NSHE Information Security

Operational Procedures and Guidelines Manual

The mission of the Information Security Office is to support the goals of the Nevada System of Higher Education by protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction.

Contents

Purpose

In accordance with Board of Regents policy (Title 4, Chapter 1, Section 24) 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. This section of the Board of Regents Policy establishes standards for the maintenance and handling of sensitive data and other information, including the responsibilities of the NSHE Chief Information Security Officer.

Pursuant to subsection 4(d) of the Board of Regents Policy Section 24, the NSHE Chief Information Security Officer may develop an operations manual or similar document providing technical guidance to the Unit and NSHE institutions for the development of information security plans. This is that document.

For purposes of this document, "sensitive data" refers to Personal Information as that term is defined in NRS 603A.040 and any other data identified in state and federal law that NSHE or any of its Institutions are required to protected from unauthorized access, use, and disclosure.

This document is designed to provide guidance in the development of Institutional and System Administration information security programs. This includes an overview of the requirements to comply with the Board of Regents adoption of the NIST Cybersecurity Framework as a standard for NSHE, suggested baseline standards of common processes and controls, accepted guidelines for NSHE-wide non-academic information systems, and an overview of obligations under multiple regulatory requirements.

1. Cybersecurity Framework

The Board of Regents have adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework as the standard for security controls for NSHE in Board Policy Title 4, Chapter 1, Section 24, Subsection 3.

The purpose of a standard framework is to define a common language for managing security risk and communicating overall cybersecurity posture to external stakeholders such as auditors, insurance underwriters, and regulators. The framework is not designed to be a static "checkbox" but is meant to be an ongoing process of evaluation and improvement.

1.1 Overview

There are five Cybersecurity Framework Core Functions that are built upon one or more process-specific categories to support cybersecurity management. The categories, in turn, are comprised of a number of subcategories that provide process assessments and security control references to determine a current state and target goals. The Core Functions include:

- **Identify:** This function develops the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect:** This function develops and implements the appropriate safeguards to ensure delivery of services and support the ability to limit or contain the impact of a potential cybersecurity event.
- **Detect:** This function develops and implements appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond:** This function develops and implements the appropriate activities to take action regarding a detected event and to contain the potential impact of a cybersecurity event.
- **Recover:** This function develops and implements appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

The categories within each function cover a wide-spectrum of information security activities while providing a technical neutral structure that can be applied equally well among the varied resources and capabilities of each unique NSHE institution. These categories allow institutions to map current technology, processes and policies so there is limited to no effort-loss from previous security implementations.

The categories in each function include:

Identify		
• Asset Management • Risk Assessment	• Business Environment • Risk Management Strategy	• Governance
Protect		
• Access Control • Information Protection Policies and Procedures	• Awareness & Training • Maintenance	• Data Security • Protective Technology

Detect		
• Anomalies & Events	• Continuous Monitoring	• Detection Processes
Respond		
• Response Planning	• Communications	• Analysis
• Mitigation	• Improvement	
Recover		
• Recovery Planning	• Improvements	• Communications

References for controls for each category and sub-category is provided within the framework implementation guide and these controls map to multiple international standards such as ISO27001/2, NIST 800-53, COBIT, ISA 62443, and the Center for Internet Security Critical Security Controls. The inclusion of accepted standards not only aids institutions that have made efforts in following a standard integrate it into an NSHE adopted framework but gives guidance to those institutions who have not applied a standard to their cybersecurity efforts.

The NIST Cybersecurity Framework uses Framework Profiles to aid in implementation. The Profile is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. The Profile enables each institution to establish a roadmap for reducing cybersecurity risk that is well aligned with institutional goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Use of a Current Profile, which describes the current state of cybersecurity activities and a Target Profile, which indicates the outcomes needed to achieve desired cybersecurity risk management goals is recommended. Comparison of profiles will assist institutions in revealing gaps to be addressed and produce an action plan to address the gaps.

Framework Implementation Tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor and sophistication in cybersecurity risk management practices and the extent to which cybersecurity risk management is informed by business needs. While organizations identified as Tier 1 are encouraged to consider moving toward Tier 2 or greater, Tiers do not represent maturity levels. Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective. Successful implementation of the Framework is based upon achievement of the outcomes described in the organization's Target Profile(s) and not upon Tier determination.

The framework offers a structured and common approach to cybersecurity activities allowing for continuous improvement, better communication, ongoing monitoring, and a baseline for internal auditing purposes. Such a risk-based approach enables NSHE institutions to gauge resource estimates to achieve cybersecurity goals in a cost-effective, prioritized manner.

1.2 Current Profile

1.2.1 The Current Profile describes the current state of cybersecurity activities for the Institution aligned with the Functions, Categories, and Subcategories of the Cybersecurity Framework considering legal/regulatory requirements, institutional goals, risk tolerance, and resources.

1.2.2 The NSHE Chief Information Security Officer will make available a Current Profile Template for all NSHE Institutions and System Computing Services as well as provide additional guidance and assistance as needed.

1.2.3 The institution representative to the NSHE Information Security Officers Council is responsible for submitting his/her institutional Current Profile to the NSHE Chief Information Security Officer.

1.2.4 Pursuant to NSHE Policy, the Current Profile will be **submitted every two years, by June 30th in odd numbered years.**

1.2.5 The NSHE Chief Information Security Officer will submit all Current Profiles to NSHE Internal Audit **within 15 days of the published institutional due date**.

1.2.6 The NSHE Chief Information Security Officer will submit to the NSHE Director of Compliance and NSHE Chief Internal Auditor a report identifying the status of NSHE Institution compliance with NSHE policy to submit Current Profiles. This will be done concurrently with the submission of Current Profiles to NSHE Internal Audit.

1.3 Target Profile

1.3.1 The Target Profile indicates the outcomes needed to achieve desired cybersecurity goals and identify activities the Institution will engage in over the following 18-24 months aligned with the Functions, Categories, and Subcategories of the Cybersecurity Framework.

1.3.2 The NSHE Chief Information Security Officer will make available a Target Profile Template for all NSHE Institutions and System Computing Services as well as provide additional guidance and assistance as needed.

1.3.3 The institution representative to the NSHE Information Security Officers Council is responsible for submitting his/her institutional Target Profile to the NSHE Chief Information Security Officer.

1.3.4 Purusant to NSHE Policy, the Target Profile will be **submitted every two years, by October 31st in odd numbered years.**

1.3.5 The NSHE Chief Information Security Officer will submit all Target Profiles to NSHE Internal Audit **within 15 days of the published institutional due date**.

1.3.6 The NSHE Chief Information Security Officer will submit to the NSHE Director of Compliance and NSHE Chief Internal Auditor a report identifying the status of NSHE Institution compliance with NSHE policy to submit Target Profiles. This will be done concurrently with the submission of Target Profiles to NSHE Internal Audit.

