University System of New Hampshire

KEENE IT POLICIES
HIGH LEVEL MAPPING

OVERVIEW

The Enterprise Technology & Services (ET&S) Policy & Standard initiative consolidates all existing USNH and institutional information technology policies into a new structure that is applicable across the entirety of USNH. The decision to consolidate all institutional information technology functions and resources into a single organization makes this consolidation necessary.

This document provides a high-level mapping of the existing Keene State College IT policies to the new Technology/Cybersecurity Policies & Standards.

POLICIES

Access Controls Required for KSC Computers and Data Policy

Guidelines for Communications to Students Policy

Keene State College Data Access Policy

Disposal and/or Disposition of KSC Technology Assets

Electronic Data Retention Policy

GAL Policy

IT Security: Federal, State or Local Laws Policy

Anti-virus for KSC Network for Students

NetID Password Policy

Network File Storage, Backup & Recovery

Policy for Connecting Network Devices to the KSC LAN

Policy for non-KSC Affiliated Network Users

Appendix A: USNH Acceptable Use Policy Mapping

Appendix B: Access Controls Required for KSC Computers and Data Policy Mapping

Appendix C: USNH Information Classification Policy Mapping

Appendix D: GAL Policy Mapping

Appendix E: IT Security: Federal, State or Local Laws Policy

Appendix F: Policy for non-KSC Affiliated Network Users

University System of New Hampshire

COMPUTER AND NETWORK USE POLICY (CNUP)

https://www.keene.edu/administration/policy/detail/cnup/

This policy covers the use of institutional and USNH information technology resources.

To Be Replaced By:

- USNH Acceptable Use Policy (AUP)

Detailed mapping of the provisions in this policy to the new USNH AUP are provided in *Appendix A: USNH Acceptable Use Policy Mapping*.

ACCESS CONTROLS REQUIRED FOR KSC COMPUTERS AND DATA POLICY

https://www.keene.edu/administration/policy/detail/usnhacp/

This policy is intended to increase protection for computers and data resources used in the transaction of USNH and Keene State College business and to define how KSC will comply with the USNH System Access Control Policy, which is section 5.7 of the existing USNH Information Technology Security Policy

To Be Replaced By:

- USNH Cybersecurity Policy
- USNH Information Classification Policy
- USNH Password Policy
- Confidential Information Handling Standard
- Endpoint Management Standard
- Information Technology Resource Secure Disposal Standard
- Password Management Standard
- Public/Sensitive Information Handling Standard
- Protected (FERPA) Information Handling Standard
- Remote Access and VPN Standard
- Restricted Information Handling Standard

As the provisions in this policy are split across multiple USNH policies and several USNH Standards, a detailed mapping of the provisions in this policy is provided in *Appendix B: Access Controls Required for KSC Computers and Data Policy Mapping*.

University System of New Hampshire

GUIDELINES FOR COMMUNICATIONS TO STUDENTS POLICY

https://www.keene.edu/administration/policy/detail/student-communications/

This policy is owned by Marketing & Communications and provides guidance for sending electronic communications to Keene students.

Recommendations:

- Recommend changes to this Marketing Policy when new USNH Acceptable Use Policy becomes effective to ensure references to institutional CNUP are replaced.
- Confirm technical information in this Policy with USNH ET&S Email Admins, recommend any modifications to Marketing & Communications based on that review.
- Request review of Email Security & Use Standard by KSC Marketing & Communications to ensure buy-in and alignment with KSC business practices
- Request removal of "IT" indicator from the Policy

KEENE STATE COLLEGE DATA ACCESS POLICY

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

This policy identifies two data categories for the purpose of determining who is allowed to access institutional information and what security precautions must be taken to protect institutional information against unauthorized access.

To Be Replaced By:

- USNH Information Classification Policy (replaces existing USNH Data Classification Policy)
- Public/Sensitive Information Handling Standards
- Protected Information Handling Standard
- Restricted Information Handling Standard
- Confidential Information Handling Standard

Detailed mapping of the provisions in this policy to the new USNH Information Classification Policy and proposed Standards are provided in *Appendix C: USNH Information Classification Policy Mapping*.

DISPOSAL AND/OR DISPOSITION OF KSC TECHNOLOGY ASSETS

https://www.keene.edu/administration/policy/detail/disposal-and-or-disposition-of-ksc-technology-assets/

University System of New Hampshire

This policy defines requirements for the disposal of institutionally owned information technology resources.

To Be Replaced By:

- Endpoint Management Standard
- Information Technology Resource Secure Disposal Standard

No detailed mapping required as the existing policy will be replaced in total for endpoint devices by the Endpoint Management Standard and for all other information technology resources with the Information Technology Resource Secure Disposal Standard.

ELECTRONIC DATA RETENTION POLICY

https://www.keene.edu/administration/policy/detail/data-retention-policy/

This policy defines the retention period for employee emails and documents stored in file shares and other shared storage mechanisms.

To Be Replaced By:

- Email Security and Use Standard
- Shared File Storage Standard

No detailed mapping required as the existing policy will be replaced in by the two referenced Standards.

