Privileged Access Policy

Policy Title:
Privileged Access Policy

Responsible Executive(s):
Chief Information Security Officer

Responsible Office(s):
University Information Security Office

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

I. Policy Statement

This Privileged Access Policy covers all Loyola employees who have administrative access to any Loyola servers. In addition, please note that this policy covers all IoT devices. This policy was created to ensure 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.

II. Definitions

Not applicable.

III. 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. After logging on, the user can use the appropriate system command to elevate their account privileges. 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 super user 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 super user after an initial logon as a normal user. Users who require super user access to NetWare servers should have additional rights tied to their UVID.

System Access –Windows servers
Users who are part of the Server Operations 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 at regular intervals and anytime a team member leaves the team. Users who are

not part of the Server Operations team who require frequent administrator access to a Windows system must have an account on the system with administrator privileges to which only they know the password. Users who are not part of the Server Operations team who require infrequent access to a Windows server must work with the Server Operations 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.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Chief Information Security Officer	Enforcing the Privileged Access Policy at the University by setting the necessary requirements.

VI. Related Policies

Please see below for additional related policies:

- Security Policy

Approval Authority:	ITESC	**Approval Date:**	April 13th, 2015
Review Authority:	Jim Pardonek	**Review Date:**	June 14th, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu