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

جامعة الإمام عبد الرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

Data Classification Policy

Version: 2.0

CODE: DICT.I.06-21.CS.E.V2.0

1 Table of Contents

2 Intellectual Property Information

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

3 Document Control

1.1 Information

Title	Classification	Version	Status
DATA CLASSIFICATION POLICY	RESTRICTED	V2.0	ACTIVE

1.2 Revision History

Version	Author(s)	Issue Date	Changes
V1.0	DR. BASHAR ALDEEB	09/01/2021	CREATION
V1.1	DR. SAMER BANI AWWAD	12/03/2022	REVIEW AND UPDATE
V2.0	BAHA NAWAFLEH	28/12/2023	REVIEW AND UPDATE

1.3 Document Review

Date of Next Scheduled Review
01/01/2025

1.4 Distribution List

#	Recipients
1	ALL DICT DEPARTMENTS
2	LEGAL AFFAIRS
3	IAU WEBSITE
4	

1.5 Approval

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

4 Introduction

Information and technology security is essential for the success of the IAU. To this end, the Head of Cybersecurity Management develops, establishes, and organizes the necessary security operations to protect information and technology assets. This document outlines the Data Classification Policy within the IAU in accordance with relevant policies, regulatory procedures, legislative requirements, and regulations. This policy is part of the IAU's overall policy framework and is authorized by the designated authority from the date of its approval.

5 Objective

The objective of this policy is to define the necessary requirements and standards for classifying, handling, and protecting data in accordance with relevant laws, regulations, and legislations.

6 Applicability and Scope

The provisions of this policy apply to all affiliates or individuals engaged in work within the IAU, including hospitals and health centres under its umbrella, whether through permanent or temporary contracts, whether directly or indirectly. This also includes suppliers, external contractors, and any person with permanent or temporary access rights to data within the IAU, regardless of its source, form, or nature, and to the systems, devices, and databases of the IAU.

7 Policy

7.1 General Policy Requirements

7.1.1 Data classification and information must reflect its sensitivity, value, and importance to the operations of the IAU.

7.1.2 The Office of Data Management at the IAU must develop a plan for data classification, including a roadmap of activities and key milestones for data classification within the university.

7.1.3 The Office of Data Management at the IAU must identify and compile a list of all data groups and sources within the university.

7.1.4 Priorities for data groups and records that need to be classified must be determined by the Office of Data Management at the IAU based on their importance for classification.

7.1.5 Data should be classified upon creation or receipt from external sources, within a specified timeframe.

7.1.6 All important and sensitive data within the IAU must be classified.

7.1.7 An evaluation of the IAU's data must be carried out through a Business Impact Assessment, including the following steps:

- Identify categories that may be affected, including entities, individuals, persons, and the environment.
- Choose the potential impact levels for each category, ranging from "No Impact" to "Low," "Medium," and "High."
- Determine classification levels for data groups and records based on the assessed impact level:
  - ○ If the impact assessment is "High," classify data as "Top Secret."
  - ○ If the impact assessment is "Medium," classify data as "Confidential."
  - ○ If the impact assessment is "Low," classify data as "Restricted."
  - ○ If there is "No Impact," classify data as "Public."

7.1.8 Data classification must be based on the conducted Business Impact Assessment.

7.1.9 The possibility of classifying low-impact data as "Public" rather than "Restricted" should be studied by the Office of Data Management at the IAU. The assessment should include:

- Examining whether disclosing such data contradicts the laws of the Kingdom of Saudi Arabia, such as the Anti-Cybercrime Law and E-Commerce Law.
- Identifying potential benefits of disclosing such data and ensuring if these benefits outweigh the negative impacts.
- If publishing low-impact data does not violate any prevailing laws and its benefits outweigh the negative impacts, it should be classified as "Public."

7.1.10 All affiliates of the IAU must use classified data based on the principle of necessity for knowledge.

7.1.11 Access rights of affiliates to classified data should be restricted according to the principle of least privilege required for performing their tasks and responsibilities.

7.1.12 In cases of uncertainty about the level of classification to be selected, data should be classified at the highest classification level.

7.1.13 Accumulated or aggregated data must be classified according to their previously defined classification. In cases of differing classification levels, the higher classification should be applied.

7.1.14 If information and technology assets hold data of different classification categories, information and technology assets should be classified according to the highest classification category.

7.1.15 The necessary awareness and training must be provided to affiliates within the IAU regarding data classification and handling, in alignment with its sensitivity and impact level.

