SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

National Data Governance Policies

Version 1 - 5/5/2020

Public

Data Classification Policy

1. Data Classification Policy

1.1 Scope

The provisions of this Policy shall apply to all data received, produced, or managed by public entities regardless of its source, form, or nature. This shall include paper records, meetings, communications through social media and applications, emails, information stored on electronic media, audio or video cassettes, maps, photographs, handwritten documents, or any other form of recorded information.

1.2 Main Principles for Data Classification

Principle 1: Open by Default

Data shall primarily be accessible (in the development sector) unless its nature or sensitivity requires higher levels of classification and protection, and top secret (in the political and security sectors) unless its nature or sensitivity requires lower levels of classification and protection.

Principle 2: Necessity and Proportionality

Data shall be classified into levels based on its nature, sensitivity and impact, taking into consideration balancing its value against its confidentiality level.

Principle 3: Timely Classification

Data shall be classified upon its creation or upon being received from other entities; said classification should be timebound.

Principle 4: Highest Level of Protection

If information includes an integrated dataset with different classification levels, the highest classification level shall be approved.

Principle 5: Segregation of Duties

The duties and responsibilities of workers – vis-à-vis data classification, access, disclosure, use, modification, or destruction – shall be segregated to prevent any overlap of powers and avoid dispersal of responsibilities.

Principle 6: Need to Know

Data access and use shall be made pursuant to the Need-to-Know principle and for the least possible number of people.

Principle 7: Least Privilege

The privileges of personnel members shall be limited to minimal access required to perform the tasks and responsibilities assigned to them.

1.3 Data Classification Levels

Table 1 herebelow outlines the master data classification levels, as compatible with the relevant impact level, along with guiding examples for each level.

Classification Level	Impact Level	Description	Examples
Top Secret	High	Data shall be classified as “Top Secret” if unauthorized access to or disclosure of such data or its content has an exceptionally serious and irreparable effect on the following: - National interests, including violations of conventions and treaties, adverse damage to the reputation of the Kingdom, diplomatic relations and political	- Information on the encryption keys and mechanisms used for national infrastructure; - Information on terrorism crimes and plans threating national security; - Information on weapons and ammunitions or strategic military locations or any source of defensive or offensive force - Information on the movements of armed forces

		affiliations, or to the operational efficiency of the security or military operations, national economy, national infrastructure or government functions; - The functionality and performance of public entities, causing damage to the national interest; - The health and safety of individuals at a massive scale, especially senior officials; - The environmental or natural resources.	or other military forces, or VIPs - Information that affects the State's sovereignty
Secret	Medium	Data shall be classified as "Secret" if unauthorized access to or disclosure of such data or its content has a serious effect on the following: - National interests such as partial damage to the reputation of the Kingdom, diplomatic	- Information on logistics storage or economic storages; - Information on vital installations; - Memorandums of Understanding with international companies to establish commercial or strategic economic interests in the Kingdom;

		relations, operational efficiency of the security or military operations, national economy, national infrastructure or government functions; - Financial loss for organizations, leading to bankruptcy or to inability of the entities to perform their duties or major loss for competitive abilities or a combination thereof; - Significant harm or injury to the life of individuals; - Long-term damage to the environmental or natural resources; - Investigation of major cases, as defined by law, such as terrorism funding.	- Information related to bilateral agreements and diplomatic Memorandums of Understanding between the Kingdom and other countries.
Restricted	Low	Data shall be classified as “Restricted” if unauthorized access to or disclosure of such	- Information that damages the reputation of a public figure; - Detailed statements of individual transactions;

		data or its content causes: - Limited negative effect on the functioning of public entities or economic activities in the Kingdom or on a particular individual's business; - Limited damage to any entity's assets and limited loss to its financial and competitive status; - Limited, short-term damage to environmental or natural resources.	- Results of practical research and studies before publication thereof; - Information related to products under manufacturing, which may damage fair competition; - Information related to sensitive administrative appointments and decisions; - Information on an individual's medical file; - Personally Identifiable Information (PII) such as name, address, National Identification Number, phone numbers, bank account and license numbers, and biometric identifiers; - Information on employee salaries; - Documents such as tactical level plans, marketing programs prior to public release and technology innovation plans; - Supplier contracts and quotations;

