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

Personal Data Protection Policy

Version: 2.0

CODE: DICT.I.06-13.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

1 Table of Contents 2
2 Intellectual Property Information 3
3 Document Control 4
3.1 Information 4
3.2 Revision History 4
3.3 Document Review 4
3.4 Distribution List 4
3.5 Approval 4
4 Introduction 5
5 Objective 5
6 Applicability and Scope 5
7 Policy 6
7.1 General Policy Requirements 6
7.2 Personal Data Protection 8
7.3 Rights of Data Subjects 9
7.4 Privacy by Design Principle 10
7.5 Transfer of Personal Information 10
7.6 Privacy Notice 11
7.7 Privacy Violations 12
7.8 Awareness and Training 13
8 Roles and Responsibilities 14
9 Policy Ownership 15
10 Policy Changes 15
11 Compliance 15
12 Related Policies, Standards and Procedures 16
13 References 17

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
PERSONAL DATA PROTECTION POLICY	RESTRICTED	V2.0	ACTIVE

3.2 Revision History

Version	Author(s)	Issue Date	Changes
V1.0	DR. BASHAR ALDEEB	18/02/2021	CREATION
V1.1	DR. SAMER BANI AWWAD	06/05/2022	REVIEW AND UPDATE
V2.0	BAHA NAWAFLEH	05/01/2024	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 personal data is essential for the success of the IAU's operations. To achieve this, the Data Management Office within the university is committed to enabling measures and controls to mitigate the risks of unauthorized disclosure, leakage, unauthorized access, modification, and tampering of personal data. This document outlines the policy for the protection of personal data within the IAU, in accordance with relevant organizational policies, regulatory procedures, legislative requirements, and regulations.

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

5 Objective

The aim of this policy is to establish the necessary requirements for preserving the privacy and confidentiality of personal data and safeguarding individuals' rights when dealing with personal data within the IAU. This is in accordance with the Personal Data Protection System and the Personal Data Protection Policy issued by the National Data Management Office.

6 Applicability and Scope

The provisions of this policy apply to all affiliates or individuals working within the IAU, including its hospitals and affiliated healthcare centres, whether under permanent or temporary contracts, and whether directly or indirectly engaged. This also includes suppliers, external contractors, and any person with permanent or temporary access rights to IAU data, regardless of the data's source, form, or nature, as well as to the university's systems, devices, and databases.

The following circumstances are exempted from the scope of application of this policy:

- Direct collection or processing of personal data without the knowledge of the data subject, or processing for purposes other than those for which the data was collected, or disclosing the data without consent, or transferring it outside the Kingdom, in the following cases:
- When the collection or processing of personal data is required to fulfil regulatory requirements in accordance with the Kingdom's laws, regulations, and policies, or to comply with legal obligations or enforce an agreement in which the Kingdom is a party.

- When the collection or processing of personal data is necessary to protect public health or safety or the vital interests of individuals.

7 Policy

7.1 General Policy Requirements

7.1.1 Based on the data management, governance, and personal data protection strategy and plan, the Cyber Security Management Office must develop a plan for safeguarding personal data that fulfils operational and strategic personal data protection requirements. This plan should align with the Personal Data Protection Policy issued by the National Data Management Office. The plan should include a roadmap outlining activities and milestones aimed at achieving and maintaining full compliance with the Personal Data Protection Policy issued by the National Data Management Office. It should also specify the necessary resources and budget for achieving full compliance with the Personal Data Protection Policy.

7.1.2 All possible options for data subjects must be identified and their implicit or explicit consent obtained regarding the collection, usage, or disclosure of their data.

7.1.3 Disclosure of personal data to external parties should be limited to specific purposes outlined in the privacy notice for which the data subject has provided implicit or explicit consent.

7.1.4 Processing of personal data should be restricted to the purposes specified in the privacy notice, retaining it as long as necessary to achieve those purposes or as required by the laws, regulations, and policies in the Kingdom. Safe disposal methods should be employed to prevent leakage, loss, misappropriation, misuse, or unauthorized access.

7.1.5 Privacy controls and mechanisms should include appropriate technical means, which should be assessed by the IAU.

7.1.6 Personal data should be protected throughout its acquisition, transfer, processing, and disposal stages.

7.1.7 Collection of personal data should be minimized to the extent necessary to fulfil the specified purposes in the privacy notice.

7.1.8 The Office of Data Management in the IAU is responsible for identifying, documenting, and obtaining approval for the storage of personal data based on the purposes for which it was collected and will be

used. In cases where data collection is necessary, the reasons should be clarified, including the need for collection, categorization of personal data, business requirements, and the purpose of collecting each category of personal data.

7.1.9 Personal data should be accurately and fully retained in relation to the specified purposes outlined in the privacy notice.

