وزارة الاقتـــصاد
الرقمـي والريادة

DATA CLASSIFICATION & MANAGEMENT POLICY

(2019)

E-Government Strategies

Policies and Strategies Directorate

Table of Content:

Table of Exhibits

1. Introduction

This document sets out a proposed Data Classification and Management Policy for the Government of Jordan (the "Policy"). The Policy is intended to provide guidelines and direction to government entities in Jordan on how to classify their existing data under the proposed Data Classification Scheme.

It is proposed that the Policy should be adopted by the Cabinet of Ministers, and implemented under the stewardship of the Ministry of Digital Economy and Entrepreneurship (MoDEE), in line with the guidelines provided in this document.

The document is structured as follows:

- Section 2 explains the purpose of the Policy.
- Section 3 defines the Policy and in particular its Scope, Data Classification Scheme, principles for Data Classification and Data Management, and the structure and flow of a Data Management Program.
- Appendix I provides a glossary of the terms used throughout this document.
- Appendix II discusses the three most common Data Management Models.
- Appendix III provides concrete examples of Data Classification under this Policy.
- Appendix IV includes the text of the Jordan Open Government Data Licence.
- Appendix V provides a summary of the relevant legal framework.

2. Purpose of the Policy

The general purpose of this **Data Classification and Management Policy (the "Policy")** is to establish a framework for the classification and management of existing and future Government data in Jordan, consistent with the goals set in several Government policy documents or initiatives.

In particular, as stated in the MoDEE's "**General Policy for the Information & Communications Technology and Postal Sectors, 2018**" (the "**ICTP Policy 2018**"), "*Government data collected and stored over the years represents a valuable resource that can, if made available in an appropriate manner, contribute to community and economic development and enable citizens and other stakeholders to participate in decision-making and in developing policies. The release of government data can also lead to greater trust in government and the public sector through the increased transparency and accountability its release provides. Nevertheless, the storage, circulation and release of government data must be undertaken in a manner that ensures national security and individuals' privacy is maintained.* ***This means that government data must be managed in accordance with a data classification scheme*** *and the release of data for publication must be subject to data policies that maintain security and privacy.*"[1]

The above policy direction is a logical consequence of several related broader Government policy initiatives and legal framework provisions in this area including, in particular, those briefly described below:

- Under the **Open Government Data Policy 2017**[2] **("OGD Policy")** (launched as part of the 3rd National plan 2016-2018 of **Open Government Partnership ("OGP") Initiative**), Government entities must disclose and publish all data subject to disclosure in open formats, while recognizing legitimate reasons for confidential and restricted access to certain information in line with applicable legislation. The OGD Policy also defines principles for open data, and requires Government entities to conduct an inventory of existing data early in the process of development of their respective open data policy.
- According to the Government's "**Fourth National Action Plan 2018-2020 under the Open Government Partnership Initiative (OGP)**"[3], weak dissemination and pre-disclosure of governmental data can affect citizens' rights to access data and exclude them from participation in public decision-making processes. Further, because of the absence of reliable sources, conflicting information is allowed to proliferate via media and non-media

[1] ICTP Policy 2018, paragraphs 139 and 140.
[2] http://moict.gov.jo/uploads/Policies-and-Strategies-Directorate/Policies/Open-Government-Data-policy.pdf
[3] OGP-4th plan

sources. This all leads to poor access of information by corporations, academia and entrepreneurs, which undermines the country's growth and development.

- The freedom to "seek, receive and impart information" held by Government authorities is guaranteed by **Article 19 of the International Covenant on Civil and Political Rights of 1966, ratified by Jordan**, which is subject to the respect or the rights or reputations of others, and the protection of national security, public order, public health or morals.
- Citizen's access to Government data through modern technology means is also consistent with the goals pursued by the **Right to Access to Information Law No. 47 of 2007**.
- Finally, the MoDEE's "**General Policy for the ICT and Postal Sectors 2018**" mentions that "*Government requires that all government entities participate in the development of common standards and where possible enable exchange of data between applications and the development of integrated data sets*."[4]

To fulfil the above Government obligations and objectives, the more specific aims of this Policy include:

- The definition of a Data Classification Scheme and procedures for Government Data;
- Setting out general rules and guidelines for the governance and management of such Government Data;
- Allowing Government entities to identify which Data should be proactively disclosed to the public based on Jordan's Open Government Data Policy 2017 and the other documents mentioned above;
- Facilitating broader adoption and implementation, across Government entities, of new technologies for Data Management, such as the Cloud;
- Providing guidelines on Data Management and the improvement of Data Accessibility and Availability; and
- Specifying standard definitions of Data Management terminology to promote consistency.

In the information age, all information has value and should be viewed as an asset. Nevertheless, maximizing the value obtainable from information is conditional on Data Availability and Accessibility to persons or processes that can add such value. However, these notions must be balanced with information security and degrees of confidentiality justified through the principles mentioned above. Efficient application of the current Data Classification Policy should provide effective means to achieve such a

[4] Paragraph 151.

balance and add significant value to the National Economy. It will also help unlock the currently under-exploited and under-shared asset value of Government Data, and thus contribute to the National Economy.

3. Data Classification Policy

3.1. Scope of the Policy

The Policy applies to all data under the custody of the Government of Jordan, regardless of form.

This Policy applies to all Data under the ownership or custody[5] of the Government of Jordan ("Government Data"), whether generated by Government Entities or entrusted for safekeeping to Government Entities by Private Entities or persons.

The Policy covers all such Government Data in any form, such as electronic, printed, audio visual, and includes live, backup and archived Data, as well as own, externally acquired or third-party sourced Data.

This Policy does not apply to Data produced, stored, disseminated or shared by Non-Government Entities, Private Entities or citizens of Jordan in their conduct of affairs with other Non-Government Entities, Private Entities or citizens – or otherwise. Such Data remain subject to any applicable data protection, industrial property or other relevant laws.

This Policy is subject to all laws of Jordan in effect including, but not limited to, **"the State Secrets and Documents Law No. 50"** of the year 1971 and any provisions that may replace it in the future. Other laws and policies of relevance are listed in Appendix IV.

Under ICTP Policy 2018[6], the Government will designate the **Ministry of Digital Economy and Entrepreneurship (MoDEE)**) as being responsible for government digital transformation operations. The same Ministry has been also responsible for implementing Jordan's e-government Program, assigned to it at its launch in March 2001.

