University System of New Hampshire

USNH ACCEPTABLE USE POLICY MAPPING

UNIVERSITY OF NEW HAMPSHIRE

MAPPING TO CURRENT UNH POLICY

The new USNH Acceptable Use Policy does not fundamentally change the intent of the existing institutional policy 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.

- UNH – Acceptable Use for Information Technology Resources Policy

NEW PROVISIONS FOR UNH

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

- **Scope**
  - Allows for Business Application Owners or Technology Service Owners to establish more restrictive requirements for use of specific information technology resources
- **Policy Statement:**
  - 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
  - Establishes that acceptable use is ethical, reflects academic integrity, and demonstrates respect for intellectual property, ownership of data, and information technology resource security.

University System of New Hampshire

- Adds the following as explicitly prohibited:
  - Use that damages the integrity of information technology resources, whether they belong to USNH or not
- Outlines additional requirements for the use of personal devices on USNH networks and/or to access USNH information technology resources

UNH - Acceptable Use for Information Technology Resources

Current Policy: https://www.usnh.edu/policy/unh/vi-property-policies/f-operation-and-maintenance-property

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

5.1 Introduction. Information technology (IT), the large and growing array of computing and electronic data communications resources, is an integral part of the fulfillment of the University of New Hampshire's teaching, research, administrative, and service roles. Members of the University community have access to these IT resources and attendant responsibilities not to misuse them. This Acceptable Use Policy (AUP) provides guidelines for the acceptable use of the University's IT resources as well as for the University's access to information to manage these resources.

- **NP** = Section 1

5.1.2 Use of information technology resources can be broadly categorized as acceptable, allowable, or prohibited.

- **Removed, unnecessary excess language, adopted simpler approach taken in other institution's existing policies**

5.1.3 Acceptable use of information technology resources is legal use consistent with the mission of the University of New Hampshire, i.e., use that furthers the University's mission of learning and teaching, research, and outreach.

- **NP** = 4.1.1 and 4.3.3.1

5.1.4 Allowable use is legal use for other purposes that do not impinge on acceptable use. The amount of allowable use will vary over time based on the capacity reserve of information technology resources available beyond Acceptable use.

- **Removed, unnecessary excess language, adopted simpler approach taken in other institution's existing policies**

5.1.5 Prohibited use is illegal use and all other use that is neither acceptable nor allowable.

- **NP** = 4.4.1

5.1.6 Most IT use parallels familiar activity in other media and formats, making existing University policies important in determining what use is appropriate. Using electronic mail ("e-mail") instead of standard written correspondence, for example, does not fundamentally alter the nature of the communication, nor does it alter the guiding policies. University policies that already govern freedom of expression, discriminatory harassment, and related matters in the context of standard written expression, govern electronic expression as well. This AUP addresses circumstances that are particular to the IT arena and is intended to augment, but not to supersede, other relevant University policies.

- **NP** = 4.1.3

5.1.7 For statements of other applicable University policies consult the University System of New Hampshire Policy Manual (OLPM); the Financial and Administrative Procedures Manual (FAP); the handbooks for faculty, PAT staff, and operating staff; the Student Rights, Rules, and Responsibilities; and policies that govern use of particular IT systems and labs.

- **Removed, unnecessary excess language, adopted simpler approach taken in other institution's existing policies**

See, too, the links to online documents in the Policy Cross-references section below.

- **NP** = Section 9

5.2 Purpose. The purpose of this AUP is to ensure an information technology infrastructure that promotes the basic missions of the University in teaching, research, administration, and service. In particular, this AUP aims to promote these goals:

5.2.1 To ensure the integrity, reliability, availability, and performance of IT resources.

5.2.2 To ensure that use of IT resources is consistent with the principles and values that govern use of other University facilities and services.

5.2.3 To ensure that IT resources are used for their intended purposes.

5.2.4 To establish processes for addressing policy violations and sanctions for those committing violations.

- **NP** = Section 1

5.3 Definitions

5.3.1 OLPM. "OLPM" is the University System of New Hampshire On-line Policy Manual, which is the master compilation of formal System-wide and Campus-wide institutional policies.

