University System of New Hampshire

USNH CYBERSECURITY POLICY OVERVIEW AND MAPPING

USNH INFORMATION TECHNOLOGY SECURITY POLICY MAPPING

Current Policy Link: https://www.usnh.edu/policy/usy/vi-property-policies/f-operation-and-maintenance-property - Section 5

Annotations below indicate how each of the provisions in this policy are addressed by the new USNH Cybersecurity Policy and/or the relevant USNH Cybersecurity Standards.

- *Italics* = existing Policy language
- **NP =** USNH Cybersecurity Policy
- **ST=** USNH Cybersecurity Standard
    - (future) = a Standard that will be developed to provide additional details but that is not planned to be published when the new Cybersecurity Policy becomes effective

5.1 The institutions and individuals of the University System of New Hampshire (USNH), including ITEC and the USNH Information Security Committee (ISC), shall provide appropriate security to protect the privacy of information, safeguard electronic and derivative information against unauthorized use and modification, protect systems against unauthorized access, protect systems and related operations against disruptions, and prevent the loss of or damage to IT resources.

- **NP** = Section 5.1

5.2 Information Technology Security Organization

USNH will establish and maintain an organizational structure with clearly assigned responsibilities for oversight and enforcement of USNH IT resources security, and a process for maintaining accountability for activities and system configurations that are inconsistent with the policy.

- **NP** = Section 5.2
- **ST** = USNH Cybersecurity Roles & Responsibilities Standard (future)

5.3 Physical and Environmental Security

USNH and each USNH institution, manager, provider and user of USNH IT resources is responsible for protecting, to the best of its ability, USNH IT resources. USNH and all USNH institutions, providers and users of USNH IT resources will institute and follow procedures, within their level of responsibility and authority, to protect those IT resources from loss, damage, compromise and unauthorized access, by creating a safe environment for the housing and use of those assets.

- **NP** = Section 5.10
- **ST** = Physical Information Technology Asset Access and Management Standard (future)

5.4 Computer, Network and Telecommunications Management

5.4.1 Network Management. USNH and providers and managers of USNH IT resources must manage the secure operation of the network environment and must do so in a manner that is consistent with a commitment to privacy and applicable USNH privacy policies.

- **NP** = Section 5.11
- **ST** =
    - Privately Managed Network Standard
    - Network Security and Management Standard
    - Wireless Network Security Standard (future)

5.4.2 Successful Operation of USNH Network Resources. USNH institutions will create appropriate policies and procedures to ensure and safeguard its IT resources from interference, threats, or other undesirable effects. In addition to IT resources, these policies and procedures shall include consideration for non-IT resources as well as consideration for devices not owned by the USNH either attached or unattached to the network.

- **NP** = Section 5.2
- **ST** = USNH Cybersecurity Roles & Responsibilities Standard (future)

5.4.3 Prevention of Loss, Modification or Misuse of Information Exchanged Between Organizations. All USNH institutions, providers and users of USNH IT resources will institute measures to safeguard the flow of data and information into and out of the networks.

- **NP** = Section 5.3
- **ST** =
    - Protected (or FERPA) Information Handling Standard
    - Restricted Information Handling Standard
    - Confidential Information Handling Standard
    - Network Security and Management Standard
    - Wireless Network Security and Management Standard (future)
    - Data Administration and Management Standard (future)

5.4.4 Protection of Wireless Air Space. USNH institutions will manage the wireless spectrum to minimize interference between wireless networks and other devices using radio frequencies.

- **NP** = Section 5.11.5
- **ST** = Wireless Network Security and Management Standard (future)

5.5 System Development & Maintenance

5.5.1 Security in Operational Systems and Prevention of Loss, Modification or Misuse of User Data in Application Systems

The appropriate level of protection must be incorporated into operational systems throughout the development process. Especially in cases where the data is sensitive or requires protection because of the risk and magnitude of loss or harm that could result from improper operation, manipulation or disclosure.

