46 tam

New Hampshire
DOT
Department of Transportation

THE STATE OF NEW HAMPSHIRE
DEPARTMENT OF TRANSPORTATION

Victoria F. Sheehan
Commissioner

William Cass, P.E.
Assistant Commissioner

His Excellency, Governor Christopher T. Sununu
and the Honorable Council
State House
Concord, New Hampshire 03301

Bureau of TSMO
December 2, 2021

REQUESTED ACTION

Authorize the Department of Transportation to enter into a service agreement with University System of New Hampshire (USNH), Concord, New Hampshire (Vendor #315187) for managed fiber network service, in the amount of $38,483.85, effective upon Governor and Council approval and once services have been installed and tested, for a five year term. 52% Highway Funds and 48% Turnpike Funds (Intra-Agency Transfers)

Funding to support this request is available in State FY 2022 and FY 2023. Funding is contingent upon the availability and continued appropriation of funds in FY 2024, FY 2025, FY 2026 and FY 2027, with the ability to adjust encumbrances through the Budget Office between State Fiscal Years if needed and justified:

04-096-096-960515-3052 Trans Sys Mgmt & Operations	FY 2022	FY 2023	FY 2024
039-500180 Telecommunications Data	$15,400.00	$4,872.00	$5,018.16
	FY 2025	FY 2026	FY 2027
	$5,168.70	$5,323.77	$2,701.22

EXPLANATION

The Department of Transportation operates a Statewide ITS program used to gather and disseminate information about road and weather conditions to the public and other State agencies. This statewide intelligent transportation system (ITS) is operated and managed from the Bureau of Transportation Systems Management and Operations (TSMO), Transportation Management Center (TMC) located within the Incident Planning and Operations Center (IPOC) in Concord.

Located at Portsmouth International Airport at Pease is a communication facility that is the focal point for wireless ITS communications along Spaulding Turnpike, Interstate 95 and NH Route 101 as well as the gathering point for safety and security camera images from all three interstate bridges with the State of Maine.

The leased services for the Statewide fiber optic cable network with USNH is intended to interconnect the TMC's ITS network directly to the seacoast ITS communications facility located at Pease, bypassing an older, complex lower bandwidth microwave radio network made up of multiple paths between Concord and Portsmouth. The leased interconnect is intended to become the primary communications path to the seacoast ITS systems including the dynamic part-time shoulder running project on Interstate 95 and over the Piscataqua River. Use of this leased service with one time construction cost will also allow for evaluation, reconfiguration and upgrades to the existing microwave system that has been in continuous duty service since November of 2011.

This service agreement has been approved by the Attorney General as to form and execution and the Department has verified that the necessary funds are available. Copies of the fully executed service agreement are on file at the Secretary of State office and the Department of Administrative Services office, and subsequent to Governor and Council approval will be on file at the Department of Transportation.

Your approval of this license agreement is respectfully requested.

Sincerely,

Victoria F. Sheehan
Commissioner

Attachments

Network Services Agreement
NH Department of Transportation and USNH

This Agreement is between State of New Hampshire Department of Transportation ("NHDOT") having a place of business at Smokey Bear Blvd, Concord, NH 03301 and the University System of New Hampshire, ("USNH") located at 5 Chenell Drive, Concord NH 03301. USNH and NHDOT are referred to individually as a "Party" and collectively as the "Parties". This Agreement describes the service and the responsibilities as agreed by both parties.

1 **Relationship** - NHDOT and USNH enter this agreement in a spirit of mutual respect and collaboration.

2 **Context** - The USNH Wide Area Network (WAN) provides data-transport, Internet, Internet 2, and other network services in support of education, research, and outreach for several New Hampshire institutions. The WAN is comprised of leased services from multiple providers as well as the IBEAM NH lightwave network. The New Hampshire IBEAM, owned by the University System of New Hampshire, is a high-speed regional optical network comprised of fiber optic cabling, network equipment and software, and monitoring systems. UNH staff, located at the University of New Hampshire in Durham, provide operations, administration, maintenance, and provisioning (OAM&P) for the USNH WAN.

3 **Prerequisites to this agreement** - There are no prerequisites to this agreement.

4 **Service Description** - Services are defined in the Service Information section of Exhibit B, Network and Internet Service Order. NHDOT may request additional network services such as DHCP, DNS, access control list (ACL) filtering, as well as Connect NH video collaboration, co-location and other services. These additional services would be included in an amendment to this agreement or in a separate agreement.

5 **Term & Termination**

5.1 Initial Service Term is defined in the Fees and Term section of Exhibit B, Network and Internet Service Order, to commence on the date that G & C approval is provided. See Paragraph 7, **Provisioning.** Renewal Term will be negotiated prior to the service end date and is contingent on approval from G&C. The termination of Service will not affect the NHDOT'S obligations to pay for other Service(s) as ordered.

5.2 Termination for Cause - Either party may terminate this Agreement upon written notice if the other party:

5.2.1 Commits a material breach of this Agreement and fails to cure such breach within thirty (30) days after the receipt of written notice of such breach from the other party; or

5.2.2 Becomes insolvent, acknowledges insolvency in any manner, ceases to do business, makes an assignment for the benefit of its creditors, or files a petition for bankruptcy.

5.3 If NHDOT terminates this agreement for any reason, NHDOT will be liable for all termination charges, of colocation fees and carrier circuit(s), including leased fiber, provided on behalf of NHDOT.

5.4 Effect of Termination - Upon termination of this Agreement for any reason, NHDOT shall pay to USNH all outstanding undisputed fees due to USNH as of the effective date of termination. In addition, any terms that by their nature extend beyond termination of this Agreement shall survive.

6 **Fees** – Fees are defined in the Fees and Term section of Exhibit B, Network and Internet Service Order and will not change during the first term of this agreement. If agreement renews beyond the first term, UNH will apply a 3% increase to the annual fee each year, beginning in the first renewal year. The annual recurring charge and annual increases can be renegotiated prior to each auto-renewal.

7 **Provisioning** - USNH WAN will work with the NHDOT technical staff to provision the new service and perform final testing. Billing will commence no sooner than the Commencement Date – that is: the date on which both parties agree that the service is functional.

8 **Acceptance of Service**

8.1 After USNH has completed provisioning the Service, there will be a one month "Interim Term" during which NHDOT will evaluate the Service. If service meets NHDOT'S reasonable expectations, which include USNH providing reliable service as described in Paragraph 4, **Service Description**, above, NHDOT will issue a written "Acceptance of Service" letter via email to the USNH Customer Account Representative.

