University System of New Hampshire

CYBERSECURITY POLICY

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: Cybersecurity & Networking
Approved Distribution: PUBLIC
Status: IN REVIEW

1 PURPOSE

This Policy informs all University System of New Hampshire (USNH) community members, which includes employees, students, prior students, alumni, parents, contractors, and vendors, of their responsibilities related to maintaining the privacy and security of institutional information and information technology resources.

Protection of information and information technology resources is critical to ensuring the confidentiality, integrity, and availability of that information and to support the ongoing success of USNH and the administrative, academic, and business units of its component institutions.

2 AUTHORITY

Authority to establish and enforce this Policy and all related Standards has been granted to the Chief Information Officer (CIO) by the USNH Admin Board.

3 SCOPE

This Policy and the related Standards apply to access and use of institutional information and information technology resources by all authorized USNH community members. It applies to information in digital format as well as information in physical formats (e.g., on paper).

For purposes of this Policy the term "information technology resources" shall include, but not be limited to, telecommunication and network equipment, desktop/laptop computers, mobile devices, servers, storage solutions, software packages, and applications which are owned by or operated on behalf of USNH, its component institutions, or any of its administrative, academic, or business units. The term shall also include non-institutional information technology resources used in the performance of official duties by faculty, staff, or administrators, but only to the extent of such use.

Critical Infrastructure Technology Resources, which includes industrial control systems (ICS) and operational technology (OT), are not in-scope for this Policy or the related Standards, unless explicitly indicated in the scope of a specific Standard.

4 AUDIENCE

USNH community members authorized to access or use institutional information and/or information technology resources should be familiar with this Policy and their responsibilities for compliance with the requirements it defines.

5 POLICY STATEMENT

5.1 CYBERSECURITY IS EVERYONE'S RESPONSIBILITY

5.1.1 All USNH community members have responsibility for protecting the confidentiality, availability, and integrity of USNH and its component institution's information and information technology resources.

5.1.2 All USNH and component institution information and information technology resources are assets of USNH. The provisions outlined in this Policy:

5.1.2.1 Apply to any USNH or component institution information, regardless of where or how it is accessed, captured, stored, processed, transmitted, or otherwise managed or what format it is in.

5.1.2.2 Apply to any device that accesses, captures, stores, processes, transmits, or otherwise manages institutional information and/or utilizes a USNH-owned or managed information technology resource, regardless of whether that device is itself an institutional information technology resource (owned and managed by USNH or its component institutions) or a non-institutional information technology resource (personally owned).

5.1.3 All USNH administrative, academic, and business units shall implement and enforce appropriate cybersecurity controls to:

- Protect the privacy and confidentiality of institutional information in all formats
- Safeguard institutional information against unauthorized use, modification, destruction, and loss
- Protect information technology resources from unauthorized access, compromise, modification, disruption, and destruction

5.1.4 Situations that are not covered by this Policy, or its related Standards, or situations for which

clarity is required to ensure compliance, shall be raised to the attention of the Chief Information Security Officer (CISO) for guidance and resolution.

5.2 GOVERNANCE

5.2.1 An organizational structure with clearly assigned responsibilities for oversight and enforcement of cybersecurity across the University System shall be established and maintained and led by the CISO.

5.2.2 The CISO shall develop and maintain a Cybersecurity Program and all its components, including this Policy and all related Policies, Standards, processes, and procedures.

5.2.3 The CIO shall be responsible for approval of the Cybersecurity Program and all related components. The CIO has the authority to delegate approval for aspects of this program to the CISO.

5.2.4 Standards, processes, and procedures outlining the requirements to comply with this, and other information technology or cybersecurity policies, shall be established in alignment with best practices and industry framework(s) identified in the Cybersecurity Program.

5.2.5 Cybersecurity Policies and Standards shall be maintained in an easily accessible location appropriate for authorized community members.

5.2.6 Processes required to monitor adherence to this Policy and the related Standards shall be established, implemented, monitored for effectiveness, and regularly reviewed, to enable and ensure continuous improvement.