This Policy is thus adopted by the MoDEE under the sponsorship and ultimate supervision of Council for Digital Transformation and Public Administration.

5 For the definition of "Data Owner" and "Data Custodian" see Appendix I.

6 Paragraph 149.

3.2. Data Classification Scheme

Data covered by this Policy are hereby classified under the following four (4) categories:

- **Public**
- **Confidential and shared**
- **Sensitive**
- **Secret**

Any terms currently in use by different Government entities for their classification of data based on the required level of security should be analysed and aligned with those used above, in order to ensure a unified terminology across all Government entities.

Generally, Data Classification Schemes rely on the different **potential impact of a possible Data Security breach** (i.e., the unintended or unauthorised loss **of Data Confidentiality, Data Integrity or Data Availability**).

Data covered by this Policy are hereby classified under four (4) categories:

- Public
- Confidential and shared (requiring a "medium level" of security)
- Sensitive (requiring a "high medium" level of security)
- Secret (requiring the highest level of security)

The Table below lists the Data Classification categories under this Policy, and the corresponding categories under the State Secrets and Documents Law.

Data Classification under the Policy	Corresponding categories under the State Secrets and Documents Law
Secret	Top Secret
Sensitive	Secret
Confidential and shared	Restricted
Public	Ordinary

Exhibit 1: Data Classification categories under the Policy and corresponding categories under the State Secrets and Documents Law

In addition to the above categories under the State Secrets and Documents Law, various Government entities in Jordan may currently use other, different, data classification terminologies for the different types of data they manage. These alternative classification policies currently in use must be aligned as soon as possible with the one introduced above, which should henceforward apply across all Government entities. Reliance on a uniform data classification system across all Government entities will be indispensable for the design of common principles, protocols and procedures for the exchange, combination, processing and broader use of Government data from different sources.

Any such required alignment process should be the task of the Government entity currently in charge of such alternative data classification systems in use. It should involve a careful analysis of the Security standards currently in place for such systems and map these against those applicable under the Data Classification set out in this document.

The Exhibit below provides a reference to the impact level of a Security breach associated with each of the above four Data Classification categories, and a few indicative examples of the type of information that could be brought under each of these categories.

Data classification categories	Impact of possible Data Security breach	Examples of data or other information falling under the relevant category
Secret (highest level of security)	Security breaches relating to such Data can be expected to have a severe or catastrophic effect on the State's operations or assets, public security, public health or the lives of citizens.	Information relating to confidential exchanges with other countries, national defence or national security
Sensitive ("high medium" level of security)	Security breaches relating to such Data are very likely to cause serious damage to State or public legitimate interests, and possibly also to individuals.	Formal or informal information between different government authorities in the preparation of an official government document or policy; information relating to public criminal investigations, or involving business secrets or industrial property that may not be publicly disclosed

Confidential and shared (a "medium level" of security)	Disclosure of such Data outside the Government authorities authorized to share or other security breaches may cause limited harm to the State or the public, and potentially more important harm to individuals whose Data are affected by such a breach.	Information which, while sensitive (e.g., because it relates to sensitive personal data) is exchanged and needs to be shared between certain Government authorities in the framework of their duties (e.g., minutes of meetings, information on citizens, inventories etc.)
Public	Disclosure of such Data to the public will have no negative impact and may actually add value to the Data. Nevertheless, it is still important to ensure the Data Set's integrity and continuing public availability after its release to the public.	Information on government authorities' structures, tasks, list of persons responsible for specific tasks; budgets, policies, work plans, reports, studies, statistics, procedures, agreements with private or public parties, procurement procedures and policies, etc.

Exhibit 2: Impact level and examples of information for each Data Classification category

Examples of Data Classifications under this Scheme can be found in **Appendix** III.

3.3. Data Classification and Data Management Principles

Data Classification has implications for the location of and controls over the Data concerned, and the related disclosure standards and access rights.

Data Classification can rely on certain indicators to identify obvious examples of Public Data, but in other cases it will require individual assessment, consistent with the principles and procedures of Data Management set out in this section.

As stated in the General Policy for the Information & Communications Technology and Postal Sectors,[7] Data Classification determines:

- where data are held
- any required controls over their storage, management, use and disposal
- the person(s) to whom they may be circulated or disclosed, and
- the person(s) by whom they may be accessed.

This Policy recommends the following high-level approach as regards each of the above parameters and each of the four classes of data defined under the Policy. These recommendations should not be interpreted as absolute rules, as they may need to be fine-tuned to the circumstances of particular Data Sets, evolving technology and security standards, and the experience gained with the Policy's implementation across different Government entities. However, deviations from these recommendations will need to be justified.

[7] Paragraph 143.

	Location	Level of required controls	Persons to whom the data may be circulated or disclosed	Persons by whom the data may be accessed
Secret	Jordan	Highest	Set of a defined number of addressees within defined State units	Data Steward, Program Lead and Steering Committee (These terms are explained in section 4.4)
Sensitive	Jordan, with possible exceptions (secure data centers/cloud)	High	All officials within one, and possibly more, defined Government units	All officials within the Government unit responsible for Management of the Data
Confidential & Shared	Jordan or int'l secure data centers (cloud), with possible case by case restrictions, if justified	High	All officials within all Government units on a need to know basis	All officials within the Government unit responsible for Management of the Data, and defined other Government officials/units
Public	Jordan and int'l	Medium	The public in general	The public in general

Exhibit 3: Detailed descriptions of data classification levels

The Data Classification process can and should employ several very simple and clear indicators for the task of Classification. Further details and examples are provided in other sections, but the below four indicators should serve to provide general guidance:

1. Data or printed information that are already in the public domain or were public information in the past and will likely continue to be public information, should be presumed to be **Public Data** under this Policy.
2. Data or information that, under the State Secrets and Documents Law No. 50, qualify as "Top Secret" should be presumed to qualify as "Secret" under this Policy; and those qualifying as "Secret" should now be presumed to be "Sensitive" under the present

Policy. Government Entities already have codes and policies that cover, manage and restrict this type of information under the State Secrets and Documents Law No. 50.

3. Any publication or disclosure of Data or information that would be a violation of any law of Jordan (such as those listed in Appendix III) would be illegal, and are thus be excluded from a qualification as Public; they may, however belong to one of the other categories.
4. All other Data Classification tasks require assessment under the Data Management principles described below.