8.2 Commencement Date will be the next business day following UNH's receipt of Acceptance of Service from NHDOT.

8.3 If, at the end of the Interim Period, the Service does not meet NHDOT'S reasonable expectations, NHDOT may issue a written "Rejection of Service" letter via email or US Mail to USNH. If NHDOT issues a Rejection of Service as described, NHDOT may withdraw from this Agreement with no obligations to USNH.

9 **Billing** – USNH will issue an invoice for Service to NHDOT upon Acceptance of Service, and at the beginning of each subsequent billing cycle as defined in the Fees and Term section of Exhibit B, Network and Internet Service Order. NHDOT will notify UNH Information Technology Business Service Center of any changes or problems via the email address or phone number listed in Exhibit A, Notices and Contact Information.

10 **Network Downtime**

10.1 Definition - Downtime due to the USNH internal network or those network elements over which USNH has direct control and lasts 15 minutes or longer. USNH is not responsible for 3rd party fiber-optic cable, electrical power, customer action or inaction, or events of force majeure as defined in paragraph 24.

10.2 Service Credit - In the event NHDOT experiences downtime (as defined in 10.1 above), NHDOT will receive a Service Credit based on the cumulative unavailability of the affected service in a given calendar month as set forth in the following table.

Service Credit:

1 second – 30 Minutes	No Credit
30 Minutes – 2 Hours	25% of MRC
2 Hours – 12 Hours	50% of MRC
12 Hours or greater	100 % of MRC

10.3 NHDOT must request a Service Credit within seven (7) days of the downtime or NHDOT will forfeit the Service Credit.

10.4 In the event USNH discovers, or is notified by NHDOT, that NHDOT is experiencing a performance problem, USNH will take all necessary actions to identify and correct the performance problem.

11 Support

11.1 The service includes live phone and email support. USNH Wide Area Network engineers shall provide support during USNH business hours 8am – 4:30pm Monday through Friday, excluding UNH holidays.

11.2 USNH shall provide Operations, Administration, Maintenance and Provisioning which includes operation of multiple test, monitoring, and logging systems to assure optimal operation of service. These systems provide 24/7 notification to USNH network staff of critical outages. USNH Staff responds to critical outages outside USNH business hours on a best-effort basis.

11.3 Problem Notification

11.3.1.1 NHDOT'S technical contact is to report problems via telephone call to the USNH WAN Hotline: (603) 862-BITS (2487) or via email to wan.netops@unh.edu.

11.3.1.2 Problem Notifications will be entered and tracked in the USNH trouble-ticketing system with an associated "Incident Number". Upon commencement of Problem Resolution, USNH staff will provide NHDOT with the Incident Number.

11.4 Problem Resolution - USNH WAN service depends on fiber and network providers and common carriers. USNH will be responsible to work with providers to resolve outage on NHDOT'S behalf.

11.5 USNH network staff response time and resolution time objectives to a Problem Notification during business hours are based on severity as follows:

Problem Severity Level	Description	Response Time Objective	Resolution Time Objective
CRITICAL	A complete outage.	60 Minutes	2 Hours
MAJOR	A significant degradation of the service.	2 Hours	4 Hours
MINOR	A minor degradation of service	4 Hours	Next Business Day

11.6 Upon resolution of the Problem, USNH WAN staff will close the Incident and notify NHDOT that the Incident has been closed.

12 **NHDOT responsibility** - In order to assure the most rapid recovery of diminished service ("Problem"), NHDOT shall provide accurate and detailed information in reporting the Problem. In addition, if deemed necessary by the USNH technical staff, NHDOT shall cooperate and participate with the USNH staff in the work of troubleshooting the Problem. Among other activities, this required cooperation shall include timely execution of the following:

12.1 Providing accurate description of the problem symptoms;

12.2 observing and reporting on the status of power and LED indicators on the USNH equipment at NHDOT'S site;

12.3 reporting log and other information from NHDOT'S networking equipment or other network-connected equipment;

12.4 capturing network trace information on NHDOT equipment using TCPDUMP, Wireshark, or similar test programs;

12.5 disconnecting NHDOT equipment from the network that USNH staff determine is potentially causing the problem;

12.6 disconnecting and reconnecting power to the IBEAM equipment to initiate a reboot;

12.7 providing access to NHDOT facilities (e.g. data room or telecom closet).

12.8 NHDOT will provide a host IP interface with PING capability on NHDOT'S network.

13 **Client NMS Portal** - NHDOT may request access to USNH WAN web-based network monitoring platform ("NMS portal") to have read-only view of up/down status and usage statistics. NHDOT will keep NHDOT'S NMS portal login information confidential.

14 **Ongoing maintenance** - USNH will, from time to time, modify, upgrade, or replace software and hardware components in the Service. USNH will work with NHDOT to schedule such work to minimize any down-time impact on NHDOT'S users. Maintenance down-time is not counted in the service level Network Downtime calculation.

15 **USNH WAN equipment** – Any USNH WAN equipment on site is owned by USNH. If any USNH WAN equipment is placed on NHDOT's site, NHDOT will provide appropriate electrical power and secure space, and assure temperature in space will not exceed 80 degrees Fahrenheit. NHDOT will not touch, move, power-down, nor otherwise alter the state of the USNH WAN equipment on NHDOT'S premise without express permission of USNH IT network staff. NHDOT can request that USNH move equipment, and USNH staff will work with NHDOT to coordinate such a change in a timely manner. NHDOT will assist USNH to make reasonable arrangements to perform this work.

16 **NHDOT network** - It is presumed that NHDOT is connecting a local area network (NHDOT LAN) to the USNH WAN service. NHDOT shall operate NHDOT LAN in a responsible manner. NHDOT is solely responsible for the selection, implementation, and maintenance of security features for protection against unauthorized or fraudulent use of service.

17 **Appropriate Use** –

17.1 NHDOT use of USNH WAN shall comply with the USNH Acceptable Use Policy (AUP). USNH staff are bound by the USNH AUP as well. The USNH AUP can be found on the USNH Internet website at http://www.usnh.edu/olpm/UNH/VI.Prop/F.htm#5 The AUP can be attached as an exhibit to this agreement at NHDOT'S request.

17.2 NHDOT use of USNH WAN shall comply with the Internet2 Network Acceptable Use Policy (AUP), which can be found at: http://www.internet2.edu/media/medialibrary/2013/09/18/Internet2_Network_Acceptable_Use_Policy_1.pdf. The AUP can be attached as an exhibit to this agreement at NHDOT'S request.