5.3.2 FAP. "FAP" refers to the Financial and Administrative Procedures Manual that applies to all the USNH Campuses, as approved by the Board of Trustees or the Financial Policies and Planning Council.

5.3.3 AUP. "AUP" is the Acceptable Use Policy for Information Technology resources and refers to this document.

5.3.4 University. The term "University" means the University of New Hampshire (UNH), both the Durham and Manchester Campuses.

5.3.5 IT Resources. Following the definition in the OLPM (USY.VI.F.4.2), "technological resources shall include, but not be limited to, telephones, voice mail applications, desktop computers, computer networks and electronic mail applications, which are owned or operated by UNH. The term shall also include non-institutional technological resources used in the performance of official duties by faculty, staff, or administrators, but only to the extent of such use."

5.3.6 User. A "user" is any person, whether authorized or not, who makes any use of any IT resource from any location. For example, users include those who access IT resources in a University computer lab, or via an electronic network. A "user's status" means their relationship with the University, i.e., student, faculty, staff, contractor, alumni/alumnae, member of public, etc.

5.3.7 Disciplinary Authority. If informal resolution does not work or the misuse is more serious, referral is made to the existing University judicial or disciplinary process, as appropriate for the status of the user. For example, students are covered by the Student Code of Conduct and Judicial Process, staff is covered by the OLPM, and faculty is covered by the collective bargaining agreement. This may include University police when the law appears to be broken.

5.3.8 Systems Authority. While the University as an entity is the legal owner or operator of all its IT Resources, it delegates oversight of particular systems to the head of a specific subdivision, department, or office of the University ("systems authority"), or to an individual faculty member, in the case of IT resources purchased with research or other funds for which they are individually responsible. For example, the systems authority for the centrally managed Exchange environment is the Assistant Vice President, Enterprise Technology Services.

5.3.9 System Administrator. Systems authorities may designate another person as a "system administrator" to manage the particular system resources for which the system authority is responsible. Systems administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular IT resources, in accordance with existing policies and procedures.

5.3.10 Computer account. A "computer account" is any access name and its associated password that is assigned to a user for access to information technology resources.

5.3.11 Specific authorization. This means documented permission provided by the applicable system administrator.

- **NP** = Section 8

5.4 Scope

5.4.1 This Policy applies to all users of IT resources, including but not limited to University students, faculty, and staff, and to the use of all IT resources. These include systems, networks, and facilities administered by UNH Information Technology (UNH IT), as well as those administered by individual schools, departments, University laboratories, and other University-based entities. This includes the general public.

5.4.2 Use of University IT resources, even when carried out on a privately owned computer that is not managed or maintained by the University, is governed by this policy.

- **NP** = Section 2 and Section 3

5.5 Acceptable Use of IT Resources. Although this policy sets forth the general boundaries of acceptable use of IT resources, students, faculty, and staff should consult their respective governing policy manuals for more detailed statements on permitted and appropriate use. This includes the University System of New Hampshire Policy Manual (OLPM); the Financial and Administrative Procedures Manual (FAP); the handbooks for faculty, PAT staff, and operating staff; the Student Rights, Rules, and Responsibilities; and specific restrictions that system administrators may place on resource use.

- **Removed, unnecessary excess language, adopted simpler approach taken in other institution's existing policies, intent is addressed in section 5 and section 9**

IT resource authorities or administrators may elect to impose stricter controls than those required by this policy. In all cases where the controls are less restrictive than those of this AUP, this AUP applies.

- **NP** = Section 2

5.5.1 IT resources may be used only for their authorized purposes, that is, to support the University's primary mission of teaching, research, and outreach (BOT.II.H.1.1). The particular purposes of any IT resources, as well as the nature and scope of authorized use and incidental personal use, may vary according to the duties and responsibilities of the user.

  - **NP** = 4.3.3.2, 4.7

5.5.2 Proper authorization. Users are entitled to access only those elements of IT Resources that are consistent with their authorization.