Once Data Classification has been carried out, the remaining **Data Management** should be guided by the following general principles:

- **Data Management Program:** Government Entities following the Policy must implement a Data Management Program (see Section 3.4, below), aimed at defining and following the organizational requirements required to implement the appropriate Data Management policy principles within the respective government units. These requirements cover, in particular, the determination of the appropriate organizational structure for the Policy's implementation, roles and responsibilities within the relevant organization, the required qualifications of key personnel, and the design of a Data Classification process for effective implementation.
- Not all Data exhibit equal risk of unintended disclosure, nor are all Data of equivalent value to the Public. The classification and management applied to the Data must be commensurate with the risk associated with inappropriate disclosure or loss. Therefore, **Data Management and Data Classification cannot be administered in a single manner across the entirety of an organization**. Each Data Area must be assessed for the Data and Information Assets it contains.
- **Data Access:** Use of and access to (whether internal to the organization or externally) Data depends on their Data Classification levels. To ensure that Data are not misused, are used ethically, according to any applicable law and with due consideration for individual privacy, access privileges must be defined based on the relevant users' roles, this Policy and the Data Management Program described in more detail below. Four categories of access privileges should be defined: (a) Read Only; (b) Read, Save and Print; (c) Read, Comment and Discuss; and (d) Change and Edit.

- Government Data under the scope of this Policy should be considered, by default, as **qualifying for classification as Public Data, and hence be suitable for disclosure and publication under the OGD Policy, unless** one of the conditions for exception and/or other classification set out under the Data Management Program is met.
- **Open Government Data Licence:** Unless specified otherwise on a case by case basis every citizen of Jordan shall have a right to access any and all Public Data under the Jorden Open Government Data Licence, whose current version is attached hereto as Appendix IV, and which may be **updated from time to time.**
- **Data Retention: To the extent possible, the Data Classification and Data Management Program** p**rocess** should also take into account and plan a retention schedule for each Data Set.
- **Data Security:** Access to Data must be controlled in accordance with the security practices set forth under the Data Management Program described below. The relevant approval and a consideration of appropriate use should be required before access is granted or otherwise made available (whether internal or external).
- **Data Transit:** Secret and Sensitive Data under this Policy will not generally be transmitted between different Government entities, other than under a very closely defined number of allowed destinations (e.g. limited to different security services, or selected units of the same Ministry). Confidential and shared Data may be exchanged between Government entities only but, if so, must be protected by strong encryption and other security controls, both while at rest and during their transit.
- **Universality:** This Policy applies to Data in all formats, whether digital files, electronic documents, emails, online transactions, Data held in databases or on tape or disks. Nevertheless, an access right granted for one purpose is not universally granted for all purposes. Each new use case must be approved under the applicable Data Management procedures, in a new request or an amendment to the original request, even if an End User already has access to the Data.

3.4. Data Management Program

This Policy is adopted by the government, under the general oversight of the Council for Digital Transformation and Public Administration.

Responsibility for the supervision of the Policy's implementation lies with the [Provisional name: Government Data Classification Department – GDCD], within the MoDEE.

The Digital Transformation Skill Centre established in each Government entity shall be the unit responsible by default for the implementation of this Policy, unless a separate unit is established by decision at the level appropriate to that Government entity. The responsible unit is referred to in this policy as the Steering Committee.

The Steering Committee will have responsibility for establishing Data Classification policies and guidelines for ensuring the appropriateness of Public Data, and for achieving maximum value from Data. It will appoint a Program Lead, who should manage and facilitate the implementation of the Program, prepare and review Data Sets before submitting to Steering Committee for approval, administer published Data, and respond to new requests.

The Program Lead may also act as the Data Steward, or appoint one or more persons responsible for this task. Data Stewards will have direct responsibility for Data Integrity and Data Quality, and the implementation of Data Classification within their Data Area.

Before any Government Data are published for the first time, verification and approval with the Data Steward is required to ensure that the Quality, Integrity, and Security of Data will not be compromised. The Data Sets to be published require final approval by the Steering Committee.

It is recommended that each Government entity's Data Management Program should include the following steps:

1. **Launch, with the creation of the Steering Committee**
2. **Appointment of a Program Lead**

3. **Decision on the Data Management model, definition of Data Areas and appointment of Data Steward(s)**
4. **Selection of 1-3 Data sub-areas for pilot programs**
5. **Creation of Data Inventories by Data Stewards for their Data sub-Area**
6. **Data Classification and definition of Access rights, first by the Data Steward with clearance by the Program Lead**
7. **Adjustments to, and approval of, Data Classification/Access rights by the Steering Committee**
8. **Publication and repeat from step 5, once the Pilot Program has been completed.**

Without aiming to impose any specific technology for Data Management, this Policy highlights general principles that should govern the choice of any such technology for the purposes of this Policy.

An effective Data Management Program should make optimal use of the available technical solutions and other constraints (e.g., budget or limited technical resources), to ensure the required level of safety for the entry, storage, retrieval, transfer and processing of the Government Data concerned. The use of emerging technologies, such as the cloud, can address challenges such as the absence of common IT systems and interfaces across the administration today, address security challenges through broad (but user-controlled) network access and reduce costs, resource pooling, rapid elasticity and on-demand service.

3.4.1 General Oversight

The **Digital Transformation and Public Administration Council** exercises general oversight over this Policy, which is hereby adopted by the **MoDEE**, in the framework of its mandates, powers and duties described above, in Section 3.1.

Within the MoDEE, a dedicated unit [Provisionally proposed name: Government Data Classification Department – GDCD] shall have responsibility for the supervision of the Policy's implementation by all Government entities covered by its scope, technical assistance on its interpretation and any required coordination. The GDCD shall report to HE the Minister of the MoDEE.

3.4.2 Steering Committees

Pursuant to the General Policy for the Information & Communications Technology and Postal Sectors, 2018, "*Government requires that each ministry, governorate, municipality and other public sector entity establishes a Digital Transformation Skill Centre. The Skill Centres will be responsible for their respective entity's business processes, electronic services and IT systems and applications. The skill centre will therefore provide the leadership for digital transformation projects for the entity*."[8]

Accordingly, within each of the above Government entities, the **Digital Transformation Skill Centre** established under the above policy shall also be the unit responsible by default for the implementation of this Policy, unless a separate unit is established by decision at the level appropriate to that Government entity (e.g., Minister, Chairman, supervisory authority etc.) The unit responsible for the implementation of this Policy in each Government entity shall be referred to hereafter in the text of this Policy as the "**Steering Committee**".