18 **Suspension of service** - USNH may suspend service without billing relief for the following: Non-payment; AUP violation; failure to protect USNH equipment on NHDOT site; failure to provide safe working environment for USNH staff when working at NHDOT site; violation of the terms of this agreement. USNH will provide a 10-day minimum notice period before suspending service except for egregious AUP violations. Egregious violations may result in immediate suspension of service until the violation is cleared.

19 **Good Faith Performance** - The Parties will act in good faith in their performance of this Agreement. Neither party will unreasonably withhold nor delay actions required in this Agreement.

20 **Confidentiality** - The Parties will respect the privacy of each other's information – That is: Neither Party will observe, capture, view, nor share with other parties, any of the information flowing

through or stored in the other Party's equipment (or in print form), and will not allow other parties to do so either – with the following exception: In order to troubleshoot or modify USNH WAN service, USNH WAN personnel may capture data packets and observe data patterns on the USNH WAN. When performing said troubleshooting or modification, USNH staff will respect the privacy of NHDOT'S information as described.

21 **Insurance** - Each Party shall maintain general liability insurance to protect against any damage that the Party's employees may cause inadvertently to the opposite Party's equipment. In addition, each Party will maintain workers' compensation insurance at statutory limits.

22 **Force Majeure** - If performance of this Agreement or any obligation under this Agreement is prevented, restricted, or interfered with by causes beyond either Party's reasonable control ("Force Majeure"), and if the party unable to carry out its obligations gives the other party prompt written notice of such event, then the obligations of the party invoking this provision, other than delay in the payment of money due and payable hereunder, shall be suspended to the extent necessary by such event. The term Force Majeure shall include, without limitation, acts of God, fire, explosion, vandalism, storm or other similar occurrence, orders or acts of military or civil authority, or by national emergencies, insurrections, riots, wars, supplier failures, shortages, breaches, or delays.

23 **Assignment** - Neither Party may assign nor transfer this Agreement, nor any interest in this Agreement without the prior written consent of the other Party whose agreement will not unreasonably be withheld. Action by either Party in violation of this provision will relieve the other Party from any further obligations arising from this Agreement.

24 **Amendment to this Agreement** - This Agreement may be amended, extended, or terminated by mutual agreement. Amendment must be in writing and signed by authorized personnel from both Parties.

25 **Notices** - All notices must be in writing and given by U.S. mail, certified and postage prepaid, or nationally recognized overnight courier that regularly maintains records of items delivered. Notices will be made to the Business and Billing Contacts defined in Exhibit A, Notices and Contact Information section.

26 **Governing Law** - This Agreement shall be interpreted, construed, and governed according to the laws of the state of New Hampshire and any disputes arising hereunder shall be brought in a court of competent jurisdiction in the State of New Hampshire.

27 **Effectiveness; Date** - This Agreement will become effective when all the parties have signed it. The date this Agreement is signed by the last party to sign it (as indicated by the date associated with that party's signature) will be deemed the date of this Agreement.

Note: Signatures follow on next page.

Each party is signing this Agreement on the date stated opposite that party's signature.

NH DEPARTMENT OF TRANSPORTATION

By: ______________________ Typed Name: VICTORIA SHEEHAN

Title: COMMISSIONER Date: 12/16/21

Approved by the Attorney General (Form, Substance and Execution)

Emily C. Goering Date: 1/20/2022

State of New Hampshire, Department of Justice

Approved by NH Governor and Council

______________________ Date: ______________________

UNIVERSITY SYSTEM OF NEW HAMPSHIRE

By: ______________________ Typed Name: Tony Bargardo

Title: Manager WAN Services USNH Date: 10/21/2021

Exhibit A
Notices and Contact Information

USNH:

Customer Account Representative

Tony Bargardo
Manager Wide Area Network services
University of New Hampshire
50 College Rd, Durham, NH 03824
(603) 862-6677

Technical Contact

NetworkNH -University of New Hampshire
50 College Rd, Durham, NH 03824
wan.netops@unh.edu
(603) 862-2487 (862-BITS)

Billing Contact

UNH ET&S LAN/WAN
50 College RD
Durham, NH 03824
(603) 862-1030
telecom@unh.edu with subject line: Billing Inquiry – Network Services Agreement

Emergency contacts:

During Normal Business Hours:
USNH WAN NetOps Hotline:
(603) 862-2487 (862-BITS) or Wan.netops@unh.edu
During Non-Business Hours:
UNH Police Dispatch (603) 862-1392

NHDOT :

Primary Contact:	**Business Contact:**	**Technical Contact:**
Susan Klasen	Janelle Marquez	Thomas Dunigan
Susan.M.Klasen@dot.nh.gov	Janelle.N.Marquez@dot.nh.gov	Thomas.F.Dunigan@doit.nh.gov
603-271-6862	603-271-6862	603-223-4354

Exhibit B

Network and Internet Service Order

NetworkNH

University of New Hampshire

Service Order #:		
Account Representative:	Tony Bargardo	603-862-6677
System Engineer:	wan.netops@unh.edu	603-862-2487
Customer PO#:		

Customer Information - New Hampshire Department of Transportation

	Contract Contact	Billing	Technical
Name:	Susan Klasen	Same as Customer Info	Susan Klasen
Title:	Administrator, Bureau of TSMO		Bureau of TSMO, TMC
Address:	110 Smokey Bear Blvd.		PO Box 483
City, State, Zip	Concord, NH 03302		Concord, NH 03302-0483
E-Mail Address:	Susan.Klasen@dot.nh.gov		Bureau56@dot.nh.gov
Phone Number:	(603) 223-4364		603-271-6862

A Location Information

Location Address:	Pease Water Tower, Interanational Drive
Location Floor/Suite:	43° 4'41.29"N, 70°47'55.25"W
Location City, State, Zip:	Pease Tradeport, Newington, NH
Location Phone Number:	N/A
Local Contact:	N/A
Local Contact Email:	N/A
Local Contact Phone:	N/A
Hand-off Type:	1000 Base T

Location Details/Comments:

Connection type will be 1G ethernet.

Z Location Information

Location Address:	110 Smokey Bear Blvd.
Location Floor/Suite:	
Location City, State, Zip:	
Location Phone Number:	
Local Contact:	
Local Contact Email:	
Local Contact Phone:	
Hand-off Type:	

Location Details/Comments:

Service Information

Service Type:	New
Customer Request Date*:	8/1/21

*Does not constitute a contractual obligation, but is for informational purposes only

Service consist of a layer 2 point to point service between the a and Z locations. Service to Commence upon approval of G&C and once services have been installed and tested. Term of this service is 5 years.

