


King AbdulAziz University
Cyber-Security Center

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

Table of Contents

<i>Objectives</i>	<i>4</i>
<i>Scope and Applicability of the Work.....</i>	<i>4</i>
<i>Policy Clauses</i>	<i>4</i>
<i>Roles and Responsibilities</i>	<i>5</i>
<i>Compliance with the Policy</i>	<i>6</i>

Objectives

The objective of this policy is to provide and fulfill cyber-security requirements based on best practices and standards, so as to ensure that cyber-security risks related to employees (both regular staff and contractors) at King AbdulAziz University are addressed before, during, and at the end/termination of their work.

This document aims to comply with cyber-security requirements and related legislative and regulatory requirements, which is itself a legislative requirement expressed in Regulation 1-9-1 of the Essential Cyber-Security Controls promulgated by the National Cyber-Security Authority.

Scope and Applicability of the Work

This policy covers all King AbdulAziz University systems, and applies to all employees of King AbdulAziz University.

Policy Clauses

General Clauses

1-1 Cyber-security requirements relating to employees must be defined.

1-2 Employees working with sensitive systems at King AbdulAziz University must be Saudi citizens who possess the necessary qualifications.

1-3 Cyber-security controls pertaining to human resources must be implemented during the lifecycle of employees' work at King AbdulAziz University, which is comprised of the following stages:

- Pre-employment
- Period of employment
- End or termination of employment

1-4 Employees at King AbdulAziz University must understand and agree to their job roles, terms, and responsibilities relating to cyber-security.

1-5 Responsibilities relating to cyber-security and the Non-Disclosure Agreement must be included in contracts of employment at King AbdulAziz University (the terms of which apply both during and after the end/termination of employment with King AbdulAziz University).

1-6 Violations relating to cyber-security must be included in the list of human resources violations at King AbdulAziz University.

1-7 Accessing information about employees with prior permission is forbidden.

1-8 Key performance indicators (KPI) must be used to ensure continual development of cyber-security requirements relating to human resources.

Pre-Employment

2-1 Employees must agree to comply with the Cyber-Security Policies prior to being granted access powers to King AbdulAziz University systems.

2-2 The roles and responsibilities of employees must be defined with implementation of the principle of non-conflict of interest being taken account.

2-3 Employees' roles and responsibilities relating to cyber-security must be defined in their job descriptions.

2-4 The roles and responsibilities relating to cyber-security must include the following:

- Protection of all King AbdulAziz University assets from unauthorized access or sabotage.
- Implementation of all required cyber-security operations.
- Compliance with the Cyber-Security Policies and Standards of King AbdulAziz University.
- Compliance with the Raising Levels of Cyber-Risk Awareness Program.

2-5 A cyber-security evaluation must be conducted for employees in cyber-security positions, technical positions holding important and sensitive powers, and positions related to sensitive systems.

Period of Employment

3-1 An awareness program concerned with increasing cyber-security awareness levels, which includes the Cyber-Security Policies and Standards, must be provided on a regular basis.

3-2 The Human Resources Office must inform the relevant departments of any change made to employee roles and responsibilities, in order that the necessary actions relating to revoking or modifying access privileges may be taken.

3-3 Application of cyber-security requirements relating to human resources must be ensured.

3-4 Extent of commitment to cyber-security must be included among the aspects of employee evaluation.

3-5 The Need-to-Know principle must be applied in the assignment of tasks.

End or Termination of Employment

4-1 Procedures for the end or termination of professional service must be defined in a way that covers cyber-security requirements.

4-2 The Human Resources Office must inform the relevant units in the event that the end or termination of an employment relationship is approaching in order for the necessary measures to be taken.

4-3 The return of all King AbdulAziz University assets and the cancelation of all employee access powers on the final day of employees' tenure, prior to their obtaining the necessary documentation, must be ensured.

4-4 The responsibilities and duties that will remain in effect subsequent to the end of employee service at King AbdulAziz University, including the Non-Disclosure Agreement, must be defined, and these responsibilities and duties must be included in all employment contracts.

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 General Office for Human Resources and the Deanship of Information Technology.

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.