- **NP** = Section 5.3
- **ST** =
  - Protected (or FERPA) Information Handling Standard
  - Restricted Information Handling Standard
  - Confidential Information Handling Standard
  - Vendor Cloud Service Security Standard
  - Data Administration and Management Standard (future)
  - System Acquisition, Development, and Maintenance Lifecycle Standard (future)

5.5.2 Protection of Confidentiality, Authenticity and Integrity of Information

USNH will protect the confidentiality, authenticity and integrity of information.

- **NP** = Sections 5.1 and 5.3
- **ST** =
  - Protected (or FERPA) Information Handling Standard
  - Restricted Information Handling Standard
  - Confidential Information Handling Standard
  - Data Administration and Management Standard (future)

5.5.3 Conducting IT Projects and Support Activities in a Secure Manner

Changes and updates to systems and data must be traceable to accountable individuals and source documents under a defined management process.

- **NP** = 5.12
- **ST** =
  - System Acquisition, Development, and Maintenance Lifecycle Standard (future)
  - Security Configuration Management Standard (future)

5.5.4 Maintaining Security of Application System Software and Data

All USNH institutions and providers of USNH IT resources will provide and implement reasonable and adequate security measures to protect the information stored in IT resources.

- **NP** = Sections 5.3, 5.10, 5.11, 5.12, 5.13
- **ST** =
  - Endpoint Management Standard
  - Network Security and Management Standard
  - Privately Managed Network Standard

  - Vendor Cloud Service Security Standard
  - Data Center Facility Security, Access, and Use Standard (future)
  - Email Security and Use Standard
  - Information Technology Resource Disposal Standard (future)
  - Information Technology Resource Inventory Management Standard (future
  - Physical Information Technology Asset Access and Management Standard
  - Security Configuration Management Standard (future)
  - Security Logging and Monitoring Standard (future)
  - Server Security and Management Standard (future)
  - System Acquisition, Development, and Maintenance Lifecycle Standard (future)
  - Vulnerability and Patch Management Standard (future)
  - Wireless Network Security and Management Standard (future)

5.6 Disaster Recovery and Business Continuity Management Planning

5.6.1 Disaster Recovery and Response Management Plan. USNH and each USNH institution will develop, keep current, and publish adequate disaster recovery plans to minimize the effects of a disaster and support restoration of USNH critical operations following a disastrous event.

- **NP** = Section 5.4

5.6.2 Business Continuity Plan. A "Business Continuity Plan" shall be developed and implemented at all USNH institutions to facilitate the re-establishment and continuance of critical business functions after a disaster occurs.

- Removed – Business Continuity across all business units is not within the purview of ET&S; business continuity for ET&S operations will be part of the ET&S Contingency Plan along with the Information Technology Disaster Recovery Plan

5.7 System Access Control

5.7.1 Control Access to Information. Computer systems and resources used for the transaction of USNH business shall be protected from theft, malicious destruction, unauthorized alteration or exposure, or other potential compromise resulting from inappropriate or negligent acts or omissions.

5.7.1.1 Computer systems shall require utilization of employee-specific passwords for access. Passwords for access to USNH systems shall comply with industry standards as established by the institutional Chief Information Officers within the technological capabilities of each system.

- **NP** = Section 5.8.6
  - Also supported by the existing USNH Password Policy
- **ST** =
  - Access Management Standard
  - Privileged Access Management Standard
  - Password Management Standard (future)

5.7.1.2 Password change schedules will be established and communicated to password holders at timely intervals.

- Already addressed in the USNH Password Policy

5.7.1.3 Employee-specific passwords shall be treated as sensitive, confidential information and shall not be shared. Employee-specific passwords also shall not be stored on-line or written down unless adequately secured from unauthorized viewing.

- Already addressed in the USNH Password Policy

5.7.1.4 Authorized users of computer systems will take reasonable and appropriate measures to prevent access to systems by unauthorized persons.