7.1.16 The Cyber Security Management should allocate security controls for protecting and processing data based on their classification. This ensures secure processing, sharing, and deletion of data, consistent with cyber security policies and relevant legal and regulatory requirements. Some examples of these controls include:

- Access management
- Restricting the use of classified data as "Top Secret" to specific locations, such as IAU facilities.
- Encryption.

7.1.17 All unclassified data within the IAU must be treated as restricted until classified.

7.1.18 All information and technology assets, including documents and physical media, must be labelled according to data classification.

7.1.19 Data within the IAU should be classified based on the sender's classification level (whether sent from within or outside the Kingdom), following applicable regulations and international agreements.

7.1.20 The Office of Data Management at the IAU must classify email messages according to the classification levels outlined in this policy.

7.1.21 The IAU must publish the granted classification levels for data groups.

7.1.22 Classified data must be stored and retained in accordance with IAU policies and relevant legal and regulatory requirements.

7.1.23 When using mobile devices or personal devices to access classified data, necessary controls must be implemented to protect the data in alignment with IAU policies and relevant legal requirements.

7.1.24 The IAU must classify its main data groups into internal and external data groups as follows:

- Internal: Primary data groups owned and managed by the IAU, representing the single source of truth across various entities.
- External: Primary data groups owned and managed by other governmental entities.

7.1.25 The IAU must classify its reference data groups into internal and external reference data groups as follows:

- Internal: Reference data owned and managed by the IAU, representing the "true source of information" across various entities.
- External: Reference data owned and managed by other governmental entities or considered standard data in the sector issued by external organizations such as ISO.

7.1.26 The IAU must document a list of specified data groups and records, along with all activities carried out during the data classification process. The record should include at least:

- List of specified data groups.
- Granted classification levels for data groups.
- Dates of classification level assignments for data groups.
- Imposed classification periods on data groups.
- Approved classification levels.

7.1.27 4-1-27: The IAU must review all classified data groups to ensure their suitability for the granted classification level, following the National Data Management Office's data classification policy.

7.1.28 4-1-28: The IAU must establish key performance indicators to measure the progress achieved in the data classification plan and implementation process within the IAU. These indicators should include at least:

- Percentage of classified data groups.
- Percentage of data groups classified at a specific classification level.
- Percentage of low-impact data classified as "Restricted."
- Percentage of classified data groups that underwent review and approval.

7.2 Data and Information Classification Levels

7.2.1 All data created, used, maintained, or possessed by the IAU must be classified into one of the following four classifications:

- Top Secret: Highly sensitive data is considered "Top Secret." This includes data that, if disclosed, could cause significant financial losses to the IAU, result in severe and exceptional damage to national security, cause significant harm to public interests, or cause severe and exceptional harm to the national economy or foreign relations.

- Secret: Sensitive data is classified as "Secret." This includes data that, if disclosed, could cause financial losses and result in severe damage to national security and the national economy.
- Confidential: Data and information that the disclosure of which is expected to have any negative impact on the operations of the IAU, its activities, its personnel, or related personal data.
- Unrestricted: Data that the IAU explicitly agrees to publish to the public under the classification "Unrestricted." Disclosing such information to unauthorized individuals does not cause any harm or damage to the IAU.

8 Roles and Responsibilities

The Data Management Office Management shall:

- The Director of the Data Management Office at the IAU is responsible for adopting the policy from the authorized entity and ensuring its implementation.
- The Director of the Data Management Office is responsible for adopting standards, procedures, and guidelines to ensure necessary compliance with the security requirements of the IAU's operations.
- The Director of the Data Management Office must ensure the alignment between this policy and the operations of the IAU.
- The Director of the Data Management Office is responsible for resolving any conflicts arising from this policy.
- The Director of the Data Management Office must provide the necessary resources to identify, procure, and implement technical solutions to meet the policy requirements wherever possible.
- The Data Management Office Management must periodically review the policy according to the established timeline.
- The Data Management Office Management must coordinate with relevant departments to monitor compliance and implementation.

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

- Ensure the dissemination of this policy to all affiliates within the IAU or the file.
- Report any violations or non-compliance with this policy to the Data Management Office Management.

8.1.1 Ensure that users of the IAU's information and technology assets are responsible for adhering to this policy and reporting any security incidents or non-compliance with this policy to the Data Management Office.

9 Policy Ownership

The Head of the Data Management Office in the IAU is responsible for this policy.

10 Policy Changes

The policy must be reviewed at least annually or when there are changes in legislative and regulatory requirements. Changes should be documented and endorsed by the authorized entity in the IAU.