Service Term:	G&C Approval	I	5 year term

Fees

	Service Type	Monthly Recurring Charge (MRC)	Non Recurring Charge (NRC)
Service:	Internet		
Symmetrical Bandwidth:	0 Mbps	$0.00	
Protection Level:	Unprotected	$0.00	
Service:	Transport		
Symmetrical Bandwidth:	200 Mbps	$400.00	$13,000.00
Protection Level:	Unprotected	$0.00	$0.00
Service:	Amortized NRC	$0.00	
Symmetrical Bandwidth:	0 Mbps	$0.00	$0.00
Protection Level:	Unprotected	$0.00	$0.00
Totals:		$400	$13,000

This section covers circuit installation only. Inside wiring and cross connects are not included unless otherwise stated.

Billing Cycle ○ Monthly ● Quarterly ○ Annual

Terms

The terms and conditions contained in the Network Service Agreement are hereby incorporated by reference and are made a part of this Service Order. Any ambiguity or conflict in such terms and conditions between this Service Order and the Network Service Agreement and all exhibits attached thereto shall be governed and controlled by the terms and conditions as contained in the said Network Service Agreement

Additional Comments

Acceptance

NetworkNH Signature:		Customer Signature:	
Name:	Tony Bargardo	Name:	
Title:	Manager of WAN Services USNH	Title:	
Date:	10/21/21	Date:	

Client Acceptance: Pricing, contract, and payment information subject to UNH approval.

Subsection USNH Online Policy Manual – VIII. Cybersecurity Policies and Standards

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

University System
of New Hampshire

ENTERPRISE TECHNOLOGY & SERVICES
GLOSSARY OF TERMS

Access: The ability to make use of any information technology resource or to gain entry to a physical area or location.

Access Control: Process or procedure designed to manage, allow, and restrict use of USNH information and information technology resources and/or physical entry to the physical spaces that house them, for the purposes of preventing unauthorized use.

Account: A mechanism used to establish personalized access to a computer, website, or other information technology resource, generally tied to a set of credentials like a username and password.

Administrative/Operational Control: Process or procedure intended to safeguard information or information technology resources that is primarily implemented and executed by people, rather than by other information technology resources.

Administrator: A person who manages an application, a database, a network, or an information technology resource.

Anti-malware Software: A program or tool that detects many forms of malicious software called malware (e.g., viruses and spyware) and prevents them from infecting computers. It may also cleanse already-infected computers.

Asset: A tangible or intangible resource of value that an organization possesses or employs in order to achieve the organization's mission/business objectives.

Audit Log: A chronological record of information technology resource activities, including records of system accesses and operations performed in a given period that is used for operational purposes.

Audit Record: An individual entry in an audit log related to an audited event.

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to [information technology] resources.

Authentication Factor: A piece of information used to verify the identity of a community member, device, or information technology resource.

Authorization: Access privileges granted to a user, program, or process or the act of granting those privileges."

Availability: Protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data.

Backup: A copy of information, files, and programs made to facilitate recovery, if necessary.

Baseline: Formally approved configuration for an information technology resource.

Birthright Access: Accounts, privileges, and/or authorizations automatically granted based on a community member's coarse-grain role(s).

Breach: A cybersecurity incident in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, used, modified, or destroyed by an individual unauthorized to do so.

Bulk Email: Sending large quantities of email with similar content to multiple recipients.

Business Application Owner: An individual outside of Enterprise Technology & Services (ET&S) who is responsible for delivery, administration, support, and management of a non-ET&S managed information technology resource, generally, this resource is a vendor cloud-hosted service.

Business Continuity Plan: The procedures and instructions an organization will follow to continue business operations or rapidly recover operational capabilities in the event of a natural or other disaster; it covers business processes, assets, human resources, business partners and more.

Central Authentication: Verification of an identity for the purposes of allowing access to information technology resources that can be leveraged to access many resources. Often referred to as single-sign on or reduces sign-on.

Centrally Managed Account: A type of authorization created and managed in a central directory, allowing access many information technology resources.

Chief Information Officer (CIO): Executive leader responsible for the management, implementation, and usability of information and information technology resources.

Chief Information Security Officer (CISO): Executive leader responsible for the development, implementation, oversight, and maintenance of an organization's information security or cybersecurity program.

Cloud Service: Information technology capability provided for a fee using a third-party provider's infrastructure (e.g., servers, hardware, networking equipment), information system, or application that is accessed over the internet. Includes Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS).

Coarse-grained Role: A designation used to describe a specific relationship with the University System and/or one of its component institutions.

Compensating Control: A management, operational, physical, or technical safeguard or countermeasure employed in lieu of the recommended or required safeguard or countermeasure that provides equivalent or comparable protection or risk mitigation.

Compromised Account: Access to an information technology resource or resources that is known to be vulnerable to attack or misuse by unauthorized parties because of exposure, breach, or intentional/unintentional revelation.

Computer-based Training: An educational delivery mechanism where content is provided via a computer program rather than by a person.

CONFIDENTIAL Information: Tier 5 of the proposed USNH Information Classification Framework which includes information requiring the highest level of protection and most restrictive security controls and safeguards. It includes electronic Personal Health Information (ePHI) covered by HIPAA and specific information/data used in some grant-funded research efforts.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Management: A collection of activities focused on establishing and maintaining the integrity of information technology resources, through control of the processes for initializing, changing, and monitoring the configurations of those resources.

Credentials: A set of USNH attributes, generally represented by a username and password, that uniquely identifies an entity such as a person or a device.

Critical Business Process: Business processes performed by any administrative, academic, and business unit that involve information that is classified as PROTECTED, RESTRICTED, or CONFIDENTIAL per the proposed USNH Information Classification framework.

Cybersecurity: The ability to protect or defend the use of cyberspace from cyber-attacks. The practice of protecting information and information technology resources from "unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

Cybersecurity Event: Anomalous or unexpected activity with the potential to adversely impact the confidentiality, integrity, or availability of institutional information, regardless of its format, or any information technology resource.

Cybersecurity Incident: An anomalous or unexpected event, set of events, condition, or situation that actually or potentially jeopardizes the confidentiality, integrity, or availability of institutional information, regardless of format, an information technology resource or the information that resource captures, processes; stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Data Steward: A business subject matter expert designated as accountable for a specific type or types of institutional information who determines the classification of that information, approves access to and use of that information and provides institutional authority for mandating information security controls to protect that information.

Deprovision: To remove access to an information technology resource or resources.

Disaster Recovery Plan: A plan that, when activated, designates how critical information technology resources will be restored and outlines the resources required to achieve restoration of those resources after a natural or human-induced disaster.