Government entities or their respective Steering Committee directly should communicate to the GDCD, their respective titles, contact details and initial composition not later than [three] months from the adoption of this Policy.

The Steering Committee's size and qualifications should be commensurate to the size of the Government entity and the volume, complexity and sensitivity of the Data it produces manages. It should be preferably comprised of staff familiar with the Data within the Government entity in question, and relevant laws of Jordan. The Steering Committee should have leadership and oversight role of the Data Management Program within the Government entity in question.

Where the size of the Government entity or the Data it is responsible for are not sufficient to justify a Steering Committee, that entity may appoint a single Program Lead instead and/or arrange for its Data Management Program to be managed by another, supervisory, Government Entity which has established its own Steering Committee.

The Steering Committee should have responsibility for establishing Data Classification policies and guidelines for ensuring the appropriateness of Public Data, and for achieving maximum value from Data. It should oversee the progress made by the Project Lead, and approve or modify proposed Data Set Classifications by Program Leads and Data Stewards (see below). The Steering Committee should meet regularly to address a variety of Data Management Program issues and concerns, and should be entrusted with its continuous improvement.

[8] Paragraph 129.

3.4.3 Program Lead

Each Steering Committee must appoint one or joint, **Program Lead(s**), who should manage and facilitate the implementation of the Program, prepare and review Data Sets before submitting to Steering Committee for approval, administer published Data, and respond to new requests. The Program Lead should regularly report to the Steering Committee.

During each phase of the Data Management Program, the Program Lead should:

- Provide an advisory role to Data Stewards (see below)
- Monitor and measure the progress of the overall Program and phases.
- Continually improve Data Access and ensure that End Users have enough information about the Data to interpret them correctly and consistently.
- Be the central point of contact regarding requests for Data Sets to be made "Public", or requests from other Government Entities for sharing of Data that are classified as "Confidential & Shareable".

3.4.4 Data Steward

Depending on the size of the organization and its Data, the Program Lead may also act as the **Data Steward**, or appoint one or more persons responsible for this task. Data Stewards will have direct responsibility for Data Integrity and Data Quality, and the implementation of Data Classification within their Data Area. Data Stewards will responsible for ensuring the requirements of the Data Classification Policy and procedures are followed within their organizational unit by establishing standards for their Data Area, together with the Steering Committee and the Program Lead, and by raising awareness of the Policy requirements within their area of responsibility. Data Stewards must have a solid understanding of how the Data in question add value to Jordan, and how End Users can and do employ the Data.

In order to provide a complete and accurate assessment and report to the Data Owner and the Steering Committee, Data Stewards should first obtain an inventory of all Data and Information Assets under their stewardship. This inventory should include location (i.e. where the Data are stored), name of Data Set, Data Labels, and date range of records. Further, to the best of their ability, Data Stewards should assign one of the four Classification categories to the Data Set, and if necessary, to the Data Labels. The inventory report should then be submitted to the Program Lead for review, and finally to the Steering Committee for final approval.

Data Stewards shall have the responsibility for ensuring the highest levels of Data Integrity and validated Data Quality for Data created and updated under their stewardship. Data Creators must ensure appropriate procedures are followed to uphold the Quality and Integrity of the Data they create. Data Elements must be kept up to date throughout every stage of the workflow and operations, preferably in an auditable and traceable manner

Before any Data or Information Asset is published (other than what has already been published), verification and approval with the Data Steward is required to ensure that the Quality, Integrity, and Security of Data will not be compromised. The Data Sets that are to be published require final approval by the Steering Committee.

3.4.5 Data Management Program Implementation Steps

It is recommended that each qualifying organisation's Data Management Program should preferably follow the steps set out below. Each of these steps (with exception of the first point) should be approved by the Steering Committee, taking into consideration the organisation's specific needs and resources.

1. **Launch of Program:** Creation of the Steering Committee, preferably from within the organisation. If necessary, the qualifying organisation may have to recruit external advisors or experts, at least on a temporary basis during a transitional phase, to address the Steering Committee members' lack of experience in this area.

2. **Appoint a Program Lead:** Responsible for the daily progress of the Program, this office will undertake most of the work to jump-start the Program.

3. **Data Areas:** The Steering Committee, with assessment input from the Project Lead, should decide on an organizational level model for Data Management (see 0). Although it is possible to choose multiple models within an organization, it is not advisable. Based on the chosen management model, Data Areas can now be defined, and Data Stewards can be appointed by the Project Lead to each of the areas.

4. **Pilot Programs:** With Data Areas having been defined, and with input from the Data Owners, the Project Lead can begin to select one to three Data sub-Areas ideal for implementing pilot programs.

5. **Data Inventory:** Data Stewards begin assessing and creating the Data Inventory for their Data sub-Area. At first, it might be easier to create a general inventory before diving into too much detail. Also, it is recommended to limit the exercise to the scope of the Pilot Program. There will be time later to go through all Data in phases. At the end of this section, the Data Steward(s) should have an accurate inventory of Data within the scope of the assigned Pilot Program.

6. **Classification-I:** Data Stewards should try to classify the inventoried Data themselves, then submit the results to Program Lead, who will review and make recommendations. This process will help Data Stewards become familiar with their role. In the same phase, and taking into consideration the relevant Government entity's structure, organisation, tasks and human resources, Data Stewards should also propose different Access groups within and outside the organisation. Access groups should be classified in different categories, and include references to the group members' position/title, their authorized personal IDs and a government IP dedicated address using the government official title rather than the individual's name (unless the access group includes the public at large). This is because Access rights will depend on a person's position within the organization and not on the identity of that individual, which may change over time as people move to other positions.

Each access group should be given different access permits by the Data Steward, under one of the following four categories:

a) Read only
b) Read, Save & Print
c) Read Comment and Discuss
d) Change and Edit

These different Access permits should be encoded through different access codes attached to the relevant position, personal ID and pre-defined IP address.

7. **Classification-II:** After clearance from the Project Lead, the Inventory and Classification report will be submitted to the Steering Committee. The Steering Committee should review the proposed release of the Data Set and Classification Data set, request corrections if necessary, and finally approve publication of the Data.

