University System of New Hampshire

CYBERSECURITY MATURITY MODEL CERTIFICATION STANDARD V2.0 LEVEL 2

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: Cybersecurity & Networking
Approved Distribution: Designated Reviewers Only
Status: In-Force (Subject to Change when US Department of Defense Provides Final Guidance)

1 PURPOSE

This Standard aims to establish procedures and policies for CMMC (Cybersecurity Maturity Model Certification). It is a certification program created by the Department of Defense (DoD) that assesses an organization's cybersecurity posture. As a Department of Defense partner, USNH had identified a need to achieve at least Level 2 certification within the Cybersecurity Maturity Model Certification (CMMC) V2.0. Below are 6 general steps to NIST 800-171 compliance. By following these 6 steps and the 110 National Institute of Standards and Technology (NIST) 800-171 controls, USNH can demonstrate CMMC V2 Level 2 compliance.

1. Locate and Identify: Identify the systems on your network that hold or might hold Controlled Unclassified Information (CUI). These storage locations could include local storage, Network Attached Storage devices, cloud storage, portable hard drives, flash drives. Removal of CUI from approved locations is not permitted to hold CUI classification.

2. Categorize: Categorize your data and separate CUI files from non-CUI files. Use this step to reduce unnecessary duplication of data. Steps 1 and 2 are completed by the PI and form the foundation that allows for the effective implementation of additional security controls.

3. Implement Required Controls: Implement the 110 NIST 800-171 controls. Local IT may be able to assist the Primary Investigator (PI) with some of the controls during this stage, but the PI is responsible for NIST/CMMC V 2.0 Level 2 compliance.

4. Training: The PI must ensure anyone who has access to their CUI receives training on the fundamentals of information security on a regular basis. In addition, the PI must train individuals on their specific processes and procedures for handling CUI.

5. Monitor: The PI is responsible for providing access and monitoring those who access CUI.

6. Assessment: Conduct security assessments by examining all systems that may contain CUI. Security assessments must be completed on a regular basis.

2 SCOPE

This standard applies to all USNH business and academic units and USNH-owned information systems that collect, store, process, share or transmit CMMC related data. CMMC is a unified standard that takes into account the various information security standards and best practices that need to be implemented within the defense industrial base supply chain to protect federal contract information (FCI) and controlled unclassified information (CUI). This standard focuses on Level 2 certification within the Cybersecurity Maturity Model Certification (CMMC) V2.0 for FCI related information. Both CUI (Controlled Unclassified Information) and FCI (Federal Contract Information) include information created or collected by or for the Government, as well as information received from the Government. However, while FCI is any information that is “not intended for public release,” CUI is information that requires safeguarding and may also be subject to dissemination controls. Both CUI and FCI are considered unclassified, but still sensitive information that requires a certain level of safeguards. For Level 1/FCI only related issues, please refer to the CYBERSECURITY MATURITY MODEL CERTIFICATION STANDARD V2.0 LEVEL 1 Standard.

3 AUDIENCE

All USNH community members who access USNH CMCC Version 2.0 Level 2 related data and resources. Organizations seeking Level 2 requirements will require 3rd party certification. Requirements will mirror NIST SP 800-171. CMMC V2 has eliminated all practices and maturity processes that were unique to CMMC 1.0 and aligns with the 14 levels and 110 security controls developed by the National Institute of Technology and Standards (NIST) to protect CUI.

4.1 ACCESS CONTROL (AC) domain focuses on the tracking and understanding of who has access to your systems and network. This includes user privileges, remote access, and internal system access. This follows NIST Control Number 3.1.

