 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Cloud Security	Last Review date	19/5/2021
	Policy Number	IT-13	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

## Overview

The policy applies to all University data i.e. information that arises from University teaching, research, and administration, and applies to all staff, students, and other parties who have access to University data.

## Scope

This policy is applicable to all the cloud services subscribed by University of Sharjah from cloud service providers.

## Purpose

The objective of this policy is to make sure that the provisioning of a cloud service is in accordance with the academic and security requirements and relevant laws and regulations.

## Definitions


CSP – Cloud Service Provider

## Policy

### General

The University of Sharjah shall:

1. Avoid storing classified data with a Cloud Service Providers (CSP), outside the legal jurisdiction or geographical boundaries of the United Arab Emirates, including for CSP's Backup or Disaster Recovery purposes.
2. Cloud service agreement shall include security requirements/controls for acceptable usage of data on the cloud
3. Define and communicate required security controls to Cloud Service Provider (CSP) for the handling of data in accordance with the data classification. (ref. UoS Classification and ownership policy).
4. Ensure that adequate cloud security controls are implemented by Cloud Service Provider (CSP) as per the architecture and deployment model approved by The University.
5. Develop and maintain a formal agreement with Cloud Service Provider (CSP) addressing the following information security requirements as a minimum:
  - a. Information security risks and mitigation.
  - b. Data protection and storage.
  - c. Information security incidents handling.
  - d. Change, Recovery and Restoration.

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Cloud Security	Last Review date	19/5/2021
	Policy Number	IT-13	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

### Cloud Service Contractual Requirements

Before moving a service out of the University of Sharjah to any third party, a rigorous legal analysis and evaluation shall be conducted.

1. **Non-Disclosure Agreement:** sign an NDA with the cloud service provider before provisioning any service.
2. **Data Ownership:** Ensure that the University of Sharjah retains the “Exclusive” right to data ownership throughout the duration of the agreement. The ownership includes all copies of data available with the cloud service provider including backup media copies if any.
3. **Data Location:** “Specify” in the contract the country(s) where it is acceptable for the data to be stored.
4. **Legal Prevalence:** ensure that the cloud service provider’s own data privacy policy complies with the applicable legal and regulatory requirements.
5. **Data Breach Notification:** Ensure that University of Sharjah is “immediately” notified of any confirmed breach without delay.
6. **Data Breach Penalty:** Ensure that the cloud service provider will be responsible for any financial losses or penalties that may occur due to a cloud service provider breach.
7. **Right to be forgotten:** contractually state that the cloud service provider will completely delete/eliminate any trace of Data/information at the end of the Agreement as stated in the contract.


### Data Portability and Compliance:

1. The University of Sharjah shall ensure that Cloud Service Provider (CSP) has the adequate measures and processes to support data portability whenever the University decides to move its data.
2. The University of Sharjah shall ensure proper cloud security controls are implemented by CSP, addressing periodic testing of the continuity and communicating the results to The University.
3. The University of Sharjah shall conduct periodic reviews or audits to verify CSP compliance with the applicable security policies and contractual requirements.

### Policy Compliance

#### Compliance Measurement

The Security team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology	Effective Date	30/5/2021
	Policy Subject	Cloud Security	Last Review date	19/5/2021
	Policy Number	IT-13	Next Review date	19/5/2022
	Responsible Entity	IT Center	Approved By	VC for Financial & Admin. Affairs

### Exceptions

Any exception to the policy must be approved by the Information security committee.

### Non-Compliance

Non-conformance to this policy could result in disciplinary action including, but not limited to, informal or formal warnings, and termination of contract.

### 1. Reference

Standard	Control Ref
ISO 27001:2013	A.10.1.1, A.10.1.2, A.18.1.5