



الجامعة الإسلامية العالمية ماليزيا
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
يُونَيْبَرَسِيْتِيْ اِسْلَامْ اِنْتَارَا اِنْجَسَا مَلِيْسِيَا

Garden of Knowledge and Virtue

Guideline for Management of Cloud Computing Services in IIUM

International Islamic University
Malaysia (IIUM)

Document Change Log

Version	Revision	Date	Pages Affected	Remarks/Change Reference
Version 01	00	25/6/2025	-	Initial Document

Responsibility and Activity Log

Requestor	Description	Submission Date	Approval Date
Muhamad Hairulnizam Hasan	Initial Draft	25/6/2025	25/6/2025

SECTION 1: INTRODUCTION

1.1 OBJECTIVE

The objective of this document is to provide a cloud computing service guidelines for IIUM. This ICT Guideline shall apply to all KCDIOs who plan to subscribe to the cloud computing services. This is to ensure that the cloud computing environment is managed through good governance and practices for the benefit of the University.

1.2 SCOPE

1.2.1 This guideline applies to all Kulliyahs, Centres, Divisions, Institutes, and Offices (KCDIOs) within IIUM that plan to subscribe to or manage cloud computing services, including Infrastructure (IaaS), Platform (PaaS), and Software (SaaS) models. It governs the entire cloud service lifecycle, from initial assessment using the server requirement matrix and data classification to procurement, security management, cost control, and final service termination.

1.2.2 The scope mandates compliance for all involved staff and system administrators, ensuring that all cloud activities adhere to the University's governance, security policies, and the national Cloud Framework Agreement. It excludes personal, non-official use of cloud services that does not involve university data or resources.

1.3 APPLICABILITY

IIUM communities that are involved in the cloud computing services environments management, and usage are affected by this guideline

1.4 TERMS AND DEFINITIONS

Terms	Definitions
IIUM/University	International Islamic University Malaysia
KCDIO	Kulliyah, Centre, Division, Institute and Office
ITD	Information Technology Division
ITD Director	Information Technology Division Director
DCCM	Data Center and Cloud Management Unit
System Administrators	System administrator is a person who is responsible for the management of the servers/services that is subscribed in the cloud

CSP	Cloud Service Provider
CFA	Cloud Framework Agreement
MSP	Managed Service Provider
CLOUD COMPUTING SERVICE	Cloud computing services are computing models that provide computing source configuration by demand, easy, secure, flexible, with competitive cost online through the internet network available
REQUESTOR	The party (KCDIO) is initiating the request to subscribe to cloud computing services.

1.5 CLOUD COMPUTING SERVICE DEFINITION

Cloud computing services are computing models that provide computing source configuration by demand, easy, secure, and flexible, with competitive cost online through the internet network available.

SECTION 2: EXPLANATION OF THE IMPLEMENTATION OF THE GUIDELINES

2.1 GUIDELINE STATEMENTS

2.1.1 Cloud Computing Classification

Cloud computing services consist of three (3) implementation models:

Infrastructure as a Service (IaaS)	This service model is the provision of basic infrastructure for computing resources such as Central Processing Unit (CPU), memory (RAM), storage, security and virtual networking to support the operation of the user's application or software. This model allows users to manage and control the operating system (OS), storage, applications, and network components
Platform as a Service (PaaS)	This service model is the provision of a platform to develop application software over the Internet, as needed and subscription-based. CSP provides the necessary platforms in the system development cycle such as operating systems, development tools, databases, programming languages and libraries through the services provided. Users just need to use the platform to develop applications more easily and smoothly

Software as a Service (SaaS)	This service model is the provision of application software over the Internet, as needed and subscription-based. CSP is responsible for managing all ICT infrastructure, maintenance and security requirements. Users only need a connection to the Internet via a fixed device web browser or a mobile device to configure the application as needed
------------------------------	---

2.1.2 Server Requirement Matrix

The server requirement will go through the following criteria matrix to determine whether the server will go to the private cloud at IIUM Gombak campus or a public cloud subscription.

CLASSIFICATION	VERY LOW (1)	LOW (2)	MEDIUM (3)	HIGH (4)	VERY HIGH (5)
Data classification	Unclassified	Restricted	Confidential	Secret	Top Secret
CPU requirement	2 cores	4 cores	8 cores	16 cores	>16 cores
Memory requirement	2GB	4GB	8GB	16GB	>16GB
Storage requirement	100GB	250GB	500	1TB	>1TB
Estimated Data transfer (monthly)	50GB <	50GB – 100GB	100GB – 500GB	500GB – 1TB	> 1TB
Scalability	None clustered	2 servers	3 servers	4 servers	> 4 servers
System architecture	Standalone without DB	Standalone with internal DB	Integration with other services	Integration with DB	Integration with other services and DB
Tolerance to downtime	>12 hrs	8 hrs – 12 hrs	4hrs – 8 hrs	1 hr – 4hrs	<1hr

The recommendation is based on the total score of the criteria matrix above:

Total Score	Recommendation	Explanation
8 - 20	Stay On-Prem	These systems generally have low resource requirements, high sensitivity, and may not benefit much from the flexibility and scaling advantages of the cloud.
20 -30	On-Prem, on Cloud or Hybrid	These systems still have manageable resource requirements but may benefit from some cloud features like backup, high availability, and security. However, due to sensitivity or high downtime tolerance, they may still be best kept on-prem. Cloud migration can be considered, but a hybrid solution may be better (e.g., some workloads moved to the cloud, others stay on-prem).
30 - 40	On Cloud	These systems have significant resource requirements and/or scalability demands (e.g., high CPU, memory, storage, or data transfer). Cloud platforms are ideal here because they can offer elasticity, better disaster recovery, and reduced overhead costs for on-prem infrastructure. If these systems require integration with other services and tolerate minimal downtime, the cloud can support these needs efficiently.

