SOUTH DAKOTA BOARD OF REGENTS

Policy Manual

SUBJECT: Security of Information Technology Systems

NUMBER: 7:4

A. PURPOSE

To define the role and authority of Information Technology Services (ITS) in supporting and upholding the security and integrity of the Board of Regents (BOR) information technology (IT) environment.

B. DEFINITIONS

1. **Board of Regents:** Includes the system office, the six public universities, centers, the School for the Deaf, and the School for the Blind and Visually Impaired.
2. **Computing Resources:** All devices including, but not limited to, personal computers, laptops, PDAs and smart phones owned by the BOR, the user or otherwise, which are part of or are used to access:
   - Network peripherals and related equipment and software;
   - Data communications infrastructure, peripherals, and related equipment and software;
   - Voice communications infrastructure, peripherals, and related equipment and software; and,
   - All other associated tools, instruments, facilities, and services that make use of any technology resources owned, operated, or controlled by an institution.

   Computing Resources or components thereof may be individually assigned or shared, single-user or multiuser, stand-alone or networked, mobile or stationary.
3. **Data:** Includes all information and data that is used by or belongs to the BOR or that is processed, stored, maintained, transmitted, copied on, or copied from BOR computing resources.
4. **Functional Unit(s):** Includes any campus, college, program, service, department, office, operating division, vendor, facility or other entity or defined unit of BOR that has been authorized to access or use computing resources or data.
5. **Protected Information:** Data or information that has been designated as private, protected, or confidential by law or by BOR. Protected information includes, but is not limited to, employment records, medical records, student records, education records, personal financial records (or other individually identifiable information), research data, trade secrets, and classified government information. Protected information shall not

include public records that by law must be made available to the general public. To the extent there is any uncertainty as to whether any data constitutes protected information, the data in question shall be treated as protected information until a determination is made by the BOR.

6. **Security Breach:** Any known or suspected compromise of the security, confidentiality, or integrity of data or computing resources that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and/or access to data. Good faith access or acquisition of data by an individual or functional unit is not a breach of the security of the system provided that the information is not improperly used or subject to subsequent unauthorized access, use, or disclosure.
7. **User:** Any person or entity that utilizes computing resources including, but not limited to, employees, faculty, staff, agents, vendors, consultants, contractors or subcontractors of the institution.

C. POLICY

Institutions of higher education are subject to various regulatory requirements designed to protect the privacy of education records, financial information, medical records, and other personal information maintained by BOR entities relative to its students and employees. Further, the BOR seeks to maintain as confidential certain research data, intellectual property, and other proprietary information owned, licensed, or otherwise maintained or used by the BOR. IT systems that are not properly secured are subject to misuse and/or unauthorized access. Everyone associated with providing and using information technology services should be diligent in their protection of data, use of computing resources, administration and maintenance of systems, response to security threats, and policies and directives. Information related to intrusions, attempted intrusions, unauthorized access, misuse, or other abnormal or questionable incidents should be quickly reported to Information Technology Services, so the event can be recognized, mitigated, and hopefully avoided.

1. Responsibilities

1.1. BOR functional units operating or utilizing computing resources are responsible for managing and maintaining the security of the data, computing resources and protected information. This requirement is especially important for those computing resources that support or host critical business functions or protected information.

1.2. The chief information officers (CIO) or security officers have the authority to:

- develop and implement policies necessary to minimize the possibility of unauthorized access to protected information and BOR information technology infrastructure;
- consult and educate users and functional units relative to their individual and collective responsibilities to protect data and secure computing resources; and
- take reasonable actions to mitigate incidents or concerns relating to security of data or computing resources. This includes establishing guidelines, procedures, standards, and security resources, conducting security audits, and providing consulting services to functional units for all BOR and institutional computer systems or other computing resources.

1.3. Users within functional units are required to report any suspected or known security breaches or flaws relating to the security of BOR computing resources to the institution CIO or security officer. They will assess reported breaches and flaws and provide advice as to an appropriate response as well as report appropriate security attempts or breaches to the Chief Networking and Security Officer. A failure to report suspected or known security breaches or flaws is cause for disciplinary action, including termination of employment. Users should immediately discontinue any use of computing resources or practice that could reasonably lead to a security breach.

1.4. The Chief Networking and Security Officer, local CIO, or security officer has the authority to assume control over the response to any suspected or known security breach or flaw involving BOR's information technology infrastructure, data, and computing resources regardless of the functional unit involved. Appropriate remedies may be taken to secure the computing resources and mitigate any unauthorized use, disclosure, or access to data, including the removal of devices to more secure facilities and denying access to computing resources and/or data. This authority will be exercised if the IT personnel determines that the functional unit does not have the means and/or ability to access and/or react appropriately in a timely manner to a specific security incident.

2. Reporting Security Breaches

2.1. Intrusion attempts, security breaches, and other security related incidents or flaws perpetrated against or involving computing resources either attached to a BOR operated network or in a functional unit shall be reported immediately to the Chief Networking and Security Officer, campus CIO or security officer. This is critical for systems supporting vital functions and/or hosting institutional or protected information. Users within functional units must:

- Report any security breaches in order to obtain advice and assistance;
- Report any systematic unsuccessful attempts (i.e. log in attempts, probes, or scans); and
- When feasible, send detailed reports as soon as the situation is detected.

3. Response to Attempts or Security Breaches

3.1. Upon receiving a report, the CIO, security officer or Chief Networking and Security Officer will respond according to ITS standard operating procedures. In order to protect institutional data and systems, as well as to protect threatened systems external to the institution, the IT personnel may place limits or restrictions on technology services provided on or from any computing resources.

3.1.1. Limitations may be implemented through the use of policies, standards, and/or technical methods and could include, but may not be limited to, usage eligibility rules, password requirements, or restricting or blocking certain protocols or use of certain applications known to cause security problems.

3.1.2. Restrictions may be deployed permanently based on continuing threat or risk after appropriate consultation with affected constituents, or they may be deployed temporarily, without prior coordination, in response to an immediate and serious threat.

3.1.3. Restrictions deployed temporarily will be removed when the risk is mitigated to an acceptable level, or where the effect on BOR functions caused by the restriction approaches or exceeds risk associated with the threat.

3.2. In order to protect BOR data and systems, as well as to protect threatened systems external to BOR, the Chief Networking and Security Officer or CIO may unilaterally direct that a specific computing resource be isolated from BOR, campus, or external networks, given:

- Information reasonably points to the system as having been compromised;
- There is ongoing activity associated with the system that is causing or will cause damage to other institutional computing resources or data, or to systems of other internal or external users, or where there is significant risk of such damage occurring;
- All reasonable attempts have been made to contact the responsible technicians or functional unit management, or contact has been made but the technician or functional unit managers are unable to or choose not to resolve the problem in a reasonable time.

3.3. Isolation is removed when the risk is mitigated to an acceptable level, or where loss of access or function caused by the isolation approaches or exceeds risk associated with the threat, as determined between the responsible functional unit, Chief Networking and Security Officer, local CIO or security officer.

FORMS / APPENDICES:

None

SOURCE:

BOR December 2010, May 2019.