  - **NP** = 4.3.3.2

5.5.3 Allowable use. Incidental personal use of IT resources is allowed, such as Web browsing and personal e-mail, as long as it is consistent with this AUP and any applicable departmental work-unit policies and guidelines. The capacity of IT resources available beyond acceptable use will vary over time and so individual use will be restricted if it interferes with the University's primary mission.

- **NP** = 4.7

5.6 Prohibited Use. Prohibited use is illegal use and all other use that is neither acceptable nor allowable. The following categories of use are inappropriate and prohibited.

- **NP** = 4.4

5.6.1 Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others. Users must not interfere with, or attempt to interfere with, the normal use of IT resources by other users. Interference includes: denial of service attacks, misusing mailing lists, propagating chain letters or hoaxes, and intentional or unintentional sending of unwanted e-mail to users without specific authorization or a way to opt-out ("slamming").

- **NP** = 4.4.3.6.1

Other behaviors that cause a network traffic load or computing load that interferes with the normal and intended use of the IT resources is also prohibited.

- **NP** = 4.4.1

5.6.2 Use that is inconsistent with the University's non-profit status. The University is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters.

- **NP** = 4.4.3.3.1

As a result, commercial use of IT resources for non-University purposes is generally prohibited, except if specifically authorized and permitted under University conflict-of-interest, outside employment, and other related policies (FAP 8-006).

- **NP** = 4.4.3.3.2

System administrators are expected to develop more detailed guidance for the use of e-mail, Web pages, and other services on specific IT resources.

- **Removed, inconsistent with existing policies at other institutions, intent addressed by development of related Standards which will provide detailed guidance for use of specific resources**

5.6.3 Use of IT resources in a way that suggests University endorsement of any political candidate or ballot initiative is also prohibited. Users must refrain from using IT resources for the purpose of lobbying that connotes University involvement, except for authorized lobbying through or in consultation with the University System of New Hampshire General Counsel's Office.

- **NP** = 4.4.3.3.3

5.6.4 Harassing or threatening use. This category includes, for example, discriminatory harassment, display of offensive or sexual material in the workplace, and repeated unwelcome contacts with another.

- **NP** = 4.4.3.2 and 4.4.3.3.5

5.6.5 Use that damages the integrity of University or other IT resources. This category includes, but is not limited to, the following activities:

- **NP** = 4.4.3.4

5.6.5.1 Attempts to defeat system security. Users must not defeat or attempt to defeat any IT resources security, such as by analysis ("cracking") or guessing and applying the password of another user, or by compromising room locks or alarm systems. This provision does not prohibit, however, UNH IT or system administrators from using security-scanning programs within the scope of their systems authority.

- **NP** = 4.4.3.4.3

5.6.5.2 Unauthorized access or use. The University recognizes the importance of preserving the privacy of users and data stored in IT systems. Users must honor this principle by refraining from, or assisting, unauthorized access to IT resources. This applies to a variety of situations:

- **NP** = 4.4.3.1.1

5.6.5.2.1 For example, a non-University organization or individual may not use non-public IT resources without specific authorization.

  - **NP** = 4.4.3.1.4

5.6.5.2.2 For example, privately owned computers may be used to provide public information resources, but such computers may not host sites or services, across the University network, for non-University organizations without specific authorization.

  - **NP** = 4.6.3

5.6.5.2.3 For example, users are prohibited from accessing or attempting to access data on IT resources that they are not authorized to access.

  - **NP** = 4.4.3.1.1

5.6.5.2.4 For example, users must not make or attempt to make any deliberate, unauthorized changes to data on an IT system.

  - **NP** = 4.4.3.3.4

5.6.5.3 Networking equipment and software. Unless specifically authorized, by the network system administrator no user will connect networking equipment (routers, hubs, "sniffers," etc.)

to the campus network, nor operate network services software (routing, "sniffing," name service, multicast services, etc.) on a computer attached to the network.

- **NP** = 4.8.1

5.6.5.4 Disguised use: Users must not conceal their identity when using IT resources, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.

- **NP** = 4.4.3.5

5.6.5.5 Distributing computer hoaxes and viruses. Users must not knowingly distribute or launch hoaxes, computer viruses, worms, or other rogue programs intended to compromise IT resources.

