NSCS Information Security Standard 4: Information Protection

4.1 Information Classification

To assist with securely managing and controlling information access, NSCS uses a data classification scheme. The following rules form the basis of the data classification system:

- NCSC data is assigned a Data Steward, a classification, and is controlled accordingly.
- Technology Resources will be classified as high risk if they process or store medium or high risk data or if they are assigned to a user with access to medium or high risk data.

The NSCS uses three data classification categories in alignment with the work of the joint University of Nebraska/NSCS Data Governance Committee as recorded in University Policy ITS-05: Data Classification and Storage Policy.

High Risk Data (Confidential and Highly Restricted):

High risk institutional data are highly confidential. Data are considered high risk if:

- The loss of confidentiality, integrity, or availability of the data or system could have a SEVERE adverse impact on the NSCS mission, safety, finances, or reputation.
- Protection of the data are required by law/regulation.
- The data carries a security classification established by an authorized agency of the federal government.
- The System Office and/or College is required to self-report to the government and/or provide notice to the individual if the data are inappropriately accessed.
- Examples of high risk data include:
    - Health Information, including Protected Health Information (PHI)
    - Health Insurance policy ID
    - Social Security Numbers
    - Credit Card Numbers
    - Bank account numbers
    - Passport/Visa numbers
    - Driver's license numbers

Medium Risk Data:

Medium risk institutional data are confidential data requiring high levels of protection due to the following circumstances:

- The loss of confidentiality, integrity, or availability of the data or system could have a SIGNIFICANT negative impact on our mission, finances, or reputation.

- Protection of the data may be required by law/regulation.
- The data may carry a security classification established by an authorized agency of the federal government.
- The System Office and/or College may be required to self-report to the government and/or provide notice to the individual if the data are inappropriately accessed.
- Data received or collected is subject to contractual confidentiality provisions.
- Examples of medium risk data include, but are not limited to:
    - FERPA non-directory information
        - Academic data such as grades still associated with user information
    - NUID/SAP ID numbers
    - Employment applications and files

High Risk and Medium Risk Data are collectively referred to as Sensitive Information throughout this document.

Low Risk Data:

Low risk institutional data are data routinely used in conducting business not covered by international, state, or federal privacy and security laws. Generally, this is information that can be made available to the public without risk of harm to the NSCS or any entities with an affiliation to the NSCS.

4.2 Hard Copy Data Protection

The physical controls requirement for protection of physical or paper copies of data include:

- High Risk data in any format must be transported in a secure manner.
- Limit display of Sensitive Information in open, accessible areas.
- Avoid downloading or printing Sensitive Information and obviate Sensitive Information unless required by law or there is an unavoidable business-related need.
- Limit distribution of documents with Sensitive Information and know who is receiving the documents and how it will be used.
- Always store media containing Sensitive Information in a secure location such as a locked filing cabinet and know who has access to the location. When a Data Owner or Data User is not present the preferred method for protecting Sensitive Information is the two-lock rule. Normally the first is a locked file cabinet and the second a locked door.
    - Do not leave Sensitive Information in unsecured locations, such as a personal vehicle or residence.
    - Shred paper containing Sensitive Information with a cross-cut shredder before discarding or place in the shredder service bins.

- Escorts are required when individuals need access to areas with unsecured Sensitive Information, and precautions such as covering Sensitive Information that cannot be secured should be utilized. Access by custodial or maintenance employees or 3rd party vendors should be considered as non-authorized personnel.

  References: NSCS Policies 3650 and 5018

4.3 Account Authorization and Management

4.3.1 Access Authorization

- The NSCS Information Technology (IT) departments will rely upon the identity stores provided through the TrueYou Identity and Access Management system sponsored under the NeSIS/NeBIS projects for the provisioning of employee and student credentials, including prospective and former students.

- The Colleges will have a procedure to manage and review credentials for other associated individuals not present in TrueYou such as campus guests, third-party contractors, volunteers, emeriti, or potential employees.

- The NSCS and Colleges shall utilize the principles of least privilege for access to Technology Resources.
- Need-to-know is verified prior to giving a user access to information.