5.2.7 Owners of all USNH information and information technology resources shall be assigned (e.g., information/data stewards, business application owners, technology service owners) and shall act as the authorizing manager for that asset.

5.3 PROTECTION OF USNH INFORMATION

5.3.1 All institutional information shall be classified according to the information classification system outlined in the *USNH Information Classification Policy*.

5.3.2 Pursuant to the relevant Standards, USNH community members shall adhere to established information handling requirements, respect the privacy of others whose information they have access to, and take appropriate precautions to protect that information from unauthorized disclosure or use.

5.3.3 Administrative, logical, and physical controls shall be implemented for all institutional information, regardless of the format of the information (e.g., electronic, stored on removable media, printed). Required controls shall be based on the information's classification and documented in the relevant Standard(s).

5.3.4 Access to and use of all institutional information, regardless of classification or format, shall be

authorized by the designated information steward.

5.3.5 All institutional information shall be encrypted per the requirements outlined in the relevant Standard(s).

5.3.6 All institutional information that is stored in physical formats shall be secured per the requirements outlined in the relevant Standards.

5.3.7 Access to institutional information tied to another specific community member's account shall only be authorized as outlined in the relevant Standard.

5.3.8 Access to institutional information shall only be granted to a vendor or other external party after all requirements defined in the relevant Standard(s) have been met.

5.3.9 Appropriate media sanitization methods as defined in the relevant Standard(s) shall be used to remove all institutional information from each information technology resource that is capable of storing data, prior to the release of that resource for disposal or re-use, or at the cessation of organizational control over that resource.

5.4 PROTECTION, CONTINUITY, AND RESILIENCE

5.4.1 USNH information and information technology resources shall be protected from natural and human hazards in alignment with the *Cybersecurity Risk Management Standard* and other relevant USNH Standard(s).

5.4.2 USNH information, regardless of where it is stored or by whom it is managed, shall be backed up according to requirements established in the relevant Standard(s).

5.4.3 The CIO and the CISO have the authority to act, with appropriate communication to business application owners, technology service owners, and the USNH community, if possible, to ensure that enterprise information technology resources do not pose a threat to the mission or operations of USNH or its component institutions, institutional information, or other information technology resources.

5.4.4 Enterprise Technology & Services (ET&S) shall develop, publish, and maintain an *Information Technology Disaster Recovery Plan* designed to minimize the effects of a disaster and support restoration of critical enterprise information technology resources and operations following a disaster.

5.5 RISK MANAGEMENT

5.5.1 Risk must drive cybersecurity decision making, investment, and prioritization.

5.5.2 The CISO shall be responsible for establishment, management, and maintenance of a Cybersecurity Risk Management Program which shall be documented in the relevant Standard(s).

5.5.3 All administrative, academic, and business units shall be required to participate in this Program, if requested to do so, and are responsible for implementing Risk Action Plans developed as a result of that participation.

5.5.4 All enterprise Information technology resources and critical administrative, academic, or business processes shall be assigned a security categorization as outlined in the relevant Standard(s). This categorization shall be used in formal and informal risk assessments involving that resource.

5.5.5 Cybersecurity risk assessments shall be performed, documented, actioned, tracked, reviewed, and revised as dictated by the relevant Standard(s).

5.5.6 Cybersecurity risks that are not mitigated, transferred, or avoided shall require risk acceptance as outlined in the relevant Standard(s).

5.6 PERSONNEL SECURITY

5.6.1 All USNH employees, including student workers that work with certain types of information, shall be subject to a background check according to the process dictated by USNH Human Resources.

5.6.2 USNH community members who manage institutional information and/or information technology resources on behalf of the University System, or its component institutions, shall be required to review and sign the *Enterprise Technology & Services Confidentiality and Cybersecurity Agreement*.

5.6.3 USNH community members authorized to access or use institutional information or information technology resources may be required to sign data-specific agreements and/or complete additional training requirements prior to being provided with that access.