- **NP** = 4.4.3.6.1 and 4.4.3.4.3

5.6.5.6 Removal of data or equipment. Without specific authorization by a system administrator, users must not remove any University-owned or administered IT resource equipment from its normal location.

- **NP** = 4.4.3.6.2

5.6.6 Violation of law

5.6.6.1 Illegal use of IT resources, i.e., use in violation of civil or criminal law at the federal, state, or local levels is prohibited. Examples of such uses are: promoting a pyramid scheme; distributing illegal obscenity; receiving, transmitting, or possessing child pornography; infringing copyrights; and making bomb threats.

- **NP** = 4.4.3.2

5.6.6.2 With respect to copyright infringement, users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for limited "fair use". Educational use must meet the normal fair use guidelines.

- **NP** = 4.3.3.3 and 4.4.3.2.3

5.6.7 Violation of University contracts. All use of IT resources must be consistent with the University's contractual obligations, including limitations defined in software and other licensing agreements.

- **NP** = 4.4.2

5.6.8 Violation of external data network policies. Users must observe all applicable policies of external data networks when using such networks.

- **NP** = 4.4.3.4.2

5.7 Personal Account Responsibility. Users are responsible for maintaining the security of their own accounts and passwords for access to IT resources. Accounts and passwords are normally assigned to individual users and are not to be shared with any other person without authorization by the applicable system administrator. Users are presumed to be responsible for any activity carried out under their IT system accounts or posted on their personal Web pages.

- **NP** = 4.2.2, 4.4.3.1.2, 4.4.3.1.3

5.8 Personal Identification. Upon request by a system administrator or other University authority, users must produce valid identification.

- **Removed, inconsistent with existing policies at other institutions, cannot practically be enforced/implemented, intent covered in identity verification requirements included in Identity Management Standard, Access Management Standard, and Account Management Standard**

5.9 Conditions of University Access to Resources. There are circumstances when a user's access to IT resources may be deactivated or terminated or expectations of privacy may be waived under the following special conditions.

- **NP** = 4.5 and 4.9
- **ST =** Access to Password Protected Information Standard

5.9.1 Special Conditions. The following special conditions for institutional access to IT materials, without the consent of the user, would operate under the procedural safeguards specified in UNH.VI.F.4.4.

5.9.2 Diagnosis. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT resources.

5.9.3 Required by law. When required by federal, state, or local law or administrative rules.

5.9.4 Reasonable grounds. When there are reasonable grounds to believe that a violation of law may have taken place and access and inspection or monitoring may produce evidence related to the violation.

5.9.5 Essential business. When such access to IT resources is required to carry out essential business functions of the University.

5.9.6 Health and safety. When required to preserve public health and safety.

- **NP** = 4.5
- **ST =** Access to Password Protected Information Standard

5.10 Process. Consistent with the procedures specified in the OLPM for institutional access to materials and records without the consent of the user, such access is to be logged by the system administrator for subsequent review by the appropriate Vice President (UNH.VI.F.4.4).

- **NP** = 4.5
- **ST** = Access to Password Protected Information Standard

5.10.1 User access deactivation. The University, through the appropriate system administrator, may deactivate a user's information technology privileges, even in the absence of a suspected AUP violation, when necessary to preserve the integrity of IT resources. The system administrator must notify the user in writing of any such action within 48 hours (UNH.VI.F.4.4).

- **NP** = 4.9, some requirements removed as they are inconsistent with other institution's policies and not practically enforceable

5.10.2 Security scanning systems. By attaching privately owned personal computers or other IT resources to the University's network, users consent to the University use of security scanning programs while connected to the network.

- **NP** = 4.6.2.1

5.10.3 Logs. Most IT systems routinely log user actions for a variety of reasons, including system recovery, trouble-shooting, usage reporting, and resource planning. All system administrators are expected to establish and post a description of the logging policies and procedures for the systems they manage. This may take the form of a privacy statement or a more general operational statement.

- **Removed, inconsistent with existing policies at other institutions**

5.10.4 Encrypted material. University faculty and staff, as employees, may encrypt files, documents, and messages for protection against unauthorized disclosure while in storage or in transit. However, such encryption must allow officials, when properly required and authorized, to decrypt the information (UNH.VI.F.4).

