BOARD OF REGENTS
BRIEFING PAPER

1. AGENDA ITEM TITLE: HANDBOOK and *NSHE Procedures and Guidelines Manual* Revision: Computing Resources and Information Security

MEETING DATE November 29-30, 2017

2. BACKGROUND & POLICY CONTEXT OF ISSUE:

Existing Board policy includes provisions governing computing resources (*Title 4, Chapter 1, Section 22*). In response to requests from NSHE institutions, System staff recommends updating this policy and adding authority for the Chancellor to adopt related procedures and guidelines providing more specific direction for implementing the computing resource policy. The current policy does not address NSHE's obligations to comply with the Nevada Public Records Act and state and federal laws governing discovery in litigation, subpoenas, and national security. Because NSHE has such obligations, it is proper to notify users that NSHE will comply with its obligations. Proposed revisions within the *Handbook* and the *Procedures and Guidelines Manual* clarify that electronic records and files may be reviewed in order to comply with these obligations; in such instances, the user will be notified unless NSHE is prohibited by law or subpoena from doing so.

In addition, there are a number of situations involving computer users that are not addressed in the current policy and the absence of direction for those situations can cause difficulties for campuses attempting to conduct business when employees are unexpectedly absent for extended periods. The proposed policy and procedures/guidelines revisions will increase efficiency and effectiveness by enabling campuses to obtain necessary information pursuant to prescribed processes. In the revisions, for circumstances when the user is absent without notice, timelines are provided according to which, when approved by the president or the president's designee(s), an Information Technology (IT) unit/department may establish an automatic reply on the absent user's email directing senders to another employee and may examine email or computer files reasonably necessary to conduct business. Similarly, when a user leaves the employment of NSHE, emails or files remaining on an NSHE-owned computer may be reviewed as reasonably necessary as determined by the president or the president's designee(s). In addition, as reasonably determined by the president or the president's designee(s), IT may be authorized to review emails or computer files, if necessary, for the protection of life, limb, or property or for the maintenance of order.

Proposed changes to the policy also discourage users from storing personal or family financial, medical, business, or other personal records on NSHE computers. Finally, the revisions confirm that any disciplinary action taken for violation of the policy or procedures/guidelines may only be taken pursuant to the Board policy, Nevada law, or an institution student code of conduct.

The proposed changes also update the Board's policy on information security to adopt the nationally recognized standards of the National Institute of Standards and Technology and recognize in policy the NSHE Chief Information Security Officer, who is responsible for the development and management of an information security program for the Chancellor's Office, NSHE Computing Services, and NSHE institutions.

3. SPECIFIC ACTIONS BEING RECOMMENDED OR REQUESTED:

The Board of Regents is requested to approve the attached revisions to the Computing Resources Policy under *Title 4, Chapter 1, Section 23* and a new section under Chapter 4 of the *NSHE Procedures and Guidelines Manual*. In addition, approve a new *Section 24* under *Title 4, Chapter 1* of the *Handbook* establishing the NSHE Information Security Policy that protects sensitive data from unauthorized access, use and disclosure and sets forth standards for the maintenance and handling of sensitive data and other information. Finally, delete Chapter 4, Section 9 (Interim Information Security Plan for NSHE) and Chapter 14 (Data and Information Security) as these older sections of the *NSHE Procedures and Guidelines Manual* are replaced by these updated policies. See the attached policy proposal.

4. IMPETUS (WHY NOW?):

At the request of NSHE institutions, System staff recommends updating the Computing Resources and Information Security policies and adopting related procedures and guidelines.

5. BULLET POINTS TO SUPPORT REQUEST/RECOMMENDATION:

- The proposed revision informs users of NSHE's obligation to comply with the Nevada Public Records Act and state and federal laws governing discovery in litigation, subpoenas, and national security.
- The proposed revision informs users and confirms that any disciplinary action taken for violation of the policy will only be taken pursuant to the NSHE Handbook, Nevada law, or institution student code of conduct.
- The proposed revision encourages users not to store personal or family financial, medical, business, or other personal records on NSHE computers; screen savers are excepted.
- The proposed revision and procedures/guidelines increase efficiency and effectiveness by:
    - Allowing, under certain circumstances when a user is absent without notice, the establishment of an automatic email reply directing senders to another employee.
    - Allowing the review of the content of emails and files left on a NSHE computer by a user who has left the employ of NSHE as reasonably necessary as determined by the president or the president's designee(s).
    - Allowing the review of the content of emails and files on a user's NSHE computer under certain circumstances when the user is absent without notice and the review is necessary to conduct business as determined by the president or the president's designee(s).
    - Allowing the review of the content of emails and files on a user's NSHE computer under certain circumstances, as determined by the president or the president's designee(s), to protect life, limb, or property or for the maintenance of order; the changes also enhance NSHE's efforts to maintain a safe environment.
- The proposed revision informs users that, to comply with federal or state law of an executive order concerning national security, a president or the president's designee(s) may authorize IT to examine certain emails and computer files.
- In those limited instances where a president or the president's designee(s) may authorize a review of emails or computer files, the review is limited to the matter necessary for the purpose of the review.