- 3.1.1 - AC-2, AC-3 - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). Maintain list of authorized users defining their identity and associated role and sync with system, application, and data layers. Account requests must be authorized before access is granted.
- 3.1.2 - AC-17 - Limit information system access to the types of transactions and functions that authorized users are permitted to execute. Utilize access control (derived from 3.1.1) to limit access to applications and data based on role and/or identity. Log access as appropriate.
- 3.1.3 - AC-4 - Control the flow of sensitive data in accordance with approved authorizations. Provide architectural solutions to control the flow of system data. The solutions may include firewalls, proxies, encryption, and other security technologies.
- 3.1.4 - AC-5 - Separate the duties of individuals to reduce the risk of malevolent activity without collusion. If a system user accesses data as well as maintains the system in some way, create separate accounts with appropriate access levels to separate functions.
- 3.1.5 - AC-6(1&5) - Employ the principle of least privilege, including for specific security functions and privileged accounts. Only grant enough privileges to a system user to allow them to sufficiently fulfill their job duties. 3.1.4 references account separation.
- 3.1.6 - AC-6(2) - Use non-privileged accounts or roles when accessing non-security functions. Users with multiple accounts (as defined in 3.1.4 and 3.1.5) must logon with the least privileged account. Most likely, this will be enforced as a policy.
- 3.1.7 - AC-6(9-10) - Prevent non-privileged users from executing privileged functions and audit the execution of such functions. Enable auditing of all privileged functions, and control access using access control lists based on identity or role.
- 3.1.8 - AC-7 -Limit unsuccessful logon attempts. Configure system to lock logon mechanism for a predetermined time and lock user account out of system after a predetermined number of invalid logon attempts.
- 3.1.9 - AC-8 - Provide privacy and security notices consistent with applicable sensitive data rules. Logon screen should display appropriate notices.
- 3.1.10 - AC-11(1) - Use session lock with pattern hiding displays to prevent access/viewing of data after period of inactivity. Configure system to lock session after a predetermined time of inactivity. Allow user to lock session for temporary absence.
- 3.1.11 - AC-12 - Terminate (automatically) a user session after a defined condition. Configure system to end a user session after a predetermined time based on duration and/or inactivity of session.
- 3.1.12 - AC-17(1) - Monitor and control remote access sessions. Run network and system monitoring applications to monitor remote system access and log accordingly. Control remote access by

running only necessary applications, firewalling appropriately, and utilize end to end encryption with appropriate access (re 3.1.1).

- 3.1.13 -AC-17(2) -Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. Any application used to remotely access the system must use approved encryption methods.
- 3.1.14 - AC-17(3) - Route remote access via managed access control points. Remote access is used by authorized methods only and is maintained by IT Operations.
- 3.1.15 - AC-17(4) - Authorize remote execution of privileged commands and remote access to security-relevant information. Remote access for privileged actions is only permitted for necessary operational functions.
- 3.1.16 - AC-18 - Authorize wireless access prior to allowing such connections. Organization officials will authorize the use of wireless technologies and provide guidance on their use. Wireless network access will be restricted to the established guidelines, monitored, and controlled.
- 3.1.17 - AC-18(1) - Protect wireless access using authentication and encryption. Wireless access will be restricted to authorized users only and encrypted according to industry best practices.
- 3.1.18 - AC-19 - Control connection of mobile devices. Organization officials will establish guidelines for the use of mobile devices and restrict the operation of those devices to the guidelines. Usage will be monitored and controlled.
- 3.1.19 - AC-19(5) - Encrypt CUI on Mobile devices and mobile computing platforms. Mobile devices will be encrypted.
- 3.1.20 -AC-20, AC-20(1) - Verify and control/limit connections to and use of external information systems. Guidelines and restrictions will be placed on the use of personally owned or external system access. Only authorized individuals will be permitted external access and those systems must meet the security standards set out by the organization.
- 3.1.21 - AC-20(2) - Limit use of organizational portable storage devices on external information systems. Guidelines and restrictions will be placed on the use of portable storage devices.
- 3.1.22 - AC-22 - Control information posted or processed on publicly accessible information systems. Only authorized individuals will post information on publicly accessible information systems. Authorized individuals will be trained to ensure that non-public information is not posted. Public information will be reviewed annually to ensure that non-public information is not posted.

4.2 AWARENESS AND TRAINING (AT) domain focuses on ensuring that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

- 3.2.1 - AT-2, AT-3 - Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards and procedures related to the security of organizational information systems. Users, managers, and system administrators of the information system will receive initial and annual training commensurate with their role and responsibilities. The training will provide a basic understanding of the need for information security, applicable policies, standards, and procedures related to the security of the information system, as well as user actions to maintain security and respond to suspected security incidents. The content will also address awareness of the need for operations security.