11 Compliance

All affiliates within the IAU and relevant external parties/contractors must comply with the provisions of this policy. The Head of the Data Management Office in the IAU must ensure continuous monitoring of compliance and submit necessary reports periodically to the authorized entity.

Necessary measures must be taken to ensure compliance with the provisions of this policy. This may involve periodic reviews by the Data Management Office or relevant departments, and corrective actions taken by the authorized entity in the IAU based on recommendations from the Head of the Data Management Office regarding any violations of this policy. Disciplinary actions should be proportional to the severity of the incident as determined by the investigation, and may include, but are not limited to:

- Revoking access privileges to data, information technology assets, and systems connected to the IAU.
- Issuing written warnings or terminating the service of the affiliate, as deemed appropriate by the IAU.

Non-compliance with any provisions of this policy - without obtaining prior exemption from the Data Management Office in the university - requires taking appropriate actions according to the policies and regulations applicable in the IAU, or as deemed appropriate, and in accordance with contractual terms with any individuals or entities contracted with.

12 Related Policies, standards and Procedures

- ❖ DICT.I.06-01.CS.E. V2.0 - General Cybersecurity Policy
- ❖ DICT.I.06-02.CS.E. V2.0 - Cybersecurity Compliance Policy
- ❖ DICT.I.06-03.CS.E. V2.0 - Data Protection Policy

- DICT.I.06-20.CS.E. V2.0 - Data Storage and Retention Policy
- DICT.I.06-13.CS.E. V2.0 - Personal Data Protection Policy
- DICT.I.06-29.CS.E. V2.0 - Encryption Policy
- DICT.I.06-42.CS.E. V2.0 - Workstations, Mobile Devices and BYOD Security Policy
- DICT.I.06-11.CS.E. V2.0 - Data Sharing Policy
- DICT.I.06-53.CS.E.V2.0 Data Loss Prevention Standards
- DICT.I.06-56.CS.E.V2.0 Data Cybersecurity Standards
- DICT.I.06-58.CS.E.V2.0 Database Security Standards
- DICT.I.06-61.CS.E.V2.0 Data Protection Standards
- DICT.I.06-71.CS.E.V2.0 Encryption Standards
- DICT.I.06-79.CS.E.V2.0 Workstations, Mobile Devices and BYOD Security Standards

13 References

Department Name:	National Institute for Standards and Technology (NIST)	National Data Management Office	ISO 27001:2013 Standards	Cybersecurity Controls for Cloud Computing	Cybersecurity Controls for Social Media Accounts of Entities	Cybersecurity Controls for Remote Work	Cybersecurity Controls for Sensitive Systems	Core Cybersecurity Controls
Requirements of the General Policy	RA-2, AC-3, AC-4, AC-16, MP-2, MP-3, SC-16	National Data Governance Policies Controls and Specifications for National Data Management, Governance, and Personal Data Protection	A.8.2	-	1-1-5-2	1-6-2	2-1-6-2	3-2-7-2
Levels of Data and Information Classification	RA-2, AC-3, AC-4, AC-16, MP-2, MP-3, SC-16	National Data Governance Policies Controls and Specifications for National Data Management, Governance, and Personal Data Protection	A.8.2	-	1-1-5-2	1-6-2	2-1-6-2	3-2-7-2

14 Annex 1: Data Classification

The classification levels of data have been aligned based on the table provided below, in accordance with the classifications issued by the National Centre for Documents and Archives, approved by Cabinet Decision No. (595/M) dated 10/5/1421 AH, and the classifications issued by the National Data Management Office. These classifications will be issued as a unified data classification system by Royal Decree.

Classification of the National Data Management Office:		The classification of the National Centre for Documents and Archives	
Top Secret	Unauthorized access to, disclosure of, or tampering with this data or its content may result in significant financial losses, substantial harm to national security, and significant damage to national interests.	Top Secret	Documents and records whose disclosure to others would harm national security.
Confidential	Unauthorized access to, disclosure of, or tampering with this data or its content may lead to financial losses or partial damage to the reputation of the IAU or national interests.	Highly Confidential	Documents and records whose dissemination would harm public or private interests.
Restricted	Unauthorized access to, disclosure of, or tampering with this data or its content may have a negative impact on the operations of the IAU, its activities, its workforce, or personal data.	Confidential	Documents and records related to individual subjects or issues that, if disclosed or accessed, would have adverse effects on the social life of groups and individuals.

Available or Public	When unauthorized access to, disclosure of, or tampering with this data does not result in any negative effects on the operations of the IAU or national interests.	Available or Public	Documents and records related to non-confidential public topics that have been published or communicated to legal or natural entities.