2 Baseline Controls

Process and controls that establish a minimum baseline for the protection and security of sensitive data must be established at all NSHE Institutions.

2.1 General Controls

A starting baseline of controls that have been successful at eliminating many vulnerabilities are the first five (5) controls of the Center for Internet Security Critical Security Controls. At least one State has identified the Critical Security Controls as the measure of due care when determining if there was negligence in a breach. Similar to data breach notification laws, we are likely to see this measurement of due care in cybersecurity be adopted throughout the United States over the next several years.

These first five (5) controls map directly with the NIST Cybersecurity Framework, NSHE's adopted cybersecurity guiding framework, as shown in the table below:

Critical Control 1:	Foundational Controls	NIST CSF Mapping
Inventory of Authorized and Unauthorized Devices	**1.1:** Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to public and private networks. Active tools such as NMAP and passive tools that identify hosts based on traffic analysis should be used.	**ID.AM-1** **ID.AM-3**
	1.2: If DHCP is used, deploy DHCP server logging and use this information to improve asset inventory and help detect unknown systems	
	1.3: Ensure that all equipment acquisitions update the inventory system as new, approved devices are connected to the network.	
	1.4: Maintain an asset inventory of all systems and record at least: the network address, machine name(s), purpose of each system, an asset owner, and the department associated with each device. This may include desktops, laptops, servers, network equipment, printers, SAN's, and VOIP telephones.	
	1.5: Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. This should be connected to the inventory data to determine authorized versus unauthorized systems.	
Critical Control 2:	Foundational Controls	NIST CSF Mapping
	2.1: Devise a list of authorized software and version that is required in the enterprise for each type of	**ID.AM-2**

Inventory of Authorized and Unauthorized Software	system, including servers, workstations, and laptops. Monitor the list to validate that authorized software has not been modified.	
	2.2: Deploy application whitelisting that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be extensive to avoid inconveniencing users when using common software, or narrow to accommodate special-purpose systems.	
	2.3: Deploy software inventory tools throughout the organization covering each of the operating system types in use. The tool should identify the underlying operating system as well as the applications installed on it. Tie the software and hardware asset inventory together.	
Critical Control 3:	Foundational Controls	NIST CSF Mapping
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	**3.1:** Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying OS and applications installed. The CIS Benchmarks may help in this regard.	**PR.IP-1**
	3.2: Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization’s change management processes.	
	3.3: Store the master images on a securely configured server, validate with integrity checking tools (e.g. sha1sum), and ensure only authorized changes are made to these images.	
	3.4: Perform all remote administration of servers, workstations, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as TLS or IPSEC.	
	3.5: Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. Routine and expected changes should be accounted for as well as alerting	

	for unexpected or unusual changes. Suspicious changes may include: owner and permission changes to files or directories; the use of alternate data streams; and the introduction of extra files into key system areas.	
	3.6: Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.	
	3.7: Deploy system configuration management tools, such as AD Group Policy Objects for Windows Systems or Puppet for Unix systems that will automatically enforce and redeploy configuration settings to systems at regular schedule intervals.	
Critical Control 4:	Foundational Controls	NIST CSF Mapping
Continuous Vulnerability Assessment and Remediation	**4.1:** Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner.	**ID.RA-1**
	4.2: Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.	
	4.3: Perform vulnerability scanning in authenticated mode either with agents running locally on each end system or with remote scanners that are given rights on the system being tested. Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. Only authorized employees should have	

	access to the vulnerability management user interface.	
	4.4: Ensure that the vulnerability scanning tools you are using regularly update with all relevant important security vulnerabilities.	
	4.5: Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe.	
	4.6: Monitor logs associated with any scanning activity and associated scanning accounts to ensure that this activity is limited to the timeframes of legitimate scans.	
	4.7: Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed, either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such risk acceptance should be reviewed periodically to determine if newer compensating controls or subsequent patches can address vulnerabilities, or if conditions have changed, increasing the risk.	
	4.8: Establish as process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets. A phased rollout can be used to minimize impact on the organization. Establish expected patching timelines based on the risk rating.	
Critical Control 5:	Foundational Controls	NIST CSF Mapping
Controlled Use of Administrative Privileges	**5.1:** Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of the administrative privileged functions and monitor for anomalous behavior.	**DE.CM-4** **DE.DP-1**
	5.2: Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.	
	5.3: Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewall, wireless access points, and other systems to have values consistent with administration-level accounts.	

	5.4: Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrator's group, or when a new local administrator account is added on a system.	
	5.5: Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.	
	5.6: Use multi-factor authentication for all administrative access, including domain administrative access. A variety of techniques can be used including: smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.	
	5.7: Where multi-factor authentication is not supported, users accounts shall be required to use long passwords on the system (longer than 14 characters)	
	5.8: Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/Unix, RunAs on Windows, and other similar facilities for other types of systems.	

3 Password Controls

Applicable NIST CSF Areas: PR.AC-1; PR.AC-7; PR.IP-11; PR.MA-2; DE.AE-2; DE.AE-5; DE.CM-3; DE.CM-6; DE.CM-7

Each Institution and System Administration Unit should establish, through policy, standards for passwords for users, privileged accounts, service accounts, and monitor authentication activity for anomalous events related to user passwords that could indicate compromise.

Institutions and System Administration Units should take into account additional controls, such as multi-factor authentication, in determining a password policy for their environment. Each Institution and System Administration Unit will be required to identify appropriate password controls to external and internal audit and defend their policy standard.

The following provides general password guidelines, elements of the NIST 800-63 Digital Authentication Guidelines, and use of multi-factor authentication in system-wide applications such as Workday.

3.1 General Password Guidelines

The following are general guidelines and suggestions for establishing a password policy if the NIST 800-63 Digital Authentication Guidelines are not able to be followed. Each element should be addressed.

User Accounts:

a) Minimum Password Length: 8 characters
b) Password Expiration: Not to exceed 180 days
c) Password Reuse: Previous 6 passwords
d) Complexity: A combination of 3 of 4 complexity settings (Upper case, lower case, numbers, non-alphabetic characters)
e) Prevent the use of username or partial username in password.

Privileged Accounts:

Accounts that require elevated privileges such as administrator level accounts and service/automation accounts should have a higher standard applied.

a) Minimum Password Length: 18 characters
b) Password Expiration: 180 days OR upon separation of an employee with knowledge of the password.
c) Password Reuse: Previous 6 passwords
d) Complexity: A combination of 3 of 4 complexity settings (Upper case, lower case, number, non-alphabetic characters)
e) Default password created and/or used during installation MUST be change upon completion of any installation/implementation.

