Tabuk University Data Classification Policy

V.1.0

Description

Document Name	Data Classification Policy
Institution	Tabuk University
Document Owner	Data Governance Unit
Issue Number	1.0
Status	Release
Issue Date	September 1, 2024
Security Classification	Internal

Date of Modification

Version	Date	Modification	Edit	Review	Approval
1.0	September 1, 2024	None	Dr. Aisha Al-Hakami Data Management Officer	Dr. Maryam Al-Shahri Data Accessibility Officer	Dr. Mohammed Mutab Al-Otaibi Data Governance Unit Supervisor

Approvals

Name	Designation	Date	Signature
Dr. Mohammed Mutab Al-Otaibi	Data Governance Unit Supervisor	September 1, 2024	---
Data Governance Executive Committee	---	September 16, 2024	---

Table of Definitions

Term	Definition

University	University of Tabuk
University Departments	Vice-rectors, Deanships, Units, Departments, Sections.
Data Governance	A set of practices and procedures that help ensure the management of data assets at the university, from developing a data plan, developing the standards and policies to implementation and compliance.
Data Management	The process of developing, implementing, and overseeing plans, policies, programs, and practices to enable the university to govern data and enhance its value as a valuable and precious asset.
Data Element	A data element is a unit of data with a precise concept and clear attribute that represents a characteristic of its data entity—for example, a customer ID number and a customer name are the customer's data elements.
Data Dictionary	A data dictionary is a centralized list containing the detailed attributes specified for data elements (such as the element's name, description, source, and the data type it contains (i.e., a date, number, letter, etc.)
Data Quality	Data quality is the ability of data to meet the business, system, and technical requirements of the university. Data quality is typically measured in terms of completeness, relevance, timeliness, accuracy, consistency, relevance, and integrity.
Data Security	Data security represents the processes and technologies used to protect data from unauthorized access, viewing, modification, or deletion, whether accidental, intentional, or malicious.
Data Structure	Data structure includes the models, policies, rules, or standards that govern what data is collected and how it is stored, organized, and used in a database system.
Metadata	It is the information that describes the nature and characteristics of data elements, including business, technical, and operational data.
Data Reference	Data reference refers to the assumed reliability that ensures data definitions, data quality standards, and shared access rights are maintained.

Data Stewardship	Data stewardship is the assumed reliability by which recommendations are developed and decisions are implemented by the business data representative.
Business Glossary	It is a centralized list of business terminology that is documented and shared across the university.
Data Classification Levels	The following classification levels are available: (Highly confidential), (Confidential), (Restricted), (Public).

1. Introduction

This document represents the data classification policy of the University of Tabuk, referred to as the University within this document.

This document consists of main sections, including this introduction, followed by the purpose, scope, roles and responsibilities, policy provisions, and references.

All users are required to carefully read, understand, and fully comply with the University of Tabuk's Open Data Policy. If any information or part of this document is unclear, please contact the Data Management Office for clarification.

The University's Data Management Office is the owner of this document.

This document is valid for three years from its date of issuance. The Data Management Office must review and update this document at least annually, or it may be updated immediately upon any amendments or changes related to relevant legislative and regulatory requirements. The document version number will be changed whenever any modification is made, whether substantial or minor. These updates or modifications must be approved by the Data Management Office.

2. Purpose of the Document

In response to the National Data Management Office's initiative and related initiatives calling for the development of data governance policies in government agencies, based on the developed national data governance policies, the University's Data Management Office developed a data classification policy document, in line with the National Data Management Office's policies.

This policy aims to establish the basic rules and guidelines for the University's Data Management Office and relevant vice-rectors, deanships, units, departments, and divisions to classify data in a manner that reflects the university's business needs and the best possible practices from both an IT and business perspective.

3. Scope and Application of the Policy

The Data Classification Policy applies to all data produced, received, or handled by the University—whether produced or used before or after the adoption of this policy—regardless of its source or nature. This data and information may be of various forms and contents, including, but not limited to: paper records, meeting documents, emails, computer-stored data and information, audio and video tapes, maps, photographs, manuscripts, handwritten documents, or any other form of electronic or non-electronically recorded information that is publishable.

4. Policy Review Schedule

This policy must be reviewed regularly, at least once a year, as directed by the Policy Supervisor and requested by the University's Data Management Office.

