NEVADA SYSTEM OF HIGHER EDUCATION
PROCEDURES AND GUIDELINES MANUAL

CHAPTER 14

DATA AND INFORMATION SECURITY

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.
(B/R 12/09)

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.
(B/R 12/09)

Section 3. Information Security Plans – Operational and Technical Controls

1. <u>Encryption Technology</u>. 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. <u>Audit Logs</u>. 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. <u>Network Security</u>. 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.
(B/R 12/09)

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.
(B/R 12/09)