University System of New Hampshire

USNH INFORMATION CLASSIFICATION POLICY & RELATED STANDARDS OVERVIEW AND MAPPING

USNH

OVERVIEW

The proposed USNH Information Classification Policy replaces the existing USNH Data Classification Policy as well as existing policy provisions from institution level policies ensuring all USNH institutions and community members are using the same classification structure for institutional information.

MAPPING TO CURRENT POLICIES

The new USNH Information Classification Policy fundamentally changes the USNH Data Classification Policy, impacting all institutions, in the following ways:

- Renames from "Data" to "Information" to cover information in all forms, not just digital
- Replaces all institution level information classification and handling policies so that all institutions are following the same classification model
- Splits the "Restricted" Classification into three separate classifications, to make it easier to define clear handling requirements to meet different regulatory needs, as follows:
    - TIER 5–CONFIDENTIAL – Includes HIPAA, PCI-DSS, and some Research information based on contractual requirements
    - TIER 4-RESTRICTED: - includes SSN, FLMA, GLBA, other protected personally identifiable information, information technology information, and some Research information based on contractual requirements
    - TIER 3 – PROTECTED – includes FERPA and some Research information based on contractual requirements
- Expands to include the following new sections:
    - Information Handling Requirements
    - Clarification on Classification
    - Enforcement
    - Exceptions
    - Roles & Responsibilities

The new Policy will be supported by documented Information Handling Standards for each Tier.

University System of New Hampshire

USNH Data Classification Policy Mapping

Current Policy Link: https://www.usnh.edu/policy/usy/vi-property-policies/f-operation-and-maintenance-property#6

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

- *Italics* = existing Policy language
- **NP =** USNH Information Classification Policy (or other Policy when named)
- **ST=** USNH Cybersecurity Standard
- **Removed –** provisions that are not being carried forward at this time

6.1 *Purpose. To have appropriate protection for information, it is important to first understand what it is that needs to be protected. The purpose of the Data Classification Model is to define data categories, provide examples of each category, and provide a model that can be used by USNH institutions for classifying and protecting information. As such, this model is a foundation for policies pertaining to the protection of information.*

- **NP =** Section 1

6.2 *Scope. This model applies to every student, faculty, and staff member at USNH, as well as any members of the general community working with or for USNH.*

- **NP =** Section 2, Section 3

6.3 *Delegation of Authority. The institutions within the University System shall use this policy as a model when adopting policies regarding the minimum level of protection required for each category of data. USNH Institutions may combine one or more of the USNH data categories to meet their local needs. Institutional policies shall be consistent with applicable BOT and USY policies.*

- **NP =** Section 1

6.4 *Restricted Data*

6.4.1 *Definition: Data is Restricted if protection is legally defined and/or it is required by federal and/or state law.*

- **NP =** Section 4.3

6.4.2 Examples.

6.4.2.1 *SSNs and other personally identifiable information as defined by state of NH reporting requirements*

- **NP =** Section 4.3.4.1

6.4.2.2 *Information protected by FERPA, HIPAA, FMLA and GLB*

- **NP =**
  - FERPA – Section 4.4
  - HIPAA – Section 4.2 and specifically 4.2.3.1
  - FMLA and GLBA – Section 4.3.4.2

6.4.2.3 *Research information that requires protection by law*

- **NP =** Section 4.3.4.3

6.4.2.4 *Information protected through "Affirmative Action" and/or "disability regulation"*

- **NP =** Section 4.3.4.4

6.5 *Sensitive Data*

6.5.1 *Definition: Data is Sensitive if controlled access is required by institutional policy, by the data proprietor/steward, by contract, for ethical reasons, and/or if it is at high risk of damage or inappropriate access. It includes data which if compromised, would result in high institutional cost, harm to clients, harm to institutional reputation or unacceptable disruption of the institution to be able to meet its mission. It includes other data explicitly identified as requiring controlled access, but it does not include restricted data as defined above.*

- **NP =** Section 4.5

6.5.2 *Examples*

6.5.2.1 *Directory information as defined by the institution*

- **NP =** Section 4.5.4.1

6.5.2.2 *Information that is not restricted, and is not public*

- **NP =** Section 4.5.3

6.5.2.3 *Intellectual property*

- **NP =** Section 4.5.4.2

6.5.2.4 *Information technology infrastructure, design, security, authentication stores*

- **NP =** Section 4.3.4.5
- This is a change of classification. In the existing Policy, this information is classified as SENSITIVE, going forward it will be RESTRICTED

6.6 *Public Data*

6.6.1 *Definition: Data is Public if it is not restricted or sensitive and it is explicitly identified as public. It includes data that may be provided to anyone without any further oversight.*

- **NP =** Section 4.6

6.6.2 *Examples.*

6.6.2.1 *Contact information of employees that is approved for publication in the public directory*

- **NP =** Section 4.6.2.1

6.6.2.2 *Campus map that has been explicitly approved for public display*

- **NP =** Section 4.6.2.2

6.6.2.3 *Academic calendar that has been explicitly approved for public display*

- **NP =** Section 4.6.2.3