King AbdulAziz University
Cyber-Security Center

Settings and Hardening Policy

Restricted-Internal

Document Authorization:

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

Document Versions:

Version	Date	Editor	Reasons for Revision
1.0	15/11/2021 CE	Shuruq bint Khalid Banafi	
1.1	14/11/2022 CE	Ashwaq bint Samir Abd al-Jawad	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, for the protection, hardening, and configuration of settings for resisting cyber-attacks of King AbdulAziz University informational and technical assets and applications, through focus on the essential objectives of cyber-security, 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 1-6-2-2 and Control 1-6-3-5 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 information and technical assets and applications within King AbdulAziz University, and applies to all King AbdulAziz University employees.

Policy Clauses

1– All informational and technical assets within King AbdulAziz University, as well as approved applications and programs, must be identified, and technical security standards must be provided for them.

2– Technical security standards for all informational and technical assets, applications, and programs authorized within King AbdulAziz University must be developed, documented, and approved.

3– The hardening and settings of King AbdulAziz University computer hardware, systems, applications, network devices, and security devices must be configured in accordance with the approved technical security standards for resisting cyber-attacks.

4– One of the following methods must be employed to develop technical security standards:

4-1 Suppliers' security configuration guidance, in accordance with King AbdulAziz University regulatory policies and procedures, relevant legislative and regulatory requirements, and best international standards.

4-2 Hardening and settings guides from reliable sources that are compatible with industry standards, such as the Center for Internet Security (CIS), the Security, Networks, and System Administration Institute (SANS), the National Institute for Standards and Technology (NIST), the Defense Information and Systems Administration (DISA), the Security Technical Implementation Guides (STIG), etc.

4-3 King AbdulAziz University technical security standards must be developed in a manner commensurate with the nature of the operations concerned and in accordance with suppliers' hardening and settings guides and factory standards.

5– Controls pertaining to technical security standards must cover the following, as a minimum:

5-1 Suspending or changing factory and default accounts.

5-2 Preventing the installation of undesired software.

5-3 Disabling unused network ports.

5-4 Disabling unused services.

5-5 Limiting the use of storage media and external storage.

5-6 Changing default settings that may be exploited in cyber-attacks.

6– Settings and hardening must be reviewed, and their application ensured, in the following cases:

6-1 Periodic review of settings and hardening for informational and technical assets, in which their implementation is ensured according to the approved technical security standards.

6-2 Review of settings and hardening prior to initiating and launching projects and changes relating to informational and technical assets.

6-3 Review of settings and hardening prior to initiating and launching applications.

6-4 Periodic review of the settings and hardening of industrial control systems, in which their application is ensured, according to the approved technical security standards.

7– An image of the settings and hardening of King AbdulAziz University informational and technical assets must be approved, in accordance with the technical security standards, and maintained in a secure place.

8– An approved image must be employed to install or update informational and technical assets.

9– The technologies and techniques necessary for central management of settings and hardening must be provided, and the capability to automatically implement or update settings and hardening must be ensured for all informational and technical assets according to well-defined and planned timelines.

10– A system for monitoring settings that is compatible with the Security Content Automation Protocol (SCAP) must be provided, to ensure that settings are in accordance with the approved technical security settings and are fully implemented; any unauthorized changes must be reported.

11–Key Performance Indicators (KPI) must be employed to ensure the continual development of settings and hardening management.

12– Cyber-security requirements relating to the settings and hardening of King AbdulAziz University informational and technical assets and applications must be reviewed yearly, or in the event of changes to relevant legislative or regulatory requirements or standards.

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.

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.