University System of New Hampshire

USNH INFORMATION CLASSIFICATION POLICY & RELATED STANDARDS OVERVIEW AND MAPPING

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.

DETAILED EXPLANATION OF CHANGES

There are five fundamental changes to the existing USNH Policy being proposed:

First, we are proposing that the name of the policy be changed to USNH Information Classification Policy. Using the word "information", which is inclusive of, but not limited to data aligns the naming of the policy more clearly with its intent and the way it should be implemented – classification, and the handling requirements associated with the different tiers of classification, is applicable to all institutional information, regardless of its form. Using the word "data" can imply that the policy only applies to information stored digitally.

This does not change anything demonstrably at any institution as most non-digital information is already treated as in-scope for classification.

Second, we are proposing that the tiered classification structure outlined in the new Policy be implemented and enforced at all institutions. Currently, the USNH Data Classification Model is used/implemented to varying degrees across the four institutions. Moving forward, all institutions need to adopt/implement the same Policy for information classification and the same Standards for information handling.

This represents a change for all institutions and is necessary to support the consolidation of information technology resources, services, and functions at the system-level.

Third, we are proposing that the existing classification structure, which includes three classifications, be expanded to five classification "tiers". This represents a change for all institutions and is intended to make it easier to define and enforce specific information handling requirements aligned with regulation and industry standard. The use of Tiers is intended to provide a quick visual reference to indicate the order of the classifications (e.g., Tier 5 Confidential is more stringent that Tier 3 Protected).

The proposal is to split the "RESTRICTED" classification, which currently includes any information that is protected by regulation, including FERPA, GLBA, HIPAA, and PCI-DSS, into three distinct classification tiers outlined below:

- 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

This change is being proposed to make is easier to define and document clear information handling Standards for each Tier. By moving FERPA and HIPAA/PCI to new, separate tiers, we can more closely align the security controls required to safeguard each type of information, without imposing any of the more onerous security controls, required to ensure compliance with other regulations, on the broader academic community.

This represents a demonstrable change for all institutions.

Four, to better support the USNH community in understanding their information handling responsibilities, we will be documenting Information Handling requirements for each Tier as a Cybersecurity Standard. This accomplishes two goals 1) further reinforcing consistency in data handling across all USNH institutions and 2) providing documented standards that can be used to demonstrate compliant practices for audits and assessments.

In this instance a "Standard" is a type of policy document that provides all the detailed information needed to comply with a policy or with part of a policy. For example, the Information Classification Policy requires that "All USNH and component institution information shall be protected appropriately based on the classification of that information." The individual Information Handling Standards for each classification tier define the specific security controls that equate to "protected appropriately". Each Information Handling Standard will define and document things like where information can be stored, how it can be shared, who it can be shared with, if it can be emailed, etc.

These Standards are being documented with the help of the appropriate data stewards at each institution and will become effective at the same time as the new Policy. Currently, we plan to develop the following Standards in support of this Policy:

- Public and Sensitive Information Handling Standard
- Protected Information Handling Standard
- Restricted Information Handling Standard
- Confidential Information Handling Standard

This represents a demonstrable change, to varying degrees, for all institutions as some detailed information handling requirements were defined in institutional policies.

Five, the existing Policy was expanded to include the following new sections:

1. Information Handling Requirements
2. Clarification on Classification
3. Enforcement
4. Exceptions
5. Roles & Responsibilities

This is a demonstrable change to the USNH Data Classification Policy, but does not represent a material change across existing institutional policies.

Mapping to Existing Policies

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

- USNH Data Classification Policy
- PSU – Sensitive and Confidential Information Policy (FIN-002)
- KSC – Data Access Policy

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

USNH Data Classification Policy Mapping

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

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

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

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

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

KEENE STATE COLLEGE DATA ACCESS POLICY

Current Policy: https://www.keene.edu/administration/policy/detail/data-access/

Updated: 9/1/2017

1.1 OVERVIEW

The Keene State College Data Access Policy identifies two data categories for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect the information against unauthorized access. The guiding principles for this policy are defined in the USNH Information Technology Security Policy.

- **NP** = Section 4.1
- **ST=**
    - Public and Sensitive Information Handling Standard
    - Protected Information Handling Standard
    - Restricted Information Handling Standard
    - Confidential Information Handling Standard

The Data Access Policy applies to data owned by the College. College-owned data includes all paper and electronic data prepared, supplied, used or retained by college employees, within the scope of their employment, or by agencies or affiliates of the College, under a contractual agreement. This policy covers all data created through all college operations.

