جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
عمادة الاتصالات وتقنية المعلومات
Deanship of Information and Communication Technology

جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

Cloud Computing Security Policy

Version: 2.0

CODE: DICT.I.06-43.CS.E.V2.0

جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
عمادة الاتصالات وتقنية المعلومات
Deanship of Information and Communication Technology

1 Table of Cont.

2 Intellectual Property Information

This document is the intellectual property of the Deanship of Information and Communication Technology (DICT) at Imam Abdulrahman bin Faisal University (IAU). The content of this document is intended solely for authorized recipients. Any distribution, disclosure, publication, or copying of this document without written permission from DICT is strictly prohibited.

3 Document Control

3.1 Information

Title	Classification	Version	Status
CLOUD COMPUTING SECURITY POLICY	RESTRICTED	V2.0	ACTIVE

3.2 Revision History

Version	Author(s)	Issue Date	Changes
V1.0	DR. BASHAR ALDEEB	11/01/2021	CREATION
V1.1	DR. SAMER BANI AWWAD	16/03/2022	REVIEW AND UPDATE
V2.0	BAHA NAWAFLEH	17/12/2023	REVIEW AND UPDATE

3.3 Document Review

Date of Next Scheduled Review
01/01/2025

3.4 Distribution List

#	Recipients
1	ALL DICT DEPARTMENTS
2	LEGAL AFFAIRS
3	IAU WEBSITE
4	

3.5 Approval

Name	Position Title	Decision Number	Date
DR. NIHAD AL-OMAIR	VICE PRESIDENT OF DEVELOPMENT AND COMMUNITY PARTNERSHIP	61945	06/03/2024

4 Introduction

It is essential for the IAU to protect its information and technological assets in order to ensure their success and operational continuity. Given the nature of its operations, the university heavily relies on cloud service providers, underscoring the necessity of following and implementing the required security controls to safeguard it from threats.

This policy is included within the framework of the university's policy and falls under the authority granted by the governing entity, starting from the date of its approval.

5 Objective of the Policy

This policy defines the cybersecurity requirements set for establishing and utilizing cloud services for storing or processing the information assets of the IAU, without exposing its data and computing resources to security risks.

6 Applicability and Scope

The provisions of this policy apply to all affiliates or individuals working within the IAU, whether under permanent or temporary contracts, directly or indirectly. This includes suppliers, external contractors, and anyone with permanent or temporary access rights to the university's data, regardless of its source, form, or nature, as well as to the university's systems, devices, and databases.

This policy also applies to all external cloud services, such as official email, document storage, Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS).

7 Policy

7.1 General Policy Requirements

7.1.1 Official authorization by the Head of Cybersecurity Management is required for the use of cloud computing services for IAU business purposes. Affiliates are not permitted to create cloud service accounts or enter into cloud service contracts for the storage, processing, or exchange of university-related communications or data owned by the university without obtaining the necessary approvals as outlined in this policy.

7.1.2 Approval of External Processing (Cloud) Service Providers:

All external processing (cloud) service provider engagements must be approved by the Cybersecurity Management and Information Technology Management within the university. Additionally, the Head of Cybersecurity Management, in consultation with the Head of Information Executive, must assess and approve the security, privacy, and technical control requirements appropriately for cloud computing service providers.

7.2 Create Cloud Computing Services

7.2.1 For any cloud services requiring user agreement with terms of service, these agreements must be reviewed and approved by the Head of Information Officers of Information Technology, Legal Affairs, Information Security, and Business Continuity.

7.2.2 Cloud service providers are not allowed to use university data for secondary purposes. The cloud service provider must ensure the application of multi-layered security tools within the internal network. This includes, but is not limited to, Intrusion Prevention Systems (IPS) for detecting and blocking malicious activities, Intrusion Detection Systems (IDS) for immediate alerts, File Integrity Monitoring (FIM) for data integrity and prevention of unauthorized changes, and Data Loss Prevention (DLP) for monitoring and blocking all types of data leaks.

7.2.3 Contracts with cloud service providers must include rights for auditing, review, and monitoring, and should be reviewed and approved by the Head of Information Officers of Information Technology, Legal Affairs, Information Security, and Business Continuity.

7.2.4 Data must be classified prior to hosting it on the cloud.

7.2.5 An assessment of cybersecurity risks associated with hosting applications or services in the cloud must be conducted before selecting a cloud computing service provider and hosting.

