نـتـقـدم بثـقـة
Moving Forward
with Confidence

رؤية عُمان 2040
OmanVision

سلطنة عُمان
وزارة النقل والاتصالات وتقنية المعلومات
Sultanate of Oman
Ministry of Transport, Communications and
Information Technology

National Data Governance and Management Policies

Document Control

Version	First
Date	2024
Author	Ministry of Transport, Communications and Information Technology

Issuance and Publication

Issuing authority	General Directorate of Polices and Governance
Email	governance@mtcit.gov.om
Date of Issuance	2024

Distribution list

1	All units of the State's Administrative Apparatus.
2	Regulatory bodies for various sectors

Table of Contents

1.0 Terms and Definitions

Terms	Definitions
Analytics Business Case	The analytics business case outlines the rationale for a sponsor to invest in an analytics initiative. It defines the problem that the initiative aims to address or the opportunity that it aims to realize, identifies potential risks that could hinder the initiative's success, outlines the financial implications of implementation, and provides an estimate of when the investment is expected to yield results or value.
Business Glossary	A Business Glossary is the agreed-upon definitions of business terms, and it relates these to data. The purpose of a business glossary is to document and store an entity's business concepts, terminology, definitions, and the relationships between the terms.
Business Impact Level	An indicator of the degree of potential harm or negative consequences to the Sultanate, an entity or an individual resulting from unauthorized access or disclosure as determined through the data classification impact assessment.
Certified Data Element	Certified data element refers to a data element that has undergone a formal review process and has been verified for accuracy, quality, and compliance with entity standards and policies by an authoritative role within the entity.
Coexistence Architecture Pattern	Master data will be migrated into a central hub and is also updated back within the source systems.
Consolidation Architecture Pattern	Master data will be migrated into a central hub from the source systems. It will be consolidated, cleansed, and integrated to create a golden record, that can then be consumed by the target systems. Any updates made to the master data within the hub are not automatically applied to the source systems.
Controlling Entity	The entity that determines the purpose and manner of processing personal data, whether the data is processed by it or by the processing unit.
Critical Data Element	Critical data elements (CDEs) are essential data for an entity's operations or decision-making. Their accuracy, completeness, and timeliness are crucial for entity's success. Effectively managing CDEs improves data quality, reduces errors, and facilitates informed decision-making. Examples include PII (Personal Identifiable Information), Customer data, employee identification number, financial transaction amount etc.
DAMA	Data Management Association (DAMA) is a non-profit, vendor independent, global association that aims to advance the data management profession. DAMA provides a forum for data management professionals to exchange ideas, best practices, and experiences related to the management and governance of data assets within organizations. DAMA International is known for its publication of the Data Management Body of Knowledge (DMBoK), a comprehensive compilation of fundamental principles, methodologies, and ideas essential for data governance and management.
Data Archival	Data archival is the method of securely storing inactive data for compliance, historical reference, or other purposes in secondary or long-term storage solutions.
Data Availability Requirements	The timeliness in terms of frequency of updates at which the data is required to be available to the users. (E.g., real-time, near real time, batch etc.)
Data Classification Register	A data classification register is a centralized record that documents the classification of different types of data within an organization. It serves as a repository for information about the sensitivity, importance, and handling requirements of various data assets.
Data Dictionary	The data dictionary is the collection of metadata providing information needed to use the data (e.g., data types, details of structure, security restrictions)

Data Disposal	Data Disposal refers to removal of the data asset from all places of active storage within the entity. The scientific destruction of documents and information must be carried out on all copies whose final fate has been approved for destruction, ensuring the destruction process guarantees that the data cannot be recovered as per the standards of the Documents and Archives Authority.
Data Governance	Data Governance is the exercise of oversight and control over an entity's data assets for their effective management, thus enabling realization of the entity's strategic business objectives.
Data Governance and Management Office	A Data Governance and Management Office is a centralized unit within an entity responsible for overseeing and implementing data governance initiatives. It manages policies, processes, and standards related to data management, ensuring that data is accurate, consistent, secure, and compliant with regulations and entity's goals.
Data Governance Committee	Data Governance Committee is a group within an entity that is responsible for overseeing and guiding data governance initiatives. It typically comprises of representatives from various departments and functions who collaborate to establish data policies, standards, and processes, along with ensuring compliance with data regulations. The committee is tasked with making decisions regarding data management, resolving data-related issues, and promoting a data-driven culture throughout the entity.
Data Lakehouse	A hybrid data platform that aims to combine the capabilities of a data lake and a data warehouse.
Data Lineage	Data lineage is the systematic tracking of data movement over time, providing visibility into its source, evolution, and destination within the data processing pipeline.
Data Management	Data Management is the development, execution, and supervision of plans, policies, programs, and practices that deliver, control, protect, and enhance the value of data and data assets throughout their lifecycle.
Data Model	Data model is a structured representation of how data is organized, stored, and accessed within a database or information system, defining entities, attributes, and relationships. It serves as a blueprint for database design and development, ensuring data consistency and facilitating communication among stakeholders.
Data Monetization	Data monetization refers to extracting economic value or generating revenue from an entity's data assets. This includes both direct approaches, such as the sale of data products and datasets for revenue generation, as well as indirect methods aimed at optimizing costs through the enhancement of operational efficiencies.
Data Platform	Data platform is a centralized technology infrastructure that facilitates the ingestion, storage, processing, analysis, and management of large volumes of data from diverse sources.
Data Products	Data products are valuable assets that can be monetized through various means, including direct sales, licensing, subscriptions, or partnerships. Additionally, these products are typically designed to fulfill specific needs, solve operational issues, or support decision-making processes (e.g., conversational chatbot systems, predictive models, personalized recommendation systems etc.)
Data Profiling	Data Profiling is a form of data analysis used to inspect data and assess quality. Data profiling uses statistical techniques to discover the true structure, content, and quality of a collection of data. Results of data profiling can be used to identify opportunities to improve the quality of both data and metadata.
Data Quality Index	Data Quality Index provides a comprehensive overview of the data quality scores across entity specific dimensions over a period. The purpose of a Data Quality Index is to help organizations understand the overall health and reliability of their data assets.
Data Retention	Data retention is a practice that focuses on what information to be retained or archived, where it should be kept, and how long it should be kept.
Data Sharing Agreement	Data sharing agreement is a formal contract or agreement between parties that outlines the terms, conditions, and responsibilities related to the sharing of data. It specifies the types of data to be shared, the purpose of the sharing arrangement, the methods of data transfer and storage, data security measures, limitations on data usage, and processes for handling sensitive or confidential information.