5. Compliance Monitoring

All university employees and contractors must adhere to this policy, and university entities must ensure its implementation within their offices (deanships, units, departments, etc.). Compliance with the provisions of this policy is subject to periodic review by the University's Data Management Office. Failure to comply with or violation of any of its provisions will result in legal accountability, and necessary action will be taken as recommended by the University's Steering Committee.

6. Roles and responsibilities

Term	Definition
Steering Committee	Define data accountability by identifying business data representatives and business data specialists, reviewing and approving data classification levels, and making decisions to resolve issues and escalations.
Data Governance Unit	The Data Management Office is responsible for developing a data classification policy in line with the National Data Management Office's guidelines. This includes: -Preparing the data classification policy document and related updates. -Monitoring data classification activities to ensure that all data assets at the university are classified.

	-Preparing, reviewing, updating, and approving procedural manuals to clarify the university's policy implementation mechanism. -Submitting reports related to data classification activities and compliance reports with the university's data classification policy, and escalating data classification activities and compliance with the policy. -Developing awareness programs to raise awareness and promote the practice of data classification.
Business Administrations	The university's business departments implement the policy to classify and approve data, including: -Inventorying non-electronic data. -Preparing, reviewing, updating, and approving data guides. -Classifying data across the university in accordance with the principles and controls of the policy.
Information Technology Management	Applying controls to data according to approved classifications, in addition to providing technical and informational support to relevant entities to implement the policy. This includes: -Inventorying the university's databases. -Providing all information about the electronic data stored in databases to enable the university's business departments to classify data. -Providing the necessary data to prepare data directories for the university's databases based on the templates approved by the Data Management Office and sharing them with relevant organizational units. -Implementing protection policies and controls for electronic data at the university based on its classification.

	-Informing data representatives and the Data Management Office of any violations or non-compliance. -Installing, managing, and operating tools and systems for detecting data leaks at the university, and detecting and addressing violations, breaches, and security vulnerabilities.
Cybersecurity Management	Alignment with the policies and controls issued by the National Cybersecurity Authority, and monitoring, supervising, and controlling the implementation of controls on classified data.
Risk management	Review policy compliance reports and identify risks of non-compliance.

7 .Policy Clauses

University data entities must be defined and classified appropriately in accordance with classification standards that comply with the requirements, regulations, and policies set by the National Data Management Office**.**

1.1 Key Principles of Data Classification

- Principle One: Data Availability by Default

The default stance for data is accessibility (in the developmental domain), unless its nature or sensitivity necessitates higher levels of classification and protection. Conversely, data is presumed to be highly confidential (in the political and security domains), unless its nature or sensitivity necessitates lower levels of classification and protection**.**

- Principle Two: Necessity and Proportionality

Data shall be classified into levels according to its nature, level of sensitivity, and degree of impact, while taking into consideration the balance between its value and its degree of confidentiality**.**

- Principle Three: Timely Classification

Data shall be classified upon its creation or when it is received from other entities, and the classification must occur within a specific timeframe**.**

- Principle Four: The Highest Level of Protection

The highest classification level shall be adopted when the content of an integrated dataset includes various classification levels**.**

- Principle Five: Segregation of Duties

The duties and responsibilities of employee -with respect to data classification, access, disclosure, use, modification, or destruction- shall be segregated in a manner that prevents overlapping jurisdiction and avoids diffusion of responsibility.

- Principle Six: Need-to-Know

Access to and use of data shall be restricted based on a genuine need-to-know basis and shall be limited to the fewest possible employees within the University.

- Principle Seven: Least Privilege

The management of employee privileges within the University shall be restricted to the minimum privileges necessary to perform their assigned tasks and responsibilities.

8. General Controls for Data Classification

Based on the classification levels, the Data Governance Unit shall identify and implement appropriate security controls to protect the data, thereby ensuring its secure handling, processing, sharing, and disposal. In the event that data is not classified upon its creation or receipt according to the classification standards, such data shall be treated as 'Restricted' until it is properly classified. Furthermore, any data that was not classified at the time of this Policy's issuance must be classified within a specific timeframe, according to an action plan prepared by the Data Governance Unit and approved by the Executive Committee. Below are some examples of controls that may be utilized when classifying data. Reference may be made to controls and guidelines issued by the National Cybersecurity Authority and the Saudi Authority for Artificial Intelligence about data protection:

- Security Markings

- Text-based security markings shall be applied to paper and electronic documents (including emails) in accordance with each classification level.

