Adopted: 01/25/2011 Revised: 07/01/2016, 05/23/2017

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
2. Policy for Computer Use Outside the United States
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.
2. The password must consist of **at least three (3) of the following four (4)** criteria: upper-case letters, lower-case letters, numbers, and special characters.
3. Passwords will expire every ninety (90) days.
4. A new password may not be the same as any of the previous six (6) passwords.

Adopted: 01/25/2011 Revised: 07/01/2016, 05/23/2017

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 contact the IT Help Desk or visit password.uca.edu to unlock the account, or wait for 30 minutes.

HOW TO CREATE AN EASY-TO-REMEMBER STRONG PASSWORD

Although complexity of passwords is good; research shows that the more characters your password contains the harder it is for an attacker to compromise your password.

Passwords should not be easy to guess and should not consists of common words or phrases alone. 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.

There are several simple ways to create a strong password. First is known as letter replacement. Simply use the first letter of each word in a sentence or phrase that you can easily remember and replace certain characters in the password with special characters and/or numbers to create the password. Another method is to create what is known as a word salad. This method strings together several words, along with numbers and/or special characters, to create a strong password.