- **Removed, inconsistent with existing policies at other institutions**

5.11 Enforcement Procedures

- **NP** = Section 5

5.11.1 Complaints of Alleged Violations. An important element in the enforcement of violations of this AUP is the intent, i.e., whether a violation was carried out with knowledge and awareness of the consequences. For minor violations the expectation is to resolve the violation at the lowest level of system administration involved. System administrators are expected to apply judgment in reporting a violation to a formal judicial or disciplinary process. The AUP administrator may be consulted for interpretive advice, as described below. Seen as a simple diagram:

An individual who believes that they are harmed by an alleged violation of this policy may file a complaint in accordance with established University complaint or grievance procedures. The individual is also encouraged to report the alleged violation to the systems authority responsible and to refer the matter to University disciplinary authorities.

- **NP** = 4.10

5.11.2 Reporting Observed Violations. If an individual has observed or otherwise is aware of an alleged violation of the AUP, but has not been harmed by the alleged violation, they may report the matter to the systems authority responsible for the facility most directly involved and refer the matter to University disciplinary authorities.

- **NP** = 4.10

5.11.3 Disciplinary Procedures. When possible, the goal is to resolve issues of use and misuse informally between the user and relevant system administrator, including use of informal departmental procedures if helpful.

Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures for students, faculty, and staff, as outlined in the relevant student regulations (e.g., Student Rights, Rules, and Responsibilities), the faculty handbook, or staff handbook. Faculty or staff who are members of University-recognized bargaining units are covered by disciplinary provisions set forth in the agreement for their bargaining units. Factors to consider in an alleged incident are: its nature, the intent, extent of damage, and history of offenses, leading to a recommended action.

Systems administrators may participate in formal disciplinary proceedings as deemed appropriate by the relevant disciplinary authority. And, at the direction of the appropriate disciplinary authority, systems administrators are authorized to investigate alleged violations.

- **NP** = Section 5

5.11.4 Penalties. Users found to have violated this AUP are subject to penalties provided for in other University policies dealing with the underlying conduct. Such users may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The appropriate penalties shall be determined by the applicable disciplinary authority in consultation with the system administrator.

System administrators in violation of their authority are also subject to penalties as provided in other University policies.

- **NP** = Section 5

5.11.5 Legal Liability for Unlawful Use. In addition to University discipline, users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT resources.

- **NP** = 4.4.3.2

5.11.6 Appeals. Users found in violation of this policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the formal appeals provisions of the relevant disciplinary authority.

- **NP** = Section 5

5.12 Policy Development

5.12.1 This AUP will be periodically reviewed and modified under the direction of the Assistant Vice President for Computing and Information Services, in consultation with University committees and constituencies. This Assistant Vice President will designate an AUP administrator to assist with:

5.12.1.1 Interpretation. For questions or assistance about the interpretation of this AUP, contact the AUP administrator.

- **NP** = Contact Section

5.12.2 Review. This AUP will be reviewed for accuracy as needed, but not less than once a year, by the AUP administrator.

- **NP** = 4.11

5.13 Policy Cross-references. The following links are to related online policies and documents. There are other important policies and documents that are not yet online.

5.13.1 Digital Millennium Copyright Act

5.13.2 FAP on Charitable and Political Contributions Procedure 8-006

5.13.3 Library Records Confidentiality

5.13.4 NH RSA 638:16,17,18. State statutes on computer crime

5.13.5 OLPM on Mailing Lists and Directories (UNH.III.B)

5.13.6 OLPM on Privacy and Security of Technological Resources (UNH.VI.F.4)

5.13.7 Student Rights, Rules, and Responsibilities. See Appendix for the Family Educational Rights and Privacy Act of 1974 (FERPA), a/k/a "The Buckley Amendment."

5.13.8 UNH Primer on Copyright Law and Recommended Procedures

5.13.9 UNHINFO Privacy Statement

- **NP** = Section 9

This AUP was modeled, with permission, on the appropriate use policy at Yale University and conforms to UNH.III.E for institutional policy development, review, and approval.