University System of New Hampshire

USNH CYBERSECURITY POLICY
OVERVIEW AND MAPPING

OVERVIEW

The new USNH Cybersecurity Policy consolidates existing policy provisions from multiple USNH and institution level policies and expands upon what already exists to establish a current, comprehensive, USNH-wide Policy that covers all aspects of Cybersecurity.

MAPPING TO CURRENT POLICIES

For the most part, the new USNH Cybersecurity Policy does not fundamentally change the intent of the mapped provisions in the existing policies, but focuses on:

- Updating language to reflect current terminology and concepts
- Adjusting responsibilities to address organizational changes
- Using consistent terminology across all Cybersecurity Policies & Standards
- Breaking vague or general provisions into explicit Policy requirements
- Ensuring the entire Policy is written at the appropriate level of detail and moving implementation or compliance details to the related Standards, where they belong
- Removing provisions that are outside the purview of Enterprise Technology & Services

New sections that represent material changes to the intent of the existing policies are outlined later in this document.

The following existing policies will be replaced in full by the new USNH Cybersecurity Policy. A complete mapping of each impacted policy's provisions to the new Policy is provided below.

- USNH Information Technology Security Policy
- UNH – Privacy and Security of Technological Resources Policy
- KSC - IT Security: Federal, State or Local Laws 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)

UNH – Privacy and Security of Technological Resources Policy Mapping

Current Policy: https://www.usnh.edu/policy/unh/vi-property-policies/f-operation-and-maintenance-property#4

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 or other USNH Policy as noted
- **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

4.1 Purpose. This policy informs users of technological resources about certain privacy and security issues related to their use in compliance with the related University System policy (USY VI.F.4).

- **NP** = Section 1

4.2 Scope. This policy applies to access and use of technological resources by faculty, staff, administrators, students and any other person whether inside or outside the academic community. For purposes of this policy the term "technological resources" shall include, but not be limited to, telephones, voice mail applications, desktop computers, computer networks and electronic mail applications, which are owned or operated by UNH. The term shall also include non-institutional technological resources used in the performance of official duties by faculty, staff, or administrators, but only to the extent of such use.

- **NP** = Sections 3 and 9

4.3 Privacy and Security Issues. Users of UNH technological resources should keep the following considerations in mind as they decide how to use those resources:

4.3.1 Although UNH will endeavor to maintain appropriate security mechanisms to prevent unauthorized access of records resident on technological resources, due to the nature of the resources, there is no way to guarantee the privacy of such records.

- **NP** = This is addressed in the new USNH Acceptable Use Policy

4.3.2 Using the delete function on a technological resource application may delete only one record of the address of the record and not the record itself -- "deleted" records may remain resident on the resource for an indefinite period of time.

- Removed, this level of detail/language is not really appropriate for a Policy/Standard, if the intent is to tell community members not to delete records or to provide guidance on when and how to delete records, that will be addressed in the Information Handling Standards

4.3.3 Electronic records can be very easily copied and disseminated. As a result, electronic communications can be redistributed to an audience much broader than the original author may have intended.

- Removed, this level of detail/language is not really appropriate for a Policy/Standard, it reads more like a training tip than a statement of Policy.

4.3.4 Like all records, electronic records are subject to the possibility of involuntary disclosure. For example, by legal process (i.e. subpoena or court order) or, in certain cases, under the New Hampshire Right-to-Know law.

- **NP** = 5.3.7, also covered more specifically in the USNH Acceptable Use Policy
- **ST** = Access to Password Protected Information Standard

4.3.5 Under University System policy, all records resident on UNH technological resources are owned by UNH (although the copyright and other intellectual property rights may or may not be owned by UNH) (see USY VI.F.4) and may be accessed, copied, or deleted by appropriate UNH officials under the process established in subsection 4.4 below.

- **NP** = 5.1.2 also covered in more detail in the USNH Acceptable Use Policy

4.4 Institutional Access to Records. Under the circumstances and utilizing the process set forth below appropriate UNH officials can gain access to, copy and delete records resident on technological resources owned or operated by UNH.

4.4.1 Where there exists a legitimate official need to access, copy, or delete a record resident on a technological resource owned or operated by UNH, the UNH employee having such a need

shall make a written application to one of the Vice Presidents (Academic Affairs, Finance and Administration, Student Affairs, or Research and Public Service), describing the records sought and setting forth the legitimate official need(s) sufficient to justify the request. The Vice President shall review the application, make any such further inquiry as he or she deems appropriate, determine whether there is a sufficient legitimate official need, and inform the applicant of the decision in writing. Unless the Vice President determines it would be impractical or would defeat the institutional justification to do so, the author of the record and the holder of the account in which the record resides shall be notified of a decision to allow access to, or copying, or deletion of, a record.

