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

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

Cookies Policy

Version: 2.0

CODE: DICT.I.06-12.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
COOKIES POLICY	RESTRICTED	V2.0	ACTIVE

3.2 Revision History

Version	Author(s)	Issue Date	Changes
V1.0	DR. BASHAR ALDEEB	29/01/2021	CREATION
V1.1	DR. SAMER BANI AWWAD	04/06/2022	REVIEW AND UPDATE
V2.0	BAHA NAWAFLEH	23/12/2023	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 technological assets is crucial for the success of the IAU. For this purpose, the Cybersecurity Management defines security controls for all information and data. Personal data is an essential element that must be protected within the IAU and its affiliated entities. Therefore, it is necessary to establish measures and controls to safeguard the data retained, stored, and associated with users on the IAU's websites. This aims to mitigate the risks of unauthorized disclosure, leakage, unauthorized access, tampering, and forgery.

5 Objective of the Policy

This policy establishes guidelines for the practices carried out within the IAU regarding the handling and usage of cookies in its services.

6 Applicability and Scope

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

7 Policy

7.1 Requirements of the General Policy

7.1.1 Regularly review and protect the property of stored cookies on the IAU's website, deleting them as needed for affiliates and beneficiaries.

7.1.2 Store cookies for affiliates and beneficiaries accurately and securely, processing or transferring them in accordance with work requirements.

7.1.3 Obtain explicit consent from data subjects, if necessary and justified by relevant laws and regulations, before collecting and processing cookies.

7.1.4 Clearly indicate the use of cookies for services on the IAU's Website, informing users about the type of data collected, shared, stored, and processed, while granting them the right to disable cookies.

7.1.5 Provide the option to erase stored data through cookies and associated data when possible.

7.1.6 Implement identity protection and encryption technologies to safeguard personally identifiable information stored in cookies.

7.1.7 Ensure that IAU affiliates are aware of the policy's content and understand their roles in protecting personal identification data for both affiliates and beneficiaries.

7.1.8 Implement appropriate technical and organizational measures to ensure that data stored in cookies is only stored when necessary. This applies to the quantity of personal data collected, its processing, storage duration, and access restrictions. The IAU should ensure that personal data is not automatically made available to an unspecified number of individuals without taking measures to protect data privacy.

8 Roles and Responsibilities

The Management of Cybersecurity responsibilities:

8.1.1 The Head of the Cybersecurity Department must approve the policy from the authorized party and work towards its implementation.

8.1.2 The Head of the Cybersecurity Department is responsible for adopting standards, procedures, and guidelines to ensure necessary compliance with security requirements for assembly operations.

8.1.3 The Head of the Cybersecurity Department should ensure alignment between this policy and the assembly's operations.

8.1.4 The Head of the Cybersecurity Department should resolve any conflicts arising from this policy.

8.1.5 The Head of the Cybersecurity Department must provide the necessary resources to identify, acquire, and implement technological solutions to meet policy requirements wherever possible.

8.1.6 The Cybersecurity Department must disseminate the cybersecurity compliance policy to all departments, affiliates, and authorized users of the assembly's technical and information assets.

8.1.7 The Cybersecurity Department is responsible for coordinating with relevant departments to monitor compliance and implementation.

8.1.8 The Cybersecurity Department should conduct regular reviews of the policy according to the defined schedule.

The Deanship of Information and Communication Technology shall:

8.1.9 Commit to and implement this policy, as well as report any security incidents to the Cybersecurity Department.

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 assembly or department.

8.1.11 Report any breaches or non-compliance with this policy to the Cybersecurity Department.

University affiliates shall:

8.1.12 Adhere to the provisions of this policy and report any security incidents or non-compliance with its provisions to the Head of the Cybersecurity Department.

9 Ownership of the Policy

The Head of the Cybersecurity Department in the assembly is responsible for this policy.

10 Policy Changes

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

11 Commitment

All individuals within the assembly and external parties/contractors must adhere to the provisions of this policy.

The Head of the Cybersecurity Department in the assembly is responsible for continuous monitoring of compliance and submitting necessary reports to the authorized party regularly.

Necessary actions must be taken to ensure compliance with the policy. This can be achieved through regular reviews by the Cybersecurity Department or related departments, and corrective actions taken by the authorized party in the assembly based on recommendations from the Head of the Cybersecurity Department in the case of policy violations.

Disciplinary actions, proportionate to the severity of the incident as determined by the investigation, may include:

Revoking access to data, IT assets, and assembly-connected systems.

- Issuing a written warning or termination of employment/service as deemed appropriate by the assembly.
- Non-compliance with any provisions of this policy, without prior exemption from the Cybersecurity Department, necessitates appropriate actions according to assembly policies, regulations, contractual terms, and circumstances.

These sections outline the ownership of the policy, procedures for policy changes, commitment to compliance, and the consequences of non-compliance.

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.06-03.CS.E.V2.0- Data Protection Policy
- ❖ DICT.I.06-21.CS.E.V2.0- Data Classification Policy
- ❖ DICT.I.06-13.CS.E.V2.0- Personal Data Protection Policy
- ❖ DICT.I.06-29.CS.E.V2.0- Encryption Policy
- ❖ DICT.I.06-33.CS.E.V2.0- Access Control Policy
- ❖ DICT.I.06-53.CS.E.V2.0 Data Loss Prevention Standards
- ❖ DICT.I.06-56.CS.E.V2.0 Data Cybersecurity Standards
- ❖ DICT.I.06-58.CS.E.V2.0 Database Security Standards
- ❖ DICT.I.06-61.CS.E.V2.0 Data Protection Standards
- ❖ DICT.I.06-71.CS.E.V2.0 Encryption 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
Requirements of the Public Policy	-	-	-	-	-	-	1-15-2

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