- Access

- Logical and physical access to data shall be granted based on the principles of 'Least Privilege' and 'Need-to-Know.'

- The Information Technology Department shall prevent access to data immediately upon the expiry or termination of an employee's professional service at the University, and this action shall be included in the employee off-boarding procedures.

- Usage

- Classified data shall be used in accordance with the requirements of the classification levels. For example, the use of data classified as 'Highly confidential' shall be restricted to specified locations, whether physical (such as offices) or virtual (using hardware encryption or specialized applications).

- Storage

- Data classified as 'Highly confidential,' 'Confidential,' and 'Restricted,' as well as portable devices that process or store such data, shall not be left without continuous monitoring within the University.

- Data classified as 'Highly confidential,' 'Confidential,' ' and 'Restricted,' when stored physically or electronically and left unattended, shall be protected using an encryption method approved by the National Cybersecurity Authority.

- Data Sharing

- Entities shall determine the appropriate physical and digital means for securely exchanging data, thereby ensuring the reduction of potential risks and compliance with data sharing regulations.

- A mechanism for data exchange must be agreed upon, regardless of whether the entities (requesters) will utilize currently employed means for data exchange or not. Examples include the Government Integration Channel, the National Information Center Network, and the Secure Government Network, or establishing a new direct connection, utilizing removable storage media, a wireless network, remote access, or a Virtual Private Network (VPN), etc.

- Data Retention

- A retention schedule that specifies the retention period for all data shall be prepared.

- The retention period shall be determined based on relevant contractual, regulatory, and legal requirements.

- The retention schedule shall be reviewed periodically, annually, or whenever changes occur to the relevant requirements.

- Data Disposal

- All data shall be securely disposed of in accordance with the Data Retention Schedule, after obtaining the approval of the Business Data Representative.

- Data classified as ' Highly Confidential,' and 'Confidential,' that is controlled electronically, shall be disposed of using state-of-the-art electronic media disposal methods.

- All physical documents shall be disposed of using a paper shredder.

- A detailed record of all disposed data shall be prepared.

- Archiving

- Data shall be archived in secure and reliable storage locations.

- Backup copies of archived data shall be retained.

- Archived data classified as ' Highly Confidential,' and 'Confidential,' shall be protected using an encryption method approved by the National Cybersecurity Authority.

- A detailed and documented list of users authorized to access archived data shall be prepared.

- Declassification (Downgrading)

- Data shall be declassified or its classification level shall be reduced to the appropriate limit after the classification period ends, when protection is not required or is no longer required at the original classification level.

- In the event that data is incorrectly classified, the data user must notify the Business Data Governance Unit to determine the necessity of reclassifying it appropriately.

- Factors that aid in data declassification shall be determined when the classification levels are first established, and these factors must also be recorded in the Data Asset Register. These factors may include the following:

- A specific timeframe after data creation or receipt (e.g., two years post-creation).
- A specific timeframe after the last action was taken on the data (e.g., six months from the date of last use).
- Following a specific date (e.g., scheduled for review on January 1, 2024).
- Following certain circumstances or specific events that directly impact the data (e.g., a change in strategic priorities or a change in University personnel).

- Declassification (or downgrading) or reduction of classification levels—beyond factors that clearly aid in declassification—requires a sound understanding of the confidential data's content and the context in which it was established.

1.2 Identification of all University data and its sources

- The Business Data Governance Unit shall identify all University data, and participating entities of the University shall identify and document the data they possess.
- The sources of University data shall be defined as follows:

- Internal Data Sources: Business departments and internal systems that generate data for the University through the execution of business processes and services. These sources include, but are not limited to, physical or digital copies of reports worked on by internal departments, or data defined through the systems utilized.

- External Data Sources: External entities that provide agreed-upon data to the University for the execution of business processes and services. These sources include: student data providers, relevant government entities (electronic or physical data), and other regulatory bodies.

- **Data exchange channels should be identified as follows:**

  - Automated channels: include all automated and semi-automated channels, such as SMS, email, and integrations of technical and business systems.
  - Manual channels: non-technical channels, such as CDs, storage units, USB external hard drives, and paper documents.

- The Data Governance Unit cooperates with the concerned business departments in the university to include and describe the internal and external data sources, in addition to the related data exchange channels.
- The data governance unit is responsible for recording, listing, describing, and maintaining the data source and its related channels.

