University Rule 4-004E: Change Management Rev. 0

I. Purpose and Scope

A. The purpose of this Change Management Rule is to outline the requirements for ensuring that changes to IT Resources and Information Systems are formalized prior to execution.

B. The purpose of this Change Management Rule is to outline the requirements for ensuring that changes to IT Resources and Information Systems are formalized prior to execution.

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. **Change** - An event or action which modifies the configuration of any component, Application, Information System, or Service.

B. **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.

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

D. **IT Technicians** - IT Technicians develop, administer, manage and monitor the IT Resources, Information Systems, and Electronic Resources that support the University's IT infrastructure, are responsible for the security of the IT Resources, Information Systems, and Electronic Resources they manage, and assure that security-related activities are well documented and completed in a consistent and auditable manner.

III. Rule

A. Change Execution

Prior to executing a change to University Information Systems in the production environment, IT Technicians shall:

1. Capture the business requirement for the Change.
2. Identify the Change activity via a unique identifier that will be logged and recorded.
3. Plan and test the Change as appropriate.
4. Assess the potential impacts the Change may have to the confidentiality, integrity and availability of the Information System and its Information Assets.
5. Communicate the details of the Change to key stakeholders and other appropriate personnel.
6. Capture Change rollback requirements to recover from an unsuccessful change.
7. Receive approval from the Change Advisory Board as appropriate.

B. Post Change Execution

After executing a Change to University IT Resources and Information Systems, IT Technicians shall:

1. Log the successful or unsuccessful status of the Change.
2. In the event of an unsuccessful Change, document the issue and the lessons learned.

C. Segregation of Duties

1. The University shall ensure that no single individual can access, modify, or use Information Systems without authorization or detection to reduce the opportunities for unauthorized or unintentional changes to University IT Resources and Information Systems in any environment.

2. The University shall physically, logically or virtually separate test, development and production environments to reduce the risk of unauthorized access and/or changes to University IT Resources and Information Systems.

[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