4.4.2 In cases where the Vice President grants the application, the author of the record or the holder of the account in which the record resides may appeal the decision to the President. Any such appeal must be in writing and submitted to the President within 48 hours of the decision. The President shall review the appeal, make any further inquiry as he or she deems appropriate, determine whether there is a sufficient legitimate official need, and inform the author or account holder of the decision in writing. The President's decision shall be final.

4.4.3 UNH technological resource system managers may maintain, control, monitor, and investigate such standard log files as may be useful for making a technological resource operate efficiently and securely. Information contained in such system log files shall be held in a confidential manner and, subject to the dictates of this policy, shall be used only for purposes of tuning systems and networks, obtaining generic and routine statistics about a system or network or for security access.

- **NP** = 5.3.7
- **ST** = Access to Password Protected Information Standard

4.5 University Identifier Policy

4.5.1 Introduction

4.5.1.1 The creation of, and compliance with this policy will help protect the privacy of students, faculty, and staff at the University of New Hampshire (UNH) by minimizing the use of Social Security Numbers (SSNs) as the primary means of identification, by limiting access to and visibility of the SSN when the use of SSNs is necessary, providing guidance for handling the non-SSN university identifier and establishing protection requirements for other legally protected personally identifiable information (PII).

- **NP** = 5.3
  - Also addressed in the new USNH Information Classification Policy (replaces the existing USNH Data Classification Policy)
- **ST** = RESTRICTED Information Handling Standard

4.5.2 Scope

4.5.2.1 This policy applies to all UNH persons, such as every student, faculty, staff member, and anyone else handling SSNs or other legally protected personally identifiable information (PII).

- **NP** = Sections 3 and 4

4.5.2.1.1 Exceptions to this policy shall be granted only by authorized University authorities, which shall be at a minimum the appropriate Vice President or higher (e.g. VP of Human Resources or VP of Student Affairs), the UNH Information Technology Security Officer, and the data owner or steward (Registrar for student SSNs, HR of employee SSNs, etc.)

- **NP** = Section 7
- **ST** = Cybersecurity Exception Standard

4.5.2.2 Authorized personnel in this policy consist of those University employees who have received approval for data access by the appropriate data steward. Authorized personnel may include non-university persons employed by service providers that receive approval for data access by the appropriate data steward, were explicitly cleared through the standardized university security review process and for which the university has a current contract in place with the appropriate security provisions documented. Authorization shall be managed by the data stewards.

- **NP** = 5.3.4, 5.3.8, and 5.13
- **ST** = Vendor Cloud Service Security Standard

4.5.2.3 Approved processes will be those that are approved by the appropriate data steward, university CIO's office and appropriate Vice President.

- NP = Section 7
  - All exceptions to Cybersecurity Policies and Standards will use the USNH Cybersecurity Exception process which is detailed in the USNH Cybersecurity Exception Standard.
- **ST** = Cybersecurity Exception Standard

4.5.3 Collection and Management

4.5.3.1 SSNs will be collected, shared and or used only where legally required or as authorized in UNH VI.F.4.5.2.1.1.

4.5.3.2 SSN values shall be collected in a confidential manner so that unauthorized persons cannot view or hear the SSN during the collection.

4.5.3.3 Other legally protected personally identifiable information (PII), such as but not limited to credit card numbers, account information, and combination of PII referenced

in the state of NH privacy protection and breach reporting statutes shall be handled through approved processes.

- **NP** = 5.3
- **ST** =
  - Public/Sensitive Information Handling Standard
  - Protected Information Handling Standard
  - Restricted Information Handling Standard
  - Confidential Information Handling Standard

4.5.4 Storage and Access

4.5.4.1 SSNs at rest shall be stored on centrally-managed, secure servers designed and approved for such use and conforming to accepted and appropriate industry security standards.

4.5.4.1.1 Servers used for this purpose will comply with the principles documented in the IT Server Protection Policy.

4.5.4.1.2 SSNs stored at rest should be encrypted. If they are not encrypted, administrators of the stored services should apply compensating security measures and seek the next reasonable opportunity to enable encryption at rest.