GAL POLICY

https://www.keene.edu/administration/policy/detail/gal-policy/

This policy defines requirements for use of the Global Address List.

To Be Replaced By:

- USNH Acceptable Use Policy
- USNH Password Policy
- Email Security and Use Standard

Additionally, some content from this Policy may belong in a KSC Marketing & Communications Policy going forward. Full recommendation is available in the mapping in the appendix.

Detailed mapping of the provisions in this policy to the new Policies and Standards are provided in *Appendix D: GAL Policy Mapping*

University System of New Hampshire

IT Security: Federal, State or Local Laws Policy

https://www.keene.edu/administration/policy/detail/it-security-federal-state-or-local-laws/

This policy provides an overview of specific federal laws.

To Be Replaced By:

- USNH Cybersecurity Policy
- USNH Acceptable Use Policy
- Access to Password Protected Information Standard
- DMCA Compliance Standard
- Protected Information Handling Standard

Detailed mapping of the provisions in this policy to the new USNH AUP are provided in *Appendix E: USNH Cybersecurity Policy Mapping*.

Anti-virus for KSC Network for Students

https://www.keene.edu/administration/policy/detail/antivirus/

This policy establishes the requirement that students have anti-virus on their device before connecting to the KSC network.

To Be Replaced By:

- Endpoint Management Standard

Recommend moving recommendations for Windows and Macs to a KB article.

No detailed mapping required as the existing policy will be replaced in by the referenced Standard.

NetID Password Policy

https://www.keene.edu/administration/policy/detail/domain-password/

This policy establishes level of service, population served and the extent of qualified services available at the Repair Center.

To Be Replaced By:

- USNH Password Policy

Recommend retiring this Policy ASAP as it is already superseded by the USNH Password Policy that became effective in early 2020. Information contained in this Policy related to account claiming, resources accessed via NetID, how to change and reset passwords, and tips for creating secure passwords should be added to the KB.

Network File Storage, Backup & Recovery

https://www.keene.edu/administration/policy/detail/netstorage/

This policy establishes standards for use of the Q drive at KSC.

To Be Replaced By:

- Shared File Storage Standard

Recommend moving all non-Policy text to the KB ASAP.

No detailed mapping required as the existing policy will be replaced in by the referenced Standard.

Policy for Connecting Network Devices to the KSC LAN

https://www.keene.edu/administration/policy/detail/network-hardware/

This policy establishes ITS as being responsible for support and maintenance of the Keene LAN.

To Be Replaced By:

- USNH Cybersecurity Policy, 5.11
- USNH Acceptable Use Policy, 4.9 specifically
- Network Security and Management Standard

No detailed mapping provided as the existing policy will be replaced in by the referenced Policy provisions and Standard.

Policy for non-KSC Affiliated Network Users

https://www.keene.edu/administration/policy/detail/network-guest/

This policy outlines the requirements for granting sponsored access to KSC information technology resources.

University System of New Hampshire

To Be Replaced By:

- USNH Cybersecurity Policy
- USNH Acceptable Use Policy
- Identity Management Standard
- Sponsored/Guest Access Management Standard

Detailed mapping of the provisions in this policy to the new Policies and Standards is provided in *Appendix F: Policy for non-KSC Affiliated Network Users Mapping*.

University System of New Hampshire

APPENDIX A: USNH ACCEPTABLE USE POLICY MAPPING

Note: this information is identical to the same information provided in the stand alone KSC CNUP to USNH AUP Mapping Document.

OVERVIEW

The new USNH Acceptable Use Policy consolidates existing policy provisions from the institutional AUP/CNUPs into a single, comprehensive, USNH-wide Policy that defines acceptable use of information technology resources for all USNH institutions and community members.

MAPPING TO CURRENT POLICIES

The new USNH Acceptable Use Policy does not fundamentally change the intent of the existing institutional policies defining acceptable use of information technology resources. It pulls from all four of the institutional policies to create a comprehensive and inclusive system-wide Policy. Additionally, the new Policy contains:

- Updated language to reflect current, consistent terminology across all Cybersecurity Policies & Standards
- Adjusted responsibilities to address organizational changes
- Explicit Policy requirements in place of vague or general provisions
- Provisions written at the appropriate level of detail, moving implementation or compliance details to the related Standards, where they belong

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

- KSC – Computer and Network Use Policy (CNUP)

NEW PROVISIONS FOR KSC

As the USNH AUP is a consolidation of the existing institutional policies, there are some policy provisions that will be new for the KSC community.

