BOARD OF REGENTS
BRIEFING PAPER
HANDBOOK REVISION: Information 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 information makes colleges and universities prime targets for identity theft and malicious computer-based attacks. With continually emerging technology and growing threats of compromise, institutions of higher education must have adequate security procedures and an individual who has responsibility and authority for the development, maintenance, and compliance of information security policies and procedures. Appropriate information security and assignment of a responsible individual are particularly pertinent to college campuses and college networks that must balance broad access and information requirements with mandated policies and best practices for protecting sensitive information.

Currently, the NSHE *Procedures and Guidelines Manual* includes guidelines for the institutions to follow for compliance with Graham Leach Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA) regulations, but does not address general security practices and controls. State and federal regulatory requirements will continue to add compliance obligations to organizations collecting and storing sensitive information. The growing threats and expanding regulatory requirement place emphasis on the need for consistent information security practices across the NSHE. Therefore, staff recommends the Board's policy on data security be updated to require institutional information security plans. Further, the proposal requires the establishment of an Information Security Officer function at each NSHE institution responsible for the implementation of their respective security plans (*Title 4, Chapter 1, Section 22*). In addition, this proposal includes basic administrative, operational, technical, and physical controls to be in place as part of each institution's required information security plan (*P&G Manual, Chapter 14, Section 1-4*).

SPECIFIC ACTIONS BEING RECOMMENDED OR REQUESTED:

Amend Title 4, Chapter 1 to require the establishment of institutional security plans and the designation by each institution of an information security officer. Further, establish guidelines for certain administrative, operational, technical and physical controls to be included institutional security plans. (See attached policy proposal.)

IMPETUS (WHY NOW?):

Given the recent number of breaches occurring at higher education institutions resulting in loss of personally identifiable and sensitive information, the identification of an individual with responsibility and authority to protect information assets and resources is advised.

BULLET POINTS TO SUPPORT REQUEST/RECOMMENDATION:

- NSHE institutions will take the steps necessary to identify roles and responsibilities to protect personal data stored or maintained on institutional computing devices.
- NSHE institutions will identify an individual responsible for the development, maintenance, and compliance with information security policy, procedures, standards and guidelines.
- The policy will increase awareness among NSHE institutions of information security issues and promote information security collaboration and consistency among all NSHE institutions.

POTENTIAL ARGUMENTS AGAINST THE REQUEST/RECOMMENDATION:

If adopted the policy may require additional resources on the part of the institutions to identify an individual responsible for the development, maintenance, and compliance of information security policy and procedures.

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

Do not adopt the policy as proposed, but rely on the currently established policy that does not identify a responsible individual for development, maintenance and compliance with information security policy, federal and state laws.

COMPLIANCE WITH BOARD POLICY:

❑ Consistent With Current Board Policy: Title #_____ Chapter #_____ Section #_____

X Amends Current Board Policy: *Title 4, Chapter1, Section 22*

X Amends Current Procedures & Guidelines Manual: *new Chapter 14, Sections 1-4*

❑ Other:_____

X Fiscal Impact: Yes__**X**___ No_____

Explain: *If adopted the policy may require additional resources on the part of the institutions to identify an individual responsible for the development, maintenance, and compliance of information security policy and procedures.*

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

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

Section 22. Computing Resources Policy

. . . .

7. [~~Data~~] ***Information*** 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 ***an information security plan that includes*** [~~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. ***The plan must provide for the encryption of personal information when transmitted electronically, or stored on any device that moves beyond the physical control of the institution or its data storage contractor, and for any additional protections required by Chapter 603A of Nevada Revised Statutes.*** 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 periodically to ensure that sensitive data are retained or destroyed as appropriate. [~~Each institution~~] ***The plan*** must [~~maintain~~] ***include*** 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. ***The Vice Chancellor for Information Technology shall establish guidelines for the development of institutional information security plans.***

   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.

   d. Each NSHE institution must designate an individual to perform the function of Information Security Officer who is responsible and has authority to implement compliance with this policy. The responsibilities of the Information Security Officer shall include, implementing the institutional information security plan, developing data risk assessment strategies to identify vulnerabilities and threats to information resources, providing for incident response planning and notification procedures, conducting information security awareness training and education, and ensuring compliance with NSHE and institution policy and federal and state law pertaining to the protection of sensitive information. The Information Security Officer will participate in NSHE-wide information security meetings, programs, and collaborative efforts.

PROPOSED AMENDMENT
Procedures and Guidelines Manual
Chapter 14, Sections 1-4

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

CREATE A NEW CHAPTER 14 – DATA AND INFORMATION SECURITY

Section 1. Information Security Plans - Requirements

1. ***Pursuant to Board policy, each NSHE institution must develop and maintain an information security plan. Each plan must include administrative, operational and technical, and physical controls as outlined in this chapter.***

2. ***Institutional information security plans shall include appropriate risk assessment provisions to identify vulnerabilities and threats to institutional information resources and major enterprise systems, including but not limited to scheduled network and system vulnerability scans. Identified vulnerabilities must be remediated as appropriate to the level of risk.***

3. ***Institutional information security plans shall include an incident response procedure for identifying, containing, and mitigating an incident that includes but is not limited to a breach of security or other threats to institutional systems and information.***

4. ***Institutional information security plans must include guidelines for security awareness training intended to educate students and employees on appropriate security-conscious behavior and also the security best practices they need to incorporate in their daily activities.***

5. ***Any unauthorized or unintentional disclosure or breach of sensitive data must be reported to the Vice Chancellor for Information Technology.***

Section 2. Information Security Plans – Administrative Controls

1. ***Least Privileges. Administrative controls must include the appropriate assignment of responsibility within the institution to determine individual access to system and network resources, including information and data as is appropriate for an individual's job duties and responsibilities.***

2. ***De-Provisioning Privileges. Administrative controls must include procedures for the decommissioning of privileges and accounts upon separation from employment with the institution and upon a change in job duties to ensure system and network resources reflect only privileges necessary for an employee's current job responsibilities. Accounts that have not been used for a defined and documented period of time appropriate to the account type must be identified and de-provisioned.***

Section 3. Information Security Plans – Operational and Technical Controls

1. ***Encryption Technology. Institutions must employ in transit and in storage, encryption technology that is appropriate to protect personally identifiable information and other***

sensitive data. Personally identifiable information stored on removable media, including, but not limited to, laptops, personal digital assistants (PDAs), thumb drives, and CD/DVDs, must be encrypted before the device is taken beyond the physical controls of the campus or control of a data storage contractor.

2. ***Audit Logs. All systems that handle sensitive information or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to identify events that may impact the confidentiality, integrity or availability of sensitive information, including, but not limited to, security and administrative access. The Information Security Officer or his designee must establish retention periods for logs and review audit logs periodically to ensure that appropriate events are consistently logged and abnormal events are identified and investigated.***

3. ***Network Security. Technical controls must include appropriate network security devices configured to detect and prevent network traffic that threatens network and system resources, including sensitive data (e.g. firewalls, intrusion detection systems). Configurations are subject to periodic audits.***

Section 4. Information Security Plans – Physical Controls

Physical controls limiting physical access to facilities housing personally identifiable information must be implemented through the use of appropriate locking or other physical security mechanisms that include methods of identification verification for all equipment that is vulnerable to unauthorized access. Such controls may include combination locks, key locks, badge readers, manual sign in/out logs, and other methods of identification verification.

RENUMBER CHAPTER 14 AS CHAPTER 15