5.7 AWARENESS & TRAINING

5.7.1 A Cybersecurity Awareness and Training Program, designed to reduce the risks of error, theft, fraud, misuse, or other compromise of institutional information and information technology resources, shall be established and documented in the relevant Standard(s).

5.7.2 USNH community members shall be informed of their responsibilities for the protection of institutional information and information technology resources and provided appropriate training to aid in fulfilling those responsibilities.

5.7.3 USNH community members with specific cybersecurity responsibilities shall be informed of these responsibilities and provided appropriate training to aid in fulfilling those responsibilities, prior to being granted any privileged or elevated access necessary to fulfill those responsibilities.

5.8 IDENTITY AND ACCESS MANAGEMENT

5.8.1 Access to institutional information shall be restricted to only those individuals with approved authorizations.

5.8.2 Institutional information shall only be shared, including verbally, in paper form, or via digital means, with those individuals who are authorized to receive it, using the appropriate mechanism for the information's classification as defined in the relevant Policies and Standards.

5.8.3 Access to institutional information stored in or managed by information technology resources shall be protected from unauthorized access through the management of identities, authentication credentials, accounts, and authorized access permissions.

5.8.4 Each USNH community member shall be assigned a single, primary USNH identity according to the requirements defined in the relevant Standard(s).

5.8.5 Use of USNH username shall be restricted to approved uses as established in the relevant Standard(s).

5.8.6 Access to institutional information and information technology resources shall be granted in accordance with the requirements and restrictions defined in the relevant Standard(s).

5.8.7 Passwords used to secure access to information technology resources shall follow the requirements established in the *USNH Password Policy*.

5.8.8 Accounts used to access information technology resources shall be approved, created, enabled, modified, disabled, removed, and used in accordance with the requirements established in the relevant Standard(s).

5.8.9 Privileged access to information technology resource shall be granted and managed in accordance with the requirements established in the relevant Standard(s).

5.8.10 Remote access to information technology resources shall comply with the established security requirements, usage restrictions, recommended configurations, and implementation guidance provided in the relevant Standard(s).

5.9 REGULATORY COMPLIANCE

5.9.1 Use and operation of information and information technology resources shall comply with federal, state, and local laws, USNH and component institution policies, and contractual obligations.

5.9.2 Access to and use of institutional information protected by regulation or industry requirement, including but not limited to the following, shall follow all requirements defined in the relevant Standard(s):

- FERPA – Family Educational Rights and Privacy Act
- HIPAA – Health Insurance Portability and Accountability Act
- GLBA – Gramm-Leach Bliley Act

- PCI-DSS – Payment Card Industry – Data Security Standard

5.9.3 The CISO shall institute programs, processes, procedures, and training, as needed, to inform USNH community members and administrators about the security controls needed to comply with applicable laws, regulations, USNH policies, and contractual obligations.

5.9.4 The CISO shall periodically conduct an audit of security controls implemented by administrative, academic, and business units to ensure compliance with applicable laws, regulations, USNH policies, and contractual obligations.

5.10 Physical and Environmental Security

5.10.1 USNH community members authorized to access and/or use information and information technology resources shall take appropriate measures, as outlined in relevant Standard(s), to prevent physical access to that information and those resources by unauthorized persons.

5.10.2 Technology Service Owners and Business Application Owners shall institute and enforce procedures, within their level of responsibility and authority, to protect the information and information technology resources under their control in compliance with the relevant Standard(s).

5.10.3 Physical access to facilities where specific types of information or information technology resources are housed or stored shall be restricted to authorized personnel. Examples of specific types include, but are not limited to:

- Information stored in paper format with a classification that requires physical access be restricted
- Infrastructure components including, but not limited to, networking equipment (e.g., switches and routers)
- Servers that are capturing, storing, processing, transmitting, or otherwise managing institutional information
- Endpoints that require specific physical security controls to meet research grant requirements or other contractual obligations

5.11 Network Management

5.11.1 All USNH networks shall be managed in such a manner that the confidentiality, integrity, and availability of institutional information and information technology resources are safeguarded from interference, unauthorized access, or compromise consistent with USNH's commitment to privacy, and the requirements defined in the relevant Standard(s).