8. **Publish** and repeat from step 5, once the Pilot Program has been completed. Repeat periodically or set up internal procedures allowing Data Stewards to update their inventory on a regular basis, and repeat the process for the publication of new or updated Data.

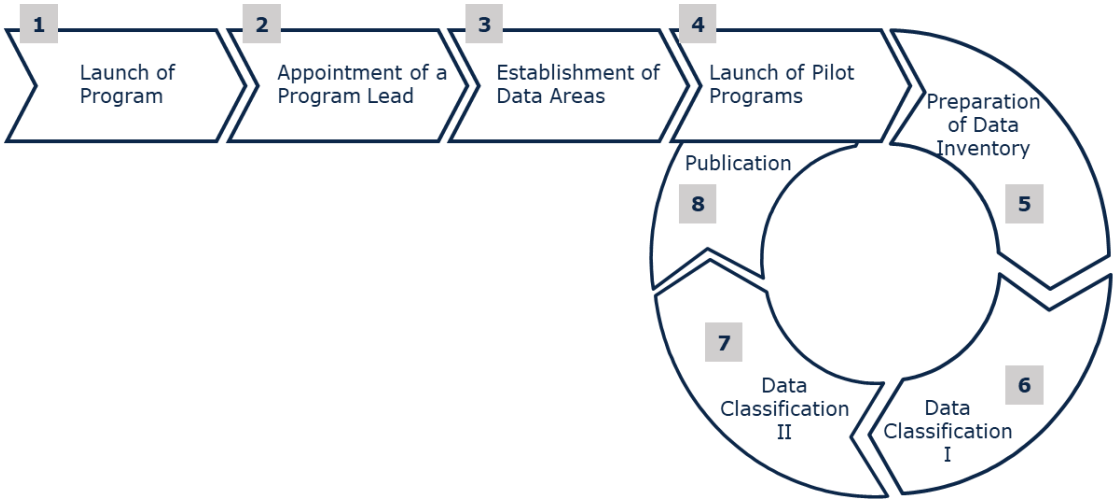

Exhibit 4: Data management flow chart

3.4.6 Technical Solutions

An effective Data Management Program should make optimal use of the available technical solutions and other constraints (e.g., budget or limited technical resources) faced by Government Entities generally.

The Government is committed to continuing to "*develop, upgrade and update its digital transformation infrastructure to ensure that it has the required capacity, availability, performance, reliability and security for effective use by all public sector entities*."[9] It also intends to "*use cloud services to expand Government-owned storage capacity and to benefit from the data management and application services available in the cloud*."[10]

In the case of electronic data, safety is inherently linked to the technology solutions used to enter, store, retrieve, transfer and process the Data concerned. The use of emerging technologies, such as the cloud, can address challenges, such as the absence of common IT systems and interfaces across the Jordanian administration today, address security challenges through broad (but user-controlled) network access and reduce costs, resource pooling, rapid elasticity and on-demand service.

[9] ICTP Policy 2018, paragraph 146.
[10] ICTP Policy 2018, paragraph 147.

Technical solutions applied as part of a Data Management Program should aim to address security threats, for example by:

- Meeting the Data Security needs of different classes of data;
- Ensuring that a proper system is in place for the proactive defence in depth, monitoring, logging and alerting against potentially alarming incidents events;
- Using advanced encryption over secured end-to-end optical fiber on all network links; and
- Minimizing the impact of stolen laptops and mobile devices of the personnel, by ensuring that such devices hold the minimum amount of information cached and following security protocols that remove any cached information from a device when it next logs on.

3.5. Timetable for Implementation

Implementation of this Data Classification Policy will rely on a series of interrelated activities, which can be grouped under four “blocks”: Governance Structure; Business Processes; Information/Data Access and Technology.

Responsibility for the implementation of the first block (Governance Structure) should lie primarily with the MoDEE and (once it is established) the Data Classification Department. Primary responsibility for the implementation of the second and third blocks should lie with each of the Government entities participating in the Policy, acting in coordination with the Data Classification Department.

Implementation of the fourth block (Technology) will require input from each participating Government entity but will greatly benefit from coordination with, and guidelines from, the Data Classification Department. This will be necessary to ensure optimized economies of scale and integration, and harmonized technical interfaces, common standards and procedures, and smooth data flow across all Government Entities participating in the Policy.

The Exhibit that follows provides an overview of the content of each of these blocks and an indicative timetable for their implementation, once the Data Classification Policy has been officially approved.

Block	Activities involved	Indicative Timetable
Governance Structure	▶ Establish Data Classification Department within the MoDEE ▶ Define roles & responsibilities ▶ Establish links and initial coordination with internal / external stakeholders	Two months from the Policy's approval
Business Processes	▶ Design business processes at the level of each participating Government authority ▶ Define Key Performance Indicators (KPIs) per stakeholder ▶ Establish and initiate ongoing communication between stakeholders	Start: 3 months from the Policy's approval Complete within 12 months from the Policy's approval
Information/Data Access	▶ Identify the available information at the level of each participating Government authority ▶ Define appropriate data management model	Start: 3 months from the Policy's approval Complete within 12 months from the Policy's approval
Technology	▶ Evaluate alternative technologies for Data Management and the Policy's implementation ▶ Determine most effective and efficient model(s) ▶ Leverage innovative products and solutions	Ongoing process, starting 3 months from the Policy's approval

Exhibit 5: Implementation Blocks and Timetable

Appendix I - Glossary of Terms Used

Name	Definition
Data	A broad term for any type of stored Information Assets.
(Data) Accessibility	The property of Data of being accessible at the right place, for the right uses and in a timely manner.
Data Area	A subset of Data that has been entrusted to a team including the Data Owner and Data Stewards. This team could include an entire department (e.g. Finance) or a single function such as Procurement.
(Data) Availability	The property of Data of being available and usable. Data may sometimes be available but not accessible, for example in the event of a temporary technical problem.
(Data) Classification	A process for the organization of Data of any kind into categories allowing their more efficient management and use.
Data Classification Roles and Responsibilities	A set of rules on the roles and responsibilities in relation to the classification of Data.
(Data) Confidentiality	A property that Data should not be made available or disclosed to unauthorized persons or entities.
Data Creator	Any person who accesses, inputs, amends, deletes, extracts and analyses Data for day-to-day purposes
Data Custodian	The person(s) having administrative and/or technical control over a Data Set, with responsibility for classifying data and providing guidelines for its lifecycle management. The Data Custodian will often exercise, through delegation, operational responsibility for part of the Data Owner's tasks.
Data Dictionary	A reference tool that provides a description and inventory of all core Data Elements. It is built from Metadata.