Data Storage	Data Storage refers to the physical or logical procedures used to store, retrieve, and manage data in a structured manner.
Data Subject	The natural person who can be identified through their personal data.
DCAM	Data Capability Assessment Model (DCAM) published by EDM council is a structured resource that defines and describes the capabilities needed to establish and sustain a successful data management initiative in any organization. It outlines capabilities across 8 components of data governance and management to assess maturity of an organization using a well-defined maturity model.
Declassification	Removal of a previously applied data classification label from a data asset, thus making it unclassified. This is done when the risks of damage posed by the loss, misuse and unauthorized disclosure of the contents of the data asset no longer exists due to changed circumstances.
Downgrade of data classification	Application of a new data classification label that is lower than the previously applied data classification label.
Environments	Isolated instances of an application that facilitate the purposes of different stages of a software development lifecycle. (E.g., Development, Testing/QA, UAT and Production)
Impact Assessment	Impact assessment is the process of evaluating the potential effects or negative consequences to the sultanate, an entity or individual from unauthorized access or disclosure of the data elements. Based on this assessment, the data elements are assigned with classification labels corresponding to their Business Impact Levels
KPI (Key Performance Indicator)	A key performance indicator (KPI) is a metric used to assess the effectiveness of an entity or a specific task. KPIs focuses on the most critical areas, offers a foundation for strategic and operational enhancements, and establishes an analytical basis for making decisions.
Master Data	Data that provides context for business activities. It includes the details of the data objects involved in business transactions such as customers, products, employees, vendors, citizens etc.
Open Data	Open data is a specific kind of public data that is not only accessible to the public but also free to use, modify and distribute with minimal or no restrictions. It is usually provided in a machine-readable format (like CSV, JSON, XML) under an open license that allows for widespread use and distribution, only requiring acknowledging the original source. Examples include, datasets released under open licenses, government transparency initiatives etc.
Originating entity	For a particular data asset, the entity that has the authority to decide on its data classification as the producer of the data asset.
Ownership	Ownership refers to the legal or formal rights and responsibilities associated with possessing data. Ownership involves accountability for the data's accuracy, security, and appropriate use within an entity.
Payback Period	The period for an investment to generate its initial cost through produced income or cost savings. Payback period is often used as a simple measure to assess the risk and profitability of an investment.
Policy	Policy is a set of principles or rules established by an entity to govern decision-making, actions, and behaviors within a specific context or domain.
Process	Within the context of data management and governance, processes are series of activities that needs to be performed to manage the data across the entire data lifecycle.

Processing unit	The entity that processes personal data for the benefit of and on behalf of the controller.
Public Data	Public data refers to the information that is available on request, often through government websites or public records. However, it may have some limitations regarding its use and distribution. For instance, public data might be accessible for viewing but not for commercial use without permission. Examples include, census data, public health statistics, budget reports and financial statements of public institutions.
Reference Data	Data that is used solely to relate data in a database to information beyond the boundaries of an entity. For e.g., country codes, ISD codes, state codes etc.
Registry Architecture Pattern	Master data elements from source systems will not be brought into the hub. The hub will hold the minimum amount of information required to uniquely identify a master data record. Master data resides in sources and the hub uses cross-reference for linkage.
Return on Investment (ROI)	Return on investment is a financial metric to calculate the profitability or effectiveness of an investment compared to its cost. It measures the return generated from an investment compared to the initial investment cost.
Root Cause Analysis	Root cause analysis is a process of understanding factors that contribute to problems and the ways they contribute. Its purpose is to identify underlying conditions that, if eliminated, would effectively remediate the issue, and prevent its recurrence.
Secure Sharing Media	Any medium or channel for data sharing that is secure and approved for exchanging data among the government entities to ensure its protection. (E.g., The government integration channel, Unified Government Portal etc.)
Security Controls	As per National Institute of Standards and Technology (NIST), security controls are the safeguards or countermeasures prescribed for an information system or an entity designed to protect the confidentiality, integrity and availability of its information and meet a set of defined security requirements. (E.g., Encryption, Masking etc.)
Self Service Reporting	Capability of a data platform where end users can independently generate, customize, and access reports or insights from a company's data without the direct involvement of IT or data analysts.
Service Level Agreement	Service Level Agreements (SLAs) are formal agreements between two parties. These agreements outline the specific levels of service that the provider is committed to delivering, including quality, responsiveness, availability, and other performance metrics. SLAs also typically define the responsibilities and expectations of both parties, along with processes for monitoring, reporting, and addressing service-related issues or discrepancies.
Stewardship	Stewardship refers to the responsible management and oversight of data. Data stewardship involves the proactive care and management of data assets to ensure their quality, integrity, and usability.
Supplementary Markers	The optional markers (caveats and dissemination limiting markers) applied on top of the primary data classification labels to further restrict the dissemination of data to a segment of the intended audience.
Target Systems	A system that utilizes data from an upstream system that is responsible for its production is referred to as a target system for the upstream system.
Third Party	An entity that works under the supervision of the control unit or processing unit and is authorized to process data for the account of the control unit or processing unit, and whose headquarters are in the Sultanate of Oman.
Users	Any individual or an entity that consumes data is termed as a user.

