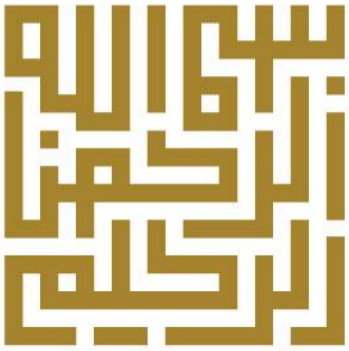
جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

Vice Presidency for Development and Community Partnership

Data Governance Policies at Imam Abdulrahman bin Faisal University

Data Management Office

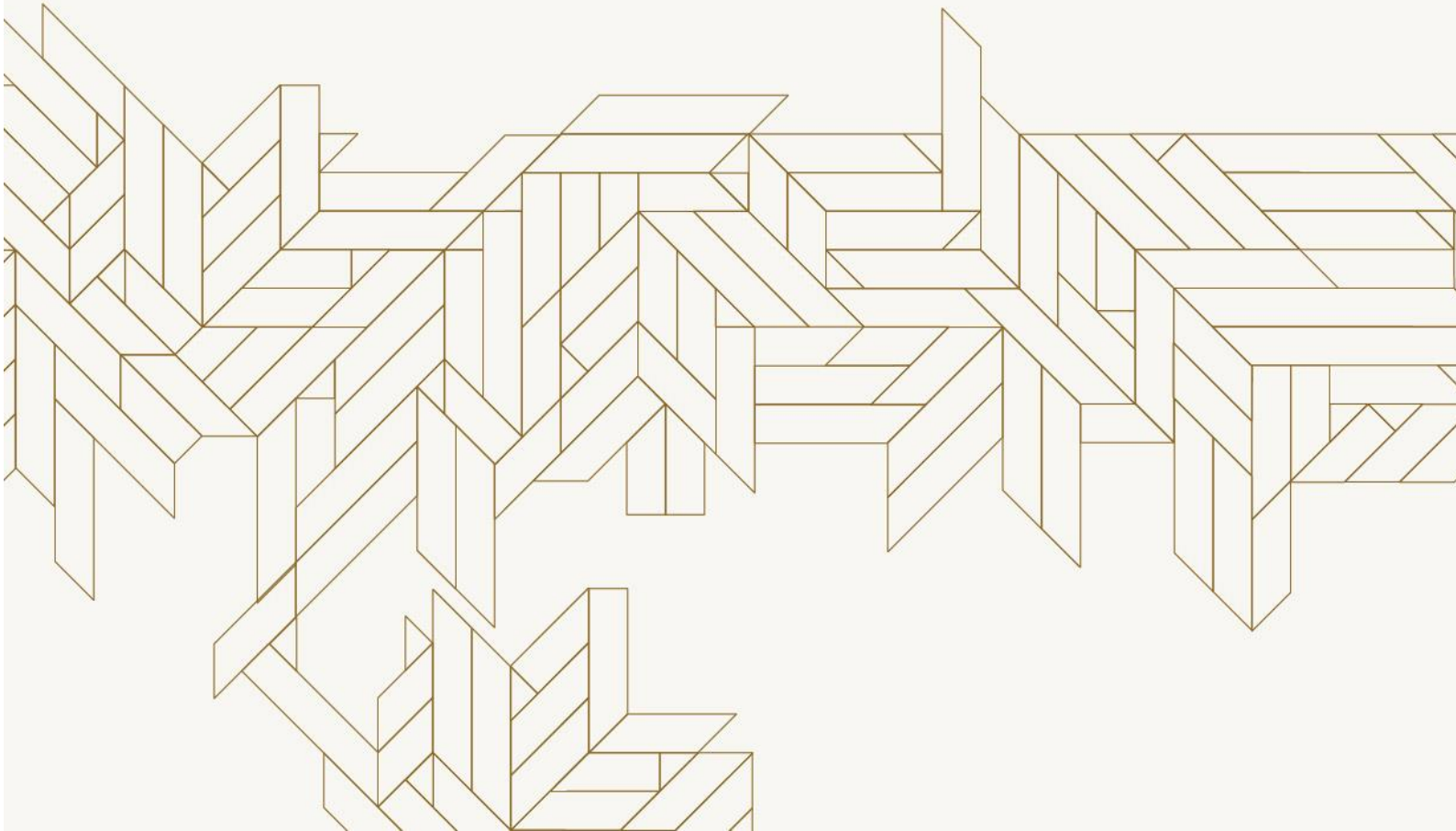
2022



This Guidebook was approved by

Imam Abdulrahman bin Faisal university board meeting number (101) on 6/4/1444 AH

The Board of Trustees of Universities meeting number (14) on 24/8/1444 AH



Contents

1. Introduction

In the era of digital transformation, data is one of the most important assets owned by the university, so the Office of Data Management was established at Imam Abdulrahman bin Faisal University by a decision of His Excellency the President of the University No. (42/42708) dated 4/7/1442 AH, in compliance with Royal Order No. (59766) dated 20-11-1439 AH, which includes the establishment of a data management office in government agencies linked to the first official in the entity, where the importance of the Data Management Office lies in preserving these assets, enabling them and enhancing the value gained from them in decision-making and looking ahead to the future.

1.1 Vision of Data Management Office at Imam Abdulrahman bin Faisal University

A distinguished university in data governance and empowerment in a way that enhances the university's vision and objectives.

1.2 Mission

Managing the university's national data, and working on its digitization, development and empowerment to enhance assets and capabilities and protect personal and sensitive data, by developing the necessary strategies, legislation, policies and controls issued by the National Data Management Office and supporting their application and ensuring compliance with them.

1.3 Objectives

1. Developing systems, policies, standards and controls for data management and personal data protection at the university level.
2. Supporting internal bodies in the application of data management systems, standards and policies and the protection of personal data.
3. Follow up the compliance of internal entities with data management systems, standards and policies and the protection of personal data by building relevant performance measurement indicators.
4. Develop strategies and programs to benefit from the university's data and utilize it to support decision-making and support research projects.

1.4 Responsibilities of IAU Data Management Office

- Identifying the needs and requirements of the Data Management Office in order to contribute to the success of the tasks assigned to it.
- Establishing communication controls between the office and the relevant authorities inside and outside the university.
- Controlling the communication between the National Data Management Office and the various entities in the university.
- Following- up the data of the academic and administrative bodies within the university according to the annual report forms from the " Adaa" platform.
- Providing technical services and solutions to university units and related parties
- Standardization of data handling in all university entities.
- Easy and accurate real-time determination to enhance the university's financial statements.
- Reduce the costs of IT operations and the team dedicated to reporting and reduce errors, conflicts, and unnecessary redundancies.
- Increasing the reliability and integrity of available data
- Carrying out new types of analysis as needed

- Reduce costs of accessing historical data.
- Complete other tasks as directed by the supervisor of the Strategic Planning Department.
- Availability and utilization of data for research purposes.

1.5 IAU Data Governance Policies Preparation

The data governance policies of Imam Abdulrahman bin Faisal University have been prepared in line with the data governance policies issued by the National Data Management Office and based on the evidence issued by the Office, namely :

- National Data Governance Policy

  The second edition on26/05/2021

  PoliciesAr.pdf (sdaia.gov.sa)

This English version was translated and prepared by the Data Management Office at Imam Abdulrahman bin Faisal University by counting on the above-mentioned document.

2. Terminologies and Definitions

The following is an explanation of what is meant by the words and terms in the document as defined in the National Data Governance Policy Manual published on the website of the National Data Management Office.

Verification: Ensure the identity of any user, process, or device as a prerequisite for allowing access to technical resources. **Permit:** Define the rights and privileges of access to data and technical resources of any user, program, or process, and control the levels of reaching it. **Availability of data:** Ensure appropriate and reliable access to data when needed. **Confidentiality of data:** Maintain authorized restrictions on access to or disclosure of data. **Data Integrity:** Protect data from unauthorized modification or destruction.	**Data:** A set of facts in their initial form or in a disorganized form such as numbers, letters, images, video, audio recordings or emoticons. **Personal data:** Every statement - whatever its source or form - will lead to the individual being specifically identified, or make it recognizable directly or indirectly when combined with other data, including, but not limited to, name, ID numbers, addresses, contact numbers, bank, and credit card numbers, still or animated user photos, and other data Personalized **Data access:** The ability to logically and physically access the data and technical resources of the entity for the purpose of use.

Protected Data:
Data classified as (strictly confidential, confidential, restricted)

Processing of Personal Data:
All operations conducted on personal data by any means, whether manual or automated, including, but not limited to, collecting, transmitting, storing, sharing, destroying, analyzing, extracting patterns, inferring from and linking data with other data.

Controller:
Any government agency or independent public legal entity in the Kingdom, and any person with a natural or private legal capacity; specifies the purpose and manner of processing personal data; whether the data is processed by it or by the processing authority.

Processing Entity:
Any government agency or independent public legal entity in the Kingdom, and any person with a natural or private legal capacity; processed personal data for and on behalf of the Controller.

Disclosure of Personal Data:
Enabling anyone - except the controller - to obtain, use or access personal data by any means or for any purpose.

Data access level:
A level based on permissions and privileges that restrict access to data and technical resources to authorized persons as required to accomplish their assigned tasks and responsibilities.

General information:
Data after processing – unprotected – received, produced, or handled by public bodies regardless of their source, form or nature.

Open Data:
A specific set of public information - machine-readable - is available to the public free and unrestricted and can be used or shared by any individual or public or private entity.

Sensitive data:
Data whose loss, misuse, unauthorized access, or modification would cause serious harm or adversely affect national interests, the activities of government agencies or the privacy of individuals and the protection of their rights.

Data Classification Levels:
The following classification levels: (strictly confidential), (confidential), (restricted), (general)

Metadata:
Information that describes the data and its characteristics, including business, technical and operational data.

Machine-readable data:
Means data structured in a specific format that can be read and processed automatically using computers, tablets, and other devices.

National Open Data Platform:
It is a unified national platform at the level of the Kingdom concerned with the management, preservation, and publishing of open data sets.

Open Data License:
License for regulating the use of open data.

Open Format:
Any widely accepted format that is not proprietary, not specific to a particular platform, and is machine-readable, enables the automated processing of such data, and facilitates analysis capabilities and research.

Applicant:
Any public or private sector, third sector, or individual applying for data sharing.

Individual:
The person applying for access to public information.

Personal Data Holder:
The natural person to whom the personal data relate or whoever represents him or whoever has legal authority over him or her.

Personal Data Leakage:
Disclosure of personal data, obtaining it, or enabling access to it without a permit or legal basis, whether intentionally or unintentionally.

Implied Consent:
Consent not expressly given by the data subject, but implicitly given by the person's actions and the facts and circumstances of the situation, such as signing contracts or agreeing to terms & conditions.

