University System of New Hampshire

INFORMATION CLASSIFICATION POLICY

Responsible Executive/University System Officer: Chief Information Officer
Responsible Office: Enterprise Technology & Services
Approved Distribution: PUBLIC
Status: IN REVIEW

1 PURPOSE

This Policy informs all University System of New Hampshire (USNH) community members of their responsibilities related to maintaining the privacy and security of institutional information. To effectively safeguard institutional information, the USNH community must have a shared understanding of what needs to be protected and what kind of protection is required for different types of institutional information.

To facilitate that shared understanding, this Policy establishes a model for the classification of institutional information that defines each classification and provides examples of the kind of information associated with each classification. This model shall be used by all USNH institutions to classify information. The classifications defined here form the foundation for any other Policies or Standards pertaining to the protection of information.

This Policy and the related Information Handling Standards define the minimum requirements for each information classification tier.

2 SCOPE

This Policy applies to all institutional information, regardless of storage format (e.g. data/digital, paper).

3 AUDIENCE

All USNH community members should understand this policy and how it applies to the institutional information they interact with.

4 POLICY STATEMENT

All USNH and component institution information shall be protected appropriately based on the classification of that information. Institutional information shall only be shared between, and released

to, authorized parties when there is a need to know, and as necessary, to execute job-related duties.

4.1 CLASSIFICATION STRUCTURE

To facilitate the development and communication of clear Standards, processes, and procedures for implementing the appropriate security controls for each type of institutional information, the Information Classification Model is separated into distinct tiers. Each tier in the model encompasses specific types of institutional information which require the level of protection.

4.2 TIER 5 – CONFIDENTIAL INFORMATION

4.2.1 Information is Confidential if protections mandated by regulation, law, or contract include specific, stringent requirements for use, handling, and sharing of that information.

4.2.2 If compromised or exposed, Confidential Information would result in substantial institutional cost, harm to institutional reputation, and/or unacceptable disruption of the institution's ability to meet its mission.

4.2.3 Examples of Confidential Information

4.2.3.1 Electronic Personal Health Information (ePHI) or non-electronic Personal Health Information (PHI) as defined by HIPAA

4.2.3.2 Research information that contractually requires specific, stringent security or privacy controls

4.2.3.3 Information protected by PCI-DSS

4.3 TIER 4 - RESTRICTED INFORMATION

4.3.1 Information is Restricted if the information is not considered Confidential and protection is:

- legally defined
- required by federal and/or state law (excluding FERPA)
- required by contract or industry standard

4.3.2 Additionally, information can be designated as Restricted by the data steward of that information.

4.3.3 If compromised or exposed, Restricted information could result in significant institutional cost, harm to institutional reputation, and/or unacceptable disruption of the institution's ability to meet its mission.

4.3.4 Examples of Restricted Information

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

4.3.4.2 Information protected by FMLA and GLBA

4.3.4.3 Research information that requires protection by law or contract

4.3.4.4 Information protected through "Affirmative Action" and/or "disability regulation"

4.3.4.5 Information technology infrastructure, design, security, and authentication stores

4.4 TIER 3 - PROTECTED INFORMATION

4.4.1 Information is Protected if privacy controls are required by regulation or law but required protections do not rise to the level of those mandated for Restricted or Confidential Information.

4.4.2 If compromised or exposed, Protected information may result in serious institutional cost, harm to institutional reputation, and/or unacceptable disruption of the institution's ability to meet its mission.

4.4.3 Examples of Protected Information

4.4.3.1 Information protected by FERPA

4.4.3.2 Research information that requires protection by contract

4.5 TIER 2 - SENSITIVE INFORMATION

4.5.1 Information 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.

4.5.2 It includes information which, if compromised, could result in high institutional cost, harm to clients, harm to institutional reputation or unacceptable disruption of the institution's ability to meet its mission.

4.5.3 It includes other information explicitly identified as requiring controlled access, but that does not require the level of protection dictated in the higher tiers. Any institutional information that has not been designated as falling under another tier must be considered sensitive.

