جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Backup	Last Review date	19/5/2021
	Policy Number	IT-08	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

Overview

University of Sharjah requires Backup and recovery for all enterprise level data which is essential to business/ academic and DR needs. Any loss of data due to file corruption, virus, security or human error can impact the university's ability to perform its operations. An effective backup policy is crucial to the University of Sharjah's development and educational provisioning system.

Scope

The University of Sharjah requires that computer systems maintained by Information Services be backed up periodically, that the backup media be stored at a secure off-site location, and that recovery tests are performed regularly. As a result, Information Services will adhere to information technology best practices that call for daily, weekly, monthly, and yearly system backups.

Purpose

The purpose of this policy is to safeguard the University's information assets, prevent loss of data due to accidental deletion or corruption, and to facilitate restoration of information and business process should a system failure occur.

Business and academic Information and services are a vital part of UoS and should be protected. Simply saving information is not enough; performing backups of all information within The University of Sharjah and will help prevent business down time and/or loss of data and services. Failure due to computer malfunction, human error, and natural disasters could cause interruptions that are unrecoverable without adequate backups.

Policy

The policy of the systems backup is to provide a means to restore the integrity of the enterprise system and data in the event of a hardware/software failure or physical disaster and provide a measure of protection against human error or the inadvertent deletion of important files. System backups are not intended to serve as an archival copy or to meet records retention requirements.

جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Backup	Last Review date	19/5/2021
	Policy Number	IT-08	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

General:

1. Full backups of all The University of Sharjah's data shall be performed regularly for systems requiring full / incremental backup. Full backups are retained for 1 month before being overwritten.
2. Incremental backups of the University of Sharjah's data shall be performed regularly in systems requiring incremental backup. Incremental backups shall be retained for 1 week before being overwritten.
3. Where possible backups shall be run overnight.
4. Upon completion of backups, media copies shall be moved automatically to a secure remote site for disaster recovery purposes.
5. Backups shall be stored in secure locations. A limited number of authorized personnel shall have access to the backup application and backup media copies.
6. Any member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or services.
7. Additional protection from cyber attacks shall be provisoned for backup.

Backup Requirements:

Information backup requirements of all information systems within The University of Sharjah shall be identified and documented.

1. Information stored on a shared network drive shall be backed up regularly. Information stored locally on user's computers will not be included.
2. The Information system owners shall decide on the frequency and type of back up for their respective application, database and operating systems and network devices.
3. The IT backup team shall record and maintain the backup requirements for all information systems. The details of backup requirements shall include type of information to be backed up, backup frequency, storage media, retention period and disposal criteria.
4. Critical information should be fully backed-up on a weekly basis.

Backup of Information:

1. Backup of information shall be taken on a daily, weekly and monthly basis as per defined backup schedule.
2. Backup of systems, applications and device configs shall be taken before and after applying any changes such as upgrades and patching.
3. In the event of the failure of scheduled backup, IT Operations shall ensure

rescheduling of backup. IT Operations will notify data owner and investigate the cause of failure to rectify the issue.

4. Backups and archives, when technically feasible, shall be encrypted.

Backup restore and testing:

Backup media shall be randomly tested for consistency of recovery by the backup team at least once every 90 days.

Backup Media handling and storage:

1. The Backup team shall ensure that separate backup media are used for daily, weekly, monthly & yearly backups.
2. All backup media shall be clearly identified and labelled.
3. Backup copies of critical data shall be stored at a defined offsite location.
4. Offsite location for storage of backup media shall be in remote proximity of the primary site.
5. Offsite backup shall be maintained in a fire resistant cabinet and must be equipped with appropriate physical security.
6. Access to backup media while onsite, in-transit, or offsite shall be restricted to authorized personnel.
7. In the unlikely event that a system cannot conform to this policy, the ITC director will inform the Chancellor detail the specific actions being taken and/or resources needed to comply with the intent of this policy.
8. All backup media shall be disposed-off and destroyed in a secure manner at the end of their life or when they are irrevocably corrupted.
9. This policy is subject to change, per review by information technology leadership. Additionally, the policy will be reviewed on an annual basis for changes coinciding with information technology environment changes at the university.
10. Record of the movement of backup media shall be properly documented by authorized personnel.
11. The disposal process must ensure the following:
    a. The media is properly wiped of data by, for example, degaussing.
    b. Labels / tags containing reference to The University of Sharjah's information are removed.
    c. Non-reusable data backup storage media are physically destroyed.

Cloud Backup

The cloud service provider will contractually adhere to the UoS backup policy to ensure the continuity of services (ref. UoS Business Continuity Policy) and availability of applications and information stored in the cloud facility.

Reference

Standard	Control
ISO 27001:2013	A.12.3.1