- Already addressed in the USNH Password Policy

5.7.1.5 All data on computers or electronic storage devices (including but not limited to desktop, laptop, server, or handheld devices) shall be wiped clean of files and data prior to transfer or surplus.

- **NP** = Section 5.12.7
- **ST** = Information Technology Resource Secure Disposal Standard (future)

5.7.1.6 Social Security Number (SSN) is a particularly sensitive data item for all constituents. Whenever the SSN is utilized and/or displayed, the following shall apply to mitigate its exposure to unauthorized access.

- **NP** = Section 5.3
- **ST** =
  - Restricted Information Handling Standard
  - Data Administration and Management Standard (future)

5.7.1.6.1 A SSN shall not be sent via e-mail unless encrypted or masked for all but the last four (or fewer) digits of the number.

- **ST** = Restricted Information Handling Standard

5.7.1.6.2 Shared electronic and paper reports shall have all but the last four (or fewer) digits of the SSN masked. In the limited cases where SSN is required for regulatory compliance related to employment, payroll processing, provision of benefits, and tax reporting, access to the information shall be limited to those with need to know.

- **ST** =
  - Restricted Information Handling Standard
  - Data Administration and Management Standard (future)

5.7.1.6.3 Paper and electronic documents containing a SSN shall be disposed of in a secure fashion.

- **ST** = Restricted Information Handling Standard

5.7.1.6.4 Personal information which links a SSN with a person shall not be publicly displayed.

- **ST** =
  - Restricted Information Handling Standard
  - Data Administration and Management Standard (future)

5.7.1.7 Access to systems and sensitive data from outside the USNH managed environment (for example, from employee homes or during travel) will meet the same level of secure access as is provided in the USNH-managed environment.

- **NP** = Section 5.8.9
- **ST** = Remote Access and VPN Standard (future)

5.7.1.8 The Chief Information Officer at each USNH institution will establish standards and interpret this policy to assure that it is implemented in a manner consistent with the technologies at each institution.

- Changed to reflect Organizational Changes
- **NP** = Sections 5.2.2 and 5.2.3
- **ST** = Cybersecurity Roles & Responsibilities Standard (future)

5.7.2 Control Access to Systems. Access to systems will be limited to staff who have a need to access them as determined by job responsibilities.

- **NP** = Section 5.8
- **ST** =
  - Access Management Standard
  - Privileged Access Management Standard

5.8 User Awareness & Training

5.8.1 Reducing Risks of User Error, Theft, Fraud or Misuse of Facilities. USNH institutions and providers of USNH IT resources will institute measures to reduce risks of user error, theft, fraud or misuse of IT resources, by providing appropriate user information and training.

5.8.2 Educating Users about Information Technology Security Threats and Concerns. USNH and its member institutions will communicate to all constituents their responsibility for protecting the technology environment, and provide the information necessary to help them protect IT resources against threats.

- **NP** = Section 5.7
- **ST** = Cybersecurity Awareness & Training Standard

5.9 Compliance

5.9.1 Compliance with federal, state and local laws, USNH and institutional policies, and contractual obligations. The use and operation of USNH IT resources will comply with federal, state and local laws, USNH and institutional policies, and contractual obligations. USNH GLBA Information Security Program

- **NP** = Section 5.9, 5.3
  - Also covered in the new USNH Acceptable Use Policy
- **ST** =
  - Protected (or FERPA) Information Handling Standard
  - Restricted Information Handling Standard
  - Confidential Information Handling Standard
  - Cybersecurity Awareness and Training Standard
  - Data Administration and Management Standard (future)

5.9.1.1 The USNH Information Security Committee (ISC) oversees and coordinates the USNH Gramm-Leach-Bliley Act Information Security Program to ensure the protection of customers' nonpublic financial information, including information obtained by USNH in connection with a financial service provided to a student, employee or other third party.

