Southern
New Hampshire
University

Acceptable Use Policy

1 Introduction

Southern New Hampshire University (the University) makes available to its community information and information technology resources in support of our mission and the success of our learners. Our technology resources are valuable assets that must be used and managed responsibly to ensure the confidentiality, integrity, availability, and privacy of SNHU's institutional information and our technology ecosystem.

The University strives to provide a robust, resilient, and reliable information technology ecosystem. Because these resources are shared and limited, community members are required to use these resources responsibly, for their intended purpose, and in alignment with acceptable practices, and by their use, agree to comply with all applicable University policies; federal, state, and local laws; and contractual obligations.

The SNHU community includes faculty, adjunct faculty, staff, students, learners, senior leadership, members of the Board of Trustees (the Board), vendors, consultants, contractors, outside agencies and other external groups with which the University has relationships.

If an individual is in violation of the Acceptable Use Policy, the University may take the following action:

- Restriction of and possible loss of access or privileges
- Disciplinary action
- Termination of employment
- Termination of contract or other business agreement
- Expulsion from the University
- Requirement to repay costs incurred by the University
- Referral to law enforcement for legal action

2 Policy

2.1 Scope

This policy applies to the use of all technology resources owned, provisioned, entrusted to, managed by, or managed on behalf of the University, regardless of whether that use is for business reasons or for personal use. It includes, but is not limited to:

- User computers (e.g., desktops, laptops, tablets)
- Hardware (e.g., servers, switches, routers, storage media),
- Software (e.g., operating systems, business applications, licensed software)

- User accounts issued to enable access to any SNHU technology resource
- Technology Services (e.g., networks, voice communication, electronic messaging and collaboration tools)
- Institutional information in use by or entrusted to the University

Additionally, this Policy applies to the use of personally owned devices when those devices are used to conduct University business.

All SNHU community members who are granted access to or use of the University's technology resources and/or institutional information are subject to this Policy. This specifically includes anyone granted guest vendor access to any SNHU technology resource.

2.2 Purpose

This Policy establishes requirements for the use and management of SNHU's institutional information and technology resources to safeguard the confidentiality, integrity, and availability of these mission critical assets and preserve the privacy of institutional information.

2.3 Policy Statement

All institutional information and technology resources are assets of the University and shall remain the property of SNHU.

Members of the University community shall be individually responsible for the appropriate use of all technology resources assigned to them.

Members of the University community shall only access the institutional information and technology resources for which they have been authorized based on a valid business or educational need.

When an employee is issued a SNHU-managed user device (e.g., laptop, desktop), it is the institution's expectation this device will be used as the primary means to access SNHU content and conduct SNHU business.

Community members shall have no expectation of privacy when using University technology resources unless otherwise required by University policy or applicable law.

The University reserves the right to monitor all activity for compliance with this Policy and for security purposes (see the Security Monitoring Standard).

Acceptable Use

This section of the Policy defines the acceptable use of institutional information and technology resources at Southern New Hampshire University.

Acceptable use of institutional information and SNHU technology resources is always ethical, legal, and reflects academic integrity in accordance with the SNHU Code of Conduct. It adheres to all University policies and aligns with information security requirements and best practices. It supports our core values and is free from intimidation or harassment.

To ensure acceptable use of these University assets, each community member shall:

- Protect all SNHU credentials issued to them and all technology resources they are authorized to access from unauthorized use.
- Be responsible for all access to University technology resources using their credentials and/or any activity originating from their device (e.g., SNHU-issued laptop, personal laptop).
- Access only the institutional information and/or technology resources they have been authorized to access.
- Protect all SNHU institutional information, including digital and hard copy, in accordance with the Data Classification and Data Protection Policies and Standards.
- Use only legal versions of copyrighted software in compliance with vendor license requirements.
- Report any suspicious or unusual activity, unexplained service interruption or degradation, suspected theft, loss, or compromise of institutional information and/or technology resources to your supervisor or the Information Security Management Office immediately.
- Limit personal use of University technology resources to incidental, intermittent, and minor use that is consistent with applicable law and University policy, that does not expose the University to risk, and that does not interfere with University operations.
- Return University assets when separating from the University.