Classification Level	Impact Level	Description
Top Secret	**High**	Data is classified as "Top Secret" when unauthorized access to, disclosure of, or tampering with this data or its contents leads to severe and exceptional harm that cannot be mitigated or rectified in the following areas: • National interests, including violation of agreements and treaties, damaging the reputation of the Kingdom, diplomatic relations, political affiliations, operational efficiency of security or military operations, the national economy, national infrastructure, or government affairs. • Performance of public entities resulting in harm to national interests. • Public health and widespread safety, as well as the privacy of senior officials. • Environmental or natural resources.
Confidential	**Medium**	Data is classified as "Secret" if unauthorized access to such data, or disclosure of it or its contents, leads to significant harm in the following areas: • National interests, such as causing partial damage to the reputation of the Kingdom, diplomatic relations, operational efficiency of security, military, economic, or national infrastructure operations, and government functions. • Financial loss at an organizational level leading to bankruptcy, inability to perform duties, significant loss of competitiveness, or a combination thereof. • Causes severe harm or injury affecting the lives of a group of individuals.

		• Leads to long-term damage to environmental or natural resources. • Investigation of specific major cases as defined systematically, such as terrorism financing cases.
Restricted	**Low**	Data is classified as "Restricted" if unauthorized access to such data, or disclosure of it or its contents, leads to: • Limited negative impact on the operations of public entities, economic activities in the Kingdom, or on the work of a specific individual. • Limited damage to the assets of any entity and limited loss to its financial and competitive status. • Limited short-term damage to environmental or natural resources.
Available or Public	**Not applicable**	Data is classified as "Public/Available" when unauthorized access to such data, or disclosure of it or its contents, does not result in any of the impacts, provided that there is no impact on the following: • National interests • Activities of entities • Personal interests • Environmental resources

Main Impact Category	National Interests		
Sub-Impact Category	The reputation of the Kingdom.		
Considerations	Will the information be of interest to local or international media? Will it give a negative impression?		
Impact Level			
Available	**Restricted**	**Confidential**	**Top Secret**
Not applicable	**Low**	**Medium**	**High**
No impact on vital national interests	Does not affect reputation	Affects reputation to some extent	Significantly affects reputation

Main Impact Category	National Interests		
Sub-Impact Category	The reputation of the Kingdom.		
Considerations	Will the information be of interest to local or international media? Will it give a negative impression?		
Impact Level			
Available	**Restricted**	**Confidential**	**Top Secret**
Not applicable	**Low**	**Medium**	**High**
No impact on vital national interests	Does not affect reputation	Affects reputation to some extent	Significantly affects reputation

Main Impact Category	National Interests		
Sub-Impact Category	………………………		
Considerations	Do the information pose a threat to relations with friendly countries? Will it increase international tension? Could it lead to protests or sanctions from other countries?		
Impact Level			
Available	**Restricted**	**Confidential**	**Top Secret**
Not applicable	**Low**	**Medium**	**High**
There is no impact on vital national interests.	There will be no significant impact on diplomatic relations, and there will be a minor effect in the short term.	Negatively affecting diplomatic relations in the long term.	Severing diplomatic relations and political affiliations, or threatening treaties and treaty obligations, or both.

Main Impact Category	National Interests		
Sub-Impact Category	National Security / Public Order		
Considerations	Do the information - if disclosed - assist in organizing terrorist activities or committing serious crimes? Does it constitute a source of panic for everyone?		
Impact Level			
Available	**Restricted**	**Confidential**	**Top Secret**
Not applicable	**Low**	**Medium**	**High**
No impact on vital national interests.	No significant impact on the operational efficiency of security operations at a regional or local level, and it prevents the detection of minor crimes in the short term.	Long-term impact on the ability and effectiveness of security agencies to investigate and prosecute serious organized crimes that contribute to internal instability.	Operational efficiency for maintaining public order, national security, or intelligence operations of military and security forces is significantly affected.

Main Impact Category	National Interests		
Sub-Impact Category	The national economy		
Considerations	Does the disclosure of information lead to economic losses at the national level?		
Impact Level			
Available	**Restricted**	**Confidential**	**Top Secret**
Not applicable	**Low**	**Medium**	**High**
-	Slight impact on the national economy with a recoverable decrease in the gross domestic product (GDP), employment rate, stock market prices, or purchasing power, resulting in a negative reflection on only one sector.	Long-term impact on the national economy with a recoverable decrease in the gross domestic product (GDP), unemployment rate, stock market prices, or purchasing power, resulting in a negative reflection on one or more sectors.	Long-term impact on the national economy with an irrecoverable decrease in the gross domestic product (GDP), stock market prices, unemployment rate, purchasing power, or other relevant indicators, resulting in a negative ripple effect across all sectors in the Kingdom.

