King AbdulAziz University
Cyber-Security Center

Cloud Computing and Hosting Cyber-Security Policy

Restricted-Internal

Document Authorization:

Role	Name	Date	Signature
Owner	Cyber-Security Center	14/11/2022 CE	

Document Versions:

Version	Date	Editor	Reasons for Revision
1.0	15/11/2021 CE	Shuruq bint Khalid Banafi	
1.1	14/11/2022 CE	Daniyal ibn Muhammad al-Ghazzawi	In accordance with the requirements of the Authority

Table of Contents

Objectives

The purpose of this policy is to provide and fulfill cyber-security requirements, based on best practices and standards, relating to the protection of King AbdulAziz University informational and technical assets on cloud computing and hosting services, so as to ensure that cyber-security risks are addressed or reduced, through focus on the essential objectives of protection, which are: Confidentiality, integrity, and availability of information.

This policy aims to comply with cyber-security requirements and the relevant legislative and regulatory requirements, which is itself a legislative requirement expressed in Control 4-2-1 of the Essential Cyber-Security Controls (ECC-1:2018) promulgated by the National Cyber-Security Authority.

Scope and Applicability of the Work

This policy covers all King AbdulAziz University informational and technical assets on cloud computing services that are hosted, processed, or managed by external parties, and this policy applies to all King AbdulAziz University employees.

Policy Clauses

1– **General Clauses**

1-1 All cyber-security requirements relating to external parties, as expressed in the Cyber-Security Policy for External Parties, must be applied to all providers of cloud computing and hosting services.

1-2 The Cyber-Security Center must verify the efficiency and reliability of cloud computing and hosting services, in addition to their licensure and officially-recorded presence within the Kingdom of Saudi Arabia.

1-3 Cyber-security requirements for cloud computing and hosting services must be applied in accordance with King AbdulAziz University regulatory policies and procedures and relevant legislative and regulatory requirements.

1-4 King AbdulAziz University must carry out assessments of the cyber-risks potentially attendant upon the use of hosting applications or services in the cloud prior to selecting cloud computing and hosting providers.

1-5 Hosting sites for critical systems, or any of their technical components, must be within King AbdulAziz University, or on cloud hosting services provided by government agencies or domestic companies that conform to the Controls of the National Cyber-Security Authority pertaining to cloud computing and hosting services, with attention being given to the classification of the data to be hosted. (CSCC-4-2-1-1)

1-6 The Cyber-Security Center must develop, document, and approve procedures for using cloud services.

1-7 Contracts with providers of cloud computing and hosting services must include the following, at a minimum:

1-7-1 Cyber-security requirements and service level agreements (SLA).

1-7-2 Non-disclosure clauses that include data deletion and destruction agreements between the provider and King AbdulAziz University based on the classification of data, with attention being given to the Data Classification Policy.

1-7-3 Operational continuity and disaster recovery requirements.

1-7-4 Cloud computing and hosting services provider contracts must include the ability of King AbdulAziz University to terminate the services provided without justifications or conditions.

1-8 The implementation of cyber-security requirements pertaining to cloud computing and hosting services providers must be reviewed periodically, at a minimum once a year.

2– **Cyber-Security Requirements for Data Hosting/Storage**

2-1 Data must be classified prior to hosting/storage by cloud computing and hosting services providers. (ECC-4-2-3-1)

2-2 Cloud computing and services providers must return data (in a usable form), and delete it in a manner not susceptible to roll-back, at the end/termination of service. (ECC-4-2-3-1)

2-3 The site, hosting, and storage of King AbdulAziz University information must be within the Kingdom of Saudi Arabia (ECC-4-2-3-3), with attention being given to regulations and legislative aspects, so as to prevent King AbdulAziz University data from being subject to the laws of any other nations.

2-4 The Cyber-Security Center must ensure the segregation of the King AbdulAziz University environment (including virtual servers, networks, and databases) from other environments affiliated to other entities on cloud hosting services. (ECC-4-2-3-2)

2-5 Permission must be obtained from the Cyber-Security Center for the hosting of critical servers or any part of their technical components.

2-6 King AbdulAziz University must ensure that requirements pertaining to data privacy are applied to data hosted on cloud computing services.

2-7 Data and information transmitted to, stored on, or transmitted from cloud services must be encrypted, in accordance with the legislative and regulatory requirements pertinent to King AbdulAziz University.

2-8 King AbdulAziz University must ensure that cloud computing and hosting providers make backup versions periodically, and protect backup versions in accordance with the Backup Policy adopted by King AbdulAziz University.

2-9 King AbdulAziz University must ensure that cloud computing and hosting providers are unable to view stored data, and that access privileges for service providers are limited to the privileges necessary for managing and maintaining the data, or are in accordance with operational requirements.

2-10 Cloud computing and hosting service providers must restrict access to cloud services pertaining to King AbdulAziz University to authorized users only, and must use identity authentication measures, in accordance with the Identity and Access Management Policy adopted by King AbdulAziz University.

2-11 Cloud computing and hosting service providers must provide to King AbdulAziz University the necessary technologies and tools for managing and monitoring the cloud services provided to the University.

2-12 The Cyber-Security Center and the General Office for Legal Affairs must ensure that cyber-security requirements clauses pertaining to data hosting are included in contracts with cloud hosting service providers.

3– **Other Requirements**

3-1 King AbdulAziz University must ensure that events logs for hosted informational assets are activated.

3-2 King AbdulAziz University must ensure that cyber-security events logs are monitored periodically.

3-3 King AbdulAziz University must ensure that the clock synchronization for cloud services infrastructure is in agreement with the King AbdulAziz University clock synchronization.

3-4 Key Performance Indicators must be used to ensure the continual development of protection for informational and technical assets on cloud computing services.

3-5 Cyber-security requirements pertaining to cloud computing and hosting services must be reviewed periodically.

3-6 This policy must be reviewed at least once a year.

Roles and Responsibilities

–Responsible Party and Owner of the Document: Director of the Cyber-Security Center.

–Updating and Review of the Document: The Cyber-Security Center.

–Implementation and Application of the Document: The Deanship of Information Technology, the General Office for Legal Affairs, and the Cyber-Security Center.

Compliance with the Policy

1– The Director of the Cyber-Security Center must ensure the compliance of King AbdulAziz University with this policy periodically.

2– All employees of King AbdulAziz University must comply with this policy.

3– Any violation of this policy may subject the offender to disciplinary action, in accordance with the procedures followed by King AbdulAziz University.