Local Administrator Rights Policy

As per section 5.2.2, item 17, of the Commonwealth of Virginia (COV) ITRM SEC 501-01, states that [the agency] require local administrator rights, or the equivalent on non-Microsoft Windows-based IT systems, be granted only to authorized IT staff.

Local administrator rights access gives users complete and unrestricted access to computers, including the ability to install any hardware or software and as such, are considered “privileged accounts”. The associated risks with this level of access include, but are not limited to:

- Users intentionally or unintentionally installing or download malicious code or software from unreliable sources potentially increasing the risk of exposure to exploits such as viruses, worms, spy-ware, keystroke loggers, phishing software and Trojan horses on campus computers, servers, and on the Commonwealth of Virginia (COV) network.
- Users intentionally or unintentionally making changes to the security configuration of the system making the system more vulnerable to attack.
- Users intentionally or unintentionally installing unlicensed software
- Users intentionally or unintentionally installing unapproved patches that could compromise the stability of the system

In lieu of the associated risks, TNCC has implemented the following mitigating controls:

- Restricted functionality of the classroom and lab computers through the use of group policies and installed the Deep Freeze application. Deep Freeze restores the computer to its original state after a user logs off.
- Network segmentation, in which classroom computers are in a demilitarized zone (DMZ) which isolates and prevents them from connecting to the college’s administrative network.
- Network Access Control (NAC) that verifies AV, patches, and updates; the NAC prevents users from accessing the network until user AV, patches, and updates are current.
- Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) solutions and a Checkpoint firewall.

Employees that determine they cannot perform their jobs without administrative rights must follow the procedure referenced in the following document: TNCC Logical Access Control - Account Management - Local Administrator Rights