Rule R4-004D: Access Management

Revision 2. Effective date: September 12, 2023

I. Purpose and Scope

A. Purpose

The purpose of this Access Management Rule is to outline the requirements for authorizing, authenticating, terminating, and reaccrediting access to the University's Information Systems and Information Assets and to outline the requirements for password management.

B. Scope

The scope of this rule is all University administrative units, including colleges, divisions, departments, and centers, and all members of the University community, including students, staff, faculty, other permanent or temporary employees, contractors, research collaborators, vendors, and third-party agents.

This rule supports section D, titled Access Management, of the University of Utah Information Security Policy 4-004.

II. Definitions

The definitions provided in Policy 4-004 apply for this rule.

III. Rule

A. Account Authorization

1. Prior to granting a User access to any University Information System that creates, stores, processes, or transmits Restricted or Sensitive Data, the Account Provisioner shall implement the following Controls:

   a. confirm that the request for User access has been appropriately authorized;

   b. confirm that the level of access requested is:

      i. appropriate for the User's job description and job function; and

      ii. appropriate for the Information System and/or the Information Asset;

   c. assign the appropriate role-based access to the User based on business role and job function; and

   d. maintain a log of Users' access to the Information System.

2. Account Provisioners may not grant a User permanent administrative rights or permissions on an assigned Workstation without an exception to policy as described in Policy 4-004.

B. Account Authentication

1. All University IT Resources, IT Systems, and Electronic Resources must use the Information Security Office's authentication services wherever technically feasible.
2. Account Provisioners shall assign each User a unique Account.
3. Wherever technically feasible, two-factor authentication (2FA) or multifactor authentication (MFA) shall be used.
    a. Users may only enroll devices for 2FA that belong or have been assigned to them personally and may not share 2FA tokens.
    b. If a User receives a 2FA or MFA prompt for the User's Account that the User did not initiate, the User shall decline the prompt.

C. Account Modification and Termination

1. User employment status changes shall be immediately communicated to the appropriate Account Provisioner.
2. Upon notification that a User has changed job roles within the University or has terminated a contract or employment with the University, Account Provisioners shall modify, remove, or disable the User's access to the University's Information Systems as appropriate.
3. Certain events may require that a User's access rights be immediately removed. In these situations, as directed by the cognizant authority, the User's rights shall be revoked, and the respective help desk notified immediately.

D. Account Reaccreditation

1. At least annually, Account Provisioners shall review User access rights to University Information Systems to confirm that each User for whose access the Account Provisioner is responsible has the authorized and appropriate level of access.

E. Password Management

1. When managing passwords, the following are required:

   a. configuration of passwords to be a minimum of 14 characters – passphrases are encouraged;

   b. issuance of temporary passwords via a secure method;

   c. temporary passwords shall be changed on first login;

   d. temporary passwords shall be unique;

   e. all default vendor passwords shall be changed at first login;

   f. passwords may not be hard-coded or stored on Information Systems in an unprotected form;

   g. if any Account is suspected of being compromised, the password shall be changed immediately; and

   h. passwords shall be kept confidential. Sharing a password is a violation of this policy.

Sections IV- VII are for user information and are not subject to the approval of the Academic Senate or the Board of Trustees. The Institutional Policy Committee, the Policy Owner, or the Policy Officer may update these sections at any time.

IV. Policies/ Rules, Procedures, Guidelines, Forms, and other Related Resources

A. Policies/ Rules.

1. Policy 4-004: University of Utah Information Security Policy

B. Procedures, Guidelines, and Forms. [*reserved*]

C. Other Related Resources. [*reserved*]

V. References

A. 45 C.F.R. 164: Health Insurance Portability and Accountability Act (HIPAA): Security and Privacy

B. Family Educational Rights and Privacy Act of 1974 ("FERPA", 20 U.S.C. § 1232g)

C. Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541)

D. ISO 27002:2013, Information Technology - Security Techniques - Code of Practice for Information Security Controls

E. NIST 800 Series, Federal Information Security Standards

F. Policy 3-070: Payment Card Acceptance

G. Policy 4-001: University Institutional Data Management

H. Policy 4-003: World Wide Web Resources Policy

I. Policy 5-111: Disciplinary Actions and Dismissal of Staff Employees

J. Policy 6-400: Code of Student Rights and Responsibilities

K. Policy 6-316: Code of Faculty Rights and Responsibilities

L. Pub. 111-5, Division A, Title XIII, Subtitle D: Health Information Technology for Economic and Clinical Health Act (HITECH Act)

M. Omnibus HIPAA Rule: 45 CFR Parts 160 and 164 - Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule

N. Utah Board of Higher Education Policy R345: Information Technology Resource Security

VI. Contacts

The designated contact officials for this Regulation are:

A. Policy Owner(s) (primary contact person for questions and advice): Chief Information Security Officer

B. Policy Officer(s): Chief Information Officer

See Rule 1-001 for information about the roles and authority of policy owners and policy officers.

VII. History

Revision History

A. Current version. Revision 1.

1. Approved by President Randall as an Interim Rule on September 12, 2023 with effective date of September 12, 2023. Rule finalized with no changes after Board of Trustees approval of Policy 4-004 revisions on November 14, 2023.

2. Legislative History

3. Editorial Revisions

B. Previous versions.

1. Revision 0. Effective date April 6, 2016.

C. Renumbering

1. Not applicable.