7.1.10 Personal data should not be used for training or research purposes.

7.1.11 Regular review of personal data should be conducted, and data should be deleted as per operational requirements or the expiration of the retention period.

7.1.12 An initial assessment of personal data protection should be carried out by the IAU to evaluate the existing personal data protection environment. The assessment should include at minimum:

- Identification of types of personal data.
- Location and method of storing personal data.
- Current processing and uses of personal data.
- Challenges of personal data protection in compliance with the issued Personal Data Protection Policy by the National Data Management Office.

7.1.13 Data hosting should comply with the regulations set by the National Cyber Security Authority to ensure that data remains within the Kingdom of Saudi Arabia, either on the university's servers or with national cloud service providers.

7.1.14 The IAU is required to store and process personal data exclusively within the Kingdom of Saudi Arabia. This requirement must be included in contracts or related documents with external parties. If the need arises to share personal data with a foreign entity, approval from the National Data Management Office must be obtained.

7.1.15 The Office of Data Management within the IAU should conduct internal audits to monitor compliance with personal data protection rules. The results of these audits should be documented in a report submitted to the Data Protection Officer in the university. In cases of non-compliance, corrective actions should be taken and reported to the regulatory authority and the National Data Management Office.

7.1.16 In cases where data management tasks are outsourced by the IAU to external parties, compliance of the external party or any subsequent contracts they may engage in to process personal data should be verified in accordance with the personal data protection requirements of the university.

7.1.17 The IAU should maintain an audit log for a reasonable period of no less than 24 months, which should be made available to the National Data Management Office upon request in accordance with the Personal Data Protection Policy issued by the National Data Management Office. The log should, at a minimum, include records of each data collection or processing activity related to any personal data.

7.1.18 Any changes or updates related to systems, laws, and regulations should be monitored and reflected in the Personal Data Protection Policy.

7.2 Personal Data Protection

7.2.1 Measures must be in place to ensure the ability to recover and access personal data promptly in the event of a physical or technical incident.

7.2.2 Data concealment and obfuscation techniques must be employed to safeguard personal data.

7.2.3 The Office of Data Management must carry out effective testing and assessment of technical and organizational measures to ensure the security of personal data processing.

7.2.4 An annual risk assessment should be conducted for the operation and usage of information systems containing personal information. This assessment should encompass data collection, processing, storage, and transmission across all systems, whether performed manually or automatically. The risk assessment results should include at a minimum:

- Documentation
- Impact analysis and likelihood assessment
- Evaluation based on regulatory obligations and criticality.

7.2.5 Personal data should be sufficient, relevant, and limited to what is necessary for the intended processing purposes.

7.2.6 Personal data must be accurate, appropriate, and up to date. Appropriate measures should be taken to promptly rectify or correct inaccurate personal data relevant to the purposes.

7.2.7 If personal data is obtained from sources other than the data subject, the data subject should be informed. The IAU should also send a privacy notice to the data subject.

7.2.8 Appropriate security controls must be implemented to protect personal data from leakage, damage, loss, misappropriation, misuse, unauthorized access, alteration, or unauthorized modification — in accordance with guidelines issued by the National Cyber Security Authority and the National Data Management Office.

7.2.9 Administrative controls and technical measures adopted in the information security policies of the IAU should be employed to ensure personal data protection, including but not limited to:

7.2.10 Granting access rights to data based on roles to avoid overlapping responsibilities and minimize dispersion of authority.

7.2.11 Applying administrative and technical procedures that document the stages of data processing, allowing identification of the responsible user for each stage (usage logs).

7.2.12 Having affiliates engaged in data processing operations sign an undertaking to maintain data confidentiality and only disclose it as per the policies, procedures, regulations of the IAU, and relevant laws.

7.2.13 Selecting personnel engaged in data processing operations based on their integrity and responsibility, in accordance with the nature and sensitivity of the data and the access policy adopted by the IAU.

7.3 Rights of Data Subjects

7.3.1 The Data Management Office must notify the data subject of the legal basis or actual need for collecting their personal data and the purpose thereof. Data must not be processed in a manner inconsistent with the purpose for which consent was given, whether implicit or explicit.

7.3.2 Data subjects have the right to withdraw their consent for the processing of their personal data at any time, unless there are legitimate reasons that require otherwise.

7.3.3 Data subjects have the right to access their personal data in order to review, correct, complete, update, or request the disposal of unnecessary portions. They are also entitled to obtain a clear copy of their personal data.

7.3.4 Methods and mechanisms must be defined and provided through which data subjects can access their personal data for review, updating, and correction.

7.4 Privacy by Design Principle

7.4.1 The Data Management Office must adopt the principle of privacy by design and ensure that privacy requirements are met in current or new systems and programs that collect or process personal data.

