University System of New Hampshire

B. Acceptable Use Policy

1. Purpose

The information technology resources provided by the University System of New Hampshire (USNH) and its component institutions support the educational, instructional, research, and administrative activities of the University System and those institutions. Use of these resources is a privilege that is extended to USNH community members. Inappropriate or improper use of these shared resources can impede or negatively impact availability for the rest of the community. As such, all community members are required to behave in a responsible, ethical, and legal manner during that use.

This policy defines acceptable use of information technology resources at USNH and its component institutions and outlines the responsibilities and obligations of community members who are granted access to or use of these resources. Specifically, this policy supports the following objectives:

- Safeguarding the confidentially, availability, integrity, and privacy of institutional information and enterprise information technology resources
- Providing a reliable information technology environment for all USNH community members
- Guaranteeing use of enterprise information technology resources is consistent with the principles and values that govern use of other USNH and component institution resources (e.g., facilities)
- Confirming that enterprise information technology resources are used for their intended purposes

2. Scope

This policy applies to anyone who utilizes USNH information technology resources, and all uses of those resources, irrespective of where the resources are being used. This includes students, faculty, staff, contractors, vendors, prior students/alumni, parents, volunteers, and external customers utilizing services provided by USNH.

For purposes of this policy only, any individual who is authorized to access or use a USNH or component institution information technology resource is considered a member of the USNH community.

This policy covers the use of all information and information technology resources owned, managed, licensed, or entrusted to USNH or one of its component institutions, regardless of who is providing those resources, how they are being provided, or how they are being accessed. Referred to throughout this policy as institutional information and USNH information technology resources, this includes, but is not limited to:

- Information technology resources administered by Enterprise Technology & Services (ET&S) or contracted vendors
- Information technology resources administered or managed by individual administrative, academic, or business units
- Institutionally owned endpoint devices
- Institutional telecommunication services including voicemail
- Personally owned endpoint devices that connect to any USNH network
- Devices, regardless of device ownership, that connect to any USNH information technology resource, including students' use of devices

Business Application Owners or Technology Service Owners have the authority to establish more restrictive requirements governing use of those resources in their care. When there are additional use restrictions for a specific information technology resource, individuals who need access to that resource shall be informed of those restrictions, and agree to abide by them, prior to access being granted.

3. Audience

This Policy applies to all USNH community members granted access to any USNH information technology resource.

4. Policy Statement

4.1 Information Technology Resources are Shared

4.1.1 USNH provides information technology resources to authorized members of the USNH community and others in support of each USNH component institution's mission and the mission of the University System.

4.1.2 To ensure access to and reliability of this shared resource, USNH and its component institutions shall safeguard the confidentiality, integrity, availability, and privacy of these information technology resources and the institutional information captured, stored,

processed, transmitted, or otherwise managed by them.

4.1.3 USNH and component institution policies that govern freedom of expression, discriminatory harassment, and related matters in the context of standard written expression, also govern electronic expression as well. This Policy addresses circumstances that are particular to information technology resources and is intended to augment, but not to supersede, other relevant USNH and component institution policies.

4.2 Community Member Rights and Responsibilities

4.2.1 Members of the USNH community shall be provided with the use of information technology resources. While accessing and using these resources, community members shall have a reasonable expectation of:

- reliable use of these shared resources
- protection from abuse and intrusion by others sharing these resources

4.2.2 Community members shall be responsible for exercising good judgment in the use of those resources including respecting the rights and privacy of others, respecting the security and integrity of the information technology resources they are given access to, and observing all relevant laws, regulations, contractual obligations, and USNH policies and standards.

4.2.3 Any suspicious activity related to enterprise or institutional accounts or information technology resources shall be reported immediately according to the Cybersecurity Incident Reporting process.

4.3 Acceptable Use

4.3.1 Acceptable Use of information technology resources is always ethical, reflects academic integrity, and shows restraint in the consumption of shared resources.

4.3.2 It demonstrates respect for intellectual property, ownership of data, information technology resource security, and freedom from intimidation and harassment.

4.3.3 The following are explicitly defined as acceptable:

4.3.3.1 Use that supports the administrative, academic, research, outreach, service, and operational mission of USNH and each of its component institutions.