Third Parties:
Any government agency or independent public legal entity in the Kingdom, and any person with a normal or private legal capacity other than the data subject, the controller or the processing entity and authorized persons, that is concerned with the processing of personal data.

Public Entity:
Any government agency or independent public legal entity in the Kingdom, or any of its affiliates, any company that manages public facilities and national infrastructure or its operation or maintenance, or the performance of a public service in relation to the management of such facilities or infrastructure.

Regulator:
Any government agency or independent public legal entity that handles regulatory or supervisory functions and responsibilities for a specific sector in the Kingdom of Saudi Arabia based on a statutory document.

Office of the Authority:
Data Management and Privacy Office in the public entity.

Office:
National Data Management Office.

Child:
Every person under the age of eighteen years.

Eligibility:
The person's authority to issue actions in a legally significant manner.

Business Data Representative:
Is the person responsible for the data collected and retained by the public entity in which he works, often at a high administrative level. It can be found more than one business data representative.

Data User:
Any person who is granted access to the data for the purpose of accessing, using, or updating it in accordance with the tasks authorized by the business data representative.

Data Sharing Request:
Custom Data Sharing Request Form which includes information about the applicant, the data requested, and the purpose for which data sharing was requested.

Data Sharing Agreement:
A formal agreement signed between two parties – a government entity with any other party - to agree to share data according to specific terms and conditions and in accordance with the principles of data sharing.

Security Controls:
Devices, procedures, policies, and physical safeguards used to ensure the integrity, protection, means of processing and access to data.

Disclosure:
Enabling anyone - except the controller - to obtain, use or access personal data by any means and for any purpose.

Privacy Notice:
It is an external statement addressed to individuals that explains the content of personal data, the means of collecting them, the purpose of processing them, how to use them, the entities with which this data will be shared, the period of retention, and the mechanism of disposal.

Privacy Policy:
It is an internal document addressed to the employees of the entities that clarifies the rights of the data subjects and the obligations that must be complied with to preserve the privacy of the data subjects and protect their rights.

Transfer of Personal Data:
Sending personal data to a party outside the geographical borders of the Kingdom – by any means – with the aim of processing it, whether directly or indirectly, in accordance with the specific purposes based on legal grounds, including transportation for security purposes, for the protection of public health or safety, or in implementation of an agreement to which the Kingdom is a party.

Data Sharing Mechanism:
The way data is shared - includes the means of data transmission, the parties involved in sharing, and participation form: Direct Engagement, Service Provider Engagement, Multi-Party Engagement.

Less Eligibility:
Who has incomplete eligibility, such as the young person who is distinguished - who is over seven and under eighteen years of age – the careless, the foolish, the mentally handicapped, and so on.

Guardian:
One of the parents or a person who has guardianship over the affairs of the child in accordance with the provisions of the Shariah or the relevant regulations.

Guardianship:
An authority established by the Shariah for the guardian that gives him the authority to act and manage the affairs of the child on his behalf with regard to his body, self, money and what achieve his interests, including making decisions regarding the processing of his personal data.

Accreditation List:
A list approved by the National Data Management Office containing the names of countries that have a sufficient level of protection of data subjects' rights in relation to the processing of their personal data.

Government data:
Is the data produced by government agencies.

Unprocessed data:
Data that has not been subjected to advanced processes of processing and is exchanged in its initial form, such as basic citizen data, which is displayed on the national identity card, except for processing imposed by laws, regulations, and policies for the purpose of data sharing.

Government services:
The basic services provided by government agencies, which can be provided by a third party on behalf of the government agency.

Data Provider:
Any individual, government entity or private entity that directly or indirectly supplies data or provides data products for financial compensation.

Explicit Consent:
Written or electronic consent that is explicit and specific and issued with the free and absolute will of the data subject indicating his acceptance of the processing of his personal data.

Sensitive Personal Data:
Any personal statement that includes a reference to the child's origin, ethnic or tribal similarities, religious, intellectual, or political beliefs, or indicates his membership in civil associations or institutions. as well as criminal and security data, biometric identification data, genetic data, health data, location data, and data indicating that the individual is of unknown parents.

Direct Marketing:
Any communication, by whatever means, through which a marketing or advertising material is directed to a specific person.

Direct Transfer:
Transferring personal data from the sending party to the receiving party without passing the data to any other party.

Indirect transfer:
Transferring personal data from the sending party to the receiving party through one or more other parties.

Data Beneficiary:
Any individual, government entity or private entity that requests data or benefits from data products in exchange for money.

Marketing:
An activity of exchanging, trading, or supplying raw data or processed data in exchange for cash or other in-kind value.

Government Agency:
Any government agency or independent public entity in the Kingdom, or any of its affiliates. Any company that manages, operates, or maintains public facilities or national infrastructure, or carries out a public service in relation to the management of such facilities or infrastructure, shall be considered as the government entity.

Data Sample:
Data that is used to build, train, and test predictive models and AI algorithms to reach certain results.

Artificial Intelligence Technologies:
It is a set of predictive models and advanced algorithms that can be used to analyze data and predict the future or facilitate decision-making on future predicted events.

Accidental transfer:
The transfer of personal data on an infrequent or regular basis – usually on a one-off basis – to a limited number of persons, for example, the transfer of data for the purpose of utilizing a service in another country for the benefit of the data subject.

Data products:
Data-driven services or applications after using data with the aim of creating added value by combining, enriching, configuring, analyzing or representing other data, including but not limited to predictive or descriptive insights and analytics, interactive dashboards (platforms) and others.

Revenue Generation from Data:
Transform intangible value of data into real or material value directly (by supplying unprocessed data) or indirectly (by supplying data products)

Revenue generation model:
The strategy of managing the entity's revenue flows and the resources required for each revenue flow and the target consumers.

Pricing model:
The mechanism used to determine the in-kind value (price) of data and data products.

Facial recognition techniques: Techniques that enable analysis of key facial features (biometrics) to identify the personal identity of individuals in still or (visual) images. **Developer:** Any normal or legal personality that develops artificial intelligence systems by building predictive models using data and algorithms to achieve specific goals. **User:** Any normal or legal personality that applies or uses artificial intelligence systems to achieve specific goals. **Data Subject:** The individual to whom the personal data relate or whoever represents him or who has legal jurisdiction over him.	**Business model:** A structure that describes the way in which market value can be created by exploiting business opportunities, including key partners, key activities, customer segments, revenue model and revenue streams, and explains the logical links between them and how they work together. **Private party:** Any private legal person licensed to work in the Kingdom – whether local or foreign - is considered as a private individual who is a citizen or an official resident of the Kingdom and who provides data or data products. **Non-profit:** Any non-governmental entity licensed to work in the Kingdom and provide its services and products in a non-profit manner.

3. Data Governance Policies

To raise the level of maturity of the field of data and artificial intelligence and to promote the maximum utilization of data wealth and its protection, Imam Abdulrahman bin Faisal University adopts a set of policies that were derived from the policies issued by the National Data Management Office regarding national data governance, which are summarized as follows:

Data Classification Policy

Protecting the confidentiality of national data and their classification on four levels.

Personal Data Protection Policy

Organize the collection, processing and sharing of personal data and the preservation of digital national sovereignty.

Data Sharing Policy

Promote the sharing of data to achieve complementarity between government agencies and to obtain data from their sources.

Information Freedom Policy

Organize the access of beneficiaries to public information or obtain it in all its forms from government agencies.

Open Data Policy

Open (unprotected) data and information are made available to the general beneficiary.

Children and their Equivalent Personal Data Protection Policy

Assisting competent authorities in protecting children and those of similar status from potential risks (violence, abuse, threat, or exploitation) arising from the collection and processing of their personal data through websites and digital applications.

General rules for transferring the personal data outside the geographical borders of the Kingdom

Maintaining digital national sovereignty over personal data and working to provide the best levels of protection when transferring personal data outside the geographical borders of the Kingdom to ensure the preservation of the privacy of its owners and the protection of their rights.

4. Policy 1: Data Classification Policy

The provisions of this policy apply to all data collected, owned, produced, or dealt with by Imam Abdulrahman bin Faisal University, regardless of its source, form, or nature, including paper records, meetings, communications through means of communication and applications, e-mail messages, data stored on electronic means, audio or video tapes, maps, photographs, manuscripts, handwritten documents, and any other form of recorded data.

4.1 Key principles of data Classification

Principle 1: The principle of data is to be available

The principle in the data is to be available (in the development field) unless its nature or sensitivity requires higher levels of classification and protection, and very confidential (in the political and security field) unless its nature or sensitivity requires lower levels of classification and protection.

Principle 2: Necessity and proportionality

The data are classified into levels according to their nature, level of sensitivity, and degree of impact, taking into account the balance between their value and degree of confidentiality

Principle 3: Classification in a timely manner

The data is classified when it is created or when it is received from other parties and the classification is within a specified period of time.

Principle 4: Higher level of protection

The higher level of classification is adopted when the content of an integrated set of data contains different levels of classification.

Principle 5: Segregation of duties

The tasks and responsibilities of workers shall be separated - in relation to the classification of data, access to it, disclosure, use, modification or destruction - in a way that prevents overlap of competence and avoids the dispersion of responsibility.

Principle 6: The need to know

Access to and use of data is restricted on the basis of the actual need for knowledge, and for the minimum number of workers possible.

Principle 7: Minimum Privileges

The management of the employees' privileges shall be restricted to the minimum privileges necessary for the performance of the tasks and responsibilities entrusted to them.

4.2 Levels of data Classification

The data owned by Imam Abdulrahman bin Faisal University or received from internal or external parties, or dealt with according to the classification levels of the main data received from the National Data Management Office in line with the level of impact resulting from the disclosure or leakage of these data, as shown in the table below:

Degree of impact	Classification Level	Description
High	**Strictly Confidential**	Data shall be classified as **strictly confidential** if unauthorized access to, or disclosure of, such data or its content would result in significant, exceptional and irreparable harm to: • The national interests, including violation of agreements and treaties, damage to the Kingdom's reputation, diplomatic relations, political affiliations, operational efficiency of security or military operations, national economy, national infrastructure, or government business. • The performance of public bodies to the detriment of the national interest. • The health and safety of individuals on a large scale and the privacy of senior officials • Environmental or natural resources.
Average	**Confidential**	Data shall be classified as **confidential** if unauthorized access to or disclosure of the data or its content would cause serious harm to: • National interests such as partial damage to the reputation of the Kingdom, diplomatic relations or the operational efficiency of security or military operations, the national economy or infrastructure and governmental actions • There is a financial loss at the organizational level that results in the bankruptcy or inability of the parties to perform their tasks or a serious loss of competitiveness or both • Causes serious harm or injury affecting the lives of a group of individuals.