7.4.2 The Data Management Office must regularly conduct a privacy impact assessment for all systems that collect or process personal data. This assessment includes:

- Applying principles of personal data protection.
- Fulfilling responsibilities of the control unit.
- Implementing security controls to protect personal information.
- Ensuring the legal basis for processing personal data.
- Guaranteeing the collection, use, processing, storage, and sharing of personal data according to authorized purposes specified in the privacy notice.
- Adopting the privacy by design principle for all new or modified systems and processes.

7.4.3 The Head of Cybersecurity Management must implement appropriate techniques for identity concealment of data and encryption to protect personal data.

7.4.4 The Data Management Office must fulfil the following documentation requirements and make them accessible through data subjects' records regarding personal data processing activities:

- Objectives of processing personal data.
- Processing activities conducted on personal data.
- Processing categories of personal data.
- Agreements and mechanisms for transferring personal data to and from other organizations after obtaining consent or a request from the data subject.
- Retention schedules for personal information.
- Existing security controls to protect personal information.

7.5 Transfer of Personal Information

7.5.1 Any transfer of personal data must be based on the consent or request of the data subject.

7.5.2 Before transferring personal data outside the office, a privacy impact analysis must be conducted.

7.5.3 Appropriate notifications, including recipients' details and the purpose of each disclosure, must be sent to the data subject before transferring personal data to them. This notification should include the date, nature, and purpose of each disclosure, as well as the names and addresses of the recipients to whom the personal data has been disclosed.

7.5.4 Data protection measures must be ensured at the receiving party, including the following details:

- Name of the organization and relevant details.
- Objectives of processing personal data.
- Categories of individuals and processing of personal data.
- Categories of recipients of personal data.
- Agreements and mechanisms for transferring personal data.
- Retention schedules for personal information.
- Relevant technical and organizational controls implemented in the office.

7.6 Privacy Notice

7.6.1 The office of data management must identify, document, approve, and implement the requirements for providing a privacy notice to the data subject regarding the following:

7.6.2 Activities that affect the privacy of personal data, including collection, use, sharing, retention, and disposal.

7.6.3 How the IAU uses personal data and the consequences of exercising or not exercising those options.

7.6.4 The right to access and correct personal data if necessary.

7.6.5 The types of personal data collected by the IAU and the purpose for which that information is collected.

7.6.6 How the IAU uses personal data.

7.6.7 If the IAU shares personal data with external entities, the categories of those entities and the purposes of such sharing.

7.6.8 How individuals can access or obtain their personal data.

7.6.9 How personal data is protected.

7.6.10 The duration for which personal data will be stored.

7.6.11 The right to request access, correction, erasure, or restriction of processing of personal data, as well as the right to object to its processing and the right to data portability.

7.6.12 The right to withdraw consent at any time.

7.6.13 The right to lodge complaints, ask questions, or express concerns to the IAU, and to file a complaint with the supervisory authority.

7.6.14 Whether the provision of personal data is legally required or contractually necessary, and if the data subject is obligated to provide personal data and has been informed of the potential consequences of not providing this data.

7.6.15 Changes in practices or policies affecting personal data or changes in activities affecting privacy, before or as soon as possible after the change.

7.6.16 The office of data management must inform the data subject before lifting processing restrictions if processing is restricted by the data subject. Personal data must only be processed, excluding storage, with the consent of the data subject.

7.6.17 The office of data management must notify any correction, erasure, or processing restriction of personal data to each recipient to whom the data has been disclosed, and the controller must inform the data subject upon request.

7.7 Privacy Violations

7.7.1 The office of data management must develop, document, approve, and implement a privacy incident response plan and execute it when necessary.

7.7.2 The office of data management must prepare and document the necessary procedures for managing and addressing privacy violations. This includes specifying tasks and responsibilities related to the specialized team and determining the cases in which regulatory authorities and the IAU should be notified, based on the administrative hierarchy and the severity of the impact.

7.7.3 If a privacy violation occurs, the office of data management must follow the incident response plan and procedures and notify the Head of Cybersecurity Management.

7.7.4 The IAU must develop, document, approve, and implement procedures for notifying data subjects about privacy violations without delay.

7.7.5 The office of data management must notify the regulatory authority in case of a personal data breach within the timeframe specified in the Data Protection Policy issued by the National Data Management Office. The specified timeframe for notification is 72 hours.

7.7.6 The office of data management must document the process of managing data breaches for immediate management and resolution of personal data protection violations. This documentation is crucial for determining the functions and responsibilities of the relevant team. The data breach management process should include, at a minimum:

- Conducting an incident review
- Formulating an immediate response to the incident
- Implementing a permanent corrective action
- Conducting tests on corrective measures to verify the effectiveness of personal data protection solutions.