6. POTENTIAL ARGUMENTS AGAINST THE REQUEST/RECOMMENDATION:

The current policy is adequate.

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

Do not adopt the proposed revisions.

8. COMPLIANCE WITH BOARD POLICY:

❑ Consistent With Current Board Policy: Title #_____ Chapter #_____ Section ____
X Amends Current Board Policy: *Title 4 Chapter 1 Section 23* and *new Section 24*
X Amends Current Procedures & Guidelines Manual: *Chapter 4, Section 9, new Section 9 and Chapter 14.*
❑ Other:_____
❑ Fiscal Impact: Yes_____ No_X___
Explain:_____

POLICY PROPOSAL - *HANDBOOK*
TITLE 4, CHAPTER 1, SECTION 23
Computing Resources Policy

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

Section 23. Computing Resources Policy

1. Principles: Academic freedom in teaching and research and the right of freedom of speech for faculty, staff and students are fundamental principles of the ***Nevada System of Higher Education (***NSHE***)***. Nothing in this section limits or removes the right of free speech or the academic freedom of faculty, staff, and students engaged in the learning process, nor relaxes their responsibilities as members of the NSHE community. This computer resources policy seeks to achieve objectives necessary for the legitimate and proper use of the NSHE computing resources. It is intended that these ends should be achieved in ways that maximally respect the legitimate interests and rights of all computer users. The NSHE acknowledges its responsibilities to respect and advance free academic inquiry, free expression***,*** reasonable expectations of privacy, due process, equal protection of the law, and legitimate claims of ownership of intellectual property. ***The NSHE also acknowledges its obligations to comply with the Nevada Public Records Act and federal and state laws governing discovery in litigation, subpoenas, court orders and national security.*** Each institution within NSHE may adopt further computing resources policies congruent with these principles.

2. ***Applicability and Definitions***

   a. This policy applies to all NSHE institutions, the Chancellor's Office and the Nevada System of Higher Education Computing Services.

   b. For purposes of this section:
      i. "President" means the chief executive officer of a member institution, and the term shall also include the Chancellor where the context of this policy requires with respect to the Unit or the special units.
      ii. "Unit" means the combined administrative unit consisting of the Chancellor's Office and the NSHE Computing Services.
      iii. "User" includes faculty, staff and students.
      iv. "NSHE policies" include the Board of Regents Handbook and the NSHE Procedures and Guidelines Manual.

3. Procedures and Guidelines

In addition to the provisions of this section, the Chancellor is directed to establish procedures and guidelines necessary to implement the Computing Resource Policy, including but not limited to, circumstances in which a user's email may be accessed when the user is absent without notice or leaves the employment of NSHE or in emergency situations.

4. Use of Computing Resources

a. The computing resources of the NSHE are the property of the NSHE and are intended for support of the instructional, research, and administrative activities of System institutions ***and the Chancellor's Office***. Examples of computing resources are system and campus computing facilities and networks, electronic mail, Internet services, lab facilities, office workstations and NSHE data. Users of NSHE computing services, data and facilities are responsible for appropriate and legal use. Appropriate use of system computing resources means 1) respecting the rights of other computer users, 2) protecting the integrity of the physical and software facilities, 3) complying with all pertinent license and contractual agreements, and 4) obeying all NSHE ***policies*** [~~regulations~~] and state and federal laws.

b. Students enrolled in kindergarten through twelfth grades using NSHE computing facilities and networks for K-12 classes and activities must abide by school district and NSHE policies. K-12 students enrolled in NSHE courses will be treated as NSHE students and therefore must abide by NSHE policies.

c. Inappropriate use of computing or networking resources, as defined in this section, may result in the loss of computing privileges. If a violation of appropriate use occurs, a warning [~~will~~] ***may*** first be given, ***if required by federal or state law or NSHE policies,*** notifying the [~~individual~~] ***user*** that their action violates policy or law and that their access will be suspended if the action continues. [~~All NSHE Code~~] ***The applicable NSHE policies, Nevada law*** and campus by-laws shall be followed if the need to suspend computing privileges [~~from~~] ***of*** faculty, staff, or students occurs. However, if the security and operation of the computing systems or networks are jeopardized, access may be immediately cancelled.