- **Scope**
  - Includes community members who utilize information technology resources, existing policy only includes the resources
  - Includes personally owned endpoints as described below
  - Allows for Business Application Owners or Technology Service Owners to establish more restrictive requirements for use of specific information technology resources
- **Personally Owned Endpoints**

  - Included in the scope of the policy when used to connect to a USNH network or to perform USNH/institutional business
  - Specific requirements related to the use of personally owned endpoints are outlined
- **Policy Statements**
  - Establishes that USNH information technology resources are shared, and responsible use of those shared resources benefits the entire community
  - Establishes that community members have a responsibility to report any suspicious activity related to any USNH or component institution information technology resource
  - Identifies the following types of use as explicitly prohibited:
    - use that is illegal, disruptive, or that has the potential to negatively impact other community members or shared information technology resources
    - use that violates a USNH or component institution policy, a contractual obligation, or that does not align with the mission of USNH and its component institutions
    - Use to libel, slander, harass, defame, intimidate, or threaten anyone
    - use that is inconsistent with the University System's non-profit status
    - use for the purpose of lobbying that connotes USNH or component institution involvement in or endorsement of any political candidate or ballot initiative
    - Use that results in the display of obscene, lewd, or sexually harassing images or text in a public area or location that can be in view of others
    - Masquerading as or impersonating others or otherwise using a false identity
    - Removal of any USNH-owned or administered information technology resource from its normal location without authorization
  - Defines specific requirements related to connection to and use of USNH network resources

KSC CNUP - MAPPING

Current Policy: https://www.keene.edu/administration/policy/detail/cnup/

Annotations below indicate how each of the provisions in these policies are addressed by the new USNH Acceptable Use Policy and/or the relevant USNH Cybersecurity Standards.

- *Italics* = existing Policy language
- **NP =** USNH Acceptable Use Policy section
- **ST=** USNH Cybersecurity Standard
- **Removed –** provisions that are not being carried forward at this time

Summary

The Information Technology Group (IT Group) has developed the Computer and Network Use Policy (CNUP). This policy is designed to guide individuals in the acceptable use of computers, information systems, and networks owned by Keene State College. More importantly, it is meant as an application of best practices to ensure availability, integrity, reliability, privacy, and confidentially of college owned computers, information systems, and networks. Keene State College makes computing and network resources available to faculty, staff, students, and the general public to support the educational, scholarship, research, and service mission of the college.

- **NP** = Section 1, Section 2, and 4.1.2

Scope

The Computer and Network Use Policy establishes policy for the use of Keene State College IT and network resources by authorized individuals. It is not designed to cover any situations and circumstances beyond this scope. CNUP supplements other more specifically targeted USNH and KSC policies. The function of this policy is to supplement other USNH and KSC policies and procedures. In cases where multiple policies and/or laws apply these other documents take precedence over CNUP and CNUP will supplement and support them. IT resource owners have the authority to manage their resources to best fit their needs and have the right to establish more restrictive policies and procedures governing their use.

- **NP** = Section 2

User Responsibilities

The computing and network resources and services owned by Keene State College are limited and should be used wisely and carefully with consideration for the needs of others.

- **NP** = 4.1.1, 4.2.2

By using computers, information systems, and networks owned by Keene State College, you assume personal responsibility for acceptable use and agree to comply with this policy, other applicable KSC and USNH policies, as well as applicable federal, state, and local laws and regulations.

- **NP** = Section 3

Failure to uphold CNUP acceptable uses constitutes a violation of this policy and may be subject to disciplinary procedures applicable to students, staff, and faculty.

- **NP** = Section 5

Acceptable Uses

All users may…

- **NP** = 4.3

Use computing or network resources to support the educational, scholarship, research, and service mission of the college.

- **NP** = 4.3.3.1

Use computing or network resources for personal computing in compliance with this policy.

- **NP** = 4.7

Use only approved computing devices when connecting to the KSC network.

- **NP** = 4.8

The following unacceptable uses apply to all uses of KSC technology resources. In the constantly changing world of information technology, it is impossible to enumerate all non-acceptable uses of KSC computers, information systems, and networks. All users are expected to conduct themselves within acceptable use boundaries and may not infringe on the following examples of unacceptable use.

Unacceptable Uses

All users may not…

- **NP** = 4.4

Use IT resources without proper authorization

- **NP** = 4.4.3.1.1

Attempt to monitor, intercept, analyze or modify network traffic or transactions not specifically addressed to your computer

- **NP** = 4.4.3.6.1

Harass, defame, intimidate or threaten anyone through the use of computing or network resources for sexual harassment issues, see KSC Discrimination & Discriminatory Harassment or the USNH Complaint & Grievance Policy.

- **NP** = 4.4.3.2.1 and 4.4.3.2.2

Use computing or network resources for profit, commercial use or for the purpose of lobbying that connotes College involvement or endorsement of any political candidate or ballot initiative

- **NP** = 4.4.3.3.2 and 4.4.3.3.3

Attempt to alter or reconfigure any KSC IT resources, e.g. network infrastructure, servers

- **NP** = 4.4.3.3.4

Attempt to obtain privileges for which you are not authorized

- **NP** = 4.4.3.1.1

Attempt to access, modify and/or delete another user's files, configuration or software without the expressed agreement of the owner

- **NP** = 4.4.3.1.1

Attempt to learn another user's password(s) or personal information

- **NP** = 4.4.3.1.2

Attempt to alter or obscure your identity or your computer's identity, including but not limited to IP Address and email address, while communicating on any network

- **NP** = 4.4.3.5.1

Interfere with or disrupt computer or network accounts, services or equipment of others including but not limited to consumption of excessive IT resources, (e.g. local area network or Internet bandwidth) through the propagation of worms or viruses or the inappropriate sending of broadcast messages to large number of hosts

