



Administrator Access Policy – Staff

Purpose

This document defines LMU policy regarding local administrator rights to LMU Staff on University workstations.

The University is committed to providing members of LMU community with reliable technology in stable operating condition while appropriately addressing the University needs and maintaining University system integrity and data security.

Levels of Access

There are two security access levels to a university owned computer: General and Administrator.

The General access level allows most administrative powers with some restrictions. Installation of software or hardware that makes changes to the underlying operating system will require the assistance of ITS. General Access Level will generally assure the highest level of stability for your computer.

Administrator access level allows the client to have complete and unrestricted access to the computer. This includes the ability to install any hardware or software, edit the registry, manage the default access accounts and change file level permissions. Manipulating these may cause serious stability issues with your system and if abused, may result in the cancellation of administrator access.

By default all LMU Staff members are assigned General access level rights on their individual workstations. Exceptions may be granted to staff members that require Administrator level access to perform a specific job related task. Requests for these exceptions must be submitted in writing with the approval of a Dean or division Vice President. The use of these rights and the level of access to the workstation are to be in accordance with the University Acceptable Use Policy.

Guidelines

- LMU workstations are University property and are intended for University business.
- Individuals will refrain from installing applications downloaded from the Internet or software not compatible with the workstation's operating system. Installation of these applications may damage files and expose LMU's network to virus attacks and malicious coding.
- Individuals will refrain from installing unauthorized software as it may monopolize local processor power, resulting in noticeable system slowdown or degradation of performance.
- Individuals will not install applications that may establish network share protocols which result an increase in bandwidth utilization. This prevents net congestion and degradation of performance across wide areas of the campus.



- Individuals should refrain from downloading applications (software) that are illegal or not licensed on University owned equipment.
- The University strongly recommends and encourages individuals to utilize the ITS support staff to install any software that is necessary on their workstation.
- Individuals will refrain from altering or removing any standard software as originally installed by ITS.
- Individuals with administrator level access must sign to acknowledge that they have read the University Acceptable Use Policy and Administrator Rights Policy. A signed copy will be kept on file in ITS.
- ITS is unable to troubleshoot non-standard applications.
- Non-standard software will be removed as part of a normal repair process if necessary to restore system functionality.
- ITS highly recommends that individuals save all documents in the 'My Documents' folder. If additional compartmentalization is required, subfolders may be created within the My Documents folder. In the event that the workstation operating system (OS) is compromised, ITS will run a back-up script which backs-up the contents of the 'My Documents' folder and other user configuration settings, then re-image the system to the original configuration or a similar configuration.
- All University workstations are configured with remote support software. This software allows ITS staff to remotely control the workstation if necessary for troubleshooting.
- ITS will not remotely access individuals' workstations for troubleshooting without the individuals approval.
- The occurrence of repeated instances of OS integrity problems may result in the removal of administrator level access.

Name (print)

Dept.

Extension

Signature of Requestor

Date

Signature of Dean or Dept. Head

Date



Administrator Access Policy - Faculty

This document defines LMU policy regarding local administrator rights to the LMU Academic Community on University workstations.

The University is committed to providing members of LMU community with reliable technology in stable operating condition while appropriately addressing the University needs and maintaining University system integrity and data security.

Levels of Access

There are two security access levels to a university owned computer: General and Administrator.

The General access level allows most administrative powers with some restrictions. Installation of software or hardware that makes changes to the underlying operating system will require the assistance of ITS. General Access Level will generally assure the highest level of stability for your computer.

Administrator access level allows the client to have complete and unrestricted access to the computer. This includes the ability to install any hardware or software, edit the registry, manage the default access accounts and change file level permissions. Manipulating these may cause serious stability issues with your system and if abused, may result in the cancellation of administrator access.

By default all members of the Academic Community are granted administrator access level rights on their individual workstations. The use of these rights and the level of access to the workstation are to be in accordance with the University Acceptable Use Policy. The following points are expressed in the Acceptable Use Policy and are of particular significance when paired with administrator access level rights.

Guidelines

- LMU workstations are University property and are intended for University business.
- Individuals should refrain from installing applications downloaded from the Internet or software not certified for use with the workstation operating system. Installation of these applications may damage files and expose LMU's network to virus attacks and malicious coding.
- Individuals should refrain from installing unauthorized software as it may monopolize local processor power, resulting in noticeable system slowdown or degradation of performance.
- Individuals should refrain from installing certain applications that may establish network share protocols which cause an increase in bandwidth utilization. The installation of such applications can cause net congestion and degrade performance accross wide areas of the campus.
- Individuals are to refrain from installing from any type of media or downloading from the web any unlicensed applications (software) on University owned equipment.



- The University strongly recommends and encourages individuals to utilize the ITS support staff to install any software that is necessary on their workstation.
- Individuals should refrain from altering or removing any standard software as originally installed by ITS.
- Individuals with administrator level access should sign to acknowledge that they have read the University Acceptable Use Policy and Administrator Rights Policy. A signed copy will be kept on file in ITS.
- ITS is unable to troubleshoot non-standard applications.
- Non-standard software may be removed as part of a normal repair process if necessary to restore system functionality.
- ITS highly recommends that individuals save all documents in the 'My Documents' folder. If additional compartmentalization is required, subfolders may be created within the My Documents folder. In the event that the workstation operating system (OS) is compromised, ITS will run a back-up script which backs-up the contents of the 'My Documents' folder and other user configuration settings, then re-image the system to the original configuration or a similar configuration.
- All University workstations are configured with remote support software. This software allows ITS staff to remotely control the workstation if necessary for troubleshooting.
- ITS will not access individuals' workstations without the individuals approval and only to solve a reported problem.
- The occurrence of repeated instances of OS integrity problems may result in the removal of administrator level access.

Name

Dept.

Extension

Signature

Date