d. In congruence with *Nevada Revised Statutes* (NRS) 281A.400, NSHE employees shall not use the NSHE computer resources to benefit their personal or financial interest. However, in accordance with NRS 281A.400(7), limited use for personal purposes is allowable if the use does not interfere with the performance of an employee's duties, the cost and value related to use is nominal, and the use does not create the appearance of impropriety or of NSHE endorsement. ***Users are discouraged from storing personal or family financial, medical, business or other records on NSHE computers.*** Personal use shall not interfere with official institutional ***or Unit*** use. [~~An employee~~] ***Any user*** who intentionally or negligently damages NSHE computing resources shall be held responsible for the resultant expense. [~~These policies also apply to NSHE students.~~]

e. A NSHE account given to students, faculty, and staff is for the use only of the person to whom it is given. Unauthorized access or privileges are not allowed. In electronic communication such as mail, the user should not misrepresent his or her identity. No user ***shall*** [~~should~~] attempt to disrupt services of the computing and network system, including the knowing propagation of computer viruses or the bombardment of individuals, groups, or the system with numerous repeated unwanted messages.

[~~3~~]***5***. Privacy Issues:

The NSHE provides security measures to protect the integrity and privacy of electronic information such as administrative data, individual data, personal files, and electronic mail. All Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232 g; 34 CFR Part 99 requirements are followed. Users must not circumvent security measures. While computing

resources are System property and all rights are retained regarding them, these rights will be balanced with a reasonable and legitimate expectation that technical staff and administrators will not casually or routinely monitor traffic content or search files. ***Except as provided herein, the*** [~~The~~] content of files ***of a current user*** shall only be examined when there is a reasonable suspicion of wrongdoing or computer misconduct as determined by the [~~institution~~] President or his or her designee. Examination of files shall be limited to the matter under consideration. Disciplinary matters involving computer and network systems shall be handled in accordance with [~~Title 2,~~] Chapter 6 or Chapter 10 of the NSHE Code, ***Nevada law, or an institutional student conduct process.*** Within the limits of the capability of the computer system, NSHE shall protect the legitimate privacy interests of users and those about whom information is stored.

[~~4~~]***6***. Software Management Responsibility: Users of NSHE computing resources are responsible for the legality of their software at all times. Data or software written or created by NSHE staff or students must not be copied or used without the author's permission. All commercial software must be licensed. Users must be aware of the license conditions and should never copy software without consulting the license agreement. Evidence of legal ownership is required. Individual ***users*** [~~employees and students~~] are responsible for not installing illegal computer software on NSHE equipment. All NSHE institutions ***and the Unit*** will enforce copyright laws and provide appropriate software management controls.

[~~5~~]***7***. Internet Policy

The NSHE agreement with the provider for Internet access prohibits:

a. attempted unauthorized access or destruction of any customers' information;
b. knowingly engaging in any activities that will cause a denial-of-service to any customers; and
c. using products and services to interfere with the use of the network by other customers or authorized users, or in violation of the law or in aid of any unlawful act.

[~~6~~]***8***. Legal Context: All federal and state laws, ***NSHE policies,*** [~~Code and regulations~~] and individual institutional policies are applicable to computer and network usage. Violation of [~~NSHE Code~~] ***NSHE policies*** [~~provisions~~] may result in disciplinary action. Violation of applicable laws may result in civil damages and criminal sanctions under state and federal law. [~~Applicable statutes are summarized by System Computing Services and NSHE legal staff and can be found on the NSHE homepage on the World Wide Web. This list is by no means exhaustive, but it provides the individual user an overview of the provisions of these and other statutes as they relate to computer use.~~]

[~~7. 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 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 Statues*. 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 where data are stored, both physically and electronically, and must audit these areas annually to ensure that sensitive data are retained or destroyed as appropriate. The plan must 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 Statues* 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 Statues* 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.]

