What is Administrative Rights Access?

Administrative rights access privileges on end-point computer devices are typically reserved for an institution's information technology personnel who are responsible for computer system maintenance and user support. This is because administrative rights access privileges allow a user to perform certain actions (e.g. install software, modify computer system settings, manage users, and run certain software) which can negatively impact the security, stability and usability of a computer, other CSUN computers, and the CSUN network. CSUN needs to ensure the highest level of security, stability, and usability for computers by limiting the use of administrative rights privileges to those users who have demonstrated a need, understand the responsibilities associated with this special access, and obtained MPP supervisor and Dean/VP or designee approval.

What are the CSU policies and standards governing administrative rights?

Per CSU Information Security policies, CSUN must ensure that any changes to a computer must go through a change control process and that local administrative rights must not be granted to the campus account used for activities such as web browsing. In addition per the 2016 Information Security Audit**,** CSUN was cited for **permitting local administrative rights which could allow disabling of security controls and the installation of unauthorized software.**

Per CSU policy and the audit, CSUN must ensure that computers

- Are created from a current standard secure configuration checklist.
- Have up to date anti-virus software installed and maintained on the computers. Regular updates to virus definitions and software must be activated
- Are configured to allow automatic application of software updates through a patch management system

Therefore, CSUN users with administrative rights must not block or in any manner disable and/or revise any services on the workstation that may prevent malware scans and other routine maintenance procedures.

Do I need Administrative Rights Access to Install Software?

As an alternative to acquiring Administrator Rights Access, CSUN has trained technology staff (central IT staff, college technical staff, Student Affairs technical staff) available to help install software on university-owned devices.

Responsibility of Users Granted Administrative Rights Access

Users who have been granted administrative rights access on their computer must:

- change their CSUN password every 90 days
- not interfere or disable any patching, software upgrades, malware checking or Level 1 data scanning
- purchase all software through central purchasing and maintain the license information for audit purposes

- conform to the End User License Agreement (EULA) associated with any software installed on their end point computer device. The EULA is a legal contract between the manufacturer and/or the software author and the end user of an application; it details how the software can and cannot be used and any restrictions that the manufacturer has. [Note that all End User License Agreements must be reviewed by a CSUN procurement unit (Purchasing, TUC, AS, USU, or University Foundation) - even for free software.
- routinely check for and eliminate spyware, or any similar data gathering and reporting software, from their workstations
- never share their username and password with others
- immediately report any system failures and/or security compromises to the IT Help Center
- read and adhere to the CSUN Acceptable use and Information Security policies
- never use their administrative rights userID to browse the web

How does Administrative Rights Access work at CSUN?

If your request for administrative rights is granted and additional userId for your computer(s) will be created by IT staff. You will receive an email with the special Administrative Rights userID which will be followed up by a phone call from IT staff with your password. This additional Administrative Rights userID is to be used only when you need to use administrative rights on your university-owned computer and only for the specific purpose the administrative rights were granted to you. Ordinarily, you will login using your regular CSUN userID credentials; you must not routinely login using your Administrative Rights userID.

Abuse of Administrative Rights Access

If a user abuses his/her Administrative Rights Access, CSUN will revoke the administrative rights access.

Abuse is defined as, but not limited to:

- downloading software that is malicious to the CSUN network
- downloading unlicensed/illegal software
- downloading copyrighted material without permission
- downloading malware to your machine that are specifically attributed to the use of administrative rights
- causing a breach of Level 1 or Level 2 data
- interfering with patches, upgrades or malware scans

How to Request Administrative Rights Access

For audit purposes, CSUN must retain documentation showing that administrative rights have been requested and approved. To apply for Administrative Rights Access, a CSUN employee must follow these steps:

1. Read this administrative request and understand the responsibilities of being granted administrative rights on your computer.
2. Complete and sign the Administrative Rights Request Form
3. Submit the form to iso@csun.edu

(This process will be available online later in 2019)

CSUN INFORMATION TECHNOLOGY	Administrative Rights Access Request Form

REQUESTOR INFORMATION
Name:
Employee ID:
Department Name:
Email Address:
Reason for Administrative Access ☐ **My productivity would be severely hampered by not having administrative rights.** ☐ **I need to run critical software that can only run using administrative rights (e.g. PeopleTools).** ☐ **Other (Please Specify)**

To be completed by Requestor
I have read this document and agree to all of the policies and standards referenced in this document. I understand that approval for gaining Administrative Rights Access is to conduct official university business as requested in this document. I understand that violations of the items listed above will result in removal of my administrative rights.

Requestor Signature: _____

Date: _____

To be completed by the Head of the Department or Unit:
I request granting of Administrative Rights Access to this individual on the basis of business needs articulated above:

Department or Unit Head Name: _____

Department or Unit Head Signature: _____

Date: _____

To be completed by VP/Dean or their Designee:
I approve granting of Administrative Rights Access to the above named individual and accept the risk on behalf of my division or college:

VP/Dean or Designee Name: _____

VP/Dean or Designee Signature: _____

Date: _____