Name	Definition
Data Element	A single Data item. For example, an individual's surname is a Data Element.
(Data) Integrity	The reliability, accuracy and completeness of Data throughout the Data Life Cycle, through avoidance of any changes by accident or through a malicious or otherwise illegal act.
Data Label	An identifier for similar Data. (For example, a Data Label can be "Surnames", for the surnames of all individuals in a list.)
Data Life Cycle	The process for planning, creating, managing, storing, implementing, protecting, improving and disposing of Data.
Data Management	All aspects of managing Data as a valuable resource.
DO	Data Owner
Data Owner(s)	The person(s) with the authority and responsibility, under legislation, regulation or policy, for the collection, Classification, Integrity and Security of a Data Set either directly or through delegation by the person or entity that ultimately owns the Data – i.e., the State in the case of Government Data.
Data Quality	The overall utility of a Data Set as a function of its ability to be easily processed and analyzed for other uses.
(Data) Security	The preservation of Data Confidentiality, Data Integrity and Data Availability and possibly additional properties such as access control, authentication, incident detection, reporting and solutions, change management and version control.
Data Set	A group of Data Elements, *e.g.*, historical weather data.
Data Steward	The person(s) responsible for ensuring Data Integrity and Data Quality, and the implementation of Data Classification within its area of responsibility

Name	Definition
Government Entity	Any ministry, department, agency, municipality, district, or educational, financial, non-profit, corporate and regulatory institution or other instrumentality or entity that is created and empowered by the constitution or laws of, and under the administration of Jordan.
Information Asset	Any collection of Data containing knowledge and information, regardless of Data Classification and recognized as having at least a potential value.
Metadata	Metadata are Data about the Data. They contain a descriptor of each Data Set and Data Labels, for purposes of discovery and identification. Metadata are used to catalogue the Data and to enable software and operational systems to assess the Data. Data Stewards add interpretive information to the Metadata so that the meaning of each Data Label is clear and can be used consistently across all systems. Data Dictionaries are built from the Metadata.
Non-Government Entity, Private Entity	Private entities, such as corporations, foundations, organisations or citizens. They are not subject to this Policy.
OGD Policy	The Government's Open Data Policy
Open Government Data, OGD	Data produced by the government and made available for all bodies, which are subject to disclosure under the Law of Right to Access to Information No. 47/2007, and Personal Data Protection Law.
OGP	Open Government Partnership
Open Data	Data that can be freely accessed, used, re-used, and re-distributed by anyone, anywhere, and for any purpose, which are made available online in open format, with no legal encumbrances and do not contain sensitive / protected information in accordance with the law. The use terms for Open Data can be defined by a Data licence, which in some cases may include restrictions on their commercial use.
Personal Identifiable Information, PII	Any Data that can be used to identify a specific individual and can thus potentially cause harm to that individual, if disclosed, as a breach of privacy.

Name	Definition
PL	Program Lead
SC	Steering Committee

Exhibit 6: Glossary of Terms

Appendix II – Data Management Models

II.1.Subject-Based Data Management Model

The subject-based Data Management model assigns Data Stewards for generalized subjects such as "stakeholders", "services" or "financials" which allows the Data Steward to focus on Data that touch upon its domain. In complex or very large environments, there can be more than one Data Steward for each subject area.

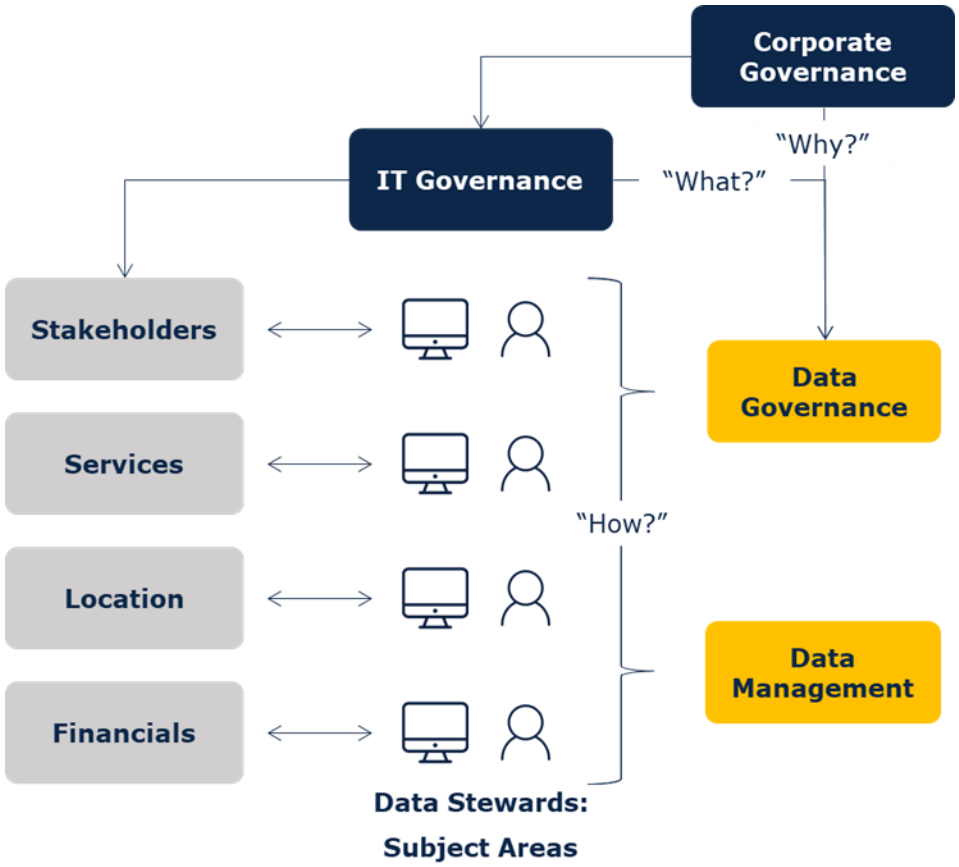

Exhibit 7: Subject based data management model

Benefits of the subject-based Data Management model are as follows:

- Data ownership boundaries are usually clear, which reduces the complexity of the Data Management processes.
- The Data Steward's knowledge of the accompanying business rules and usage environments for his/her Data subject area are likely to increase over time.

