FAYETTEVILLE STATE UNIVERSITY
POLICY ON
Computer Administrative Rights

Authority: Chancellor, Fayetteville State University

Category: Faculty & Staff

Applies to: Faculty, Staff, and Students

History: Approved on……
First Issued on…….

Related Policies: UNC Policy Manual 1400.1 – The Use of Information Technology

Information Security Policy
University Email Policy
Data Classification Policy

Contact for Info: Chief Information Officer – (672-1477)

---

1. INTRODUCTION AND POLICY STATEMENT

FSU provides desktops and laptops to faculty and staff to perform university related functions. This policy is intended to support the goal of insuring the highest level stability and usability of the FSU issued computers. This is based on the premise that computers are productivity tools where stability and usability are most important. In such environment limiting **administrative privileges** is an IT best practice because change management is one of the foundations of providing stable computing environment.

Administrative rights are restricted by default on all desktops and laptops since they can have a profound impact on stability and usability. 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 University's policy is to restrict the use of administrative rights.

Administrative rights are typically reserved for Information Technology Services (ITTS) 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 **power users**.

Power User Responsibilities

Power 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 FSU network;
- reporting any system failures and/or compromises in security measures to the ITTS Help desk; and
- adhering to all ITTS Policies

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

The Alternative to Power User Status

As an alternative to personally acquiring administrator rights on the workstation the ITTS division highly recommends contacting ITTS Helpdesk to schedule software installations.

Information Technology Services Terms of Support

The ITTS division will continue to provide Microsoft system patches, application software patches, antivirus updates, and application software updates through the SCCM client management portal to all FSU workstations. This pretty much covers most of the need for administrative rights. FSU 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.

ITTS will not be able to restore a configuration customized by the user. In the event of a computer failure, the ITTS Client Services group will restore the original base image on the computer.

The base image includes an operating system and any software maintained by the ITTS

department. All documents that are synchronized to the network server will be restored if possible. All FSU issued desktop machines must be administered in accordance with standard configurations, and all computers must:

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

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

Loss or Denial of Power User Status

If a user abuses his/her administrative access, ITTS 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 (intentionally or accidentally) that is malicious to the FSU network;
downloading unlicensed/illegal software;
downloading copyrighted material without permission;
public exposure of sensitive data
not adhering to ITTS policies and procedures.

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, FSU must have on file documentation showing that Administrative Rights have been formally requested and approved. If a FSU employee, would like to be granted the power user status, they must follow these steps:

1. Submit a formal request via e-mail articulating the need for such status
2. Receive approval from the CIO or Deputy CIO
3. ITTS Client Services staff member will configure the desktop and the user to have Power User status.

.