Domain: The portion of an email address that follows the @ symbol that acts as a common suffix to designate email addresses that are under the control of a specific organization.

Elevated Access: Authorization within an application that allow a community member to perform functions within that application that regular users of that application cannot perform, including making configuration changes, authorizing use by other community members, and modification to information stored within the application.

Encryption: The transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

Endpoint/Endpoint Device: An electronic computing device that connects to a network and communicates back and forth with that network. Endpoints include desktop computers, laptop computers, tablets, mobile devices, or any similar network enabled device.

Exception: A temporary exemption from being required to comply with a USNH or institutional Policy or Standard.

FAIR™: FAIR, which stands for Factor Analysis for Information Risk, is a cyber risk framework used for quantitative analysis of information security risk.

FERPA: FERPA, which stands for Family Educational Rights and Privacy Act, is a "federal law that protects the privacy of student educational records."

Fine-grained Role: A designation used provide information technology resource access to community members who are part of a specific group, like all students in Chemistry 101 or all incoming students.

Firewall: A part of a computer system or network that is designed to block unauthorized access while permitting outward communication.

GLBA: GLBA, which refers to the Gramm Leach Blilley Act, is a federal law that requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. At USNH, GLBA is applicable to information provided for financial aid purposes.

Guest/Lab Account: A type of account that is used to provide access to specific information technology resources for individuals who are participating in an activity, like a summer camp, at a USNH institution or that is used to administer shared devices in a computer lab.

HIPAA: HIPAA, which refers to the Health Insurance Portability and Accountability Act, is a federal law that mandates specific privacy and security requirements for handling and protecting personal health information (PHI).

Host-based Firewall: A firewall that runs on and protects an individual server or endpoint device instead of an entire network.

Identifier: Unique data used to represent an identity and associated attributes. A USNH username and USNH ID number are examples of identifiers.

Identity: The set of physical and behavioral characteristics by which an individual [entity] is uniquely recognizable.

Identity System of Record: An information system that is used to capture, store, process, transmit, and otherwise manage the information contained in identity records. Examples at USNH include the Banner HR system and each of the component institution's student information systems.

Incident: See Cybersecurity Incident

Information: Facts, data, or instructions in any medium or form.

Information Security: See Cybersecurity.

Information Steward:. See Data Steward.

Information Technology Resource: Any hardware, software, firmware, equipment, Internet of things (IoT) devices, applications, information systems, etc. used to access, capture, store, process, utilize, integrate, interface with, transmit, or otherwise manage information.

Institutional Information: Information, in any format, created, collected, recorded, captured, stored, processed, transmitted, or otherwise managed by or for the University System and its component institutions, to conduct USNH business.

Institutionally Owned Endpoint: A computer or computing device intended for end-user use purchased by the University System or one of its component institutions.

Integrity: Ensuring the authenticity of information—that information is not altered, and that the source of the information is genuine – and of information technology resources – that resources are functioning as intended, without any unauthorized modifications or alterations.

Internet Connected Device: A physical object that can connect to the internet including, but not limited to, desktop computers, laptops, tablets, smart phones, sensors, household appliances, and wearable technology like a smart watch.

Internet of Things (IoT): The interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data.

Keystroke Logging: The process used to record the keys struck on a keyboard without the knowledge of the user.

Least Functionality: Configuring information technology resources such that they provide only those capabilities needed to perform the activities assigned to them and restrict the use of capabilities, such as ports, protocols, or services, that are not essential to those activities.

Least Privilege: Access control strategy requiring that community members only be given access to the information, information technology resources, and specific capabilities within those resources, necessary to perform their job duties.

Local Authentication: Verification of an identity for the purposes of allowing access to a single information technology resource.

Locally Managed Account: A type of authorization created and managed on or for a specific information technology resource.

Log: A record of the events occurring within an organization's information technology resources and networks.

Logical Control: Tools and protocols used by information technology resources to enforce security measures.

MAC Address: A media access control address or MAC address is a unique hardware identification number that uniquely identifies each device on a network.

Mitigate: The effort to reduce loss by making a deficiency less severe and lessening the impact of potential damages.

Multi-factor Authentication (MFA): Access that requires the use of two or more different factors including (i) something you know (e.g., password/PIN); (ii) something you have (e.g., authentication app on a mobile device, token); or (iii) something you are (e.g., biometric).

Network Device: A piece of equipment that enables communication and data transmission between information technology resources across a network or networks. Examples include gateways, routers, wireless access points, networking cables, and switches.

Non-Primary Identity: A unique identifier established for a USNH community member that is separate from their primary identity. Examples of non-primary identities are Pool, Secondary, Service, System Administrator.

NTP: Network Time Protocol (NTP) is a protocol used to synchronize time on all participating information technology resources to within a few milliseconds of Coordinated Universal Time (UTC).

Out of Band: A circumstance where a different method (e.g., process, procedure, tool, etc.) or frequency is used or required instead of the standard method or frequency.

Password: A trusted secret compromised of "a string of characters (letters, numbers and other symbols) that are used" as part of confirming the identity of a person, device, or information technology resource.

Patch: An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

PCI-DSS: The Payment Card Industry – Data Security Standard (PCI-DSS) is a set of "operational and technical requirements" developed by the PCI Security Standards Council that defines required security practices for all "organizations accepting or processing payment transactions" or that develop information technology resources used to process them.

Personally Identifiable Information (PII): Any information about an individual that can be used to distinguish or trace an individual's identify and any other information that is linked or linkable to an individual.

Personally Owned Endpoint: A computer or computing device purchased by a USNH community member using money that was not provided by or associated with USNH or one of its component institutions.

Phishing: Tricking individuals into disclosing sensitive information by claiming to be a trustworthy entity in an electronic communication (e.g., internet web sites, email).

Physical Security: Safeguards used to protect the locations where information and information technology resources are stored or housed against unauthorized access.

Policy: High-level statement of principle intended to provide direction to the USNH community.

Portable Device: An endpoint device that is small enough to be carried from one location to another as part of regular use (e.g., laptop, tablet, mobile phone).

Primary Identity: The identity associated with a user's USNH username. Each individual person has only one primary identity across the entire University System of New Hampshire and its component institutions.

Privileged Access: An escalated level of permissions for an information security resource that is granted to community members that are responsible for the administration of those resources. administrative services such as system maintenance, data management, and user support.

Procedure: An established or official way of doing something.

PROTECTED Information: Tier 3 of the proposed USNH Information Classification Framework which includes information requiring safeguards and specific privacy handling procedures. It includes student information and educational records protected under FERPA.

