Procedure P4-004K: Backup and Recovery

Revision 0. Effective date: November 6, 2024

I. Purpose and Scope

A. Purpose.

The purpose of this Backup and Recovery Procedure is to outline the Asset backup and recovery process for all University administrative units, including colleges, divisions, departments, and centers.

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 K, titled Backup and Recovery, 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.

III. Procedure

A. For the Assets for which they are responsible, IT managers shall:

1. create a backup and recovery plan that, at a minimum, includes:
    a. all federal, state, and local laws, regulations, and statutes, as well as contractual obligations applicable to the Asset, including retention requirements;
    b. backup schedule;
    c. physical storage location;
    d. the appropriate Information System Media (e.g., external hard drives, network-attached storage (NAS), and cloud storage);
    e. the order in which data should be restored; and
    f. documentation for the entire backup and recovery process, including step-by-step instructions, ensuring all IT Technicians who will implement the plan have access to the documentation and any other relevant information.
2. at least annually, assess and update the backup strategy to accommodate changes in data volume, storage options, and/or technological advancements to ensure the effectiveness of the backup and recovery plan; and
3. in consultation with the applicable data owner, determine the backup frequency based on the prevalence of data changes and the acceptable level of data loss.

B. IT Technicians shall implement the backup and recovery plan by following these steps:

1. maintain a current and accurate Asset inventory;
2. select the appropriate backup method, which could include full backups, incremental backups, and differential backups;
3. implement automated backup processes to ensure regular and consistent backups, utilizing backup software or built-in operating system tools to schedule and automate the backup process;
4. make the backup immutable to ensure data integrity;
5. safeguard the backup data by employing Encryption techniques to protect it from Unauthorized Access;
6. at least quarterly, perform tests to ensure that Information Assets can successfully be restored from the backups to guarantee their effectiveness in case of data loss or system failure;
7. store at least one copy of the backups in an off-site location (e.g., cloud storage) to mitigate the risk of data loss due to physical damage or disasters affecting the primary location; and
8. at least weekly, monitor the backup process to ensure it runs smoothly without any errors or interruptions and review backup Logs and reports to identify and promptly address any issues.

C. For more specific implementation requirements, please access Procedure P4-004L and Procedure P4-004J.

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

1. Procedure R4-004J: Log Management and Monitoring

2. Procedure P4-004L: Media Handling

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