SOUTH DAKOTA BOARD OF REGENTS

Budget and Finance

AGENDA ITEM: 7 – S (5)
DATE: April 2-4, 2019

****

SUBJECT

New BOR Policy 7:7 – Personally Identifiable Information (Second Reading)

CONTROLLING STATUTE, RULE, OR POLICY

Gramm-Leach-Bliley Act (GLBA)
Health Insurance Portability and Accountability Act (HIPAA)
Family Educational Rights and Privacy Act (FERPA)

BACKGROUND / DISCUSSION

Protecting student and employee data is of the utmost importance to the universities and the Board of Regents. In December 2017, the Board approved BOR Policy 5:14 – Protection of Social Security Numbers as an initial step to protect data. BOR Policy 7:7 – Personally Identifiable Information is a broader policy that addresses not only Social Security Numbers (SSNs) but also the use, handling and storage of any personally identifiable information including names, birth dates, financial account information, driver's licenses, education records, photos, etc. as defined in the policy.

This policy has been reviewed by legal counsel, the Business Affairs Council (BAC), the Academic Affairs Council (AAC), Human Resources, and the Council of Presidents and Superintendents (COPS). After further review by the Technology Affairs Council (TAC), additional changes have been made since the first reading by the Board in December 2019. Those additional changes are highlighted in yellow on the attached.

IMPACT AND RECOMMENDATIONS

Protecting personal information has become paramount in this age of cyber scams, attacks and breeches. This policy addresses the necessary use and protection of all personally identifiable information that must be handled with care.

ATTACHMENTS

Attachment I – BOR Policy 7:7 – Personally Identifiable Information

****

DRAFT MOTION 20190402_7-S(5):

I move to approve the second reading of the new BOR Policy 7:7 – Personally Identifiable Information as shown in Attachment I.

SOUTH DAKOTA BOARD OF REGENTS

Policy Manual

SUBJECT: Personally Identifiable Information

NUMBER: 7:7

A. PURPOSE

To ensure members of the university community employ reasonable and appropriate administrative, technical, and physical safeguards to protect the integrity, confidentiality, and security of all personally identifiable information (PII), irrespective of its source or ownership or the medium used to store it. All individuals who review, have access to, dispense, receive, or store personally identifiable information have responsibilities to safeguard it.

B. DEFINITIONS

1. **Data Trustee:** These are institutional or school officials who are responsible for data accuracy, integrity and security and who have oversight, planning and policy-making responsibilities within their respective areas of regental institutional operations.
2. **Data Steward:** A Data Steward establishes procedures for handling PII in accordance with this policy. The Data Steward is authorized to grant, modify, and revoke access privileges for PII within their purview as assigned by the Data Trustee.
3. **Data Custodian:** Any person that collects, handles, or utilizes data classified as personally identifiable information by the institution including employees, volunteers, students, vendors, contractors, auditors, or a person or organization acting as an official agent of the institution and performing a business function or service on behalf of the institution.
4. **Minimum Necessary:** This is the standard of collecting and utilizing the least amount of information and to have the fewest number of people required to satisfactorily perform a particular function accessing the data.
5. **Personally Identifiable Information (PII)**: Personally identifiable information includes information that can be used to distinguish or trace an individual's identify or, when combined with other personal or identifying information, is linked or linkable to a specific individual. PII includes the following specific information, but is not limited to these items:
    - Name (used in conjunction with other elements below)
    - Social security numbers (SSN)
    - Financial account information as governed by Gramm-Leach Bliley Act (GLBA) – Nonpublic Personal Information that is collected by the institution about an individual in connection with providing financial services including credit card

information, bank account information, debit card numbers, and account payment information

- Cardholder data as governed by the Payment Card Industry requires that the primary account number when stored, processed, or transmitted with the cardholder's name, service code, and/or expiration date be protected in accordance with applicable Data Security Standards
- Driver's license or other government-issued identification numbers
- Protected health information as defined by the Health Insurance Portability and Accountability Act (HIPAA) is information, including demographic information data, that relates to the individual's past, present, or future physical or mental health or condition, data related to the provision of health care to individuals, or any record tied to the payment of healthcare services.
- Student education records as defined by Family Educational Rights and Privacy Act (FERPA) – All records maintained by the institution that directly relate to a current or former student. Student records include written, electronic, video, audio and photos.
- Non-public pictures
- Date and place of birth (used in conjunction with other elements listed above)
- Mother's maiden name (used in conjunction with other elements listed above)

C. POLICY

1. Use of Personally Identifiable Information

1.1. PII may be utilized or shared only on a minimum necessary basis and only to those individuals who are authorized to use such information as part of their official university duties, subject to the following requirements:

- The PII released is narrowly tailored to a specific business requirement;
- The information is appropriately safeguarded and used only for the specific official university business purpose for which authorization was obtained;
- The PII is not further disclosed or provided to others without proper authorization by the appropriate data trustee.