3.2 NIST 800-63 Digital Authentication Guidelines

The NIST 800 Digital Authentication Guidelines revisit passwords and changes many of the long held "standards" related to complexity and expiration. The new guidelines favor the user but places additional burdens on the verifier.

The guidelines for passwords are in section 5.1.1 Memorized Secrets in the SP800-63b document that is linked to in the references section of this document.

a) A minimum of 8 characters
b) A maximum of 64 characters
c) Password verifiers shall not permit users to store a "hint" that is accessible to an unauthenticated user.
d) Verifiers shall not prompt users for specific information (e.g. What was the name of your first pet?) when choosing a password.
e) When establishing or changing a password, passwords shall compare the secrets against a list that contains values known to be commonly-used, expected, or compromised.

f) If a password is found in the "known-bad" list, the user must select a different password and given reason for the rejection.
g) Failed login attempts must be rate-limited
h) Complexity rules should NOT be required
i) Arbitrary expiration should NOT be required however password changes shall be forced if there is evidence of a compromise
j) The use of password managers is encouraged to allow for a "paste" functionality.
k) Password must be stored in a form that is resistant to offline attacks, including both salted and hashed using a one-way key derivation function.

3.3 Multi-Factor Authentication

NSHE has mandated the use of multi-factor authentication for access to the Workday environment from external or "untrusted" networks. The standards for the Workday environment are:

a) Registration for multi-factor is required at first login.
b) One or more MFA factors must be enabled in the Okta spoke
    a. SMS
    b. Okta Verify (Android + iPhone app for "push" notifications)
    c. Voice calling
    d. Duo, Yubikey, Google Authenticator or other 3rd party options
    e. Security questions may be enabled for non-administrative roles but is not preferred and may not meet NIST 800-63 Guidelines.
c) MFA re-authentication may be set per device at 7 days (examine NIST 800-63B requirements for MFA)
d) Okta admins may bypass MFA when a user signs in from a "trusted" network. This may be multiple CIDR subnets. This may be on an Institutional LAN, VPN NAT pools, authenticated WiFi networks (not guest WiFi), or particular buildings

It is strongly encouraged that multi-factor authentication be used for administrator access to systems, especially remote access.

3.4 Transmission and Storage of Passwords

a) Passwords should not be inserted into email messages or other forms of unencrypted electronic communications except when passed as a one-time password with no other identifying information.
b) Passwords should not reside unencrypted in any script, code, file, or other process where it can be discovered through visual inspection or intercepted transmission. Appropriate controls should be in place to protect these files.

c) Sharing of assigned, named user accounts and passwords is prohibited. This does not apply to service/system accounts that may be shared with appropriate personnel on a need-to-know basis and when changing those passwords comply with section 2.2.1.

4 Access to Resources

Applicable NIST CSF Areas: PR.AC-3; PR.AC-4; PR.IP-11; PR.PT-3

4.1 Least Privilege

Access to system and network resources must be appropriate for the individual student, faculty, or staff member. The practice of "Least Privilege", the granting of users, programs, or processes the access specifically needed to perform their business task and no more must be applied whenever possible.

4.2 Self-Requesting Access

To reduce the risk of fraud and unauthorized access to resources without collusion, faculty and staff members should not be able to self-request access to resources or elevate their own privileges. Such requests should be submitted by the individual's immediate supervisor or through an appropriate data owner.

4.3 Responsibility to Protect Information

All faculty and staff members should be aware of their responsibility to protect sensitive information wherever it is located.

4.4 Encryption Technology

NRS 603A.215 section 5(b) defines encryption.

a) "Encryption" means the protection of data in electronic or optical form, in storage, or in transit using:

   i. An encryption technology that has been adopted by an established standards body, including, but not limited to, the Federal Information Processing Standards, issued by the National Instituted of Standards and Technology, which renders such data to be indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data;
   ii. Appropriate management and safeguard of cryptographic keys to protect the integrity of the encryption using guidelines promulgated by an established standard setting body including, but not limited to, the National Institute of Standards and Technology; and
   iii. Any other technology or method identified by the Office of Information Security of the Division of Enterprise Information Technology Services of the Department of Administration in regulation adopted pursuant to NRS603A.217.

b) Institutions must employ in transit and in storage, encryption technology that is appropriate to protect personally identifiable information and other sensitive data as per NRS 603A.215 section 5(b). Personally identifiable information stored on removable media, including but not limited to, laptops, flash drives, mobile devices, and CD/DVD’s must be encrypted before the device is taken beyond the physical controls of the institution or control of a data storage contractor (e.g. off-site storage).

c) Sensitive information protected by and defined by federal and state law and/or regulation (e.g. NRS, HIPAA, FERPA) shall not be stored at any time on workstations, laptops, mobile devices, or removable media unless that data is encrypted within NSHE and NRS standards.

5 Security Data Classification

Applicable NIST CSF Areas: ID.AM-3; ID.AM-5; ID.BE-4 ; ID.RA-3; ID.RA-5;

The purpose of this Guideline is to establish a framework for classifying data based on its level of sensitivity, value, and criticality to NSHE and NSHE Institutions. Classification of data will aid NSHE Institutions in determining baseline security controls for the protection of data.

5.1 Definitions

1. **Confidential Data** is a generalized term that typically represents data classified as Restricted, according to the data classification scheme defined in this Guideline. This term is often used interchangeably with sensitive data.
2. **Institutional Data** is defined as all data owned or licensed by the Institution.
3. **Non-public Information** is defined as any information that is classified as Internal or Restricted according to the data classification scheme defined in this Guideline.
4. **Sensitive Data** is a generalized term that typically represents data classified as Restricted according to the classification scheme defined in this Guideline. This term is often used interchangeably with confidential data.
5. **Data Steward** is a senior-level Institution employee who oversees the lifecycle of one or more sets of Institutional Data.

5.2 Data Classification

Data will be classified into one of at least three categories however, Institutions may choose to include additional classification categories to further define Institutional data based on their needs. Additionally, Institutions may rename the categories defined below according to their needs so long as the intent of the classification categories are satisfied.

5.2.1 Restricted

Data that is of a highly sensitive nature and whose inappropriate handling or disclosure could result in detrimental consequences for NSHE and the Institution. Restricted data warrants the most stringent security measures and access controls be applied. Restricted data is typically governed by statutory, regulatory, and/or local, state and federal laws to be strictly and specifically protected.

