Password Policy 8/17/08

1.0 Overview
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Western Carolina University's entire network. As such, all Western Carolina University (WCU) employees (including contractors and vendors with access to WCU systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope
The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any WCU facility, has access to the WCU network, or stores any non-public WCU information.

4.0 Policy
- All system-level passwords (e.g., root, enable, AD admin, application administration accounts) must be changed every 30 days.
- All production system-level passwords must be part of the global password management database administered by the Information Technology Division.
- General campus user Active Directory passwords:
  - Will have a maximum password age of 90 days (60 days for admin/system level accounts)
  - Will be a minimum of 8 characters
  - Will not contain the user accounts name or parts of the users full name that exceed two consecutive characters
  - Will contain characters from 3 of the 4 following categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (1 through 10)
    - Non-alphabetic characters (for example !, $, #, %, &)
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords for WCU accounts must be different from passwords for non-WCU access (e.g. personal email accounts, online banking accounts, etc.).
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- User-level and system-level passwords must follow the General Password Construction Guidelines found on the IT Division web site (www.wcu.edu/it).
- Passwords are not to be shared with anyone.
- If an account or password is suspected to have been compromised, report the incident to ITS Help Desk where a record of the incident can be created and tracked, and change all passwords

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action.

6.0 Definitions
Terms | Definitions
--- | ---
Application Administration Account | Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).