University System of New Hampshire

USNH CYBERSECURITY POLICY
OVERVIEW AND MAPPING

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