2.1.3 Data Classification Process

The requestor should refer to the Guidelines of Data Classification and Labelling from OSICS for the data classification process. Data classification must align with national and institutional data privacy standards. For cloud deployments, classified data must be protected in compliance with IIUM security policies and government data protection requirements, including encryption and appropriate access controls.

2.1.4 Cloud Computing Service Subscription

2.1.4.1 The cloud computing service subscription is managed under the CFA that has been signed between the Government and the appointed MSP.

2.1.4.2 The list and price of the cloud services offered by CSP are based on the catalogue managed by MSPs.

2.1.4.3 KCDIOs must ensure that the Cloud Computing Services involving the storage of official documents or information are managed in accordance with security regulations in clause 8.6 and subject to compliance with information security management guidelines through cloud computing in public service or other directives issued by the Office of the Chief Security Officer Malaysia (CGSO).

2.1.4.4 The Proposal needs to be submitted to the appointed evaluation committee for approval/recommendation before proceeding with the MSP for subscription.

2.1.4.5 The cost of the cloud services shall be borne by the requestor.

2.1.4.6 Cost Management – KCDIOs shall ensure appropriate cost estimation, usage monitoring, and budget control mechanisms are in place. Cost tracking must be done using the available tools provided by MSP/CSP and reconciled against usage reports regularly. Cost anomalies should be reported to ITD.

2.1.5 Cloud Server Operating System

The operating system installations that are currently supported by DCCM are as outlined in the Guideline on the Management of Virtual Server Management Environment in IIUM Data Centre.

2.1.6 Security and Access Control

2.1.6.1 All cloud computing services must implement robust security controls including:

- (a) Identity and Access Management (IAM), with role-based access control (RBAC) and multi-factor authentication (MFA).
- (b) Network security, including segmentation, firewalls, and VPN access where required.
- (c) Encryption of data at rest and in transit using CSP-supported mechanisms.

2.1.6.2 Security configurations must comply with IIUM's ICT Security Policies and industry standards such as ISO/IEC 27001 and ISO/IEC 27017.

2.1.7 Incident Response and Management

2.1.7.1 Incident response procedures for cloud-based services must integrate with the University's overarching incident response framework.

2.1.7.2 CSPs and MSPs must provide reporting mechanisms, response time guarantees, and support channels in the event of:

- (a) Data breaches

- (b) Downtime/service disruptions
- (c) Unauthorised access

2.1.7.3 Post-incident review and lessons learned must be documented and submitted to ITD and relevant university committees.

2.1.8 Cloud Service Termination

2.1.8.1 Notification to Cloud Service Provider (CSP)

The subscriber/the person in charge shall formally notify the Cloud Service Provider (CSP) to verify the defined procedures and timelines for service termination and the formal handover of data.

2.1.8.2 Data Retrieval and Migration

The subscriber/the person in charge shall do backup and download all critical data and configuration files into approved storage devices

2.1.8.3 Data Deletion and Sanitisation

All organizational data shall be deleted from the cloud infrastructure, whether performed manually or via the Cloud Service Provider (CSP). A formal Certificate of Data Destruction or equivalent proof of erasure is required for all final deletions.

2.2 IMPLEMENTATION AND NON-COMPLIANCE

2.2.1 The Director of ITD holds the responsibility for the implementation of this guideline and shall take necessary actions in the event of violation of this guideline.

2.2.2 This guideline is applicable to all staff of the University and any infringement of the guideline may be subject to disciplinary actions.

SECTION 3: ADMINISTRATION OF THE GUIDELINES

3.1 OWNERSHIP OF THE GUIDELINES

ITD is responsible for the formulation and maintenance of this guidelines to ensure it remains current, effective, and aligned with the strategic direction of the University, and communicate any changes of the guidelines to the relevant stakeholders.

3.2 REVIEW AND REVISION PROCESS

This guideline shall be reviewed from time to time to ensure its continued relevance and effectiveness, with reviews conducted at least annually or as circumstances require.

SECTION 4: REFERENCE DOCUMENT

- 4.1 This policy shall be read together with the following documents of:
- 4.1.1 IIUM ICT Policy
 - 4.1.2 ICT Regulation
 - 4.1.3 IIUM Information Management Policy
 - 4.1.4 IIUM ICT security procedure
 - 4.1.5 IT Infrastructure Library(ITIL)
 - 4.1.6 Control of Business IT(COBIT)
 - 4.1.7 Policy for Procurement of ICT Resources
 - 4.1.8 IIUM Financial Policies and Procedures
 - 4.1.9 Dasar Perkhidmatan Perkomputeran Awan Sektor Awam
 - 4.1.10 Perolehan Perkhidmatan Pengkomputeran Awan (Cloud) Sektor Awam
 - 4.1.11 Garis Panduan Pengurusan Keselamatan Maklumat Melalui Perkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam
 - 4.1.12 Guideline on Data Classification and Labelling
 - 4.1.13 ISO/IEC 27001 – Information Security Management System
 - 4.1.14 ISO/IEC 27017 – Cloud-specific Security Controls
 - 4.1.15 ISO/IEC 27018 – Protection of Personal Data in the Cloud
 - 4.1.16 Guideline on the Management of Virtual Server Environment in IIUM Data Center

Title of Guideline : Guideline for Management of Cloud Computing Services in IIUM
Number of Guideline : IIUM-ISMS-L3-011
Approving Authority : ITD Management
Approval Date : 25/6/2025
Effective Date : 25/6/2025
Version No. : 01
Revision No. : 00