COLLEGE POLICY: 466

INFORMATION TECHNOLOGY USER ACCESS CONTROL

Purpose

This policy provides a framework for how 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 from obtaining unauthorized privileges or access.

Scope

This policy applies to all college employees, students, consultants, contractors, agents, and authorized users who have access to any college information technology or 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 meet the following requirements:
        i. Minimum length of 14 characters
        ii. Meet complexity requirements including upper- and lower-case letters, numbers, and special characters.
        iii. Pass Entra ID Password Protection requirements. This prevents the use of common, easily guessed passwords, or passwords found from previous breaches.
        iv. Should be unique and not reused.
        v. Passwords never expire unless account credentials have been compromised.

        Sharing passwords is strictly prohibited per College Policy 465 Acceptable Use of Information Technology Resources.

    c. Multifactor Authentication (MFA) is required for all user accounts, including guest accounts. MFA is implemented via Microsoft Entra ID using the Microsoft Authenticator mobile app. If the user does not have a mobile, or the mobile device is incapable of installing the Microsoft Authenticator App, a physical hardware key will be assigned to the user.

    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 the time their job duties change.

c. Access rights will be immediately disabled or removed when the user is terminated or ceases to have a legitimate reason to access designated systems.

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 why the policy exception is needed.

    c. Risks created by the policy exception.

Policy History:
November 2, 2026
May 5, 2025
March 7, 2022

PROCEDURE: 466-1

USER ACCOUNT PROVISIONING AND MANAGEMENT

User account provisioning and management encompasses four major actions:

1. New account creation for employees (account provisioning):

    a. New employee accounts are automatically provisioned by the ERP system during the onboarding process.

    b. To track account provisioning, HR user account provisioning ticket in the IT ticketing application. The supervisor is responsible for ensuring that the employee has read and agrees to the terms set forth in Policy 465 Acceptable Use of Information Technology Resources.

    c. DISS will process the account request ticket and complete the account creation process. Once the creation process is completed, the account request ticket will be closed.

    d. HR will receive a notification that the account request ticket is complete so they can complete the onboarding process.

2. Modification of existing accounts (account review):

    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. To track account changes, HR will submit a user account review ticket in the IT ticketing application.

    c. DISS will complete the account review process and adjust the account as needed. Once the process review is complete, DISS will close the ticket.

    d. HR will receive a notification that the account review ticket is complete.

3. Retirement of existing accounts (account deprovisioning):

    a. If a user account needs to be deprovisioned, HR will submit an account deprovisioning ticket in the IT ticketing system.

    b. The user's Active Directory account will be automatically disabled by the ERP account provisioning service at midnight 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. HR will receive a notification that the account deprovisioning ticket is complete.

e. If a terminated employee is rehired, HR 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. All vendors or third parties requesting access to institutional data or systems must undergo a security assessment before engagement. Assessment includes a review of the vendor/third-party Security Scorecard profile, if available. Other documentation required for assessment may include security certifications, penetration and vulnerability testing results, and security incident history. Vendors must maintain appropriate cyber insurance coverage. Vendors or third parties found to be at high risk via the Security Scorecard profile or requested security documentation, will not be granted access.

    b. Vendors or third parties requesting accounts or access to systems with institutional data must specify data handling requirements, security obligations, breach/incident notification procedures, and audit rights. Agreements must prohibit use of institutional data for vendor purposes and require return or destruction of data upon contract termination.

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

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

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

    f. Vendor/third-party access to systems is granted through Entra ID guest accounts with conditional access policies enforcing MFA on all accounts. These accounts may have additional security or conditional access policies applied to them.

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

h. Vendor/third-party accounts will be reviewed at least annually, during contract renegotiation, or after an identified security incident.

6. Requesting Remote Access

    a. Submit a technology work order request in our IT 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:

September 21, 2026
April 7, 2025
December 9, 2024
October 3, 2022
February 7, 2022