Section: 500 ς Facilities	Subject: 560- Operations and Maintenance
Policy: Information Technology Acceptable Use	Approved: August 3, 2021
Policy #: CCS 562.07	
Approved: Susan Huard, Interim Chancellor	Effective Date: August 3, 2021

INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

I. Policy Statement

Information technology resources are used by individual employees, students, and other persons affiliated with the Community College System of New Hampshire (CCSNH) and its Colleges. These resources are to be used for educational and business purposes in serving the interests of CCSNH and its Colleges. Misuse of information technology resources poses legal, privacy and security risks and therefore it is important for all users to understand the appropriate and acceptable use of such resources. Effective security and protection is a team effort. It is the responsibility of every user to know this policy, the standards contained herein, and to conduct their activities accordingly.

II. Policy Purpose

This policy establishes the proper use of CCSNH information technology resources and makes IT Users aware of what CCSNH deems as acceptable and unacceptable use.

III. Scope of Policy

This policy applies to employees, students and any other person who has access to CCSNH information technology resources including computers, email, Internet, social media, the network and any other CCSNH information technology or storage system
. All IT Users are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with CCSNH policy and standards.

IV. Privacy

CCSNH reserves the right to monitor, duplicate, record, and/or log all use of CCSNH technology resources with or without notice. This includes, but is not limited to, email, Internet access, file access, logins, and/or changes to access levels. **IT Users shall have no expectation of privacy in the use of CCSNH technology resources.**

V. General Use, Access and Ownership

5.1 CCSNH Information Assets stored on electronic and computing devices, whether owned or leased by CCSNH, employees, students, or a third-party, remain the property of CCSNH. Computer and telecommunication equipment, software, operating systems, storage media, Intranet, network accounts providing electronic mail, Internet access and browsing, and related network systems, are the property of CCSNH. These systems are to be used for educational and business purposes serving the interests of CCSNH and i ih nBTal and

- Contain special characters (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/)

6.3 IT Users should not create passwords that:

- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
-

6.4 IT Users should not write passwords down or store them anywhere in their office or in a file on a computer system or mobile devices (phone, tablet) without encryption. Instead, IT Users should create passwords that can be remembered easily. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

6.5 All system-level passwords (for example: root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.

6.6 All user-level passwords (for example: email, web, desktop computer, and so on) must be changed at least once a year.

6.7 Passwords must not be shared with anyone, including administrative assistants, secretaries, managers, co-workers, and family members. All passwords are to be treated as sensitive, confidential CCSNH information.

6.8 Passwords must not be inserted into email messages or other forms of electronic communication or saved using the "Remember Password" feature of applications (for example, Internet browsers).

6.9 Any IT User suspecting that his/her password may have been compromised must report the incident and change all passwords.

VII. Unacceptable Use

7.1.3 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of software products that are not appropriately licensed for use by CCSNH.

7.1.4 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CCSNH or the end user does not have an active license is strictly prohibited.

7.1.5 Violation of federal, state or local laws and regulations regarding access and use of information resources (*e.g.*, Family Education Rights and Privacy Act, Gramm-Leach-Bliley Act, Computer Fraud and Abuse Act, code of professional conduct, etc.).

7.1.6 Except for Internet browsing, accessing data, a server or an account for any purpose other than CCSNH educational or business purposes, even if access is otherwise authorized, is prohibited.

7.1.7 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate CCSNH official should be consulted prior to export of any material that is in question.

7.1.8 Introduction of malicious programs into the network or server (*e.g.*, viruses, worms, Trojan horses, email bombs, etc.)

7.1.9 Using a CCSNH technology resource to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws and policies.

7.1.10 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data that the IT User is not an intended recipient of or logging into a server or account that the IT User is not expressly authorized to access. For purposes of this section, disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

7.3.2 When an employee is expressing his or her beliefs and/or opinions in blogs or