COLLEGE POLICY: 466

INFORMATION TECHNOLOGY USER ACCESS CONTROL

PURPOSE

This policy provides a framework for the way in which user accounts and access privileges are created, managed, and removed. It includes how new users are authorized and granted appropriate privileges, as well as how these are reviewed and revoked when necessary and includes appropriate controls to prevent users obtaining unauthorized privileges or access.

SCOPE

This policy applies to all college employees, students, consultants, contractors, agents, and authorized users accessing who have access to any college information technology and information management systems.

RESPONSIBILITY AND AUTHORITY

Campus management is responsible for the oversight, implementation, and monitoring of user access control policies. All policies and procedures related to user access control practices are subject to approval by the UA Cossatot Chancellor's Cabinet, Board of Visitors, and UA System Board of Trustees.

The Director of Information Technology will ensure the user access control process is established, implemented, and maintained. Information Technology staff will continuously monitor and update procedural controls as needed.

POLICY

User access controls manage the access of users to system and network resources by granting users access only to the specific resources they require to complete their job-related duties. Access controls are necessary to ensure only authorized users can obtain access to system data and information technology systems.

1. General Requirements
   a. The college will provide access privileges to college information technology systems (including networks, systems, applications, and devices) based on the following principles:
      i. Need to access – users will be granted access to systems and resources that are necessary to fulfill their job roles and responsibilities.
      ii. Least privilege – users will be granted the minimum privileges necessary to fulfill their job roles and responsibilities.
2. Requesting User Access
   a. Requests for users' accounts and access privileges must be formally documented and appropriately approved.
   b. Requests for special accounts and privileges (such as vendor accounts,

application and service accounts, system administration accounts, shared / generic accounts, test accounts and remote access) must be formally documented and approved.

c. Application and service accounts must only be used by application components requiring authentication; access to the passwords must be restricted to authorized IT administrators or application developers only.

3. Access Control Requirements

    a. All users must use a unique user ID to access college systems and applications. Shared account access is not allowed unless special circumstances exist and have been documented and approved by management and IT.
    b. Passwords must be set in accordance with the password requirements of the system or application being accessed. The use of strong passwords, where available, is required. Sharing passwords is strictly prohibited per College Policy 465 Acceptable Use of Information Technology Resources.
    c. Some systems and applications may require an additional verification step via multifactor authentication (MFA). This additional step requires the use of an authenticator application on a mobile device or a phone call to a mobile device or office phone. The MFA requirement is not optional and is required for all employees.
    d. System sessions are configured to lock after 15 minutes of inactivity.
    e. User access and privileges may be revoked at any time

4. User Access Audit and Review

    a. Existing user accounts and access rights will be reviewed annually to detect dormant accounts and accounts with excessive privileges.
    b. Existing user accounts and access rights of employees who change job roles and responsibilities will be reviewed immediately at them time their job duties change.
    c. Access rights will be immediately disabled or removed when the user is terminated or no longer has a legitimate reason to access designated systems.
    d.

5. Remote Access

    a. The college will provide remote access privileges to information technology systems (including networks, systems, applications, and devices) based on the following principles:
        i. Need to access – users will be granted access to systems and resources that are necessary to fulfill their job roles and responsibilities.
        ii. Least privilege – users will be granted the minimum privileges necessary to fulfill their job roles and responsibilities.
        iii. Remote access must be secured using an encrypted connection via our VPN client software.

iv. Multi-factor authentication is required for all remote access users.
v. User remote access privileges may be revoked at any time.

6. Policy Exceptions

   Exceptions to this policy must be documented and formally approved by the IT Director. Policy exceptions must describe:

   a. The nature of the exception.
   b. A reasonable explanation for the why the policy exception is needed.
   c. Risks created by the policy exception.

RELATED DOCUMENTS

NIST IR7316, Assessment of Access Control Systems
NIST SP 800-39, Managing Information Security Risk

Policy History:
May 5, 2025
March 7, 2022

User account provisioning and management encompasses five major actions:

1. New account creation for employees:

    a. The new employee is onboarded by HR. Once the hire process is completed, the user’s Active Directory account will be provisioned automatically by the ERP system.

    b. HR will submit a New User Account Request Form on behalf of the supervisor.

    c. DISS will process the account request form~~s~~ and complete the account creation process. Once processed, the contents of the New User Account Request Form will be dynamically populated to a list hosted on the DISS SharePoint site. This list will be used to document account creation process.

    d. The employee will receive a welcome email to the personal email address they provided during onboarding. This email will contain a link to College Policy 465 – Acceptable Use of Information Technology Resources, a link to activate their account and create a new password, and instructions on how to setup multifactor authentication on their device.

2. Modification of existing accounts:

    a. When an employee changes titles/positions within the college, all account privileges, permissions, and group memberships of the employee will be audited and adjusted as needed by DISS.

    b. HR will submit a User Account Audit Form on behalf of the employee.

    c. DISS will evaluate the User Account Audit Form and make necessary modifications to the account as necessary. Modifications to the account will be documented in the User Account Audit list hosted on the DISS SharePoint site.

3. Retirement of existing accounts:

    a. When an employee leaves the college, the supervisor will submit an “Account Deletion Form”.

    b. The user’s Active Directory account will be automatically disabled by the ERP account provisioning service on the date of termination.

    c. Once the account is disabled, DISS will remove all security and group memberships from the account and reset the password. LMS accounts will also be disabled.

   d. If a terminated employee is rehired, the supervisor will restart the account creation process at step 1.

4. Maintenance of existing accounts:

   a. DISS is responsible for the maintenance of user accounts for all UA Cossatot systems.

   b. Account audits will be conducted by DISS at least once a year to ensure stale accounts are removed and existing accounts are properly maintained.

5. Third Party/Vendor Access Accounts

   a. Third-party and vendor access to UA Cossatot systems will be provided as needed.

   b. Requests for third-party and vendor accounts will be submitted and tracked via our ticketing system.

   c. Requests for third-party and vendor accounts will be reviewed and approved by the IT Director.

   d. Accounts will be created with the principle of least privilege.

   e. Accounts will only be available for the duration of the project or support session. Accounts will be disabled upon completion.

   f. IT will perform regular user access reviews of these accounts.

6. Requesting Remote Access

   a. Submit a technology work order request in our ticketing system. Include the following information in the request:

      i. The system(s) to be accessed remotely.

      ii. The reason for requesting remote access.

   b. IT will review the request for remote access.

      i. If the request is approved, the user account and user device will be configured for remote access.

      ii. If the request is denied, the user will be notified.

Procedure History:

April 7, 2025
December 9, 2024
October 3, 2022
February 7, 2022