5.11.2 Designated Network Administrators shall be responsible for management of all USNH networks and implementation of all required security controls to safeguard those networks, as defined in the relevant Standard(s).

5.11.3 Access to the information technology resources used to provide and manage USNH networks shall be appropriately restricted, both physically and logically, to ensure only authorized personnel have access.

5.11.4 USNH networks shall be monitored to detect cybersecurity incidents as required in the relevant Standard(s).

5.11.5 USNH wireless networks shall be managed, and the wireless spectrum monitored, to minimize interference between wireless networks and other devices using radio frequencies.

5.12 Information Technology Resource Management

5.12.1 Appropriate safeguards and controls shall be incorporated into the lifecycle of all information technology resources as required by the relevant Standard(s).

5.12.2 Required safeguards and controls shall be determined by the classification of the institutional information being accessed, captured, stored, processed, transmitted, or otherwise managed and/or the security categorization of the information technology resource(s).

5.12.3 Configuration changes made to information technology resources, regardless of where they are hosted or who manages them, shall be approved using the procedures defined in the relevant Standard(s).

5.12.4 Regular maintenance activities (e.g., applying patches, installing updates, arranging for annual service calls) shall be performed on all information technology resources according to the requirements defined in the relevant Standard(s).

5.12.5 All administrative, academic, and business units shall develop and maintain a comprehensive inventory of information technology resources for which they are responsible.

5.12.6 Software used to conduct USNH or component institution business shall comply with all Cybersecurity Policies and Standards, including software and applications that reside on USNH owned or managed information technology resources as well as software and applications that are provided by and/or managed by vendors.

5.12.7 Endpoint devices used to connect to USNH networks shall be configured, managed, used, maintained, and disposed of according to the requirements defined in the relevant Standard(s).

5.12.8 All servers connecting to USNH Networks shall be configured, administered, and managed in accordance with the requirements defined in the relevant Standard(s).

5.12.9 Administrative, academic, and business units shall not deploy, implement, or build enterprise information technology services that duplicate services provided by Enterprise Technology & Services (ET&S) (e.g., email servers) without the express written permission of the CIO. Unauthorized services may be blocked from accessing the network.

5.12.10 Enterprise telecommunication services and the information technology resources used to provide them shall be appropriately protected from intentional, unintentional, inappropriate, or

negligent acts or omissions according to the requirements in the relevant Standard(s).

5.13 VENDOR MANAGEMENT

5.13.1 Procurement and/or use of vendor information technology resources that capture, store, process, transmit, or otherwise manage institutional information shall require approval by Cybersecurity & Networking and follow the requirements defined in the relevant Standard(s). This includes vendor cloud-hosted applications and vendor-supported information technology resources that are hosted on-premise.

5.13.2 Administrative, academic, and business units that procure information technology resources from vendors, and who choose to manage and support those vendor applications internally, rather than engage in a support agreement with Enterprise Technology & Services (ET&S) for management of those resources, shall obtain ET&S approval and be responsible for:

- Ensuring appropriate cybersecurity controls are implemented
- Implementing and managing access controls aligned with the *Access Management Standard* and the *Accounts Management Standard*
- Providing support to the USNH community
- Maintaining that information technology resource (e.g., applying security patches, handling upgrades, monitoring performance)
- Managing the relationship with the vendor
- Maintaining appropriate audit trail artifacts and annual attestation(s)

5.14 INCIDENT MANAGEMENT

5.14.1 All members of the USNH community are responsible for reporting cybersecurity incidents, including any suspected, potential, or actual unauthorized disclosure of institutional information, to Cybersecurity & Networking immediately per the process identified in the *Cybersecurity Incident Response Plan*.

5.14.2 Cybersecurity events and incidents shall be investigated, mitigated, remediated, documented, and tracked according to the *Cybersecurity Incident Response Plan*.