2. Handling of Personally Identifiable Information

2.1. Personally identifiable information shall be collected, stored, transmitted and disposed of using the following guidelines. Each organizational unit of the institution is responsible for ensuring that personally identifiable information with their unit is:

2.1.1. Collected only as necessary in conjunction with academic and business needs as determined by data trustees;

2.1.2. Restricted in its distribution and accessibility as is consistent with good internal control practices, where employees with access to information are trained and informed of applicable restrictions;

2.1.3. Properly secured by the use of such safeguards as secured file storage and rooms, encryption, security controlled access, and other appropriate technology tools;

2.1.4. Disposed of through approved secure means such as shredding and erasing hard drives and other media.

2.2. PII shall be shared internally only on a need-to-know basis and externally only consistent with law, business and educational necessity with adequate protections. PII provided to third parties must be under the strict guidance that the information be kept secure and used only for a specific official authorized business purpose and shall be governed by written confidentiality agreements signed by both parties including provisions to have the PII destroyed via approved methods upon termination of agreements.

3. Responsibility for Sensitive and Confidential Information

3.1. Data trustees are responsible for administering the PII policy and providing necessary training to their staff. Further, data trustees are required to have an auditing plan to insure compliance and to modify or revoke privileges and to report violations when they are identified. See BOR Policy 3:5 – Confidentiality of Student Records for compliance with the Family Education Rights and Privacy Act (FERPA).

3.2. Custodians of personally identifiable information shall strive to minimize the collection, use and release of personally identifiable information regardless of its source or medium to the minimum necessary required to complete a particular transaction or to fulfill a particular purpose.

3.3. Responsibility to manage and oversee personally identifiable information is usually held at the highest level of oversight within each unit. Board of Regents or university counsel, the Registrar (student data), Human Resources (employee data), or the CIO shall be consulted when there is any doubt about the use, release, restrictions or laws governing PII.

3.4. Data stewards shall be identified and entrusted with the authority to grant, modify, and revoke access privileges as determined and authorized by data trustees.

3.5. Consistent with applicable state or federal law, university or board policy, custodians of personally identifiable information shall take reasonable and appropriate steps to limit access to and further use or transfer of information, and ensure the information is maintained in a form and manner that is appropriately secure in light of the nature and sensitivity of the information. See BOR Policy 7:4 – Security and IT Systems for further clarification of data management and maintenance responsibilities.

4. Violations of Policy

4.1. Violations of this policy resulting in the misuse of, unauthorized access to, or unauthorized disclosure or distribution of personally identifiable data may subject individuals to legal or disciplinary action, in accordance with the procedures

applicable to the status of the individual, up to and including the termination of employment, student status, or contract with the institution, or in the case of students, suspension or expulsion from the institution.

4.2. Known or suspected violations of this policy should be reported to the data trustee, security officer, or the university CIO promptly. Upon receiving such notice, the data trustee will notify the university CIO. Upon determining and assessing the extent and significance of the violation, the university CIO shall appropriately escalate the violation to the appropriate personnel including the BOR CIO, human resource director, university and BOR legal counsel.

5. Photography Use

5.1. Photographs of students are considered directory information so long as they are used only for university purposes. Therefore, if a student has not requested that the university maintain the confidentiality of the student's directory information, the university is not prohibited by FERPA from using and publishing photographs of the student, along with the student's name, solely for university administrative and directory purposes.

5.2. Private photographs or videos of students cannot be used publicly without student's permission.

5.2.1. A Photography Release shall be used with subjects, such as staff, faculty, and alumni, who are not covered by FERPA. The Photography Release shall also be used with students who are covered by FERPA, but who the university will be using for promoting in a significant way in either a print or electronic medium (for example, on the Internet or in slide shows or videos). The Photography Release will clarify the rights and responsibilities of both the subject and the institution.

5.3. General Campus and Event Photography – As a general rule, it is not necessary to obtain a release from any individual or group photographed in a public venue or while attending a public event.

FORMS/APPENDICES:

None

SOURCE:

BOR _____, 2019.