- **NP** = Section 2

This policy classifies College data into two categories – restricted or unrestricted data. These categories are expected measures to protect College data and are outlined below.

- **NP** = Section 4.1

Keene State College expects all employees, partners, consultants and vendors to abide by Keene State College Data Access Policy.

- **NP** = Section 3

1.2 DATA STEWARDS

Data Stewards are charged with the role of ensuring the Data Access Policy is followed within their area of responsibility. Data Stewards are College officials with decision-making responsibilities and management oversight of functional units/departments.

- **NP** = Section 4.8.1
- **ST=**
    - Public and Sensitive Information Handling Standard
    - Protected Information Handling Standard
    - Restricted Information Handling Standard
    - Confidential Information Handling Standard
- **Glossary of Terms –** Data Steward Definition

Data Steward Responsibilities include:

- *Define restricted data for department/unit.*
- *Ensure employees within department/unit are trained on expectations for restricted data.*

- *Oversee that restricted data is limited to those with authorized roles in a 'need to know' responsibility.*
- *Perform annual internal review to confirm appropriate user access with respect to restricted data being used within unit/department. For Colleague internal review of user access, ITG will facilitate annual review with Data Stewards.*
- *Ensure operational unit/department procedures adhere to outlined access, transmission and storage protocols for restricted data.*
- *Support use of SIS/HR & Finance systems as the official "source of truth" for data and proactively support the retirement of shadow systems.*
- *Resolve stewardship issues and use of data elements that cross multiple operational units/departments.*
- *Understand laws, regulations, retention requirements that are specific to data assigned to Data Steward.*
- *Approve restricted data use requests with UNSH. Coordinate with Director Enterprise Information Systems or IT Security Manager regarding data sharing requests to share restricted data outside USNH.*
- *May assign a designee to perform the above duties.*
    - **ST=**
        - Public and Sensitive Information Handling Standard
        - Protected Information Handling Standard
        - Restricted Information Handling Standard
        - Confidential Information Handling Standard

All Employees - Expectations for Use of College Data

- *Access data only in a manner consistent with assigned responsibilities and in a manner consistent with furthering the College mission.*
- *Abide by applicable laws, regulations, standards, and policies with respect to restricted data.*
- *When there is a question regarding use of College data, seek clarification from appropriate Data Steward.*
    - **NP** =
        - Section 4.8
        - Section 7.4
        - New USNH Acceptable Use Policy
    - **ST=**
        - Public and Sensitive Information Handling Standard
        - Protected Information Handling Standard
        - Restricted Information Handling Standard
        - Confidential Information Handling Standard

University System of New Hampshire

Data Classification Protocols		
	Restricted Data	*Unrestricted Data*
Data Classifications	*Data is classified as "restricted" if data protection is required by federal or state law/institutional policy and/or data is defined as restricted by Data Steward. Examples: SSN, Credit Card data, Protected Health Information* • **NP** = Sections 4.2, 4.3, 4.4, 4.5	*Data is classified as "unrestricted" if it is not considered to be restricted. Examples: Admissions Requirements Course catalogue, directory information as defined on www.keene.edu, Institutional Report* • **NP** = Section 4.6
Access Protocol	*Data access is limited to those with authorized roles in a 'need to know'function.* • **NP** = Section 4	*At the discretion of the data steward, anyone may be given access to unrestricted information. However, care should always be taken to use Keene State College data appropriately and to respect all applicable laws. Data that is subject to copyright must only be distributed with the permission of the copyright holder.* • **NP** = Section 4.6
Storage Protocol	*Electronic restricted data is to be stored only on OneDrive or Q: drives. Electronic restricted data is not to be stored on C: drive, nor on removable media. In the rare case when SSNs are used outside of Colleague or Banner, NIST-approved encryption must be used. Restricted data in paper form should be secured via secure print at multi-function print*	*No storage requirements.*

Data Classification Protocols		
	stations and restricted data in paper form is be disposed of via KSC approved locked shred bins.	
Transmission Protocol	*NIST-approved encryption is required when transmitting restricted data. Encryption must be employed for compliance with FERPA, HIPAA, PCI-DSS and/or federal/state requirements. SSNs must be encrypted during all types of electronic transmissions. A data sharing agreement and notification to appropriate Data Steward is required when restricted data is transmitted to an external source outside of USNH.*	*No transmission requirements.*
Identifiable Human Subjects Research Protocol	*Identifiable Human Subjects research data. Any human subjects research data set containing data elements that would allow the human subjects/participants to be identified is considered restricted data, and must conform to the outlined access, transmission and storage protocols outlined within this policy.*	*De-identified Human Subjects research data are not considered restricted data for the purposes of this policy. De-identified means that the information does not identify an individual, and there is no reasonable basis to believe that the information can be used to identify an individual. Information is considered de-identified under this policy if the eighteen identifiers outlined in the HIPAA Privacy Rule are removed from the information and if no code exists enabling the linkage of the identifying information to private information or specimen. Coded Human Subjects research data are not considered restricted*