4.3.3.2 Use of information technology resources for which the community member has been authorized to access and use so long as that use adheres to the intended use of those resources.

4.3.3.3 Use that protects the intellectual property of others and the rights of copyright holders of music, videos, images, texts, and other media.

4.4 Prohibited Use

4.4.1 Use of USNH information technology resources that is illegal, disruptive, or that has the potential to negatively impact other community members or shared information technology resources is prohibited.

4.4.2 Use that violates a USNH or component institution policy, a contractual obligation, or that subverts the mission of USNH, or its component institutions is prohibited.

4.4.3 Additionally, the following uses of USNH information technology resources are explicitly prohibited:

4.4.3.1 Unauthorized Use

4.4.3.1.1 Use or attempted use of any information technology resources without permission.

4.4.3.1.2 Use of another community member's credentials, even if the community member gives their permission.

4.4.3.1.3 Sharing any password associated with enterprise or component institution credentials in violation of the USNH Password Policy.

4.4.3.1.4 Allowing or enabling use of USNH information technology resources by any individual or organization that is not affiliated with USNH or one of its component institutions.

4.4.3.2 Illegal Use

4.4.3.2.1 Use of USNH information technology resources in violation of civil or criminal law at the federal, state, or local levels or in violation of any regulation.

4.4.3.2.2 Use of USNH information technology resources to libel, slander, harass, defame, intimidate, or threaten anyone.

4.4.3.2.3 Use that violates copyright laws through inappropriate reproduction or dissemination of copyrighted material.

4.4.3.3 Inappropriate Use

4.4.3.3.1 Use that is inconsistent with the University System's non-profit status.

4.4.3.3.2 Use of USNH information technology resources for profit and/or commercial use, including non-USNH or component institution business purposes.

4.4.3.3.3 Use for the purpose of lobbying that connotes USNH or component institution involvement in or endorsement of any political candidate or ballot initiative.

4.4.3.3.4 Attempting to alter or reconfigure any USNH information technology resource without proper authorization.

4.4.3.3.5 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.

4.4.3.4 Damaging Use

4.4.3.4.1 Use that damages the integrity of information technology resources, whether they belong to USNH or not.

4.4.3.4.2 Use of information technology resources to gain unauthorized access to networks or other information technology resources, whether they belong to USNH or not.

4.4.3.4.3 Use that seeks to circumvent, defeat, or attempt to defeat information technology resource security controls.

4.4.3.5 Disguised Use

4.4.3.5.1 Use that attempts to alter or obscure the identity of the community member or the identity of an endpoint or other connected device while communicating with any USNH network

4.4.3.5.2 Masquerading as or impersonating others or otherwise using a false identity without authorization, while accessing and/or utilizing USNH information technology resources.

4.4.3.6 Disruptive Use

4.4.3.6.1 Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of other community members (e.g., consumption of excessive bandwidth, distribution of malicious programs, spamming internal distribution lists).

4.4.3.6.2 Removal of any USNH-owned or administered information technology resource from its normal location without authorization.

4.5 Privacy

4.5.1 Student educational records stored on or accessible via USNH information technology resources shall only be shared and used in accordance with the Family Educational Rights and Privacy Act of 1974 (FERPA). Handling requirements for information protected by FERPA are provided in the Protected Information Handling Standard.

4.5.2 While all USNH community members shall have a reasonable expectation to a certain degree of privacy related to their use of information technology resources provided by USNH and its component institutions, there are specific circumstances under which access to information or information technology resource use for a specific community member shall be authorized for USNH officials, ET&S personnel, law enforcement, other community members, or other external parties.

4.5.3 Some of those circumstances allow for this access without the knowledge and/or consent of the impacted community member.

4.5.4 The rules governing when and how that access is granted and to whom it can be granted for allowable circumstances shall be documented in the Access to Password Protected Information Standard.

4.5.5 ET&S reserves and retains the right to access, affect, and inspect information technology resources, and the information stored within those resources, without the consent of community members, to the extent necessary to manage and administer those resources (e.g., backup and caching of information and communications, the logging of activity, monitoring of general usage patterns, and other activities necessary or convenient for the provision of service).

4.6 Use of Personally Owned Devices

4.6.1 USNH and its component institutions shall allow community members to connect personally owned devices to USNH networks and to use personally owned endpoint devices to access approved institutional information and USNH information technology resources on-campus or remotely.