- 3.2.2 - AT-2, AT-3 - Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. Personnel with security-related duties and responsibilities will receive initial and annual training on their specific operational, managerial, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Training will address required security controls related to environmental and physical security risks, as well as training on indications of potentially suspicious email or web communications, to include suspicious communications and other anomalous system behavior.
- 3.2.3 - AT-2(2) - Provide security awareness training on recognizing and reporting potential indicators of insider threat. Users, managers, and administrators of the information system will receive annual training on potential indicators and possible precursors of insider threat, to include long-term job dissatisfaction, attempts to gain unauthorized access to information, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices. Security training will include how to communicate employee and management concerns regarding potential indicators of insider threat in accordance with established organizational policies and procedures.

4.3 AUDIT ACCOUNTABILITY (AU) – Focuses on creating, protecting, and retaining information system audit records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful, unauthorized, or inappropriate information system activity. identifying, tracking and ongoing maintenance of media. It also includes policies about protection, data sanitation and acceptable transportation.

- 3.3.1 - AU-2, AU3, AU-3(1), AU-6, AU12 - Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful, unauthorized, or inappropriate information system activity. The organization creates, protects, retains information system audit records (follow appropriate retention schedule based on data source and applicable regulations) to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

- 3.3.2 - AU-2, AU3, AU-3(1), AU-6, AU12 - Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. The organization correlates network activity to individual user information order to uniquely trace and hold accountable users responsible for unauthorized actions.
- 3.3.3 - AU-2(3) - Review and update audited events. The organization reviews and updates audited events annually or in the event of substantial system changes or as needed, to ensure that the information system is capable of auditing events, to ensure coordination with other organizational entities requiring audit-related information and provide a rational for why auditable events are deemed adequate to support security investigations.
- 3.3.4 - AU-5 - Alert in the event of an audit process failure. The information system alerts personnel with security responsibilities in the event of an audit processing failure and maintains audit records on host servers until log delivery to central repositories can be re-established.
- 3.3.5 - AU-6(3) - Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity. The organization employs automated mechanisms across different repositories to integrate audit review, analysis, correlation, and reporting processes to support organizational processes for investigation and response to suspicious activities, as well as gain organization-wide situational awareness.
- 3.3.6 - AU-7 - Provide audit reduction and report generation to support on demand analysis and reporting. The information system's audit capability supports an audit reduction and report generation capability that supports on demand audit review, analysis, and reporting requirements and after-the-fact security investigations; and does not alter the original content or time ordering of audit records. The system provides the capability to process audit records for events based on a variety of unique fields, to include user identity, event type, location, times, dates, system resources, IP, or information object accessed.
- 3.3.7 - AU-8, AU-8(1) - Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. The information system uses internal system clocks to generate time stamps for audit records, and records time stamps that can be mapped to UTC; compares system clocks with authoritative NTP servers and synchronizes system clocks when the time difference is greater than 1 second.
- 3.3.8 - AU-9 - Protect audit information and audit tools from unauthorized access, modification, and deletion. The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

- 3.3.9 - AU-9(4) - Limit management of audit functionality to a subset of privileged users. The organization authorizes access to management of audit functionality to only authorized individuals with a designated audit responsibility.

4.4 CONFIGURATION MANAGEMENT (CM) Establishes and maintains baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

- 3.4.1 - CM-2, CM-6, CM-8, CM-8(1) - Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. Baseline configurations will be developed, documented, and maintained for each information system type. Baseline configurations will include software versions and patch level, configuration parameters, network information including topologies, and communications with connected systems. Baseline configurations will be updated as needed to accommodate security risks or software changes. Deviations from baseline configurations will be documented.
- 3.4.2 - CM-2, CM-6, CM-8, CM-8(1) - Establish and enforce security configuration settings for information technology products employed in organizational information systems. Security settings will be included as part of baseline configurations. Security settings will reflect the most restrictive appropriate for compliance requirements. Changes or deviations to security settings will be documented.
- 3.4.3 - CM-3 - Track, review, approve/disapprove and audit changes to information systems. Changes or deviations to information system security control configurations that affect compliance requirements will be reviewed and approved. The changes will also be tracked and documented. Change control tracking will be audited annually.
- 3.4.4 - CM-4 - Analyze the security impact of changes prior to implementation. Changes or deviations that affect information system security controls pertaining to compliance requirements will be tested prior to implementation to test their effectiveness. Only those changes or deviations that continue to meet compliance requirements will be approved and implemented.
- 3.4.5 - CM-5 - Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system. Only those individuals approved to make physical or logical changes on information systems will be allowed to do so. Authorized personnel will be approved and documented. All change documentation will include the authorized personnel making the change.
- 3.4.6 - CM-7 -Employ the principle of least functionality by configuring the information system to provide only essential capabilities. Information systems will be configured to deliver one function per system where practical.