2.0

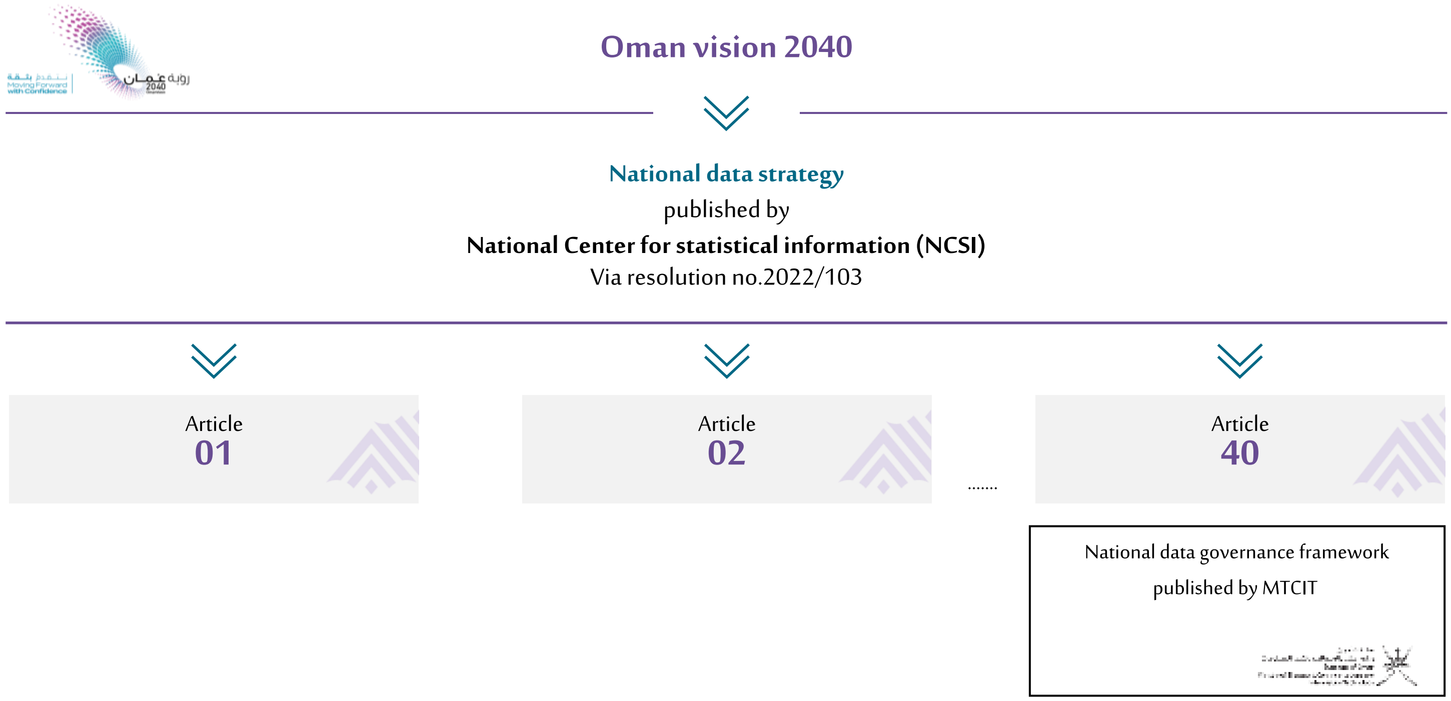
Introduction

2.0 Introduction

The Sultanate of Oman, aligning to the objectives of 'Vision 2040', has planned several strategic digital transformation programs for driving economic growth, innovation, and public welfare.

As a significant step in this direction, the 'National Data Strategy' was published by the National Center for Statistical Information (NCSI) via the Royal Decree no. 2022/103. Article (40) of the 'National Data Strategy' entrusts the Ministry of Transport, Communications, and Information Te chnology (MTCIT) with the following responsibilities:

- 'Preparing policies and standards for data management and governance and following up on the commitment of units of the state's administrative apparatus and other public legal persons to these policies.'
- 'Preparing the necessary guidelines and guides to support the application of policies and standards.'
- 'Preparing and presenting awareness workshops for units of the state's administrative apparatus and other public legal persons.'
- 'Adopting initiatives based on technical data and coordination between beneficiaries from the government and private sectors.'
- 'Preparing and supervising the implementation of open data programs.'



Oman vision 2040

National data strategy
published by
National Center for statistical information (NCSI)
Via resolution no.2022/103

Article 01

Article 02

....

Article 40

National data governance framework published by MTCIT

Figure-1: Development of the National Data Governance Framework

The framework consists of 3 components providing the necessary requirements for data governance and management across 14 domains. Together, the 3 components will ensure the establishment of a robust data governance and management practices across the government entities within the Sultanate of Oman. A brief description of the 3 components is provided below:

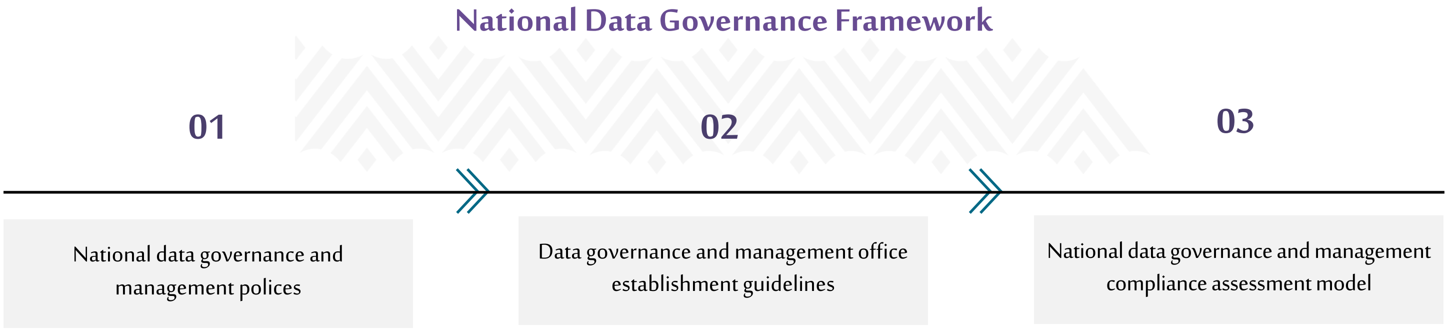
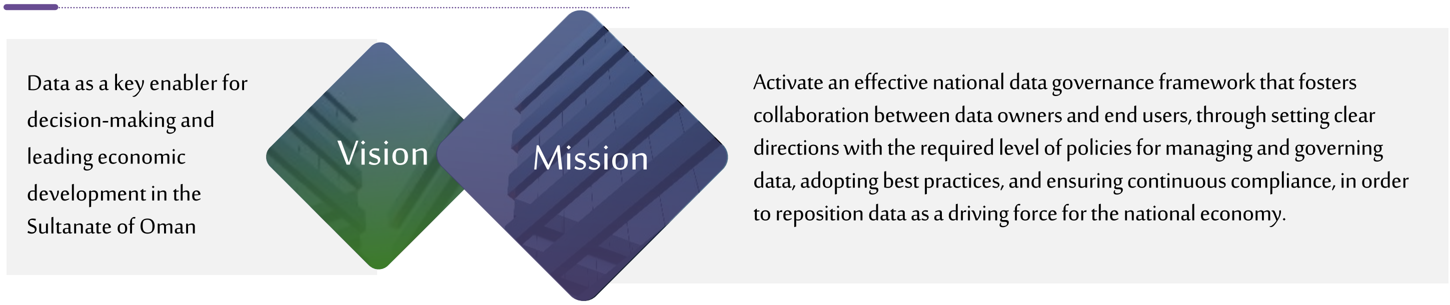

National Data Governance Framework
01
02
03
National data governance and management polices
Data governance and management office establishment guidelines
National data governance and management compliance assessment model

Figure-2: National Data Governance Framework Ecosystem

- **National Data Governance and Management Policies** – The policies outline the necessary requirements across 13 out of the 14 data governance and management domains to establish a robust data governance practice within the government entities. The Document and Content Management domain will be covered by the existing policies/laws developed in the sultanate. For further details, please refer **Appendix 1- Document and Content Management related policies.**
- **Data Governance and Management Office Establishment Guidelines** – The guidelines provide the necessary elements to support the government entities for establishing their Data Governance and Management Office including the mandate, services and processes, organization structure, roles, and responsibilities, positioning within the entity and governance model.
- **National Data Governance and Management Compliance Assessment Model** - The model outlines the compliance assessment methodology, the implementation priorities, and the assessment criteria for enabling the government entities to comply with the national data governance and management policies.

2.1 National Data Governance Vision and Mission



Data as a key enabler for decision-making and leading economic development in the Sultanate of Oman

Activate an effective national data governance framework that fosters collaboration between data owners and end users, through setting clear directions with the required level of policies for managing and governing data, adopting best practices, and ensuring continuous compliance, in order to reposition data as a driving force for the national economy.