- **NP** = 4.4.3.4 and 4.4.3.6

Interfere with or circumvent the IT Group's responsibilities and procedures

- **NP** = 4.4.3.4 and 4.4.3.6

Consume excessive IT resources, e.g. Local Area Network or Internet Bandwidth

- **NP** = 4.4.3.6.1

Abuse email privileges - see email policy

- **NP** = 4.4.3.6.1

Download and/or share copyrighted material for which you do not have the proper authorization

- **NP** = 4.4.3.2.3

Use unauthorized computing devices when connecting to the KSC network

- **NP** = 4.8.3

Federal, State and Local Laws

All computer and network users are bound by federal, state, and local laws relating to harassment, copyright, security, and privacy relating to digital media. The IT Group will cooperate fully, upon the advice of college legal counsel, with any local, state or federal officials investigating an alleged crime committed by an individual using Keene State College information technology resources. (more…)

- **NP** = 4.4.3.2.1

Policy Enforcement

IT Group system administrators or network administrators may be required to investigate violations of this policy in order to ensure compliance. The IT Group may restrict the use of computers and networks

when faced with evidence of violation of this policy or federal, state, or local laws. The IT Group is sensitive to these issues and will remain professional and conscientious while evaluating potential violations. When violations do occur, the IT Group follows the CNUP violation process.

- **NP** = 4.10 and Section 5
- **ST** = Access to Password Protected Information Standard

IT Group Responsibilities

Beyond controlling access and protecting against unauthorized access and computer or network threats, the IT Group plays a proactive role in implementing and enforcing security or network procedures by following higher education best practices. Using hardware infrastructure and software tools, utilities and applications, the IT Group will maintain a network and computing environment enabling authorized campus users secure, reliable access to internal and external networking resources and applications.

- **NP** = Section 7

Shared and limited technology resources often require prioritization, the IT Group will assign these priorities while managing the network:

Highest: Applications and services directly associated with the college mission. Applications and services supporting the college's business functions.

Medium: Non-academic residential personal computing.

Lowest: Personal activity, not related to college business, academic and research functions.

- **ST** = Network Security Standard

The IT Group will respect and strive to ensure users' privacy and intellectual property while managing the computing and network infrastructure and information application transactions and data. The IT Group does not actively monitor network traffic or view content. However, while researching computing and/or network issues, system administrators or network administrators may need to use tools or utilities that expose content or users' internet habits. Under these circumstances, the IT Group will hold this information and knowledge in strictest confidence.

- **NP** = Section 4.5

The IT Group will not intentionally release or expose a user's personal information, e.g. name, SSN, Date of birth, etc. to anyone external to KSC or to unauthorized KSC employees. There are many laws and regulations concerning this issue. (more…..)

- **NP** = Section 4.5

At times the IT Group may need to reconfigure network and/or computing resources to mitigate situations that negatively impact access to IT resources. These actions include, but are not limited to, temporarily disabling access to an individual system, temporarily disabling access to/from a specific

segment of the LAN or modifying priorities. Though rare and short in duration, these steps are necessary to isolate problems and enable a quick resolution.

- **NP** = Section 5

To report a CNUP violation and/or suspected CNUP violations, contact the Security Manager.

- **NP** = 4.10

About this Policy
Computer and Network Use Policy (CNUP)
Ownership: Information Technology
Last Modified: Aug 10, 2018 – kpare@keene.edu
Categories: IT

- **NP** = Document History Section included in all Policies and Standards

University System of New Hampshire

APPENDIX B: ACCESS CONTROLS REQUIRED FOR KSC COMPUTERS AND DATA POLICY MAPPING

Note: this information is identical to the same information provided in the stand alone KSC Access Controls Mapping Document.

MAPPING TO CURRENT POLICIES

The provisions in the existing KSC Access Controls Required for KSC Computers and Data Policy will be replaced by the following USNH Policies and Enterprise Technology & Services Standards. A detailed mapping is provided below.

- USNH Cybersecurity Policy
- USNH Information Classification Policy
- USNH Password Policy
- Confidential Information Handling Standard
- Endpoint Management Standard
- Information Technology Resource Secure Disposal Standard
- Password Management Standard
- Public/Sensitive Information Handling Standard
- Protected (FERPA) Information Handling Standard
- Remote Access and VPN Standard
- Restricted Information Handling Standard

ACCESS CONTROLS REQUIRED FOR KSC COMPUTERS AND DATA

Current Policy: https://www.keene.edu/administration/policy/detail/usnhacp/

Annotations below indicate how each of the provisions in these policies are addressed by the new USNH Acceptable Use Policy and/or the relevant USNH Cybersecurity Standards.

- *Italics* = existing Policy language
- **NP =** USNH Policy
- **ST=** USNH Cybersecurity Standard
- **Removed –** provisions that are not being carried forward at this time

OVERVIEW

Control access to information, computer systems and resources used for the transaction of USNH business shall be protected from theft, malicious destruction, unauthorized alteration or

exposure, or other potential compromise resulting from inappropriate or negligent acts or omissions.