- When identifying internal data sources, a description of the place of data storage and the place of their management should be recorded.
- **When identifying external data sources, the following information should be considered**:
  - Whether there is an official data sharing agreement and/or a service level agreement with the University.
  - Whether the external party will provide the data to the University in whole or in parts.
  - Communication channels used for data exchange.
  - Applied security mechanisms.
  - The expected level of data quality (depending on the data quality policy and business needs).
  - External IT solutions comply with the University's standards and regulations for data protection and security.
  - The external party complies with the standards and principles of data management adopted at the University and the National Data Management Office.

9. Responsibilities for data definition and classification

The Data Governance Unit facilitates the classification of the identified data entities in coordination with the business data representatives within the university, and the table below specifies the matrix of roles and responsibilities for identifying and classifying data:

#	Procedure	Business data representative	Data Governance Unit	Information Technology Department
1	Identification of sources of data elements	A	C	R
2	Definition of data dictionary values	C	R	C
3	Application of data classification criteria	R	R	R
4	Verification of data classification results	A	R	R
5	Dissemination of the classification results	A	R	A
6	Preservation of the definition and classification of data	R	R	R

- R (Responsible body): one or more roles that perform the work required to accomplish the task.
- A (Accountable body): the role that is ultimately held accountable for completing the task correctly and completely
- C (Consultative body): one or more of the roles that are consulted for the required work.

- Any difference in classification should be escalated according to the "problem escalation procedure".
- All data entities should be documented using approved forms.

- All data entities and related characteristics should be defined and classified.

10. Data elements classification levels

The University's data elements shall be classified from both an institutional and executive level perspective.

10.1 Classification of data entities by institutional level

The university data elements shall be classified from the institutional level perspective into the following categories:

- Administrative data entities: includes all data elements, functions, and activities of the University's governance business (e.g., strategic planning, project management, performance management)
- Key business data elements: include data entities related to the functions of "key business value chain at the University".
- Supporting data entities: these include data entities related to supporting business functions and activities at the University (e.g., information technology, human resources, logistics, and others)

10.2 Classifying data entities by executive level

The university data elements shall be classified from the executive level perspective into the following categories:

- Importance: classification of data in terms of their importance for daily business within the University, in comparison with the ability of the university to continue business in the absence of such data.
- Privacy and data security: classification of data based on the rights and access rules of stakeholders and the results of assessing the impact of access to or dissemination of data.
- Data structuring: classifying data based on its structure (paper, digital,...) and the formats of its information when stored.
- Business functions: classifying data based on the main "business value chain" and linking them to the functions that created the data
- Storage: classifying data based on where the data is stored inside or outside the university buildings.

10.3 The details of classifying data entities by executive level

The university data elements shall be classified from the executive level perspective into the following categories:

#	Classification category	Value	Selection criteria
1	Importance (Only one value)	Critical data entities	If the data entity is used in critical business processes, and cannot be regenerated if lost.
		Non-critical data entities	If the data entity is not used in critical business processes, or can be regenerated if lost.
2	Privacy and data security (Only one value)	High impact: 'Highly Confidential,'	Data is classified as " Highly Confidential,' if unauthorized access to or disclosure of such data or its content results in serious and exceptional irreparable damage to: - National interests, including violation of agreements and treaties, damage to the reputation of the kingdom, diplomatic relations, political affiliations, operational efficiency of security and military operations, national economy, national infrastructure, or government business. - The performance of the University, which harms the national interest. - The health and safety of individuals on a large scale and the privacy of senior officials. - Environmental or natural resources.
		Average impact: 'Confidential,'	Data is classified as "'Confidential,' data" if unauthorized access to or disclosure of such data or its content results in serious and exceptional irreparable damage to: - National interests such as partial damage to the reputation of the Kingdom and diplomatic relations, or the operational

			efficiency of security and military operations, the national economy, national infrastructure, and government business. - A financial loss has occurred at the organizational level that leads to bankruptcy, the inability of entities to perform their tasks, a serious loss of competitiveness, or both. - Causes serious harm or injury that affects the life of a group of individuals. - Lead to long-term damage to environmental or natural resources. - Investigation of major cases identified by the system, such as cases of financing terrorism.
		Low impact: Restricted	Data is classified as "restricted" if unauthorized access to or disclosure of such data or its content results in serious and exceptional irreparable damage to: - Limited negative impact on the work of public authorities or economic activities in the Kingdom or on the work of a specific person. - Limited damage to the assets of any entity and limited loss on its financial and competitive position. - Limited short-term damage to environmental or natural resources. Restricted data is classified into three categories ● Restricted-level A: if the impact is at the level of the entire labor sector or any of the economic activities. ● Restricted-level B: if the scope of impact is at the level of activities of a specific group of the labor sector.