Examples of restricted data elements include but may not be limited to:

Protected Health Information (HIPAA)

- Names;
- All geographical subdivisions smaller than a State, including street address, city, county precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code;
- All elements of dates (except year) for dates directly related to an individual, including birth datae, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except

that such ages and elements may be aggregated into a single category of age 90 or older;

- Phone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code

Student Education Records (FERPA)

- Social Security Number
- Grades including test scores, assignments, and course grades
- Student financial information, credit cards, bank accounts, wire transfers, payment history, financial aid, grants, and student bills
- Biometric identifiers
- Date of birth
- NSHE defined FERPA Directory Information (when requested to be held private by a FERPA protected individual)

Credit Cardholder Data (PCI-DSS)

- Primary Account Number (PAN)
- Cardholder Name
- Expiration Date
- Service Code
- Full track data (magnetic-stripe data or equivalent on a chip)
- CAV2/CVC2/CVV2/CID
- PINs/PIN blocks

Personally Identifiable Information (Nevada Revised Statute 603A.040)

- 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 elements are not encrypted;
- Social Security number
- Driver’s license number, driver authorization card number or identification card number;

- 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;
- A medical identification number or a health insurance identification number;
- A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account;
- The term does not include the last four digits of a social security number, the last four digits of a driver's license number, the last four digits of a driver authorization card number or the last four digits of an identification card number or publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Authentication Verifier

- An Authentication Verifier is a piece of information that is held in confidence by an individual and used to prove that the person is who they say they are. In some instances, an Authentication Verifier may be shared amongst a small group of individuals (e.g. service account). An Authentication Verifier may also be used to prove the identity of a system or server. Examples include:
  - Passwords
  - Shared secrets
  - Cryptographic private keys

5.2.2 Internal

Data should be classified as Internal when the unauthorized disclosure, alteration, or destruction of that data could result in a moderate level of risk to NSHE, its Institutions, or its affiliates. This data is intended to be protected from external dissemination and public consumption because of business, regulatory, and ethical concerns.

Internal data may be released to individuals outside the NSHE or Institutional community only with approval from the data steward, designated executive sponsor, or when required by law.

By default, all Institutional data not explicitly classified as Restricted or Public data should be treated as Private data. A reasonable level of security controls should be applied to Internal data.

5.2.3 Public

Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to NSHE or the Institution. Examples of public data include press releases, course information and research publications.

While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

5.3 Reclassification

On a periodic basis, it is important to reevaluate the classification of Institutional Data to ensure the assigned classification is still appropriate based on the changes to legal and contractual obligations as well as changes in the use of the data or its value to NSHE or the Institution. This evaluation should be conducted by the appropriate Data Steward.

Conducting an evaluation on an annual basis is encouraged; however, the Data Steward should determine what frequency is most appropriate based on available resources. If a Data Steward should determine the classification of a certain data set has changed, an analysis of security controls should be performed to determine whether existing controls are consistent with the new classification.

5.4 Calculating Classification

Unfortunately, there is no perfect quantitative system for calculating the classification of a particular data element. In some situations, the appropriate classification may be more obvious, such as when federal laws require the Institution to protect certain types of data (e.g. PII, HIPAA). If the appropriate classification is not inherently obvious, consider each security objective using the following table as a guide.

	Potential Impact		
Security Objective	**Low**	**Moderate**	**High**
Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, assets or individuals.
Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational

	operations, assets, or individuals.	operations, assets, or individuals.	operations, assets, or individuals.
Availability: Ensuring timely and reliable access to and use of information	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, assets, or individuals.

As the total potential impact to the Institution increases from Low to High, the classification of data should become more restrictive moving from Public to Restricted.

6 PeopleSoft Administration

6.1 Practices and Procedures

Polices and procedures defined in the NSHE Board of Regents Handbook, Title 4, Chapter 1, Section 24, this Information Security Operational Procedures and Guidelines Manual, and accepted industry practices such as those defined in the NIST Cybersecurity Framework will be followed.

NSHE and institutional resources assigned to iNtegrate/PeopleSoft, including but not limited to, workstations, laptops, Servers, and networks, are to be used by employees only to advance, maintain, and support the purposes of NSHE.

Employees, contractors, consultants, and student employees using personal computing equipment including mobile devices and connecting to any NSHE resource are subject to the same protection requirements defined in Board of Regents Policy and this Information Security Operational Procedures and Guidelines Manual.

6.2 Access to PeopleSoft

6.2.1 Least Privilege

Access to PeopleSoft, its underlying operating system, and any other internal system or network must be appropriate for each employee's job duties and responsibilities. The principle of "Least Privilege", assigning only privileges to a user or role that are necessary to perform the individual's work, will be followed.

6.2.2 Self-Requesting Access

No employee, contractor, consultant, or student employee may self-request access to resources or elevate their own privileges. Such requests must be submitted by the individual's immediate supervisor.

6.3 Automated Account Creation

Institution Solution's Mass Change functionality is used to automate the creation of common user accounts such as applicants, students, and faculty. Default security, such as the mass change templates, model accounts, and custom SQL should be vetted and approved through appropriate data owners, security administrators, and/or project administration teams of the Instance.

Institutional staff is responsible for establishing the pool of new user accounts that need to be created via the Mass Change Process.

6.4 Automated Security Assignment

Dynamic Role rules are used to automate additional self-service role assignments for faculty and students who attend or teach at multiple institutions. Dynamic roles are only assigned to unlocked accounts that have been previously provisioned with at least one role.

Each institution has its own distinct role queries for faculty and staff. Appropriate controls and process must be in place for the writing and maintaining of dynamic role queries.

6.5 Security Change Requests

A request for new security or for a change to existing security must be appropriately vetted and authorized through an Instance specific process that may include: authorized institutional staff such as a module lead, an advisory support group, or a project lead.

Upon approval, the PeopleSoft Security Administrator will build security as requested in a Test environment. Institutions are responsible for testing the new security functionality.

Any security work affecting Self Service functionality requires additional approval through appropriate change control processes.

6.6 Password Restrictions

Password controls must adhere to Section 3 Password Controls.

Use of the delivered e-mail forgotten password feature requires:

i. The user has a valid e-mail address assigned to their account.
ii. The user has set up a security question for their account.
iii. The user's role has a permission list that allows the e-mail forgotten functionality to be used.
iv. Upon receiving a temporary password, the user must be forced to select a new password at first login.

7 Workday Administration

7.1 Practices and Procedures

Polices and procedures defined in the NSHE Board of Regents Handbook, Title 4, Chapter 1, Section 24, this Information Security Operational Procedures and Guidelines Manual, and accepted industry practices such as those defined in the NIST Cybersecurity Framework will be followed.

NSHE and institutional resources assigned to iNtegrate2, including but not limited to, workstations, laptops, Servers, and networks, are to be used by employees only to advance, maintain, and support the purposes of NSHE.

Employees, contractors, consultants, and student employees using personal computing equipment including mobile devices and connecting to any NSHE resource are subject to the same protection requirements defined in Board of Regents Policy and this Information Security Operational Procedures and Guidelines Manual.