POLICY PROPOSAL
TITLE 4, CHAPTER 1, *new* SECTION 24
NSHE Information Security Policy

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

Section 24. NSHE Information Security Policy

1. ***It is the policy of the Board of Regents that sensitive data maintained or transmitted by a Nevada System of Higher Education (NSHE) institution, the Chancellor's Office or the NSHE Computing Services must be secure. Further, as data collectors, NSHE institutions, the Chancellor's Office and NSHE Computing Services are required to comply with Nevada Revised Statutes (NRS) 603A.010-603A.910 (Security of Personal Information). Accordingly, the Board of Regents hereby establishes this policy in order protect sensitive data from unauthorized access, use, and disclosure, and establishes standards for the maintenance and handling of sensitive data and other information.***

2. ***Definitions***

   For purposes of this section:

   a) ***"Unit" means the combined administrative unit consisting of the Chancellor's Office and the Nevada System of Higher Education Computing Services.***
   b) ***"Sensitive data" refers to personal information as that term is defined in NRS 603A.040, including but not limited to social security number, and any other data identified in state and federal law that the Unit or any NSHE institutions are required protect from unauthorized access, use, or disclosure.***

3. ***NSHE Standards for Security Controls***

   NSHE hereby adopts the National Institute of Standards and Technology (NIST) Cybersecurity Framework, currently in effect and as otherwise amended or updated, as the NSHE standards for security controls.

4. ***NSHE Chief Information Security Officer***

   The Chancellor shall appoint a Chief Information Security Officer ("CISO") for NSHE who shall be responsible for development and management of an information security program for the Unit and NSHE institutions. In addition, the NSHE CISO:

   a) ***Shall establish appropriate management and governance structures related to information security or NSHE;***

   b) ***May establish system-wide committees to assist in the development and management of the NSHE information security program;***

   c) ***Shall work with NSHE Internal Audit on any testing or validation related to the NSHE information security program and Unit and institutional compliance with the program; and***

   d) ***May develop an operations manual or similar document providing technical guidance to the Unit and NSHE institutions for the development of information security plans required by this section that includes, but is not limited to, provisions for compliance with the Graham***

Leach Bliley Financial Services Modernization Act of 1999 (15 U.S.C. § 6801 et seq. and 16 CFR §314.1 et seq.), the Health Insurance Portability and Accountability Act of 1996 (HIPPA), and Payment Card Industry Data Security Standard (PCI-DSS).

5. ***Unit and Institutional Information Security Plans***

   The Unit and each NSHE institution shall:

   a) ***Prepare and maintain a written information security plan that incorporates the NIST Cybersecurity Framework and includes, but is not limited to, the following:***

      i. ***An inventory of the Unit's or institution's current cybersecurity controls aligned with the NIST Cybersecurity Framework (the "Current Profile"); and***
      ii. ***A plan for maintaining alignment with the NIST Cybersecurity Framework that addresses any necessary improvements or emerging threats (the "Target Profile").***

   b) ***Update their Current Profile and Target Profile, every two years or sooner if required by the NSHE CISO.***

6. ***The Unit and each NSHE institution shall comply with any notification requirements applicable in the event of a breach of sensitive data or other information, including, without limitation, NRS 603A.220 (Disclosure of breach of security of system data; methods of disclosure) and any other applicable state or federal laws and regulations. Any Unit or institutional breaches of sensitive data or other information shall be reported to the NSHE CISO within 24 hours of the Unit's or institution's discovery of any such breach.***

7. ***Any use of social security numbers by the Unit or an NSHE institution shall comply with the Privacy Act of 1974 (codified at 5 U.S.C. § 552a). The Unit and each NSHE 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.***

8. ***The Unit and each NSHE institution shall comply with the disclosure requirements set forth in NRS 239B.030 (Disclosure of Personal Information to Governmental Agencies: Recorded, filed or otherwise submitted documents).***

RENUMBER SECTIONS 24 THROUGH 36 AS SECTIONS 25 THROUGH 3

Interim Information Security Plan for NSHE (formerly CM 03-03)

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

[~~Section 9. Interim Information Security Plan for NSHE (formerly CM 03-03)~~

I. **BACKGROUND**. ~~Graham-Leach-Bliley (GLB) Financial Services Modernization Act of 1999 (GLB), 15 U.S. Code §6801, 16 CFR, Part 314, mandates that in addition to complying with the Privacy Rules of Family Education and Privacy Act and Health Insurance Portability Act, financial institutions must take steps to safeguard the security of customers' financial information. The Federal Trade Commission (FTC), which regulates this area, takes the position that these safeguarding rules apply to institutions of higher education. It governs non-public, personally identifiable financial information, such as student loan application information and social security numbers. The FTC has determined that institutions must comply with the Safeguards Rule by May 23, 2003. This Chancellor's Memorandum section is intended to serve as the NSHE's Interim Information Security Plan in compliance with the FTC's Safeguards Rule. The sources for this Information Security Plan were obtained from materials provided by the National Association of College and University Business Officers and the National Association of College and University Attorneys.~~

