UADA Policy 415.4
Division Information Technology Security: Identity and Access Management

Purpose

The Identity and Access Management Policy determines the settings used for limiting access to the University of Arkansas System, Division of Agriculture (UADA) computer systems and information stored on those systems. The controls listed provide guidance on account management and privilege assignments. The guidance defines the assignment of roles and associated business functions. Other controls include login time, screen saver requirements, and similar activity-based controls. This policy establishes a minimum expectation, with respect to access controls, in order to protect data stored on computer systems at UADA.

Scope

This policy applies to UADA employees, faculty, staff, temporary employees, students, contractors, vendors, volunteers, and other personnel responsible for owning and managing UADA records and documents.

Policy

Division Information Technology Services (DITS) shall develop, disseminate, and periodically review and/or update formal, documented organization policies for access control and procedures to facilitate the implementation of the access control best practices.

General

- UADA will control user access to information assets based on requirements of individual accountability, need to know, and least privilege.
- Access to organization information assets must be authorized and managed securely in compliance with appropriate industry practice and with applicable legal and regulatory requirements (e.g., Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, identity theft laws, etc.).
- Organization information assets include data, hardware, software technologies, and the infrastructure used to process, transmit, and store information.
    - Guest/unauthenticated access may be provisioned commensurate with usage and risk.
    - Authorized users accessing organization computing resources and network with their own personal equipment are responsible for ensuring the security and integrity of the systems they are using to establish access.

Access Controls

- Access to information assets must be restricted to authorized users and must be protected by appropriate physical, administrative, and logical authentication and authorization controls.
- Protection for information assets must be commensurate with the confidentiality of the information.

- Each computer system shall have an automated access control process that identifies and authenticates users and then permits access based on defined requirements or permissions for the user or user type.
- All users of secure systems must be accurately identified, a positive identification must be maintained throughout the login session, and actions must be linked to specific users.
- Access control mechanisms may include user IDs, access control lists, constrained user interfaces, encryption, port protection devices, secure gateways/firewalls, and host-based authentication.

User Identification, Authentication, and Accountability

- User IDs
    - The access control process must identify each user through a unique user identifier (user ID) account.
    - User IDs are assigned by DITS.
    - Users must provide their user ID at logon to a computer system, application, or network.
- Individual Accountability
    - Each user ID must be associated with an individual person who is responsible for its use.
- Authentication
    - Authentication is the means of ensuring the validity of the user identification.
    - All user access must be authenticated.
        - The minimum means of authentication is a personal secret password that the user must provide with each system and/or application logon.
        - All passwords used to access information assets must conform to certain requirements relating to password composition, length, expiration, and confidentiality.
        - Multifactor authentication (MFA) is required.

Access Privileges

- Each user's access privileges shall be authorized on a need-to-know basis as dictated by the user's specific and authorized role.
- Authorized access will be based on the least privileged.
    - This means that only the minimum privileges required to fulfill the user's role will be permitted.
    - Access privileges must be defined to maintain appropriate segregation of duties to reduce the risk of misuse of information assets.
    - Any access granted to data must be authorized by the appropriate data custodian.
- Access privileges should be controlled based on the following criteria, as appropriate:
    - Identity (user ID);
    - Role or function;
    - Physical or logical locations;
    - Time of day, week, month;
    - Transaction-based access;

  - Access modes such as read, write, execute, delete, create, and/or search.
- Privileged access (i.e., administrative accounts, root accounts) must be granted based strictly on role requirements.

Access Account Management

- User ID accounts must be established, managed, and terminated to maintain the necessary level of data protection.
- The following requirements apply to network logons, as well as individual application and system logons, and should be implemented where technically and procedurally feasible:
  - Account creation requests must specify access either explicitly or for a role that has been mapped to the required access.
  - Accounts must be locked out after a specified number of consecutive invalid logon attempts and remain locked out for a specified amount of time or until authorized personnel unlock the account.
  - User interfaces into secure systems must be locked after a specified system/session idle time.
  - Systems housing or using restricted information must be configured so that access to the restricted information is denied unless specific access is granted.
  - Access must be revoked immediately upon notification that access is no longer required or authorized.
    - Access privileges of terminated or transferred users must be revoked or changed as soon as possible.
    - In cases where an employee is not leaving on good terms, the user ID must be disabled simultaneously with departure.
- User IDs will be disabled after a period of inactivity that is determined appropriate by the current business process.
- All third-party access (contractors, business partners, consultants, vendors) must be authorized and monitored.
- Appropriate logging will be implemented commensurate with sensitivity/criticality of the data and resources.
  - Logging of attempted access must include failed logons.
  - Logs should be monitored and regularly reviewed to identify security breaches or unauthorized activity.
  - Logs should be maintained for a specified period of time.
- An annual audit of secured systems must be conducted to confirm that access privileges are appropriate. The audit will consist of reviewing and validating that user access rights are still needed and are appropriate.

Access Removal - Immediate or Emergency Termination

In the event of immediate or emergency termination of an employee, contractor, or third-party user, the following steps must be taken to ensure the security of the organization’s information systems:

- In the event of involuntary terminations, the UADA Human Resource department will notify DITS upon the decision to immediately terminate access by emailing div-it-terminations@uada.edu.
- DITS must revoke all access privileges, including but not limited to:
    - Network access
    - Email accounts
    - Application access
    - Physical access to premises
- All user accounts must be deactivated within one hour of the involuntary termination notice.
- All company-owned devices must be retrieved from the terminated individual.
- Conduct an audit to ensure all access points have been secured and no unauthorized access remains.

User Access Review

- Conduct user access reviews yearly.
- Review all user accounts, including employees, contractors, and third-party users.
- Verify that access levels are appropriate for current job responsibilities.
- Document any changes made during the review process.

Compliance and Enforcement

- From 920.1 - This policy applies to UADA employees, faculty, staff, temporary employees, students, contractors, vendors, volunteers, and other personnel responsible for owning and managing UADA records and document who are permitted access.
- Persons in violation of this policy are subject to a range of sanctions, determined and enforced by UADA management, including the loss of computer network access privileges, disciplinary action, dismissal from the institution, and legal action.
- Some violations may constitute criminal offenses, per Arkansas and other local and federal laws. The organization will be responsible for reporting such violations to the appropriate authorities.

Accountability and Contacts

The Chief Information Officer for UADA is charged with the responsibility to periodically review the policy and propose changes as needed.

Reference Documents

UADA Account Provisioning Guidance and Procedure
UADA Identity and Access Management Procedure