7.2 Access to Workday

7.2.1 Least Privilege

Access to Workday and internal systems and network resources must be appropriate for each employee's job duties and responsibilities. The principle of "Least Privilege", assigning only privileges a user or role that are necessary to perform the individual's work, will be followed.

7.2.2 Single Sign-On

Authentication to the production Workday tenant for active employees will be made via NSHE Single Sign-On (SSO) architecture and require multi-factor authentication for active employees accessing Workday when accessing Workday from off-campus and/or untrusted locations.

7.2.3 Self-Requesting Access

No employee, contractor, consultant, or student employee may self-request access to resources or elevate their own privileges. Such requests must be submitted by the individual's immediate supervisor.

7.3 Segregation of Duties

Segregation of duties requires that critical business duties should not be completed by the same person/rule. Appropriate segregation of duties must be designed into the business process and assignment of roles.

7.4 Remote Access

a. Remote access to internal NSHE resources will be made available only when approved by the individual's supervisor and the appropriate request documents are completed.
b. Only approved remote access technologies may be used to access internal NSHE resources.
c. Bypassing authorized remote access technology or security monitoring, or sharing of remote access credentials will be grounds for immediate removal of access.

7.5 Role Definitions

The following are the roles within Workday as they relate to security. Each role or group will have a responsibility for handling different aspects of security for the Workday implementation and beyond.

7.5.1 Security Administrator

The Workday Security Administrator is responsible for the security configuration and setup. With configuration, the Security Administrator is responsible for new roles and security changes to existing roles and security groups.

7.5.2 Security Initiator

The Security Initiator’s primary function is to assign security within Workday. They do not have the ability to change role or security group access but can only assign pre-defined roles and groups to positions.

7.5.3 Security Partner

The Security Partner’s primary function is to validate security changes as directed by Security Initiators. Security Partner’s do have the ability to change security as well (with additional approval), but this is not the primary responsibility of this role. Security Partners have the ability to change role or security group access but can only approve and assign roles to positions.

7.5.4 Security Approver

Security Approver’s primary function is to approve (and thereby enact) security changes within the Workday system. They do not have the ability to change role or security group access but can only approve pre-defined roles and groups to individuals. The role of the Security Approver shall be outside the functional area(s) that are making and validating security requests.

7.6 Security Policy and Group Configuration

7.6.1 Security Groups

A security group is a collection of users or a collection of objects that are related to users. Allowing a security group access to a securable item in a security policy grants access to the users associated with the security groups.

Only the Workday Security Administrator role can edit Security Groups.

7.6.2 Domain Security Policies

A domain security policy is a collection of related securable elements of different types and user-specified security groups that have access to elements of each type.

Only the Workday Security Administrator role can edit Domain Security Policies.

7.6.3 Business Process Security Policies

A business process security policy secures the initiation step, step actions and process wide actions including view, rescind, cancel, and correct for a Business Process. It specifies which security groups have access to each action.

Only the Workday Security Administrator role can edit Business Process Security Policies.

7.6.4 User Based Security

User based security is tied to an individual worker within Workday. These types of roles remain on a worker regardless if they change positions within Workday. These roles are manually assigned and must be manually removed upon determination that a person no longer needs the roles access privileges. These roles are typically administrative roles within Workday for functional area configuration, integration, and report developer type rles, and security administration roles.

The only role that assigns User Based security is the Security Administrator.

7.6.5 Role Based Security

Role Based security within Workday is tied to a specific position and not a person. The campuses will be able to administer their own security assignments for a majority of the Role Based security roles within Workday. The Workday tenants are configured so that Security Partners can add roles to positions within their organizations. The assignable roles available for the Security Partner are listed below by organization. Additionally, there is an additional list of those roles by organization that are not allowed to be assigned by a Security Partner. Those roles must be assigned by the Security Administrator at NSHE.

Supervisory Organization (HCM)

> The security on the Supervisory Organization can be modified by the Security Partner assigned this organization for specific roles defined by the Security Administrator

Company (Financials)

> The security on the Company Organization can be modified by the Security Partner assigned this organization for specific roles defined by the Security Administrator.

Cost Center / Cost Center Hierarchy (Financials)

> The security on the Cost Center Organization can be modified by the Security Partner assigned this organization for specific roles defined by the Security Administrator.

Gift/ Gift Hierarchy (Financials)

> The security on the Gift Hierarchy Organization can be modified by the Security Partner assigned this organization for specific roles defined by the Security Administrator.

Grant / Grant Hierarchy (Financials)

> The security on the Grant Hierarchy Organization can be modified by the Security Partner assigned this organization for specific roles defined by the Security Administrator.

7.7 Tenant Security Configuration

7.7.1 Authentication

When navigating to Workday, users will be required to select one of two options – "Active Employee" or "Former Employee". The mechanism for authentication are different for each and are defined below:

i. **Active Employees**

Active employees in Workday will be required to authenticate through a single sign-on process using Okta. Okta allows one entry point for users to be authenticated using their own institution's authentication source (e.g. Active Directory).

Okta provides an institutional branded page where they will be asked to enter their credentials.

All active employees will be required to use multi-factor authentication when accessing Workday off-site. Multi-factor Authentication is described in 7.7.2.

ii. **Former Employees**

Upon separating from NSHE, an employee will receive their Workday User ID and a temporary password to access the system. They will be required to login to Workday with this ID and temporary password to setup a new password.

Password requirements for Workday native authentication will apply and includes:

- Password length of 8 characters
- Password must be changed every 90 days
- 6 previous passwords may not be used
- Password must contain three of the following: Upper case, Lower case, Number, Special Character.
- Accounts will be locked after five (5) unsuccessful attempts.
- Locked out accounts may reset automatically after a pre-determined period of time.

7.7.2 Multi-factor Authentication

Okta Administrators for each Institution have required and optional settings to set for mutli-factor authentication.

i. **Required**

- Enable one or more multi-factor authentication factors in the Institutional Okta spoke.
- Make the enabled factors "optional" or "required". Optional allows Okta Administrators to require multi-factor authentication only for particular applications. Required makes multi-factor authentication mandatory rather than per application.

- Require users to be prompted for multi-factor authentication when accessing the “NSHE Hub” SAML Application. Since employee access to Workday is routed through the NSHE Hub this causes multi-factor authentication to be required when accessing Workday.
- User enrollment of multi-factor authentication option should be set to “upon a user’s first sign-in”.
- Multi-factor authentication is required one per device over a certain time period not to exceed 30 days.

ii. **Optional**

Okta administraotrs may decide:

- Which multi-factor authentication factors a user may enroll/uses. SMS (text messaging), Okta Verify (Android/iPhone app with optional “push notification”), and Voice Calling are all recommended as sensible defaults. Duo, Yubikey, Google Authenticator, and other options are also available. Security Questions may be enabled for non-administrative roles though other factors are preferred.
- Whether to bypass multi-factor authentication when a user signs in from a trusted network. The Administrator may configure multiple CIDR subnets and IP’s to be considered “On Network” for their Okta Spoke (e.g. the Institution LAN, VPN NAT pools, authenticated WiFi networks, etc.) Guest networks should not be considered as trusted.

iii. **Audit of Multi-Factor Authentication**

NSHE Internal Audit and/or NSHE Information Security Office may audit for compliance with the multi-factor authentication requirements. As NSHE will not have direct access to the Institutional Okta Spoke, compliance may be demonstrated by providing configuration screen shots like any other IT system audit.

