WVSOM Local Administrative Authority

Statement of Use

WVSOM desktops and laptops are deployed to end users with accounts which limit and reduce their ability to affect operational security campus-wide. These normal accounts ***cannot*** alter firewall settings, change Windows system folders or enable/disable services. The user accounts are sufficient to allow end users to complete their daily work-related tasks.

Conversely, Local Administrative Authority associated to an account increases the risk factor when navigating the MY.WVSOM.EDU intranet and external internet sites across the campus network. It exposes the single end user computer, all other computers accessing the network, the network itself ***and*** servers to malicious programs including viruses, worms, spyware, trojan horses and other variants. It also opens up the potential for hacking which could breach confidential WVSOM data. Local Administrator accounts should only be used when absolutely necessary for unique software operability and software installations outside the normal scope of activity.

The Information Technology (IT) Department can generally create alternative methods for unique software operability. This may include registry changes, specific folder access permissions, configuration changes or batch programming to call the necessary executable files. For this reason, Local Administrative Authority will only be given under specific, defined circumstances where no viable alternative is found.

Steps for requesting and approving Local Administrative Authority accounts:

1. Completion of official request form with signature of requestor and immediate supervisor (faculty are absolved from supervisory signature) will be sent to the Chief Technology Officer. This form signifies acknowledgement of this statement of use, compliance to end user responsibilities and adherence to institutional policy GA-31 Acceptable Use.
2. The official request will include a narrative of the specific software requiring Local Administrative Authority or specific end user circumstance or job function necessitating it.
3. A review by the IT Department of the software and identification of a viable work-around.
4. A decision will be processed based on the outcome of the technical review for a work around.
5. Approval by the Chief Technology Officer, the Network Manager and Helpdesk Manager. Exception criteria for approval will include:
   a) No viable work-around for the unique software
   b) Special end user circumstance and/or job function such as working with open source software not requiring licensure.
6. If approved, creation of a local administrative account will occur within 30 days of the review process.
7. The end user assigned the account will review the Local Administrative Authority tutorial and indicate the date of completion by initialing the original request form. This must occur in conjunction with the IT Department creating the account on the computer.

If an end user is uncertain as to the risks, or preventative measures for those risks, requests for a Local Administrative Authority account should not be made.

Responsibilities of the end user approved for Local Administrative Authority; responsibilities required by the Information Technology Department:

1. The IT Department will create a new account on the end user's machine. This account will have Local Administrative Authority. Once the end user changes the password, the IT Department will not be able to remotely access this account.
2. The end user should not change any network settings and they will not be able to access the WVSOM domain from this account.
3. Only the IT Department staff will maintain Domain-wide administrator accounts.
4. The primary administrator password should not be altered; this is used by the IT Department only. Having Local Administrative Authority does not give the end user permissions to change the administrator password!
5. The Local Administrative account assigned to the end user is for installing and running local software applications which have no alternative workaround. The account assigned will conform to the Admin_NetworkUser (i.e. Admin_kransom) naming convention.
6. Operating under local administrative authority is a known security hazard. It is crucial that the security software and settings are kept up to date by the end user.
7. It is the end user's responsibility to ensure that only **legal** software is loaded on the computer. Remember that institutional computers are to be used for institutional business only. Installation of software for personal use is a violation of state law. ALL computers at WVSOM are subject to random audits and the end user may be asked to provide documentation for the software. Failure to comply with these directions will result in notification at the appropriate VP level and/or Dean for Academic Affairs, and may result in disciplinary action.
8. Under no circumstances will the end user uninstall software that has been installed by the IT Department.
9. The end user with an approved Local Administrative account will not modify the configuration of the operating system, including file and folder permissions, or hard drive encryption.
10. The Local Administrative account will only be used where administrator privileges are required. Usage of the computer for all other purposes must be under the separate, non administrator-level account originally assigned to the end user.
11. The end user agrees to abide by institutional policy GA-31 Acceptable Use of Information Technology Resources.
12. Loss of data or applications as a result of the use of local administrative authority by any administrative staff or faculty member is **not** the responsibility of the Information Technology Department.
13. In the event of a rebuild, rework, or reimaging necessitated by misuse of a Local Administrative account, the task will be undertaken as time permits.
14. The IT Department will **not** be responsible for backing up data or applications or reinstalling personal applications.
15. Reoccurrence of such events will result in the loss of the Local Administrative account assigned to the end user.
16. Any end user involved in a data or security breach related to the Local Administrative account assigned to them, will have the privilege revoked and the account disabled.
17. The Local Administrative accounts will be reviewed annually by the IT Department.
18. Users that no longer act in a role that requires the administrative privilege will have the account disabled.
19. All requests, subsequent approvals, or revocations will be documented and maintained by the IT Department.

Local Administrative Authority-Account Request and Approval Form

Requestor: ____ **Date of Request:** ______________

Title: ____

Email: ____

Make/Model/Serial Number: ____

Primary Location (Building & Room #:) ____

Detailed narrative specifying unique software and/or special need for Local Administrative Authority:

____

____

____

____

____

____

____

____

____

____

____

____

By signing this form you are acknowledging the statement of use of Local Administrative Authority and agree to abide by all responsibilities conferred with the account.

______________________________________ ______________________________________

Signature of Requestor **Signature of Immediate Supervisor**

(Not required for faculty!)

Information Technology Department Review

Assigned Technician: ____

TrackIt Ticket #:____

Date of Review: ____

Alternative to Local Administrative Account: _____**Yes** _____**No**

Explanation of results: ____

____

____

____

____

____

____

____

IT Approval Signoff:

______________________________ ______________________________

Network Manager **Helpdesk Manager**

______________________________ ______________________________

Chief Technology Officer **Date of Approval**

Local Administrative Account Assigned: ______________________________

Local Administrative Tutorial Reviewed: ______ **User Initials** **Date Reviewed:** _________