- **NP** = 5.3
- **ST** =
  - Restricted Information Handling Standard
  - Server Security and Management Standard (future)

4.5.4.2 SSNs and other legally protected PII will be stored in a manner that limits access to authorized personnel.

- **NP** = 5.3, specifically 5.3.3
- **ST** =
  - Protected Information Handling Standard
  - Restricted Information Handling Standard
  - Confidential Information Handling Standard

4.5.4.3 SSNs and other legally protected PII will not be stored on personal computers and other personal devices.

- **NP** = 5.3, specifically 5.3.3
- **ST** =
  - Protected Information Handling Standard
  - Restricted Information Handling Standard
  - Confidential Information Handling Standard

- Endpoint Management Standard

4.5.4.4 Any remaining non-electronic legally protected PII, such as but not limited to printed reports, shall be protected from non-authorized access.

- **NP** = 5.3, specifically 5.3.6
- **ST** =
  - Protected Information Handling Standard
  - Restricted Information Handling Standard
  - Confidential Information Handling Standard

4.5.4.5 Legally protected PII shall not be shared through insecure mechanisms, such as electronic mail in clear text form. Where secure methods for SSN transport are not available, solutions will be developed with urgency. When secure methods are not available, as confirmed by authorities in UNH VI.F.4.5.2.1.1, SSNs will be encrypted when transmitted electronically and/or limited to the last four digits.

- **NP** = 5.3, specifically 5.3.3
- **ST** =
  - Protected Information Handling Standard
  - Restricted Information Handling Standard
  - Confidential Information Handling Standard
  - Endpoint Management Standard

4.5.5 Use

4.5.5.1 If a business need requires the displaying of SSNs, SSNs will be masked and/or limited to the last four digits.

- **NP** = 5.3, specifically 5.3.3
- **ST** = Restricted Information Handling Standard

4.5.5.2 Use of UNH information classified as sensitive or restricted per the USNH Data Classification Policy (USY VI.F.6) in any third-party platform, application, or system hosted outside of the UNH computing environment requires satisfactory completion of a UNH Vendor Security Assessment Review.

- **NP** = 5.3.8, and 5.13
- **ST** = Vendor Cloud Service Security Standard

4.5.5.3 University departments using legally protected PII on University equipment within the department's administration shall contact the UNH Information Technology Security Office and conduct a review of security on a periodic basis.

- **NP** = 5.5 and 5.9
- **ST** = Cybersecurity Risk Management Standard

4.5.6 Use of non-SSN ID number

4.5.6.1 Student ID numbers will not be directory information as defined by UNH in relation to FERPA.

- **NP** = 5.3, 5.9
- **ST** =
  - Public/Sensitive Information Handling Standard
  - Protected Information Handling Standard

4.5.6.2 The University ID (a non-masked number) will be shared among authorized personnel.

4.5.6.3 University ID numbers, which may be visible to non-authorized personnel, must be masked to the last 4 digits.

- **NP** = 5.3
- **ST** = Public/Sensitive Information Handling Standard

4.5.6.4 University ID numbers may not be used as passwords for authentication purposes.

- **NP** = Covered by the USNH Password Policy
- **ST** =
  - Public/Sensitive Information Handling Standard
  - Identity Management Standard
  - Password Management Standard

4.5.7 Compromise

4.5.7.1 Compromise of SSNs or other legally protected PII includes any unauthorized viewing, recording, copying, destruction, modification, or creation thereof.

4.5.7.2 Any unauthorized access to or exposure of legally protected PII, as well as any known condition that may result in such unauthorized access or exposure will be reported to UNH Information Technology Security Office and the appropriate data steward immediately.

- **NP** = 5.14
- **ST** =
  - Protected Information Handling Standard
  - Restricted Information Handling Standard
  - Confidential Information Handling Standard
  - USNH Cybersecurity Incident Response Plan

4.6 Changing and Terminating Accounts.1 Permissions to access university information technology resources will be changed promptly and appropriately when the legitimate and approved business need

changes, and accounts will be disabled or terminated immediately when they are no longer needed for legitimate and approved business needs.

4.6.1 Permissions for access to university information technology resources will be granted based on legitimate and approved business needs under the guidance from data stewards. Where approval criteria is not established, a minimum of VP and CIO approval is required.

4.6.2 Supervisors will submit a change form to IT when an employee's responsibilities or employment status change in a manner that also changes their legitimate business need to access IT Systems.

4.6.3 UNH IT will monitor job status as documented in Banner HR.

4.6.4 UNH Human Resources will notify UNH Information Technology when it becomes aware of non-routine changes in employment such as leave of absence, termination or administrative leave, and will monitor for planned reduction in force (RIF) through periodic reports and notify IT of such planned RIFs.

4.6.5 When notified, IT will contact the appropriate supervisor to determine the disposition of the employee's access to IT systems. Information technology will maintain procedures to respond and modify access rights, and/or disable/terminate accounts without delay. Accounts and access rights for employees who are relieved of their duties, fired or whose employment is changed or modified under similar adverse or unexpected conditions will be disabled or terminated immediately.