		• Lead to long-term damage to environmental or natural resources. • Investigation of major systemically defined cases, such as terrorist financing cases.
Low	**Restricted**	Data shall be classified as **restricted** if unauthorized access to, or disclosure of, such data or its content would result in: • Limited negative impact on the work of public bodies or economic activities in the Kingdom or on the work of a specific person. • Limited damage to the assets of any party and limited loss on its financial position and competitiveness. • Limited damage in the near term to environmental or natural resources.
There is none	**Public**	Data shall be classified as **public** when the unauthorized access, disclosure or disclosure of such data does not result in any of the above effects in the absence of any effect on the following: • National interest • Activities of the entities • Individual Interests • Resources Environment

Table 1: Data Classification Levels

Based on the classification levels mentioned in the previous table, each data owner at the university in cooperation with the Data Management Office at the university determines and applies the appropriate security controls to protect the data to ensure that it is dealt with, processed, shared, and disposed of safely.

4.3 Data Classification Controls

Based on the classification levels, the University determines and applies appropriate data protection security controls to ensure that they are handled, processed, shared, and disposed of securely, and if the data is not classified when created or received in accordance with the classification criteria, such data is treated as "restricted" until it is properly classified. Data that has not been classified at the time of issuance of this policy must be classified within a specified period of time under a work plan prepared by the university and approved by His Excellency the President of the university.

Below are some examples of controls that can be used when classifying data. Reference can be made to the National Cybersecurity Authority's data protection controls and guidelines:

Protective Tags

Text protection tags are applied to paper and electronic documents (including emails) according to each classification level.

Arrival

- Logical and physical access to data is granted based on the principle of "minimum privileges" and "the need to know".
- The right of access to the data shall be denied as soon as the professional service of the employees of the entity ends or ends.

Usage

Data classified according to the requirements of classification levels are used, for example, the use of "strictly confidential" classified data is restricted to specific locations, whether physical – such as offices – or virtual, using hardware coding or special applications.

Storage

- Data classified as “strictly confidential”, “confidential” and “restricted”, as well as mobile devices that process or store such data, shall not be left unattended.
- Data classified as “strictly confidential”, “confidential”, and “restricted” that is not monitored while physically or electronically stored must be protected using an encryption method approved by the National Cybersecurity Authority.

Data Sharing

- Entities identify appropriate physical and digital means to securely share data to ensure that potential risks are minimized, and data sharing systems are complied with.
- The data exchange mechanism should be agreed upon, whether the entities will use the means currently used to exchange data, for example the government integration channel, the network of the national information center, the secure government network, setting up a new direct connection, removable storage media, wireless network, remote access, virtual private network, etc.

Data Retention

- A timeline is prepared that specifies the retention period of all data.
- The retention period shall be determined based on the relevant commercial, contractual, regulatory, and legal requirements.
- The retention period schedule is reviewed periodically - yearly or if there are changes to the relevant requirements.

Data Disposal

- All data shall be disposed of securely in accordance with the data retention schedule after obtaining the approval of the Business Data Representative.
- Data classified as “strictly confidential” and “confidential” that is controlled electronically are disposed of using the latest methods of disposing of electronic media.
- All paper documents are disposed of using a shredder.
- A detailed record of all data disposed of should be prepared.

Archiving

- The data shall be archived in secure storage locations according to the method recommended by the Business Data Representative.
- Backup copies of archived data are maintained.
- Archived data classified as “top secret” and “confidential” is protected using one of the encryption methods approved by the National Cybersecurity Authority.
- A detailed list of users authorized to access archived data is prepared and documented.

Cancellation of classification (declassification)

- Data should be de-classified or downgraded to the appropriate level after the classification period expires when protection is not required or is no longer required at the original level of the classification.
- If the data is incorrectly classified, the data user must notify the business data representative to determine the extent to which it needs to be properly reclassified.
- Factors that help to declassify data should be identified when first determining classification levels and recorded in the data asset register. These factors may include:
    - A specific period after the data has been generated or received (for example: two years after creation).
    - A specified period after the last action on the data (for example: six months from the date of last use).
    - After a specific date has passed (e.g., scheduled for review on 1 January 2023)
    - After certain circumstances or events that directly affect the data (for example: a change in strategic priorities or a change in government agency staff).
- De-classification - raising confidentiality - or lowering classification levels, away from the factors that help de-classify so clearly, requires a proper understanding of the content of the confidential data and the context in which it is contained.

4.4 Data Classification Steps

Step 1 – Inventory of assets and identification of data of Imam Abdulrahman bin Faisal University

The first step is to inventory and identify all the data owned by the university, which can be limited to the data of students at the deanship of Admission and Registration, the data of employees at the Human Resources management, the data of graduate students at the Deanship of Graduate Studies, university hospital data, and other data related to various assets.

Step 2 - Appointment of the Data Classification Officer

The University shall delegate a person responsible for the classification process as soon as all the data have been determined, a representative from the University's Data Management Office in cooperation with a representative from the data owner so that he/she understands the nature and value of the data within the entity.

Step 3 - Conduct the impact assessment process

The business data representative shall follow the steps necessary for the process of assessing the potential impact of the following actions:

- Disclosure of or unauthorized access to such data
- Modify, destroy data, or both
- Lack of timely access to this data

Step 4 – Identify relevant systems (only if impact level is low)

Additional evaluations should be carried out if the specific impact level is “low”, with a view to maximizing the level of classification of data classified as “public”. The Office of Data Management of the University, in cooperation with the representative of the data owners, examines whether the disclosure of these data is contrary to the regulations of the Kingdom of Saudi Arabia, such as the system of combating information crimes and the electronic trading system... Etc ., if disclosure is contrary to regulations, then the data must be classified as “restricted”.

Step 5 - Balancing the Advantages of Disclosure and Negative Effects

After ascertaining the level of low impact and ensuring that the disclosure will not be a violation of any system in force, the potential benefits of disclosing such data must also be evaluated and whether these benefits outweigh the negative effects. The potential benefits include using the data to develop new value-added services or increasing the transparency of processes. If the advantages are greater than the negative effects, the data is classified as “public”. If the benefits are lower than the negative effects, the data is classified as “restricted”.

Step 6 – Reviewing the Classification Level

The classification of data must be examined by the Office and ensure that the data is classified according to its nature and impact.

Step 7 - Applying Appropriate Controls

The final step in the data classification process is to protect all data according to the classification level by applying the relevant controls.

5. Policy 2: Personal Data Protection Policy

Imam Abdulrahman bin Faisal University applies the provisions of this policy as it processes personal data related to individuals such as employees, students, patients, employees of the university hospital and the like. Note that personal data related to individuals are collected from their owners directly and with their knowledge and processed for the purpose for which they were collected.

5.1 Key principles for personal data protection

Principle 1: Responsibility

The privacy policies and procedures of Imam Abdulrahman bin Faisal University should be defined and documented through the University's Data Management Office in coordination with the National Data Management Office and approved by His Excellency the President (or whomever he delegates) and disseminated to all parties concerned with its application.

Principle 2: Transparency

To prepare a notice on the privacy policies and procedures of Imam Abdulrahman bin Faisal University specifying the purposes for which the personal data are processed in a specific, clear, and explicit manner.

Principle 3: Selection and Consent

All possible options for the holder of personal data should be identified and his or her consent (implied or explicit) needs to be obtained regarding the collection, use or disclosure of his or her data.

Principle 4: Limiting data collection

The collection of personal data shall be limited to the minimum data that can be collected for the purposes specified in the privacy notice.

Principle 5: Limiting the use, retention, and disposal of data

To restrict the processing of personal data for the purposes specified in the privacy notice for which the data subject provided his implicit or explicit consent, and to retain it for as long as necessary to achieve the specified purposes or as required by the laws, regulations, and policies in force in the Kingdom and destroy it in a safe manner to prevent leakage, loss, embezzlement, misuse, or unauthorized access.

Principle 6: Data access

The means by which the data subject has access to his or her personal data are identified and made available for review, updating and correction.

Principle 7: Limiting Disclosure

The disclosure of personal data to third parties is restricted for the purposes specified in the privacy notice for which the data subject has given his or her implicit or explicit consent.

Principle 8: Data Security

The personal data shall be protected from leakage, damage, loss, embezzlement, misuse, unauthorized modification, or access – according to what is issued by the National Cyber Security Authority and the competent authorities.

Principle 9: Data quality

Personal data shall be held in an accurate, complete, and directly related manner for the purposes specified in the Privacy Notice

Principle 10: Monitoring and compliance

Monitor compliance with the controller's privacy policies and procedures, and address privacy queries, complaints, and disputes.

5.2 Data Subjects rights

1- The right to know, including notification of the legal basis or the actual need to collect personal data, and the purpose thereof. Otherwise, its data shall be processed in a manner inconsistent with the purpose for which it was collected and for which it gave its implicit or explicit consent.

2- The right to revoke his or her consent to the processing of his or her personal data at any time unless legitimate purposes require otherwise.

3- The right to have access to personal data at the university, to have access to it, to request that it be corrected, completed or updated, and to request that it be destroyed as needed, and to obtain a clear copy of it.

5.3 Obligations of Imam Abdulrahman bin Faisal University

1- The university shall be responsible for the preparation and application of policies and procedures relating to the protection of personal data, and the President – or his delegate - shall be responsible for their approval and adoption.

2- To establish a data management office to prepare data governance policies that are linked to the data management offices in the government agencies that were established by Royal Decree No. 59766 dated 11/20/1439 AH, provided

that the tasks and responsibilities of the office include setting appropriate standards to determine the levels of sensitivity of personal data.

3- The University of Imam Abdulrahman bin Faisal shall assess the risks and potential effects of personal data processing activities and present the results of the evaluation to His Excellency the President – or his delegate – to determine the level of acceptance and approval of risks.

4- The university shall review and update contracts and service level and operating agreements in accordance with the privacy policies and procedures adopted by the senior management.

5- The university shall prepare and document the procedures necessary to manage and address privacy violations and determine the tasks and responsibilities related to the competent working group, and the cases in which the regulatory body and the Office are notified according to the administrative hierarchy - based on the measurement of impact.

6- The university, represented by the Data Management Office and those who support it, shall prepare awareness programs to promote a culture of privacy and raise the level of awareness in accordance with the privacy policies and procedures adopted by the senior management.

7- The data subject shall be notified, in an appropriate manner at the time of data collection, of the purpose, the actual legal basis/ need, the means and methods used to collect, process, and share personal data, as well as security measures to ensure privacy protection in accordance with the laws, regulations and policies in force in the Kingdom.

8- Notify the data subject about other sources that are used in the event that additional data are collected indirectly (from others).

9- To provide the data subject with the options available regarding the processing of personal data and the mechanism used to practice these options.

10- The consent of the data subject to the processing of the personal data shall be obtained after determining the type of consent (explicit or implied) to the nature of the data and the methods of collecting them.