			• Restricted-level C: if the scope of impact is at the level of the activities of the university or a specific affiliate.
		No impact General	Data is classified as" public data " when unauthorized access to, disclosure of such data, or their content does not entail any of the listed effects.
3	Data structure (One or more values)	Paper form	In case the data entities or one of their properties is saved in paper form.
		Digital files, video, photos, audio, documents (unstructured, semi-structured)	In case the data entities or one of their properties is saved in one of the following digital file formats: video, photos, audio, or documents.
		Structured database	If the data entities or one of their properties is saved in the format of a structured database.
		Special structure (e.g., biometric data)	If the data entities or one of their properties is stored in the format of biometric data that is not covered by previous classification values.
4	Business functions (Only one value)	According to the defined functions within the University's	In any business function, the data entity was created first. (only one value from the specified main business value chain).

		business value chain	
5	Storage (One or more values)	Paper form storage in the main building	If the data entities or one of their properties is stored in paper form within the university buildings.
		Digital storage in buildings (CDs and storage units, USB , and external hard drives)	If storing data entities or one of their properties within university buildings electronically using CDs, USB drives, and external hard drives.
		Local data center (server)	If data entities or one of their properties is stored within the university buildings electronically using a structured database within the local data center (server).
		Secure online cloud storage (cloud)	If data entities or one of their properties is stored on a secure online cloud storage service outside the university buildings.

Classification Considerations:

The classification at the institutional level of the university should take into account the following questions and implications when categorizing data elements.

NO	Classification category	Consideration	Impact
	Importance	1-What data entities are required to execute the key business processes? 2- Can the university regenerate the data if it is completely lost? 3- Is data used in making strategic decisions?	1-Important data sources must be taken into account in the disaster recovery plan. 2-Important data sources should be taken into account when performing data backup procedures.
	Privacy and data security	1-Is there any policy, law, or regulation related to the ability to share information? 2-Study of the impact resulting from unauthorized access to data. 3/Do data entities include any sensitive information? (For example, personal or financial) 3-What are the currently used data masking rules? 4-What are the currently encrypted data entities?	-Classifications for data sharing or use should be defined based on national policy -Encryption mechanism must be implemented at the application and database level for sensitive data entities. - -Modify/Configure Access Privileges for App Users According to Data Privacy Classification.
	Data structure	-What is the final storage display for data entities? How does the university store data? What is the source of the data?	All paper-based data entities must be digitally archived. -All metadata should contain useful information that describes structured and semi-structured data entities -Maintain up-to-date documentation of all databases that host data entities.

	Business functions	*When were the data entities first created? If possible? *Are data entities staged?	# Data source must be distributed to the relevant work roles. Focus on supporting business functions with the required permissions and controls for managing data sources.
	Storage	*How do users retrieve the data? *What are the tools and applications used to display the data entities? *Are the data entities distributed across many components? *Are there specific services the university uses to perform business procedures or data processing?	Develop and implement a comprehensive data backup strategy to include all types of storage.

Mechanism of data classification based on privacy and data security dimensions:

- Determining all university data: the first step is to inventory and identifying all data the university possesses.
- Appointing a data classification officer: The university must authorize a person to undertake the classification process once the data possesses have been identified. Often, a business data representative is the person who understands the nature and value of data within the business administration.
- Assuming responsibility for initial classification: The office is responsible for carrying out the initial classification. Given that there is often more than one data officer within the
- university, there may be more than one person responsible for data classification.
    - The data representative assesses the potential impact that would result from:
        - Disclosure or unauthorized access: disclosure of data or unauthorized access to it.
        - Modification or destructions: modification of this data, its destructions or both.
        - Untimely Access: failure to access this data in a timely manner.
- The impact assessment process begins with the application of the principle of "origin in available data" (in the development field) unless its nature or sensitivity requires higher levels of classification and protection, and highly confidential (in the political and security sphere) unless its sensitivity requires lower levels of classification.

- **Impact category identification**

  The business data representative shall identify the primary and secondary category of potential impact under one of the following main categories:

- National Interests.
- Entity Activities.
- Individual Health and Safety.
- Environmental Resources.

