BOARD OF REGENTS

BRIEFING PAPER

HANDBOOK REVISION: Data Security Policy

BACKGROUND & POLICY CONTEXT OF ISSUE:

Federal law (Pubic Law 93-579) provides, in part, that "any federal, state, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it." In addition, state law (*Nevada Revised Statutes* 239B.030) prohibits a governmental agency from requiring a person to include any personal information, including social security number, on any document that is recorded, filed, or otherwise submitted to the agency. Finally, NRS 603A.220 requires that an entity collecting data that includes personal information (including social security number) must disclose any breach of security to any resident whose personal information was acquired by an unauthorized person.

SPECIFIC ACTIONS BEING RECOMMENDED OR REQUESTED:

Amend the Board's existing data security policy (Title 4, Chapter 1, Section 22.7) to provide for the necessary compliance with Public Law 93-579 (sub B), NRS 239B.030, and NRS 603A.220. (See attached Policy Proposal.)

IMPETUS (WHY NOW?):

Revisions to NRS 239B.030 enacted during the 2007 Session of the Nevada Legislature took effect on January 1, 2008, therefore these and additional revisions to comply with existing law are brought forward at this time.

BULLET POINTS TO SUPPORT REQUEST/RECOMMENDATION:

- The proposed revisions will align Board policy with existing federal and state law.
- Adopting the revisions as proposed will effectively notify the campuses of the existing federal and state laws that require appropriate compliance.

POTENTIAL ARGUMENTS AGAINST THE REQUEST/RECOMMENDATION:

Unless a specific state or federal statute requires the collection of social security number, campuses may not require that a student's social security number be provided in filling out an on-line or paper application for admission. Campuses may request social security number as a voluntary act only and the institution must disclose how the information will be used. Long-term this may have implications for the tracking of students, which is difficult at best without a social security number. However, given the existing federal and state statutes on the matter of personal information and disclosure, at this time without formally enacted changes in such statutes the institutions must comply with the aforementioned federal and state laws.

ALTERNATIVE(S) TO WHAT IS BEING REQUESTED/RECOMMENDED:

The proposed revisions will align the Board's policy with existing mandates of federal and state law; therefore, no alternatives have been brought forward.

COMPLIANCE WITH BOARD POLICY:

- ❑ Consistent With Current Board Policy: Title #_____ Chapter #_____ Section #_____
- **X** Amends Current Board Policy: *Title 4, Chapter 1, Section 22*
- ❑ Amends Current Procedures & Guidelines Manual: Chapter #_____ Section #_____
- ❑ Other:_____
- ❑ Fiscal Impact: Yes_____ No_____
  Explain:_____

POLICY PROPOSAL
TITLE 4, CHAPTER 1, SECTION 22 (in part)
Data Security

Additions appear in ***boldface italics***; deletions are [~~stricken~~ and bracketed]

7. Data Security Policy: It is the policy of the Board of Regents that sensitive data maintained or transmitted by an NSHE institution must be secure. For the purposes of this section, "sensitive data" means any data associated with an individual, including but not limited to social security number and data that is protected by Board policy, or state or federal law.

   a. Each NSHE institution must develop and maintain policies, standards, and/or procedures that describe and require appropriate steps to protect sensitive data that is maintained on an institution's computing devices or transmitted across a public network such as the Internet. Institutional policies must include the requirements for the eradication of data when computers are sent to surplus or repurposed. Institutions must be aware of all areas that data are stored, both physically and electronically, and must audit these areas annually to ensure that sensitive data are retained or destroyed as appropriate. Each institution must maintain policies and procedures to be followed in the event that sensitive data is released inappropriately***, including but not limited to the appropriate disclosure of the breach of sensitive data pursuant to Nevada Revised Statutes 603A.220***.

   b. Pursuant to the Privacy Act of 1974 (Public Law 93-579), each institution requesting that an individual disclose his or her social security number must inform that individual whether that disclosure is mandatory or voluntary, by what authority the number is solicited, and what uses will be made of it.

   c. Each NSHE institution must adhere to the disclosure requirements established pursuant to Nevada Revised Statutes 239B.030.

NRS 239B.030 Recorded, filed or otherwise submitted documents. [Effective January 1, 2008.]

1. Except as otherwise provided in subsections 2 and 6, a person shall not include and a governmental agency shall not require a person to include any personal information about a person on any document that is recorded, filed or otherwise submitted to the governmental agency on or after January 1, 2007.

2. If personal information about a person is required to be included in a document that is recorded, filed or otherwise submitted to a governmental agency on or after January 1, 2007, pursuant to a specific state or federal law, for the administration of a public program or for an application for a federal or state grant, a governmental agency shall ensure that the personal information is maintained in a confidential manner and may only disclose the personal information as required:

(a) To carry out a specific state or federal law; or

(b) For the administration of a public program or an application for a federal or state grant.

➥ Any action taken by a governmental agency pursuant to this subsection must not be construed as affecting the legality of the document.

3. A governmental agency shall take necessary measures to ensure that notice of the provisions of this section is provided to persons with whom it conducts business. Such notice may include, without limitation, posting notice in a conspicuous place in each of its offices.

4. A governmental agency may require a person who records, files or otherwise submits any document to the governmental agency to provide an affirmation that the document does not contain personal information about any person or, if the document contains any such personal information, identification of the specific law, public program or grant that requires the inclusion of the personal information. A governmental agency may refuse to record, file or otherwise accept a document which does not contain such an affirmation when required or any document which contains personal information about a person that is not required to be included in the document pursuant to a specific state or federal law, for the administration of a public program or for an application for a federal or state grant.