11- The purpose of data collection shall be in accordance with the laws, regulations, and policies in force in the Kingdom and shall be directly related to the activity of the university.

12- The content of the data shall be limited to the minimum data necessary to achieve the purpose of its collection.

13- The collection of data shall be restricted to the content prepared in advance and shall be fair, direct, clear, secure, and free from deception.

14- The use of the data should be limited to the purpose for which it was collected.

15- Imam Abdulrahman bin Faisal University has to prepare and document the policy and procedures for retaining data in accordance with the specified purposes, regulations and relevant legislation.

16- That Imam Abdulrahman bin Faisal University, represented by its sectors that collect and store data, store and process personal data within the geographical borders of the Kingdom to ensure the preservation of the digital national sovereignty of these data, and may not be processed outside the Kingdom unless the university obtains written approval from the regulatory body, after coordinating the regulatory body with the office.

17- Imam Abdulrahman bin Faisal University to prepare and document the policy and procedures for data disposal to destroy data in a safe way that prevents its misuse or unauthorized access to it – including operational data, archived, and

backups – according to what is issued by the National Authority for Cybersecurity.

18- The University of Imam Abdulrahman bin Faisal shall include the provisions of the retention and disposal policies in the contracts if these tasks are assigned to other processing sectors.

19- Imam Abdulrahman bin Faisal University should identify and provide the means through which the data subject can access his personal data to review and update it.

20- Imam Abdulrahman bin Faisal University shall verify the identity of individuals before granting them access to their personal data in accordance with the controls approved by the National Cyber Security Authority and the competent authorities.

21- It is prohibited to share personal data with other parties except in accordance with the purposes specified after the approval of the data subject and in accordance with the regulations, regulations and policies, provided that the other parties are provided with privacy policies and procedures followed and included in contracts and agreements.

22- The data subjects must be notified and approved if the data are shared with others for use other than for the specified purposes.

23- Imam Abdulrahman bin Faisal University to take the approval of the National Data Management Office - after coordination with the regulatory body - before sharing personal data with other parties outside the Kingdom.

24- Imam Abdulrahman bin Faisal University to prepare, document and apply the necessary procedures to ensure the accuracy, completeness, modernity, and relevance of personal data for the purpose for which they were collected.

25- Administrative controls and technical measures adopted in the University's information security policies should be used to ensure the protection of personal data, for example:

- Granting access to data in accordance with the tasks and responsibilities of workers in a way that prevents overlap of competence and avoids dispersal of responsibilities.
- Apply administrative procedures and technical measures that document the stages of data processing and provide the possibility of identifying the user responsible for each of these stages (usage records).
- Signing an undertaking workers who conduct data processing operations to preserve the data and not to disclose it except in accordance with policies, procedures, regulations and legislation.
- Selection of honest and responsible data-processing personnel in accordance with the nature and sensitivity of the data and the access policy adopted by the university.
- The use of appropriate security measures – such as encryption, isolating the development and testing environment from the operating environment – for the security and protection of personal data commensurate with their nature and sensitivity and the means used to transport and store them in accordance with what is issued by the National Authority for Cybersecurity and the competent authorities.

26- Imam Abdulrahman bin Faisal University, represented by the Data Management Office, shall be responsible for monitoring compliance with privacy policies and procedures in a periodic manner and shall be presented to His Excellency the President of the University – or his delegate – as corrective

measures to be taken in the event of non-compliance and notifying the regulatory body and the office according to the organizational sequence shall be identified and documented.

6. Policy 3: Data Sharing Policy

This policy defines the data sharing controls of Imam Abdulrahman bin Faisal University with other government agencies, private entities, or individuals, regardless of the source, form, or nature of these data, including paper records, emails, and data stored on electronic means, audio or video tapes, maps, photographs, manuscripts, or handwritten documents, or any other form of recorded data. Note that the provisions of this policy do not apply if the data applicant is a government agency, and the request is for security purposes or to meet judicial requirements.

6.1 Key principles of data sharing

Principle 1: Enhancing the participation culture

All government agencies shall share the main data they produce to achieve complementarity among them to obtain data from their correct sources and to reduce duplication, incompatibility and multiplicity of sources. If the data are requested from other than its primary source, the party required to share these data must obtain the approval of the main party – the source of the data – before sharing it with the requesting party.

Principle 2: Legitimacy of Purpose

The data shall be shared for legitimate purposes based on a systemic basis or a justifiable practical need aimed at achieving a public interest without causing any harm to national interests, the activities of entities, the privacy of individuals or the integrity of the environment – except for data and entities exempted by high orders.

Principle 3: Permitted Access

All parties involved in the sharing of data have access to, obtain and use this data (which may require security scanning according to the nature and sensitivity of the data), in addition to the knowledge, skill, and persons properly qualified and trained to handle the shared data.

Principle 4: Transparency

All parties involved in data-sharing operations shall make available all information necessary for the exchange of data, including: the data required, the purpose of collection, means of transmission, methods of archiving, controls used to protect them and the mechanism for their disposal.

Principle 5: Shared Responsibility

All parties involved in the sharing of data shall be jointly responsible for the decisions to share and process the data in accordance with the specified purposes, and to ensure the application of the security controls stipulated in the Data Sharing Agreement, and the relevant laws, legislations, and policies.

Principle 6: Data Security

All parties involved in the data sharing process shall apply appropriate security controls to protect and share data in a safe and reliable environment in accordance with the relevant regulations and legislation, and in accordance with what is issued by the National Cybersecurity Authority.

Principle 7: Ethical Use

All parties involved in the sharing of data should apply ethical practices during the data sharing process to ensure that they are used within a framework of justice, integrity, honesty and respect, and not only adhere to information security policies or comply with relevant regulatory and legislative requirements only.

6.2 Steps of the Data Sharing Process

1- The applicant - whether a government or private entity or an individual - sends a request to share data to the Data Management Office at Imam Abdulrahman bin Faisal University, provided that the request is sent through the Data Management Office in the requesting party in the event that the applicant is a government agency.

2- The university Data Management Office refers the request to the Business Data Representative, who in turn directs this request to a business data specialist to evaluate and process the request.

3- The business data specialist verifies the level of classification of the required data:

a. If the level of classification is not determined, the Data Management office at Imam Abdulrahman bin Faisal University must classify the required data according to the data classification policy.

b. If the level of classification is determined to be “public”, the business data specialist can share the required data without evaluating the request according to the main principles of data sharing.

c. If the level of classification is determined to be “Restricted”, “Confidential” or “Highly Confidential”, the business data specialist shall evaluate the request in accordance with the main principles of data sharing.

4- The business data specialist in the Data Management office at the University must complete the participation process if all the principles of data sharing are fully met.

5- The business data specialist in the Data Management office at the University may not continue to share data in the event that one or more of the principles of data sharing are not met. The business data specialist must also respond to the request with observations and provide the opportunity to meet all the principles of sharing incompatible data.

6- Upon completion of all data-sharing principles, the business data specialist shall obtain the agreement of the business data representative to complete the data-sharing process.

7- The business data specialist in the Data Management office at the University of Imam Abdulrahman bin Faisal determines the appropriate controls to ensure compliance with the principles of data sharing and achieve the objectives specified for each of them, and it must be agreed between the university business data specialist, the applicant and other parties involved in the participation process to apply these controls.

8- After agreeing on the data sharing controls and adhering to their application, the business data specialist should clarify them in detail in the agreement and all participating parties must sign the data sharing agreement.

9- The data management office of the University can share the required data with the requesting party after signing the data sharing agreement.

6.3 Timeframe for data sharing

The government entity, which is required to share data, shall evaluate the request within a period not exceeding 30 days from the date of receipt of the request, and notify the applicant of the decision to participate, provided that the decision is in writing and reasoned (steps 2 to 4 of the data sharing process described above). If the request for participation is not approved, the applicant has the right to complete the requirements to meet all the principles and to request an appeal from the business data specialist to re-evaluate the request and issue the decision to participate within a period not exceeding 14 days from the date of receipt (step 5 of the data sharing process).

After obtaining the business data representative's approval to continue the sharing process (Step 6 of the data sharing process), the business data specialist develops and implements appropriate controls for data sharing and prepares a data sharing agreement within a period not exceeding 60 days from the date of the business data representative's approval (Step 7 of the data sharing process).

After signing the Data Sharing Agreement (Step 8 of the Data Sharing Process) the Business Data Specialist will share the data with the Applicant within 7 days from the date of signing the Agreement (Step 9 of the Data Sharing Process).

6.4 Data Sharing Controls

All parties involved in the data-sharing process must agree on the controls necessary to adequately manage and protect the shared data:

Statutory Basis

(Relevant principles: Principle 1: Enhancing the culture of participation, Principle 2: Legitimacy of purpose, Principle 5: Shared Responsibilities, Principle 7: Ethical use)

- To clarify the legal basis or actual need for data sharing, for example: the organization of the entity, the royal/supreme order that allows the entity to share data, or the signed agreement.

- To adhere to levels of data classification, preservation of intellectual property rights and privacy of personal data.

Delegation

(Related Principles: Principle 3: Authorized Access, Principle 6: Data Security)

- Identify the entities and persons authorized to request and receive data (compliance with the data classification policy – controls of use and access to data can be verified)

Type of data

(Relevant principles: Principle 1: Enhancing participation culture, Principle 2: Legitimacy of purpose, Principle 4: Transparency)

- To ensure that the data required are within the main data produced by the University to ensure that data are requested from their correct source.
- Determine the minimum data required to achieve the specified purposes.
- The data required shall specify the data format and the requirements for their modification or change (e.g. data format, data accuracy, level of detail, data structure, type of raw data or processed data).

Pre-processing of data

(Related Principles: Principle 6: Data Security)

- Determine whether there is a need to process the data before sharing it, and if so, agree on the required processing methods - for example, blocking, anonymity, and aggregation, provided that the data are not processed in a manner that changes the content.

- Assess the quality, validity and integrity of the required data and determine whether it requires improvement prior to sharing it. If so, the Data Management office in the university should check the data prior to sharing it.

Means of data sharing

(Related Principles: Principle 6: Data Security)

- Compliance with data protection controls issued by the National Cybersecurity Authority.
- Means of physical and digital data sharing are identified
- To verify the security and reliability of the means of participation to reduce the potential risks, as well as to benefit from the means of safe participation approved between the parties.
- The mechanism of data sharing is determined, and whether the business data specialist will transfer the data directly to the applicant or a service provider will be used to complete the participation process.
- Determine whether existing means of participation (e.g., government integration channel, national information center network) will be used or whether different means (wireless Internet, remote access, virtual private network, API) will be used
- The mechanism of destroying the physical media used in data sharing shall be agreed upon.