Requests for clarification on whether a specific use is acceptable or if a specific action is authorized can be directed to the Information Security Management Office (ISMO).

Prohibited Use

This section of the Policy defines use of institutional information and technology resources that is explicitly prohibited at Southern New Hampshire University.

Community members shall refrain from the following types of use which are explicitly prohibited:

- Use of institutional information or technology resources that is unlawful, in violation of University Policy or the Employee, Faculty or Student Handbook (e.g., use/behavior that is abusive, harassing, defamatory, profane, racist, or illegal).
- Enabling or allowing an unauthorized party to access University institutional information and/or technology resources.
- Exposing or disclosing institutional information categorized as Confidential to any unauthorized individuals (e.g., speaking, posting, or sharing it publicly, failing to position screen away from public view, failing to secure hard-copies, sharing passwords).
- Storage of Confidential: High Risk information on portable/removeable media (e.g. USB drives, external hard drives).
- Leaving a SNHU-issued user endpoint unattended and/or unsecured (e.g., without initiating screen lock, without logging out of the system).
- Failing to provide reasonable physical protection to University-issued assets to avoid theft.
- Attempting to circumvent any security controls or to gain access to institutional information or technology resources without authorization.
- Masquerading, impersonating others, or otherwise using a false identity in an attempt to obscure the identity of the community member or the identity of an endpoint or

other connected device while accessing or utilizing any SNHU technology resource.

- Changing or removal of any computer settings, software or controls that safeguard the confidentiality, integrity, or availability to institutional information and/or technology resources (e.g., antivirus software, group/active directory policies, system folder permissions, user permissions, screen lock settings, audit or log settings).
- Installation of any software on a University technology resource that is unauthorized.
- Deliberate introduction of malicious software to a University-issued technology resource (e.g., malware, hacking/cracking tools, anti-forensic or network tunneling software).
- Use of third-party technology resources for the capture, storage, processing, transmission, or management of institutional information categorized as Confidential without specific approval from the Information Security Management Office (ISMO).

Use of Personally Owned Devices

Use of a personally owned endpoint device (e.g., laptop, desktop, tablet, phones) to conduct SNHU business shall be subject to all aspects of this Policy.

Institutional information categorized as Confidential shall not be stored, in any form, on a personally owned device.

University staff using a personally owned device to access Confidential Information classified as Low Risk or Moderate Risk shall ensure the required security controls are implemented and in use (see Secure Configuration Standard).

Community members, regardless of their role, may not access the Confidential: High Risk Information of others from a personally owned device.

Although not required to do so, all SNHU community members are authorized to use personal devices for the purpose of validation such as for multi-factor authentication.

Personally owned devices of any kind shall not be used to take pictures or record video in any area of the University where a reasonable expectation of privacy exists (e.g., the gym, locker room, bathroom).

3 Roles and Responsibilities

Standard information security roles and responsibilities can be found in the Glossary (see link above under Definitions).

Roles and responsibilities specific to this policy are listed here:

Community Member:

- Follow all local, state, federal, and international laws and regulations and SNHU policies and standards governing access to and use of institutional information and technology resources.
- Respect the rights and privacy of other community members.
- Safeguard the confidentiality, integrity, and availability of SNHU institutional information and technology resources.

- Protect all SNHU-issued credentials (username and password).
- Report any suspicious activity related to enterprise or institution accounts, institutional information, and/or technology resources to the ISMO immediately.
- Avoid engaging in any prohibited use of institutional information and/or technology resources.
- Understand the ramifications of using a personally owned endpoint or other device to conduct University business.

4 Roles and Responsibilities

SNHU Community Members are expected to comply with the requirements defined in this Policy.

Violations will be subject to the University's applicable disciplinary policies and processes.

5 Exceptions

Requests for exceptions to this Policy shall be submitted to the ISMO for consideration and may, when warranted, be escalated to the Information Security Council (ISC) for review. The ISC may choose to elevate the exception request to the University's Leadership Council.