- 3.4.7 - CM-7(1-2) - Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services. Only those ports and protocols necessary to provide the service of the information system will be configured for that system. Applications and services not necessary to provide the service of the information system will not be configured or enabled. Systems services will be reviewed to determine what is essential for the function of that system.
- 3.4.8 - CM-7(4-5) - Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. The information system will be configured to only allow authorized software to run. The system will be configured to disallow running unauthorized software. The controls for allowing or disallowing the running of software may include but is not limited to the use of firewalls to restrict port access and user operational controls.
- 3.4.9 - CM-11 - Control and monitor user-installed software User controls will be in place to prohibit the installation of unauthorized software. All software for information systems must be approved.

4.5 IDENTIFICATION AND AUTHENICATION (IA) Identify information system users, processes acting on behalf of users, or devices.

- 3.5.1 - IA-2, IA-5 - Identify information system users, processes acting on behalf of users, or devices. Systems will make use of institutionally assigned accounts for unique access by individuals. Should service accounts be necessary for device or process authentication, the accounts will be created by the central identity management team. Institutional and service accounts are managed centrally and deprovisioned automatically when an individual leaves.
- 3.5.2 - IA-2, IA-5 - Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. Per control 3.5.1, the accounts in use will be assigned and managed by the university's central identity management system. Accounts are provisioned as part of the established account creation process. Accounts are uniquely assigned to faculty, staff upon hire; students upon matriculation; or affiliates when sponsored by an authorized faculty or staff member. Access to data associated with the project is controlled through role-based authorization by the project's PI. Initial passwords are randomly generated strings provided via a password reset mechanism to each faculty, staff, student or affiliate. The password must be reset upon first use. Passwords must comply with the university's Password Policy.
- 3.5.3 - IA-2(1-3) - Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. Any network access to servers and virtual machines hosting the project data requires multifactor authentication provided by university regardless of if the account is privileged or unprivileged.

- 3.5.4 - IA-2(8-9) - Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. Only anti-replay authentication mechanisms will be used. The authentication front-end technologies include shibboleth, SSH, Microsoft remote desktop protocol. Backend authentication mechanisms in use include Kerberos and Active Directory.
- 3.5.5 - IA-4 - Prevent reuse of identifiers for a defined period. Per control 3.5.1, the accounts in use will be assigned and managed by the university's central identity management system. Accounts are provisioned as part of the established account creation process. Accounts are uniquely assigned to faculty, staff, students, and affiliates (guests). Account identifiers are not reused.
- 3.5.6 - IA-4 - Disable identifiers after a defined period of inactivity. User accounts or identifiers associated with a project or contract covered by NIST 800-171 are monitored for inactivity. Disable account access to the in-scope systems after 180 days of inactivity.
- 3.5.7 - IA-5(1) - Enforce a minimum password complexity and change of characters when new passwords are created.   Account passwords must be a minimum of 8 characters and a mix of upper/lower case, numbers and symbols.
- 3.5.8 - IA-5(1) - Prohibit password reuse for a specified number of generations. Users may not re-use the same password when changing their password for at least 6 changes.
- 3.5.9 - IA-5(1) - Allow temporary password to use for system logons with an immediate change to a permanent password. New employees will receive an account and instructions for creating a password during the hiring process. New students receive notification of their account and will need to set their initial password. Temporary passwords are only good to allow for a password reset.
- 3.5.10 - IA-5(1) - Store and transmit only encrypted representation of passwords. Passwords are not stored in reversible encryption form in any of our systems. Instead, they are stored as one-way hashes constructed from passwords using AES256 or stronger encryption.
- 3.5.11 - IA-6 - Obscure feedback of authentication information. The most basic feedback control is never informing the user in an error message what part of the of the authentication transaction failed. In the case of shibboleth, for example, the error message is generic regardless of whether the user-id was mistyped, the password was wrong, or (in the case of MFA) there was a problem with the MFA credential provided — the failure simply says that the credentials were invalid. Likewise, unsuccessful authentications at the Kerberos KDCs don’t distinguish between the “principal not found” and the “invalid key” case. LDAP-based authentication interfaces only return a “failure to bind” message from both the main LDAPs and the AD.