II. **SCOPE OF THE SECURITY PLAN:** ~~This Plan applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the Institution, whether in paper, electronic or other form, which is handled or maintained by or on behalf of the Institution or its affiliates. For these purposes, the term nonpublic financial information shall mean any information (i) a student or other third party provides in order to obtain a financial service from the Institution, (ii) about a student or other third party resulting from any transaction with the Institution involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person.~~

III. ~~Elements of the Security Plan~~

1. **Risk Identification and Assessment**. ~~This element is intended to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information whether in electronic, paper or other form. The Security Program Officer will coordinate the establishment of procedures for identifying and assessing such risks in each relevant area of the Institution's operations, including: (1) Employee training and management; (2) Information systems and information processing and disposal; and (3) Detecting, preventing and responding to attacks.~~
2. **Designing and Implementing Safeguards**. ~~The program officer will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards.~~
3. **Overseeing Service Providers**. ~~The security program officer shall coordinate with those responsible for the third party service procurement activities among the affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access.~~

4. **Adjustments to Plan**. The program officer is responsible for evaluating and adjusting the plan based on the risk identification and assessment activities undertaken pursuant to the program, as well as any material changes to the institution's operations or other circumstances that may have a material impact on the Plan.

IV. **DESIGNATED PROGRAM OFFICER**. The president of each institution shall designate a security program officer for the coordination and execution of the information security plan. This designation must be made by May 23, 2003. All correspondence and inquiries should be directed to the security program officer.

V. **RELEVANT RISK ASSESSMENT AREAS**. The following have been identified as relevant areas to be considered when assessing the risks to customer information:

- Employee Management and Training
- Information Systems
- Managing System Failures
- Student Loans
- Student Card Office
- Admissions
- Registrar's Office
- Financial Aid Office
- Accounts Receivable Office
- Residence Life
- Student Health Center
- Continuing Education
- Business Centers
- System Computing Services

VI. **SECURITY POLICY COORDINATION**. The security program officer will coordinate with the above offices to maintain the information security program. The security program officer will provide guidance in complying with all privacy regulations. Each relevant area is responsible to secure customer information in accordance with all privacy guidelines. A written security policy that details the information security policies and processes will be maintained by each relevant area and will be made available to the security program officer upon request. In addition, the information technology department and System Computing Services will maintain and provide access to policies and procedures that protect against any anticipated threats to the security or integrity of electronic customer information and that guard against the unauthorized access or use of such information.

VII. **SERVICE PROVIDER' CONTRACTS**. Each of the institutions within NSHE will select appropriate service providers that are given access to customer nonpublic financial information in the normal course of business and will contract with them to provide adequate safeguards. In the process of choosing a service provider that will have access to customer information, the evaluation process shall include the ability of the service provider to safeguard customer information. Contracts with service providers shall include the following provisions:

- An explicit acknowledgment that the contract allows the contract partner access to confidential information;
- A specific definition of the confidential information being provided;
- A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- A guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;

- A guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information;
- A provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract;
- A stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract;
- A stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles NSHE to immediately terminate the contract without penalty;
- A provision allowing auditing of the contract partners' compliance with the contract safeguard requirements; and
- A provision ensuring that the contract's protective requirements shall survive any termination agreement.

These standards shall apply to all existing and future contracts entered into with such third party service providers. While contracts entered into prior to May 23, 2003 may be grandfathered, the Security Program Officer, in cooperation with the Vice Chancellor for Legal Affairs Office, will take steps to ensure that all relevant future contracts include a privacy clause and that all existing contracts are in compliance with GLB.

VIII. **REASSESSMENT OF INFORMATION SECURITY PLAN**. This information security plan shall be evaluated and adjusted in light of relevant circumstances, including changes in the institution's business arrangements or operations, or as a result of testing and monitoring the safeguards. Periodic auditing of each relevant area's compliance shall be done by the security program officer. Annual risk assessment will be done through the security program officer. Evaluation of the risk of new or changed business arrangements will be done through the Vice Chancellor for Legal Affairs Office.

NSHE Procedures and Guidelines Manual
CHAPTER 4, *new* SECTION 9
Computing Resources Procedures and Guidelines

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

Section 9. Computing Resources Procedures and Guidelines

Title 4, Chapter 1 of the Board of Regents' Handbook directs the Chancellor to establish procedures and guidelines governing computing resources, including but not limited to, circumstances in which access to a user's email may be accessed when the user is absent without notice or leaves the employment of NSHE or in emergency situations.