Use and preservation of data

(Relevant Principles: Principle 2: Legitimacy of Purpose, Principle 4: Transparency, Principle 6: Data Security, Principle 7: Ethical Use)

- Define data protection requirements when sharing data and apply specific controls to protect data after sharing it.
- Impose appropriate restrictions on the permissible use or processing of data (if any), such as processing restrictions, spatial or temporal limitations, or exclusive or commercial rights.
- The rights of all parties involved in the participatory process are determined by conducting audits and revisions.
- The dispute settlement and arbitration procedures shall be agreed upon.
- To determine whether there is a third party to benefit from the data after sharing it and agreeing on the organized mechanism for that.

Duration of data sharing, number of sharing times and cancellation of sharing

(Relevant Principles: Principle 2: Legitimacy of Purpose, Principle 6: Data Security)

- Specify the duration of data sharing and the deadline for accessing or storing data.
- Determine the number of times data will be shared, the requirements for review, modifications, and actions to be taken at the end of the agreement (such as anonymizing, cancelling access to, or destroying data).
- Identify the parties entitled to terminate the sharing of data prior to the agreed date, the regular document, and the period of notice allowed.

Liability provisions

(Related Principles: Principle 5: Shared Responsibility)

- That it is agreed to determine the responsibilities in case of non-compliance with the terms of the agreement, and other obligations between the

participating parties such as termination of the agreement and corrective actions.

- The rules on liability provisions for sharing erroneous data, technical problems in the process of transferring data, or inadvertent or irregular loss of data which may cause other harm.

6.5 General Rules for Data Sharing

Imam Abdulrahman bin Faisal University is committed to the following rules when sharing data with any other party:

1- Prioritize approved and secure means of participation for data exchange.
2- The business data specialist in the Data Management office is responsible for sharing data after all the principles of data sharing have been completed, in addition to determining the appropriate controls for participation.
3- The university shall appoint or authorize the appropriate person – according to the qualifications and training required - to deal with the data in a correct manner, provided that he is authorized to request, receive, access, store and destroy the joint data.
4- The identity of the personal data subject must be concealed, unless it is necessary for the purpose of sharing, with the controls necessary to preserve the privacy of the data subject in accordance with the personal data privacy policy.
5- Metadata should be attached when sharing data in cases where this is required.
6- The data-sharing participants shall be responsible for the protection and use of data in accordance with the specified purposes. The University's

Data Management Office shall have the right to review compliance periodically or randomly in accordance with the controls specified in the Data Sharing Convention.

7- The Office shall prepare a data-sharing manual containing a data-sharing request form and a standard data-sharing agreement form.

8- After coordination with the Office, the regulatory authorities shall prepare the mechanisms, procedures and controls related to the settlement of the dispute in accordance with a specified time frame.

9- In the event of a dispute between the parties involved in the data-sharing process, the same regulator shall have the right to notify the regulatory body and to demand the settlement of the dispute between the parties involved. In the event that the dispute is not resolved, the National Data Management Office shall be notified and the Office shall settle the dispute.

10- In the event that there is an aspect of data sharing that is not covered by this policy, the Data Management office at Imam Abdulrahman bin Faisal University has the right to set additional rules that do not conflict with the principles of data sharing, while providing sufficient justification and notifying the National Data Management Office.

11- Imam Abdulrahman bin Faisal University is keen in sharing its data to find the appropriate balance between the need to share data and ensure the protection of the confidentiality of data and the potential risks to the individual or community

12- The university retains all requests for data sharing and related decisions.

13- Imam Abdulrahman bin Faisal University develops, adopts, and publishes its data sharing policy.

14- Entities inside and outside the university must not share the shared data with another party or entity without the consent of the data producer.

15- Imam Abdulrahman bin Faisal University, represented by the Data Management Office, shall be responsible for monitoring and implementing this policy.

7. Policy 4: Information Freedom Policy

This policy applies to all requests for access to public information – unprotected - produced by Imam Abdulrahman bin Faisal University, regardless of their source, form, or nature – including paper records, e-mail messages and information stored on computers, audio or video cassettes, maps, photographs, manuscripts, handwritten documents, or any other form of recorded information.

The provisions of this policy do not apply to protected information represented by:

1- Information the disclosure of which would prejudice the national security, policies, interests or rights of the Kingdom.
2- Military and security information
3- Information and documents obtained under an agreement with another country and classified as protected.
4- Inquiries, investigations, seizures, inspections, and surveillance relating to a crime, offence, or threat.
5- Information containing recommendations, proposals or advice for legislation or a governmental decision yet to be issued.
6- Information of a commercial, industrial, financial, or economic nature the disclosure of which would unlawfully result in profit or loss.
7- Scientific or technical research, or rights involving an intellectual property right, the disclosure of which would prejudice a moral right.
8- Information related to competitions, tenders and auctions, the disclosure of which undermines the fairness of the competition.
9- Information that is confidential or personal under another system or requires certain legal procedures to access or obtain it.

7.1 Key Principles of Information Freedom

Principle 1: Transparency

The individual has the right to know information about the activities of Imam Abdulrahman bin Faisal University in order to enhance the integrity, transparency and accountability system.

Principle 2: Necessity and proportionality

Any restrictions on requesting access to or obtaining protected information received, produced, or dealt with by Imam Abdulrahman bin Faisal University must be justified in a clear and explicit manner.

Principle 3: Original in Public Information Disclosure

Everyone has the right of access to public information – which is not protected – and the applicant does not necessarily have to have any specific intent or interest in such information in order to have access to it, nor is he or she subject to any legal question relating to this right.

Principle 4: Equality

All requests for access to public information shall be treated on the basis of equality and non-discrimination between individuals.

7.2 Rights of Individuals to Access or Obtain Public Information from Imam Abdulrahman bin Faisal University

First: Individuals have the right to access and obtain any unprotected information at Imam Abdulrahman bin Faisal University.

Second: Individuals have the right to know the reason for refusing to see or obtain the required information.

Third: Individuals have the right to appeal the decision to reject the request for access and to obtain the required information.

7.3 Obligations of Imam Abdulrahman bin Faisal University with regard to public information

1- Imam Abdulrahman bin Faisal University shall be responsible for the preparation and application of policies and procedures related to the practice of the right of access to public information, and His Excellency the President of the University (or his representative) shall be responsible for approving.

2- Imam Abdulrahman bin Faisal University shall establish an administrative unit that shall be linked to the University's Data Management Office and shall be responsible for developing, documenting and monitoring the implementation of the policies and procedures adopted by the higher management of the University related to the right of access to information, provided that the tasks and responsibilities of the unit include setting appropriate standards to determine the levels of data classification in the absence of such data - in accordance with the data classification policy – and to be used as a main reference when processing requests to access or obtain public information.

3- The university shall verify the identity of individuals before granting them the right to access or obtain public information in accordance with the controls approved by the National Cyber Security Authority and the relevant authorities.

4- The university shall identify and provide the possible means (public information request forms) – whether paper or electronic – through which the individual can request or obtain public information.

5- The University shall establish the criteria necessary to determine the fees resulting from the processing of requests for access to public information or to obtain

it based on the nature and size of the data, the effort exerted on public information or to obtain it based on the nature and size of the data, the effort exerted and the time spent - according to the policy document to generate income from the data.

6- The University shall document all records of requests for or access to information and decisions taken in respect of requests, which records shall be reviewed to address cases of misuse or non-response.

7- The University shall prepare and document the policies and procedures for maintaining and disposing of records of applications in accordance with the regulations and legislation related to the work and activities of the University.

8- The university shall notify the individual, in an appropriate manner, in the event that the application is rejected in whole or in part, indicating the reasons for the rejection and the right to appeal and how to practice this right within a period not exceeding 15 days from the adoption of the decision.

9- The university should prepare awareness programs to promote a culture of transparency and raise the level of awareness in accordance with the policies and procedures of freedom of information adopted by the university's senior management.

10- The University represented in the Data Management Office shall be responsible for monitoring compliance with the policies and procedures of freedom of information periodically and shall be presented to the President of the University or his delegate. Corrective actions to be taken in the event of non-compliance shall be identified and documented, and the regulatory body and the National Data Management Office shall be notified according to the administrative hierarchy.

7.4 Key steps to access or obtain information

First: Applications are submitted by filling out a "public information application form" – electronic or paper – and submitting it to the university as the required information body.

Second: The University shall, within a specified period of time (not exceeding 30 days), receive the request for access to public information, by taking one of the following decisions:

1- **Approval**: If the university approves the request to access or obtain the information in whole or in part, the individual must be notified in writing or electronically of the fees applied, and the university must make this information available to the individual within a period not exceeding (10) working days from the receipt of the amount. 2

2- **Refusal**: If a request for access to or obtaining of information is refused, the refusal must be in writing or electronically, provided that it includes the following information:

- Determine whether the application has been rejected in whole or in part
- Reasons for rejection, if applicable
- The right to appeal this refusal and how to practice this right.

3- **Extension**: In the event that it is not possible to process the request for access to information on time, the university should extend the period in which a reasonable period will be responded to according to the size and nature of the information required – for example, not exceeding (30) additional days – and provide the individual with the following information:

- Notice of extension and expected date of completion
- Reasons for delay
- The right to appeal against this extension and how this right is practiced.

4- **Notice**: If the information requested is available on the university's website or is not within its competence, the individual must be notified in writing or electronically, including the following information:

- The type of notice, for example, the data required are available on the site or are not within its competence.
- The right to appeal this notice and how to practice this right.

Third: If the individual wishes to appeal against the rejection of the application by the university, he/she can submit a written or electronic notice of the grievance to the university's data management office within a period of time not exceeding (10) working days from his/her receipt of the university's decision. The grievance committee in the university's data management office reviews the application, takes the appropriate decision, and notifies the individual of the review fees – to be recovered if the committee approves the application – and the appeal decision.

7.5 General Provisions

First: The Imam Abdulrahman bin Faisal university undertakes to harmonize this policy with its organizational documents – policies and procedures – and circulate them to all its affiliates or associated with them in order to achieve integration and ensure the achievement of the goal of its preparation.

Second: Imam Abdulrahman bin Faisal university must balance the right to access and obtain information with other necessary requirements such as achieving national security and maintaining the privacy of personal data.

Third: The public bodies must comply with this policy and document compliance periodically in accordance with the mechanisms and procedures determined by the university after coordination with the National Data Management Office

Fourth: After coordination with the National Data Management Office, the university prepares the mechanisms, procedures and controls related to dealing with complaints according to a specific time frame and according to the organizational sequence.

Fifth: Public bodies must notify the National Data Management Office in the event that the request for access to public information is rejected or the period for providing this information is extended, which is within the scope.

Sixth: When contracting with other parties - such as companies that conduct public services – the public body must periodically verify the compliance of other parties with this policy in accordance with the mechanisms and procedures specified by the body, provided that this includes any subsequent contracts carried out by other parties.