4.5.4 Examples of Sensitive Information

4.5.4.1 Directory information as defined by the institution or by regulation

4.5.4.2 Intellectual property

4.5.4.3 Fundraising data

4.6 TIER 1 - PUBLIC INFORMATION

4.6.1 Information is Public if it is explicitly identified as public by the data steward responsible for that information. It includes information that may be provided to anyone without any further oversight.

4.6.2 Examples of Public Information

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

4.6.2.2 Campus map that has been explicitly approved for public display

4.6.2.3 Academic calendar that has been explicitly approved for public display

4.7 INFORMATION HANDLING REQUIREMENTS

4.7.1 With the input, oversight, and approval of the institutional data stewards, Cybersecurity & Networking shall be responsible for the development, publication, and maintenance of Standards defining the required security controls for each of the defined tiers.

4.7.2 Administrative, academic, and business units shall be responsible for the development and maintenance of clear and consistent information handling procedures, aligned with those Standards, in support of operations and business processes that involve the collection, access, use, processing, storage, or transmission of institutional information.

4.8 CLARIFICATION ON CLASSIFICATION

4.8.1 While designated Data Stewards at each institution are responsible for determining the appropriate classification for the information under their stewardship, Cybersecurity & Networking is the central point of contact for questions about or clarification on the appropriate classification of a specific type of information or data element and for the required security controls for each classification.

5 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 Chief Information Officer and/or Chief Information Security Officer.

Employees who are members of institutionally recognized bargaining units are covered by the disciplinary provisions set forth in the agreement for their bargaining units.

6 EXCEPTIONS

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

7 ROLES AND RESPONSIBILITIES

7.1 ADMINISTRATIVE, ACADEMIC, AND BUSINESS UNITS:

7.1.1 Develop and maintain clear and consistent information handling procedures, aligned with the published Information Handling Standards, in support of operations and business processes that involve the collection, access, use, processing, storage, or transmission of institutional information.

7.2 CYBERSECURITY & NETWORKING:

7.2.1 Develop Standards defining required security controls for each Classification Tier defined in this Policy.

7.2.2 Provide guidance to USNH community members on the Information Classification Model.

7.3 DATA/INFORMATION STEWARDS:

7.3.1 Determine the appropriate classification for each type of information under their purview.

7.4 USNH COMMUNITY MEMBERS:

7.4.1 Understand the classification of all institutional information with which they interact.

University System of New Hampshire

8 DEFINITIONS

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

- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- CONFIDENTIAL Information
- Data/Information Steward
- Exception
- FERPA
- GLBA
- HIPAA
- Information
- Institutional Information
- PCI-DSS
- Policy
- Procedure
- PROTECTED Information
- PUBLIC Information
- RESTRICTED Information
- Security Control
- SENSITIVE Information
- Standard
- USNH Community Member

9 RELATED POLICIES AND STANDARDS

- USNH Cybersecurity Policy
- Cybersecurity Exception Standard
- Protected (or FERPA) Information Handling Standard
- Restricted and Confidential Information Handling Standard
- Sensitive and Public Information Handling Standard

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, and 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 the Admin Board in APRIL 2021)
Approved by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, 14 JUL 2020, v1 CHIEF INFORMATION OFFICER, B POIRIER, 23 OCT 2019, V0.2 USNH INFORMATION SECURITY COMMITTEE (ISC), V0.2
Reviewed by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, 14 JUL 2020, v0.3 CHIEF INFORMATION OFFICER, B POIRIER, 23 OCT 2019, V0.2 USNH INFORMAITON SECURITY COMMITTEE (ISC), 09 OCT 2019, V0.1, V0.2
Revision History:	REVISED, UPDATE TO NEW FORMAT, R BOYCE-WERNER, V0.3 REVISED, PER USNH ISC REVIEW, OCT 2019 V0.2 REVISED, R BOYCE-WERNER, OCT 2019, v.01