BOARD OF REGENTS
BRIEFING PAPER
HANDBOOK REVISION: Data Security Policy

BACKGROUND & POLICY CONTEXT OF ISSUE:

Colleges and universities process large amounts of personal information from students, employees, and the general public gained through admissions records, research efforts, etc. The storing and maintaining of sensitive data makes colleges and universities prime targets for identity theft. With continually emerging technology institutions of higher education must have sufficient security procedures. The theft of personal data has become of issue across the country. The matter of appropriate data security is particularly pertinent to college campuses and college networks that must balance wide network access with data security.

A number of federal policies currently exist that protect different types of data to varying degrees. For example, the Graham-Leach-Bliley Act (GLBA) is intended to protect non-public financial information; and the Health Insurance Portability and Accountability Act (HIPPA) provides standards to protect the privacy and security of health information. Further, the Family Educational Rights and Privacy Act is intended to protect the privacy of student education records.

Currently, the NSHE *Procedures and Guidelines Manual* includes guidelines for the institutions to follow for compliance with GLBA and HIPPA regulations. While there are a number of existing NSHE policies and procedures in place to address the mandates of GLBA, HIPPA, and FERPA, none are specific to the use of institutional computing devices, and none address the need for a contingency plan should secure data be inappropriately or accidentally released.

SPECIFIC ACTIONS BEING RECOMMENDED OR REQUESTED:

Amend Title 4, Chapter 1 by adding a new subsection to Section 22 that provides that 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. This policy will provide for the protection of data that is specifically protected by Board policy, including the personnel and payroll files of the NSHE under Title 2, Section 5.6.2. (See attached policy proposal.)

IMPETUS (WHY NOW?):

Given the recent number of breaches in security data across the nation, sufficient data security policies and procedures are advised.

BULLET POINTS TO SUPPORT REQUEST/RECOMMENDATION:

- NSHE institutions will take the steps necessary to protect personal data stored or maintained on institutional computing devices.
- NSHE institutions will adopt procedures to be followed in the event that protected data is ever inappropriately released or stolen.
- The policy will increase awareness among NSHE institutions of data security issues.

POTENTIAL ARGUMENTS AGAINST THE REQUEST/RECOMMENDATION:

If adopted the policy may require additional resources on the part of the institutions to establish the required procedures and develop appropriate contingency plans for breaches of data security.

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

Do not adopt the policy as proposed, but rely on the currently established procedures that provide for compliance with GLBA, HIPAA, and FERPA.

COMPLIANCE WITH BOARD POLICY:

- ❑ Consistent With Current Board Policy: Title #_____ Chapter #_____ Section #_____
- **X** Amends Current Board Policy: *Title 4, Chapter 1, Section 22.7*
- ❑ Amends Current Procedures & Guidelines Manual: Chapter #_____ Section #_____
- ❑ Other:_____
- ❑ Fiscal Impact: Yes_____ No_____
  Explain:_____

POLICY PROPOSAL
TITLE 4, CHAPTER 1, SECTION 22
Data Security Policy

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

INSERT THE FOLLOWING SUB- SECTION 7 AT TITLE 4, CHAPTER 1, SECTION 22 AS FOLLOWS:

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.***

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.