Figure-3: National Data Governance Vision and Mission

2.2 Scope and Applicability

The scope of the National Data Governance and Management Policies covers 14 domains out of which policies for 13 domains are outlined in this document. The policies for the Document and Content Management domain are covered in the existing domain specific policies/laws. Please refer the **Appendix 1- Document and Content Management related policies** for further details. The policies are applicable to all the government entities of the Sultanate of Oman. For the private sector entities, the policies shall be enforced through the concerned sector regulators.

This document should be read in conjunction with the Data Governance and Management Office Establishment Guidelines and National Data Governance and Management Compliance Assessment Model for a comprehensive view of the National Data Governance Framework requirements.

2.3 Guiding Principles

Data is a national asset
Develop practices that enable realization of the inherent value of data as a national asset to drive innovation and unlock economic growth through data integrity, monetization, transparency and accountability.
01

A data-driven culture is encouraged
Establish processes and develop skills required for entities to utilize their data, derive meaningful insights and leverage technology to improve their decision making and operational efficiency.
02

Data is shared and is available on time
Develop practices to facilitate seamless internal and external sharing of data, ensuring that data users obtain information in a timely manner, thereby improving the quality and efficiency of decision-making processes.
03

Data is trusted by all stakeholders
Establish practices for providing reliable, accurate and fit for purpose data to build data trust and confidence thereby, facilitating informed decision making.
04

Data is understood uniformly across all stakeholders
Establish practices that enable a uniform understanding of the data to facilitate efficient data exchange and analysis thereby promoting reliability and efficiency in utilizing data assets within the entity.
05

Data practices are compliant with regulatory requirements
Develop data governance and management practices that uphold the regulatory requirements to ensure lawful, ethical and responsible handling of data across the business processes of the entities.
06

Data is managed across its lifecycle as per business needs
Develop practices that help collect, store, dispose/archive data as per its relevance and purpose along with delivering it to the data consumers.
07

Figure-4: National Data Governance Guiding Principles

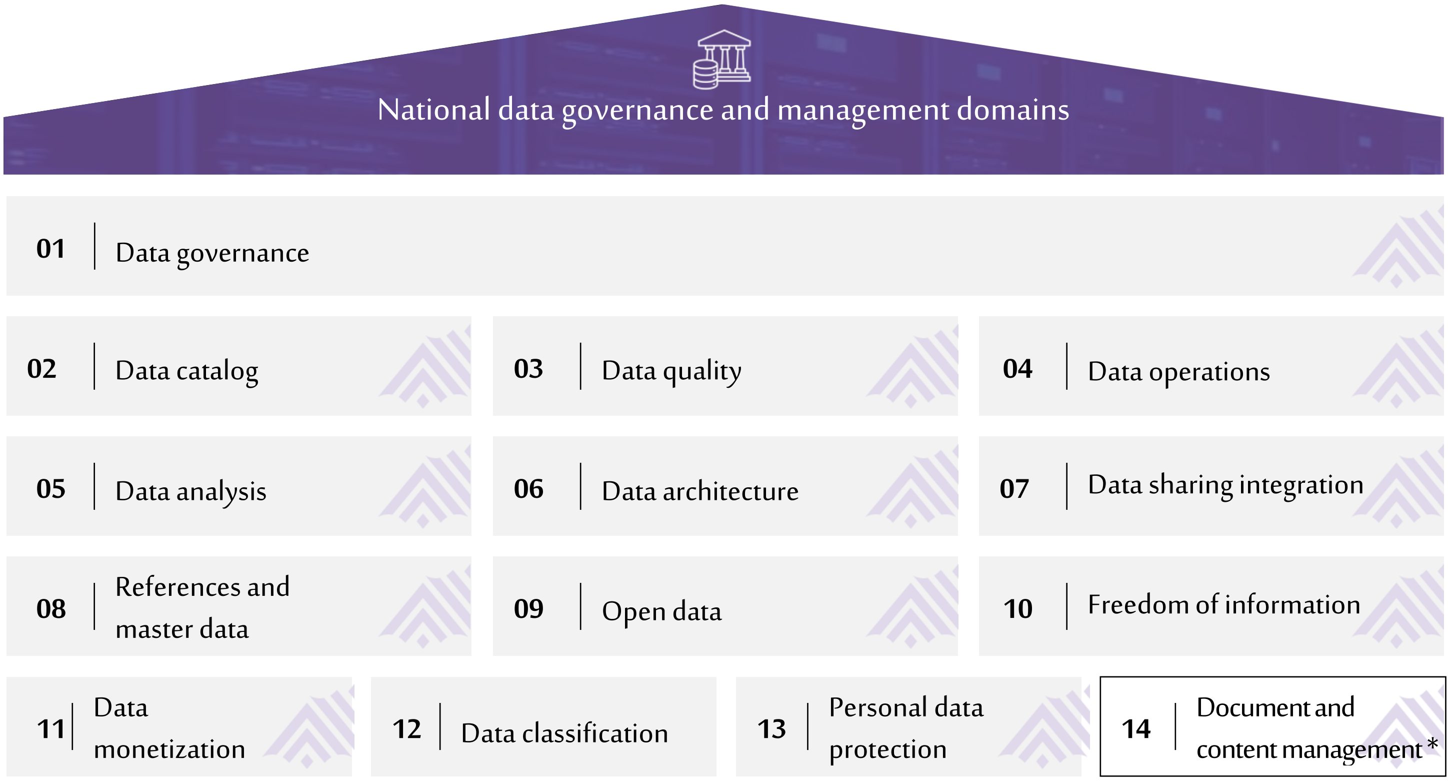
3.0

Data Governance and Management Framework Overview

3.0 Data Governance and Management Framework Overview

3.1 Data Governance and Management Domains

The domains of the National Data Governance Framework are aimed at establishing standardized methodologies for working with data across the government entities and enabling them to realize the Sultanate's ambition of economic development by leveraging data. The framework consists of 14 domains (Document and Content Management domain will be governed by the existing laws/policies outside this document) which collectively outline the capabilities required for the government entities to govern and manage their data. This framework is based on international leading practices such as DAMA, DCAM etc. and tailored for the Sultanate.



