Adopted: June 6, 2017
Revised: November 28, 2017

University of Central Arkansas
User Account Management Policy

Rationale:

This policy governs the creation, management and deletion of user accounts; granting and revocation of authorized privileges associated with a user-account; and authentication by which users establish their rights to use a given account.

Scope

This policy applies to all accounts directly managed by the University of Central Arkansas (UCA).

Related Policies

This policy does not replace nor supercede any existing UCA policy or applicable local, state, or federal law. Policies related to this include:

- Board Policy 412 - http://uca.edu/board/files/2010/11/412.pdf
- UCA Password Policy
- UCA Remote Access Policy
- UCA Network Security Policy
- Arkansas Code Ann. § 5-41-206 - Arkansas Computer Password Disclosure

Policy

1. **Access Control**

    a. Unless otherwise authorized, the creation, deletion, disabling, and changes to user accounts and privileges must be carried out by trained and authorized IT staff.

    b. Directory usernames are automatically generated by the University's ERP system using the following format: first initial + last name + a sequential number. Except in the cases of a legal name change, or an employee having a legacy username (i.e. abc12345), usernames will not be changed. In either of these cases, the individual may request that another username be automatically generated by the University's ERP system using the same format as above. Under extraordinary circumstances, the CIO of the University may approve an exception to the above.

    c. An unalterable log will be kept of all account creations, deletions, and changes.

    d. Account details will only be divulged to the user after proof of identity has been established.

e. A review period will be established, at an appropriate level for each system, which minimizes information security risks yet allows UCA's business activities to be carried out.

f. Upon receiving a proper notification from UCA Human Resources regarding an individual's termination of employment, the employee's network account (and access to all associated services including by not limited to network and pool drives; learning management system; and ERP system; VPN; and email) will be disabled at close of business on the final day of employment.

    i Terminated employees may still access the relevant portions of the Self Service application pertaining to payroll, tax forms, leave information, and personal information by utilizing a non-network login credential provided by IT.

    ii In certain emergency circumstances, including but not limited to involuntary termination or suspension; incapacitation; or death, the employee's immediate supervisor may contact IT to request an immediate suspension of the employee's network account.

    iii A request may be made in writing (email is acceptable) by a terminated employee's immediate supervisor to the CIO of the University, to grant proxy access to the terminated employee's network account to another active UCA employee to ensure continuity of services and avoid lapses in communication to the university. This access may include local computer access; network drive and pool drive access; and/or email access.

    iv Employees who retire in good standing with the University, may request (with approval of their division Vice President) to retain access to their University email account. A procedure will be established by IT to facilitate the formal request to retain an email account.

2. Managing Privileges

a. A user account will have the least privilege which is sufficient for the user to perform their role within UCA.

b. Changes in the privilege of an account must be authorized by the UCA "owner" of the system to which the account affects.

c. Procedures shall be established to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the University.

d. Users' privilege rights will be periodically reviewed.

3. Authentication/Password Management

a. Whenever possible, Active Directory will be used by all users to authenticate their access for any UCA system.

b. The user responsible for their account will keep the accounts authentication details secret and will not divulge it to any other person for any reason.

c. The account must not be used by the user where there is a possibility that the account details may be revealed.

d. Passwords can only be changed by the user or suitably trained and authorized IT staff.

e. If a user suspects their password is no longer secret it must be changed immediately and the system “owner” notified.