		data for the purposes of this policy, so long as the code and the data are separately stored. Coded data means that: (1) identifying information (such as name or social security number) that would enable the investigator to readily ascertain the identity of the individual to whom the private information or specimens pertain has been replaced with a number, letter, symbol, or combination thereof (i.e., the code); and (2) a key to decipher the code exists, enabling the linkage of the identifying information to the private information.
	• **NP** = Section 4.7 • **ST=** ○ Public and Sensitive Information Handling Standard ○ Protected Information Handling Standard ○ Restricted Information Handling Standard ○ Confidential Information Handling Standard	
	Keene State College Restricted Data examples, but not limited to:	
Functional Area	*Restricted Data Examples*	*Data Steward*

University System of New Hampshire

Data Classification Protocols		
Academic data	*Grades, registration data, curriculum management, degree audits, use of Student SSN*	*Registrar*

	• **NP** = Section 4.4, 4.5,4.7
	• **ST=**
	  ○ Protected Information Handling Standard
	  ○ Restricted Information Handling Standard	

Admissions data	*High school transcripts, GPA, admissions status, Use of applicant SSN*	*Director of Admissions*

	• **NP** = Section 4.3, 4.4, 4.5, 4.7
	• **ST=**
	  ○ Public and Sensitive Information Handling Standard
	  ○ Protected Information Handling Standard
	  ○ Restricted Information Handling Standard	

Campus Safety data	*Campus Safety/local Police investigations, door access data, closed circuit camera data, parking data*	*Director of Campus Safety*

	• **NP** = Section 4.3, 4.4, 4.5, 4.7
	• **ST=**
	  ○ Public and Sensitive Information Handling Standard
	  ○ Protected Information Handling Standard	

Data Classification Protocols		
	○ Restricted Information Handling Standard	
Dean of Students (Dean's file)	*Student conduct data, leave of absence, withdrawals, probation, suspension, student record review*	*Associate Vice President of Student Affairs/Dean of Students*
	• **NP** = Section 4.4, 4.7 • **ST=** ○ Protected Information Handling Standard	
Financial Aid data	*Financial aid award data, tax return data, contribution income, Use of applicant and student SSN for financial aid*	*Director of Financial Aid*
	• **NP** = Section 4.3, 4.7 • **ST=** ○ Restricted Information Handling Standard	
Finance/Business Office	*Credit card transactions, ACH numbers, banking account information*	*Director of Accounting and Banking Services*
	• **NP** = Section 4.2, 4.3, 4.7 • **ST=** ○ Restricted Information Handling Standard ○ Confidential Information Handling Standard	
Residential Life data	*Housing assignments, roommate preferences, student conduct data*	*Associate Dean of Student and Director of Residential Life*

Data Classification Protocols		

	• **NP** = Section 4.4, 4.5, 4.7
	• **ST=**
	  ○ Public and Sensitive Information Handling Standard
	  ○ Protected Information Handling Standard	

Human Resource (employee) data	*Use of employee SSN, Affirmative action, background checks, employee file and history employee disciplinary action, employee gender identity, employee leave time, employee protected health information and search committee activity*	*Director of Human Resources*

	• **NP** = Section 4.3, 4.4, 4.5, 4.7
	• **ST=**
	  ○ Public and Sensitive Information Handling Standard
	  ○ Protected Information Handling Standard
	  ○ Restricted Information Handling Standard	

Institutional Research data	*Sexual assault survey results, alumni data survey, institutional reports*	*Director of Institutional Effectiveness and Institutional Research*

	• **NP** = Section 4.3, 4.4, 4.5, 4.7
	• **ST=**
	  ○ Public and Sensitive Information Handling Standard
	  ○ Protected Information Handling Standard	

Data Classification Protocols		
	○ Restricted Information Handling Standard	
Library data	*Patron data, borrowing history, library fines*	*Dean of Mason Library*
	• **NP** = Section 4.4, 4.5, 4.7 • **ST=** ○ Public and Sensitive Information Handling Standard	
Student Accounts data	*Financial data, banking numbers, bill payment status, payment plans, deposits, use of SSN for 1098-t reporting to the IRS and in the case of a Parent Plus loan refunds*	*Director of Student Accounts*
	• **NP** = Section 4.2, 4.3, 4.7 • **ST=** ○ Restricted Information Handling Standard ○ Confidential Information Handling Standard	
Sponsored Projects and Research data	*Employee history, financial conflict of interest in research screening and disclosures*	*Director of Sponsored Projects and Research Data*
	• **NP** = Section, 4.5, 4.7 • **ST=** ○ Public and Sensitive Information Handling Standard	