7.7.3 Proxy

Proxy access is turned on in non-production Workday environments for certain users allowing for testing end-to-end business processes. Proxy will not be permitted in the production environment.

7.7.4 Export Data

Exporting reports that may contain PII will be limited to internal, trusted networks only to prevent data from being downloaded to non-secured, and unknown locations. Allowing this type of access may result unauthorized access that may result in complying with data breach notification requirements per NRS.

8 Regulatory Standards

Applicable NIST CSF Areas: ID.GV-3

8.1 Health Insurance Portability and Accountability Act (HIPAA)

This section outlines the basics of HIPAA requirements and provides information that may be useful to departments who are not regularly handling health care records. For more detailed information, you may contact the NSHE Director of Compliance, or the designated HIPAA Privacy Officers for your campus.

As this is an overview of the Security and Privacy Rules and a summary of key elements, it does not contain every detail of each provision. Entities and programs that are designated as Covered Entities are responsible for understanding and implementing all elements of the provision.

8.1.1 Covered Entities

The institutions within NSHE are not primary health care providers. NSHE is designated a Hybrid Covered Entity which means that we are allowed to designate which parts of NSHE are covered. The entities and programs that are covered are free to share health care information with each other for legitimate purposes. Theose entities or programs that are not covered may not receive or obtain access to Protected Health Information (PHI) unless authorized by the patient. As an example, most of the UNR School of Medicine is covered; its Human Resources Department is not. It would not be appropriate for the School of Medicine to share a clinical record of an employee/patient with Human Resources unless the patient authorizes the disclosure. The list of covered programs and departments may be changed from time to time. Contact the NSHE Director of Compliance for the most current list.

8.1.2 Elements of Protected Health Information

HIPAA protects certain information that may identify a patient. The data elements listed below are considered Restricted data per section 4 – Data Classification Standard.

- Names;
- All geographical subdivisions smaller than a State, including street address, city, county precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code;
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Phone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;

- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code.

8.1.3 Basic Security Rule Provisions

The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical and physical safeguards to protect e-PHI. Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

Administrative Safeguards

- Security Management Processes. A covered entity must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.
- Security Personnel. A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.
- Information Access Management. Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary", the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role.
- Workforce Training and Management. A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI. A covered entity must train all workforce members regarding its security policies and procedures and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.
- Evaluation. A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

Physical Safeguards

- Facility Access and Control. A covered entity must limit physical access to its facilities while ensureing that authorized access is allowed.
- Workstation and Device Security. A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of e-PHI.

Technical Safeguards

- Access Control. A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic e-PHI.
- Audit Controls. A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.
- Integrity Controls. A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed.
- Transmission Security. A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

8.1.3 Basic Privacy Rule Provisions

A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected health information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who Is the subject of the information (or the individual's representative) authorizes in writing.

The Privacy Rule requires:

- Provision of information to patients about their privacy rights and how their information can be used;
- Adoption of clear privacy procdures;
- Training of employees so they understand the privacy procedures;
- Designating an individual to be responsible for ensuring that the privacy procedures are adopted and followed;
- Securing patient records so they are not readily available to those who do not need them.

Privacy Rule Limitations on Use

In general, treating professional are allowed to freely exchange patient information as necessary for treatment without the necessity of obtaining patient authorization. In addition, a health care provider may use and submit information to obtain payment (but not for insurance underwriting), and for internal operations purposes (such as a peer review committee), without patient authorization. If outside non-treating vendors will require access to patient health information in order to preform a service for a covere program (e.g. computer technician, copy service, record storage company, etc.), patient authorization is required unless a business associate agreement is in place. Apart from certain disclosures that may be required in response to subpoenas and other law enforcement measures, any other disclosure outside the covered department requires written patient approval.

Privacy Rule Patient Rights

Patients are required to be informed of their rights under HIPAA, which include rights related to access to records, correction of records, and accounting for disclosures. There must be a mechanism in place to receive complaints. Civil and criminal penalties are in place for violations of the law. For example, improperly providing patient data for material gain could result in a criminal violation.

8.2 Graham-Leach-Bliley for Education (GLB)

8.2.1 Background

NSHE Institutions are required by the Gramm-Leach-Bliley Act (GLBA) and its implementing regulations at 16 CFR Part 314, to implement and maintain a comprehensive written Information Security Program and to appoint a coordinator for the program. The objectives of the Information Security Program are to (1) ensure the security and confidentiality of covered information; (2) protecting against anticipated threats or hazards to the security and integrity of such information; and (3) protect against unauthorized access or use of such information that could result in substantial harm or inconvenience to customers.

8.2.2 Covered Information

"Covered information" means nonpublic personal information about a student or other third party who has a continuing relationship with NSHE Institutions or System Administration, where such information is obtained in connection with the provision of a financial service or product by NSHE Institutions or System Administration and that is maintained by NSHE Institution or System Administration or on their behalf. Non public personal information includes students' names, addresses and social security numbers as well as students' and parents' financial information. Covered information does not include records obtained in connection with single or isolated financial transactions such as ATM transactions or credit card purchases.

8.3.3 Elements of the Information Security Program Required for GLB

1. **Risk Identification and Assessment**. The written Information Security Program must provide for the identification and assessment of external and internal risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. The Coordinator of the Information Security Program will work with appropriate personnel to establish procedures for identifying and assessing risks in the following areas:

    a. *Employee Training and Management*. The Information Security Program Coordinator will coordinate with appropriate personnel to evaluate the effectiveness of current employee training and management procedures relating to the access and the use of covered information.

    b. *Information Systems*. The Information Security Program Coordinator will coordinate with the appropriate personnel to assess the risks to covered information associated with the Institution's or System Administration's information systems, including network and software design as well as information processing, storage, transmission and disposal.

c. *Detecting, Preventing and Responding to Attacks and System Failures.* The Information Security Program Coordinator will coordinate with the appropriate personnel to evaluate procedures for and methods of detecting, preventing and responding to attacks, intrusions or other system failures.