			- Requests for proposals; - New product specifications prior to its public release; - Design and implementation details of security systems (firewalls, access control, network diagrams, etc.); - Internal policies and procedures of entities; - Internal Communications/Memos; - Internal phone lists and email lists of some entities.
Public	None	Data shall be classified as “Public” if unauthorized access to or disclosure of such data or its content has none of the above-mentioned impacts, particularly effects on: - National Interest; - Activities of entities; - Interests of individuals; - Environmental resources.	- Publicly released national strategic trends; - National statistics on population, environment, and businesses by industry, and others; - Public development and economic studies; - Governmental procedures and policies; - Information on public services provided to citizens by the government; - Contact persons at organizations;

			- Advertisement for job postings; - Public announcements; - Press releases; - Publicly released financial results; - (Public) product presentations; - Information on public relations; - Any information that is publicly available on the websites of any organization; - Advertisements.

Table 1: Data Classification Levels

Data classified as “Restricted” can be further classified into one of the following sub-levels based on impact level as follows:

- Restricted – Category (A): if the impact is at the scale of an entire sector or across a general economic activity;
- Restricted – Category (B): if the impact cuts across the activities of multiple entities or the interests of a group of individuals;
- Restricted – Category (C): if the impact relates to the activity of a single entity or the interests of a specific individual.

The following table illustrates and specifies the appropriate classification level that would enable entities to assess the impact level of

unauthorized access or disclosure of the data or its content (for more information on the impact assessment process, the "Data Classification Process" section provides further details).

Every entity should – on its own – conduct the impact assessment of unauthorized access or disclosure, and the list below is considered non-exhaustive.

Main Impact Category	**National Interest**		
Impact Sub-Category	Kingdom's Reputation		
Considerations	Would the information be subject to national or international media interest? Would it give a negative impression?		
Level of Impact			
Top Secret	Secret	Restricted	Public
High	Medium	Low	None
Reputation is immensely affected.	Reputation is affected to some extent.	Reputation is not affected.	No impact on vital national interests.

Main Impact Category	**National Interest**		
Impact Sub-Category	Diplomatic Relationships		
Considerations	Would the information pose any risk to the relationship with friendly countries? Would it raise international tension? Could it lead to protests or sanctions from other countries?		
Level of Impact			
Top Secret	Secret	Restricted	Public
High	Medium	Low	None
Diplomatic relationships and political affiliations are broken, and/or conventions and	Diplomatic relationships are compromised and will be negatively affected in the long-term	No effect on the diplomatic relationships or very minimal effect in the short-term	No impact on vital national interests.

treaties terms are compromised.			

Main Impact Category	**National Interest**		
Impact Sub-Category	National Security/Public Order		
Considerations	Would this information, if released, help with the conduct or commitment of terrorist or serious crimes? Would it create an alarm to the public?		
Level of Impact			
Top Secret	Secret	Restricted	Public
High	Medium	Low	None
The operational efficiency of maintaining public order and national security or the intelligence operations of military and security forces significantly affected and compromised.	Long-term effect on the ability and efficiency of security and military forces to investigate or prosecute serious organized crimes causing internal operational instability	A negligible impact on the operational efficiency of security operations at the regional or local level, and impeding the detection of minor crimes in the short-term.	No impact on vital national interests.

Main Impact Category	**National Interest**		
Impact Sub-Category	National Economy		
Considerations	Would this information, if disclosed, cause economic losses at the national level?		
Level of Impact			
Top Secret	Secret	Restricted	Public
High	Medium	Low	None
Long-term effect on the national economy,	Long-term effect on the national	Minimal effect on the national economy,	No impact on vital national interests.

with an unrecoverable decrease in GDP, capital market rates, employment rate, purchasing power and/or other relevant indicators. All the country sectors are affected	economy, with a recoverable decrease in GDP, employment rate, capital market rates and/or purchasing power, negatively affecting one or more sectors.	with a quick recoverable decrease in GDP, employment rate, capital market rates and/or purchasing power, negatively affecting not more than one sector.	

Main Impact Category	**National Interest**		
Impact Sub-Category	National Infrastructure		
Considerations	Would access to such information cause any interruption to the critical national infrastructures (i.e. energy, transport, health…)? In case of a cyber-attack, would the critical services of the Kingdom be still available?		
Level of Impact			
Top Secret	Secret	Restricted	Public
High	Medium	Low	None
Failure and long interruption to the security and operations of critical national infrastructures; several sectors are affected, and normal life is interrupted.	Short-term failure and interruption to the security and operations of critical national infrastructures; one or more sectors are affected.	Short-term effect on the security and operations of local/regional infrastructures.	No impact on vital national interests.