5.14.3 To ensure appropriate, timely notification of potential and confirmed data breaches, the CISO, in cooperation with the USNH General Counsel's Office, shall manage all required notifications to relevant regulatory bodies pursuant to the relevant Standard(s).

5.15 POLICY MAINTENANCE

5.15.1 The CISO is responsible for documenting issues of clarity within this Policy or the related Standards raised by USNH community members and for ensuring those issues are resolved in a

timely manner through revision of this Policy and the related Standards.

5.15.2 This Policy and the related Standards shall be reviewed and maintained regularly, but no less than once per year.

6 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.

7 EXCEPTIONS

Requests for exceptions to this Policy shall be submitted and approved according to the requirements provided in the *Cybersecurity Exception Standard*.

8 ROLES AND RESPONSIBILITIES

8.1 ADMINISTRATIVE, ACADEMIC, AND BUSINESS UNIT LEADERSHIP:

8.1.1 Enforce appropriate cybersecurity controls to:

- Protect the privacy of institutional information
- Safeguard electronic and derivative information against unauthorized use and modification
- Protect information technology resources against unauthorized access, modification, and disruption
- Prevent the loss of or damage to institutional information and information technology resources

8.1.2 Develop and maintain a comprehensive inventory of information technology resources for which they are responsible.

8.1.3 Provide support, maintenance, and vendor relationship management, either directly, or through negotiated agreements with Enterprise Technology & Services (ET&S), for information technology resources procured from vendors.

8.1.4 Report all cybersecurity events or incidents to Cybersecurity & Networking.

8.2 Application Developer/System/Database/Application Administrator:

8.2.1 Ensure appropriate cybersecurity controls are applied during the information technology resource lifecycle.

8.2.2 Protect, to the extent practical, the information technology resources in their care from natural and human hazards.

8.2.3 Report all cybersecurity events or incidents to Cybersecurity & Networking.

8.3 Business Application Owner:

8.3.1 Institute and follow procedures to protect the information technology resources under their control from loss, damage, theft, compromise, and unauthorized access.

8.3.2 Ensure appropriate access management controls are implemented to reduce the risk of unauthorized access.

8.3.3 Report all cybersecurity events or incidents to Cybersecurity & Networking.

8.4 Chief Information Officer (CIO):

8.4.1 Approve all cybersecurity Policies and Standards.

8.5 Chief Information Security Officer (CISO):

8.5.1 Develop and maintain the Cybersecurity Program and all its components, including this Policy and all related Standards, processes, and procedures.

8.5.2 Ensure the Policies, Standards, processes, and procedures supporting the Cybersecurity Program are established in alignment with the framework(s) designated in the Cybersecurity Program.

8.5.3 Provide access to the Standards, processes, and procedures related to this Policy in an easily accessible location appropriate for authorized community members.

8.5.4 Monitor adherence to this Policy and all related Standards, processes, and procedures.

8.5.5 Establish the Cybersecurity Risk Management program.

8.5.6 Provide appropriate cybersecurity awareness training for all USNH community members.

8.5.7 Institute procedures to inform appropriate USNH community members about applicable laws, regulations, USNH and component institution policies, and contractual obligations.

8.5.8 Conduct an audit of security controls used to protect institutional information.

8.5.9 Review and approve exceptions to this Policy and related Standards.

8.6 INFORMATION STEWARD/DATA STEWARD:

8.6.1 Act as the authorizing manager for a designated information asset(s).

8.6.2 Authorize all access to and use of designated information asset(s).

8.7 NETWORK ADMINISTRATOR:

8.7.1 Manage all USNH networks in such a manner that institutional information and information technology resources are safeguarded from interference, unauthorized access, and compromise.

8.7.2 Manage the wireless spectrum to minimize interference between wireless networks and other devices that use radio frequencies.