4.6.2 While this is an acceptable use of USNH information technology resources, community members who choose to use personally owned devices to connect to and/or access any USNH information technology resource shall agree to the following:

4.6.2.1 Connecting to a USNH network with a personally owned endpoint or other device implies consent for USNH and its component institutions to perform security scans on that device while connected to the network.

4.6.2.2 Any personally owned device connecting to a USNH network must be registered with the appropriate component institution.

4.6.2.3 Unregistered devices may be blocked from accessing USNH networks or other information technology resources.

4.6.2.4 All personal endpoint devices connecting to USNH information technology resources must meet the requirements defined in the Endpoint Management Standard.

4.6.2.5 Personally owned endpoint devices used by USNH employees to conduct USNH or component institution business that are involved in a cybersecurity incident may be searched as part of the internal ET&S investigation or any investigation by law enforcement.

4.6.3 Although use of personally owned endpoint devices or other devices to connect to or use USNH information technology resources is considered acceptable use, these devices shall not be used to host websites, applications, or services, across any USNH network, for a non-USNH or component institution organization, without specific authorization from the Chief Information Security Officer (CISO).

4.7 Personal Use of USNH Information Technology Resources

4.7.1 Incidental personal use of USNH information technology resources is allowed (e.g., internet access, accessing personal e-mail) as long as it is consistent with this Policy, and any applicable administrative, academic, or business unit policies, procedures, and guidelines, and it does not:

4.7.1.1 Interfere with the performance of an employee's job or other responsibilities.

4.7.1.2 Consume a disruptive amount of information technology resources.

4.7.1.3 Violate any other USNH or component institution policies.

4.7.2 While this is considered an acceptable use, supervisors may impose further limits on use of USNH information technology resources for non-work purposes, in accordance with normal supervisory procedures.

4.8 Network Infrastruture

4.8.1 Unless specifically authorized, by the Chief Information Security Officer (CISO), community members shall not connect networking equipment (e.g., routers, hubs, sniffers) to any USNH network, nor operate network services (e.g., routing, name service, multicast services) on any endpoint or other device attached to a USNH network.

4.8.2 Community members shall not attempt to modify or tamper with any USNH wired and/or wireless network services nor to extend these information technology resources beyond the limits provided.

4.8.3 Unauthorized information technology resources connecting or attempting to connect to a USNH network may be denied access, have access terminated, and/or be banned from future access.

4.8.4 Detailed requirements for obtaining authorization to connect to a USNH network shall be provided in the relevant USNH Standards.

4.9 Loss of Access to Shared Information Technology Resources

4.9.1 ET&S may temporarily deactivate or restrict an individual's access to one or more shared information technology resources, even in the absence of a suspected AUP violation, when necessary to preserve the confidentiality, integrity, and/or availability of those and other information technology resources.

4.10 Acceptable Use Violations

4.10.1 If a community member observes or is otherwise aware of an alleged violation of this Policy, they should report the matter to the CISO.

4.10.2 The CISO, based on the details of the alleged violation, may investigate and, if appropriate, refer the matter to the appropriate USNH institution’s disciplinary authorities as outlined in the Enforcement section below.

4.11 Policy Maintenance

4.11.1 This Policy and the related standards shall be reviewed and maintained regularly, but no less than once per year.

5. Enforcement

Failure to comply with this policy puts the University System, its component institutions, and its information and information technology resources at risk and may result in disciplinary action. Disciplinary procedures will be appropriate for the individual responsible for non-compliance (e.g., students, faculty, staff, vendors) as outlined in the relevant institutional regulations for that individual (e.g., student conduct and/or applicable personnel policies).

Non-compliant technology and/or activities may be mitigated as deemed necessary by the CISO and/or CIO.

Employees who are members of institutionally recognized bargaining units are covered by the disciplinary provisions set forth in the agreement for their bargaining units.

6. Exceptions

Requests for exceptions to this policy shall be submitted and approved according to the requirements provided in the Cybersecurity Exception Standard.

7. Roles and Responsibilities

7.1 Business Application Owners/Technology Service Owners

7.1.1 Adhere to the rules governing access to specific community member institutional information and/or information technology resources defined in the Access to Password Protected Information Standard.