National data governance and management domains

01 Data governance

02 Data catalog

03 Data quality

04 Data operations

05 Data analysis

06 Data architecture

07 Data sharing integration

08 References and master data

09 Open data

10 Freedom of information

11 Data monetization

12 Data classification

13 Personal data protection

14 Document and content management *

* Document and content management domain will be covered by the existing domain specific/lows

Figure-5: National Data Governance Framework Domains

- **Data Governance:** The exercise of oversight and control over an entity's data assets for their effective management, thus enabling realization of the entity's strategic business objectives.
- **Data Catalog:** Emphasizes on activities required in the entity for generating, maintaining, and adding information about the entity's data to its catalog. It facilitates an effective access to high quality metadata through usage of a data catalog tool that acts as the common point of reference to the entity's metadata.
- **Data Quality:** Pertains to the implementation of practices aimed at guaranteeing the availability of quality data that satisfies the intended purpose and requirements of the data users. Enhanced data quality cultivates trust among stakeholders for data driven decision making.
- **Data Operations:** Focuses on practices for efficient handling of data across its lifecycle including data creation/acquisition, storage, retention, disposal and archival. Additionally, it also includes practices that ensure business continuity including backup and recovery along with disaster recovery.
- **Data Analytics:** Involves implementation of activities and technologies required for transforming entity's raw data records into meaningful and actionable insights to support business decision-making. It results in improved decision-making and enhanced efficiency and productivity.
- **Data Architecture:** Focuses on practices required for data modeling (conceptual, logical, and physical) along with facilitating effective data solutions to enable efficient data management, analysis, and decision-making aligning to the entity's strategic needs.

- **Data Sharing and Integration:** Focuses on implementation of practices that ensure seamless movement of data within and between entities by establishing integration methods and defining standard agreements for data sharing.
- **Reference and Master Data:** Emphasizes on implementation of practices to define and manage the entity's core data shared across its systems and the standard data that originates outside the entity with an aim to provide a single point of authoritative source for the core data elements. Thus, it reduces the risk of data redundancy and provides an authoritative source of data within the entity.
- **Open Data:** Involves establishing practices that make public data held by an entity open for the general public's access, use and sharing enabling building of a knowledge society and accelerating economic growth of the country.
- **Freedom of Information:** Fosters transparency by empowering the public with a mechanism to request and access data held by government entities along with an issue and grievance mechanism to settle disputes.
- **Data Monetization**: Focuses on effectively utilizing and leveraging entity's data assets for generating revenue or optimizing operational cost. It involves analyzing entity's data to create value, which can then be used to generate tangible outcomes through various means such as selling insights, offering data-related services, or enhancing operational efficiency.
- **Data Classification:** Focuses on categorization of data to enable a rigorous and consistent business classification scheme and process that ensures data assets are appropriately accessed and processed.
- **Document and Content Management:** Focuses on maintaining the integrity and enabling access to documents, records, and content stored across the entity. **The policies of this domain are outlined by NRAA within the "Documents and Archives Law".**
- **Personal Data Protection:** Focuses on safeguarding an individual's rights to how their personal data is collected, processed, stored, and destroyed.

3.2 Domain Mapping to the Data Lifecycle Management Phases

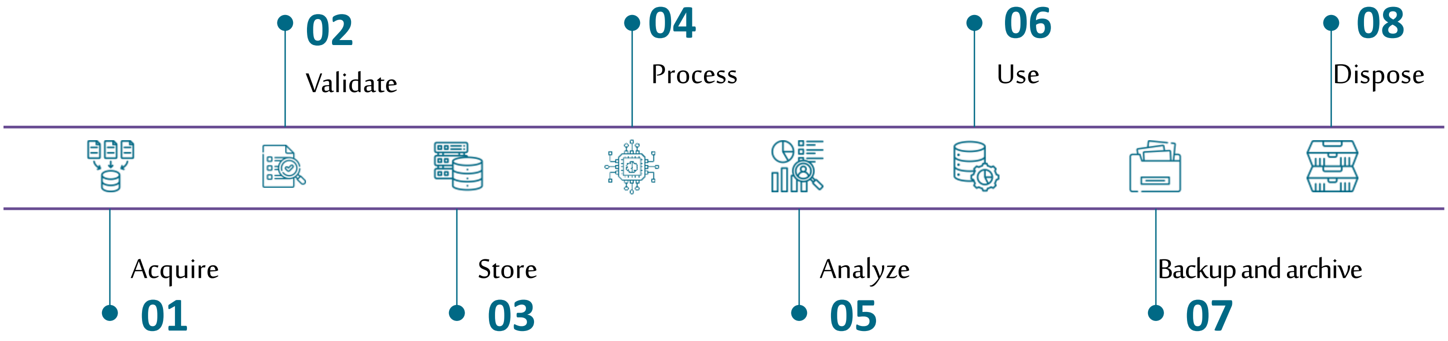


Figure-6: Data Lifecycle Management Phases

- **Acquire** – This phase involves gathering data from various data sources including user inputs, system-generated data, and third-party repositories. This crucial phase involves not only gathering data but also ensuring its reliability, relevance, and compatibility with the intended analysis or application.

  The phase is covered by the following domains:

  - Data Governance
  - Data Operations.
  - Data Sharing and Integration.
- **Validate** – This phase is a critical step that ensures the accuracy, integrity, and quality of the data being acquired. It involves verifying that the collected data meets specific criteria or standards, such as completeness and consistency to predefined formats or rules. Validation helps to identify and correct errors, anomalies, or discrepancies in the data early in the lifecycle, thus preventing downstream issues and ensuring the reliability of subsequent analyses or applications.

  The phase is covered by the following domains:

  - Data Quality.
  - Data Architecture.
- **Store** – This phase involves storing data in a secure and accessible location. This could be in databases, data warehouses, data lakes, or other storage systems. This phase ensures that the stored data remains accessible, reliable, and compliant with relevant regulations and policies.

  The phase is covered by the following domains:

  - Data Catalog.
  - Data Classification.
  - Data Operations.
  - Reference and Mater Data.
  - Personal Data Protection.
- **Process** – This phase involves cleaning, where erroneous or inconsistent data is corrected or removed, and transformation, where data is reformatted or aggregated to meet specific requirements. Data processing ensures that the information is prepared and structured in a way that facilitates efficient analysis and utilization in downstream applications.

  The phase is covered by the following domains:

  - Data Catalog.
  - Data Quality.
  - Data Architecture.
  - Data Sharing and Integration.
- **Analyze** – This phase involves techniques, such as statistical analysis to uncover patterns, trends, and relationships within the data. It focuses on extracting valuable insights and knowledge from the data that can be further used for decision making, reporting to the senior executives, optimize processes and enhance business outcomes.

  The phase is covered by the following domains:

  - Data Analytics.
  - Data Architecture.

- **Use** – This phase involves visualizing the data through charts, graphs, dashboards, or other visual aids to communicate insights effectively. Additionally, it also involves making the data available to end-users or downstream systems through appropriate channels, networks, ensuring accessibility of meaningful data for effective business operations, innovations and decision making.

  The phase is covered by the following domains:

  - Data Classification.
  - Data Analytics.
  - Open Data.
  - Data Monetization.
  - Data Sharing and Integration.
  - Freedom of Information.
  - Personal Data Protection.

- **Backup and Archive** – This phase involves taking regular backup of data as a safeguarding measure against its potential loss or corruption. In the event of data loss or a disaster, the backup serves as a means to recover the lost data and reinstate operational functionality. Archiving ensures that data is securely retained in a cost-effective manner, typically in long-term storage solutions.

  The phase is covered by the following domains:

  - Data Operations.

