University Rule 4-004D: Access Management Rev. 1

I. Purpose and Scope

A. 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. 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: University of Utah Information Security Policy, apply for purposes of this Rule, including the following:

A. **Account** - A login ID in combination with a password, PIN, or other authentication token used to access any University Information System, Electronic Resource, or IT Resource.

B. **Account Provisioners** - IT Personnel responsible for the creation, management and maintenance of User rights and privileges, objects, and attributes in relation to accessing Information Systems, Information Assets, Electronic Resources, and IT Resources.

C. **Confidential** - Any Information Asset which is classified as Restricted or Sensitive per the Data Classification and Encryption Rule.

D. **Electronic Resource** - Any resource used for electronic communication, including but not limited to internet, Email, and social media.

E. **Information Asset** - Data or knowledge stored in any electronic manner and recognized as having value for the purpose of enabling University to perform its business functions.

F. **Information System** - An Application or group of Servers used for the electronic storage, processing, or transmitting of any University data or Information Asset.

G. **IT Resource** - A Server, Workstation, Mobile Device, medical device, networking device, web camera, or other monitoring device, or other device/resource that is a) owned by the University or used to conduct University business regardless of ownership, b) connected to the University's network; and/or c) that is creating, accessing, maintaining, or transmitting Information Assets and used for electronic storage, processing or transmitting of any data or information.

H. **Restricted Data** - Any data types classified as Restricted per the Data Classification and Encryption Rule.

I. **Sensitive Data** - Any data type classified as Sensitive per the Data Classification and Encryption Rule.

J. **User** - Any person, including students, staff, faculty, permanent and temporary employees, contractors, vendors, research collaborators, and third party agents, who accesses any University Electronic Resource, Information System, and/or IT Resource.

III. Rule

A. Account Authorization

Prior to granting a User access to any University Information System that creates, maintains, processes, or transmits Confidential data, the University IT Provisioners will implement the following controls:

1. Confirm that the request for User access has been appropriately authorized.

2. Confirm that the level of access requested is:

    a. Appropriate for the User's job description and job function,

    b. Appropriate for the Information System and/or the Information Asset, and

    c. Does not compromise segregation of duties

    d. Where technically feasible, assign the appropriate role-based access to the User based on business role and job function.

After granting Users access to any University Information System that creates, maintains, processes, or transmits Confidential data, the University Provisioners will implement the following controls:

1. Maintain a formal log of Users' access to each Information System.

B. Account Authentication

1. Upon granting a User access to University Information Systems, the University Provisioners must ensure that each User is assigned a unique Account.

2. Multi-factor authentication will be utilized commensurate with the assessed level of risk for Accounts on Information Systems that create, store, process or maintain Restricted data.

C. Account Modification and Termination

1. It is critical that Human Resources, the Office of Registrar/Admissions, Research, Academic Affairs, academic and administrative units, and/or management expeditiously communicate User employment status changes to the University Provisioners.

2. Upon notification from Human Resources, the Office of Registrar/Admissions, Research, Academic Affairs, academic and administrative units, and/or

management that a User changes job roles within the University or terminates a contract or employment with the University, the University Provisioners must modify, remove, or disable access to University's Information Systems as appropriate.

3. To protect University Information Systems, the University's Account Provisioners will deactivate, disable and/or delete security access upon notification of termination as appropriate.

4. Certain events may require that a User's access rights be immediately removed. In these situations, the User's respective helpdesk should be notified immediately.

D. Account Reaccreditation

1. Periodically, commensurate with data classification requirements and the assessed level of risk, the University Account Provisioners will review User access rights to University Information Systems.

2. A formal review should be conducted in cooperation with Information System owners as well as with User's management as appropriate to confirm that each User has the authorized and appropriate level of access.

E. Password Management

When managing passwords for University Information Systems, the University Account Provisioners will implement the following controls:

1. Configure password strength as appropriate for the level of access and classification of data contained in the particular Information System.

2. Issue temporary passwords via a secure method to the User in a manner which forces the User to change the password immediately.

3. Ensure the temporary password issued is unique to the User.

4. Ensure that all default vendor passwords have been changed.

5. Ensure that passwords are never hard-coded or stored on Information Systems in an unprotected form.

When using passwords for University Information Systems, a User:

1. Must keep his/her password confidential.

2. Must not keep a record of the password in any form that cannot be stored securely via a method approved by the Information Security Office.

3. Must change his/her password if the User suspects the password or Account has been compromised.

4. Must change temporary passwords issued immediately upon first login.

[Note: Parts IV-VII of this Rule (and all other University Regulations) are Regulations Resource Information--the contents of which are not approved by the Academic Senate or Board of Trustees, and are to be updated from time to time as determined appropriate by the cognizant Policy Officer and the Institutional Policy Committee, as per Policy 1-001 and Rule 1-001.]

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

A. Rules

TBD

B. Procedures

Policy 4-004 Procedures

C. Guidelines

TBD

D. Forms

E. Other related resource materials

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

VI. Contacts

A. The designated contact Officials for this Policy are:

1. Policy Owner (primary contact person for questions and advice): Chief Information Security Officer, 801-213-3397

2. Policy Officer; Chief Information Officer, 801-581-3100

These officials are designated by the University President or delegee, with assistance of the Institutional Policy Committee, to have the following roles and authority, as provided in University Rule 1-001:

A 'Policy Officer' will be assigned by the President for each University Policy, and will typically be someone at the executive level of the University (i.e., the President and his/her Cabinet Officers). The assigned Policy Officer is authorized to allow exceptions to the Policy in appropriate cases.... "

"The Policy Officer will identify an 'Owner' for each Policy. The Policy Owner is an expert on the Policy topic who may respond to questions about, and provide interpretation of the Policy; and will typically be someone reporting to an executive level position (as defined above), but may be any other person to whom the President or a Vice President has delegated such authority for a specified area of University operations. The Owner has primary responsibility for maintaining the relevant portions of the Regulations Library... .[and] bears the responsibility for determining -requirements of particular Policies... ." University Rule 1-001-III-B & E

VII. History

A. Current version: Revision 1, effective date: April 4, 2016

Approved by Academic Senate: May 4, 2015

Approved by Board of Trustees: May 12, 2015

Background information for this version