8.7.3 Monitor and enforce compliance with this Policy on all USNH networks.

8.7.4 Report all cybersecurity events or incidents to Cybersecurity & Networking.

8.8 TECHNOLOGY SERVICE OWNER:

8.8.1 Institute and follow procedures to protect the information technology resources under their control from loss, damage, theft, compromise, and unauthorized access.

8.8.2 Create a safe environment for the housing and use of information technology resources under their control.

8.8.3 Report all cybersecurity events or incidents to Cybersecurity & Networking.

8.9 USNH COMMUNITY MEMBERS:

8.9.1 Protect the confidentiality, availability, and integrity of USNH and its component institution's information and information technology resources as required by the relevant Standard(s).

8.9.2 Follow processes and procedures provided by Enterprise Technology & Services (ET&S) and the USNH administrative, academic, and business units to ensure compliance with all required cybersecurity controls.

8.9.3 Complete all assigned cybersecurity training within the required timeframe.

8.9.4 Request clarification when needed to ensure understanding of responsibilities and requirements for complying with USNH policies and Standards.

8.9.5 Sign confidentiality and data handling agreements as required prior to accessing institutional information and/or information technology resources that require them.

8.9.6 Adhere to established information handling requirements, respect the privacy of others whose information they have access to, and take appropriate precautions to protect that information from unauthorized disclosure or use.

8.9.7 Report any suspected, potential, or actual unauthorized disclosure of institutional information per the process identified in the *Cybersecurity Incident Response Plan.*

8.9.8 Report all cybersecurity incidents to Cybersecurity & Networking.

9 DEFINITIONS

See the ET&S Policy & Standard Glossary for full definitions of each term.

- Access
- Access Control
- Account
- Administrative/Operational Control
- Administrator
- Asset
- Authentication
- Authorization
- Availability
- Breach
- Business Application Owner
- Business Continuity Plan
- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Cloud Service
- Confidentiality
- Credentials
- Critical Business Process
- Cybersecurity
- Disaster Recovery Plan
- Elevated Access
- Endpoint
- Exception
- Family Educational Rights and Privacy Act (FERPA)
- Gramm Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Identity
- Incident
- Information
- Information Security
- Cybersecurity Event
- Information Steward
- Information Technology Resource
- Institutional Information
- Integrity
- Internet of Things (IoT)
- Log
- Logical Control

- Mitigate
- Password
- Patch
- Payment Card Industry – Data Security Standard (PCI-DSS)
- Physical Security
- Policy
- Privileged Access
- Procedure
- Remote Access
- Removable Media
- Risk
- Risk Acceptance
- Risk Assessment
- Security Categorization
- Security Control
- Server
- Standard
- Technology Service Owner
- Username
- USNH Community Member
- Vendor

10 Related Policies and Standards

- USNH Acceptable Use Policy
- USNH Information Classification Policy
- USNH Password Policy
- USNH Privacy Policy

For a list of all Cybersecurity Standards related to this Policy, see the Cybersecurity Policies & Standards page.

CONTACT INFORMATION

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

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

University System of New Hampshire

DOCUMENT HISTORY

Effective Date:	01 MAY 2021 (pending final approval by USNH Admin Board in APR 2021)
Approved by:	USNH GENERAL COUNSEL'S OFFICE, 06 AUG 2020. V1 CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, 14 JUL 2020, v0.3 CYBERSECURITY POLICY & STANDARD WORKING GROUP, 21 MAY 2020, V0.2
Reviewed by:	USNH GENERAL COUNSEL'S OFFICE, 06 AUG 2020, v0.3 CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, 08 JUN 2020, v0.2, v0.3 CYBERSECURITY POLICY & STANDARD WORKING GROUP, APR/MAY 2020, V0.1, V0.2
Revision History:	REVISED PER USNH GCO REVIEW, 06 AUG 2020. V0.4 REVISED PER CISO REVIEW, 13 JUL 2020, V0.3 REVISED PER CYBERSECURITY POLICY & STANDARD WORKING GROUP, 27 MAY 2020, V0.2 REVIEW DRAFT FINALIZED, R BOYCE-WERNER, 08 MAR 2020. V0.1