SOUTH DAKOTA BOARD OF REGENTS

Budget and Finance

AGENDA ITEM: 7 – O

DATE: October 3-5, 2017

****

SUBJECT: New BOR Policy 5:14 – Protection of Social Security Numbers (First Reading)

Protecting the personal information of all members of the Regental community is a foremost commitment of the Board. The attached policy regarding the collection, storage, use and disclosure of social security numbers has been reviewed by the Council of Presidents and Superintendents (COPS), the Business Affairs Council (BAC), the Academic Affairs Council (AAC), the Technology Affairs Council (TAC), and the Human Resource Directors with suggested changes being incorporated.

A more comprehensive policy regarding personally identifiable information (PII) is being developed.

****

DRAFT MOTION 20171003_7-O: I move to approve the first reading of the new BOR Policy 5:14 – Protection of Social Security Numbers.

SOUTH DAKOTA BOARD OF REGENTS

Policy Manual

SUBJECT: Protection of Social Security Numbers

NUMBER: 5:14

A. PURPOSE

To protect personal information of all members of the regental community. The Federal Privacy Act of 1974 provides guidelines regarding state agency requests and stewardship of a social security number. This policy addresses the collection, storage, use, and disclosure of Social Security Numbers ("SSNs") for all students, faculty, staff, and other officially associated individuals.

B. DEFINITIONS

None

C. POLICY

1. Collection and Use of Social Security Numbers

SSNs shall be lawfully collected and used for the following purposes:

- Employment or Other Appointment – SSNs are required of all university employees for matters such as, but not limited to, tax withholding, FICA, Medicare, or travel reimbursement. SSNs are also required on a W9 if no EIN number is available from a consultant or vendor.
- Federal Financial Aid – SSNs are required for all students applying for student financial aid through the use of the Federal Free Application for Student Assistance (FAFSA). Students must also provide their SSNs when applying for student educational loans.
- Tuition Remission – SSNs are required for state reporting of taxable tuition remission benefits received by employees and graduate assistants.
- Benefits Management – SSNs may be required for verifying enrollment, processing and reporting of benefit programs, such as veterans' programs, medical benefits, and health insurance claims.
- IRS Requirements and Reporting Purposes – SSNs are required for federally required reporting of all Internal Revenue Service (IRS) programs associated with all taxable and non-taxable scholarships, grants, and tuition payments. SSNs are also used when reporting earnings, payments to vendors, and on other IRS correspondence.
- Information Exchange – SSNs may be used as student identifiers for the exchange of information from student academic records between appropriate institutions and agencies, including other colleges and universities or certification and licensure programs.

- Volunteers – SSNs are required for all volunteers in the system for the creation of an individual identification number in the HR/FIS system for matters such as, but not limited to, workers compensation coverage, public entity pool for liability (PEPL) coverage through the State of South Dakota, and the use of fleet vehicles.

2. Protection of Social Security Numbers

SSNs shall not be routinely used as personal identifiers.

2.1. SSNs shall not be used for regular identification or routine personal authentication purposes. A unique individual identification number is to be assigned permanently to each individual associated with the system in the form of a student ID or employee identification number. This number shall serve as the alternative to the SSN.

2.2. SSNs shall not be displayed or encoded on identification cards.

2.3. SSNs shall not be displayed or used in other mediums as part of other procedures that violate this policy.

2.4. SSNs collected for authorized purposes shall be transmitted, stored and processed in a secure manner using best higher education practices and encrypting when possible.

2.5. Physical and digital transfer of SSNs should utilize a confidential or encrypted process whenever possible. Reports containing SSNs should always be encrypted and destroyed when no longer needed.

2.6. If individuals offer their SSN over the phone, they should be used to populate approved paper forms or captured in provided software systems. Any other written forms of the SSN should be destroyed when the intended use is complete. Never share SSNs with others via text or e-mail.

2.7. Secure means to obtain SSNs will be performed utilizing university provided software systems and tools, face-to-face with an authorized employee, or via postal mail on university letterhead whenever possible.

2.8. Universities may use the last four digits of the SSN as a means of identification or verification of an individual's identity.

3. Access and Control of Social Security Numbers

3.1. Access to SSNs shall be limited to authorized individuals for authorized purposes. The institutions shall not disclose an individual's SSN to anyone outside the System except as allowed by law or upon proper written permission of the individual.

3.2. SSNs may be used in conjunction with student and employee records academic, personnel or other affiliated records within the BOR computer systems and systems managed by the universities in compliance with security standards set by the CIOs, SDBOR and in accordance with state and federal law.

3.3. The offices that have permission to use the SSNs for legal purposes are also responsible for ensuring proper storage and handling of SSNs following policies that are in compliance with security standards set by the CIOs, SDBOR and in accordance with state and federal law.

4. Misuse of Social Security Numbers

4.1. Anyone aware that SSNs are being used in violation of this policy should report it to the System Chief Networking and Security Office, the local CIO, the human resource officer, or head of department that is legally authorized to use SSNs.

4.2. Any employee storing or processing SSN information on an unauthorized system by unauthorized means (unapproved applications, script, file transfer, etc.) may be subject to disciplinary action consistent with CSA guidelines and regulations or BOR Policy 4:4 – Administrators, Professional and Student Employees (Non-faculty Exempt) Code of Conduct/Misconduct Policy; and, BOR Policy 4:14 – Faculty Discipline and Disciplinary Procedures and the COHE agreement.

FORMS/APPENDICES:

None.

SOURCE:

BOR _____ 2017.