Computer Administrator Access Policy

PURPOSE

This document defines Texas Wesleyan University's policy regarding local administrator rights to University-owned computers and provides information related to the University's desire to provide the University community with secure, reliable technology in stable operating condition while balancing the need for individual empowerment in an academic environment.

SCOPE

The Computer Administrator Access Policy applies to all who are granted "Administrator" access on University-owned computers.

TERMS AND DEFINITIONS

Administrator access level allows the user 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.

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 IT. General Access Level will generally assure the highest level of stability for a computer.

POLICY STATEMENTS

By default all University employees are assigned General access level rights on University-provided computers.

Administrator level access may be granted to an employee whose job duties include system configuration or individuals whose physical location does not permit the Service Desk to update the employee's system configuration. Individuals fitting the specified criteria must submit and exception request. If approved, Administrator level access will be granted as long as the individual complies with the guidelines below. At any time, without prior notification, Administrator level access may be removed.

Guidelines

- University-owned computers are university property and are intended for university business and classroom activities.
- Individuals should only install software related to university business and classroom activities.

- Individuals should not install software that may damage files and expose University's network to virus attacks and malicious coding.
- Individuals should refrain from installing software that may result in a system slowdown or degradation of performance.
- Individuals should not install applications that consume network bandwidth and have the potential to cause network congestion and degradation of network performance.
- Individuals should not download or install applications (software) that are illegal, improperly licensed, or unlicensed on university owned equipment.
- Individuals who download or install applications (software), other than those included in the standard configuration for all university computers, are responsible for retaining and producing documentation of appropriate licenses.
- Individuals are responsible for re-installing and configuring all non-standard software, as necessary.
- If required to restore normal system functionality, non-standard software will be removed as part of a repair process.
- If a computer enabled with Administrator access is linked to a network performance issue, the computer will be restored to its original standard configuration.
- If a computer enabled with Administrator access results in repeated (three) service calls to restore system functionality, General access rights will be restored to the system.

RELATED DOCUMENTS

Exception Request form