4.3.2 Account Creation and Access Modification

The following governance applies to NSCS accounts:

- Credentials are unique to each individual and are not to be reused and issued to another person.

- Accounts may be created and made available to an incoming employee prior to the first day of employment (contract start date as defined in NeBIS) to facilitate voluntary work of an incoming employee to adequately prepare for the first day of employment. Accounts shall be created no more than fifty-six (56) calendar days in advance of the first day of employment.

- When temporary passwords are assigned, the system must force the user to change the password upon the next login.

- A transfer to a different department, assumption of new or different duties, new systems, etc., often require a change in an individual's access to NSCS resources. In these instances, the NSCS requires a) removing access to the specific NSCS services that are no longer part of the job responsibilities and b) requesting access to the resources required of the new position or duties through the formal account management process.

4.3.3 Account Revocation

- Where processes are not in place to formally define the end of employment such as for temporary employees or contractors, Credentials should be set to automatically expire.

- Termination for cause should be coordinated with IT so that account access can be terminated expeditiously.

- Normal terminations should follow a formal process to ensure that all accounts are terminated and that all assigned equipment is returned.

- To the maximum extent possible, systems and applications should authenticate using a Central Identity Provider (CIP) to provide simultaneous revocation of credentials.

- Since CIP deactivation only removes access to systems that are CIP authenticated, additional steps are required to ensure access revocation for systems not CIP authenticated.

Account Disabling - Normal Process

- **Employees** – Access to systems containing High and Medium risk data will be removed upon the last day of employment appointment. Accounts will be disabled no later than ninety (90) calendar days after the expiration of the most recent existing employee appointment or the Keep Services Active date in NeBIS, whichever is later. Access to e-mail may be extended for a period of time via an exception request submitted by the employee's supervisor.
- **Students** - Student Credentials are provisioned and de-provisioned in accordance with roles determined by the TrueYou Identity and Access Management system.
- **Former Students** - email may be provided for life. However, should a credential go dormant for a maximum of two years, it is disabled.
- **Other accounts** - Will be disabled in compliance with the campus procedure for the maintenance of other accounts (ref. 4.3.1).

Account Disabling - Expedited Process

Upon request by the Human Resources office, the President, or General Counsel, accounts may be disabled immediately. Access to appropriate services can be extended based upon demonstrated business need and approval by the Human Resources office, the President, or General Counsel in consultation with the CISO. The account should be set to expire at the end of the approved extension period.

4.3.4 User Identification

User Passwords

- Users are to protect passwords as specified in Information Security Standard 5: *Acceptable Use and User Privacy*.
- The following comprises the minimum strength rules for NSCS user passwords:
    - Password is case sensitive.
    - Must be at least 8 characters long. Must not repeat any character sequentially more than 3 times.
    - Must not include part of your name or user name.
    - Must not be limited to a dictionary word.
- The NSCS may implement other password procedures to ensure compliance with NIST and auditor recommendations.

4.3.5 Multifactor Authentication

Multi-factor authentication (MFA) is an authentication method in which a Credential is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence. Two-factor authentication is a type, or subset, of multi-factor authentication.

When available, multi-factor authentication should be applied in the following use cases:

- VPN access to NSCS networks.
- Administrative (Privileged) Credential access.
- Access to systems which contain High Risk data.

4.3.6 Admin (Privileged) Credentials

Privileged Credentials are those with rights to perform system and/or application administration. The following requirements govern the creation, use, monitoring, and decommissioning of privileged user Credentials within NSCS.

- Elevated permissions may not be permanently assigned to a user's primary account.
    - A separate Credential must be created for each individual user who has a documented business need for elevated privileges. These accounts should be created with a standard naming convention which will serve to distinguish the Credential from a normal user Credential while at the same time clearly identifying the individual to which the Credential has been assigned.
    - Administrative permissions can be granted to a user's primary Credential for a limited period of time for the purposes of managing the user's computing device.
- Authorization for the creation of a privileged Credential must be approved by the CIO/CISO.

Each request for privileged access must include appropriate justification for the request.

