Adopted: 01/25/2011
Revised: 07/01/2016

UNIVERSITY OF CENTRAL ARKANSAS
NETWORK PASSWORD POLICY

RATIONALE

The University seeks to protect its data stored on University owned resources, cloud services, and internal servers from unauthorized access, use, alteration, modification, disclosure, deletion, destruction and/or removal.

UCA system accounts and passwords are the property of the University of Central Arkansas. No one shall disclose a UCA system password that has been assigned to them.

Accounts are assigned to specific individuals to grant access to services and information that can be sensitive or confidential. Account information may not be shared with anyone else. Disclosure of passwords can allow someone access to systems or information for which they are not authorized.

This policy is subject to revision annually or as needed.

POLICY

A. Related Policies and Laws

This policy does not supercede or replace UCA Board Policy 412. All **students and employees** should be familiar with this policy.

1. Board Policy 412 - http://uca.edu/board/files/2010/11/412.pdf

In addition to the above, all **employees** should also be familiar with the following policies:

1. Mobile Device Security Policy - http://uca.edu/it/files/2011/10/UCAMobileDevicePolicy-Adopted06022015.pdf

2. Policy for Computer Use Outside the United States - http://uca.edu/it/files/2016/02/UCAComputerUseOutsideoftheUnitedStates-02232016.pdf

3. Arkansas Computer Password Disclosure - Arkansas Code Ann. § 5-41-206 Unauthorized disclosure of passwords is a violation of state law and can be grounds for disciplinary action as set forth in the appropriate UCA handbooks.

B. Password Criteria

1. Passwords meant to provide access to UCA systems must have a minimum length of 8 characters. The password must consist of at least one of each of the

following: upper-case letters, lower-case letters, numbers, and special characters (the $ and % symbols can not be used in a password).

2. Passwords will expire every 90 days.

3. A new password may not be the same as any of the previous six passwords.

C. Password Lockouts

1. For security reasons, after three (3) unsuccessful login attempts, a user's account will be locked out.

2. Once an account is locked out, the user must call or visit the IST Help Desk to unlock the account.

HOW TO CREATE AN EASY-TO-REMEMBER STRONG PASSWORD

Passwords should not be easy to guess and should not utilize common words or phrases. Strong passwords provide the greatest protection to your account as they much harder to guess. Creating an easy-to-remember strong password is not terribly difficult.

The simplest way to create a strong password is to use a sentence or phrase that you will remember. Then take the first letter of each word to create the password. In order to make this a Valid and Strong password, replace certain letters with numbers and/or special characters. Here are some examples:

1. **Aps1ape!** is derived from the sentence "A penny saved is a penny earned."

    a. **A p**enny **s**aved **1**s **a p**enny **e**arned**!**

2. **W2thC@l!** is derived from the song lyrics "Welcome to the Hotel California."

    a. **W**elcome **2 t**he **h**otel **C@l**ifornia**!**

Please note, the above passwords are banned from use at UCA.