جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
عمادة الاتصالات وتقنية المعلومات
Deanship of Information and Communication Technology

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

# Workstations, Mobile Devices and BYOD Security Policy

Version: 2.0

CODE: DICT.I.06-42.CS.E.V2.0

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY
عمادة الاتصالات وتقنية المعلومات
Deanship of Information and Communication Technology

# 1 Table of Contents

## 2 Intellectual Property Information

# 3 Document Control

## 3.1 Information

| Title | Classification | Version | Status |
|---|---|---|---|
| WORKSTATION,MOBILE DEVICES AND **BYOD** SECURITY POLICY | RESTRICTED | V2.0 | ACTIVE |

## 3.2 Revision History

| Version | Author(s) | Issue Date | Changes |
|---|---|---|---|
| V1.0 | DR. BASHAR ALDEEB | 19/03/2021 | CREATION |
| V1.1 | DR. SAMER BANI AWWAD | 22/07/2022 | REVIEW AND UPDATE |
| V2.0 | BAHA NAWAFLEH | 18/12/2023 | REVIEW AND UPDATE |
| | | | |

## 3.3 Document Review

| Date of Next Scheduled Review |
|---|
| 01/01/2025 |

## 3.4 Distribution List

| # | Recipients |
|---|---|
| 1 | ALL DICT DEPARTMENTS |
| 2 | LEGAL AFFAIRS |
| 3 | IAU WEBSITE |
| 4 | |

## 3.5 Approval

| Name | Position Title | Decision Number | Date |
|---|---|---|---|
| DR. NIHAD AL-OMAIR | VICE PRESIDENT OF DEVELOPMENT AND COMMUNITY PARTNERSHIP | 61945 | 06/03/2024 |

# 4 Introduction

Protecting information and information technology assets is essential for the success of the IAU. To achieve this goal, the Cybersecurity Management develops, establishes, and organizes the necessary security operations to safeguard information and technology assets. This document outlines the policy for mobile devices and personal devices within the University in accordance with relevant policies, regulatory requirements, and organizational procedures.

This policy is incorporated within the framework of the IAU's policy and falls under the authority granted by the governing body, effective from the date of its approval.

# 5 Objective of the Policy

The aim of this policy is to define cybersecurity requirements based on best practices and standards, aimed at mitigating cybersecurity risks arising from the use of both organizational and mobile computing devices, mobile devices, and personal devices of affiliates (Bring Your Own Device "BYOD") within the IAU. The policy aims to protect these devices from internal and external threats by focusing on the core goals of confidentiality, integrity, and availability of information.

# 6 Applicability and Scope

The provisions of this policy apply to all affiliates or individuals working within the IAU, whether on permanent or temporary contracts, both directly and indirectly. This includes suppliers, external contractors, and anyone with permanent or temporary access rights to the IAU's data, regardless of its source, form, or nature, as well as to the IAU's systems, devices, and databases.

# 7 Policy

## 7.1 General Policy Requirements

7.1.1 Data and information stored on user devices, mobile devices, and personal devices (BYOD) must be protected based on their classification using appropriate security controls to restrict access to this information. Unauthorized affiliates should be prevented from accessing or viewing such information.

7.1.2 User devices and mobile devices, including operating systems, software, and applications, must be regularly updated with the latest updates and patches according to the IAU's patch management policy.

7.1.3 Configuration and hardening controls must be applied to user devices and mobile devices in accordance with the configuration and hardening policy.

7.1.4 Affiliates should not be granted critical and sensitive privileges on user devices and mobile devices. Privileges must be granted according to the principle of least privilege and privileges.

7.1.5 Default user accounts in operating systems and applications must be deleted or renamed.

7.1.6 Central and accurate clock synchronization must be implemented for all user devices and mobile devices.

7.1.7 User devices and mobile devices must display a banner message to allow authorized use.

7.1.8 Only a specified list of applications (application whitelisting) should be allowed, and data monitoring systems and others should be used to prevent data leakage.

7.1.9 Storage media for important and sensitive user devices and mobile devices must be encrypted according to the approved encryption standard within the IAU.

7.1.10 The use of external storage media should be prohibited, and prior authorization from the cybersecurity management should be obtained for using external storage media.

7.1.11 User devices and mobile devices, including BYOD, that have outdated or expired software (including operating systems, software, and applications) must be prevented from connecting to the IAU's network to prevent security threats from unsupported and outdated software.