- **Dispose** – This phase involves handling of data that has reached the end of its lifecycle and is no longer needed for business operations including contractual agreements and, compliance to legal requirements. Such data is securely deleted or disposed according to organizational policies and regulatory requirements.

  The phase is covered by the following domains:

  - Data Operations.

3.3 Data Governance and Management Policy structure

Every policy in this document pertains to a data governance and management domain. Each domain has been divided into sub-domains containing a set of policy statements outlining the necessary capabilities for establishing a data governance and management program. A roles and responsibilities matrix has been defined to inform on the accountable, responsible, and supporting roles for implementing the data governance and management activities. The following diagram depicts the structure of each policy within this document.

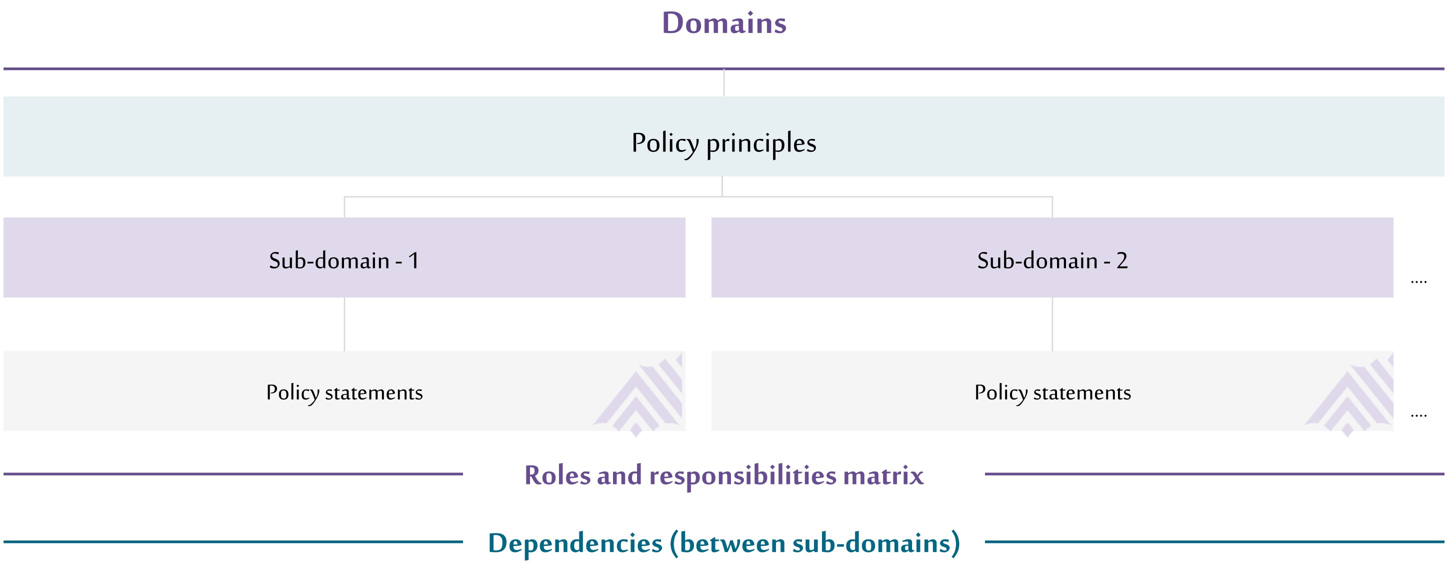


Figure-7: Policy Structure

The following table outlines the sub-domains corresponding to each of the 13 domains.

Domain ID	Domains	Sub-Domain ID	Sub- Domains
DG	Data Governance	DG.1	Data Management Strategy and Plan
		DG.2	Data Governance and Management Organization
		DG.3	Data Governance and Management Policies and Processes
		DG.4	Data Governance Training and Awareness
		DG.5	Data Governance Compliance Assessment
		DG.6	Data Governance Performance Management
DC	Data Catalog	DC.1	Data Dictionary
		DC.2	Business Glossary
		DC.3	Data Lineage
		DC.4	Data Catalog Automation Tool
CL	Data Classification	CL.1	Data Classification Impact Assessment
		CL.2	Supplementary Markers
		CL.3	Data Classification Review
		CL.4	Data Classification Artefacts
DQ	Data Quality	DQ.1	Data Quality Framework
		DQ.2	Data Quality Operations
		DQ.3	Data Quality Automation Tool
DO	Data Operations	DO.1	Data Storage
		DO.2	Backup and Restore
		DO.3	Disaster Recovery
DA	Data Architecture	DA.1	Data Architecture
		DA.2	Data Models

DSI	Data Sharing and Integration	DSI.1	Data Sharing Methods
		DSI.2	Data Sharing Agreements
		DSI.3	Data Sharing Automation Tool
AN	Data Analytics	AN.1	Business Cases
		AN.2	Data Analytics Implementation
		AN.3	Data Analytics Tools
		AN.4	Data Platforms
OD	Open Data	OD.1	Open Data Identification
		OD.2	Open Data Publishing
RMD	Reference and Master Data	RMD.1	Reference Data Management
		RMD.2	Mater Data Management
		RMD.3	Reference and Master Data Automation Tool
DM	Data Monetization	DM.1	Revenue Streams Creation
		DM.2	Cost Optimization
FOI	Freedom of Information	FOI.1	Information Request Management
		FOI.2	Issue and Grievance Management
PDP	Personal Data Protection	PDP.1	Controlling Entity Obligations
		PDP.2	Third Party Processing Unit Obligations

4.0

Data Governance Policy

4.0 Data Governance Policy

4.1 Policy Objective and Scope

The objective of this policy is to establish authority and ensure systematic planning and execution of data management practices. Additionally, it enables development of an effective governance and compliance model.

The policy provides requirements for all the government entities within the Sultanate of Oman to manage data practices through establishment of a data management strategy execution plan, data governance and management office, policies, processes along with mechanisms for continuous learning, compliance assessment and performance management.

4.2 Policy Principles

- **Data is a national asset:**

Develop practice that enable realization of the inherent value of data as a national asset to drive innovation and unlock economic growth through data integrity, monetization, transparency, and accountability.

- **A data-driven culture is encouraged:**

Establish processes and develop skills required for entities to utilize their data, derive meaningful insights, and leverage technology to improve their decision making and operational efficiency.

- **Data is trusted by all stakeholders:**

Establish practices for providing reliable, accurate and fit for purpose data to build data trust and confidence thereby, facilitating informed decision making.

- **Data practices are compliant with regulatory requirements:**

Develop data governance and management practices that uphold the regulatory requirements to ensure lawful, ethical, and responsible handling of data across the business processes of the entities.

4.3 Policy Statements

DG.1 Data Management Strategy and Plan

DG.1.1 The entity shall assess its data governance and management capabilities to identify the gaps and initiatives to be implemented for compliance to the National Data Governance Framework.