- Admin Credentials are to be used only for conducting Admin functions.
- Admin Credentials are to be reviewed annually to ensure only needed Admin Credentials remain active.
- Admin Credentials should be created with the minimum privilege levels necessary to accomplish the user's required functions.
- Passwords for Admin Credentials:
    - Must meet all the minimum requirements for user Credentials.
    - Be a minimum of 12 characters
    - Must not have the same password as the Admin's normal user Credential.
- Shared credentials must only be used when using individual credentials are not feasible and shared credentials are necessary.
- Remote access to Admin Credentials must utilize MFA.
- Where possible, local Admin Credentials should require MFA.

4.3.7 Service Accounts

The following controls for Service Accounts should be implemented to the extent possible.

- Inventory all accounts
- Use Public Key Infrastructure (PKI) authentication where possible rather than password based Credentials.
- Use randomly generated passwords that meet all the requirements for Level 3 passwords with the added requirement of 16 characters
- Change passwords when the incident response plan has been activated for impacted systems.
- Provide the minimum necessary privileges to the service account. If the service account must run with admin privileges, deny access to all directories except those needed.
- Use event logging to monitor for specific events such as the account being used for other than the assigned specific service.
- Passwords should not be embedded in a script.
- Password changes must be communicated out–of-band to the service account connection.

4.3.8 Application Integration

When new or updated integrations with NeSIS/NeBIS are to occur, the NeSIS/NeBIS change request control processes must be followed. This includes the use of any NeSIS/NeBIS data to an integrated system, even if extracted through a query/reporting tool.

The CISO of each College is the approver of all application and system integrations for that College.

The owners of applications that integrate with NSCS systems are responsible for the following:

- Providing a business justification when requesting an integration, which shall include: a brief explanation of the function that will be supported by the integration; a list of any data elements that will be transferred via the integration; the classification level of each data element; and an explanation of how data received via the integration will be used and who will have access to the data because of the integration.
- Ensuring appropriate and secure transmission of data per NSCS encryption requirements.
- Informing the owner of the connected system if the access granted is either more restrictive or more permissive than needed.
- Ensuring data made available via the integration are not redistributed or made available beyond what was documented in the business justification.
- Maintaining the security of any credentials issued to facilitate the integration. This includes requesting credentials be changed or revoked if their confidentiality has been compromised either through normal activity (such as employee termination), malicious activity, or when the credential is no longer needed.

The owners of NSCS systems who provide access (integration) to remote applications are responsible for the following:

- Reviewing business justifications for integration requests and for obtaining approval from the responsible Data Stewards for the data being requested prior to making them available via the integration.
- Ensuring appropriate and secure transmission of data per the NSCS encryption requirements.
- Maintaining an internal, up-to-date list of all active integrations that includes: contact information for the owners of each application integrated with the enterprise system; a copy of the business justification provided by the application owner; a record of any approvals obtained from NSCS units permitting access or transmission of data via the integration; a list of any credentials associated with the integration, the individuals issued credentials, and the expiration date of the credentials.
- Communicating any changes to the enterprise system that will impact an integration to the owner of the affected application(s).
- Providing security guidance to all individuals granted credentials used for integration.
- Granting the appropriate level of access to the application following the principal of least privilege.
- Communicating the expiration of any credentials to the individuals they were issued to in a timely manner.
- Coordinating the rotation or revocation of credentials used for an integration with the application owner.

4.4 Confidentiality and Privacy

4.4.1 Securing Data - Data Encryption

When properly implemented, encryption provides an enhanced level of assurance that the data cannot be viewed or otherwise discovered by unauthorized parties in the event of theft, loss or interception. Data must be stored in compliance with the Data Classification and Use Matrix, with particular care given to the storage of High Risk data. The following are standard practices for NSCS device and media requiring encryption:

Devices and Media Requiring Encryption

STORAGE MEDIA	CHARACTERISTIC(s)	High	Medium	Low
Servers	Enterprise (many users). Includes database and application and web servers; file and print servers.	Highly Recommended	Recommended	None
Workstations	Varies (single to many users). Examples: Offices (private or shared); open work areas; public service areas; computer labs.	Required	Recommended	None
Laptops, Mobile Devices	Single user. Office, shared area	Required	Recommended	None
NSCS owned Smartphones, Cell Phones	Single user.	Required	Recommended	None
Employee personal Smartphones, Cell Phones	Single user.	See BYOD policy	See BYOD policy	See BYOD policy
Storage Media external to a computing device	Varies (single to many users).	Required	Recommended	Optional

Alternative methods for protection may be used when there are documented processes and procedures in place and the methods are approved by the CISO.

