Nashville State
Community College

NSCC Policy 08-05-00 Authorization for Use

Purpose

The purpose of this policy is to assure that the use of computing resources is properly authorized in compliance with the goals of the College and with appropriate approvals.

Policy

1. Access to the computing system will be assigned and controlled by the Director of the Technology Services Division.

2. Any individual whose request for access is denied may appeal to the appropriate Vice President and ultimately to the President of the College.

3. Authorized use of the computing facilities includes:

    a. Work for the administrative units consistent with the goals and objectives of the College.

    b. Work for the instructional units consistent with the goals and objectives of the College.

    c. Approved contract work for outside agencies. This work must be approved in writing by the President or his designee. A copy of the contract will be filed by the Director of Computer Services.

d. Approved research work by faculty and staff. This work must be approved in writing by the President or his designee. A copy of the approval form will be filed by the Director of Technology Services.

e. Approved consulting work by faculty and staff. This work must be approved in writing by the President or his designee. Consulting work will receive the lowest priority and will be charged at the prevailing commercial rate. A copy of the approval form will be filed by the Director of Technology Services.

f. Work by students taking courses at the College which require use of computing facilities.

g. Courses which do not normally require the use of the computing facilities must be approved in writing by the instructor of the course and the appropriate division head. A copy of the approval form will be filed by the Director of Technology Services. These students will receive the same priority as other students at the College.

4. Any use of the computing facilities contrary to the above may be termed misuse and appropriate action will be taken. Appropriate action for students can include revoking the right to use the facilities, probation, suspension, financial assessment, or legal prosecution. Appropriate action for faculty and staff can include financial assessment and legal prosecution.

5. Software developed by faculty or staff on College time or equipment becomes property of the College. Any exception must be requested in writing and approved by the President. If the proper authorizations are not obtained, the employee may be charged for the unauthorized use of the resources. This charge will be at the current market rate for the estimated usage of the facilities.

6. The ability for non-TSD faculty or staff to install software or reconfigure computers when needed for instruction or the fulfillment of other job responsibilities not in

conflict with the above provisions and the college Acceptable Use Policy will be granted upon approval of the "Authorization for Local Computer/Device Administrative Permissions" (see following page).

Sources

TBR Policy 1:08:00:00 Section IV

Change Log

Date	Change	By
1/31/2017	Added section 6	PAK
1/31/2017	Added Authorization for Local Permission form	PAK
3/15/2017	Formatted for new policy format	PAK

Authorization for Local Computer/Device Administrative Permissions

Administrative Rights allow the user computer login account access to all of computer's/device's operational functions and allow the user to make configuration changes to it including loading and deleting software. Once your account has administrative rights, you then have a responsibility to maintain your computer/device to prevent malicious system intrusions, viruses, or malware from entering the NSCC network through it. In order to ensure security and properly maintain NSCC assets as required of TSD by the State of Tennessee and TBR, you must agree to adhere to the following requirements before these permissions may be established. Any violation of this agreement may result in removal of administrative permissions from your computer/device.

1. NSCC computers, devices, and its networks are state assets; hardware, software, and data on these systems are not to be considered personal property.
2. All usage of the computer/device and any software will be in accordance with the "NSCC Acceptable Use Policy" which can be found at the following link: https://www.nscc.edu/legal/acceptable-use
3. For the protection of NSCC networked systems as a whole, TSD maintains critical software updates, anti-virus software, and firewall settings using various clients that are pre-installed on all campus systems. The Microsoft SCCM, Dell Kace, Sophos Anti-Virus clients (or equivalent future products and systems), and their associated administrator accounts are not to be removed or modified in any way that would interfere with the ability of these applications to access or modify computers/devices for these purposes.
4. Additionally, no changes will be made to the "Technician" local administrator account, nor the local domain administrator accounts/groups. These accounts and groups are necessary to manage software, hardware, and to provide assistance should problems occur with the operating system, NSCC licensed software, and/or in the event the computer/device experiences network connectivity issues.
5. Local administrative rights will be granted via a separate account with a separate password (which cannot be reset via MyNSCC), with the login name format lastname_i.admin. This account will have no email access and may have other restrictions as determined by TSD based on the use case. The administrative account is to be used only for computer administrative tasks (i.e. software installation), and not for routine network access. The initial password for this account will be set by TSD and will require a change upon first login and every 30 days thereafter.
6. Once you have local administrator permissions to your computer/device, if additional software or configurations which are not part of the base image (not licensed by or installed by TSD) are installed, TSD **will not** be responsible for supporting or replacing the application(s)/configuration(s). Furthermore, in the event that said software or configurations cause issues resulting in your computer/device no longer functioning properly, TSD **will only** be responsible for restoring the system back to its original configuration as when you first received it.
7. TSD is not responsible for data backups, selective backups, or backup images. Hardware such as external hard drives or USB flash drives used for this purpose are the sole responsibility of the employee, and/or the employee's department and remain subject to the provisions of the NSCC Acceptable Use Policy.

Approved by President's Cabinet 6/14/21

I have read, understand, and agree to adhere to the above policy.

[Control]		
Print Employee Name	Employee Signature	Date
[Control]		
Print Supervisor Name	Supervisor Signature	Date
TSD Director’s Signature		Date
Account Name Created		Expiry Date
Technician’s Signature		Date