7.2.6 The cloud service provider must ensure an independent third party conducts security testing to verify secure isolation, proper configuration of virtual routing and forwarding (VRF) and share a copy of the report with the university.

7.2.7 Applications, services, data, or any related technical component must be hosted by a cloud service provider within the Kingdom of Saudi Arabia.

7.2.8 Hosting locations for sensitive systems or any of their technical components must be within the university or in cloud services provided by a government entity or a national company compliant with the National Cyber Security Authority controls related to cloud services and hosting, considering data classification.

7.2.9 University must ensure the application of data privacy requirements on data hosted in the cloud.

7.2.10 Data and information transferred to, stored in, or transferred from cloud services must be encrypted according to relevant legislative and regulatory requirements within the university.

7.2.11 The cloud service provider must provide access rights to secure the network devices protecting the university environment. Firewall and Internet Protocol (IP) address restrictions must be managed through dedicated security resources for cloud services.

7.2.12 The cloud service provider must provide a fixed and detailed log of activities they have conducted to protect and secure the university environment and provide more details in the current Service Level Agreement.

7.2.13 The cloud service provider must ensure security testing and implement Border Gateway Protocol (BGP), along with additional security controls to enhance protection.

7.2.14 University must ensure that the cloud service and hosting provider performs periodic backups and protects backup data according to the approved backup policy.

7.2.15 Contracts should outline termination clauses that allow the university to terminate the contract and require the cloud service provider to return university data in a usable format and then permanently delete it upon contract termination.

7.2.16 Cloud services must be used only within the Kingdom of Saudi Arabia. Approval from the Head of Cybersecurity Management is required for using cloud services outside the Kingdom, following relevant regulatory and legislative procedures.

7.2.17 The cloud service provider must implement and monitor cybersecurity controls to protect the confidentiality, integrity, and availability of university data.

7.2.18 Logical separation of university data from other data held by the cloud service provider is required. The cloud service provider must be able to identify and distinguish university data from other data permanently. Additional security controls must be implemented by the cloud service provider, including but not limited to firewall usage and IP address restrictions, to limit the activity of systems that read and write data from memory to ensure isolation and full separation from network users.

7.2.19 The cloud service provider must provide evidence of proper and secure separation between production, development, and test environments if the service is managed by them.

7.2.20 Disaster recovery and business continuity procedures related to cloud computing must be developed and implemented securely.

7.2.21 The cloud service and hosting provider must offer the necessary technologies and tools to the university for managing and monitoring its cloud services.

7.2.22 University must ensure that the cloud service and hosting provider cannot access stored data and that the access privileges granted to the service provider are limited to the necessary permissions for carrying out service management and maintenance activities, or as per business requirements.

7.2.23 The cloud service provider must adhere to data governance policies issued by the National Data Management Office and provide the required assurance to the university.

7.2.24 Affiliates must create cloud service accounts only with cloud service providers approved by the Head of Information Officer of Information Technology.

7.2.25 Contracts with cloud computing and hosting service providers must include at a minimum the following:

- Cybersecurity requirements and Service Level Agreement (SLA) clauses.
- Non-disclosure clauses, including data deletion and destruction in accordance with an agreement between the service provider and the university based on data classification and data classification policy.
- Business continuity and disaster recovery requirements.
- Contracts with cloud computing and hosting service providers must allow the university to terminate the service without justification or conditions.
- Data retrieval requirements in a usable format upon service termination.

7.3 Access Controls

7.3.1 User accounts must be created according to the university's Access Control Policy.

7.3.2 Cloud service and hosting providers must restrict access to the university's cloud services only to authorized users, using user identity verification methods in accordance with the university's Access Control Policy.

7.3.3 User accounts in external (cloud) services must comply with the current security requirements of the university, including strong password policies, as per the Password Policy.

7.4 Sensitive Data Storage

7.4.1 The Head of Cybersecurity Management or their delegate must approve the types of data that may be stored in external (cloud) environments.

7.4.2 Approval from the Head of Cybersecurity Management is required for hosting sensitive systems or any of their technical components.

7.4.3 Personal cloud service accounts are not allowed for storing, processing, or exchanging communications related to the university or its owned data.

