University System of New Hampshire

USNH INFORMATION CLASSIFICATION POLICY & RELATED STANDARDS OVERVIEW AND MAPPING

PLYMOUTH STATE UNIVERSITY

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
    - This is a change for PSU, whose existing policy is based on three classification tiers, but not the three tiers defined in the UNH Data Classification Policy.
    - PSU has been using Public, Sensitive, and Confidential so the change for PSU community member is that "Confidential" will be split into three classifications as defined in the next bullet point.
- 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.

In addition to replacing the USNH Data Classification Policy, the following institutional policy will also be replaced in full by the new USNH Information Classification Policy. A complete mapping of each of the impacted policy's provisions to the new Policy is provided below.

- PSU – Sensitive and Restricted Information Policy (FIN-002)

PSU – Sensitive and Restricted Information Policy Mapping

Current Policy: https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2018/10/FIN-ITS-002-Sensitive-and-Confidential-Information.pdf

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

Sensitive and Confidential Information / FIN-ITS-002

I. Purpose of the policy

The Sensitive and Confidential Information Policy is intended to help employees determine where information should be stored and what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed without proper authorization. Plymouth State University expects all users of its administrative data to manage, access, and utilize this data in a manner that is consistent with the University's need for security and confidentiality.

- **NP** = Section 1

II. Applicability and Authority

Applies to all employees including students acting in an employee role (e.g. student workers, grad students, etc.) and anyone granted access to university data.

- **NP** = Section 3

III. Detailed Policy Statement

University System of New Hampshire

This policy establishes three data security classifications:

- *Confidential – Specific data elements subject to more stringent security requirements (typically a legal obligation to protect).*
    - **NP** = 4.2, 4.3, 4.4
- *Sensitive – Unless otherwise classified, all information used in the conduct of university business is restricted, and not open to the general public.*
    - **NP** = 4.5
- *Public – University data that has been explicitly made available to the public, with no authentication required.*
    - **NP** = 4.6

All information at Plymouth State University should be protected.

- *Plymouth State University administrative functional areas must develop and maintain clear and consistent procedures for access to university administrative data, as appropriate.*
    - **NP** = 4.7.2

- *Such information shall only be shared between, and released to, authorized parties with a need to know and as necessary to execute job-related duties.*
    - **NP** = Section 4

- *Students exercising their rights pursuant to the PSU Student Handbook shall be considered authorized parties.*
    - **Removed, inconsistent with existing Policy at other institutions**

- *All information that is protected under local, state and federal law is confidential and is to be stored in a secure manner.*
    - **NP** = 4.2, 4.3, 4.4

- *Information not protected by law is sensitive and shared accordingly.*
    - **NP** = 4.5

- *Confidential information is only shared between and disseminated to others in the necessary performance of job duties.*
    - **NP** = Section 4

IV. Procedures

It is NOT permissible to transmit sensitive information via Email unless it is separately encrypted (e.g. Adobe Secure document Envelope).

- **ST=**
    - Public and Sensitive Information Handling Standard

- Protected Information Handling Standard
- Restricted Information Handling Standard
- Confidential Information Handling Standard

All sensitive information, data, and/or files containing sensitive data must be stored in an ITS approved secure location, which includes but is not limited to:

- *PSU/USNH Hosted Shared drive*
- *USNH SharePoint*
- *Secure database (e.g. PSU Banner, USNH Banner)*
- *Encrypted media (Encrypted drive only)*
- *Moodle*
- *Microsoft OneDrive for Business*
  - **ST=**
    - Public and Sensitive Information Handling Standard
    - Protected Information Handling Standard
    - Restricted Information Handling Standard
    - Confidential Information Handling Standard

Upon receiving an appropriately authorized written request from Human Resources, the Chief Information Officer (CIO) or Chief Security Officer (CSO) can grant access to data to support an official investigation of prohibited activity.

- *Information will be disclosed to relevant parties in order to fulfill any requirements pursuant to a subpoena issued for such a purpose, under the direction of the Chief Information Officer (CIO), any Principal Administrator or the President. Information sharing will be limited to only those personnel whose access is required, and such personnel shall respect the sensitive, confidential nature of the investigation.*
  - **ST=** Access to Password Protected Information Standard

Sensitive data includes but is not limited to:

- *Personal Identifying Information*
- *Name in combination with date of birth and/or social security number or other information that can be used to identify an individual.*
  - **NP** = 4.3, 4.4

- *Security-related information (including but not limited to card validation codes/values, full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.*
  - **NP** = 4.2

- *Any data protected by local, state and/or federal law, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA),*

- **NP** = 4.2

- *the Family Educational Rights and Privacy Act of 1974 (FERPA),*
  - **NP** = 4.4

- *the Graham-Leach-Bliley Act of 1999 (GLB).*
  - **NP** = 4.3

- *Confidential academic information such as student performance and/or research on human participants.*
  - **NP** = 4.4, 4.3, 4.2

- *Confidential administrative information such as Human Resources and/or financial records.*
  - **NP** = 4.5

V. Non-compliance

Members of the PSU community who violate this policy will be subject to disciplinary action, up to and including termination of employment and/or expulsion.

- **NP** = Section 5

VI. Definitions

Confidential *All user information that is protected under law.*

Sensitive *All information not protected under law and not deemed public*

- **NP** = Section 8

VII. Related Policies / References for More Information

- *Student Handbook http://www.plymouth.edu/office/student-life/psustudent-handbook/handbook/rights-of-students/*
- *Acceptable Use Policy*
- *Email Use Policy*

  - **NP** = Section 9

Policy Title: Sensitive and Confidential Information
Effective date: 08/11/2014
Last Revision: 10/23/2018