- **NP** = USNH Cybersecurity Policy, section 5.8

The USNH System Access Control Policy will increase protection for computers and data resources used in the transaction of USNH and Keene State College business. Given that security is a combination of policies/standards, business practices and technical controls, KSC will rely on all three to ensure our compliancy with the USNH System Access Control Policy. It is the responsibility of every KSC employee to comply and practice safe computing practices as outlined by USNH and KSC policies, standards and procedures.

- **NP** = USNH Cybersecurity Policy, section 5.8 replaces the USNH System Access Control policy provisions noted here

WORKSTATIONS

KSC employees must take responsibility and appropriate measures to prevent access by unauthorized persons. All Windows workstations will automatically lock with a black screen after 20 minutes of inactivity. All Macintosh computers will be configured to sleep mode after 20 minutes of inactivity. All lab and classroom computers will log the user out after a period of inactivity. NetID passwords will be required to unlock the screen. The only computers exempted are workstations that have been identified as public access kiosks.

To protect campus resources from theft, malicious destruction, alterations or other inappropriate or negligent acts, all KSC computers and network printers must be physically locked down. Laptop users must be particularly conscientious of locking down the computer when you are not in your office. Use the lock provided to you by the IT Group. If you cannot locate your laptop lock, please contact the HelpDesk.

- **NP** = USNH Cybersecurity Policy, section 5.10.1 and 5.12.7
- **ST** = Endpoint Management Standard

DATA SECURITY

All data on all computers or electronic storage devices (including, but not limited to desktops, laptops, servers) shall be wiped clean of files and data prior to transfer to surplus. Our current surplus vendor uses Department of Defense standards for wiping all hard drives.

- **NP** = USNH Cybersecurity Policy, section 5.3.9

- **ST** =
  - Endpoint Management Standard
  - Information Technology Resource Secure Disposal Standard

PASSWORDS

All KSC employees must log into the KSC network using their NetID. All KSC NetID passwords are set to expire every 6 months. KSC employees should create their password keeping in mind that it is important to create a strong, complex password. You should never share your passwords with anyone or have them easily accessible by having them written down on a piece of paper.

- **NP** =
  - USNH Cybersecurity Policy, section 5.8.7
  - USNH Password Policy
- **ST** =
  - Password Management Standard

PROTECTING SOCIAL SECURITY NUMBERS

Never send Social Security Numbers through email unless they are encrypted. Never print or share Social Security Numbers that have all of the numbers visible. Never publicly display Social Security Numbers. If you don't really need that information, don't use it. Always shred important information when you no longer need it or dispose of those documents through lock boxes around campus.

- **NP** =
  - USNH Cybersecurity Policy, section 5.3
  - USNH Information Classification Policy
- **ST** =
  - Public/Sensitive Information Handling Standard
  - Protected (FERPA) Information Handling Standard
  - Restricted Information Handling Standard
  - Confidential Information Handling Standard

ACCESSING KSC DATA FROM HOME OR ON THE ROAD

If you are accessing sensitive data from home or during travel, it is your responsibility to provide the same level of security that would be provided within the KSC environment. Your computer should be set to install all patches and run an automatically updated anti-virus product.# Access Controls Required for KSC Computers and Data

University System of New Hampshire

- **NP** = USNH Cybersecurity Policy, section 5.8.10
- **ST** =
    - Endpoint Management Standard
    - Remote Access and VPN Standard

ABOUT THIS POLICY

Access Control Policy for KSC Computers and Data
Ownership: Information Technology
Last Modified: Aug 19, 2019 – kpare@keene.edu
Categories: IT
For questions regarding this policy, please contact the policy owner.

- **NP** = Document History Section included in all Policies and Standards

University System of New Hampshire

APPENDIX C: USNH INFORMATION CLASSIFICATION POLICY 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.

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

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 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.*	*At the discretion of the data steward, anyone may be given access to unrestricted information. However, care*

Data Classification Protocols		
	• **NP** = Section 4	*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.*
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.*

Data Classification Protocols		
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*

Data Classification Protocols		
		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
	• **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	

Data Classification Protocols		
	○ 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*
	• **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	

University System of New Hampshire

Data Classification Protocols		
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
	  ○ 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	

Data Classification Protocols		
	○ 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	
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	

Data Classification Protocols		
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

University System of New Hampshire

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

University System of New Hampshire

APPENDIX D: GAL POLICY MAPPING

Note: this information is identical to the same information provided in the stand alone KSC GAL Policy Mapping Document.

MAPPING TO CURRENT POLICIES

The provisions in the existing KSC GAL Policy will be replaced by the following USNH Policies and Enterprise Technology & Services Standards. A detailed mapping is provided below.

- USNH Cybersecurity Policy
- USNH Password Policy
- Email Security and Use Standard

GAL POLICY

https://www.keene.edu/administration/policy/detail/gal-policy/

Annotations below indicate how each of the provisions in these policies are addressed by the new USNH Policies and/or the relevant ET&S Cybersecurity Standards.