8 Roles and Responsibilities

The Cybersecurity Management shall:

8.1.1 The Head of Cybersecurity Management must approve the policy from the authority and work on its implementation.

8.1.2 The Head of Cybersecurity Management must approve standards, procedures, and guidelines to ensure necessary compliance with university operations' security requirements.

8.1.3 The Head of Cybersecurity Management must ensure alignment between this policy and the university's operations.

8.1.4 The Head of Cybersecurity Management must resolve any conflicts arising from this policy.

8.1.5 The Head of Cybersecurity Management must provide necessary resources for identifying, procuring, and implementing technical solutions to meet policy requirements wherever possible.

8.1.6 The Cybersecurity Management must disseminate the cybersecurity compliance policy to all departments, affiliates, and users authorized to access technical and information assets of the university.

8.1.7 The Cybersecurity Management must coordinate with relevant departments to monitor compliance and implementation.

8.1.8 The Cybersecurity Management must periodically review the policy according to the established timeline.

The Deanship of Information and Communication Technology shall:

8.1.9 Adhere to this policy, implement the controls mentioned in this policy, and report any security incidents to the Cybersecurity Management.

Top Management, Heads of Departments, Heads of Units, and Advisers shall:

8.1.10 Ensure the dissemination of this policy to all affiliates within the university or unit.

8.1.11 Report any violations or non-compliance with this policy to the Cybersecurity Management.

8.1.12 All affiliates within the university must adhere to the provisions of this policy and report any security incidents or non-compliance with any provisions stated in this policy to the Head of Cybersecurity Management.

9 Ownership of the Policy

The Head of Cybersecurity Management within the university is responsible for this policy.

10 Policy Changes

The policy must be reviewed at least annually or whenever there are changes in legislative and regulatory requirements. Any changes should be documented and approved by the authorized personnel within the university.

11 Compliance

All individuals within the university, including external parties/contractors, must adhere to the provisions of this policy. The Head of Cybersecurity Management in the university must ensure continuous monitoring of compliance and provide regular reports on this matter to the authorized personnel.

Necessary measures must be taken to ensure compliance with the provisions of this policy. This can be achieved through periodic reviews by the Cybersecurity Management or relevant departments. Corrective actions should be taken by the authorized personnel within the university based on recommendations provided by the CISO regarding any violations of this policy. Disciplinary measures should be proportional to the severity of the incident as determined by the investigation in this regard. Disciplinary actions may include, but are not limited to, the following:

- Revoking access rights to data, information technology assets, and connected systems of the university.
- Issuing a written warning or terminating the employment of the individual, as deemed appropriate by the university.

- Non-compliance with any provisions of this policy, without prior exception granted by the Cybersecurity Management, should result in appropriate actions being taken in accordance with the university's policies and regulations or as deemed suitable, and in accordance with contractual terms with any individuals or entities contracted by the university .

12 Related Policies, Standards and Procedures

- DICT.I.06-01.CS.E.V2.0 - General Cybersecurity Policy
- DICT.I.06-02.CS.E.V2.0 - Cybersecurity Compliance Policy
- DICT.I.06-33.CS.E.V2.0 - Access Control Policy
- DICT.I.06-27.CS.E.V2.0 - Acceptable Use of Assets Policy
- DICT.I.06-04.CS.E.V2.0 - Asset Management Policy
- DICT.I.06-15.CS.E.V2.0 - Password Management Policy
- DICT.I.06-21.CS.E.V2.0 - Data Classification Policy
- DICT.I.06-07.CS.E.V2.0 - Backup Management Policy
- DICT.I.06-49.CS.E.V2.0 Identity And Access Management Standards
- DICT.I.06-60.CS.E.V2.0 Asset Classification Standards
- DICT.I.06-62.CS.E.V2.0 Asset Management Standards
- DICT.I.06-65.CS.E.V2.0 Backup and Restoration Standards
- DICT.I.06-69.CS.E.V2.0 Password Management standards
- DICT.I.04-35.CS.E.V2.0 Backup and Restoration Procedures

13 References

Department Name	National Institute of Standards and Technology (NIST	ISO 27001:2013	Cybersecurity Controls for Cloud Computing	Cybersecurity Controls for Social Media Accounts of Entities	Cybersecurity Controls for Remote Work	Cybersecurity Controls for Sensitive Systems	Core Cybersecurity Controls
Cloud Requirements	AC-20	A.13.1.2	1-ش-1-3	-	1-1-3	1-2-4	3-4-2

---------- End od Document ----------