Appropriate Use of Administrative Privileges

Purpose
The purpose of this document is to identify what is required of users given administrative privileges on a USFSP technology resource. All USFSP system administrators and users given administrative privileges are responsible for understanding and complying with this standard. If the conditions stated in this standard are not met administrative privileges will be revoked by Campus Computing.

Scope
This standard applies to all USFSP system administrators and USFSP employees given administrative privileges on a USFSP technology resource.

Device Management Responsibilities
Having administrative privileges comes with additional device management responsibilities. Users granted administrative privileges will be held accountable for the following mandatory device management responsibilities:

- Maintain the stability and integrity of the device by
  - installing updates to the Operating System, applications, and security software
  - routinely run scans for viruses and malware using USFSP standard security applications (Symantec Endpoint Protection and Cisco Source Fire AMP)
  - resolving basic system issues
  - performing regular backups of persistent data and ensuring retention schedules of data
  - disabling server services
- Purchase, manage, and license applications not licensed by the USF System and be able to provide proof of purchase or ownership of licenses to Campus Computing upon request
- Take adequate steps to protect the device (and data) from loss, theft, or damage
- Immediately report security compromises to Campus Computing
- In the event the device becomes unusable, return the device to Campus Computing to perform a system restore or refresh. Campus Computing will attempt to recover lost or damaged data.
- Submit the device to Campus Computing annually for a device security assessment
- Notify Campus Computing when administrative privileges are no longer required or when employment has ended

Appropriate Uses of Administrative Privileges
Administrative privileges should only be used when performing device management responsibilities or when performing the system administration tasks requested on the Local Administrative Privileges Request Questionnaire. A separate user account will be created and used for the sole purpose of performing device management and system administration tasks.
Inappropriate Uses of Administrative Privileges
Using administrative privileges requires a higher degree of responsibility. A user account with administrative privileges is NOT to be used to perform daily computing tasks. Administrative privileges can be revoked by Campus Computing for any of the following inappropriate uses of administrative privileges:

- Failure to adhere to USF System or USFSP policies, standards, procedures, or guidelines posted on [www.usf.edu/it](http://www.usf.edu/it) and [www.usfsp.edu/computing](http://www.usfsp.edu/computing)
- Violation of the [Florida Computer Crimes Act](http://floridacode.com) (Florida Statue, Chapter 815) or any other state or federal laws
- Performing unsafe computer practices that lead to a data or security breach such as installing malware or giving access to unauthorized persons
- Installing unlicensed or illegal software; not complying with End User License Agreements (EULAs); not complying with copyright laws
- Violating University user account policies and procedures such as sharing user account passwords, provisioning additional accounts, or changing account privileges
- Tampering with or removing University security and/or management software
- Preventing Campus Computing access to device resources such as altering system files or locking directories or files
- Connecting to a USFSP wired network without permission from Campus Computing
- Not performing device management responsibilities
- Requiring excessive support from Campus Computing or other technology groups as a result of having administrative privileges
- Accessing data or systems outside the scope of job responsibilities
- Sharing data or systems with unauthorized individuals
- Using access to satisfy personal curiosity about an individual, system, practice, or other type of entity