II.2.Function-Based Data Management Model

The function-based Data Management model focuses on a given line of business to undertake the Data Steward responsibilities. Each business line is responsible for managing the Data in their work domain.

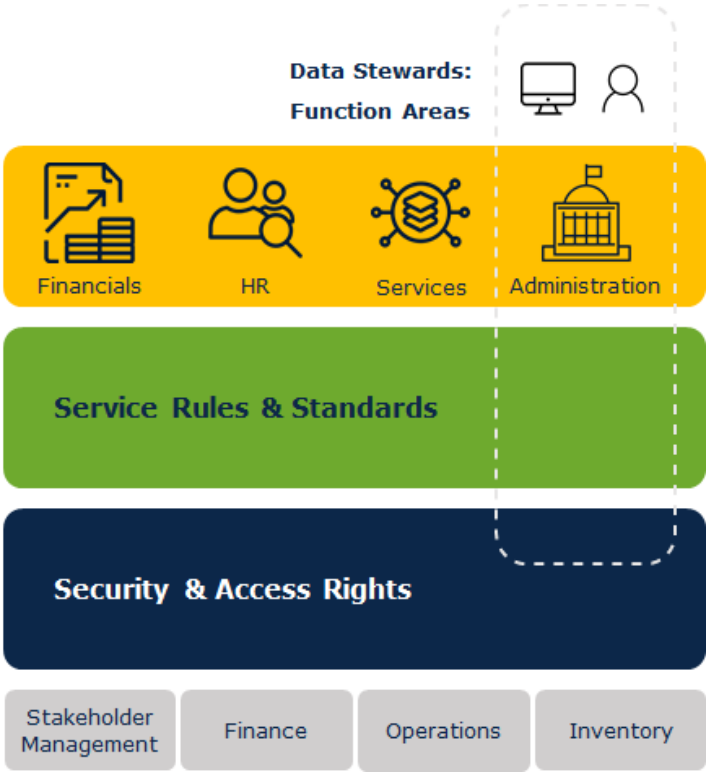

Exhibit 8: Function based data management model

Benefits of the function-based Data Management model are as follows:

- Scope of the Data is bounded by the business line, which makes it easier for the Data Steward to establish definitions and rules and mitigates the need for complex workflow.
- Functional Data Stewards that are naturally affiliated with business objectives of their departments, can achieve increased efficiency of Data Classification with an overall view of the business line rather than specific tasks.

II.3.Process-Based Data Management Model

The process-based Data Management model assigns Data Stewardship responsibility to discrete business processes. In this case, Data Stewards may be responsible for multiple Data domains or application/systems that participate in a given business process.

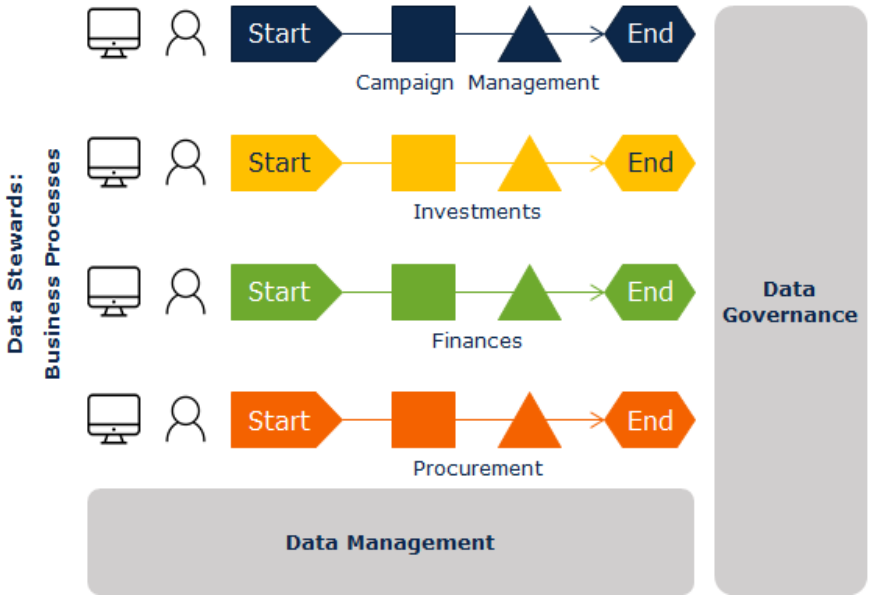

Exhibit 9: Process based data management model

The benefits of the process-based Data Management model are as follows:

- Organizations become comfortable circumscribing their business processes. Data stewardship is therefore seen as a natural extension of process definition.
- Success measurement is easier given that measuring Data Quality or Availability in the context of the business process that consumes the Data is a reliable and easy-to-explain benefit of Data Stewardship.
- Once a company launches Data Stewardship for business processes, it is easy to justify additional Data Stewards for other processes. The process-oriented model is a very effective way to entrench Data Stewardship.

Appendix III – Examples of Data Classification

Hypothetical classification examples of specific and real Data instances are provided below:

III.1. Straightforward Examples of Data Classification

Data	In the Custody of, or Entrusted to Jordan	Illegal under Law 50	Illegal under Other Laws	Confiden-tial to Private Entity	PII[11]	Involves Public Benefit	Already Public Realm	Classification
Personal Interaction on Social Media	no	--	--	--	--	--	--	*Outside the Scope of the Policy*
Details of intelligence officers	yes	yes	--	--	--	--	--	*Secret*
Undisclosed locations of military units	yes	yes	--	--	--	--	--	*Secret*
Health records of individuals	yes	no	yes	--	--	--	--	*Confidential & Shared or Sensitive*
Personal finances, tax-related matters and debts	yes	no	no	yes	yes	no	--	*Confidential & Shared*
Historic Meteorological Data	yes	no	no	no	no	yes	yes	*Public*
Statistical Economic Data	yes	no	no	no	no	yes	yes	*Public*
River Water Quality Monitoring	yes	no	no	no	no	yes	no	*Public*

[11] PII =Personal Identifiable Information, i.e., any Data that can be used to identify a specific individual and can thus potentially cause harm to that individual, if disclosed, as a breach of privacy.