4.6 INCIDENT RESPONSE (IR) Establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery and user response activities.

- 3.6.1 - IR-2, IR-4, IR-5, IR-6, IR-7 - Establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities. Develop an institutional incident response policy; specifically outline requirements for handling of incidents involving CUI.
- 3.6.2 - IR-2, IR-4, IR-5, IR-6, IR-7 - Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization. Develop an institutional incident response policy; specifically outline requirements for tracking and reporting of incidents involving CUI to appropriate officials.
- 3.6.3 - IR-3, IR-3(2) - Test the organizational incident response capability. Develop an institutional incident response policy; specifically outline requirements for regular testing and reviews/improvements to incident response capabilities.

4.7 MAINTAINENCE (MA) Perform maintenance on organizational information systems.

- 3.7.1 - MA-2, MA-3, MA-3(2-1) - Perform maintenance on organizational information systems. All systems, devices, supporting systems for organizational information systems must be maintained according to manufacturer recommendations or organizationally defined schedules.
- 3.7.2 - MA-2, MA3, MA-3(2-1) - Provide effective controls on the tools, techniques, mechanisms and personnel used to conduct information system maintenance. Organizations will put in place controls that limit the tools, techniques, mechanisms and personnel that will be used to maintain information systems, devices, and supporting systems. This can include a list of authorized tools, authorized personnel, and authorized techniques and mechanisms. Any such maintenance must occur within the context of other information systems controls in place.
- 3.7.3 - MA-2 - Ensure equipment removed for off-site maintenance is sanitized of any sensitive data. Any media that is removed from the premises for maintenance or disposal must be sanitized according to the organization's media sanitization policies.
- 3.7.4 - MA-3(2) - Check media containing diagnostic and test programs for malicious code before the media are used in the information system. Any media that is provided by authorized maintenance personnel (and not normal Systems administrators/owners) for troubleshooting, diagnostics, or other maintenance must be run through an anti-virus/anti-malware program prior to use in an organizational information system.
- 3.7.5 - MA-4 - Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. All remote access to an information system for maintenance or diagnostics must occur via an approved remote solution using multi-factor authentication. A remote session must be disconnected when maintenance is complete.

- 3.7.6 - MA-5 - Supervise the maintenance activities of maintenance personnel without required access authorization. All activities of maintenance personnel who do not normally have access to a system must be monitored. The organization will define approved methods for supervision.

4.8 MEDIA PROTECTION (MP) Protects (i.e., physically control and securely store) information system media containing sensitive data, both paper and digital.

- 3.8.1 - MP-2, MP-4, MP-6 - Protect (i.e., physically control and securely store) information system media containing sensitive data, both paper and digital. Responsible parties for data in these systems will document and ensure proper authorization controls for data in media and print. Documented workflow, data access controls and media policy will be enforced to ensure proper access controls.
- 3.8.2 - MP-2, MP-4, MP-6 - Limit access to sensitive data on information system media to authorized users. All CUI systems will be managed under least access rules.
- 3.8.3 - MP-2, MP4, MP-6 - Sanitize or destroy information system media containing sensitive data before disposal or release for reuse. All managed data storage will be erased, encrypted, or destroyed using mechanisms with sufficient power to ensure that no usable data is retrievable from storage devices identified in the workflow of these systems/services.
- 3.8.4 - MP-3 - Mark media with necessary sensitive data markings and distribution limitations. All CUI systems will be identified with an asset control identifier.
- 3.8.5 - MP-5 - Control access to media containing sensitive data and maintain accountability for media during transport outside of controlled areas. Only approved individuals are to have access to media from CUI systems. A chain of evidence will be maintained for any media removed from these systems.
- 3.8.6 - MP-5(4) - Implement cryptographic mechanisms to protect the confidentiality of sensitive data stored on digital media during transport unless otherwise protected by alternative physical safeguards All CUI data on media will be encrypted or physically locked prior to transport outside of the institution’s secure locations.
- 3.8.7 - MP-7 - Control the use of removable media on information system components. Removable media will only be allowed if there are processes in place to control them. Removable media must be able to support physical encryption and key vaulting must be utilized to ensure recoverability.
- 3.8.8 - MP-7(1) - Prohibit the use of portable storage devices when such devices have no identifiable owner. Only approved portable storage devices under asset management are to be used to store CUI data.
- 3.8.9 - CP-9 - Protect the confidentiality of backup sensitive data at storage locations. Data backups will be encrypted on media before removal from a secured facility.