DG.1.2 A data management strategy shall be established in alignment to the entity's strategic business objectives. The strategy, at minimum, shall include the following:

- Data governance and management vision, mission, and guiding principles.
- Initiatives across the data governance and management domains.
- Key performance metrics to continuously monitor execution of the data management strategy.

The entity shall obtain approval of the data management strategy from the entity's data governance committee.

DG.1.3 A data management strategy execution plan shall be developed to implement the data management strategy. The plan, at minimum, shall include the following:

- Data management projects and scope.
- Estimated budget for data management strategy execution plan implementation.
- Key risks and its corresponding mitigation plan.
- Key success factors.

The entity shall obtain approval of the data management strategy execution plan from the entity's data governance committee.

DG.1.4 The approved data management strategy and the data management strategy execution plan shall be maintained and published on the internal portal of the entity.

DG.1.5 The data management strategy execution plan shall be periodically reviewed and updated. The entity shall document the outcome of the periodic review along with outlining any changes made.

DG.2 Data Governance and Management Organization

DG.2.1 The entity shall establish a data governance and management office[1] to operationalize the entity's data management strategy.

DG.2.2 The entity shall establish data governance roles to entrust the accountability and responsibility of operationalizing the initiatives of the data management strategy. The data governance roles, at minimum, shall include the following:

- Data Governance and Management Head.
- Data Management Officer.
- Data Governance and Compliance Officer.
- Data Owners.
- Business Data Stewards.
- IT Data Steward
- Enterprise Data Architect.
- Data Protection Officer.

DG.2.3 A governance model shall be established for the data governance and management office for governing its functioning and handling the data governance related issues arising within the entity. The governance model, at minimum, shall include the following:

- Data Governance Committee – To set the strategic direction for data governance and management program within the entity.
- Data Governance and Management Working Team – To implement the data governance and management policies and related practices across all business units within the entity.

DG.2.4 The entity shall document and maintain the decisions taken by the data governance committee along with its approval.

DG.2.5 The entity shall periodically monitor and track the performance of its data governance and management office.

DG.3 Data Governance and Management Policies and Processes

DG.3.1 The entity shall develop entity specific data governance and management policies in alignment with the 'National Data Governance and Management Policies' covering the data domains.

The entity shall obtain approval of the data governance and management policies from the entity's data governance committee.

DG.3.2 The entity shall develop entity specific data governance and management processes in alignment with the 'National Data Governance and Management Policies'. The processes, at minimum, shall include the following:

- Process participants.
- Process step preconditions.
- RACI matrix.
- Process Key Performance Indicators.

The entity shall obtain approval of the data governance and management processes from the entity's data governance committee.

DG.3.3 The approved data governance and management policies and processes shall be maintained and published on the internal portal of the entity.

DG.3.4 All changes to the data governance and management policies and processes shall be documented with clear indication of the approvals obtained.

DG.4 Data Governance Training and Awareness

DG.4.1 The entity shall assess the data governance awareness and skills of the stakeholders and map their skill levels. The results of the skill level mapping shall be used to develop the appropriate training sessions for the stakeholders.

DG.4.2 Training and awareness plan shall be developed to increase the adoption of the National Data Governance and Management policies. The plan, at minimum, shall include the following:

- Objectives of the training and awareness sessions.
- Training and awareness session topics covering all the domains of 'National Data Governance Framework'.
- Stakeholder groups intended for the training and awareness sessions.
- Training schedule.

The entity shall obtain approval of the training and awareness plan from the entity's data governance committee.

DG.4.3 A communication plan shall be established to communicate the updates on the data governance and management initiatives to the intended stakeholders. The communication plan, at minimum, shall include the following:

- Stakeholder impact analysis.
- Stakeholder classification based on the impact analysis.
- Objectives of the communication.
- Communication messages.
- List of intended stakeholders.
- Channels of communication.
- Frequency of communication.

The entity shall obtain approval of the communication plan from the entity's data governance committee.

DG.4.4 The entity shall periodically conduct training and awareness sessions for the intended stakeholders on the National Data Governance Framework guidelines.

DG.4.5 The entity shall periodically review and update the training, awareness, and communication plan.

DG.5 Data Governance Compliance Assessment Framework

DG.5.1 The entity shall document and report evidence corresponding to the compliance assessment criteria to MTCIT as per the requirements outlined in the 'National Data Governance and Management Compliance Assessment Model'.

DG.5.2 The entity shall establish data governance compliance assessment framework in alignment with the 'National Data Governance and Management Compliance Assessment Model'. The framework shall include, at minimum the following:

- Periodic processes for measuring compliance.
- Activities needed to plan and perform compliance assessments.
- Activities needed for reporting the results of a compliance assessment.
- Activities needed to address and escalate cases of non-compliance

DG.6 Data Governance Performance Management

DG.6.1 The entity shall establish KPIs (Key Performance Indicators) to monitor its performance across all data governance and management domains. The KPIs, at minimum, shall include the following:

- Indicator Name.
- Indicator Owner.
- Calculation equation.
- Data Sources for calculating the indicator.
- Measurement frequency.
- Baseline and target values.

DG.6.2 The entity shall periodically monitor the KPIs to verify that the implemented data governance and management initiatives and projects achieve their target objectives and outcomes and performance report of the data governance and management domains to the data governance committee.

4.4 Roles and Responsibilities Matrix

Key Activities	Data Governance and Management Head	Data Governance and Compliance Officer	Data Management Officer	Data Owner	Business Data Steward	IT Data Steward
Develop data management strategy and data management strategy execution plan.	A	R	C	C	C	-
Approve data management strategy and data management strategy execution plan*.	A/R	I	I	I	I	-
Develop data governance and management policies and processes.	A	R	I	C	C	C
Approve data governance and management policies and processes*.	A/R	I	I	I	I	I
Data governance awareness.	A	R	C	I	C	C
Monitor Data governance compliance.	A	R	C/I	C/I	C/I	C/I
Monitor Data governance performance.	A	R	R	C/I	C	I

R – Responsible, A – Accountable, C – Consulted, I – Informed

*Approvals shall be provided by the Data Governance Committee

4.5 Dependencies

- None

4.6 Policy Enforcement and Compliance

- The Data Governance and Management Head shall be responsible for implementing and enforcing the data governance policy within their respective entities.
- MTCIT shall be responsible for assessing the compliance of the government entities to the data governance policy.

5.0

Data Catalog Policy

5.0 Data Catalog Policy

5.1 Policy Objective and Scope

The objective of this policy is to establish a common understanding of the entity wide data among the users and enable them to trace it back to its certified source. The policy provides the necessary requirements for the government entities to establish standardized methods for development of a data catalog across the government entities in Oman including the Data Dictionary, Business Glossary and Data Lineage.

A data dictionary provides understanding on how the data is stored, interpreted, and utilized within information systems, whereas a business glossary provides understanding of the meaning and context of terms used in business processes, reports and systems.