7.1.12 User devices and mobile devices, including BYOD, that do not have up-to-date security software should be prevented from connecting to the IAU's network to avoid security risks that may arise from unauthorized access, malware, or data leakage. Security software includes mandatory programs such as antivirus software, intrusion detection/prevention software, and host-based firewalls.

7.1.13 User devices and mobile devices, including BYOD, must be configured to automatically lock after a period of inactivity (maximum of 5 minutes).

7.1.14 Central management of user devices and mobile devices should be done through the IAU's Active Directory domain controller or a central administrative system.

7.1.15 Appropriate group policy settings should be applied to user devices and mobile devices to enforce suitable policies and install necessary software settings.

7.1.16 Appropriate group policy settings should be implemented within the university to ensure compliance with regulatory and security controls across all user devices and mobile devices.

7.1.17 The university allows its affiliates to use their own devices (BYOD) within the university to access its information or process them after applying the necessary controls, including the use of licensed operating systems and software.

7.1.18 The use of IAU-issued mobile devices must be aligned with the IAU's business interests and not for personal purposes, and affiliates must be aware of this.

7.1.19 The university must define all acceptable types and models of devices that are allowed for use within the IAU.

7.1.20 The university must centrally manage and periodically review all registered mobile devices.

7.1.21 The university must take necessary measures to protect against unauthorized access in case of loss or theft of mobile devices.

7.1.22 All mobile devices connected to the IAU's networks must be securely configured to comply with minimum security requirements.

7.1.23 Authorized affiliates by the IAU's cybersecurity management should have access to all data stored on any device owned by the IAU, including email messages, documents, call records, and communications sent or stored on organizational resources.

7.1.24 Copying or sharing any confidential information in any form, including but not limited to CDs, external storage media (USB), email attachments, etc., is strictly prohibited unless authorized for specific organizational purposes.

7.1.25 Capturing or recording images, videos, audio, or any form of surveillance or eavesdropping in secured areas or on organizational data without proper consent is prohibited.

7.1.26 Using mobile devices for photography, video recording, audio recording, or any form of spying or eavesdropping is prohibited.

7.1.27 Lost IAU-owned laptops, personal devices, and personal digital assistants must be reported immediately to the cybersecurity management.

7.1.28 The central management of user devices and personal devices (BYOD) should be done using a Mobile Device Management (MDM) system.

## 7.2 Security of User Devices, Both Collective and Mobile

7.2.1 User devices must be allocated to the technical team with critical privileges and isolated within a private network for network management purposes. These devices should not be connected to any other network or service.

7.2.2 Critical and sensitive user devices, which possess advanced privileges, must be configured to send logs to a central logging and monitoring system, following the IAU's cybersecurity event management and monitoring policy. Users should not have the capability to disable this functionality.

7.2.3 Affiliates are prohibited from installing new systems on collective or mobile computing devices without proper authorization from the IAU's cybersecurity management.

7.2.4 Usage of gaming software on organizational systems is prohibited, and installing, transferring, or utilizing such software within the IAU's network is strictly forbidden.

7.2.5 Submission of free or shareware applications (whether downloaded from the internet or acquired through other means) to the IAU's technical and information assets must undergo a formal assessment and approval process.

7.2.6 Laptops should be carried in hand luggage during travel to prevent damage and unauthorized access.

7.2.7 Access to mobile systems using mobile devices should only be allowed temporarily after conducting a cybersecurity risk assessment and obtaining approvals from the cybersecurity management.

7.2.8 Encryption of mobile device drives that have access to sensitive systems must be full and comprehensive.

7.2.9 All personnel in the university should be aware that their mobile devices, belonging to the IAU, are part of the organizational network and are subject to the same rules and regulations as other organizational assets.

7.2.10 Physical security of user devices within organizational premises must be ensured, and affiliates should be educated about this aspect.

## 7.3 Personal Devices Security (BYOD)

7.3.1 Data and information belonging to the university stored on affiliates' personal devices (BYOD) must be separated and encrypted.

7.3.2 Access to organizational systems by affiliates should only be granted to authorized individuals and solely based on work necessity.

7.3.3 The physical security and logical access security (for example, laptops, tablets, networking devices, personal digital assistants, smartphones, external storage media, etc.) of all personal devices are the sole responsibility of their owners. The university is not liable for any data loss or disclosure of personal information from affiliates' personal devices when connected to the organizational network or in cases where the device is lost or isolated within the IAU.

### 7.4 Other Requirements

7.4.1 Regular backups of data stored on users' devices and mobile devices must be conducted in accordance with the approved backup management policy of the IAU.

