University Rule 4-004M: Business Continuity and Disaster Recovery Rev. 0

I. Purpose and Scope

A. The purpose of this Business Continuity and Disaster Recovery Rule is to counteract interruptions to business activities and protect essential business processes from major failures or disasters.

B. This Rule supports section M, titled Business Continuity and Disaster Recovery, of the University of Utah Information Security Policy 4-004.

II. Definitions

For the purposes of this Policy and any associated Regulations, these words and phrases have the following meanings:

A. **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.

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

III. Rule

A. Information Security Requirements in Business Continuity and Disaster Recovery

To ensure that the University's information security requirements are included in business continuity and disaster recovery management, the University's business continuity and disaster recovery plans will contain the following key elements:

1. Identification and prioritization of the University's essential business processes

2. Inventory of the personnel, Information Assets and Information Systems involved in essential business processes

3. Understanding the impact of natural and facility threats on the safety of Users and essential business processes

4. Understanding of the impact of information security incidents on essential business processes

5. Identification of resources required to address any identified information security requirements to mitigate the impact of information security incidents on essential business processes

6. Identification of personnel roles and responsibilities with regards to business continuity and disaster recovery procedures

7. Implementation of business continuity and disaster recovery procedures that support the safe and timely recovery and restoration of essential business processes

B. Business Continuity and Disaster Recovery Supporting Procedure Requirements

To ensure that the University's business continuity and disaster recovery plans are consistent and that the plans consistently address the University's information security requirements, supporting procedures will be adopted that incorporate the following elements:

1. Conditions for activating the business continuity and/or disaster recovery plans.

2. Roles and responsibilities of business continuity and disaster recovery plan execution.

3. The actions to be taken under the following conditions:

a. Emergency – following a disaster or security incident which interrupts or jeopardizes business operations.

b. Failover – temporarily moving essential business processes to pre-established alternative locations and restoring operations in the required time frames.

c. Resumption – returning to normal business operations.

4. Business Impact Analysis

The University will, with full involvement of business process owners:

a. Identify events that interrupt essential business processes,

b. Formally capture the likelihood and impact of these interruptions and their consequences to information security, and

c. Assign criticality tiers for applications and Information Systems that support these business processes.

5. Testing and Maintaining Business Continuity and Disaster Recovery Plans

To ensure that the University's business continuity and disaster recovery plans are up to date and effective, and that all personnel are aware of their roles and responsibilities, the plans will be tested and updated regularly using a variety of the following techniques:

a. Table-top discussions and hypothetical testing of likely scenarios

b. Scenario simulation

c. Technical recovery testing with actual shut downs

d. Alternate site activation testing

e. Complete rehearsals

6. Lessons learned should result in updates and revisions to the business continuity and disaster recovery plan.

[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.]

I. 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 Resources Material

II. 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

III. 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

IV. 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