Main Impact Category	**National Interest**
Impact Sub-Category	Functions of Government Entities

Considerations	Would the release of the information limit the ability of government entities to carry out their daily operations and functions?		
Level of Impact			
Top Secret	Secret	Restricted	Public
High	Medium	Low	None
Inability of all government entities to conduct their functions and daily operations for a long period of time.	Inability of one or more government entities to deliver one or more of their functions for a short period of time.	Inability of one or more government entities to deliver one or more of their non-core function(s) for a short period of time.	No impact on vital national interests.

Main Impact Category	**Entity Activities**		
Impact Sub-Category	Profits of Private Entities		
Considerations	Would disclosure of this information lead to financial loss or bankruptcy of private entities operating public facilities? For example, the possibility of fraud, illegal transfers of funds, illegal appropriation of assets.		
Level of Impact			
Top Secret	Secret	Restricted	Public
High	Medium	Low	None
Significant impact on the private entities, causing damage to the vital national interests.	Entities incurring heavy financial losses, possibly leading to bankruptcy.	Non-serious damage in the form of limited financial loss to an entity or any of its assets.	No impact on entity activities.

Main Impact Category	**Entity Activities**
Impact Sub-Category	Functions of Private Entities
Considerations	Would the release of this information cause any damage to private entities operating public facilities? Would it cause their loss of

	their leading role or of any of their assets? Would it lead to terminating a significant number of employees? Would it affect the competitiveness of the private entity?		
Level of Impact			
Top Secret	Secret	Restricted	Public
High	Medium	Low	None
Significant impact on the private entities, causing damage to the vital national interests.	Inability of the entity to perform its core functions, and significant loss of its competitiveness.	Inability of the entity to perform one of its core functions, and limited loss of its competitiveness.	No impact on entity activities.

Main Impact Category	**Individuals**		
Impact Sub-Category	Health/Safety of Individuals		
Considerations	Would release of this information lead to disclosure of the names or locations of individuals? (e.g. names and locations of undercover agents, people under special protection orders)		
Level of Impact			
Top Secret	Secret	Restricted	Public
High	Medium	Low	None
General or massive loss of life; loss of life of an individual or group.	Significant harm or injury impacting the life of an individual.	Minor injury with no risk to the life or health of an individual.	No impact on individuals.

Main Impact Category	**Individuals**		
Impact Sub-Category	Privacy		
Considerations	Would release of this information lead to violation of the privacy of individuals? Would it infringe any intellectual property rights?		
Level of Impact			
Top Secret	Secret	Restricted	Public

High	Medium	Low	None
Disclosure of the personal information of a VIP, affecting the national interest.	Disclosure of the personal information of a VIP	Disclosure of the personal information of an individual.	No impact on individuals.

Main Impact Category	Environment		
Impact Sub-Category	Environmental Resources		
Considerations	Would this information be used to develop any service/product that could potentially destroy environmental or natural resources of the country?		
Level of Impact			
Top Secret	Secret	Restricted	Public
High	Medium	Low	None
Irreparable catastrophic effect on the environment.	Long-term effect on the environment or natural resources.	Short-term or limited effect on the environment or natural resources.	No impact on the environment.

Table 2: Categories and Levels of Data Classification Impact Assessment

1.4 Data Classification Controls

Based on the data classification levels, entities shall identify and implement appropriate data protection controls to ensure secure handling, processing, sharing and disposal of data. If data is not classified at the time of creation or receipt as per the classification criteria, it shall be treated as “Restricted” until correctly classified.

The data that was not classified at the time of issuing these Policies shall be classified within a specific period of time according to an action plan to be prepared by the entity and approved by its head. Below are some

examples of the controls that can be used when classifying data (refer to the data protection controls and guidelines published by the National Cybersecurity Authority).

Data Classification controls include but are not limited to the following:

Protective Marking

- Protective marking shall be applied to paper and electronic documents (including emails) as per each classification level.