4.9 PERSONNEL SECURITY (PS) Screen individuals prior to authorizing access to information systems containing sensitive data.

- 3.9.1 - PS-3, PS-4, PS-5 - Screen individuals prior to authorizing access to information systems containing sensitive data. The organization will screen individuals prior to authorizing access to the information system, in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Criteria may include, for example, position sensitivity background screening requirements.
- 3.9.2 - PS-3, PS-4, PS-5 - Ensure that sensitive data and information systems containing sensitive data are protected during and after personnel actions such as terminations and transfers. The organization will disable information system access prior to individual termination or transfer. Within 48 hours of termination or transfer, the organization will revoke any authenticators/credentials associated with the individual, retrieve all organizational information system-related property from the individual, retain access to organizational information and information systems formerly controlled by the individual, and notify the information security office and data owner of the change in authorization.

4.10 PHYSCIAL PROTECTION (PP) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

- 3.10.1 - PE-2, PE-5, PE-6 - Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. The university will design physical security protections (including guards, locks, cameras, card readers, etc.) as necessary to limit physical access to the area to only authorized individuals. Output devices such as printers should be placed in areas where their use does not expose data to unauthorized individuals.
- 3.10.2 - PE-2, PE-5, PE-6 - Protect and monitor the physical facility and support infrastructure for those information systems. The university will review the location and type of physical security in use (including guards, locks, card readers, etc.) and evaluate its suitability for the organization's needs.
- 3.10.3 - PE-3 - Escort visitors and monitor visitor activity. All visitors to sensitive areas will be always escorted by an authorized employee.
- 3.10.4 - PE-3 - Maintain audit logs of physical access. Logs of physical access to sensitive areas are maintained according to retention policies. This includes authorized access as well as visitor access.
- 3.10.5 - PE-3 - Control and manage physical access devices. Physical access devices (such as card readers, proximity readers, and locks) will be maintained and operated according to the manufacturer recommendations. These devices will be updated with any changed access control

information as necessary to prevent unauthorized access. The university will review the location and type of each physical access device and evaluate its suitability for the organization's needs.
- 3.10.6 - PE-17 - Enforce safeguarding measures for sensitive data at alternate work sites (e.g., telework sites). All alternate sites where sensitive data is stored or processed must meet the same physical security requirements as the main site.

4.11 RISK ASSESSMENT (RA) Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of sensitive data.

- 3.11.1 - RA-3 - Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of sensitive data. The stewards of the system/services will provide an initial and periodic risk assessment. The assessments will be impact scored using FIPS 199. Changes in the environment that may affect the system or service, changes in use of or infrastructure will be documented and assessed as modified. The impact analysis is to be a living document and incorporated into a larger risk assessment profile for the system/service.
- 3.11.2 - RA-5, RA- 5(5) - Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified. Systems will be periodically scanned for common and new vulnerabilities. Any vulnerability not documented will be risk assessed and documented. Reports regarding the scans will be made available to system stewards and owners in a timely manner.
- 3.11.3 - RA-5 - Remediate vulnerabilities in accordance with assessments of risk Stewards and owners upon recognition of any vulnerability will provide an action plan for remediation, acceptance, aversion, or transference of the vulnerability risk including a reasonable time frame for implementation. All high vulnerabilities will be prioritized.

4.12 SECURITY ASSESSMENT (CA) Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application. An annual security assessment will be conducted to ensure that security controls are implemented correctly and meet the security requirements for the compliance environment.