- **NP** = 5.8
- **ST** =
  - Access Management Standard
  - Privileged Access Management Standard
  - Account Management Standard (future)

4.6.6 Situations that are not covered by this policy or where there is question about whether an employee's account or access rights should be changed or terminated will be brought to the attention of the UNH Information Security Officer for guidance.

- **NP** = 5.1.4

KSC - IT Security: Federal, State or Local Laws Mapping

Current Policy: https://www.keene.edu/administration/policy/detail/it-security-federal-state-or-local-laws/

The IT Group will cooperate fully, upon the advice of the College legal counsel, with any local, state or federal officials investigating an alleged crime committed by an individual using Keene State College information technology resources.

- **NP** = 5.3.7, 5.9.1, primarily covered in the new USNH Acceptable Use Policy
- **ST** = Access to Password Protected Information Standard

All existing federal, state, or local laws apply to Keene State College computer and network use. Laws relating to privacy and information technology have become complex. There is no single, comprehensive set of computer use and/or network use laws but there are a few laws specifically applicable to college or university computer use. The Educause Computer and Network Security Task Force published IT Security for Higher Education: A Legal Perspective (The excerpts below were extracted directly from the EDUCAUSE/Internet2 Computer and Network Security Task Force web site) and identified the following laws specifically pertinent to colleges and universities:

- **NP** = 5.9

Family Education Rights and Privacy Act (FERPA)

FERPA is the keystone federal privacy law for educational institutions. FERPA generally imposes a cloak of confidentiality around student educational records, prohibiting institutions from disclosing "personally identifiable education information," such as grades or financial aid information, without the student's written permission. FERPA also grants to students the right to request and review their educational records and to make corrections to those records. The law applies with equal force to electronic records as it does to those stored in file drawers. While violations of FERPA do not give rise to private rights of action, the U.S. Secretary of Education has established the Family Policy Compliance Office which has the power to investigate and adjudicate FERPA violations and to terminate federal funding to any school that fails to substantially comply with the law.

To learn more about FERPA, go directly to the U.S. Department of Education FERPA Web pages.

- **NP** = 5.9
- **ST** = Protected Information Handling Standard

Electronic Communications Privacy Act (ECPA)

The ECPA broadly prohibits the unauthorized use or interception by any person of the contents of any wire, oral or electronic communication. Protection of the "contents" of such communications, however, extends only to information concerning the "substance, purport, or meaning" of the communications. In other words, the ECPA likely would not protect from disclosure to third parties information such as the existence of the communication itself or the identity of the parties involved. As a result, the monitoring by institutions of students' network use or of network usage patterns, generally, would not be prohibited by the ECPA.

- *The intent of this provision is covered in the USNH Acceptable Use Policy, this type of information isn't appropriate for a Policy/Standard as it is informational not prescriptive*

Computer Fraud and Abuse Act (CFAA)

The CFAA criminalizes unauthorized access to a "protected computer" with the intent to obtain information, defraud, obtain anything of value or cause damage to the computer. A "protected computer" is defined as a computer that is used in interstate or foreign commerce or communication or by or for a financial institution or the government of the United States. In light of the "interstate or foreign commerce" criterion, the act of "hacking" into a secure web site from an out-of-state computer, which may have occurred when the Princeton admissions officer accessed Yale's "secure" web site, could be considered a CFAA violation (although both schools took pains to say that they were not seeking any civil or criminal prosecutions). The fact that both ECPA and CFAA are criminal statutes considerably raises the ante.

- *The intent of this provision is covered in the USNH Acceptable Use Policy, this type of information isn't appropriate for a Policy/Standard as it is informational not prescriptive*

USA Patriot Act

The USA PATRIOT Act, passed six weeks after September 11, 2001, grants law enforcement increased access to electronic communications and, among other things, amends FERPA, ECPA and the Foreign Intelligence Surveillance Act of 1978 (FISA), in each case making it easier for law enforcement personnel to gain access to otherwise confidential information. Perhaps most significant in the context of higher education is an amendment that potentially prohibits institutions from revealing the very existence of law enforcement investigations. Under Section 215 of the USA PATRIOT Act, which amends Sections 501 through 503 of FISA, the FBI can seize with a court order certain business records pursuant to an investigation of "international terrorism or other clandestine intelligence activities," and record-keepers are prohibited from disclosing the FBI's action to anyone "other than those persons necessary to produce the tangible [records] … ." The same goes for investigations into data banks storing information, such as information about who may have accessed certain library resources - thus, librarians may not even reveal that an inquiry has been made.