Access

- Access to data – logical and physical – shall be granted based on the principles of "Least Privilege" and "Need to Know."
- Access shall be denied immediately upon the expiration or termination of the professional service of entity employees.

Usage

- Classified data shall be used as per the requirements of the classification levels. For example, "Top Secret" data shall only be used within specified locations whether physical (e.g. offices) or virtual (e.g. using cryptography or special applications).

Storage

- Data classified as "Top Secret," "Secret" and "Restricted," as well as mobile devices that process or store such data, shall not be left unattended.
- Unattended "Top Secret," "Secret" and "Restricted" data shall be protected while being physically or electronically stored, using any of

the encryption mechanisms approved by the National Cybersecurity Authority.

Data Sharing

- Entities shall decide on the appropriate physical and digital means of secure data sharing that ensure minimization of potential risks and compliance with data sharing regulations.
- Entities shall agree on the data sharing mechanism, whether they will utilize existing sharing mediums, e.g. Government Service Bus, National Information Center Network, or Secured Government Network, or will set up a new direct connection, removable storage media, Wi-Fi, remote access, VPN, etc.

Data Retention

- A schedule defining the retention period of all data shall be prepared.
- The retention period shall be defined based on the applicable business, contractual, regulatory and legal requirements.
- The retention schedule shall be reviewed periodically/annually or when there are changes in the relevant requirements.

Disposal of Data

- All data shall be securely disposed of according to the data retention schedule upon the approval of the relevant Business Data Executive.
- Data which is classified as “Top Secret” or “Secret” and which is electronically controlled shall be disposed of by using the latest electronic media disposal methods.
- All paper-based data shall be disposed of using a cross-cut shredder.
- A detailed log of all disposed of data shall be maintained.

Archiving

- Data shall be archived in secure storage locations, as recommended by the relevant Business Data Executive.
- Archived data shall be backed up.
- Archived data classified as “Top Secret” and “Secret” shall be protected using any of the encryption mechanisms approved by the National Cybersecurity Authority.
- A detailed list of users authorized to access archived data shall be prepared and documented.

Declassification

- Data shall be declassified or downgraded upon the expiration of the classification period, or when protection is no longer required at the original classification level.
- In case data has been wrongly classified, a data user shall notify the Business Data Executive to determine the extent to which it is required to re-classify such data appropriately.
- Data declassification triggers shall be set when the initial classification levels are first applied and shall be captured in the data register. These triggers may include:

  o A specified period after data creation or receipt (e.g. two years after creation);

  o A specified period after taking the last action on data (e.g. six months from the date of the last use);

  o After the lapse of a specific date (e.g. to be reviewed on 1 January 2021);

o After particular circumstances or events that have a direct impact on the data (e.g. a change of strategic priorities or a change of the employees of government entities).

- Declassification or downgrading of data, beyond the clear declassification triggers, shall require a sound understanding of both the sensitive data content and its context.

1.5 Data Classification Process

Step 1: Identify all data of the entity

The first step to be taken by an entity is to prepare an inventory of all the data owned by such entity.

Step 2: Appoint Responsible of Performing data classification

Upon completion of a data inventory, the Entity shall assign the responsibility for performing the classification to a particular person, usually the Business Data Executive, who is an employee of the entity's office and who best understands the data and its value. This person shall be responsible for making the initial classification. As there could be several Business Data Executives within the Entity, there could be more than one classifier.

Step 3: Conduct impact assessment process

The Business Data Executive shall follow the steps required for an assessment of the potential impact arising from:

- The disclosure of or unauthorized access to such data;
- Amendment and/or destruction of such data;
- Lack of access to such data in a timely manner.

The impact assessment process shall be initiated with the application of the 'Open by Default' principle (in the Development sector) unless its nature

or sensitivity requires higher levels of classification and protection; and the Top-Secret classification (in the political and security sectors) unless its nature or sensitivity requires lower levels of classification.

Step 3.a: Identify the impact category

The first stage of the impact assessment process is to identify the main and subcategory of the potential impact in any of the following main categories:

- National interest
- Entity activities
- Health or safety of individuals
- Environmental resources.

Step 3.b: Identify the impact level

The second stage implies that the Business Data Executive must assign to each potential impact a level of impact depending on the following:

- The impact duration and the difficulty to control the damage;
- The time to recover and repair the damage after its occurrence; and
- The size of the impact (on a national or regional level, several entities, single entity, multiple individuals, etc.)