2. **Designing and Implementing Safeguards**. The Information Security Program Coordinator will coordinate with appropriate personnel to design and implement safeguards, as needed, to control the risks identified in assessments and will develop a plan to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

3. **Overseeing Service Providers**. The Information Security Program Coordinator shall coordinate with those responsible for 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 Program**. The Information Security Program Coordinator will evaluate and adjust the Information Security Program as needed, based on the risk identification and assessment activities undertaken pursuant to the Information Security Program, as well as any material changes to the NSHE or Institution operations or other circumstances that may have a material impact on the Information Security Program.

8.3.4 Service Provider Contracts

Each of the Institutions within NSHE will select appropriate service providers that are given access covered 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 covered information, the evaluation process shall include the ability of the service provider to safeguard covered 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 contract safeguard requireme6tns; and
- A provision ensuring that the contract's protective requirements shall survive any termination agreement.

The Information Security Program Coordinator, in cooperation with Institution and System Legal Counsel, will take steps to ensure that all relevant future contracts include a privacy clause and that all existing contracts are in compliance with the Gramm-Leach-Bliley Act.

8.3 Payment Card Industry Data Security Standard (PCI-DSS)

All Institutions and System Administration Units that accept credit or debit cards must protect credit card data in compliance with the currently enforced version of the Payment Card Industry – Data Security Standard. Each institution is responsible for meeting the reporting requirements as defined by the acquiring bank and the NSHE Banking and Investment Department by deadlines identified.

8.3.1 Components of PCI-DSS

If a merchant at an Institution or System Administration Unit has IP-based devices that are engaged in credit card transactions, whether through processing, transmitting, or storing credit card data, the following PCI requirements must be addressed. Each requirement listed in the table below may have multiple sub-categories within the PCI-DSS itself, so it is incumbent upon the Institution to assure compliance with all required elements.

Goals	**PCI DSS Requirements**
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know. 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

8.3.2 Quarterly Scanning

Institutions that maintain IP-based devices that are engaged in credit card transactions are required to have scans conducted quarterly by an Approved Scanning Vendor. Institutions that are in-scope for this scan must upload the quarterly scan using the approved NSHE portal provided by the merchant services provider. A copy of the scan, in PDF format, must be submitted to the Banking & Investment Department at the time of upload.

8.3.3 Self-Assessment Questionnaire (SAQ)

The SAQ is a validation tool for merchants and service providers to report the results of their PCI-DSS self-assessment, if they are not required to submit a Report on Compliance (ROC). The SAQ includes a series of yes-or-no questions for each applicable PCI DSS requirement. If an answer is no, the Institution or merchant may be required to state the future remediation date and associated actions.

There are different SAQs available to meet different merchant environments. If you are not sure which SAQ would apply, you may seek additional advice from the System Office or the acquiring bank.

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Not applicable to face-to-face channels*.
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Applicable only to e-commerce channels*.
B	Merchants using only: • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. Not applicable to e-commerce channels.
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. *Not applicable to e-commerce channels.*
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. *Not applicable to e-commerce channels.*
P2P3	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solutions, with no electronic cardholder data storage. *Not applicable to e-commer channels.*
D	SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types. SAW D for Service Providers: Al service providers defined by a payment card brand as eligible to complete a SAQ.

8.3.4 Attestation of Compliance (AOC)

After completing the appropriate Self-Assessment Questionnaire, an authorized institution business officer must sign an Attestation of Compliance and submit both the SAQ and AOC to the Banking and Investment Department no later than **January 25th** of each year. The NSHE Banking and Investment Department may have each Institution submit these required documents through the NSHE portal provided by the merchant service provider.

8.4 Federal Red Flags Rule – Identity Theft Prevention Program

8.4.1 Policy and Purpose

This policy is intended to meet the requirements of the FTC "Red Flag Rule." The Nevada System of Higher Education and its institutions have adopted this policy, except where separately approved institution specific policies have been approved. This policy, and any other approved institution specific policies, shall be included in the NSHE Procedures and Guidelines Manual. Oversight of this policy is through the chancellor's Office and institution presidents.

After the initial approval of policies by the Board of Regents in June 2009, amendments may be approved by the chancellor. Institutions may also develop additional procedures with the approval of the institution president.

Identity theft is a fraud committed or attempted using the identifying information of another person without authority. It is the policy of NSHE to undertake reasonable measures to detect, prevent, and mitigate identity theft in connection with the opening of a "covered account" or any existing "covered account," and to establish a system for reporting a security incident.

8.4.2 Background

In 2003, the U.S. Congress enacted the Fair and Accurate Credit Transaction Act of 2003 (FACT Act) which required the Federal Trade Commission (FTC) to issue regulations requiring "creditors" to adopt policies and procedures to prevent identify theft. ·

In 2007, the Federal Trade Commission (FTC) issued a regulation known as the Red Flag Rule. The rule requires "financial institutions" and "creditors" holding "covered accounts" to develop and implement a written identity theft prevention program designed to identify, detect and respond to "Red Flags." That regulation became enforceable on August 1, 2009.

8.4.3 Definitions

Covered Account - A covered account is a consumer account designed to permit multiple payments or transactions. These are accounts where payments are deferred and made by a borrower periodically over time such as a tuition or fee installment payment plan.

Creditor - A creditor is a person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal, or continuation of credit Examples of activities that indicate a college or university is a "creditor" are:

- Participation in the Federal Perkins Loan program;
- Participation as a school lender in the Federal Family Education Loan Program;
- Offering institutional loans to students, faculty or staff;
- Offering a plan for payment of tuition or fees throughout the semester, rather than requiring full payment at the beginning of the semester.

Identifying Information - Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer's Internet Protocol address, routing code or financial account number such as credit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Red Flag - A red flag is a pattern, practice or specific activity that indicates the possible existence of identity theft.

Security Incident - A collection of related activities or events which provide evidence that personal information could have been acquired by an unauthorized person.

8.4.4 Identification of Red Flags

Broad categories of "Red Flags" include the following:

- **Alerts** - alerts, notifications, or warnings from a consumer reporting agency including fraud alerts, credit freezes, or official notice of address discrepancies.
- **Suspicious Documents** - such as those appearing to be forged or altered, or where the photo ID does not resemble its owner, or an application which appears to have been cut up, re-assembled and photocopied.
- **Suspicious Personal Identifying Information** - such as discrepancies in address, Social Security Number, or other information on file; an address that is a mail-drop, a prison, or is invalid; a phone number that is likely to be a pager or answering service; personal information of others already on file; and/or failure to provide all required information.
- **Unusual Use or Suspicious Account Activity** -such as material changes in payment patterns, notification that the account holder is not receiving mailed statement, or that the account has unauthorized charges;
- **Notice from Others Indicating Possible Identify Theft** -such as the institution receiving notice from a victim of identity theft, law enforcement, or another account holder reports that a fraudulent account was opened.