7.1.2 When warranted:

7.1.2.1 Establish more restrictive requirements governing use of information technology resources in their care.

7.1.2.2 Provide USNH community members with any additional requirements governing use of that specific information technology resource prior to granting access to that resource.

7.1.2.3 Ensure USNH community members agree to abide by information technology specific requirements before access is granted.

7.2 Chief Information Security Officer (CISO)

7.2.1 Determine if alleged violations of this policy require investigation or further action.

7.2.2 Refer violations of this policy, where appropriate, to the relevant USNH institutional disciplinary authority.

7.2.3 Document issues of clarity within this policy or the related standards raised by USNH community members.

7.2.4 Ensure issues with this policy raised by USNH community members are resolved in a timely manner through revision of this policy and the related standards, if needed.

7.2.5 Ensure this policy and related standards are reviewed and maintained regularly, but no less than once per year.

7.3 USNH Community Members

7.3.1 Observe all relevant laws, regulations, contractual obligations, and USNH policies and standards in relation to their access and use of USNH and component institution information technology resources.

7.3.2 Exercise good judgement in the use of USNH information technology resources.

7.3.3 Respect the rights and privacy of other community members.

7.3.4 Respect the security and integrity of USNH information technology resources.

7.3.5 Protect all enterprise and component institution credentials (username and password) issued to them.

7.3.6 Report any suspicious activity related to enterprise or institutional accounts or information technology resources immediately according to the Cybersecurity Incident Reporting process.

7.3.7 Avoid engaging in any prohibited use of information technology resources including the connection of networking equipment to any USNH network and modification or tampering with any USNH network service.

7.3.8 Understand the ramifications of using a personally owned endpoint or other device to access USNH information technology resources.

7.3.9 Report alleged violations of this policy to the CISO.

7.4 Enterprise Technology & Service (ET&S)

7.4.1 Provide information technology resources in support of USNH and component institution missions and objectives.

7.4.2 Safeguard the confidentiality, integrity, availability, and privacy of institutional information and USNH information technology resources.

7.4.3 Cooperate, upon the advice of the USNH General Counsel's Office (GCO), with any local, state, or federal investigation involving or pertaining to use of institutional information or USNH information technology resources.

7.4.4 Adhere to the rules governing access to specific community member institutional information and/or information technology resources defined in the Access to Password Protected Information Standard.

8. Definitions

See the ET&S Cybersecurity Policy & Standard Glossary for full definitions of each term.

- Acceptable Use
- Anti-virus
- Authorization
- Availability
- Business Application Owner
- Chief Information Security Officer
- Confidentiality
- Copyright
- Credentials
- Cybersecurity Incident
- Encryption
- Endpoint Device
- Exception
- Information Technology Resource
- Information
- Institutional Information
- Integrity
- Intellectual Property
- Password
- Personally Owned Device
- Policy
- Privacy
- Prohibited Use

- Standard
- Technology Service Owner
- Username
- USNH Community Member
- Vulnerability

CONTACT INFORMATION

For USNH community members: Questions about this Policy, requests for additional information or training, or reports of violations can be directed to Cybersecurity Governance, Risk, and Compliance (GRC) via this Support Form (https://td.unh.edu/TDClient/Requests/ServiceDet?ID=172).

All other requests can be submitted here: Submit an IT Question (https://td.unh.edu/TDClient/Requests/TicketRequests/NewForm?ID=ne440qM8v2g_).

up (/policy/usy/viii-cybersecurity-policies-and-standards)

OUTLINE

‹ A. Cybersecurity Policy (/policy/usy/viii-cybersecurity-policies-and-standards/cybersecurity)

C. Information Classification Policy › (/policy/usy/viii-cybersecurity-policies-and-standards/information-classification)

Printer-friendly version (/book/export/html/1357)

This page last updated **Wednesday, August 3, 2022**. For information on the adoption and effective dates of policies please see explanation on the OLPM Main Menu (/policy).

University System of New Hampshire

SYSTEM OFFICE | 5 CHENELL DRIVE, SUITE 301, CONCORD, NH 03301

Main: 603-862-1800 | TTY Users: 7-1-1 or 800-735-2964 (Relay NH)