Password Standard Policy

Applies To:	All	Policy Number:	ITS-0040
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
These standards cover the minimum password requirements for all electronic devices owned or leased by the University that can be protected by a password.

Purpose
To ensure that all electronic devices are secured by a password of a certain complexity, and to ensure that more sensitive devices have more complicated passwords.

Policy

User Passwords - All user passwords will be at least eight characters long. All passwords are required to contain at least one character and at one number. All passwords are required to be changed every 90 days. When a password is changed, it cannot be set to any of its previous 10 values.

Under no circumstances should a user password be shared with anyone – even trusted entities such as the ITS Help Desk Staff or your supervisor. If you need to share access to your account with your supervisor or for support purposes, you should be present and are to enter your own password.

Administrative Passwords - All passwords for administrative accounts, which have additional privileges beyond a normal user must adhere to the user password policy and may not be based on any word that is found in a dictionary. When an administrative password is changed, it cannot be set to its previous value. Administrative passwords cannot be provided to student workers.

Service Passwords - All passwords used to allow servers to communicate with one another in an automated fashion require stronger passwords as they are infrequently changed. They must be at least 12 characters long. Service passwords cannot be provided to student workers. Service account passwords must be changed whenever the administrator responsible for the account leaves the organization or changes roles.

Documentation of Administrative and Service Passwords for Business Continuity/Disaster Recovery
For business continuity and disaster recovery purposes, all administrative passwords are to be provided to the AVP for IT at the time they are established or updated. The AVP for IT will store these passwords in a locked safe and at the secured storage location where backup tapes are stored.

History and Updates
July 1, 2016: Initial Policy