7.4.2 IAU data stored on mobile devices and personal devices (BYOD) should be deleted in the following scenarios:

- Loss or theft of the mobile device.
- Termination or end of the employment relationship between the user and the IAU.
- Reuse or disposal of mobile devices, especially those used to access cloud services.

7.4.3 Affiliates should be educated about the proper use of devices and their responsibilities towards them, in alignment with the acceptable use policy of authorized assets within the IAU. Special awareness sessions should be conducted for users with important and sensitive privileges.

## 8 Roles and Responsibilities

**The Cybersecurity Management responsibilities:**

8.1.1 Have the Head of Cybersecurity Management endorse the policy on behalf of the authorizing entity and oversee its implementation.

8.1.2 Have the Head of Cybersecurity Management approve standards, procedures, and guidelines to ensure necessary compliance with the security requirements of the IAU's operations.

8.1.3 Ensure alignment between this policy and the IAU's activities.

8.1.4 Resolve any conflicts arising from this policy.

8.1.5 Provide the necessary resources for identifying, procuring, and implementing technical solutions to meet the policy requirements, wherever possible.

8.1.6 Disseminate the compliance policy for cybersecurity to all departments, affiliates, and users who are authorized to access the technological and informational assets of the IAU.

8.1.7 Coordinate with relevant departments to monitor compliance and implementation.

8.1.8 Periodically review the policy as per the predetermined schedule.

**The Deanship of Information and Communication Technology shall:**

Adhere to this policy, implement the controls mentioned in this policy, and report any security incidents to the Management of Cybersecurity.

**Top Management, Heads of Departments, Heads of Units, and Advisers shall:**

8.1.9 Ensure the dissemination of this policy to all affiliates within the university or department.

8.1.10 Report any violations or non-compliance with this policy to the Cybersecurity Management.

8.1.11 Ensure that all affiliates within the university shall adhere to the provisions of this policy and report any security incidents or non-compliance with any provisions of this policy to the Head of Cybersecurity Management.

## 9 Ownership of the Policy:

The Head of Cybersecurity Management in the university is responsible for this policy.

## 10 Changes to the Policy:

The policy should be reviewed at least annually or when there are changes in legislative and regulatory requirements. Any changes should be documented and approved by the authorized entity in the IAU.

## 11 Compliance:

All personnel within the IAU, including external parties or contractors, must comply with the provisions of this policy. The Head of Cybersecurity in the university is responsible for ensuring continuous monitoring of compliance and submitting necessary reports periodically to the authorized entity.

Necessary actions should be taken to ensure compliance with the provisions of this policy. This can be achieved through regular reviews by the Cybersecurity department or related departments. Corrective actions should be taken by the authorized entity in the university based on recommendations provided by the Head of Cybersecurity regarding any violations of this policy. Disciplinary actions should be proportional to the severity of the incident, as determined by the investigation. These disciplinary actions may include, but are not limited to:

- Revoking access privileges to data, information technology assets, and connected systems of the IAU.
- Issuing written warnings or terminating the employment of the individual as deemed appropriate by the IAU.

Non-compliance with any provisions of this policy, without obtaining prior exception from the Cybersecurity department, should result in appropriate actions taken in accordance with existing policies and regulations within the IAU, or as deemed suitable, and in line with contractual terms with any individuals or entities contracting with the IAU .

## 12 Related Policies, Standards and Procedures

- DICT.I.06-01.CS.E.V2.0 - General Cybersecurity Policy
- DICT.I.06-02.CS.E.V2.0 - Code- Cybersecurity Compliance Policy
- DICT.I.06-04.CS.E.V2.0 - Asset Management Policy
- DICT.I.06-27.CS.E.V2.0 - Acceptable Use of Assets Policy
- DICT.I.06-60.CS.E.V2.0 Asset Classification Standards
- DICT.I.06-62.CS.E.V2.0 Asset Management Standards
- DICT.I.06-79.CS.E.V2.0 Workstations, Mobile Devices and BYOD Security Standards

## 13 References

| Department Name | The National Institute of Standards and Technology (NTIS | ISO 27001:2013 | Cybersecurity Controls for Remote Work | Cybersecurity Controls for Cloud Computing | Cybersecurity Controls for Sensitive Systems | Cybersecurity Controls for Social Media Accounts for Entities | Basic Cybersecurity Controls |
|---|---|---|---|---|---|---|---|
| Policy for Mobile Devices and Bring Your Own Device (BYOD) Security | AC-19, AC-7(2) | A.6.2.1 | 5-2 | 1-ش-5-2 | 5-52-2 | 4-2 | 6-2 |

---------- End of Document ----------