Seventh: The university shall have the right to establish additional rules for the processing of requests for specific types of public information according to their nature and sensitivity after coordination with the National Data Management Office.

Eighth: The university must prepare forms for accessing or obtaining public information – whether paper or electronic – specifying the necessary information and the possible means to provide the required information.

7.6 Information Freedom and Open Data

Open data programs and policies around the world are usually prepared and developed to support the growth of the national economic agenda and innovation, and there is no doubt that the availability and dissemination of a specific set of public information for researchers, entrepreneurs, innovators and emerging companies helps to create an environment conducive to the growth of business and indicates the existence of an open and transparent government.

Open data programs and policies are also a proactive step by parties in preserving the right of access to public information by making available or publishing a specific set of information – as open data – before requesting or obtaining access to it. Thus, effective open data programs and policies reduce the volume of requests for access to public information, which leads to a reduction in government expenditures related to the processing of requests.

8. Policy 5: Open Data Policy

Open data is a subset of public information according to the classification levels described in the data classification policy.

The provisions of this policy shall apply to all public – unprotected – data and information produced by Imam Abdulrahman bin Faisal University, whatever their origin, form or nature, including paper records, electronic mail messages, computerized information, audio or video cassettes, maps, photographs, manuscripts, handwritten documents or any other form of recorded information.

8.1 Key principles of open data

Principle 1: Data Availability is the origin

This principle ensures that public university data is made available to all through disclosure, access, or use, unless their nature requires that they do not be disclosed or that their privacy or confidentiality be protected.

Principle 2: Open and machine-readable format

Data are available and provided in machine-readable format that allows for automated processing – so that they are saved in commonly used file formats (e.g. CSV, XLS, JSON, XML)

Principle 3: Modernity of data

The most recent release of open datasets is published on a regular basis and is available to all upon availability. Data collected by the public are published as soon as possible, as soon as they are collected, whenever possible, and priority is given to data that are less useful with time.

Principle 4: Inclusiveness

Open data sets must be as comprehensive and detailed as possible and reflect the data recorded in a manner that is not inconsistent with the personal data protection policy. Metadata that illustrates and explains the raw data should be included, with explanations or equations that illustrate how the data are extracted or calculated.

Principle 5: Non-discrimination

Data sets must be made available to all without discrimination and without the need for registration – open published data can be accessed by anyone at any time without the need for verification or justification.

Principle 6: Free of charge

Open data should be made available to everyone free of charge.

Principle 7: Licensing open data in the Kingdom

Open data shall be subject to a license specifying the regulatory basis for the use of open data as well as the conditions, obligations and restrictions imposed on the user. The use of open data indicates acceptance of licensing requirements.

Principle 8: Developing the Governance Model and Inclusion of All

Open data enable universal access and participation, enhance transparency and accountability of the public and support decision-making and service delivery.

Principle 9: Inclusive development and innovation

Entities are supposed to play an effective role in promoting the reuse of open data and providing the necessary supporting resources and expertise. Entities must work in an integrated manner among the parties concerned to enable the next generation of innovators in the field of open data and to involve individuals, institutions, and all in general in launching open data capabilities.

8.2 Value assessment of public data to identify open datasets

Imam Abdulrahman bin Faisal University is working to assess the value of data to enable the widest possible dissemination of open data through the following steps:

Step 1: Identify public data and information

To assess the value of the data, the university, represented by the Data Management Office, must classify the data (according to the data classification policy) and identify all data sets that can be classified at the "public" level, which may consist of specific files, tables or records within a database, ... Etc. Thereafter, the potential benefits, applications and uses of each data set must be identified. The data area, sector or source of data can also be taken into account when analyzing potential use cases. Data sources can also be taken into consideration: data collected through direct users, data automatically collected through event logs such as electronic transactions, data collected or data developed from other data... Etc.

Step 2: Evaluate the usefulness of data

After identifying the data sets in the previous step, the main factors related to the usefulness of the data, which play a key role in assessing their value, including the completeness of the data, their accuracy, their consistency, their modernity, the restrictions imposed on them, their exclusivity to the entity, the potential risks of their publication, their accessibility, and their integration with other data, shall be studied.

Step 3: Identify Potential Stakeholders

After evaluating the usefulness of the data in the previous step, all potential stakeholders are identified.

After completing the data value assessment, the stages of the open data life cycle can be started.

8.3 Open Data General Rules

The Open Data Policy sets out the general rules and obligations that the university must comply with during the stages of the Open Data Life Cycle and includes:

- Planning for open data
- Select open data
- Open data publishing
- Update open data
- Monitoring the performance of open data

Planning for open data

Imam Abdulrahman bin Faisal University represented by the Data Management Office should:

1- Appointment of an Open Data and Information Officer in the Office of Data Management, whose primary responsibility is to support the planning, implementation, and preparation of reports on the University's Open Data Agenda and in line with this policy.

2- Develop an open data plan, including:

- Strategic objectives of open data at the university level
- Identify and prioritize the university's datasets to be published on the national open data platform.
- KPIs and targets related to open data for the university.
- Methodology and criteria for prioritization,
- Training needs related to open data

- Timelines for publishing and updating open data.

3- Develop and document the processes required at all stages of the open data life cycle, including, but not limited to:

- Determinations of general data sets to be published by the university.
- Regular checks and audits of open data compliance with information security, personal data privacy and data quality requirements and related concerns.
- Processes to ensure that data sets are published and updated as appropriate and in accordance with the established timetable, that they are comprehensive and of high quality, and that any restricted data are excluded.
- Collect observations and analyze performance at the university level and improve the overall impact of open data at the national level.

4- Ensure that the open data plan is reviewed and updated periodically.

5- Submission of an annual report to the National Data Management Office on the open data plan and the level of progress in achieving the open data objectives set out in the plan.

6- Organizing a training course on all matters related to open data with the support of the Data Management Office or in coordination with it.

7- . Launching awareness campaigns to ensure that potential users know the availability, nature and quality of open data published by the University.

Open Data Selection

1- Identify all data classified as public data on a regular basis and assess the priority of each set of data identified for publication as open data.

2- Estimate the value of the data set and prioritize its publication once a request for publication has been received or any data set has been deregistered as restricted and classified as a public data set.

3- Record and publish metadata for selected open datasets.

4- Examine whether the combination of several sets of open data will result in a higher level of data disaggregation into protected data.

Open Data Publishing

1- The university should publish its open datasets on the national open data platform.

2- Ensure that data are published in standardized, standardized, machine-readable and non-proprietary formats (e.g. CSV, JSON, XML,RDF). Data-set files should be accompanied by relevant documentation in the format and instructions on how to use them.

3- Provide data in several formats whenever possible.

Update Open Data

The University shall:

1- Ensure that all open data sets published on a regular basis are updated according to the mechanism specified in the metadata.

2- Ongoing review of published data sets to ensure that they meet specific organizational requirements.

3- Ensure that metadata is updated, especially as data elements in published open data sets change.

4- Maintain the traceability of data by documenting data sources and maintaining the repository of data set releases.

5- Disseminate open data sets with quality entries identified and documented in metadata.

Monitoring the performance of open data

Imam Abdulrahman bin Faisal University should:

1- Analyze the volume of demand for open data and the rate at which it is used to understand the volume of public demand and reprioritize data sets accordingly.

2- Collect, analyze, and respond in a timely manner to user requests submitted directly or through the national open data platform for the publication of additional data sets.

8.4 Roles and Responsibilities for Open Data

The primary responsibility of Imam Abdulrahman bin Faisal University is to ensure the publication of its open data in accordance with the open data policy. Consequently, the university must designate those responsible for the implementation of activities relating to open data as provided for and be borne by the Director of the Office of Data Management of the University and the Officer-in-Charge of Open Data and Information.

Responsibilities of His Excellency the President of Imam Abdulrahman bin Faisal University:

The President of the University - or his delegate - is the person responsible for the practices related to open data within the university, and his responsibilities include:

- **Approval of the open data plan:** Approval and supervision of the implementation of the university's open data plan.
- **Allocation of open data roles**: Allocation of different open data roles.
- **Approving the annual report of open data:** approval of the annual report of open data prepared by the Director of the Data Management office.

Responsibilities of the Director of Data Management Office at Imam Abdulrahman bin Faisal University:

The office director is the strategic manager of the University's open data operations, whose responsibilities include:

- **Strategic planning of open data:** Supervising the development of the open data plan and submitting it to the President. Also reviewing the performance of open data and identifies opportunities for improvement guided by the open data plan.
- **Supervising open data:** Reviewing the activities of identifying open data, prioritizing them, approving their publication, and ensuring the implementation of activities to update them.
- **Compliance with open data policy:** Ensure compliance of data activities with national data policies, including, for example, data classification, protection of personal data privacy and freedom of information.

- **Coordination with the National Data Management Office**: The Director of the Data Management Office is the coordinator between the university and the National Data Management Office for open data. He solves problems with open data for the University and escalates them to the National Data Management Office if necessary.

Open Data and Information Officer:

The Executive Director of Open Data within the University, whose responsibilities include:

- **Planning for open data**: Development of an open data plan, including a methodology for identifying priority open data and setting objectives and key performance indicators to be agreed with the Director of the Data Management Office and the President.
- **Managing open data:** Managing open data activities within the organization, specifically:

  - Identify open data

  - Prioritize data sets for publication

  - Prepare datasets for publication and document metadata

  - Publish open datasets on the national open data platform

  - Update, maintain and review the quality of published datasets.

- **Collection of open data requests:** review of notes on open data relevant to university and recording and analysis of requests for publication of data identified as open data.

- **Education and awareness of open data:** education and awareness of staff on open data and support for national awareness campaigns in co-ordination with the Director of the Data Management Office.
- **Coordination with the National Data Management Office (secondary):** the Open Data and Information Officer coordinates with the Office when needed as a second level.

Business Data Representative:

Assumes the following responsibilities:

- **Confirming the open data plan:** contributing to the development of the open data plan and managing the teams responsible for the implementation of the plan in coordination with the open data and information officer.
- **Prioritize open data:** advise the Open Data Officer and provide information on the value of public data sets and the investments required for their publication and updating.
- **Reviewing and approving data sets:** reviewing and approving data sets to ensure that they meet the specifications specified in the regulation in terms of quality and completeness and documenting metadata before they are submitted for publication.

Business Data Specialist:

A member of the Business Data Representative team is responsible for:

- **Identification of open data sets:** data generated and processed by the department in which it operates are regularly reviewed and, if necessary, classified as public data by the business data specialist.

- **Preparation of open data sets:** Preparation of open data sets to be published to ensure that they meet the quality and completeness specifications specified in the policy and documentation of metadata prior to their submission for publication.
- **Update of open data sets:** update of published open data sets and related metadata.

8.5 Compliance

The National Data Management Office, as the regulatory entity for national data, monitors compliance with the open data policy with the support of the Data Management Office at Imam Abdulrahman bin Faisal University.

