King AbdulAziz University
Cyber-Security Center

Cyber-Security Legislation and Regulation Compliance 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

Objectives

The purpose of this policy is to provide and fulfill cyber-security requirements, based on best practices and standards, in order to ensure that King AbdulAziz University security software is in compliance with the relevant legislative and regulatory requirements.

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 1-7-1 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 systems and procedures, and applies to all King AbdulAziz University employees.

Policy Clauses

1– A list of legislative and regulatory items pertaining to cyber-security must be identified, documented, and periodically updated.

2– The technologies necessary for verifying compliance with the requirements of legislative and regulatory entities relating to cyber-security must be provided.

3– Cyber-security policies and procedures must be reviewed periodically to ensure their compliance with the relevant legislative and regulatory requirements.

4– The implementation of cyber-security policies and procedures must be reviewed periodically.

5– Compliance with relevant legislative and regulatory requirements must be ensured, on a periodic basis, using the appropriate tools, such as:

5-1 Cyber-security risk assessments.
5-2 Vulnerabilities management.
5-3 Penetration tests.
5-4 Review of cyber-security standards.
5-5 Security source code reviews.
5-6 User surveys.
5-7 Meetings with responsible authorities.
5-8 Review of system and network privileges.
5-9 Review of cyber-security logs and incidents.

6– Necessary corrective measures must be identified, and efforts must be made to implement them, so as to correct gaps in compliance with the requirements promulgated by the relevant authorities.

7– Key Performance Indicators (KPI) must be used to ensure the continual development of the compliance program.

8– Appropriate measures must be implemented to ensure compliance with legislative and regulatory requirements relating to intellectual property and software use rights.

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.

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.