4.4.2 Transmission Security

The NSCS requires that High Risk data be encrypted during transmission. The following outline specific requirements for data encryption.

- **Unencrypted Transmission Media** – The following technologies do NOT utilize encryption and are not to be used for transmission of Sensitive Information:
    - Standard email without encryption procedures
    - Web browsing via http (as opposed to https) URLs
    - Telnet
    - FTP

- **Electronic Data Transfers** - Transfer of unencrypted sensitive information must take place via an encrypted channel when transmitted externally. Internally, Sensitive Information may be transmitted via encrypted or unencrypted channels. Colleges will use modern encryption protocols without known vulnerabilities, such as:
    - Transport Layer Security (TLS)
    - File Transport Protocol Secure (FTPS)
    - SSH File Transport Protocol (SFTP)
    - Secure Copy Protocol (SCP)
    - Connecting via an NSCS-approved Virtual Private Network (VPN)
- **Authentication** – All authentication is to be encrypted or done over encrypted connections.
- **External Access** – All unsecured connections to NSCS computing resources are to be encrypted through College approved VPN client software.
- **IT Administration** – All IT administration should be performed using an encrypted connection technology such as SSH tunneling. Where encryption of management access is not possible, access to management interfaces must be protected to the maximum extent possible.

4.5 Data Integrity

- Single point of entry – Where possible, data should be entered into the system of record (for example NeSIS for student records and NeBIS for HR/finance) directly and provided to other systems via integration rather than double entry so as to limit human error.
- Data validation techniques – Where possible, software applications should validate data for appropriate format and content upon data entry.

4.6 Data Ownership and Records Retention

Unless specified elsewhere in NSCS Policy or negotiated agreement, all data stored in NSCS information systems are property of the NSCS.

NSCS Records will be retained according to NSCS Records Retention Schedules developed by the System Office in collaboration with the Colleges.

At the direction of the NSCS General Counsel, accounts or account associated data held in NSCS information systems may be retained longer than the NSCS Retention Schedules indicate.

4.7 Data Backup and Recovery

Backups at the NSCS are used for the following purposes:

- Resiliency - Creating a durable infrastructure so that end-users rarely or never experience a disruption.
- Recovery - If a data-loss crisis occurs, a secondary copy is available to roll back a server or array to a previous point in time representing a known good state.
- Restoration - Similar to recovery, restoration converts selected data back to a previous point in time.

Data Backup Frequencies

- The Colleges will have procedures to determine backup frequencies necessary to accomplish the purposes set forth in this Standard.

4.8 Media Control, Destruction and Reuse

All media internal to IT equipment will be removed or sanitized as part of the equipment disposal process.

The following options are approved for sanitizing or destroying media. Other methods may be employed and approved by the CIO/CISO as needed to ensure data destruction.

- **Software Wipe** - Perform a software wipe using a DoD 5220.22-M compliant data wipe tool. These tools work by overwriting existing information on the hard drive or other storage device.
- **Physical Destruction** - Physical destruction can be used to destroy media unusable and non-recoverable. This include crushing in a press, shredding, or incineration. The physical destruction method should physically destroy the media holding the data and not simply the surrounding case.
- **Third-Party Vendor** - vendors used for media destruction should be certified by the National Association of Information Destruction (NAID). The procedures used to perform the media destruction must meet or exceed those used internally by NSCS. In all cases the vendor must

supply a certificate of destruction detailing the inventory of media destroyed, and the destruction method used. Third-party disposal contracts should allow for audits by NSCS on an as-needed basis.

Revision History

April/14/2019: Initial submission by PCSS
May/8/2019: Initial review by SOISO/CISOs
July/8/2019: Second review by SOISO/CISOs
July/26/2019: Third review by SOISO
Sept/30/2019: Fourth review by SOISO/CISOs with campus feedback
Nov/11/2021: Change time when accounts can be created