

---

DIVISION: <b>Administration</b>	
SUBJECT: Administrator Access to Computers Policy	Page 1 of 3
Policy Number:	Supersedes: <b>Administrator Access Policy for Faculty/Staff</b>
Effective Date:	Previous Issued: <b>6/9/2003</b>

## 1.0 STATEMENT OF POLICY

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. Therefore, administrator access to LMU-owned computers will be restricted.

## 2.0 DEFINITION

None.

## 3.0 POLICY/PROCEDURE

This document defines LMU policy regarding local administrator rights on University workstations. The University is committed to providing members of the 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 an LMU-owned computer: General and Administrator.

**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 Information Technology Services (ITS). General Access Level will generally assure the highest level of stability for computers.

**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 the computer 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 by email to helpdesk@lmu.edu providing evidence of 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.

By default all Faculty are granted administrator access level rights on their individual workstations.

Administrator access will not be granted to generic user accounts for any reason.

DIVISION: <b>Administration</b>	
SUBJECT: Administrator Access to Computers Policy	Page 2 of 3
Policy Number:	Supersedes: <b>Administrator Access Policy for Faculty/Staff</b>
Effective Date:	Previous Issued: <b>6/9/2003</b>

## **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 code.
- 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 acknowledge that they have read the University Acceptable Use Policy and Administrator Rights Policy.
- 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 will result in the removal of administrator level access.

DIVISION: <b>Administration</b>	
SUBJECT: Administrator Access to Computers Policy	Page 3 of 3
Policy Number:	Supersedes: <b>Administrator Access Policy for Faculty/Staff</b>
Effective Date:	Previous Issued: <b>6/9/2003</b>
Last reviewed by: UTC	Date: February 2010
Approved by:	Date:
Denied/Postpone:	Date:
<i>Notes:</i>	