The Educause Web pages have several USA Patriot Act documents in their resource library.

- *Removed, this type of information isn't appropriate for a Policy/Standard as it is informational not prescriptive*

TEACH Act

The TEACH Act, signed into law on November 2, 2002, relaxes certain copyright restrictions to make it easier for accredited nonprofit colleges and universities to use materials in technology-mediated educational settings. But the new law carries with it obligations that have privacy and security implications: institutions that want to take advantage of the relaxed copyright restrictions must limit "to the extent technologically feasible" the transmission of such content to students who actually are enrolled in a particular course, and they must use appropriate technological means to prohibit the

unauthorized retransmission of such information. In other words, the TEACH Act may require institutions to implement technical copy protection measures and to authenticate the identity of users of electronic course content.

- Removed, this type of information isn't appropriate for a Policy/Standard as it is informational not prescriptive

Digital Millennium Copyright Act (DMCA)

The 1998 enactment of the Digital Millennium Copyright Act (DMCA) represents the most comprehensive reform of United States copyright law in a generation. The DMCA seeks to update U.S. copyright law for the digital age for ratification of the World Intellectual Property Organization (WIPO) treaties. Key among the topics included in the DMCA are provisions concerning the circumvention of copyright protection systems, fair use in a digital environment, and online service provider (OSP) liability (including details on safe harbors, damages, and "notice and takedown" practices).

Read and learn more about the DMCA.

- **NP** = 5.9
- **ST** =
    - DMCA Compliance Standard (future)

About this Policy
IT Security: Federal, State or Local Laws
Ownership: Information Technology
Last Modified: Jul 25, 2019

ADDITIONAL SECTIONS ADDED

While much of the content in the new USNH Cybersecurity Policy can be mapped to provisions in existing policies, the following new provisions were added to this Policy and represent material changes to the original intent of the existing policies

Expansion - Section 5.8 Identity and Access Management

- Added provision formalizing existing practices at all institutions around the use of a single, primary identity for each USNH community member which is supported by the Identity Management Standard
- Added provision outlining requirements for management of accounts that mirror existing practices for most enterprise level accounts (those managed by ET&S). Detailed compliance requirements that will be documented in the Account Management Standard may require that administrative, academic, and business units who are currently managing information

technology resources (e.g., vendor cloud applications) without the assistance of ET&S implement new processes and procedures. Detailed compliance requirements for the use of Non-Primary Identities (Secondary Accounts, Service Accounts, Pool Accounts) and for Sponsored and Guest Access that will be documented in those Standards may constitution material changes for some administrative, academic, and business units at one or more of the institutions.

Standards related to this section:

- Access Management Standard
- Account Management Standard
- Identity Management Standard
- Non-Primary Identity Management Standard
- Privileged Access Management Standard
- Sponsored and Guest Access Standard

New Section – 5.6 Personnel Security

This section formalizes in Policy existing practices related to ensuring employees and other community members who are given access to information technology resources have been vetted properly and understand and acknowledge specific cybersecurity responsibilities based on their role or access that is provided to them.

- 5.6.1 relates to the existing employee background check performed by HR at each institution
- 5.6.2 relates to a new ET&S Cybersecurity Agreement that will replace the existing institution specific agreements that were signed by information technology employees. This does not constitute a material change to current practices
- 5.6.3 relates to the current practices that require community members to sign or acknowledge data specific agreements (e.g., Banner HR/Fin Agreement) before being granted access to those information technology resources. The provision provides a policy basis for the existing requirement and allows for expansion to other types of access in the future, if needed. As such, it does not constitute a material change to existing practices.

Standards related to this section:

- Personnel Security Standard (future)

New Section – 5.14 Incident Management

This section formalizes in Policy existing practices for the management of cybersecurity incidents, including data breaches, predominantly at UNH and expands those practices to cover all USNH institutions. As Incident Management is completely within the purview of ET&S, this expansion does not constitute a material change for any community members outside of ET&S. Training needed to make all USNH community members aware of their responsibilities in relation to the new provisions will be provided as part of a new Cybersecurity Awareness and Training program planned for 2021.

Standards related to this section:

- Cybersecurity Incident Response Plan
- Data Breach Notification Standard

New Concept – 7 Exceptions

The new Policy introduces the concept of Policy exceptions and directs community members to the detailed requirements related to these exceptions provided in the USNH Cybersecurity Exception Standard. This concept, section, and Standard reference will be consistent across all USNH Cybersecurity Policies and the related Standards.

Standards related to this section:

- Cybersecurity Exception Standard