COMMUNITY COLLEGE SYSTEM OF NEW HAMPSHIRE
INFORMATION TECHNOLOGY
LOCAL ADMINISTRATIVE PRIVILEGE POLICY AND PROCEDURES

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 the inappropriate use of privileged accounts significantly contributes to breaches of information security. To reduce the risks associated with potential misuse, the issuance of privileged accounts for performing local workstation and systems administration functions must be restricted and controlled.

II. Policy Purpose

This policy establishes the criteria for which local administrative rights for a CCSNH desktop, laptop or other end-user device may be granted to a CCSNH Computer User and, upon granting of local administrative rights, the terms and conditions that will apply to such use of privileged accounts for performing local administrative functions.

III. Scope of Policy

This policy applies to employees, students and any other person who has access to CCSNH computers (computer users). All computer users are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with CCSNH policy and standards. Only computer users who have been specifically granted privileged access are allowed to perform local administrative functions.

IV. Definitions

Local administrative rights means computer access that allows a single user total control over the operating system and files on a specific computer. The user can perform the same activities as CCSNH IT support staff, but only on their assigned computer.

V. Local Administrative Rights Application Process

5.1 CCSNH and the Colleges Chief Information Security Officers must establish a local administrative rights management process to ensure that only authorized individuals working at their institution have total control of the operating system and files on their assigned computer. The process must at a minimum include:

5.1.1 Review of business need with direct supervisor prior to granting local administrative rights to those personnel who require such rights to perform their duties. Assessment of business need shall include review of availability of IT support staff to install or update software. When granting local administrative rights, the principle of least privilege will be strictly observed, *i.e.*, users will only be granted access to the minimum resources required for them to perform their official functions.

5.1.2 All users requesting local administrative rights (except for those who need access in the normal performance of their job responsibilities) must complete the Administrative Rights Access Form. The completed form will be reviewed and the need for local administrative access rights will be validated by the institution's Computer Information Security Officer.

5.1.3 A system for tracking and managing all users who have been granted local administrative rights shall be established, which shall include standard procedures requiring a recurring review and revalidation of all privileged access rights, at least annually.

5.1.4 Personnel who have been granted administrative access rights must adhere to all IT policies and lack of adherence may cause revocation of local administrative access rights.

VI. Requirements for Use of Local Administrative Rights Privilege

6.1 Users who are granted local administrative rights shall:

6.1.1 Use their administrative privileges only when needed to install or update software necessary to perform their job

6.1.2 Apply changes only to an end-user device assigned to them

6.1.3 Adhere to the end-user license agreement associated with any software added

6.1.4 Comply with all existing CCSNH policies including CCSNH Acceptable Use Policy

6.1.5 Ensure that their end-user device is properly connected to the CCSNH network so that it can receive scheduled software patches and upgrades

6.1.6 Take all reasonable steps to protect against viruses and other threats

6.1.7 Be responsible for restoring any applications, configurations and associated data beyond the standard base image in the event of any failure of the device