- 3.12.1 - CA-2, CA-5, CA-7 - Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application. An annual security assessment will be conducted to ensure that security controls are implemented correctly and meet the security requirements for the compliance environment. The assessment scope includes all information systems and networks in or directly connected to the compliance environment and all security controls and procedures necessary to meet the compliance requirements of the environment. The assessment will include, but is not limited to, vulnerability scanning, penetration testing, security control testing and reviews, configuration testing and reviews, log reviews, and personnel interviews. A representative sampling of systems will be assessed. Information Security, or an independent security auditor, will conduct the assessment. A final written assessment report and findings will be provided to the CIO at the conclusion of the assessment.

- 3.12.2 - CA-2, CA-5, CA-7 - Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems. An action plan to remediate identified weaknesses or deficiencies will be maintained. The action plan will designate remediation dates and milestones for each item. Deficiencies and weaknesses identified in security controls assessments, security impact analyses, and continuous monitoring activities will be added to the action plan within 30 days of the findings being reported.
- 3.12.3 - CA-2, CA-5, CA-7 - Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls. Continuous monitoring tools will be deployed for front Internet facing systems or those used to store or transmit sensitive data. At a minimum, systems will be monitored for privileged access, permission changes, kernel modifications, and binary changes, against a control and system baseline. Continuous monitoring reports and alerts will be reviewed daily. Unauthorized changes or unauthorized access will be reported to the CISO and information system owner within 24 hours of it being reported.
- 3.12.4 - Develop, document, and periodically update systems security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationship with or connections to other systems. NIST says, "There is no prescribed format or specified level of detail for system security plans. However, organizations must ensure that the required information in 3.12.4 is appropriately conveyed in those plans."

4.13 SYSTEM AND COMMUNICATIONS PROTECTION (SC) Monitor, control and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

- 3.13.1 - SC-7 - Monitor, control and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. Enumerate policies for managed interfaces such as gateways, routers, firewalls, VPNs; organizational DMZs; and restricting external web traffic to only designated servers.

- 3.13.2 - SC-8 - Employ architectural designs, software development techniques and systems engineering principles that promote effective information security within organizational information.
- Systems- Outline organizational information security policies, to include standards for architectural design, software development, and system engineering principles designed to promote information security.
- 3.13.3 - SC-2 - Separate user functionality from information system management functionality. Enumerate the physical or logical controls used to separate user functionality from system management-related functionality to ensure that administration/privilege options are not available to general users).
- 3.13.4 - SC-4 - Prevent unauthorized and unintended information transfer via shared system resources Enumerate the controls implemented to prevent object reuse and to protect residual information.
- 3.13.5 - SC-7 - Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. Outline the policies for organizational Firewall DMZs.
- 3.13.6 - SC-7(5) - Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). Document all business need exceptions to network communications traffic (inbound/outbound) “deny all” policies.
- 3.13.7 - SC-7(7) - Prevent remote devices from simultaneously establishing nonremote connections with the information system and communicating via some other connection to resources in external networks Outline controls to prevent split tunneling in remote devices, and to mandate VPN use when necessary for business functions.
- 3.13.8 - SC-8, SC-8(1) - Implement cryptographic mechanisms to prevent unauthorized disclosure of sensitive data during transmission unless otherwise protected by alternative physical safeguards Outline the processes and automated mechanisms used to provide encryption of CUI during transmission; or document all alternative physical safeguards used to provide confidentiality of CUI during transmission.
- 3.13.9 - SC-10 - Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. Outline controls for terminating communications sessions on both internal and external networks (e.g., deallocating TCP/IP addresses/port pairs); and institute time periods of inactivity based on type of network access.
- 3.13.10 - SC-12 - Establish and manage cryptographic keys for cryptography employed in the information system Outline the processes and automated mechanisms used to provide key management within the information system (should also follow any relevant laws, regulations, and policies).