- *Italics* = existing Policy language
- **NP =** USNH Policy
- **ST=** ET&S Cybersecurity Standard
- **Removed –** provisions that are not being carried forward at this time
- **Note –** Additional recommendation

OVERVIEW

The Global Address List, or GAL, reaches every faculty and staff member at Keene State College, and does not offer an opt-out option. The list is to be used only for sharing information that is relevant and important to the entire recipient list. The uses include:

- *Communications from the Keene State President and University System of New Hampshire Board of Trustees.*
- *Crisis/urgent announcements: natural disaster alerts, mechanical failures, weather closures or delays, crime alerts, health alerts, server maintenance, and computer virus alerts.*
- *Major policy and procedural changes that must be communicated quickly.*
- *Major news events such as naming of a new Keene State College president or vice president.*
- *Financial and administrative deadlines, e.g., budget, personnel or purchasing deadlines.*
- *Registration information and academic deadlines.*

- *Logistics announcements: construction closures; traffic routing; environmental alert notices; and security announcements.*

Authority to post messages to the GAL list is limited to select individuals in President's Office, President's Cabinet, Campus Safety, IT, Human Resources, Physical Plant, Financial Services, Health Services, and Marketing and Communications to share information related to the above subjects. If a faculty or staff member has interest in sending a message that falls outside the list of topics above, the individual must contact their Principal Administrator for approval prior to sending the message. Keene State College administration reserves the right to deny posts.

  - **ST** = Email Security and Use Standard, Mass Email Communications Section
  - **Note –** This information might be beneficial to move to a KSC Marketing & Communications Policy that defines how mass email communication tools at KSC can be used and by whom

No individual may use Keene State sub-email lists to send information to the full campus community. Misuse of the GAL or other sub-lists is a personnel matter, which will result in consequences as determined by the supervisor.

  - **ST** = Email Security and Use Standard, USNH Distribution Lists Section

Keene State College has a separate "Events" email list, which can be accessed by anyone on campus to share Keene State event-related information to faculty and staff. Recipients of this email can opt out if they wish to do so. This list is to be used only to publicize events. Guidelines for using this list are below:

- *Only events sponsored by officially recognized Keene State organizations may be publicized through broadcast e-mail.*
- *Use smaller lists for events of more limited interest.*
- *Events are to be publicized with no more than one broadcast e-mail message.*
- *All "Events" messages should include a subject line that explains the purpose of the message, e.g., "Campus Event: Poetry Reading Oct. 15"*
- *Messages should include sender's name and affiliation with Keene State.*
- *Messages should be brief, 50 words or fewer, when possible.*
- *Notice of deaths through "Events" list is restricted to Human Resources only. With the permission of the employee, HR will release the information using the "Events" list.*

  - **ST** = Email Security and Use Standard, Mass Email Communications Section
  - **Note –** This information might be beneficial to move to a KSC Marketing & Communications Policy that defines how mass email communication tools at KSC can be used and by whom

UNACCEPTABLE USE

Unacceptable use of the email system puts both the offending individual and the college at risk.

Unacceptable use of the email system includes, but is not limited to:

- *Use of email to support any commercial advertising or for-profit activity.*
- *Use of email to initiate or forward chain letters.*
- *Violations of copyright laws (unlawful distribution of copyrighted printed material, audio recordings, video recordings, or computer software).*
- *A user sharing his or her password information with another person. A user should contact the HelpDesk for a new password if there is reason to believe that the password is known by other persons.*
- *Attempts to guess or break another user's password.*
- *Use of a false email address ("spoofing").*
- *Use of email to threaten or harass others.*
- *Spamming - sending unsolicited material and/or material not related to the College's mission to a large number of individuals and/or groups.*
- *The willful introduction of computer viruses or other disruptive/destructive programs into the KSC network.*

    - **NP =** USNH Acceptable Use Policy, 4.4
    - **ST=** Email Security and Use Standard, Prohibited Use of Email Services

SECURITY

- *It is the responsibility of the individual to work with the college when it comes to security of the campus network.*
- *One level of security individuals can establish is to create passwords that are complex and difficult to break.*
- *There are many techniques and best practices available for creating passwords that provide a high level of security and should be used by everyone.*

    - **NP =** USNH Password Policy, 8.2.2

ABOUT THIS POLICY

Approved by the president and Cabinet, June 2012
GAL Policy
Ownership: Information Technology, Kim Pare
Last Modified: Oct 30, 2017 – webmaster, on behalf of Kim Pare
Categories: IT
For questions regarding this policy, please contact the policy owner.

- **NP** = Document History Section provided in each ET&S Policy and Standard

University System of New Hampshire

APPENDIX E: IT SECURITY: FEDERAL, STATE OR LOCAL LAWS POLICY

Note: this information is identical to the information provided in the stand alone USNH Cybersecurity Policy Mapping for KSC Document.

MAPPING TO CURRENT POLICIES

The provisions in the existing KSC IT Security: Federal, State or Local Laws Policy will be replaced by the following USNH Policies and Enterprise Technology & Services Standards. A detailed mapping is provided below.