Data Access Policy Training Reminders to Review:

- *Data SecURity involves you.*
- *Identity Theft is about prevention, detection, and mitigation.*
  - *College students represent a known risk for identity theft.*
  - *Employees need to pay close attention to suspicious behavior or conflicting information and ask for additional information to confirm an identity.*
  - *If you have a question, talk with your Data Steward.*
- *KSC has two types of data classifications:*
  - *Restricted (data that is governed by law, institutional policy, standards and/or data that has been defined as sensitive data by your data steward).*
  - *Unrestricted (data that is considered acceptable for general public use).*
- *What can you do to protect KSC data:*
  - *Use only the minimal level of data needed to complete an assignment.*
  - *Review business practices – rethink "just because".*
  - *When printing restricted data, use secure print.*
  - *At the end of your work day, restricted data in paper forms needs to be secured. When you are done using restricted data in paper form, paper needs to be disposed of via approved KSC locked shred bin box.*
  - *Store restricted data only on Q:Drive or OneDrive - not on removable media.*
  - *In the rare case when SSNs are used outside of Colleague or Banner, SSNs must have NIST-approved encryption.*
  - *You can instantly lock your Windows computer using Windows + L. For Macs, you can use the Ctrl-Shift-Eject key combination.*
  -
    - **NP** = Section 4.7
    - **ST=**
      - Public and Sensitive Information Handling Standard
      - Protected Information Handling Standard
      - Restricted Information Handling Standard
      - Confidential Information Handling Standard

  - *Use of complex passwords represent a critical line of defense in protecting restricted data.*
  - *Do not share your account passwords. Your passwords are your responsibility, and any activity performed while you or someone else has logged in using your account is considered your responsibility.*

- *KSC's NetID passwords:*
  - *Can be between 14-64 characters in length.*
  - *Can include any and all keyboard characters, for example: !~ % ^ + * and numbers.*
  - *Can include spaces*
  - *Cannot include your NetID.*
  - *Cannot include your first or last name.*
  - *Cannot use sequences such as: 1234 or abcd.*
  - *Cannot be similar to previously used passwords.*
  - *Cannot be similar to your current password.*

Complex Passwords are difficult to guess and are difficult to crack using widely available software. Here are some techniques for building a strong and memorable password:

- *Think in terms of using a series of unusual words to build a memorable nonsense phrase or sentence. Using uppper and lower case letters, symbols, numbers and spaces makes it even stronger.*
- *Think of a favorite music lyric and add a few of the following to make it stronger: upper and lower case letters, symbols, numbers or spaces.*

Your account/password is your responsibility, and any activity performed while you or someone else has logged in with them is considered your responsibility.

  - **NP** = USNH Password Policy

- *A method for securely storing your passwords is to create an Excel file on your OneDrive containing your passwords and then apply encryption to the Excel file.*
- *How to Encrypt a Excel file:*
  - *Click File > Info > Protect Workbook > Encrypt with Password .*
  - *Enter a password, and click OK.*
  - *In the Confirm Password dialog box, reenter the password you entered in the previous step.*
- *If you have questions, talk with your Data Steward.*
  - **REMOVED** – not a security best practice, will not be carried forward to new Policies and Standards

1.3 RELATED DOCUMENTS

Federal Regulations and Policies

1. *Family Educational Rights & Privacy Act (FERPA) 20 U.S.C. § 1232g; 34 CFR Part 99)*
2. *Freedom of Information Act (FOIA)*
3. *Health Insurance Portability & Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA)*
4. *US Patriot Act*

University System of New Hampshire

USNH Policies

1. *USNH Information Technology Security Policy*
2. *USNH Personnel Policy USY V.C.8. Performance Issues*
3. *USNH Identity Theft Prevention Program*
    - **NP** = Section 9

For questions or more information, please contact securitymanager@keene.edu or Director of EIS, (mwood6@keene.edu) .

- **NP** = Contact Information Section

1.4 ABOUT THIS POLICY

Data Access Policy
Ownership: Information Technology
Last Modified: Nov 26, 2019 – kpare@keene.edu
Categories: IT
For questions regarding this policy, please contact the policy owner.

- **NP** = Document History Section