- 3.13.11 - SC-13 - Employ FIPS-validated cryptography when used to protect the confidentiality of sensitive data. Outline where FIPS-validated cryptographic is used.
- 3.13.12 - SC-15 - Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. Enumerate actions to remove or disable collaborative computing devices from information systems housing CUI; and to notify users when collaborative computing devices are in use (e.g., cameras, microphones, etc.).
- 3.13.13 - SC-18 - Control and monitor the use of mobile code. Define limits of mobile code usage, establish usage restrictions, and specifically authorize use of mobile code (e.g., Java, ActiveX, Flash, etc.) within an information system.
- 3.13.14 - SC-19 - Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. Define and establish usage restrictions, and specifically authorize the business necessary use of VoIP technologies within an information system.
- 3.13.15 - SC-23 - Protect the authenticity of communications sessions. Outline the controls implemented to protect session communications (e.g., the controls implemented to validate identities and information transmitted to protect against MITM attacks, session hijacking, and insertion of false information into sessions).
- 3.13.16 - SC-28 - Protect the confidentiality of sensitive data at rest. Outline controls used to protect CUI while stored in organizational information systems.

4.14 SYSTEM AND INFORMATION INTEGRITY (SI) Identify, report and correct information and information system flaws in a timely manner.

- 3.14.1 - SI-2, SI-3, SI-5 - Identify, report and correct information and information system flaws in a timely manner. The organization will perform all security relevant software updates, to include patching, service packs, hot fixes, and anti-virus signature additions in response to identified system flaws and vulnerabilities within the time prescribed by organizational policy (Critical/High: 5 days, Moderate: 30 days, Low: As Available). When available, managers and administrators of the information system will rely on centralized management of the flaw remediation process, to include the use of automated update software, patch management tools, and automated status scanning.
- 3.14.2 - SI-2, SI-3, SI-5 - Provide protection from malicious code at appropriate locations within organizational information systems The organization will employ malicious code protection mechanisms at information system entry and exit points to minimize the presence of malicious code. These protection mechanisms may include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices.
- 3.14.3 - SI-2, SI-3, SI-5 - Monitor information system security alerts and advisories and take appropriate actions in response. The organization will receive security alerts, advisories, and

directives from reputable external agencies, and disseminate this information to individuals with need-to-know in the organization. In the event of alerts, advisories, or directives that have widespread impact on the organization, internal security directives will be disseminated directly to information system users, managers, and administrators.

- 3.14.4 - SI-3 - Update malicious code protection mechanisms when new releases are available. The organization will update information system protection mechanisms in a timely manner.
- 3.14.5 - SI-3 - Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. The organization will perform quarterly scans of the information system, as well as real-time scanning of files from external sources.
- 3.14.6 - SI-4, SI (4) - Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks The organization will monitor the information system to detect attacks and indicators of potential attacks, as well as unauthorized local, network, and remote connections. The organization will strategically deploy monitoring devices within the information system to collect essential information system. Information gained from these monitoring tools will be protected from unauthorized access, modification, and deletion.
- 3.14.7 - SI-4 - Identify unauthorized use of the information system. The organization will monitor the information system to identify unauthorized access and use, as well as potential misuse of the information system.

4 MAINTENANCE OF PROCESSES AND PROCEDURES RELATED TO THIS STANDARD

As part of the mandatory annual review of this Standard required by the *USNH Cybersecurity Policy*, the processes and procedures that support the requirements defined in this Standard shall be reviewed and, where needed, updated to ensure currency and continuous improvement.

5 ENFORCEMENT

Failure to comply with this Policy puts the University System, its component institutions, and its information and information technology resources at risk and may result in disciplinary action. Disciplinary procedures will be appropriate for the individual responsible for non-compliance (e.g., students, faculty, staff, vendors) as outlined in the relevant institutional regulations for that individual (e.g., student conduct and/or applicable personnel policies).

Non-compliant technology and/or activities may be mitigated as deemed necessary by the CISO and/or CIO.

Employees who are members of institutionally recognized bargaining units are covered by the disciplinary provisions set forth in the agreement for their bargaining units.

CONTACT INFORMATION

For USNH community members: Questions about this Standard, requests for additional information or training, or reports of violations can be directed to Cybersecurity Governance, Risk, and Compliance (GRC) via this Support Form.

All other requests can be submitted here: Submit an IT Question.

DOCUMENT HISTORY

Effective Date:	December 16, 2022
Approved by:	Dr David A Yasenchock, Interim CISO
Reviewed by:	Dr. David A Yasenchock, Director, Cybersecurity GRC
Revision History:	V 1.00