These parameters define the four levels of impact:

- **High Impact:** Access to or disclosure of such data shall cause extremely grave or serious long-term damages that cannot be recovered or rectified.
- **Medium Impact:** Access to or disclosure of such data shall cause grave or serious long-term damages that are difficult to control.

- **Low Impact:** Access to or disclosure of such data shall cause limited or intermittent short-term damages that can be controlled.
- **No Impact:** Access to or disclosure of such data is unlikely to cause any long- or short-term damage.

All potential risks identified throughout the impact assessment process shall be specific and evidence-based, in an attempt to limit the subjectivity of the person classifying the data .

Based on the identified impacts and their levels, the Business Data Executive shall determine the data classification level:

- High Impact: data shall be classified as “Top Secret.”
- Medium Impact: data shall be classified as “Secret”
- Low Impact: further assessments need to be conducted (please refer to Steps 4 and 5)
- No Impact: data shall be classified as “Public”

A detailed description of the key considerations for each impact category and level is outlined in Table 2 “Data Classification Impact Assessment Categories and Levels”.

Steps 4 and 5 must be taken into consideration whenever the impact level identified is Low.

Go to step 6 if data has been classified as “Top Secret”, “Secret” or “Public.”

Step 4: Identify relevant laws and regulations (only if impact level is Low)

If the impact level identified is Low, additional assessments must be performed in order to maximize the classification level of the data classified as "Public."

In this regard, the Business Data Executive must study whether disclosure of such data would conflict with the Kingdom's laws, including, but not limited to, the Anti-Cybercrime Law and the E-Commerce Law. If such disclosure of data proves to be against the laws and regulations, data shall then be classified as "Restricted;" otherwise the Business Data Executive must proceed to carry out Step 5.

Step 5: Balance between the benefits of disclosure and negative impacts (only if the answer to Step 4 is "NO")

After confirming a low impact level and ensuring that the data disclosure shall not imply any breach of any existing law, an assessment of the potential benefits of this disclosure must be conducted to make sure whether or not those benefits would outweigh the negative impacts. Potential benefits include data use for the development of new value-added services, improvement of the transparency of government operations, or greater involvement of the citizens with the government.

- If benefits are greater than negative impacts, data shall be classified as "Public"
- If benefits are less than negative impacts, data shall be classified as "Restricted."

Step 6: Review classification level

The data classification reviewer – an employee of the entity's data management office – shall check all classified data to ensure that the

classification level assigned by the Business Data Executive is the most appropriate one. This classification level shall be reviewed within one month of the initial classification.

