal action. Violators may also be liable for civil or criminal prosecution under local, state, federal laws or regulations. ~~and~~ Actions by the BOR are NOT in place of actions which may be taken by the BOR, university, local, state or federal law enforcement or other authorities.

Security and Systems Administrators may participate in the disciplinary proceedings as deemed appropriate (such as providing testimony or affidavits) by the relevant disciplinary or legal authority. Moreover, at the direction of the appropriate disciplinary authority, Security and System Administrators are authorized to investigate alleged violations.

C. Penalties. Individuals found to have violated this policy may be subject to penalties provided for in policies dealing with the underlying conduct. Violators, including IT Staff, may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The appropriate penalties shall be determined by the applicable disciplinary authority in consultation with the Security Administrator or as defined in 5.B. above.

D. Legal Liability for Unlawful Use. In addition to BOR discipline, Users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT System. BOR disciplinary action does NOT in any way substitute for prosecution under local, state or federal laws.

E. Appeals. Users found in violation of this policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.

**SOURCE: BOR Acceptable Use Policy drafts July 1, 2002 and October 28, 2002.*

This Policy supersedes existing BOR IT Appropriate Use Policy.

This Policy may be periodically reviewed and modified by the BOR, who may consult with relevant committees, faculty, students, and staff.

URL = http://www.hpcnet.org/cgi-bin/global/a_bus_card.cgi?SiteID=341534

Works consulted:

The SANS Security Policy Project
EDUCAUSE Policy Initiatives Program
Yale University AUP
Cornell University AUP
University of Missouri at Kansas City AUP
Black Hills State University AUP
Dakota State University AUP
Northern State University AUP
South Dakota School of Mines and Technology AUP
South Dakota State University AUP
University of South Dakota AUP
North Dakota State University AUP
FedCIRC Incident Reporting Criteria and Rationale
CERT Incident Reporting Guidelines