1. ***The definitions set forth in Title 4, Chapter 1, Section 22 apply to this section. In addition:***
    a. ***"IT" means an NSHE institution's Information Technology unit/department and NSHE Computing Services.***
    b. ***For purposes of this section, "department/unit" means a department or unit at an institution and "Unit" as defined under Title 4, Chapter 1, Section 22 includes the combined administrative unit consisting of the Chancellor's Office and the NSHE Computing Services.***
    c. ***"President" means the chief executive officer of a member institution, and the term shall also include the Chancellor where the context of this policy requires with respect to the Unit or the special units.***

2. ***When a user leaves the employ of NSHE, the content of any emails or files remaining on NSHE owned equipment or networks, including but not limited to the user's NSHE computer, may be reviewed as reasonably necessary, as determined by the President or his or her designee(s).***

3. ***In the event a user is absent from work for more than 3 working days without notice, and the supervisor/department chair attempted to contact the user without success, upon the written request of the department/unit, IT may establish an automatic reply on the user's NSHE email account, informing senders that emails should be directed to another employee or office in the department/unit.***

4. ***In the event a user is absent from work for more than 5 working days without notice, the supervisor/department chair attempted to contact the user without success, it is reasonably necessary to access the user's email and/or computer files to conduct the regular business of the department/unit, and the institution or Unit is unable to obtain written or electronic authorization from the user to access the user's email and/or computer files due to the user's health condition, including but not limited to prolonged injury or disability or death, or other circumstances then, upon the written request of the department/unit, the President or his or her designee(s) may, upon a showing of reasonable need and in the absence of reasonable alternatives as determined by the President or his or her designee(s), authorize IT, in writing, to examine the content of the user's emails and/or computer files solely for the purpose of addressing the department/unit's need to conduct regular business. Upon such written authorization, IT shall retrieve the emails and/or computer files reasonably believed to be necessary for the department/unit to conduct its regular business and provide them to the head administrator of the department/unit. Examination of emails and/or files shall be limited to the matter necessary to conduct the regular business of the department/unit.***

5. ***In the event that an institution or the Chancellor's Office receives a public records request, valid subpoena, or a court order, the institution Office of the General Counsel (General Counsel) or the NSHE Vice Chancellor for Legal Affairs (Vice Chancellor) may request that IT preserve a user's email and/or computer files for review by the General Counsel or Vice Chancellor and production of email and/or files as required by law. In the event that the General Counsel or Vice Chancellor determines that production is required by law, the General Counsel or Vice Chancellor shall provide the user an electronic or hard copy of the production, unless prohibited by law from so doing.***

6. ***In the event that during the course of litigation in which NSHE or a NSHE employee or official volunteer is a party, the institution Office of General Counsel (General Counsel) or the NSHE Vice Chancellor for Legal Affairs (Vice Chancellor) determines that it is reasonably necessary, in order to comply with state or federal law or court rule, to preserve a user's email or computer files for the purposes of review and production, the General Counsel or Vice Chancellor may request that IT preserve a user's NSHE email and/or computer files for review by the General Counsel or Vice Chancellor and production of email and/or files as required by law or court rule. In the event that the General Counsel or the Vice Chancellor determines that production is required by law or court rule, the General Counsel or the Vice Chancellor shall provide the user an electronic or hard copy of the production, unless prohibited by law or subpoena from so doing.***

7. ***If in the event of exigent circumstances as reasonably determined by the President or his or her designee(s), it is necessary for the protection of life, limb, or property or for the maintenance of order to examine the content of emails or computer files of a user, the President or his or her designee(s) may authorize IT to examine and retrieve emails and/or computer files solely for the purpose of protecting life, limb, or property or for the maintenance of order, and provide them to the President or his or her designee(s). Examination of emails and/or files shall be limited to the matter necessary for the protection of life, limb, or property or for the maintenance of order.***

8. ***If, in order to comply with federal or state law or an executive order concerning national security, it is necessary to access a user's emails and/or computer files as determined by the President or his or her designee(s), the President or his or her designee(s) may authorize IT to examine and retrieve emails and/or computer files solely to comply with the federal or state law or executive order. Examination of emails and/or files shall be limited to the matter necessary to comply with the federal or state law or executive order.***

[~~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 CHAPTERS 15 THROUGH 19 AS CHAPTERS 14 THROUGH 18