Compliance conditions:

1- Imam Abdulrahman bin Faisal University must adhere to the open data policy and submit an annual report to the National Data Management Office, including, for example, the following:

- Progress and level of achievement of the University in its specific plan
- Objectives and KPIs set out in the Open Data Plan
- Number of open datasets selected
- Number of open data sets published.

2- After coordination with the National Data Management Office, the university shall prepare the mechanisms, procedures and controls related to the settlement of disputes related to open data according to a specific time frame and according to the organizational sequence.

3- The National Data Management Office reviews the annual reports prepared by Imam Abdulrahman bin Faisal university on the general compliance with the open data policy and shares them with the relevant authorities.

4- The Office shall periodically or randomly conduct audits to verify public compliance and review decisions regarding publication or refusal to publish data and take appropriate action in this regard.

8.6 Dealing with cases of non-compliance

In reviewing cases of non-compliance, the National Data Management Office shall follow a step-by-step methodology to analyze the cause of non-compliance and the extent of the consequences and risks thereof, and shall deal with such cases according to the following levels:

Awareness-raising the office uses awareness when dealing with accidental or unintended non-compliance cases with very limited negative effects.

Cooperate where the office cooperates with the university to prevent, deter or remedy cases of non-compliance with limited adverse consequences arising from negligence and non-compliance with the provisions and rules of this policy.

Direct intervention The Office shall investigate persistent and repeated cases of non-compliance, intentional or with severe adverse effects, and take decisions that are commensurate with the magnitude and nature of the adverse effects.

9. Policy 6: Personal data protection policy for children and the like

It includes the rights and general rules that Imam Abdulrahman bin Faisal University must observe and abide by in order to reduce erroneous practices related to the processing of personal data of children and the like and ensure their protection from negative effects and potential risks, in addition to preserving their privacy and protecting their rights.

The provisions of this policy apply to all entities in the public and private sectors, as well as non-profit actors that collect and process personal data of children and those of similar status in full or in part and by any means, whether manual or electronic. The provisions of this policy also apply to all parties outside the Kingdom that collect personal data on children and the like residing in the Kingdom through the Internet.

9.1 Rights of the child and the like with regard to the processing of personal data

The child and the like enjoy all the rights of the data subject stipulated in the personal data protection policy issued by the National Data Management Office, and these rights shall be practiced by the guardian. The child and the like shall also have the right to request the destruction of his or her personal data after he or she has reached the legal age or the end of the guardianship if the consent to the collection and processing of his or her personal data is given by the guardian.

9.2 General rules

Without violation to the general rules stipulated in the personal data protection policy, Imam Abdulrahman bin Faisal University is committed to the following additional rules that guarantee the preservation of the privacy of children and the like and the protection of their rights:

1- Imam Abdulrahman bin Faisal University shall be responsible for the preparation and application of policies and procedures related to the protection of the personal data of children and the like, and His Excellency the President of the University – or his delegate – shall be responsible for approving and approving them.

2- The University is committed to assessing the possible negative effects and risks of all activities for the processing of personal data on children and those of similar status, taking into account their interests, rights and all that relate to the condition of their families, and to presenting the results of the evaluation to the President – or his delegate – for determination and approval of the level of acceptance of the risks.

3- Imam Abdulrahman bin Faisal University is committed to reviewing and updating contracts and service and operating level agreements in accordance with the policies and procedures related to the protection of personal data for children and those of similar status approved by the Supreme Administration of the Authority.

4- Imam Abdulrahman bin Faisal University is committed to preparing and documenting the necessary procedures to manage and address privacy violations related to children and the like, and to determine the tasks and responsibilities related to the competent work team, and the cases in which the regulatory body and the office are notified according to the administrative hierarchy based on measuring the severity of impact.

5- Imam Abdulrahman bin Faisal University is committed to developing awareness programs to enhance the culture of privacy and raise the level of awareness regarding the collection and processing of personal data for children and the like.

6- Imam Abdulrahman bin Faisal University is committed to preparing and developing the privacy notice in a clear and accurate manner in a language appropriate to this category and publishing it on the website or special application (according to the guide to developing the privacy notice issued by the National Data Management Office) and the guardian's notice – in a way that suits the time of data collection – the actual purpose and basis or actual need, means and methods used to collect, process and share the personal data of children and the like, as well as how to practice rights, and security measures to protect their privacy, and any substantial changes that occur

7- Imam Abdulrahman bin Faisal University is committed to informing the governor about other sources that are used if additional data are collected indirectly (from other sources).

8- The University is committed to providing the guardian with the options available about the processing of personal data for children and those of similar status and the mechanism used to practice these options, such as, for example, personal preferences through which the desirability of sharing their data for other purposes can be expressed.

9- The University is committed to adopting the concept of privacy by design and hypothetically – within the level of protection without the direct involvement of the child or the like – when providing services specifically targeted at this group.

10- Imam Abdulrahman bin Faisal University is committed to obtaining the consent of the guardian – which can be verified after reasonable efforts – to process the

personal data of children and the like after determining the type of consent (explicit or implicit) based on the nature of the data and the methods of collecting it.

11- The purpose of collecting the personal data of children and the like shall be in accordance with the relevant regulations and directly related to the activity of the controller.

12- The content of the data shall be limited to the minimum data necessary to achieve the purpose of its collection.

13- The collection of personal data for children and those of similar status shall be restricted to the previously prepared content (described in Rule 12) and shall be in a fair manner (direct, clear, secure and free from deception or misinformation).

14- The use of the data shall be limited to the purpose for which it was collected and approved by the guardian.

15- The University is committed to preparing and documenting the policy and procedures for the retention of personal data for children and the like in accordance with the specified purposes, regulations, and relevant legislation.

16- The University is committed to storing and processing the personal data of children and the like within the geographical borders of the Kingdom to ensure the preservation of national sovereignty over these data, and it is not permissible to process them outside the Kingdom unless the University obtains written approval from the regulatory authority (in accordance with the general rules for the transfer of personal data outside the geographical borders of the Kingdom) after the coordination of the regulatory authority with the National Data Management Office when necessary.

17- The university is committed to preparing and documenting the policy and procedures for data disposal to destroy data in a safe way that prevents its loss, misuse, or unauthorized access – including operational data, archived data, and backups – according to what is issued by the National Authority for Cybersecurity.

18- The University is committed to including the provisions of the retention and disposal policies in contracts in the event that these tasks are assigned to other processors.

19- The University is committed to identifying and providing the means through which the guardian can access, review, and update the personal data of the child and the like.

20- The University is committed to verifying the identity of the guardian before granting him access to the child's personal data and the like in accordance with the controls approved by the National Authority for Cyber Security and the competent authorities.

21- It is prohibited to share the personal data of children and the like with other parties except in accordance with the purposes specified after the approval of the guardian and in accordance with the relevant regulations, and policies, provided that the other parties are provided with policies and procedures related to the protection of the personal data of children and the like and included in contracts and agreements.

22- The University shall be bound by the guardian's notice and shall obtain its approval in the event that the data are shared with other parties for use other than the specified purposes.

23- The University shall give notice to the guardian in the event that it wishes to communicate directly with the child or the like for any purpose and shall give him the opportunity to refuse such communication, explaining how he does so.

24- The University is committed to obtaining the approval of the National Data Management Office – after coordination with the regulatory body – before sharing the personal data of children and the like with other parties outside the Kingdom.

25- The University is prohibited from collecting personal data from a child or a person of equivalent status concerning a member of his or her family in any case, except the personal data of the guardian.

26- The university is committed to the requirements of protecting the privacy of children and the like from the early stages of designing services and products that target this category, including websites or digital applications.

27- The University is committed to applying appropriate measures that prevent children and those of similar status from making their personal and sensitive data available to the public in such a way that they and their families can be identified directly.

28- The University shall apply appropriate and practicable measures as far as reasonably practicable to remove personal and sensitive data from the child's publications and the like prior to their publication, including the presentation of personal files and publication through social media accounts.

29- Imam Abdulrahman bin Faisal University is committed not to make automatic decisions based on the processing of personal data of children and the like and their use for multiple purposes that have a great impact on them, including for example direct marketing.

30- The University is committed to using administrative controls, technical measures, and adequate legal safeguards to protect the personal data of children and the like.

31- The University is committed to monitoring compliance with policies and procedures related to the protection of the personal data of children and the like periodically and shall be presented to the President of the University – or his delegate – as well as identifying and documenting corrective actions to be taken in the event of non-compliance and notifying the regulatory body and the Office according to the organizational sequence.

9.3 Exceptions

1- The consent of the guardian is not required in the event that the service provided to the child, or the like is a preventive or advisory service in accordance with the tasks and competencies of the university (organizations related to children protection), provided that the university is committed to collecting the minimum data necessary to achieve the purpose, and destroy it immediately after the completion of the service.

2- The consent of the guardian is not required in the event of disclosure of his personal data to a third party in order to implement a project commitment to the university or to implement another system or to implement an agreement to which the Kingdom is a party or to which the entity to be disclosed is a judicial or security entity.

3- The consent of the guardian is not required when the sole purpose of collecting the contact data of the child or the like is to respond directly to a specific request from the child and the like, and these data are not used by calling him again or for any other purpose, and they are not disclosed, and the university deletes them from its records immediately after responding to the child's request.

4- The consent of the guardian shall not be required when the purpose of the collection of the contact data of the guardian and the child and the like is to respond directly – once or more – to the request of the child and the like, and such data shall not be used for any other purpose, nor shall it be disclosed or combined with any other data, and the guardian shall be provided with a notice thereof.

5- The consent of the guardian shall not be required when the purpose of collecting the name of the child and the like, the name of the guardian and the contact data is to protect the safety of the child and the like, and such data shall not be used or disclosed for any purpose unrelated to the safety of the child and the like, and the university shall provide the guardian with a notice thereof.

9.4 General Provisions

First: The University shall harmonize the provisions of this policy with its organizational documents and circulate them to all parts of or associated with the university in a manner that achieves integration and ensures the achievement of the objective of preparing this policy

Second: The university is committed to monitoring and documenting compliance with this policy periodically

Third: The university is committed to comply with this policy and to document compliance in accordance with the mechanisms and procedures specified by the regulatory authorities.

Fourth: The university is obligated to inform the regulatory authorities immediately and without delay and not exceeding (72) hours of the occurrence or discovery of any incident of leakage of personal data in accordance with the mechanisms and procedures determined by the regulatory authorities.

Fifth: The University shall, when contracting with other processing entities, periodically verify the compliance of the other parties with this policy in accordance with the mechanisms and procedures specified by the regulatory authority, provided that this includes any subsequent contracts made by the authority.

