University System of New Hampshire

USNH INFORMATION CLASSIFICATION POLICY & RELATED STANDARDS OVERVIEW AND MAPPING

KEENE STATE COLLEGE

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 KSC, whose existing policy is based on two classification tiers, Restricted and Unrestricted
    - "Restricted" under the old model will be split into four classifications, SENSITIVE, PROTECTED, RESTRICTED, and CONFIDENTIAL.
    - "Unrestricted" under the old model will become PUBLIC
- 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 and the Information Handling Standards. A complete mapping of each of the impacted policy's provisions to the new Policy is provided below.

- KSC – Data Access Policy

KEENE STATE COLLEGE DATA ACCESS POLICY

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

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

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

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*	*Data is classified as "unrestricted" if it is not considered to be restricted.*

University System of New Hampshire

Data Classification Protocols		
	defined as restricted by Data Steward. Examples: SSN, Credit Card data, Protected Health Information • **NP** = Sections 4.2, 4.3, 4.4, 4.5	*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 stations and restricted data in paper form is be disposed of via KSC approved locked shred bins.*	*No storage requirements.*

University System of New Hampshire

Data Classification Protocols		
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*
Academic data	*Grades, registration data, curriculum management, degree audits, use of Student SSN*	*Registrar*
	• **NP** = Section 4.4, 4.5,4.7	

Data Classification Protocols		

	• **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
	  ○ 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*

University System of New Hampshire

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

Data Classification Protocols		
	○ 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 ○ Restricted Information Handling Standard	

University System of New Hampshire

Data Classification Protocols		
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:

University System of New Hampshire

- *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*

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