Procedure P4-004M: Business Continuity and Disaster Recovery Planning

Revision 0. Effective date: November 6, 2024

I. Purpose and Scope

A. Purpose.

The purpose of this Business Continuity and Disaster Recovery Planning Procedure is to outline the requirements of a business continuity and disaster recovery plan to counteract interruptions to business activities and protect essential business processes from major failures or disasters.

B. Scope.

The scope of this procedure 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 procedure supports Section M, titled Business Continuity and Disaster Recovery Planning, of the University of Utah Information Security Policy 4-004

II. Definitions

The definitions provided in Policy 4-004 apply for this procedure. In addition, the terms below apply for the limited purpose of this procedure.

A. Business Impact Analysis (BIA) – A detailed examination of an Asset's requirements, function, and interdependencies used to characterize Asset contingency requirements and priorities in the event of a significant disruption.

III. Procedure

A. IT managers, in collaboration with data owners and business process owners, are responsible for creating and maintaining business continuity and disaster recovery plans for their respective areas of operations. The following is provided as minimum requirements for a business continuity and disaster recovery plan:

1. Identify the scope of the plan:

    a. Define the scope by identifying the critical business processes and Assets that need to be protected in case of a disaster or disruption. This shall include an inventory of all Assets.

2. Conduct a Business Impact Analysis (BIA):

    a. Perform a BIA to identify the areas that would suffer the most significant financial or operational loss in the event of a disaster or disruption. A key objective is to identify and document all critical Assets that are required for the continuity of the business unit.

3. Develop a business continuity and disaster recovery plan that includes, at a minimum:

    a. use cases and events for plan activation;

    b. a formal, documented plan incorporating University policy and contractual and regulatory requirements;

c. continuity and recovery procedures;

d. defined roles and responsibilities;

e. required training;

f. required Assets;

g. communications to prepare, detect, and quickly respond to an unplanned outage; and

h. measures for data backup, disaster recovery, and emergency operations to maintain applicable compliance requirements.

4. Test and update:

a. IT managers shall ensure the plan is tested at least annually to verify that it is effective and up to date.

b. IT managers shall review and update the plan at least annually or whenever there is a significant Change in the business environment.

Sections IV- VII are for user information about this procedure.

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

A. Policies/ Rules.

1. Policy 4-004: University Information Security Policy

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

C. Other Related Resources.

V. References

[*reserved*]

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 0.

1. Approved by Chief Information Security Officer with effective date of November 6, 2024.

B. Renumbering

1. Not applicable