Provisioning: Establishing the authorizations needed to enable access to a specific information technology resource (e.g., creating an account).

PUBLIC Information: Tier 1 of the proposed USNH Information Classification Framework which includes information specifically approved by data stewards for public distribution.

Quarantine: The process of restricting the ability of an information technology resource like an endpoint or a server to connect to network resources.

Remote Access: The ability for community members to access USNH information technology resources from external locations.

Removable Media: Any device whose primary purpose is to electronically store information that can be easily transported. Examples of removable media include USB flash drives, CD-ROM, DVD-ROM, external or portable hard drives, or any other portable computing device with storage capabilities.

Replay-Resistant Authentication: Configuration that protects against reuse of authentication information that is retransmitted with the intent of producing an unauthorized effect or gaining unauthorized access.

RESTRICTED Information: Tier 4 of the proposed USNH Information Classification Framework which includes information requiring specific security controls. It includes personally identifiable information like SSN and passport number, credit card information, and research information.

Risk: The probable frequency and probable magnitude of future loss.

Risk Acceptance: The formal process of documenting an acknowledgement of the details of a known risk that cannot or will not be mitigated.

Risk Assessment: A systematic process of identifying, analyzing, and documenting potential information security risks.

Risk Management: The program and supporting processes to manage risk to organizational operations (e.g., mission, functions, reputation), organizational assets (e.g., information, information technology resources), individuals, .and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a potential desired result.

Security Categorization: A risk management designation used across the USNH Information Security Program, to consistently express the criticality of an information technology resource or business process, based on the institutional information involved and the breadth of impact if that resource or process were compromised.

Security Configuration Baseline: An agreed configuration for a specific information technology resource designed to safeguard that resource.

Security Control: A safeguard or countermeasure prescribed for an information technology resource designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

Security Log: A chronological record of information technology resource activities, including records of system accesses and operations performed in a given period used for information security purposes.

SENSITIVE Information: Tier 2 of the proposed USNH Information Classification Framework which includes information requiring that can be shared when there are valid purposes to do so, but that cannot be shared publicly.

Segregation of Duties: A security principle that requires the use of one account for non-privileged access and a separate account to be used for privileged access to decrease the likelihood of, and potential for, unauthorized use of the privileged access.

Separation of Duties: A security principle that divides critical functions among different staff members in an attempt to ensure that no one individual has enough information or access privilege to negatively impact confidentiality, integrity, and/or availability.

Server: A "Server" is any device which provides service to other network devices regardless of the scale of those services. Specifically excluded from this definition for the purposes of this document:

1. Devices that provide individualized service to other devices, such a blue tooth devices. RF externals, etc.
2. Devices that provide service for the purpose of system management only (i.e. a device that provides service (like RDP or SSH) for the purpose of being managed by other systems)

Despite the exclusion of these types of devices, services provided by them must still be run securely and with up-to-date versions of software.

Service Account: An authorization that enables an information technology resource to communicate with and connect to another information technology resource.

Single Sign On (SSO): A capability that allows the use of one set of authentication credentials, like a username and password, to be used to access several information technology resources.

Spam: Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Standard: A published statement on a topic specifying requirements that must be satisfied or achieved in order to comply with a policy.

Susceptible: Likely or liable to be influenced or harmed by a particular thing.

Technology Service Owner: The individual within Enterprise Technology & Services (ET&S) responsible for operation and maintenance of an information technology resource.

Threat: The potential for a threat source to exploit (intentional) or trigger (accidental) a specific vulnerability.

Username: A unique character string used to designate a specific identity.

USNH Community Member: Any individual who has a relationship with the University System of New Hampshire or one of its component institutions including employees, students, applicants, prior students/alumni, donors, and sponsored users.

USNH ID: A unique nine-digit number used to designate a specific identity. Also called "9 Number".

Vendor: A third-party provider of an information technology resource or capability.

Vulnerability: Weakness in an information technology resource security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Waiver: A permanent (longer than one year) exemption from the requirement to comply with a Policy and/or Standard.

University System
of New Hampshire

ENTERPRISE TECHNOLOGY & SERVICES GLOSSARY OF TERMS

Access: The ability to make use of any information technology resource or to gain entry to a physical area or location.

Access Control: Process or procedure designed to manage, allow, and restrict use of USNH information and information technology resources and/or physical entry to the physical spaces that house them, for the purposes of preventing unauthorized use.

Account: A mechanism used to establish personalized access to a computer, website, or other information technology resource, generally tied to a set of credentials like a username and password.

Administrative/Operational Control: Process or procedure intended to safeguard information or information technology resources that is primarily implemented and executed by people, rather than by other information technology resources.

Administrator: A person who manages an application, a database, a network, or an information technology resource.

Anti-malware Software: A program or tool that detects many forms of malicious software called malware (e.g., viruses and spyware) and prevents them from infecting computers. It may also cleanse already-infected computers.

Asset: A tangible or intangible resource of value that an organization possesses or employs in order to achieve the organization's mission/business objectives.

Audit Log: A chronological record of information technology resource activities, including records of system accesses and operations performed in a given period that is used for operational purposes.

Audit Record: An individual entry in an audit log related to an audited event.

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to [information technology] resources.

Authentication Factor: A piece of information used to verify the identity of a community member, device, or information technology resource.

Authorization: Access privileges granted to a user, program, or process or the act of granting those privileges."

Availability: Protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data.

Backup: A copy of information, files, and programs made to facilitate recovery, if necessary.

Baseline: Formally approved configuration for an information technology resource.

Birthright Access: Accounts, privileges, and/or authorizations automatically granted based on a community member's coarse-grain role(s).

Breach: A cybersecurity incident in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, used, modified, or destroyed by an individual unauthorized to do so.

Bulk Email: Sending large quantities of email with similar content to multiple recipients.

Business Application Owner: An individual outside of Enterprise Technology & Services (ET&S) who is responsible for delivery, administration, support, and management of a non-ET&S managed information technology resource, generally, this resource is a vendor cloud-hosted service.

Business Continuity Plan: The procedures and instructions an organization will follow to continue business operations or rapidly recover operational capabilities in the event of a natural or other disaster; it covers business processes, assets, human resources, business partners and more.

Central Authentication: Verification of an identity for the purposes of allowing access to information technology resources that can be leveraged to access many resources. Often referred to as single-sign on or reduces sign-on.

Centrally Managed Account: A type of authorization created and managed in a central directory, allowing access many information technology resources.