7.8 Awareness and Training

7.8.1 The office of data management must develop a comprehensive awareness and training program, document it, gain approval for it, implement it, and regularly update it. The purpose of this program is to ensure that affiliates are knowledgeable about their responsibilities and privacy procedures. It includes basic privacy training as well as targeted privacy training based on the roles of affiliates who are responsible for personal data or engaged in activities involving personal data.

7.8.2 The training program should include, at a minimum, the following topics:

- The importance of protecting personal data, its impacts, and consequences for the organization and/or data subjects.
- Definition of personal data.
- Data subjects' rights.
- Responsibilities of the IAU and data subjects.
- Notifications: When to notify the organization or data subjects, and how to handle requests for collection, processing, and sharing of personal data.

8 Roles and Responsibilities

The office of data management responsibilities:

8.1.1 The CEO of the data management office should approve the policy and work on its implementation.

8.1.2 The CEO of the data management office should establish the standards, procedures, and guidelines to ensure necessary compliance with the security requirements of the Eastern Health Collection operations.

8.1.3 The CEO of the data management office should ensure alignment between this policy and the activities of Eastern Health Collection.

8.1.4 The CEO of the data management office should resolve any conflicts arising from this policy.

8.1.5 The CEO of the data management office should provide necessary resources to identify, acquire, and implement technological solutions to fulfil policy requirements where feasible.

8.1.6 The management of the data management office should periodically review the policy according to the established timeline.

8.1.7 The management of the data management office should coordinate with relevant departments for monitoring compliance and implementation.

The Director of Legal Affairs shall:

8.1.8 Identify the laws and regulations applicable to Eastern Health Collection.

8.1.9 Implement the legal aspects concerning data privacy.

8.1.10 Define privacy requirements in contracts and confidentiality agreements in coordination with the Dean of Deanship of Human Resources.

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

8.1.11 Ensure the dissemination of this policy to all affiliates within Eastern Health Collection or the file.

8.1.12 Report any breaches or non-compliance with this policy to the data management office.

8.1.13 Ensure that users of Eastern Health Collection's information and technology assets are responsible for complying with this policy and reporting any security incidents or non-compliance with this policy to the data management office.

9 Policy Ownership

The individual responsible for this policy is the CEO of the Data Management Office at Eastern Health Collection.

10 Policy Changes

The policy must be reviewed annually at a minimum or in the event of significant changes to the policies, organizational procedures of Eastern Health Collection, or relevant legislative and regulatory requirements. Changes must be documented and approved by the authorized party at Eastern Health Collection.

11 Compliance

All affiliates at Eastern Health Collection and parties (external/contractual) must comply with the provisions of this policy. The Head of Cybersecurity at IAU Collection must ensure continuous monitoring of compliance and submit necessary reports to the authorized party periodically.

Necessary measures must be taken to ensure compliance with the provisions of this policy. This can be achieved through regular reviews conducted by the Data Management Office or relevant departments. Corrective actions must be taken by the authorized party at Eastern Health Collection in accordance with recommendations provided by the CEO of the Data Management Office regarding any violation of the policy. Disciplinary actions must be proportionate to the severity of the incident based on the investigation's findings. Disciplinary actions may include but are not limited to:

- Revoking access rights to data, information technology assets, and connected Eastern Health Collection systems.
- Issuing a written warning or terminating the affiliate's service as deemed appropriate by Eastern Health Collection.

Failure to comply with any provisions of this policy - without prior authorization from the Data Management Office - requires appropriate actions to be taken in accordance with the policies and regulations in effect at Eastern Health Collection or as deemed appropriate and contractual terms with any individuals or entities contracted with.

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.06-29.CS.E.V2.0 - Encryption 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.06-04.CS.E.V2.0 - Asset Management 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.06-83.CS.E.V2.0 Data Diode Standards
- DICT.I.04-35.CS.E.V2.0 Backup and Restoration Procedures
- DICT.I.06-62.CS.E.V2.0 Asset Management Standards
- DICT.I.06-71.CS.E.V2.0 Encryption Standards
- DICT.I.04-35.CS.E.V2.0 Backup and Restoration Procedures

13 References

Department Name	European General Data Protection System	National Institute of Standards and Technology (NIST)"	ISO 27001:2013	Cybersecurity Controls for Cloud Computing	Cybersecurity Controls for Social Media Accounts for Entities	Cybersecurity Controls for Remote Work	Cybersecurity Controls for Sensitive Systems	Basic Cybersecurity Controls
Data and Information Security	Article 5 to 46	Appendix J	A.18.1.4	-	-	-	-	3-7-2

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