


King AbdulAziz University  
Cyber-Security Center

**Cyber-Security Policy for External Parties**

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	Maram bint Khalid Hambishi	In accordance with the requirements of the Authority

## Table of Contents

<b><i>Objectives</i></b> .....	<b>4</b>
<b><i>Scope and Applicability of the Work</i></b> .....	<b>4</b>
<b><i>Policy Clauses</i></b> .....	<b>4</b>
<b><i>Roles and Responsibilities</i></b> .....	<b>7</b>
<b><i>Compliance with the Policy</i></b> .....	<b>7</b>

## Objectives

This policy aims to define cyber-security requirements to ensure the protection of King AbdulAziz University informational and technical assets from cyber-security risks originating from external parties, including information technology outsourcing services and managed services, in accordance with King AbdulAziz University regulatory policies and procedures.

This policy follows the relevant national legislative and regulatory requirements and international best practices, which is itself a legislative requirement as expressed in Control 4-1-1 of the Essential Cyber-Security Controls (ECC-1:2018) promulgated by the National Cyber-Security Authority.

## Scope and Applicability of the Work

This policy applies to all services provided by external parties to King AbdulAziz University, and applies to all King AbdulAziz University employees.

## Policy Clauses

### 1– General Clauses

1-1 Standard procedures for managing King AbdulAziz University's relationships with external parties must be documented and approved prior to, during, and at the conclusion of contractual relationships.

1-2 External service-providing parties must be carefully identified and selected, in accordance with King AbdulAziz University regulatory policies and procedures and relevant legislative and regulatory requirements.

1-3 Procedures for assessing risks must be applied to external parties and services provided, and their safety must be ensured through review of external party projects within King AbdulAziz University and of cyber-event logs pertaining to external party services (if possible) prior to and during the relationship on a periodic basis.

1-4 Contracts and agreements with external parties must be prepared in such a way as to ensure the commitment of external parties to applying King AbdulAziz University cyber-security requirements and policies and relevant legislative and regulatory requirements.

1-5 Contracts and agreements with external parties must be reviewed by the General Office for Legal Affairs to ensure that the terms of agreements are binding during and after the contract period, and that violation of the terms will subject the external parties to legal accountability.

1-6 Contracts and agreements must include provisions for maintaining the confidentiality of information (non-disclosure clauses) and for secure deletion of King AbdulAziz University data by external parties at the conclusion of services.

1-7 Cyber-security requirements must be reviewed with external parties on a periodic basis.

1-8 The Cyber-Security Policy for External Parties must be reviewed on a yearly basis, and changes must be documented and approved.

## **2– Cyber-Security Requirements Pertaining to Outsourced Information Technology Services or Managed Services Provided by External Parties**

2-1 When obtaining outsourced information technology services or managed services, external parties must be chosen with care, and the following must be put into effect:

2-1-1 Procedures to assess risks to cyber-security, and to ensure the existence of means guaranteeing control over such risks, prior to the signing of contracts and agreements, or in the event of changes to relevant legislative and regulatory requirements.

2-1-2 Cyber-security managed services centers for operations and monitoring that use the remote-connection method must be located entirely within the Kingdom. (ECC-4-1-3-2)

2-1-3 Outsourced services on critical systems must be provided by national corporations and entities, in accordance with the relevant legislative and regulatory requirements. (CSCC-4-1-1-2)

## **3– Cyber-Security Requirements for External Party Staff**

3-1 Screening or vetting procedures must be carried out for outsourcing services companies, outsourcing services staff, and managed services workers engaged with critical systems. (CSCC-4-1-1-1)

3-2 Cyber-security responsibilities and non-disclosure clauses must be included in external party employment contracts (including both during and at the end/termination of employment relationships with King AbdulAziz University).

## **4– Documentation and Access Controls**

4-1 External parties must develop and follow a formal and carefully documented process for granting and revoking access rights to all informational and technical systems that process, transmit or store King AbdulAziz University information, in a way that is consistent with the cyber-security requirements and cyber-security controls pertaining to King AbdulAziz University.

4-2 Ability to access and process King AbdulAziz University information must be provided in a secure and controlled manner.

4.6 Controls relating to passwords for all users who possess access rights to King AbdulAziz University information must be applied in a way consistent with the cyber-security requirements and the objectives of the cyber-security controls pertaining to King AbdulAziz University.

4-3 A multi-factor identity verification system must be applied to access privileges for critical systems that process, transmit or store King AbdulAziz University information.

4-4 Access privileges must be revoked immediately at the end/termination of the services of any employee working for external parties and possessing access privileges to King AbdulAziz University information or informational and technical assets, or in the event of change to employee roles resulting in access no longer being required.

6.5 External parties must review access rights on a regular basis in accordance with the Cyber-Security Policies adopted by King AbdulAziz University

4-5 All audit records must be stored and maintained so as to be made available at the request of King AbdulAziz University.

## **5– Cyber-Security Requirements for Change Management**

5-1 External parties must follow a formal and appropriate change management process in accordance with King AbdulAziz University procedures and that complies with cyber-security requirements.

5-2 Changes made to King AbdulAziz University informational and technical assets must be assessed and tested prior to their application to the production environment.

5-3 The concerned parties at King AbdulAziz University must be informed of major changes that are planned to be made, as well as changes made to the informational and technical assets of King AbdulAziz University.

## **6– Cyber-Security Incidents and Operations Continuity Management Requirements**

6-1 The terms of contracts and agreements with external parties must include requirements to report cyber-security incidents, and to inform King AbdulAziz University in the event that the external party is subjected to a cyber-security incident.

6-2 Procedures for communications between external parties and King AbdulAziz University in the event that the external party is subjected to a cyber-security incident must be defined and documented, and these procedures must be reviewed and updated periodically.

2.2 An appropriate plan for operations continuity must be developed to avoid unavailability of services provided to King AbdulAziz University, in accordance with the requirements of the Operations Continuity and Catastrophic Failure Recovery Plan of King AbdulAziz University.

## **7– Data and Information Protection Requirements**

1.1 External parties must process, store, and delete King AbdulAziz University data and information in accordance with the Data and Information Protection Policy and Standards adopted by King AbdulAziz University.

1.2 Appropriate encryption controls must be applied for the protection of King AbdulAziz University data and information and to ensure that the confidentiality, integrity, and availability of King AbdulAziz University data and information is maintained, in accordance with the Cryptography Standards adopted by King AbdulAziz University.

7-1 Backup copies of King AbdulAziz University data and information must be made periodically, in accordance with the Backup Copies Management Policy of King AbdulAziz University.

7-2 King AbdulAziz University information found on critical systems and personal data that is to be processed by third parties in the test environment must not be processed, stored, or used without the use of strict controls for the protection of said data, such as data masking, data scrambling, or data anonymization. (CSCC-2-6-1-1)

7-3 King AbdulAziz University information and data present on critical systems that is subject to processing by third parties must not be transferred outside the production environment. (CSCC-2-6-1-5)

7-4 King AbdulAziz University information and data present on critical systems that is subject to processing by third parties must be classified in accordance with the Information and Data Classification Policy adopted by King AbdulAziz University. (CSCC-2-6-1-2)

## **8– Auditing**

8-1 King AbdulAziz University must carry out audits of relevant processes and systems whenever doing so is necessary or appropriate.

8-2 All external parties and their staff must cooperate fully and completely with the events log assessment and audit activities carried out by King AbdulAziz University, including the assessments performed.

## 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 Cyber-Security Center, the Deanship of Information Technology, the General Office for Human Resources, the General Office for Legal Affairs, and the General Office for Contracts and Procurement.

## Compliance with the Policy

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