- **Impact level determination:**
  - The Business Data Representative shall assign a specific level to each potential impact. The determination of the level is based on the following criteria:
    - Duration of the impact and the difficulty of controlling the damage.
    - Time required to recover and repair the damage after its occurrence.
    - Scale of the impact (e.g.) national level, regional /multiple and single entities. single entity, multiple individuals …. etc.).

  - These criteria define the four impact levels as follows:
    - 1/ High
    - Access to or disclosure of data results in serious or severe long - term damage that cannot be controlled or repaired.
    - 2/ Medium
    - Access to or disclosure of data leads to significant or serious damage that is difficult to control.
    - 3/ Low
    - Access to or disclosure of data causes limited damage, that can be controlled or intermitted short-term damage that is manageable.
    - 4/ No Impact
    - Access to or disclosure of data does result in any harm, whether in the short or long term.

- All potential and identified impacts during the assessment must base on evidence to reduce reliance on subjective judgement by the individual responsible for data classification.
- The Business Data Representative determines the data classification level based on the identified impacts and their respective levels:
  - High impact: Data is classified as '' Highly Confidential,'".
  - Medium Impact: Data is classified as 'Confidential'.
  - Low Impact: further assessments are required (refer to step 4 and 5).
  - No Impact: Data is classified as ''Public''
- A detailed description of the key considerations for each impact category and level is provided in table 2: (Impact Categories and Levels for Data Classification Assessment. located in the appendixes''.
- Additional assessment must be conducted if the impact level is classified as 'Low'', with the aim of elevating the classification level of data initially considered 'Public' to the highest appropriate level.

In this context, the Business Data Representative must examine whether the disclosure of such data conflicts with regulations in the Kingdom of Saudi Arabia, Such as the Anti-Cybercrime Law, the E-Commerce Law and others.

If the disclosure is found to be in violation of these regulations, the data must then be classified as ''Restricted'.

- Once the impact level confirmed to be'' Low'' and it is ensured that disclosure does not violate any applicable regulations, the potential benefits of releasing such data must be evaluated to determine whether those benefits outweigh the negative consequences.
- Potential benefits may include leveraging the data to develop new valued-added services or enhancing public engagement with government entities.
  - If the benefits outweigh the negative impacts, the data shall be classified as 'Public''.
  - If the benefits are less significant than the negative impacts, the data will be classified as ''Restricted''

The diagram in the annex outlines the necessary steps of conducting data classifications:

1.1 Classification Level Review

1.1.1 The Data Classification Officer must examine all classified data to ensure that the classification level assigned by the Business Data Representative is appropriate. This review must be conducted within one month of the essential classification.

1.2 Applying Appropriate Controls

1.1.2 The classification results shall be generalized and all the relevant controls and data classifications measures shall be implemented.

1.1.3 The classification process is finalized when all university-owned data has been classified, the classification levels have been verified, and the corresponding controls have been applied.

2- Appendixes

Impact Categories and Level for Data Classification Assessment

Data classified as Restricted may be further divided into sub-levels based on the scope of impact, as follows:

- Restricted - Level (A) When the impact scope affects an entire sector or a general economic activity.
- Restricted - Level (B) When the impact scope involves activities of multiple entities or affects the interests of a group of individuals.
- Restricted - Level (C) When the impact scope is limited to the activities of a single entity or interests of an individual.

The following table clarifies and identifies the appropriate classification level, enabling entities to evaluate the degree of impact from unauthorized access to, disclosure of, or content within the data. (For more information on the impact assessment process, refer to "Steps Required for Data Classification.")

Main impact category	National interest		
Sub-impact category	Reputation of the Kingdom		
Considerations	Will the information be subject to local or international media attention? Will it give a negative impression?		
Impact Level			
Highly confidential	Confidential	Restricted	Public
High	Moderate	Low	No impact
Reputation is significantly affected.	Reputation somewhat affected.	Reputation is not affected.	No impact on vital national interests.

Main impact category	National interest		
Sub-impact category	-		
Considerations	Does the information pose a risk to relations with friendly countries? Will it increase international tensions? Could it lead to protests or sanctions from other countries?		
Impact Level			
Highly confidential	Confidential	Restricted	Public
High	Moderate	Low	No impact
Cutting diplomatic ties and political affiliations or threatening agreements and treaty terms, or both.	Diplomatic relations will be negatively affected in the long term	No impact on diplomatic relations or minor impact in the short term	No impact on vital national interests.

