Title:	Information Technology Data and System Backup Standards and Procedures

Division:	Business and Finance	**Department:**	Information Technology
Procedure Contact:	Chief Information Officer		
Date Posted:	4/7/2023		
Related Policies or Procedures:	State Technology Policy 141.10 Change Management Procedure		

History

Revision Number:	Change:	Date:
1.0	Initial version	**06/18/2018**
1.1	Updates for post-change testing	**8/1/2020**
1.2	Updates to meet State Technology Policy Changes	**4/5/2023**

A. Purpose

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

B. Definitions

Backup - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

Archive - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing online storage space.

Restore - The process of bringing data back from the offline media and putting it on an online storage system such as a file server.

Business Essential - Direct negative customer satisfaction; compliance violation; non-public damage to organization's reputation; direct revenues impact.

Historical - No bearing on business operations or customers.

Mission Critical - Requires continuous availability. Breaks in service are intolerable immediately and significantly damaging.

C. Procedure

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 university, falls entirely to the user. Campus users should consult the IT 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 on a monthly basis.

2. Requirements and Scope for University Managed Systems and Data

All IT managed servers and storage, such as networked attached storage devices, are required to be backed up.

Data to be backed up includes the following information:

- User created data
- Databases (system and user)
- Application and Operating System Files
- System state data
- Registry (Windows systems)
- etc directory (Linux systems)
- Active Directory

Immutable backups are required for the following systems and/or data

- Mission critical
- Business essential
- Those containing Category 3 or Category 4 data as defined in the WA State OCIO Data Classification Standard.

2. Requirements and Scope for Hosted and Vendor Managed Systems and Data

Backup schedule, responsibilities and requirements for hosted and vendor management systems must be included in the applicable licensing or maintenance agreement.

The Chief Information Officer or their designee will periodically review and ensure that appropriate, proper backups are being made by the vendor.

3. Exclusions

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

- The machine configuration is stored in a configuration management application (e.g. Ansible) and there is no user created data present nor will any be generated under normal use.
- Turn-key servers maintained by the respective vendor.
- Servers designated as test systems.

4. Schedule for University Managed Systems and Data

A full backup is performed during the first week of every month. Incremental backups are performed daily. A full synthetic backup is duplicated to removable media or a remote medium (e.g. Cloud) during the second and last week of every month.

Operating system files and application files that are not user created may be backed up on a weekly basis as long as installation media is available.

5. Retention for University Managed Systems and Data

Full backups are retained for a minimum of one month.
Incremental backups are retained for one week or until the next full backup has been made.
The first synthetic backup set of every month is retained for one year.

6. Schedule and Retention for Hosted and Vendor Managed Systems and Data

Hosted and vendor managed backups are scheduled and retained in accordance with the vendor's policies and contractual obligations.

6. Restoration

Users that need files restored must submit a request to the IT 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 Infrastructure Services Senior Manager or Chief Information Officer.

Requests for restoration of data from hosted or vendor managed systems will be forwarded to the vendor for resolution.

7. Storage for University Managed Systems and Data

Monthly full backups are stored off-site.

8. Testing and Remediation for University Managed Systems and Data

The ability to restore data from backups shall be tested periodically. In addition, test restores shall be performed after making hardware repairs, software updates, firmware updates, or other significant changes. Testing and remediation activities will be documented by following established Information Technology Change Management practices.

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