Chief Information Officer (CIO): Executive leader responsible for the management, implementation, and usability of information and information technology resources.

Chief Information Security Officer (CISO): Executive leader responsible for the development, implementation, oversight, and maintenance of an organization's information security or cybersecurity program.

Cloud Service: Information technology capability provided for a fee using a third-party provider's infrastructure (e.g., servers, hardware, networking equipment), information system, or application that is accessed over the internet. Includes Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS).

Coarse-grained Role: A designation used to describe a specific relationship with the University System and/or one of its component institutions.

Compensating Control: A management, operational, physical, or technical safeguard or countermeasure employed in lieu of the recommended or required safeguard or countermeasure that provides equivalent or comparable protection or risk mitigation.

Compromised Account: Access to an information technology resource or resources that is known to be vulnerable to attack or misuse by unauthorized parties because of exposure, breach, or intentional/unintentional revelation.

Computer-based Training: An educational delivery mechanism where content is provided via a computer program rather than by a person.

CONFIDENTIAL Information: Tier 5 of the proposed USNH Information Classification Framework which includes information requiring the highest level of protection and most restrictive security controls and safeguards. It includes electronic Personal Health Information (ePHI) covered by HIPAA and specific information/data used in some grant-funded research efforts.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Management: A collection of activities focused on establishing and maintaining the integrity of information technology resources, through control of the processes for initializing, changing, and monitoring the configurations of those resources.

Credentials: A set of USNH attributes, generally represented by a username and password, that uniquely identifies an entity such as a person or a device.

Critical Business Process: Business processes performed by any administrative, academic, and business unit that involve information that is classified as PROTECTED, RESTRICTED, or CONFIDENTIAL per the proposed USNH Information Classification framework.

Cybersecurity: The ability to protect or defend the use of cyberspace from cyber-attacks. The practice of protecting information and information technology resources from "unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

Cybersecurity Event: Anomalous or unexpected activity with the potential to adversely impact the confidentiality, integrity, or availability of institutional information, regardless of its format, or any information technology resource.

Cybersecurity Incident: An anomalous or unexpected event, set of events, condition, or situation that actually or potentially jeopardizes the confidentiality, integrity, or availability of institutional information, regardless of format, an information technology resource or the information that resource captures, processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Data Steward: A business subject matter expert designated as accountable for a specific type or types of institutional information who determines the classification of that information, approves access to and use of that information and provides institutional authority for mandating information security controls to protect that information.

Deprovision: To remove access to an information technology resource or resources.

Disaster Recovery Plan: A plan that, when activated, designates how critical information technology resources will be restored and outlines the resources required to achieve restoration of those resources after a natural or human-induced disaster.

Domain: The portion of an email address that follows the @ symbol that acts as a common suffix to designate email addresses that are under the control of a specific organization.

Elevated Access: Authorization within an application that allow a community member to perform functions within that application that regular users of that application cannot perform, including making configuration changes, authorizing use by other community members, and modification to information stored within the application.

Encryption: The transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

Endpoint/Endpoint Device: An electronic computing device that connects to a network and communicates back and forth with that network. Endpoints include desktop computers, laptop computers, tablets, mobile devices, or any similar network enabled device.

Exception: A temporary exemption from being required to comply with a USNH or institutional Policy or Standard.

FAIR™: FAIR, which stands for Factor Analysis for Information Risk, is a cyber risk framework used for quantitative analysis of information security risk.

FERPA: FERPA, which stands for Family Educational Rights and Privacy Act, is a "federal law that protects the privacy of student educational records."

Fine-grained Role: A designation used provide information technology resource access to community members who are part of a specific group, like all students in Chemistry 101 or all incoming students.

Firewall: A part of a computer system or network that is designed to block unauthorized access while permitting outward communication.

GLBA: GLBA, which refers to the Gramm Leach Bliley Act, is a federal law that requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. At USNH, GLBA is applicable to information provided for financial aid purposes.

Guest/Lab Account: A type of account that is used to provide access to specific information technology resources for individuals who are participating in an activity, like a summer camp, at a USNH institution or that is used to administer shared devices in a computer lab.

HIPAA: HIPAA, which refers to the Health Insurance Portability and Accountability Act, is a federal law that mandates specific privacy and security requirements for handling and protecting personal health information (PHI).

Host-based Firewall: A firewall that runs on and protects an individual server or endpoint device instead of an entire network.

Identifier: Unique data used to represent an identity and associated attributes. A USNH username and USNH ID number are examples of identifiers.

Identity: The set of physical and behavioral characteristics by which an individual [entity] is uniquely recognizable.

Identity System of Record: An information system that is used to capture, store, process, transmit, and otherwise manage the information contained in identity records. Examples at USNH include the Banner HR system and each of the component institution's student information systems.

Incident: See Cybersecurity Incident

Information: Facts, data, or instructions in any medium or form.

Information Security: See Cybersecurity.

Information Steward: See Data Steward.

Information Technology Resource: Any hardware, software, firmware, equipment, internet of things (IoT) devices, applications, information systems, etc. used to access, capture, store, process, utilize, integrate, interface with, transmit, or otherwise manage information.

Institutional Information: Information, in any format, created, collected, recorded, captured, stored, processed, transmitted, or otherwise managed by or for the University System and its component institutions, to conduct USNH business.

Institutionally Owned Endpoint: A computer or computing device intended for end-user use purchased by the University System or one of its component institutions.

Integrity: Ensuring the authenticity of information—that information is not altered, and that the source of the information is genuine – and of information technology resources – that resources are functioning as intended, without any unauthorized modifications or alterations.

Internet Connected Device: A physical object that can connect to the internet including, but not limited to, desktop computers, laptops, tablets, smart phones, sensors, household appliances, and wearable technology like a smart watch.

Internet of Things (IoT): The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.

Keystroke Logging: The process used to record the keys struck on a keyboard without the knowledge of the user.

Least Functionality: Configuring information technology resources such that they provide only those capabilities needed to perform the activities assigned to them and restrict the use of capabilities, such as ports, protocols, or services, that are not essential to those activities.

Least Privilege: Access control strategy requiring that community members only be given access to the information, information technology resources, and specific capabilities within those resources, necessary to perform their job duties.

Local Authentication: Verification of an identity for the purposes of allowing access to a single information technology resource.

Locally Managed Account: A type of authorization created and managed on or for a specific information technology resource.

Log: A record of the events occurring within an organization's information technology resources and networks.

Logical Control: Tools and protocols used by information technology resources to enforce security measures.

MAC Address: A media access control address or MAC address is a unique hardware identification number that uniquely identifies each device on a network.

