NCCU Computer Administrative Rights Policy

On Windows and Macintosh computers, a user requires special administrative privileges to:

- install software,
- modify system settings,
- manage users,

These tasks are restricted by default since they can have a profound impact on the stability and usability of a computer. Due to the availability of trained and experienced support staff and the inherent dangers of inappropriate, uninformed, or unintentional use of logins with administrative rights, the Information Technology Services (ITS) policy is to restrict the use of administrative rights.

The ITS policy on administrative rights is intended to support the goal of insuring the highest level of stability and usability for computers. This is based on the premise that computers are primarily a productivity tool where stability and usability are most important. In such an environment limiting administrative privileges is an ITS "best-practice" because change management is one of the foundations of providing a stable computing environment.

Administrative rights are typically reserved for Information Technology Services personnel who are responsible for providing administrative services such as system maintenance and user support. However, in unique instances, administrative rights may be issued to faculty and/or staff on either a temporary or ongoing basis to perform tasks within the scope of their employment. Users who have demonstrated the ability to configure and manage their workstations and who possess an understanding of the responsibility of maintaining appropriate security measures may be granted administrative rights on their computer. Users who have been granted administrative rights on their workstations are herein referred to as authorized users.

Authorized User Responsibilities

Authorized users are responsible for:

- changing their AD password every 90 days;
- maintaining the integrity of their workstation;
- any accounts they create on their own computer;
- maintaining software licensing information for any software personally installed on their workstation;
- routinely checking for and eliminating spyware, or any similar data gathering and reporting software, from their workstations;
- NOT sharing their username and password with others for access to the NCCU network;

- reporting any system failures and/or compromises in security measures to the Eagle Technical Assistance Center; and
- reading and adhering to the following ITS Policies:
    - NCCU Responsible Use Policy
    - NCCU E-mail Policy
    - NCCU Wireless and Network Security Policy
    - NCCU File Sharing Policy
    - NCCU Data and Information Policy

Authorized users must not install or use software that are considered insecure or that do not incorporate an encryption scheme. These include but are not limited to email applications, FTP clients, and Telnet applications that do not employ secure connections.

The Alternative to Authorized User Status

As an alternative to personally acquiring administrator rights on the workstation the ITS department highly recommends and fully supports contacting ETAC to schedule software installations.

Information Technology Services Terms of Support

The ITS department will continue to provide Microsoft system patches, application software patches, and antivirus updates through the system wide client management platform to all NCCU workstations. NCCU computer users must not block or in any manner disable and/or revise any services on the workstation that may prevent these and other routine maintenance procedures.

ITS will not be able to restore a configuration customized by the user. In the event of a computer failure, the ITS Eagle Technical Assistance Center (ETAC) will restore the original base image on the computer.

The base image includes an operating system and any software maintained by the ITS department. All documents that are synchronized to the network server will be restored if possible. All NCCU issued desktop machines must be administered in accordance with standard configurations, and all computers must:

- be joined to the NCCU Active Directory domain;
- have remote management software installed to facilitate administration and upgrades;
- have active properly configured anti-virus software;
- and have service packs or patches as deemed necessary by ITS staff

Note: Network monitoring and intrusion detection is performed as deemed necessary and appropriate by designated ITS staff.

Loss or Denial of Authorized User Status

If a user abuses his/her administrative access, ITS will revoke this access immediately and will restore the original base image on the computer. Abuse is defined as, but not limited to:

- downloading software that is malicious to the NCCU network;
- downloading unlicensed/illegal software;
- downloading copyrighted material without permission;
- downloading viruses and/or Trojans to the NCCU network that are specifically attributed to software installations/downloads and/or;
- public exposure to sensitive data
- not adhering to ITS policies and procedures as outlined in the aforementioned policies.

Violation of this policy or repeated support problems will result in revocation of the authorized user status and/or other sanctions.

Applying for Authorized User Status

For audit purposes, NCCU must have on file documentation showing that Administrative Rights have been formally requested and approved. If a NCCU employee, would like to apply for the authorized user status, they must follow these steps:

1. Complete and sign the Administrative Rights Request Form
2. Submit the form to ITS, Attn: Change Advisory Board
3. Receive approval from Change Advisory Board *(requests are reviewed every two weeks on Tuesdays)*.

Please complete this form and submit it by Interdepartmental Mail, faxing it to 530-7454, or delivering it to the ITS Receptionist on the 3rd floor of the H.M. Michaux, Jr. School of Education.

Note: All users will be automatically granted authorized user status on their NCCU issued laptop, unless the laptop is there main office laptop and at that time it will have to be reviewed by the Change Management Review Committee.

Administrative Rights Request Form

APPLICANT INFORMATION	
Full Name:	**NCCU Email Address:**
Unit Head Name:	
Dept. Name/Building:	
Room Number:	**Office Phone Number:**
Computer Asset Tag Number:	
Reason for Administrative Access (be specific):	

All signatures must be original, no stamps or "signed for."

I _____certify that I have completed this request fully and accurately to the
(enter full name)
best of my knowledge. I have read and agree to all policies referenced in the NCCU Computer Administrative Right Policy. I understand that approval for gaining authorized user status is to conduct official university business and that the information gained is not for personal or commercial purposes. I further understand that violation of this policy will result in immediate removal of my special rights and may result in additional administrative and/or legal action.

Applicant Signature: _____**Date:** _____

Unit Head Signature: _____**Date:** _____

Important Notices:

1. No access will be given without a completed Administrative Rights Request Form. Email and telephone requests **will be denied**.
2. This form must be completed electronically, except for signatures.
3. Forms with stamped or "signed for" signatures **will be returned**.
4. Forms with corrections, white outs, or changes **will be returned**. If you make a mistake complete a new form.
5. Questions regarding this form should be directed to the ETAC by calling (919) 530-7676.

Signature of Approving Official: _____**Date of Approval:** _____