Summary

This policy outlines the appropriate use of system administrator access to University of Western States ("UWS") computing and information resources and aids in the interpretation of requirements set forth in other UWS policies.

Scope

This policy applies to all university system and application administrators and any other personnel provided with system administrator access to university computing and information technology resources.

Definitions

System Administrator Access is defined as a level of access beyond that of a regular user.

To control the scope of system administrator account access, this provision applies only to applications that have system administrative permissions to workstations, servers and/or network infrastructure, such as Mobile Device Management, Antivirus, Remote Support, Patch Management, Public DNS, etc.

Appropriate Use of System Administrator Access

System Administrator Access to university computing resources may be used only for official university business. While Policy 3601 Acceptable Use of Information Systems permits reasonable personal use of computing resources, this is restricted to non-administrative activities. Use of System Administrator Access is consistent with an individual's role and job responsibilities. When an individual's role or job responsibilities change, System Administrator Access is revised

The following activities constitute appropriate use of system administrator access to UWS computing systems:

- Installing/updating software on workstations or servers
- Starting/stopping application services
- Creating/updating user accounts
- Initiating remote scan or remote wipe on workstations
- Remote Desktop access to servers

System Administrator access may not be used for purposes not defined by the guidelines in this policy or assigned job responsibilities. The following activities constitute inappropriate use of system administrator access to UWS computing systems:

- General web browsing
- Checking and responding to email
- Accessing systems and resources not required by job responsibilities
- Creating additional unauthorized admin accounts
- Circumventing or changing UWS security restrictions
- Accessing email or other messages, or accessing the browsing history of university employees, unless specially authorized by the university president.

System Administrator accounts reduce the risk of an attacker making unauthorized use of System Administrator privileges to discover and steal sensitive data or take advantage of vulnerabilities.

Regular user accounts may be used for “high risk” activities such reading email, web browsing, reading/editing documents, etc., which may increase the likelihood of account compromise.

Related Policies: Policy 3601 Acceptable Use of Information Systems
Policy 3606 User Account Retention

Keywords: access, system administrator