Mitigate: The effort to reduce loss by making a deficiency less severe and lessening the impact of potential damages.

Multi-factor Authentication (MFA): Access that requires the use of two or more different factors including (i) something you know (e.g., password/PIN); (ii) something you have (e.g., authentication app on a mobile device, token); or (iii) something you are (e.g., biometric).

Network Device: A piece of equipment that enables communication and data transmission between information technology resources across a network or networks. Examples include gateways, routers, wireless access points, networking cables, and switches.

Non-Primary Identity: A unique identifier established for a USNH community member that is separate from their primary identity. Examples of non-primary identities are Pool, Secondary, Service, System Administrator.

NTP: Network Time Protocol (NTP) is a protocol used to synchronize time on all participating information technology resources to within a few milliseconds of Coordinated Universal Time (UTC).

Out of Band: A circumstance where a different method (e.g., process, procedure, tool, etc.) or frequency is used or required instead of the standard method or frequency.

Password: A trusted secret compromised of "a string of characters (letters, numbers and other symbols) that are used" as part of confirming the identity of a person, device, or information technology resource.

Patch: An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

PCI-DSS: The Payment Card Industry – Data Security Standard (PCI-DSS) is a set of "operational and technical requirements" developed by the PCI Security Standards Council that defines required security practices for all "organizations accepting or processing payment transactions" or that develop information technology resources used to process them.

Personally Identifiable Information (PII): Any information about an individual that can be used to distinguish or trace an individual's identify and any other information that is linked or linkable to an individual.

Personally Owned Endpoint: A computer or computing device purchased by a USNH community member using money that was not provided by or associated with USNH or one of its component institutions.

Phishing: Tricking individuals into disclosing sensitive information by claiming to be a trustworthy entity in an electronic communication (e.g., internet web sites, email).

Physical Security: Safeguards used to protect the locations where information and information technology resources are stored or housed against unauthorized access.

Policy: High-level statement of principle intended to provide direction to the USNH community.

Portable Device: An endpoint device that is small enough to be carried from one location to another as part of regular use (e.g., laptop, tablet, mobile phone).

Primary Identity: The identity associated with a user's USNH username. Each individual person has only one primary identity across the entire University System of New Hampshire and its component institutions.

Privileged Access: An escalated level of permissions for an information security resource that is granted to community members that are responsible for the administration of those resources. administrative services such as system maintenance, data management, and user support.

Procedure: An established or official way of doing something.

PROTECTED Information: Tier 3 of the proposed USNH Information Classification Framework which includes information requiring safeguards and specific privacy handling procedures. It includes student information and educational records protected under FERPA.

Provisioning: Establishing the authorizations needed to enable access to a specific information technology resource (e.g., creating an account).

PUBLIC Information: Tier 1 of the proposed USNH Information Classification Framework which includes information specifically approved by data stewards for public distribution.

Quarantine: The process of restricting the ability of an information technology resource like an endpoint or a server to connect to network resources.

Remote Access: The ability for community members to access USNH information technology resources from external locations.

Removable Media: Any device whose primary purpose is to electronically store information that can be easily transported. Examples of removable media include USB flash drives, CD-ROM, DVD-ROM, external or portable hard drives, or any other portable computing device with storage capabilities.

Replay-Resistant Authentication: Configuration that protects against reuse of authentication information that is retransmitted with the intent of producing an unauthorized effect or gaining unauthorized access.

RESTRICTED Information: Tier 4 of the proposed USNH Information Classification Framework which includes information requiring specific security controls. It includes personally identifiable information like SSN and passport number, credit card information, and research information.

Risk: The probable frequency and probable magnitude of future loss.

Risk Acceptance: The formal process of documenting an acknowledgement of the details of a known risk that cannot or will not be mitigated.

Risk Assessment: A systematic process of identifying, analyzing, and documenting potential information security risks.

Risk Management: The program and supporting processes to manage risk to organizational operations (e.g., mission, functions, reputation), organizational assets (e.g., information, information technology resources), individuals, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a potential desired result.

Security Categorization: A risk management designation used across the USNH Information Security Program, to consistently express the criticality of an information technology resource or business process, based on the institutional information involved and the breadth of impact if that resource or process were compromised.

Security Configuration Baseline: An agreed configuration for a specific information technology resource designed to safeguard that resource.

Security Control: A safeguard or countermeasure prescribed for an information technology resource designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

Security Log: A chronological record of information technology resource activities, including records of system accesses and operations performed in a given period used for information security purposes.

SENSITIVE Information: Tier 2 of the proposed USNH Information Classification Framework which includes information requiring that can be shared when there are valid purposes to do so, but that cannot be shared publicly.

Segregation of Duties: A security principle that requires the use of one account for non-privileged access and a separate account to be used for privileged access to decrease the likelihood of, and potential for, unauthorized use of the privileged access.

Separation of Duties: A security principle that divides critical functions among different staff members in an attempt to ensure that no one individual has enough information or access privilege to negatively impact confidentiality, integrity, and/or availability.

Server: A "Server" is any device which provides service to other network devices regardless of the scale of those services. Specifically excluded from this definition for the purposes of this document:

1. Devices that provide individualized service to other devices, such a blue tooth devices. RF externals, etc.
2. Devices that provide service for the purpose of system management only (i.e. a device that provides service (like RDP or SSH) for the purpose of being managed by other systems)

Despite the exclusion of these types of devices, services provided by them must still be run securely and with up-to-date versions of software.

Service Account: An authorization that enables an information technology resource to communicate with and connect to another information technology resource.

Single Sign On (SSO): A capability that allows the use of one set of authentication credentials, like a username and password, to be used to access several information technology resources.

Spam: Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Standard: A published statement on a topic specifying requirements that must be satisfied or achieved in order to comply with a policy.

Susceptible: Likely or liable to be influenced or harmed by a particular thing.

Technology Service Owner: The individual within Enterprise Technology & Services (ET&S) responsible for operation and maintenance of an information technology resource.

Threat: The potential for a threat source to exploit (intentional) or trigger (accidental) a specific vulnerability.

Username: A unique character string used to designate a specific identity.

USNH Community Member: Any individual who has a relationship with the University System of New Hampshire or one of its component institutions including employees, students, applicants, prior students/alumni, donors, and sponsored users.

USNH ID: A unique nine-digit number used to designate a specific identity. Also called "9 Number".

Vendor: A third-party provider of an information technology resource or capability.

Vulnerability: Weakness in an information technology resource security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Waiver: A permanent (longer than one year) exemption from the requirement to comply with a Policy and/or Standard.