Main impact category	National interest		
Sub-impact category	National security/public order		
Considerations	Would the publication of this information aid in organizing terrorist acts or serious crimes? Could it trigger widespread public panic?		
Impact Level			
Highly confidential	Confidential	Restricted	Public
High	Moderate	Low	No impact
The operational efficiency of maintaining public order and national security, as well as intelligence operations of the military and security forces, is significantly affected.	Long-term impact on the ability and efficiency of security agencies to investigate and prosecute serious organized crimes. that cause internal instability.	Negligible impact on the operational efficiency of security operations at the regional or local level, and prevention of the detection of minor crimes in the short term.	No impact on vital national interests.

Main impact category	National interest
Sub-impact category	National economy
Considerations	Can information disclosure cause economic losses at the national level?

mpact Level			
Highly confidential	Confidential	Restricted	Public
High	Moderate	Low	No impact
Long-term impact on the national economy involving an irreversible decline in GDP, financial market prices, unemployment rates, purchasing power, or other relevant indicators, which will adversely affect all sectors in the Kingdom.	Long-term impact on the national economy with a recoverable decline in GDP, unemployment rate, financial market prices, or purchasing power, negatively affecting one or more sectors.	An effect on the national economy that is limited to one sector and is characterized by a short-term decline in GDP, employment rate, financial market prices, or purchasing power.	No impact on the national economy.

Main impact category	National interest		
Sub-category of impact	National infrastructure		
Considerations	Does access to the information disrupt critical national infrastructure, such as energy, transportation, and communications? Will the Kingdom's essential services remain accessible during cyberattacks?		
Impact Level			
Highly confidential	Confidential	Restricted	Public
High	Moderate	Low	No impact
Disruption and failure in the security and operations of critical national infrastructure, affecting many sectors and disrupting normal life.	Interruption and disruption - Short-term impact on the security and operations of critical national infrastructure, affecting one or more sectors	Short-term damage or impact on the security and operations of local or regional infrastructure.	No impact on national infrastructure.

Main impact category	National interest		
Sub-impact category	Government Tasks		
Considerations	Will government agencies be unable to carry out their daily operations and tasks if information is disclosed?		
Impact Level			
Highly confidential	Confidential	Restricted	Public
High	Moderate	Low	No impact
The main tasks and operations of all government agencies being ineffective for a long period of time	Inability of one or more government agencies to perform one or more of their key functions for a short period of time.	Inability of one or more government agencies to perform one or more non-core functions for a short period of time.	No impact on government agency functions.

Main impact category	Individuals		
Sub-impact category: Individuals	Health/safety of individuals		
Considerations	Will the disclosure of information cause the disclosure of names, locations, etc.? For instance, the names and locations of confidential clients or persons who are subject to special protection regimes may be disclosed.		
Impact Level			
Highly confidential	Confidential	Restricted	Public
High	Moderate	Low	No impact

General or catastrophic loss of life, loss of life of an individual or group of individuals.	Serious injury or injury that threatens the life of an individual.	Minor injury without any threat to the life or health of an individual.	No impact on individuals.

Main impact category	Individuals		
Sub-impact category	Privacy		
Considerations	Will disclosure of the information violate the privacy of individuals?		
Impact Level			
Highly confidential	Confidential	Restricted	Public
High	Moderate	Low	No trace
Disclosure of personal data of a public figure.	Disclosure of personal data of a public figure.	Disclosure of personal data of an individual.	No impact on individuals.

Main impact category	Individuals		
Sub-impact category			
Considerations	Will this infringe on any intellectual property rights?		
Impact Level			
Highly confidential	Confidential	Restricted	Public
High	Moderate	Law	No impact
Affecting national interest			No impact on intellectual property rights.

Main impact cate gory	Environment		
Sub-category of impact	Environmental resources		
Considerations	Will this information lead to the development of a service or product that could result in the destruction of the Kingdom's environmental or natural resources?		
Impact Level			
Highly confidential	Confidential	Restricted	Public
High	Moderate	Low	No impact
Irreversible catastrophic impact on the environment or natural resources.	Long-term impact on the environment or natural resources.	Short-term impact on the environment or natural resources.	No impact on the environment.

14. Related documents
    - Data Dictionary Document
    - National Data Governance Policy Document.
    - Organizational manual and operating model for the National Data Management Office.
15. Sources

1. National Data Management Office (National Data Governance Policies).
2. Basic Cybersecurity Controls