Sixth: The regulatory body shall have the right to establish additional rules for the treatment of specific types of personal data for children and the like in accordance with the nature and sensitivity of these data after coordination with the Office

Seventh: The regulatory body shall, after coordination with the Office, prepare the mechanisms and procedures that regulate the process of dealing with complaints and objections according to a specific time frame and according to the organizational sequence of the bodies.

9.5 The Legal Guardian Special Provisions

1- The university may obtain the personal data of the child's guardian and the like directly, provided that it is committed to obtaining the minimum necessary data – the name and the method of communicating with the guardian – only for the sake of notification and obtaining the consent of the guardian.

2- The University is committed to using appropriate means to verify the identity of the guardian before taking his approval and granting him access to the child's personal data and the like in accordance with the controls approved by the National Authority for Cybersecurity and the competent authorities.

3- In the event that the consent of the guardian is requested and he does not provide his consent within (10)days from the date of communicating with him, the university is committed to destroying the child's personal data and the like and the guardian's data collected.

4- The controller shall be obliged not to use the personal data of the guardian for any purpose other than that for which it was collected within the limits of the consent to the collection and processing of the personal data of the child and the like.

5- The University shall be bound by the Parent's Notice of Applications and Approval of Personal Statements by the Child and the Like.

10. General rules for transferring personal data outside the geographical borders of the Kingdom

The Kingdom seeks to establish policies and standards for the transfer of personal data outside the geographical borders of the Kingdom, ensuring the preservation of national sovereignty over these data, as well as preserving the privacy of personal data holders and protecting their rights by determining the obligations of the university and processing regarding the transfer of personal data outside the geographical borders, and providing appropriate means to enable data subjects to practice their rights, and defining the roles and responsibilities of these bodies in addition to the regulatory and supervisory authorities to implement the provisions of these policies.

10.1 Rights of Data Subjects

Referring to the Personal Data Protection Policy, the basic principles of protection grant individuals specific rights with regard to the processing of their personal data, while the university's obligations set out the general rules that must be adhered to when processing them. With regard to the transboundary movement of personal data, the holder of the data has the same rights as set out in the Personal Data Protection Policy, with emphasis on the following rights:

First: The right to know, including the notification of the legal basis or the actual need to transfer his personal data outside the geographical borders of the Kingdom and the place where it is stored or hosted, and the bodies to which his personal data will be disclosed when it is transferred, and the purpose of this transfer, and taking his consent to that, and the security measures taken to protect his personal data during and after transportation.

Second: The right to revoke his consent to the processing of his personal data outside the borders – at any time – unless the purpose of the transfer of data is in the public interest, to protect the vital interests of individuals, or to implement legal requirements.

Third: The right to access his personal data at the university/external processor, to view it, to request its correction, completion, or updating, and to request its destruction of what is no longer needed, and to obtain a copy of it in a clear form.

10.2 The obligations of Imam Abdulrahman bin Faisal University regarding the transfer of data outside the geographical borders of the Kingdom

The original principle is to keep data within the geographical borders of the Kingdom, where the entity stores and processes personal data inside the Kingdom to ensure the preservation of national sovereignty over these data and the protection of the privacy of their owners, and it is not permissible to transfer or process them outside the Kingdom except after verifying the cases described below according to the following sequence:

1- If the external processing entity entrusted with the personal data processing activities in a country is included in the accreditation list, the university/internal processing entity shall obtain the written approval of the regulatory body on the transfer of data, and the regulatory body shall coordinate with the National Data Management Office.

2- If the external processing entity is in a country that is not on the accreditation list, the transfer of personal data outside the geographical boarders of the Kingdom requires an adequate level of protection – no less than the level of protection guaranteed by the policy of protection of personal data issued by the Office – after evaluating the level of protection provided by the external processor.

3- If there is no adequate level of protection, the entity shall establish appropriate safeguards to protect the rights of data subjects, such as, for example, the use of standard clauses or binding rules.

4- If the entity is unable to provide sufficient guarantees, one of the statutory exceptions requiring the transfer of data described in item (Third) below may be relied upon.

In all the cases mentioned in paragraphs (2), (3) and (4) above, Imam Abdulrahman bin Faisal University or the internal processor must obtain written approval from the organizational body for the transfer of data, and the organizational body must coordinate with the Office.

First: Assessment of the level of protection:

The party wishing to transfer the data beyond national boundaries must assess the potential effects and risks - on a case-by-case basis – to determine whether the university/external processing entity will provide an adequate level of protection of the rights of data subjects and present the results of the assessment to (the President) to determine and approve the level of acceptance of the risks. To do so, the entity must adhere to both general and legal evaluation criteria to ensure that the level of protection is appropriate in all circumstances:

A. General evaluation criteria

- **Nature and sensitivity of the data**: In assessing the level of protection, the university must take into account the type, value and volume of the data to be transferred and the degree of sensitivity thereof, as the transfer of sensitive personal data requires a high level of protection.

- **Purpose of data processing**: In assessing the level of protection, the entity must take into account the purpose of the processing, the target group of data subjects, the scope of the processing and the entities with which the data will be

shared, as the processing of sensitive personal data on a large scale requires a high level of protection.

- **Data processing period:** In assessing the level of protection, the university must take into account whether the processing will take place in a restricted or occasional manner - only once or for a limited period – or will take place on a frequent and regular basis, as the personal data to be processed on a regular and long-term basis require a high level of protection.

- **Data origin**: In assessing the level of protection, the university must take into account the country from which the data are collected -- not necessarily the country from which the data are to be transferred -- to determine the expectations of data subjects with regard to the level of protection, since the transfer of personal data collected from country that are subject to a very high level of protection requires a level at least equal to that of protection in those States.

- **Destination of data:** In assessing the level of protection, the university must take into account the stages at which personal data are transferred – sometimes more than one State – and the level of protection in the country of destination is assessed – the last stage of the transfer.

- **Security controls:** In assessing the level of protection, the university must take into account the administrative procedures, technical measures and physical controls adopted in the policies of the authority for information security, such as encryption, security controls and international standards.

If the results of the assessment of the level of protection – based on general criteria – show that in the particular circumstances of the situation the negative effects on the rights of the data subjects are limited and the potential risks are low, an assessment of the level of protection – based on legal criteria – may not be necessary in this case.

B. Legal evaluation criteria:

When the results of the assessment of the potential impacts and risks in (A) above are insufficient, those who wish to transfer data beyond national borders must observe these criteria. For example, sensitive personal data must be transmitted on a regular and widespread basis.

- **Regulations and legislation in force:** In assessing the level of protection, the entity must take into account whether the country to which the data are transferred has regulations and legislation protecting the rights of data subjects with respect to the processing of their personal data, and ensure that the participating parties are able to contract and abide by these contracts.

- **International obligations**: In assessing the level of protection, the body must take into account whether the country to which the data are to be transferred is a party to international conventions or adopts international principles and standards for the protection of personal data.

- **Rules and practices adopted**: In assessing the level of protection, the entity must take into account whether the country to which the data are to be transferred adopts rules of conduct, general practices or special standards for the protection of personal data.

Second: Appropriate guarantees:

If the entity is in a country that is not on the accreditation list and has not been subject to an assessment of the level of protection or the level of protection is insufficient, it shall provide appropriate safeguards for the protection of personal data, including:

- **Standard contractual clauses:** The entity must include in contracts and agreements model or standard clauses - to be approved by the Office – to restrict

the transfer of personal data outside the geographical limits of the Kingdom, ensuring the preservation of the privacy of its owners and the protection of their rights.

- **Binding common rules**: The university must prepare, within a multinational group, legally binding internal common rules applicable to extra-territorial transfers of personal data, including the processing and notification of privacy violations, to be approved by the National Data Management Office . Such common rules shall be included as a supplement to the service level agreements or contracts between the two bodies. The university must also obtain the approval of the regulator when there is any legal obligation to which the regulator or one of its affiliates is subject in another country that is likely to have a negative impact on the guarantees provided by the binding common rules.

- **Approved Code of Conduct:** Entities should use the Code of Conduct adopted by the regulators or the Office as an effective tool that sets out obligations for the controllers and processors to ensure that the privacy of data subjects is maintained, and their rights protected.

- **Accredited certificates**: The authorities shall seek the assistance of independent external parties that shall issue accreditation certificates confirming the existence of appropriate guarantees provided by the controllers or external processing entities. These entities also provide enforceable obligations for the application of these safeguards, including provisions related to the rights of data subjects.

- **Binding agreements between public bodies:** The public bodies, whether the controllers or the processing entity, shall sign a legally binding agreement for the transfer of personal data, provided that this agreement includes binding contractual clauses that guarantee the preservation of the privacy of the data subjects and protect their rights.

Third: Exceptions for specific cases:

Entities can transfer personal data outside the geographical limits without complying with the conditions and provisions described in item (First) and item (Second) above in specific cases, including the transfer of data outside the geographical limits of the Kingdom:

1-Based on the consent of the data subjects.

2-In implementation of a contractual obligation to which the data subject is a party.

3-In implementation of judicial requirements.

4-In implementation of the provisions of another system or international convention to which the Kingdom is a party.

5-To safeguard the public interest including the protection of public health or safety.

6-To protect the vital interests of data subjects.

In the cases mentioned in points (1), (2), (3), (4), (5), the university or internal processing entity must obtain the written consent of the organizational body to the transfer of data – on a case-by-case basis – and the organizational body to coordinate with the office. About the case mentioned in point (6), the university or the processor shall notify only the regulatory authority, and the regulatory authority shall notify the Bureau accordingly.

10.3 General Provisions

1- Imam Abdulrahman bin Faisal University and the processing entity must comply with these rules and document compliance in accordance with the mechanisms and procedures determined by the regulatory authorities

2- When contracting with processing entities– inside or outside the Kingdom – the university must periodically verify the compliance of the processors with these rules in accordance with the mechanisms and procedures determined by the regulatory authorities, provided that this includes any subsequent contracts performed by the processors.

3- The National Data Management Office shall practice the roles and functions of the regulatory authorities on the university in the event that it is not subject to regulatory authorities.

4- The regulatory authorities shall have the right to establish additional rules for the transfer of specific types of personal data according to the nature and sensitivity of such data after coordination with the Office.

5- The National Data Management Office reviews the evaluation criteria –general and legal – for the protection of personal data when transferred outside the geographical boundaries of the Kingdom and takes the decisions that regulate it.

6- The National Data Management Office shall establish a specific list of the main factor determining the appropriate level of protection, such as, for example, regulations and legislation, protection of rights and freedoms, national security, personal data protection rules, the supervisory authority for data protection, and the binding obligations undertaken by the State.

7- The National Data Management Office shall prepare, review, publish and update the accreditation list periodically, based on an assessment of the appropriate level of protection, not less than the level of protection provided by the personal data protection policy issued by the Office.

8- The National Data Management Office prepares and reviews the standard clauses for the protection of personal data.