- Changed to reflect organizational changes
- **NP** = Section 5.9
- **ST** =
  - Cybersecurity Awareness and Training Standard
  - Restricted Information Handling Standard
  - Revised USNH GLBA Information Security Program document

5.9.1.2 The USNH Information Security Committee (ISC) is responsible for developing, implementing and updating the USNH Identity Theft Prevention Program, adopted by the USNH Board of Trustees pursuant to the Federal Trade Commission's (FTC) Red Flags Rule. The ISC's responsibilities include promoting policies for protecting personally identifiable information; ensuring appropriate training of USNH staff on the Program and related policies; reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft; determining which steps of prevention and mitigation should be taken in particular circumstances; and considering periodic changes to the Program.

- Changed to reflect organizational changes
- **NP** = Section 5.9
- **ST** =
  - Cybersecurity Awareness and Training Standard
  - Restricted Information Handling Standard
  - Revised USNH GLBA Information Security Program document

5.9.2 Providing information concerning laws, policies and contractual obligations. All USNH institutions, providers and managers of USNH IT resources will institute procedures to inform users and administrators of IT resources about applicable laws, policies and contractual obligations. USNH GLBA Information Security Program

- **NP** = Section 5.9
- **ST** =
  - Cybersecurity Awareness and Training Standard
  - Restricted Information Handling Standard
  - Revised USNH GLBA Information Security Program document

5.9.3 Procedures for adjudicating security violations. Violations of this security policy constitute unacceptable use of IT resources and may violate other USNH policies and/or state and federal law. Suspected or known violations should be reported to the IT Security Officer at USNH or member institutions.

- **NP** = Section 6

5.9.4 Performing a Security Audit Process. All USNH institutions, providers and managers of USNH IT resources will periodically conduct an audit of security of IT resources.

- **NP** = Section 5.5
- **ST** =
  - Cybersecurity Risk Management Standard
  - Cybersecurity Risk Acceptance Standard
  - Security Categorization Standard
  - Vendor Cloud Service Security Standard
  - Security Assessment and Testing Standard (future)

5.10 Asset Classification & Control

5.10.1 Maintaining Appropriate Information Technology Inventory Controls. All USNH institutions, providers, managers and users of USNH IT resources will develop and maintain a comprehensive inventory of critical information assets.

- **NP** = Section 5.12.5
- **ST** =
  - Security Categorization Standard
  - Information Technology Resource Inventory Management Standard (future)

5.10.2 Inventories of assets help ensure that effective asset protection takes place, and may also be required for other business purposes, such as health and safety, insurance, or financial (asset management) reasons. The process of compiling an inventory of assets is an important aspect of risk management. An organization needs to be able to identify its assets and the relative value and importance of these assets. Based on the information an organization can then provide levels of protection commensurate with the value and importance of the assets. An *inventory should be drawn up and maintained of the important assets associated with each information system. Each asset should be clearly identified and its ownership and security classification agreed [upon] and documented together with its current location.*

- **NP** = 5.5.4, 5.12.5
- **ST** =
    - Security Categorization Standard
    - Information Technology Resource Inventory Management Standard (future)

5.10.3 Safeguarding Information Sensitivity. All USNH institutions, providers, managers and users of USNH IT resources will establish methods to identify, classify, and where necessary, restrict access to institutional data so as to recognize sensitivity, protect confidentiality or safeguard privacy as required by law, institutional policy or ethical considerations.

- NP = Section 5.3, 5.5, 5.7, 5.8. 5.9
    - Also revised USNH Information Classification Policy
- **ST** =
    - Access Management Standard
    - Access to Password Protected Information Standard
    - Confidential Information Handling Standard
    - Cybersecurity Awareness and Training Standard
    - Privileged Access Management Standard
    - Protected (or FERPA) Information Handling Standard
    - Restricted Information Handling Standard
    - Security Categorization Standard
    - Data Administration and Management Standard (future)