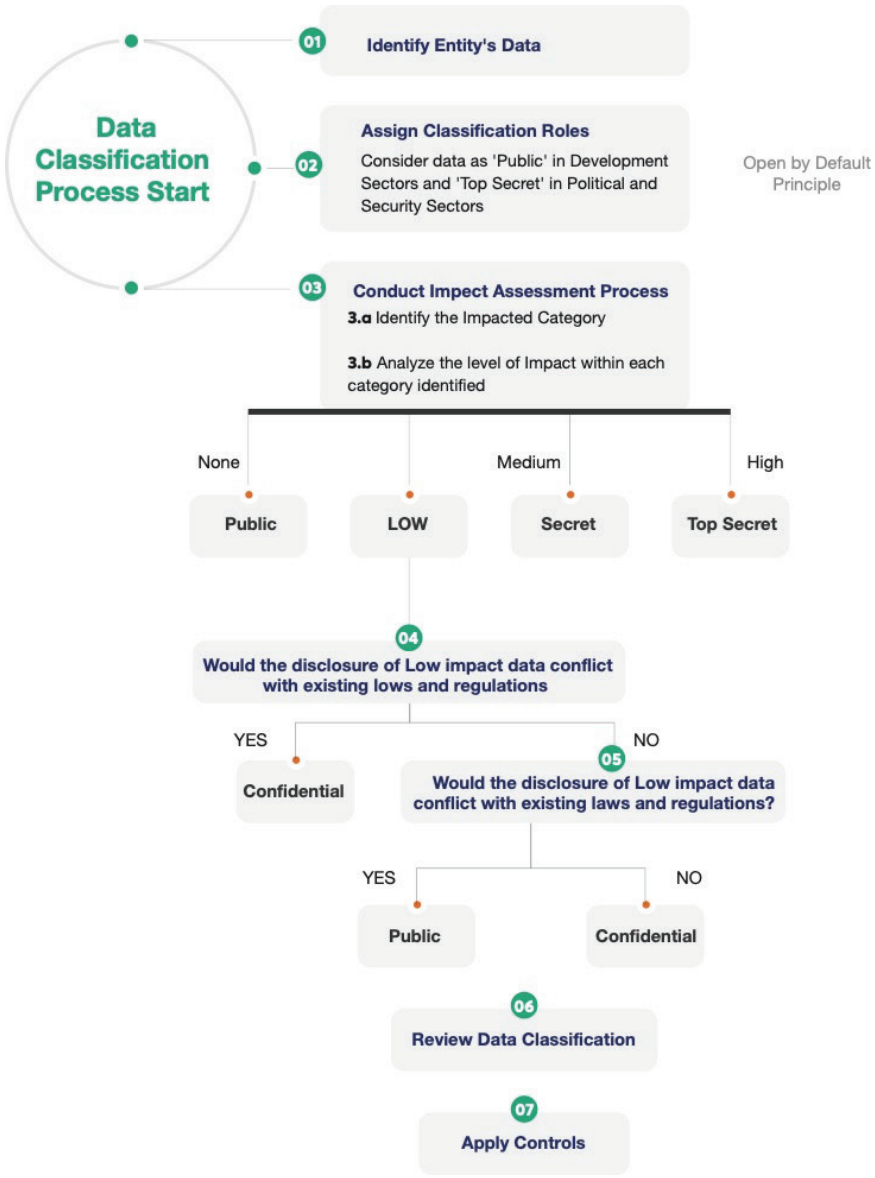
Step 7: Apply appropriate controls

The last step of the data classification process is to ensure that all data is protected as per its classification level by applying the relevant controls (refer to the section entitled “Data Classification Controls”).

The classification process shall be assumed to be concluded when all the data owned by the entity is classified, its classification levels are verified, and the relevant controls are applied.

After data classification is complete, entities can share such data with other entities or make it available or publish it as open data in case the classification level is “Public.”

Figure 2 below illustrates the steps needed to perform data classification.



1.6 Roles and Responsibilities within the Entity

All entities shall designate persons to be responsible for performing the obligations assigned to each of the job roles associated with the data classification process and the conditions for its protection as outlined below:

Business Data Executive: A person responsible for the data being collected and maintained by the entity, usually a member of senior management. The Business Data Executive shall address the following:

- **Data classification:** Classify all data collected by the entity or its affiliates;
- **Data compilation:** Ensure that data compiled from multiple sources is classified at the highest level of individual classification;
- **Data classification coordination:** Ensure that data shared between departments or entities is consistently classified and protected.
- **Data classification compliance (in coordination with Business Data Stewards):** Ensure that data is protected as per specific controls.

Data Classification Reviewer: Usually a member of senior management, a Data Classification Reviewer is responsible for reviewing and approving the data classification levels as defined by the Business Data Executive,

Business Data Steward: A Business Data Steward is usually a member of the IT and/or Information Security departments. He is responsible for protecting the data by applying the approved controls as per the provisions of the section entitled “Data Classification Controls.” He also maintains and supports the systems, databases, and servers that store data. The duties of a Business Data Steward can be outlined as follows:

- **Access control:** Ensure that proper access controls are implemented, monitored and reviewed in accordance with the Data Classification levels designated by the Business Data Executive.
- **Audit reports:** Submit an annual report to Data Administrators addressing availability, integrity and confidentiality of classified data.
- **Data backups:** Perform regular backups of data.

- **Data validation**: Validate data integrity on a periodical basis.
- **Data restoration:** Restore data from backup media.
- **Monitoring activity:** Monitor and record data activities, including information on any person accessing such data.
- **Data Classification compliance** (in coordination with Data Administrators): Ensure that the entity's data is classified and secured following the process described in these Policies and in accordance with the defined controls.

Data User: An employee who manages, accesses, uses, or updates data to complete a task authorized by the Business Data Executive. A Data user shall benefit from the data in line with the set purposes and in compliance with these Policies and all policies related to data usage across the Kingdom. The head of the entity shall assign the above roles to qualified people within the entity as he deems appropriate.