- USNH Cybersecurity Policy
- USNH Acceptable Use Policy
- Access to Password Protected Information Standard
- DMCA Compliance Standard
- Protected Information Handling Standard

IT SECURITY: FEDERAL, STATE OR LOCAL LAWS POLICY

https://www.keene.edu/administration/policy/detail/it-security-federal-state-or-local-laws/

Annotations below indicate how each of the provisions in these policies are addressed by the new USNH Policies and/or the relevant ET&S Cybersecurity Standards.

- *Italics* = existing Policy language
- **NP =** USNH Policy
- **ST=** ET&S Cybersecurity Standard
- **Removed –** provisions that are not being carried forward at this time
- **Note –** Additional recommendation

The IT Group will cooperate fully, upon the advice of the College legal counsel, with any local, state or federal officials investigating an alleged crime committed by an individual using Keene State College information technology resources.

- **NP** =
  - USNH Cybersecurity Policy, Sections 5.3.7, 5.9.1
  - USNH Acceptable Use Policy
- **ST** =
  - Access to Password Protected Information Standard
  - Protected Information Handling Standard

All existing federal, state, or local laws apply to Keene State College computer and network use. Laws relating to privacy and information technology have become complex. There is no single, comprehensive set of computer use and/or network use laws but there are a few laws specifically applicable to college or university computer use. The Educause Computer and Network Security Task Force published IT Security for Higher Education: A Legal Perspective (The excerpts below were extracted directly from the EDUCAUSE/Internet2 Computer and Network Security Task Force web site) and identified the following laws specifically pertinent to colleges and universities:

- **NP** = USNH Cybersecurity Policy, Section 5.9

Family Education Rights and Privacy Act (FERPA)

FERPA is the keystone federal privacy law for educational institutions. FERPA generally imposes a cloak of confidentiality around student educational records, prohibiting institutions from disclosing "personally identifiable education information," such as grades or financial aid information, without the student's written permission. FERPA also grants to students the right to request and review their educational records and to make corrections to those records. The law applies with equal force to electronic records as it does to those stored in file drawers. While violations of FERPA do not give rise to private rights of action, the U.S. Secretary of Education has established the Family Policy Compliance Office which has the power to investigate and adjudicate FERPA violations and to terminate federal funding to any school that fails to substantially comply with the law.

To learn more about FERPA, go directly to the U.S. Department of Education FERPA Web pages.

- **NP** = USNH Cybersecurity Policy, Section 5.9
- **ST** = Protected Information Handling Standard

Electronic Communications Privacy Act (ECPA)

The ECPA broadly prohibits the unauthorized use or interception by any person of the contents of any wire, oral or electronic communication. Protection of the "contents" of such communications, however, extends only to information concerning the "substance, purport, or meaning" of the communications. In other words, the ECPA likely would not protect from disclosure to third parties information such as the existence of the communication itself or the identity of the parties involved. As a result, the monitoring by institutions of students' network use or of network usage patterns, generally, would not be prohibited by the ECPA.

- The intent of this provision is covered in the USNH Acceptable Use Policy, this type of information isn't appropriate for a Policy/Standard as it is informational not prescriptive

Computer Fraud and Abuse Act (CFAA)

The CFAA criminalizes unauthorized access to a "protected computer" with the intent to obtain information, defraud, obtain anything of value or cause damage to the computer. A "protected computer" is defined as a computer that is used in interstate or foreign commerce or communication or by or for a financial institution or the government of the United States. In light of the "interstate or

foreign commerce" criterion, the act of "hacking" into a secure web site from an out-of-state computer, which may have occurred when the Princeton admissions officer accessed Yale's "secure" web site, could be considered a CFAA violation (although both schools took pains to say that they were not seeking any civil or criminal prosecutions). The fact that both ECPA and CFAA are criminal statutes considerably raises the ante.

- *The intent of this provision is covered in the USNH Acceptable Use Policy, this type of information isn't appropriate for a Policy/Standard as it is informational not prescriptive*

USA Patriot Act

The USA PATRIOT Act, passed six weeks after September 11, 2001, grants law enforcement increased access to electronic communications and, among other things, amends FERPA, ECPA and the Foreign Intelligence Surveillance Act of 1978 (FISA), in each case making it easier for law enforcement personnel to gain access to otherwise confidential information. Perhaps most significant in the context of higher education is an amendment that potentially prohibits institutions from revealing the very existence of law enforcement investigations. Under Section 215 of the USA PATRIOT Act, which amends Sections 501 through 503 of FISA, the FBI can seize with a court order certain business records pursuant to an investigation of "international terrorism or other clandestine intelligence activities," and record-keepers are prohibited from disclosing the FBI's action to anyone "other than those persons necessary to produce the tangible [records] … ." The same goes for investigations into data banks storing information, such as information about who may have accessed certain library resources - thus, librarians may not even reveal that an inquiry has been made.

The Educause Web pages have several USA Patriot Act documents in their resource library.

- Removed, this type of information isn't appropriate for a Policy/Standard as it is informational not prescriptive

TEACH Act

The TEACH Act, signed into law on November 2, 2002, relaxes certain copyright restrictions to make it easier for accredited nonprofit colleges and universities to use materials in technology-mediated educational settings. But the new law carries with it obligations that have privacy and security implications: institutions that want to take advantage of the relaxed copyright restrictions must limit "to the extent technologically feasible" the transmission of such content to students who actually are enrolled in a particular course, and they must use appropriate technological means to prohibit the unauthorized retransmission of such information. In other words, the TEACH Act may require institutions to implement technical copy protection measures and to authenticate the identity of users of electronic course content.