8.4.5 Detection of Red Flags

Employees shall undertake reasonable diligence to identify Red Flags in connection with the opening of covered accounts,as well as existing covered accounts through such methods as:

- Obtaining and verifying identity;
- Authenticating customers; and
- Monitoring transactions.

A data security incident that results in unauthorized access to a customer's account record or a notice that a customer has provided information related to a covered account to someone fraudulently claiming to represent the university or to a fraudulent web site may heighten the risk of identity theft and should be considered Red Flags

8.4.6 Response to Red Flags

Unless otherwise directed by the college or university, the detection of a Red Flag by an employee shall be reported to chief security officer for the institution. Based on the type of Red Flag, the appropriate administrator and the chief security officer will determine the appropriate response.

8.4.7 Security Incident Reporting

An employee who believes that a security incident has occurred shall immediately notify their appropriate administrator and, unless otherwise directed by the institution, the chief security officer. After normal business hours, notification shall be made to the institution police or other responsible after-hours administrator. Upon review of the incident, the responsible administrator shall determine what steps may be required to mitigate any issues that arise in the review. In addition, referral to law enforcement may be required.

Requirements for information security breach notification contained in Board of Regents Handbook may also be applicable.

8.4.8 Training and Program Review

All employees who process any information related to a covered account shall receive training following appointment on the procedures outlined in this document. Refresher training may be provided annually.

Periodically the policy, procedure and training shall be reviewed to assess the need for changes or improvements.

9 Usage Guidelines for Cloud Services

This section provides guidance for the provisioning and use of cloud computing services to support the processing, sharing, storage, and management of NSHE and institutional data.

9.1 Overview

Cloud computing services are application and infrastructure resources that users access via the Internet. These services, contractually provided by companies such as Apple, Google, Microsoft, and Amazon, enable customers to leverage powerful computing resources that would otherwise be beyond their means to purchase and support. Cloud services provide services, platforms, and infrastructure to support a wide range of business activities. These services support, among other things, communication; collaboration; project management; scheduling, and data analysis, processing, sharing, and storage.

Most cloud services, such as Google Docs or Office 365, make it easy for individuals to sign-up and use (self-provision) their services via an end user license agreement (EULA, often at no monetary cost. NSHE Units and NSHE institutions also locally or centrally acquire cloud services for use by members of the NSHE or institution community.

NSHE faculty, staff, and students must be very cautious about self-provisioning a cloud service to process, share, store, or otherwise manage NSHE Unit or Institutional data. Self-provisioned cloud services may present significant data management risks or are subject to changes in risk with or without notice. These agreements do not allow users to negotiate terms, do not provide the opportunity to clarify terms, often provide vague descriptions of services and safeguards, and often change without notice.

Risks with using self-provisioned cloud services include:

- Unclear, and potentially poor access control or general security provisions
- Lack of protection or control over the data, leading to a loss of security, lessened security, or inability to comply with various regulations and data protection laws.
- Data stored, processed, or shared on cloud services is often aggregated with data from other cloud consumers or mined for resale to third parties that may compromise people’s privacy
- Sudden loss of service without notification
- Sudden loss of data without notification
- The exclusive intellectual rights to the data stored, processed, or shared on cloud services may become compromised

In contrast, NSHE Units and NSHE Institutions negotiate agreements with service providers for locally as well as centrally provisioned services. The terms of these services are more clearly defined and well known by NSHE Units and NSHE Institutions. In short, NSHE Unit and NSHE Institution provisioned cloud services are vetted environments where risks are better measured and accepted.

9.2 Use of Cloud Services

9.2.1 Self-Provisioned Services

For purposes of this section, Self-Provisioned services refers to consumer-based cloud products that are primarily designed for individual, personal use. Such services should not be used to store, process, share, or manage **Restricted Data** as defined in section 5 of this document. Restricted data is:

> ***"Data that is of a highly sensitive nature and whose inappropriate handling or disclosure could result in detrimental consequences for NSHE and the Institution. Restricted data warrants the most stringent security measures and access controls be applied. Restricted data is typically governed by statutory, regulatory, and/or local, state and federal laws to be strictly and specifically protected. "***

9.2.2 Cloud Computing Usage and Responsibility

Using a third-party cloud service to handle NSHE Unit or NSHE Institutional data does not absolve you from the responsibility of ensuring that the data is properly and securely managed. Members of the NSHE community are expected to responsibly maintain and use NSHE and institutional data regardless of the resource used to access or store the data.

The care taken to review a cloud services' security and trustworthiness must match the sensitivity of the NSHE or Institutional data you are looking to support with the service and the data's governing regulatory environment. In order to use a cloud service to store, process, share, or otherwise manage Restricted Data, you should:

- Work with legal counsel and purchasing services to develop the appropriate contractual safeguards
- Monitor changes to the service's safeguards
- Know the retention period and, when applicable, the destruction date of the NSHE or Institutional data. Retention periods are defined in the NSHE Board of Regents Procedures and Guidelines Manual.
- When appropriate, securely destroy the data

9.2.3 Cloud Computing Contract Considerations

NSHE Units and NSHE Institutions should consider the following in developing contract terms with cloud computing services to ensure the minimum level of information security protection:

- Data transmission and encryption requirements
- Authentication and authorization mechanisms
- Intrusion detection and prevention mechanisms
- Logging and log review requirements
- Vulnerability scanning and audit requirements
- Security training and awareness requirements

9.3 Legal and Regulatory Considerations

NSHE Units and NSHE Institutions have many federal laws that must be followed, including but not limited to the Family Education Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley Act (GLBA).

Nevada Revised Statute (NRS) may also affect a relationship with a cloud-computing vendor. For instance, NRS establishes rules related to disclosure of Social Security Numbers as well as specific data breach notification requirements.

Private industry regulations, such as the Payment Card Industry (PCI) Data Security Standard (DSS) issued by major credit card companies defines protection standards for data elements related to cardholder information.

NSHE Units and NSHE Institutions must ensure that the use of cloud services is consistent and aligned with requirements defined by regulation or applicable industry standards.

9.4 Exit Strategy

NSHE Units and NSHE Institutions should develop an exit strategy for disengaging from the vendor or service and integrating the service into business continuity and disaster recovery plans. NSHE Units and NSHE Institutions must determine how data would be recovered from the vendor if/when a cloud service relationship is terminated.

References

NIST 800-63B Digital Authentication Guidelines	https://pages.nist.gov/800-63-3/sp800-63b.html
NIST Cybersecurity Framework	https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
NSHE NIST Profile Templates	https://security.nevada.edu/resources-information/
US Dep. Of Health & Human Services Health Information Privacy	https://www.hhs.gov/hipaa/index.html
National Conference of State Legislators Security Breach Notification Laws	http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
PCI Security Standards Council	https://www.pcisecuritystandards.org/

Index