5. On or before January 1, 2017, each governmental agency shall ensure that any personal information contained in a document that has been recorded, filed or otherwise submitted to the governmental agency before January 1, 2007, which the governmental agency continues to hold is:

(a) Maintained in a confidential manner if the personal information is required to be included in the document pursuant to a specific state or federal law, for the administration of a public program or for an application for a federal or state grant; or

(b) Obliterated or otherwise removed from the document, by any method, including, without limitation, through the use of computer software, if the personal information is not required to be included in the document pursuant to a specific state or federal law, for the administration of a public program or for an application for a federal or state grant.

➥ Any action taken by a governmental agency pursuant to this subsection must not be construed as affecting the legality of the document.

6. A person may request that a governmental agency obliterate or otherwise remove from any document submitted by the person to the governmental agency before January 1, 2007, any personal information about the person contained in the document that is not required to be included in the document pursuant to a specific state or federal law, for the administration of a public program or for an application for a federal or state grant or, if the personal information is so required to be included in the document, the person may request that the governmental agency maintain the personal information in a confidential manner. If any documents that have been recorded, filed or otherwise submitted to a governmental agency:

(a) Are maintained in an electronic format that allows the governmental agency to retrieve components of personal information through the use of computer software, a request pursuant to this subsection must identify the components of personal information to be retrieved. The provisions of this paragraph do not require a governmental agency to purchase computer software to perform the service requested pursuant to this subsection.

(b) Are not maintained in an electronic format or not maintained in an electronic format in the manner described in paragraph (a), a request pursuant to this subsection must describe the document with sufficient specificity to enable the governmental agency to identify the document.

➥ The governmental agency shall not charge any fee to perform the service requested pursuant to this subsection.

7. As used in this section:

(a) "Governmental agency" means an officer, board, commission, department, division, bureau, district or any other unit of government of the State or a local government.

(b) "Personal information" has the meaning ascribed to it in NRS 603A.040.

(Added to NRS by 2005, 2507; A 2005, 22nd Special Session, 97; 2007, 1311, effective January 1, 2008)

NRS 603A.030 "Data collector" defined. "Data collector" means any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information.

(Added to NRS by 2005, 2504)

NRS 603A.040 "Personal information" defined. "Personal information" means a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:

1. Social security number.
2. Driver's license number or identification card number.
3. Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.

➥ The term does not include the last four digits of a social security number or publicly available information that is lawfully made available to the general public.

(Added to NRS by 2005, 2504; A 2005, 22nd Special Session, 109; 2007, 1314)

NRS 603A.200 Destruction of certain records.

1. A business that maintains records which contain personal information concerning the customers of the business shall take reasonable measures to ensure the destruction of those records when the business decides that it will no longer maintain the records.
2. As used in this section:

(a) "Business" means a proprietorship, corporation, partnership, association, trust, unincorporated organization or other enterprise doing business in this State.

(b) "Reasonable measures to ensure the destruction" means any method that modifies the records containing the personal information in such a way as to render the personal information contained in the records unreadable or undecipherable, including, without limitation:

(1) Shredding of the record containing the personal information; or

(2) Erasing of the personal information from the records.

(Added to NRS by 2005, 2504)

NRS 603A.210 Security measures.

1. A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.
2. A contract for the disclosure of the personal information of a resident of this State which is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.
3. If a state or federal law requires a data collector to provide greater protection to records that contain personal information of a resident of this State which are maintained by the data collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this section.

(Added to NRS by 2005, 2504)

NRS 603A.220 Disclosure of breach of security of system data; methods of disclosure.

1. Any data collector that owns or licenses computerized data which includes personal information shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection 3, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data.
2. Any data collector that maintains computerized data which includes personal information that the data collector does not own shall notify the owner or licensee of the information of any breach of the security of the system data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
3. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section must be made after the law enforcement agency determines that the notification will not compromise the investigation.

4. For purposes of this section, except as otherwise provided in subsection 5, the notification required by this section may be provided by one of the following methods:

(a) Written notification.

(b) Electronic notification, if the notification provided is consistent with the provisions of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001 et seq.

(c) Substitute notification, if the data collector demonstrates that the cost of providing notification would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000 or the data collector does not have sufficient contact information. Substitute notification must consist of all the following:

(1) Notification by electronic mail when the data collector has electronic mail addresses for the subject persons.

(2) Conspicuous posting of the notification on the Internet website of the data collector, if the data collector maintains an Internet website.

(3) Notification to major statewide media.

5. A data collector which:

(a) Maintains its own notification policies and procedures as part of an information security policy for the treatment of personal information that is otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if the data collector notifies subject persons in accordance with its policies and procedures in the event of a breach of the security of the system data.

(b) Is subject to and complies with the privacy and security provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et seq., shall be deemed to be in compliance with the notification requirements of this section.

6. If a data collector determines that notification is required to be given pursuant to the provisions of this section to more than 1,000 persons at any one time, the data collector shall also notify, without unreasonable delay, any consumer reporting agency, as that term is defined in 15 U.S.C. § 1681a(p), that compiles and maintains files on consumers on a nationwide basis, of the time the notification is distributed and the content of the notification.

(Added to NRS by 2005, 2504)