- Removed, this type of information isn't appropriate for a Policy/Standard as it is informational not prescriptive

Digital Millennium Copyright Act (DMCA)

University System of New Hampshire

The 1998 enactment of the Digital Millennium Copyright Act (DMCA) represents the most comprehensive reform of United States copyright law in a generation. The DMCA seeks to update U.S. copyright law for the digital age for ratification of the World Intellectual Property Organization (WIPO) treaties. Key among the topics included in the DMCA are provisions concerning the circumvention of copyright protection systems, fair use in a digital environment, and online service provider (OSP) liability (including details on safe harbors, damages, and "notice and takedown" practices).

Read and learn more about the DMCA.

- **NP** = USNH Cybersecurity Policy, Section 5.9
- **ST** = DMCA Compliance Standard

ABOUT THIS POLICY

IT Security: Federal, State or Local Laws
Ownership: Information Technology
Last Modified: Jul 25, 2019

- **NP** = Document History Section provided in each ET&S Policy and Standard

University System of New Hampshire

APPENDIX F: POLICY FOR NON-KSC AFFILIATED NETWORK USERS

Note: this information is identical to the information provided in the stand KSC Policy for Non-KSC Affiliated Network Users Mapping Document.

MAPPING TO CURRENT POLICIES

The provisions in the existing KSC Policy for Non-KSC Affiliated Network Users will be replaced by the following USNH Policies and Enterprise Technology & Services Standards. A detailed mapping is provided below.

- USNH Cybersecurity Policy
- USNH Acceptable Use Policy
- Identity Management Standard
- Sponsored/Guest Access Management Standard

POLICY FOR NON-KSC AFFILIATED NETWORK USERS

https://www.keene.edu/administration/policy/detail/network-guest/

Annotations below indicate how each of the provisions in these policies are addressed by the new USNH Policies and/or the relevant ET&S Cybersecurity Standards.

- *Italics* = existing Policy language
- **NP =** USNH Policy
- **ST=** ET&S Cybersecurity Standard
- **Removed –** provisions that are not being carried forward at this time
- **Note –** Additional recommendation

This procedure outlines the requirements and procedures for acquiring and approving NetIDs and gaining KSC LAN access for individuals without a direct affiliation with KSC. Some examples of affiliated individuals are students, faculty, staff, employee contractors or vendors. Non affiliated users include but are not limited to, partners, spouses or family members of KSC affiliated individuals.

- **NP =** USNH Cybersecurity Policy, Section 5.8
- **ST=**
  - Identity Management Standard
  - Sponsored/Guest Access Management Standard

The following applies to these users:

- *Each non affiliated user will be assigned a unique KSC NetID in the Active Directory.*
  - **ST=** Identity Management Standard

- *The affiliated individual requests the NetID(s) with the Non KSC Affiliated Network User Request Form.*
- *Approval of the NetID(s) comes from the sponsoring KSC Department, i.e. the department with which the KSC affiliated individual is associated, e.g. NetIDs for Resident Directors' partners, spouses, and family member approvals come from ResLife. Vendors are sponsored by the hiring department.*
- *The NetIDs are active until the affiliated individual is no longer associated with KSC or the non affiliated user's relationship with the affiliated individual ends. All these NetIDs will have specific activate and deactivate dates based on the affiliate's relationships. These dates must be defined by the sponsoring KSC department, no open ended deactivate dates will be acceptable.*
- *It is the responsibility of the sponsoring KSC department to notify the IT group of any changes in the non affiliated users that affect their NetID status.*
- *The NetIDs for the non affiliated user will be renewed at times the affiliated user association with KSC is renewed/reviewed. A new Non KSC Affiliated Network User Request Form must be completed for renewing or adding new non affiliated users.*
- *The non affiliated user must read and agree to abide by the KSC Computer Network User Policy, with the exception of minor children. It is the responsibility of the parent/guardian to explain the KSC Computer Network Use Policy to minor children with KSC NetIDs. The affiliated user takes full responsibility for network/computer activity of all minor children for whom they requested a NetID.*
- *Non affiliated users using computers not managed by KSC must download a policy key and register the computer on the residential or wireless network.*
- *Non KSC affiliated users must use their assigned NetID whenever operating a computer on the KSC LAN. On multi-users systems, it is important to follow this rule.*

    - **ST=** Sponsored/Guest Access Management Standard

As outlined in the CNUP, KSC defines appropriate and acceptable use for computer and network use and takes action when network user violates the CNUP.

- **NP =** USNH Acceptable Use Policy
- **ST=** Sponsored/Guest Access Management Standard

ABOUT THIS POLICY

Policy for non-KSC Affiliated Network Users
Ownership: Information Technology
Last Modified: Sep 16, 2016 – kpare@keene.edu
Categories: IT
For questions regarding this policy, please contact the policy owner.