King AbdulAziz University
Cyber-Security Center

Anti-Malware Protection 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..4

Scope and Applicability of the Work..4

Policy Clauses 4

Roles and Responsibilities..5

Compliance with the Policy...6

Objectives

The purpose of this policy is to provide and fulfill cyber-security requirements, based on best practices and standards, relating to the defense of user devices, mobile devices, and private servers pertaining to King AbdulAziz University from malware threats, and to reduce cyber-risks arising from internal and external threats, 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 2-3-1 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 user devices and private servers at King AbdulAziz University, and applies to all King AbdulAziz University employees.

Policy Clauses

1– **General Clauses**

1-1 King AbdulAziz University must identify, provide, and ensure the reliability of modern and advanced protection technologies, techniques, and mechanisms.

1-2 Technologies, techniques, and mechanisms for protecting user devices, mobile devices, and servers from malware must be applied and securely managed.

1-3 It must be ensured that protection technologies, techniques, and mechanisms are capable of detecting, recognizing, and eliminating all types of malware, such as viruses, trojan horses, worms, spyware, adware, root kits, etc.

1-4 Prior to the selection of protection technologies, techniques, and mechanisms, it must be ensured that they are compatible with King AbdulAziz University operating systems, such as Windows, Unix, Linux, Mac, etc.

1-5 It must be ensured that protection technologies are capable of roll-back to earlier versions, in case updates to protection technologies cause harm to systems and operational requirements.

1-6 Privileges to disable, delete, or change the settings of anti-malware protection technologies must be restricted, such that they are available to protection system administrators only.

2– **Settings for Anti-Malware Protection Technologies, Techniques, and Mechanisms**

2-1 Settings for protection technologies, techniques, and mechanisms must be configured in accordance with the technical standards adopted by King AbdulAziz University, with consideration being given to suppliers’ guidance and advice.

2-2 Settings for anti-virus software on email servers must be configured to scan all incoming and outgoing email messages.

2-3 Individuals affiliated to external parties must not be permitted to communicate with the King AbdulAziz University network or wireless network without updated anti-virus software and appropriate settings configuration.

2-4 The availability of anti-malware program servers must be ensured, and the back-up environment must be appropriate for anti-malware program servers dedicated to non-critical tasks and operations.

2-5 Access to websites and other Internet sources known to host malware must be restricted through the use of mechanisms for filtering Web content.

2-6 Clock synchronization for all anti-malware protection technologies and mechanisms must be centrally set according to an accurate and reliable source.

2-7 Settings for anti-malware protection technologies must be configured to perform checks for suspicious content in isolated sources such as Sandbox.

2-8 Scans must be carried out periodically on user devices and servers to ensure that they are free from malware.

2-9 Anti-malware technologies must be updated automatically when new versions are available from vendors, with consideration being given to the Patch Management Policy.

2-10 Technologies for protecting email and Internet browsing from advanced persistent threats (APT protection) and from threats that usually employ previously-unrecognized viruses and malware (zero-day malware) must be provided, implemented, and securely managed.

2-11 The settings of protection technologies must be configured to allow only a specified list of whitelisted files, applications, and programs to operate on servers pertaining to critical systems. (CSCC-2-3-1-1)

2-12 Servers pertaining to critical systems must be protected by means of peripheral device protection technologies approved by King AbdulAziz University (end-point protection). (CSCC-2-3-1-2)

2-13 Reports must be prepared periodically concerning the state of anti-malware protection which provide information concerning the number of devices and servers linked to protection technologies and their condition (for example: Updated or un-updated, disconnected, etc.), and these reports must be submitted to the Director of the Cyber-Security Center.

2-14 Anti-malware protection technologies must be centrally managed and continuously monitored.

3– **Other Requirements**

3-1 The Cyber-Security Center must ensure that the necessary level of security awareness exists among employees to deal with malware and to reduce the risks it poses.

3-2 Key Performance Indicators (KPI) must be used to ensure the continual development of user device and server protection from malware.

3-3 Cyber-security requirements for the protection of user devices and servers pertaining to King AbdulAziz University from malware must be reviewed periodically.

Roles and Responsibilities

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

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

–Implementation and Application of the Document: The Servers Office in the Deanship of Information Technology and the Cyber-Security Center.

Compliance with the Policy

1– 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.