جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

Clear Desk and Clear Screen Policy

Version: 2.0

CODE: DICT.I.06-26.CS.E.V2.0

1 Table of Cont.

2 Intellectual Property Information

This document is the intellectual property of the Deanship of Information and Communication Technology (DICT) at Imam Abdulrahman bin Faisal University (IAU). The content of this document is intended solely for authorized recipients. Any distribution, disclosure, publication, or copying of this document without written permission from DICT is strictly prohibited.

3 Document Control

3.1 Information

Title	Classification	Version	Status
CLEAR DESK AND CLEAR SCREEN POLICY	RESTRICTED	V2.0	ACTIVE

3.2 Revision History

Version	Author(s)	Issue Date	Changes
V1.0	DR. BASHAR ALDEEB	07/01/2021	CREATION
V1.1	DR. SAMER BANI AWWAD	02/03/2022	REVIEW AND UPDATE
V2.0	BAHA NAWAFLEH	26/12/2023	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

Securing information and technology assets is vital for the success of the IAU. To achieve this goal, the Cybersecurity Department establishes security controls for all technical information, printed documents, and removable storage media. It also ensures the maintenance of secure offices across all IAU facilities to mitigate unauthorized access, information loss, and potential harm to data during both working and non-working hours.

This policy is an integral part of the IAU's overall policy framework and is implemented within the authority granted by the authorized entity. The policy becomes effective from the date of its approval.

5 Objective of the Policy

The purpose of this policy is to raise awareness among all affiliates within the IAU regarding the Clean Desk and Clear Screen Policy. This policy aims to safeguard the IAU's information and technology assets.

6 Applicability and Scope

The provisions of this policy apply to all affiliates or individuals appointed to work within the IAU, whether on permanent or temporary contracts, whether directly or indirectly involved. This includes suppliers, external contractors, and any person granted permanent or temporary access rights to the IAU's data, regardless of the source, form, or nature of the data. This policy also extends to encompass the systems, devices, and databases of the IAU.

7 Policy

7.1 Clean Desk Requirements

7.1.1 Affiliates must ensure that documents, papers, and computer media are stored securely in appropriate lockable cabinets or equivalent forms of secure storage when not in use, especially outside working hours.

7.1.2 All offices must remain clean, organized, and free from university assets containing personal data or classified information with a restricted or higher classification.

7.1.3 If lockable cabinets or file storage cabinets and drawers are not available, office/room doors must be secured if left unattended.

7.1.4 Confidential and restricted work-related information must be secured in safe cabinets when not needed.

7.1.5 Personal, confidential, and restricted data must be disposed of by shredding when printed from printers, copiers, scanners, and fax machines upon completion of the activity, and when no longer needed.

7.1.6 Installation of confidential and critical information/notes or personal data in front of the desk or on bulletin boards is prohibited.

7.1.7 Passwords must be kept confidential and not written on media such as paper or sticky notes.

7.1.8 Users who share or use shared printers, scanners, photocopiers, fax/telex machines, and paper shredders must ensure sufficient protective measures to prevent unauthorized access.

7.1.9 All affiliates must ensure that their work area/office is free from printed materials/documents when not in use.

7.1.10 Users of computer systems must ensure that the information displayed on the screen is not easily viewable by other affiliates, and it must not be kept in a way that allows unauthorized users to glance or quickly view the computer system screen of someone else.

7.1.11 All affiliates responsible for meetings must ensure that no personal data or confidential information is left in the office, whether on the table, paper boards, whiteboards, etc.

7.2 Screen Cleanliness Requirements:

7.2.1 Privacy screens must be installed to support the privacy of all users within the university.

7.2.2 All computer systems must be protected by passwords, screensavers, or similar controls when not in use or inactive for a period of five (5) minutes.

7.2.3 Users must manually secure their computer systems when not in use or when they leave their workstation.

7.2.4 The device must remain locked until the user regains access using the designated identification and authentication procedures.

7.2.5 All user devices located in public areas must have password-protected screens that can be activated after periods of inactivity or use to reactivate the screen.

8 Roles and Responsibilities

The Cybersecurity Management responsibilities:

8.1.1 The Head of Cybersecurity Management is responsible for approving the policy by the authorized party and ensuring its implementation.

8.1.2 The Head of Cybersecurity Management is responsible for endorsing standards, procedures, and guidelines to ensure necessary compliance with the security requirements of university operations.

8.1.3 The Head of Cybersecurity Management is responsible for ensuring alignment between this policy and university operations.

8.1.4 The Head of Cybersecurity Management is responsible for resolving any conflicts arising from this policy.

8.1.5 The Head of Cybersecurity Management is responsible for providing the necessary resources for identifying, procuring, and implementing technological solutions to meet policy requirements wherever feasible.

8.1.6 The Cybersecurity Management must coordinate with relevant departments to monitor compliance and implementation.

8.1.7 The Cybersecurity Management must ensure the necessary security requirements are fulfilled before implementing new solutions/systems within the information technology environment.

8.1.8 The Cybersecurity Management must periodically review the policy according to the established timeline.

The Deanship of Information and Communication Technology shall:

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

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

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

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

8.1.12 Ensure that affiliates within the university must adhere to the provisions of this policy and report any security incidents or non-compliance with any provisions outlined in this policy to the Head of Cybersecurity Management.

9 Policy Ownership

The individual responsible for this policy is the Head of Cybersecurity Management within the IAU.

10 Policy Revisions

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

11 Compliance

All personnel within the IAU, including external parties/contractors, must adhere to the provisions of this policy. The Head of Cybersecurity Management in the IAU must ensure continuous monitoring of compliance, and periodic reports regarding compliance should be submitted to the authorized entity.

Necessary measures must be taken to ensure compliance with the provisions of this policy. This includes conducting periodic reviews by the Cybersecurity Management or relevant departments, and taking corrective actions by the authorized entity within the IAU in accordance with the recommendations provided by the Head of Cybersecurity Management regarding any violations of this policy. Disciplinary actions should be proportionate 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, IT assets, and systems connected to the IAU.
- Issuing written warnings, or terminating the employment of the staff member, or taking appropriate actions as deemed necessary by the IAU.

In cases of non-compliance with any provisions of this policy, without obtaining prior exemption from the Head of Cybersecurity Management, appropriate actions must be taken according to the policies and regulations in place within the IAU, or as deemed appropriate, and in accordance with contractual conditions with individuals or entities contracted by 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 - Cybersecurity Compliance Policy
- DICT.I.06-27.CS.E.V2.0 - Acceptable Use of Assets Policy
- DICT.I.06-21.CS.E.V2.0 - Data Classification Policy
- DICT.I.06-67.CS.E.V2.0 Cybersecurity Incident Management Standards

13 References

Department Name	National Institute for Standards and Technology	ISO 27001:2013	Cybersecurity Controls for Cloud Computing	Cybersecurity Controls for Social Media Accounts of Entities	Cybersecurity Controls for Remote Work	Cybersecurity Controls for Sensitive Systems	Key Cybersecurity Controls
Clean Desk and Clear Screen Policy.	AC-1, AC-11, MP-1, MP-2, MP-4	A.11.2.9	-	-	-	-	-

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