



Information Technology Services Policy

Title: Privileged Access

Created: April 20, 2007

Author: J. Bazeley

Version: 1.0

Scope:

This policy covers all Loyola employees who have knowledge of a root user, superuser, or administrator password on any Loyola servers.

Purpose:

To ensure that users are either logging on to Loyola servers with their username and password before escalating their privileges, or that they have a non-shared account that has escalated privileges. This will create an auditable trail of all activity on a system, regardless of whether the system supports privilege escalation after logon.

Policy:

System Access – Unix and Linux servers

All users who want to access a Unix or Linux system as a root user or superuser must first logon to the system with an ID that uniquely identifies them, and for which only they know the password to. After logging on, the user can then use the su command to login to a privileged account. By first logging on with their user ID, the user creates an audit trail for any changes committed by the privileged account. If a user has access to a root user or superuser password for a given system but does not have an individual user account on the system, an account must be created for them.

System Access – NetWare servers

NetWare does not provide the ability to move a user's privileges to an administrator or superuser after an initial logon as a normal user. Users who require superuser access to NetWare servers should have additional rights tied to their UVID.

System Access – Windows servers

Users who are part of the System Maintenance and Administration (SMA) team will access Windows servers through the approved administrative accounts. Passwords associated with administrative accounts must meet Loyola's password standards for privileged accounts and must be changed anytime a team member leaves the team. Users who are not part of the SMA team who require frequent administrator access to a Windows system must have an account on the system with administrator privileges which only they know the password to. Users who are not part of the SMA team who require infrequent access to a Windows server must work with the SMA team to obtain a temporary account with administrator privileges. This account will be disabled once the user has performed the task that they need to accomplish.

Policy adherence

Failure to follow this policy can result in disciplinary action as provided in the Staff Handbook, Student Worker Employment Guide, and Faculty Handbook. Disciplinary action for not following this policy may include termination, as provided in the applicable handbook or employment guide.

Exceptions:

If a user is unable to follow the above policies and must remotely access a Loyola server as a root user, superuser, or administrator, they must send an email to their supervisor indicating the reason why they must do this, the time of their login, the time of their logout, and their IP address.