


King AbdulAziz University
Cyber-Security Center

Workstation and Mobile and Personal Device 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>	4
<i>Scope and Applicability of the Policy</i>	4
<i>Policy Clauses</i>	4
<i>Roles and Responsibilities</i>	6
<i>Compliance with the Policy</i>	6

Objectives

This policy aims to define cyber-security requirements, based on best practices and standards, to reduce cyber-risks arising from workstations, mobile devices, and personal devices ("Bring-Your-Own Devices", BYOD) within King AbdulAziz University, and to protect the University from internal and external threats, through focus on the essential objectives of protection, which are: Confidentiality, integrity, and availability of information.

This policy follows cyber-security requirements and the relevant legislative and regulatory requirements and best international practices, which is itself a legislative requirement expressed in Controls 2-3-1 and 2-6-1 of the Essential Cyber-Security Controls (ECC-1:2018) promulgated by the National Cyber-Security Authority.

Scope and Applicability of the Policy

This policy covers all workstations, mobile devices, and employee personal devices within King AbdulAziz University, and applies to all King AbdulAziz University employees.

Policy Clauses

1– General Clauses

1-1 Data and information stored on workstations, mobile devices, and personal devices (BYOD) must be protected in accordance with its classification, the appropriate security controls must be employed to restrict access to this information, and unauthorized employees must be prevented from accessing or viewing it.

1-2 Workstation and mobile device software must be up-to-date, including operating systems, software, and applications, and must be provided with the latest patches, in accordance with the Patch Management Policy adopted by King AbdulAziz University.

1-3 The configuration and hardening of settings must be implemented for workstations and mobile devices in accordance with cyber-security requirements.

1-4 Employees must not be given privileged access to workstations and mobile devices; privileges must only be given in accordance with the principle of minimum privileges.

1-5 Default user accounts on operating systems and applications must be deleted or re-named.

1-6 Clock synchronization for all workstations and mobile devices must be centrally set according to an accurate and reliable source.

1-7 Workstations and mobile devices must be provided with banners to enable user access.

1-8 Only a specific list of whitelisted applications, data leakage prevention solutions, data monitoring systems, etc. must be allowed.

1-9 Storage media for important and critical workstations and mobile devices, and that have advanced privileges, must be encrypted in accordance with the Cryptography Standards adopted by King AbdulAziz University.

1-10 The use of external storage media must be prohibited, and prior permission must be obtained from the Cyber-Security Center for privileges to use external storage media.

1-11 Workstations, mobile devices, and personal devices (BYOD) with out-of-date or expired software (including operating systems, software, and applications) must not be permitted to communicate with the King AbdulAziz University network, so as to forestall cyber-threats arising from expired and unpatched software.

1-12 Workstations, mobile devices, and personal devices (BYOD) that are not equipped with up-to-date protection software must be prevented from communicating with the King AbdulAziz University network, so as to avert cyber-risks that may lead to unauthorized access, malware ingress, or data theft. "Protection software" in this case includes mandatory software, such as anti-virus protection software, protection solutions against suspicious programs and activities, anti-malware protections software, host-based firewalls, and host-based intrusion detection and prevention protection systems.

1-13 The settings of workstations and non-workstation mobile devices must be configured to display a password-protected screensaver if the device is not used for 15 minutes (session timeout).

1-14 Workstations and mobile devices must be managed centrally through the Active Directory server of the King AbdulAziz University domain, or a central administrative system.

1-15 The settings of workstations and mobile devices must be configured using the appropriate domain controller to apply the appropriate policies and to install the necessary software configurations.

1-16 Appropriate group policies must be implemented at King AbdulAziz University, and applied to all workstations and mobile devices, to ensure the compliance of King AbdulAziz University with regulatory and security controls.

2– Workstation Cyber-Security Requirements

2-1 Workstations must be allocated to technical teams with important privileges, must be isolated within the management network, and must not be linked any other network or service.

2-2 The settings of important and critical workstations and those with advanced privileges must be configured to relay logs to a central logs and monitoring system, in accordance with the Cyber-Security Events Logs and Monitoring Policy; the relay of these logs must be impossible for users to halt.

2-3 Workstations must be physically-secured within King AbdulAziz University buildings.

3– Mobile Device Cyber-Security Requirements

3-1 Mobile devices must be prevented from accessing critical systems, except for limited periods of time. Such access may only occur subsequent to risk-assessment and the obtaining of the necessary approvals from the Cyber-Security Center. (CSCC-2-5-1-1)

3-2 Mobile device disks that possess access privileges to critical systems must be encrypted using full disk encryption. (CSCC-2-5-1-2)

4– Personal Device (BYOD) Cyber-Security Requirements

4-1 Mobile devices must be managed centrally using the Mobile Device Management (MDM) system.

4-2 King AbdulAziz University information and data stored on employees' personal devices must be segregated and encrypted.

5– Other Requirements

5-1 Backup versions of data stored on workstations and mobile devices must be made periodically, in accordance with the Backup Policy adopted by King AbdulAziz University.

5-2 King AbdulAziz University data stored on mobile devices, workstations, and personal devices (BYOD) must be deleted in the following cases:

- Loss or theft of mobile devices.
- End/termination of employment relationships between device users and King AbdulAziz University.

5-3 Security awareness should be spread among employees concerning the mechanisms for device usage and their responsibilities regarding them according to the Acceptable Use Policy adopted by King AbdulAziz University, and awareness training sessions should be held for users holding important and critical privileges.

5-4 Key Performance Indicators (KPI) must be used to ensure the continual development of workstation and mobile device protection.

5-5 The Workstation and Mobile and Personal Device Security Policy must be reviewed yearly, and changes must be documented and approved.

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 Servers Office in 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– The Deanship of Information Technology and the Cyber-Security Center at 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.