Data	In the Custody of, or Entrusted to Jordan	Illegal under Law 50	Illegal under Other Laws	Confiden-tial to Private Entity	PII[11]	Involves Public Benefit	Already Public Realm	Classification
University Academic Personnel Name, Dept, Specialty	yes	no	no	no	no	yes	no	*Public*
University Academic Personnel Home Address	yes	no	no	no	yes	no	no	*Confidential & Shared*
Customer list of corporations	no	--	--	--	--	--	--	*Outside the scope of the Policy*
Criminal records of individuals	yes	no	?	yes	yes	no	no	*Confidential & Shared*
Financial details of Start-ups which are stored in MoDEE	yes	no	no	yes	no	no	no	*Confidential & Shareable or Public*
List of patient names in private hospitals	yes	no	yes	yes	yes	no	no	*Confidential & Shareable*
Balance sheet of company, where Hashemite Kingdom of Jordan is majority shareholder	yes	no	no	--	--	yes	yes / no	*Public*
Balance sheet of a exchange listed, private company	yes	no	no	--	--	yes	yes / no	*Public*
Procurements details of MoDEE	yes	no	no	yes	no	yes	no	*Public*
Investment criteria of MoDEE for Entrepreneurship	yes	no	no	no	no	yes	no	*Public*

Exhibit 10: Straightforward data classification examples

III.2. Potentially Controversial Examples of Data Classification

Data	In the Custody of, or Entrusted to Jordan	Illegal under Law 50	Illegal under Other Laws	Confidential to Private Entity	PII	Involves Public Benefit	Already Public Realm	Classification
University Academic Personnel e-mail Address	yes	no	no	maybe	no	maybe	no	*Public (or possibly Confidential & Shared)*
Cell Phone Tower Locations	yes	no	no	maybe	no	yes	no	*Public (or possibly Confidential & Shared)*
Private Bank Capitalization Ratio, as reported to Central Bank	yes	no	no	maybe	no	yes	no	*Public (or possibly Confidential & Shared)*
Contract details of private companies rewarded with new contracts	yes	no	no	yes	no	yes	no	*Public (or possibly Confidential & Shared)*
Government's planned budget to invest in another country	yes	no	no	yes	no	maybe	no	*Public (or possibly Confidential & Shared)*
Financial details of municipalities	yes	no	no	yes	no	yes	no	*Public (or possibly Confidential & Shared)*
MoDEE strategic target documents	yes	no	no	yes	no	maybe	no	*Public (or possibly Confidential & Shared)*
Schedule of Ministry meetings with other countries	yes	no	no	yes	no	maybe	no	*Public (or possibly Confidential & Shared)*
Financial Reports of MoDEE	yes	no	no	yes	no	yes	no	*Public (or possibly Confidential & Shared)*
Location & details of sewerage treatment and discharge	yes	no	no	yes	no	yes	no	*Public (or possibly Confidential & Shared)*

Sales of treasury public properties details	yes	no	no	yes	no	yes	no	*Public (or possibly Confidential & Shared)*

Exhibit 11: Controversial data classification examples

Appendix IV Jordan Open Government Data Licence

Jordan Open Government Data License - Issue v1.0

This license was issued pursuant to the provisions of Article (8) Item No. (5) of the "Instructions for the Publication of Open Government Data on the Open Government Data Platform for 2019" issued in the Official Gazette No. 5561 (pages 660-663), in implementation of the Government Data Policy Approved by the Council of Ministers in 2017.
In accordance with this license, the government entity in possession of open data and publishing it on the open government data platform grants permission to the beneficiary to use this data under the conditions stated herein.

First: Definitions

The words and expressions in this license shall have the meanings assigned to them below unless the context indicates otherwise:
Entity: Any ministry, department, public official institution, public institution, body, council, authority or company wholly owned by the Government or to which the Government contributes at least 50%, and any entity that the Council of Ministers decides to make subject to the provisions of this license.
Open Data: Data that are freely accessible, used, reused or redistributed by any person, anywhere and for any purpose, and available through the Internet in an open format without legal or technical barriers, and does not contain data protected by the legislation in force.
Open government data: Open data issued by the Entity and available to all, subject to disclosure under the relevant legislation in force.
Beneficiary: The natural or legal person benefiting from open government data.

Second: Uses

1. Use of open government data by the Beneficiary should comply with all terms and conditions contained in this License.
2. This license is non-exclusive and non-assignable. Accordingly, the beneficiary has the right to continue using any open government data used under this license, under the conditions contained in the license at the time, even if those data later obtain another license.

Third: The rights
The beneficiary shall be entitled, free of charge, to the following:
1. Use open government data.

2. Copy, publish, distribute, transmit, process and make available to third parties open government data.
3. Develop new derivatives of open government data by combining them with other data or using them in a product or service.

Fourth: Obligations

The beneficiary should attribute the open government data to the publisher(s) using the following statement:
("Publishers Name", "Address (s)", "Publish Date", "Download Date", "Platform Website").

1. Non-endorsement: This license does not grant permission to the beneficiary to use open government data in any way that indicates an official status or the support of the publisher of the beneficiary.
2. Cancellation: If the Beneficiary violates any of the terms or conditions set forth in this License, the License and all rights granted under it shall be deemed void automatically.
3. DISCLAIMER: Despite the accuracy of the inventory, classification and dissemination of open government data, the publisher of such data shall not be liable for any unintentional errors or shortcomings contained in its data and consequently disclaims any liability for direct or indirect damages of any kinda result of this degradation / degradation or shortage.
4. Dispute resolution: Any dispute arising out of or due to or relating to this license or breach of any of its terms and conditions shall be dealt with in accordance with the Jordanian laws and regulations in force.
5. Compliance with International Licenses: The Jordan Open Government Data License is compatible with the license of CREATIVE COMMONS (CC-BV) version 3.
6. Language used: This license was written in Arabic, and if the license is in a language other than Arabic and there is disagreement on interpretation or interpretation, the text in Arabic shall prevail.

Appendix V Relevant Legal and Policy Framework

- Protection of State Secrets and Documents Law No. (50) of 1971.
- Right to Access to Information Law No. (47) of 2007
- Telecommunications Law and its Amendments No. (13) of 1995.
- Electronic Transactions Law No. (15) of 2015.
- Electronic Crimes Law No. (27) of 2015.
- Personal Data Protection Law – Draft
- General Policy for the Information & Communications Technology and Postal Sectors, 2018 (ICTP Policy 2018)
- Cyber security Law No. (16) of 2019
- General Policy for the ICT and Postal Sectors 2018