1. Purpose
The purpose of this rule is to provide guidelines regarding the request for administrative privileges to a Windows and/or Macintosh computers for installing software, modify system settings, and manage users.

2. Rule
2.1 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 the inappropriate, uninformed, or unintentional use of logins with administrative rights, the University’s policy is to restrict the use of administrative rights.

2.2 The University’s 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 IT “best practice” because change management is one of the foundations of providing a stable computing environment.

3. Scope
3.1 Administrative rights are typically reserved for Information Technology Services (ITS) 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 granted administrative rights on their computer. Users who have been granted administrative rights on their workstations are herein referred to as authorized users.

3.2 Authorized users are responsible for:
3.2.1 changing their AD password every 90 days;
3.2.2 maintaining the integrity of their workstation;
3.2.3 any accounts they create on their own computer;
3.2.4 maintaining software licensing information for any software personally installed on their workstation;
3.2.5 routinely checking for and eliminating spyware, or any similar data gathering and reporting software, from their workstations; and
3.2.6 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 (ETAC).

3.3 An authorized user must not install or use software that is considered insecure or which does 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.

3.4 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.

3.5 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.

3.6 ITS will not be able to restore a configuration customized by the user. In the event of a computer failure, the ITS ETAC will restore the original base image on the computer.

3.7 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:

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

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

3.9 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:

3.9.1 downloading software that is malicious to the NCCU network;
3.9.2 downloading unlicensed/illegal software;
3.9.3 downloading copyrighted material without permission;
3.9.4 downloading viruses and/or Trojans to the NCCU network,
3.9.5 public exposure to sensitive data; and/or
3.9.6 not adhering to ITS policies and procedures as outlined in the aforementioned policies.

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

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

3.11.1 Complete and sign the Administrative Rights Request Form
3.11.2 Receive approval from Robert “Bob” Northcott and/or Joe Sanders
3.11.3 Submit the form to ITS, Attn: Robert ‘Bob’ Northcott and/or Joseph ‘Joe’ Sanders

3.12 Individuals who are interested in receiving administrative rights should complete the Administrative Rights Request form and submit it via Interdepartmental Mail, facsimile to 530-7650, or personal delivery to the ITS Receptionist on the third floor of the H.M. Michaux, Jr. School of Education.

3.12.1 All users who submit an Administrative Rights Request form will be automatically granted authorized user status on their NCCU issued laptop.

4. Rule Enforcement
If the user submits a request for administrative privileges, the user must read, understand and adhere to the following ITS policies contemporaneous with the request;

4.1. NCCU Responsible Use Policy
4.2. NCCU E-mail Policy
4.3. NCCU Wireless and Network Security Policy
4.4. NCCU File Sharing Policy
4.5. NCCU Data and Information Policy