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

جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

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

Protect Printers, Scanners and Photocopiers Policy

Version: 2.0

CODE: DICT.I.06-36.CS.E.V2.0

Table of Contents

1 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.

2 Document Control

1.1 Information

Title	Classification	Version	Status
PROTECT PRINTERS, SCANNERS AND PHOTOCOPIERS POLICY	RESTRICTED	V2.0	ACTIVE

1.2 Revision History

Version	Author(s)	Issue Date	Changes
V1.0	DR. BASHAR ALDEEB	19/02/2021	CREATION
V1.1	DR. SAMER BANI AWWAD	08/07/2022	REVIEW AND UPDATE
V2.0	BAHA NAWAFLEH	25/12/2023	REVIEW AND UPDATE

1.3 Document Review

Date of Next Scheduled Review
01/01/2025

1.4 Distribution List

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

1.5 Approval

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

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

سياسة الأمن السيبراني لحماية الطابعات والماسحات الضوئية وآلات التصوير
Protect Printers, Scanners and Photocopiers Policy

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

3 Introduction

Information protection, along with the protection of information assets and technology, is essential for the success of the university. To achieve this, the Cybersecurity Management develops, establishes, and organizes the necessary security operations to safeguard information and technology assets. This document outlines the cybersecurity policy for protecting printers, scanners, and photocopiers within the office, in accordance with relevant organizational regulations, legislative requirements, and regulations.

This policy is aligned within the framework of the university's policies and under the authority granted by the authorized entity, starting from the date of its approval.

4 Policy Objective

This policy establishes the necessary requirements and procedures for safeguarding printers, scanners, and photocopiers, while providing guidance and security requirements for all affiliates of the university and external parties regarding their responsibilities and obligations in relation to the use of the university's assets and information when utilizing printers, scanners, and photocopiers.

5 Applicability and Scope

The provisions of this policy apply to all affiliates or individuals working within the university, whether under permanent or temporary contracts, whether directly or indirectly involved. This includes suppliers, external contractors, and any individual who has permanent or temporary access rights to the university's data, regardless of its source, form, or nature, as well as to the systems, devices, and databases of the university.

6 Policy

6.1 General Policy Requirements

6.1.1 Users are required, while using shared or personal printers, scanners, photocopiers, or paper shredding machines, to ensure sufficient protection mechanisms for papers and documents to prevent unauthorized access.

6.1.2 Consideration should be given to the physical locations of technical assets such as printers, copiers, and scanners according to the physical security requirements defined in the Physical and Environmental Cybersecurity Policy.

6.1.3 In the case of internal memory in technical assets like printers and scanners, the internal memory should be destroyed in compliance with the university's requirements and relevant legislative and regulatory requirements before disposing of the asset.

6.1.4 Printers and scanners settings should be securely configured, adjusted, and hardened. Examples of such settings and hardening measures include disabling unused services, changing passwords, applying updates, disabling cache storage, and/or automatically deleting stored files.

6.1.5 Scanners should be configured to send files through the university's email and not store sent files in the email inbox.

6.1.6 Identity verification should be enabled on centralized printers, scanners, and photocopiers before printing, scanning, or copying operations.

6.1.7 Monitoring and storing security event logs should follow the Event Logging Policy and Cybersecurity Monitoring.

6.1.8 Adequate awareness should be provided to users regarding cybersecurity risks associated with using printers, scanners, and photocopiers.

6.1.9 Necessary technologies for disposing of classified printed information should be provided immediately after use (such as Cross-cut shredders that cut paper both horizontally and vertically simultaneously).

7 Roles and Responsibilities

The Cybersecurity Management responsibilities:

7.1.1 The Head of the Cybersecurity Management is responsible for approving the policy on behalf of the authority and ensuring its implementation.

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

7.1.3 The Head of the Cybersecurity Management is responsible for ensuring alignment between this policy and the university's activities.

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

7.1.5 The Head of the Cybersecurity Management is responsible for providing the necessary resources to identify, procure, and implement technical solutions to meet the policy's requirements, whenever feasible.

7.1.6 Cybersecurity Management is responsible for disseminating the cybersecurity compliance policy to all departments, affiliates, and authorized users of the university or those who will be granted access to the technical and information assets.

7.1.7 The Cybersecurity Management is responsible for coordinating with relevant departments to monitor compliance and implementation.

7.1.8 The Cybersecurity Management is responsible for periodically reviewing the policy according to the established timeline.

The Deanship of Information and Communication Technology shall:

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

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

7.1.10 Ensure the dissemination of this policy to all affiliates within the university or file.

7.1.11 Report any violations or non-compliance with this policy to the cybersecurity management.

7.1.12 Ensure that all Affiliates within the university must adhere to the provisions of this policy and report any security incidents or non-compliance with the provisions stated in this policy to the Head of Cybersecurity Management.

8 Policy Ownership

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

9 Policy Changes

The policy must 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 within the university.

10 Compliance

All affiliates within the university and external parties (contractors/vendors) must adhere to the provisions of this policy. The Head of Cybersecurity Management in the university must ensure continuous monitoring of compliance and regularly submit necessary reports to the authorized entity.

Necessary measures must be taken to ensure compliance with the provisions of this policy. This can be achieved through periodic reviews conducted by the Cybersecurity Management or relevant departments. Corrective actions should be taken by the authorized entity within the university, following the recommendations provided by the Head of Cybersecurity Management regarding any violation of this policy. Disciplinary actions, proportionate to the severity of the incident and the results of the investigation, may include but are not limited to:

- Revoking access privileges to data, information technology assets, and connected university systems.
- Issuing a written warning, or terminating the employment of the affiliate, as deemed appropriate by the university.

Non-compliance with any provisions of this policy without obtaining prior exemption from the Cybersecurity Management requires appropriate actions to be taken, following the policies and regulations in place within the university, or as appropriate, and in accordance with contractual terms with any individuals or entities contracted with.

11 Related Policies, Standards and Procedures

- DICT.I.06-01.CS.E. V2.0 - Cybersecurity Policy
- DICT.I.06-02.CS.E. V2.0 - Cybersecurity Compliance Policy
- DICT.I.06-32.CS.E. V2.0 - Physical and Environmental Cybersecurity Policy
- DICT.I.06-10.CS.E. V2.0 – Cybersecurity Event Log Management and Cybersecurity Monitoring Policy
- DICT.I.06-50.CS.E.V2.0 Physical Security Standards
- DICT.I.06-68.CS.E.V2.0 Cybersecurity Events Logs and Monitoring Management standards

12 References

Department Name	National Institute for Standards and Technology	ISO 27001:2013	Cybersecurity Controls for Cloud Computing	Cybersecurity Controls for Social Media Accounts for IAU	Cybersecurity Controls for Remote Work	Cybersecurity Controls for Sensitive Systems	Core Cybersecurity Controls
General Policy Requirements	AC-1, AC-11, MP-1, MP-2, MP-4	A.11.2.9	-	-	-	-	-

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