Information Technology On-Site Backup Procedure

Office: Information Technology
Procedure Contact: Chief Information Officer

Revision History

Revision Number:	Change:	Date:
1.0	Initial Version	**02/2012**
1.1	Format Changes	**03/2014**
2.0	Updated Procedure Title, Details	**09/2019**

A. Purpose

This procedure defines the backup practices for the Information Technology Department of Southern Oregon University. This procedure typically, but not exclusively, applies to servers and networked storage. This procedure does not apply to non-SOU hosted servers, services, or systems.

B. Definitions

Backup: An additional copy of data stored on separate media for the explicit purpose of preventing data loss in the event of equipment failure or destruction.

Restore: The process of copying data from backup sources to its original location or a new location, to make the data accessible.

C. Procedures

1. Responsibility and Scope

The Department of Information Technology is responsible for the backup of data held in central systems and related databases. The responsibility for backing up data held on the workstations of individuals, regardless of whether they are owned privately or by the college, falls entirely to the user. Campus users should consult their Computing Coordinator or the Help Desk about securing locally stored data.

The Chief Information Officer shall delegate a member (or members) of the IT Department to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups periodically.

2. Requirements and Scope

Data to be backed up includes the following:

1. IT managed servers used for academic purposes

2. IT managed servers used to conduct university business

3. IT managed servers used to store end-user data

4. Other network-attached storage utilized by IT managed systems

3. Exclusions

Machines may be excluded from this requirement under the following circumstances:

1. The machine configuration is stored in a configuration management application (e.g. Puppet) and there is no user created data present nor will any be generated under normal use.

2. Turn-key servers maintained by the respective vendor.

3. Servers designated as test systems.

4. Schedule

Incremental backups are performed daily.

Backup copies are performed on a rolling 24-hour cycle to maintain a separate full copy of on-site backups.

Full backups are performed monthly.

5. Retention

Incremental backups are retained for 30 days.

Backup copies are retained for 7 days.

Full backups are retained for 365 days.

6. Restoration

Users that need files restored must submit a request to their Computing Coordinator or Help Desk. Required information include: the name of the file, creation date, the last time it was changed, and the date and time it was deleted or destroyed.

Requests for the restoration of all or parts of campus databases shall be forwarded to the Network Services Manager or Chief Information Officer.

Restoration from on-site backups (files less than 30 days old) will be performed free of charge.

Restoration from off-site backups will incur a cost, for which end-users will be billed.

7. **Storage**

   Incremental backups and backup copies are stored in the SOU Datacenter in Ashland, on separate media from the source data.

   Full backups are stored in the AWS cloud.

8. **Testing**

   The ability to restore data from backups shall be tested periodically.

This procedure may be revised at any time without notice. All revisions supersede prior procedures and are effective immediately upon approval.