Privileged Access Policy

Applies To:	All	Policy Number:	ITS-0036
Issued By:	AVP for IT	Policy Version Number:	1.0
Date Issued:	July 1, 2016	Last Review Date:	July 1, 2016
		Last Revised Date:	July 1, 2016

Scope
This policy covers all University employees who have administrative access to any University servers.

Purpose
To ensure that users are either logging on to University 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. 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 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 –Windows servers
Users who are part of the Network Services team will access Windows servers through the approved administrative accounts. Passwords associated with administrative accounts must meet the University's password standards for privileged accounts and must be changed at regular intervals or anytime a team member leaves the team.

Policy adherence
Failure to follow this policy can result in disciplinary action as provided in the ITS Departmental Policies & Procedures handbook. Disciplinary action for not following this policy may include termination, as provided in the applicable handbook or employment guide.

History and Updates
July 1, 2016: Initial Policy