Acceptable Use Policy

1 Introduction

Southern New Hampshire University (the University) supports the lawful use of information technologies and data (technology assets). Technology assets must be used for their intended purpose in serving the interests of the University's educational, instructional, research, and administrative business while respecting the rights of other technology users and the integrity of the workplace.

The University community includes faculty, adjunct faculty, staff, students, 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

The University requires users to adhere to the Acceptable Use Policy.

Users of technology assets have access to valuable University resources and legally controlled and Confidential Information.

Technology assets issued by the University remain the property of the University. Members of the University community are individually responsible for appropriate use of all resources assigned to them. Members of the University community must have a valid business or educational need and authorization to access University technology assets.

Data created and/or stored on University assets remains the property of the University unless a policy exception applies. Users should have no expectation of privacy when using University systems unless otherwise required by University policy or applicable law. The University reserves the right to monitor all activity for security purposes (see the Security Monitoring Policy). When in doubt as to whether an action is authorized, please contact your direct supervisor or the University's Information Security Management Office (ISMO).

2.1 Scope

This policy applies to all users and technology assets owned, provisioned, entrusted to, or managed by the University. It includes but is not limited to computer equipment, hardware, storage media, software, business applications, data files, business licenses, operating systems, networks, as well as use of services such as internet, voice communication, computer accounts, electronic mail, collaboration tools, and data in use or entrusted to the University or any portion or subsidiary. It also extends to:

- The use of personally-owned devices for University business
- The use of University assets for personal business

2.2 Purpose

Members of the University community are expected to follow a standard of conduct in the use of computing resources. Use of technology assets must be ethical, comply with all laws and University policies, and be used for the purpose of achieving the University mission. Members of the University community must refrain from activity known to put the well-being of the University and its members at risk.

2.3 Roles and Responsibilities

All users are responsible for knowing and complying with University policies that apply to appropriate use of its technologies and resources to include this Acceptable Use Policy (see the Employee Handbook, Student Handbook, Faculty Handbook or other agreements in place). Members of the University community are required to use assets lawfully and are individually responsible for knowing the law.

3 Procedure

3.1 Acceptable Use

This section of the policy identifies the acceptable use of technology assets at Southern New Hampshire University to protect the user and the University community.

In making acceptable use of resources, individuals covered by this policy must:

- Use resources for authorized purposes and adhere to local, state, federal, and international laws governing the use of technology assets issued by the University.
- Protect user credentials and systems from unauthorized use. Each individual is responsible for all access to University technology assets by their credentials and/or any activity originating from their system.
- Access only the information to which you have been authorized or that is publically available using the appropriate account.
- Protect Confidential Information in accordance with the Data Protection and Data Classification Policies and Standards. Examples of Confidential Information include but are not limited to personally identifiable information (PII), protected health information (PHI), student data, financial aid data, bank account information, payment card data and other data such as intellectual property, confidential, and competition-sensitive information.
- Protect data that resides on or is transmitted to and from University systems in all forms to include but not limited to electronic data and hardcopy data.
- Use only legal versions of copyrighted software in compliance with vendor license requirements and comply with third-party agreements.
- Report immediately any suspicious or unusual activity, unexplained service interruption or degradation, suspected theft, loss, or compromise of technology assets to your supervisor or University point of contact.
- Limit personal use of University technology assets to incidental, intermittent and minor use that is consistent with applicable law and University policy. Personal use must never put the University at risk and must not interfere with University business or productivity. The University is not responsible for the confidentiality, integrity, or availability of personal content on University-issued assets. Examples include but are not limited to personal files, pictures, videos, sound files, personal software or software licenses, personal emails, eBooks, user credentials that access personal accounts, and other personal electronic files residing on a University-issued asset.
- Return University assets when separating from the University.

3.2 Prohibited Use

In making acceptable use of resources, individuals covered by this policy must not:

- Use technology assets unlawfully or in violation of University policy.
- Install unauthorized software or hardware on a University-issued asset.
- Allow access to University technology assets to an unauthorized individual (individuals who do not have a user account, or business relationship with the University).
- Leave your endpoint without initiating screen lock or logging out of the system or positioning screen away from public view when accessing Confidential Information.

- Speak confidential information publicly or to unauthorized individuals.
- Access, process or store Confidential Information if not authorized.
- Fail to provide reasonable physical protection to University-issued assets to avoid theft (ways of preventing theft include storing assets out of view, locking them up, and keeping them on your person).
- Attempt to circumvent security controls.
- Change or remove any computer settings, software or controls that provide confidentiality, integrity or availability to data or systems such as antivirus software, group/active directory policies, system folder permissions, user permissions, screen lock settings, audit settings, system services.
- Deliberately introduce to a University-issued asset unauthorized software such as malware, hacking/cracking tools, anti-forensic or network tunnelling software especially through the use of a personal (non-SNHU issued) email account (be cautious when accessing these email accounts from a University-issued device).
- Share University-issued passwords.
- Physically connect personally owned devices to University assets without prior authorization.
- Disclose confidential University information to an unauthorized entity or person.
- Attempt to gain unauthorized access to any University information system.
- Use of a University technology asset that conflicts with the Employee, Faculty or Student Handbook or University policy (including but not restricted to abusive, harassing, defamatory, profane, racist, or illegal behavior).
- Use of Cloud services not specifically approved via the Security Review risk management process (see the WISP).

3.3 Use of Personally-Owned Computing Devices

Users are required to adhere to local, state, federal and international laws governing the use of personally owned devices while on University property or while conducting University business regardless of location. An example is the New Hampshire Hands- Free Law.

University staff who have been authorized to access Confidential Information using their personally owned device must use reasonable security controls, including requiring authentication to access the device (PIN, password, biometric, encryption).

Users who are not authorized to use personal devices to access Confidential Information must not:

- Access, store, or record legally regulated University information on personal devices. Privacy data, payment card and bank account information, health data, and student data are examples of data regulated by law (see the Data Classification Policy and Standard for more information on protected data).

- Use personally owned devices of any kind to take pictures or record video in the gym, locker room, bathrooms, and any other area of the University where a reasonable expectation of privacy exists.

4 Related Documents

For a complete list of related documents, please see the University Administrative Policy Library.