Main Impact Category	National Interests		
Sub-Impact Category	National Infrastructure		
Considerations	Does accessing the information lead to disabling the vital national infrastructure (such as energy, transportation, communications)? In the event of cyberattacks, will essentially services in the Kingdom remain available?		
Impact Level			
Available	**Restricted**	**Confidential**	**Top Secret**
Not applicable	**Low**	**Medium**	**High**
-	Short-term damage or impact occurs on the security and operations of local/regional infrastructure.	Temporary interruption and malfunction in the security and operations of vital national infrastructure occur,	Disruption and malfunction in the security and operations of vital national infrastructure occur, affecting various sectors and disrupting normal life.

		affecting one or more sectors	

Main Impact Category	National Interests		
Sub-Impact Category	Roles of government entities		
Considerations	Will disclosing the information hinder the ability of government entities to carry out their daily operations and tasks?		
Impact Level			
Available	Restricted	Confidential	Top Secret
Not applicable	Low	Medium	High
-	Inability of one or more government entities to perform one or more non-core tasks for a short period.	Inability of one or more government entities to perform one or more of their main tasks for a short period.	Inability of all government entities to perform their main tasks and operations for an extended period.

Main Impact Category	National Interests		
Sub-Impact Category	Private sector profits		
Considerations	Will disclosing the information lead to financial losses or bankruptcy of private entities managing public facilities? For example, the possibility of fraud, illegal money transfers, and unlawful asset seizures.		
Impact Level			
Available	Restricted	Confidential	Top Secret
Not applicable	Low	Medium	High
There is no impact on the activities of the entities.	Limited damage consists of a minor financial loss to the entity or any of its assets.	The entity incurs severe financial losses, which could lead to bankruptcy.	Significant negative impact on private entities to an extent that it harms vital national interests.

Main Impact Category	National Interests		
Sub-Impact Category	Roles of private entities		
Considerations	Will the disclosure of information lead to damages to private entities managing public facilities? Will this result in the loss of their leading role or the loss of any of their assets? Will this lead to the termination of contracts for a significant number of affiliates? Will it affect the competitive ability of the private entity?		
Impact Level			
Available	**Restricted**	**Confidential**	**Top Secret**
Not applicable	**Low**	**Medium**	**High**
No impact on the activities of the entities.	Inability of the entity to perform one of its primary tasks and a limited loss of competitiveness.	Inability of the entity to carry out its primary tasks and a significant loss of competitiveness.	A significant negative impact on private entities to the extent that it harms vital national interests.88

Main Impact Category	individuals		
Sub-Impact Category	Privacy		
Considerations	Will disclosing the information lead to a violation of individuals' privacy?		
Impact Level			
Available	**Restricted**	**Confidential**	**Top Secret**
Not applicable	**Low**	**Medium**	**High**
No impact on individuals	Disclosure of personal data for the individual	Disclosure of personal data of an important personality	Disclosure of personal data of an important individual

Main Impact Category	The environment		
Sub-Impact Category	Environmental resources		
Considerations	Will this information be used to develop a service or product that could lead to the destruction of the Kingdom's environmental or natural resources?		
Impact Level			
Available	**Restricted**	**Confidential**	**Top Secret**
Not applicable	**Low**	**Medium**	**High**
No impact on the environment	Short-term or limited impact on the environment or natural resources.	Long-term impact on the environment or natural resources.	Catastrophic and irreversible impact on the environment or natural resources.

Main Impact Category	individuals		
Sub-Impact Category	Privacy		
Considerations	This would lead to a violation of any intellectual property rights.		
Impact Level			
Available	**Restricted**	**Confidential**	**Top Secret**
Not applicable	**Low**	**Medium**	**High**
-	-	-	What affects national interests

Main Impact Category	individuals		
Sub-Impact Category	Health and safety of individuals.		
Considerations	This would lead to the disclosure of information including names or locations of individuals and the like (such as names or locations of clients, individuals subject to special protection systems.		
Impact Level			
Available	**Restricted**	**Confidential**	**Top Secret**
Not applicable	**Low**	**Medium**	**High**
No impact on individuals.	No impact on individuals.	Serious harm or injury that threatens the individual's life.	General or severe loss of life, and the loss of an individual's or a group of individuals' lives.

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