A data catalog is a detailed inventory of both the technical and business attributes of an organization's data. It serves as a centralized repository that adds business context to technical metadata. By documenting data lineage, usage trends, and reliability, the catalog empowers users to easily find the data they need for analysis, reporting, and decision-making purposes. For e.g., consider a data element 'Vehicle registration number'. The data dictionary would provide the information on the data type, permissible length of the value, format of the vehicle registration number etc. The business glossary would provide the definition of 'Vehicle registration number', its usage, related terms etc. Whereas the data catalog would provide information on its source, access permissions, owner of the data element etc.

5.2 Policy Principles

- **Data is understood uniformly across stakeholders:**
  Establish practices that enable a uniform understanding of the data to facilitate efficient data sharing and analysis thereby promoting reliability and efficiency in utilizing data assets within the entity.

5.3 Policy Statements

DC.1 Data Dictionary

DC.1.1 The entity shall create an inventory of all its data assets and identify the critical data elements for cataloging.

DC.1.2 A data dictionary shall be developed that serves as repository for the entity's technical metadata. The data dictionary, at minimum, shall include the following:

- Data element name as per the naming convention standards issued by MTCIT.
- Data element size.
- Data element type.
- Master data source for the data elements documenting the authoritative source including the application name, source module, source table name and source column name.
- Physical database, table, column, and file names.
- Access permissions.
- Retention, backup, and recovery rules for the data element.

DC.1.3 The data dictionary shall be periodically reviewed and updated.

DC.1.4 The entity shall develop and obtain approval on the processes for creating, updating the data dictionary along with certifying the metadata.

DC.1.5 An audit trail shall be maintained for viewing all updates made to the data dictionary.

DC.1.6 The data dictionary shall be stored in a central location along with appropriate access rights assigned to the relevant stakeholders.

DC.2 Business Glossary

DC.2.1 The entity shall develop a business glossary to establish and promote a common understanding of business terms used across its business processes. The business glossary, at minimum, shall include the following:

- Name of the business term.
- Definition of the business term.
- Subject area classification. (Finance, Human Resources, Procurement etc.)
- Primary data classification (Top Secret, Secret, Restricted, Confidential, Unclassified) and supplementary markers of the business term.
- Ownership and stewardship for the business term.
- Business rules associated with the business term.
- Synonyms (or aliases) used for the business term.
- Key Performance Indicators (KPIs), if applicable, along with the calculation methodology.

DC.2.2 The business glossary shall be periodically reviewed and updated.

DC.2.3 The entity shall link the business glossary to the metadata.

DC.2.4 The entity shall develop and obtain approval on the processes for creating, updating, and certifying the business glossary.

DC.2.5 An audit trail shall be maintained for viewing all updates made to the business glossary.

DC.2.6 The business glossary shall be maintained in a central location along with appropriate access rights assigned to the relevant stakeholders.

DC.3 Data Lineage

DC.3.1 The entity shall establish a data lineage to visually represent the movement and transformation logic of its metadata from source to target systems.

DC.3.2 The entity shall develop and obtain approval on the processes for creating, updating, and certifying the data lineage.

DC.3.3 An audit trail shall be maintained for viewing all updates made to the data lineage.

DC.3.4 The data lineage shall be stored in a central location along with appropriate access rights assigned to the relevant stakeholders.

DC.4 Data Catalog Automation Tool

DC.4.1 The entity shall onboard and adopt a data catalog automation tool for automating the creation, update and certification processes of the data dictionary, business glossary and data lineage.

DC.4.2 The data models related to the Data Catalog tool shall be aligned and ensured to be consistent with the enterprise data architecture.

DC.4.3 The entity shall develop a plan and obtain approval for connecting the data sources to the data catalog automation tool for onboarding the data dictionary and uploading the business glossary.

DC.4.4 Automated workflows shall be configured for data dictionary, business glossary and data lineage within the data catalog automation tool. The workflows, at minimum, shall include the following:

- Creation and update of data dictionary along with certification of metadata.
- Creation, update, and certification of business glossary.
- Creation, update, and certification of data lineage.
- Data Catalog access management.

5.4 Roles and Responsibilities Matrix

Key Activities	Data Governance and Management Head	Data Governance and Compliance Officer	Data Management Officer	Data Owner	Business Data Steward	IT Data Steward
Create the data asset inventory and identify the Critical Data Elements.	-	I	C	A	R	I
Develop the processes for creation, update and certification of business and technical metadata along with data lineage	A	R	I	C	C	C
Approve the processes for creation, update and certification of business and technical metadata along with data lineage*	A/R	I	I	I	I	I
Develop and update the Data Dictionary along with audit trail.	-	I	C/I	A	C/I	R
Develop and update the Business Glossary, maintaining audit trail along with linking to the data dictionary.	-	I	C/I	A	C/I	R
Develop and update the Data Lineage along with audit trail.	-	I	C/I	A	C/I	R
Align the data model of the data catalog with the enterprise data architecture.	A	I	R	I	I	R
Developing a plan for connecting the data sources to the data catalog automation tool.	I	I	A/R	C/I	C/I	R
Approval on the plan for connecting the data sources to the data catalog automation tool.	A/R	C/I	I	I	I	I
Configure automated workflows within the data catalog automation tool.	A	I	R	I	C/I	R

R – Responsible, A – Accountable, C – Consulted, I – Informed

*Approval shall be provided by the Data Governance Committee.

5.5 Dependencies

- Data Governance Policy.

5.6 Policy Enforcement and Compliance

- The Data Governance and Management Head shall be responsible for implementing and enforcing the data catalog policy within their respective entities.
- MTCIT shall be responsible for assessing the compliance of the government entities to the data catalog policy.

6.0

Data Classification Policy

6.0 Data Classification Policy

6.1 Policy Objective and Scope

The objective of this policy is to assist the government entities within the sultanate to categorize their data assets according to their sensitivity and enable the development of appropriate protection measures based on the level of risk associated with the data assets. The policy applies to all types of data the organization produces, receives, or deals within different kinds of resource types or structure. This includes, paper record, meetings, communications though applications and different medias, email, data stored in USB, Tapes Video, Maps, Pictures, Plans, and handwriting records, or any type of recorded data

The policy provides the necessary requirements for the government entities to establish standardized methods for classifying their data assets along with development of artifacts for maintaining the classification information.

6.2 Policy Principles

- **Classification based on the degree of damage/impact of a data asset:**

  Classify data assets based on the degree of damage or business impact that could be caused by the loss, misuse, unauthorized disclosure of data assets.

- **Unclassified by default:**

  Data assets shall remain unclassified unless their impact assessment requires them to be classified into a higher classification level.

- **Unclassified data is not public by default:**

  Unclassified information shall be treated as official unless it is wholly or partially approved for public release as indicated by a supplementary marker "FOR PUBLIC RELEASE".

- **Data is shared on a need-to-know basis:**

  The entity shall limit access of the data to the minimum number of individuals necessary to accomplish the entity's strategic objectives.

- **Data Classification is dynamic and reflects the evolving nature of data:**

  Data classification shall be assessed and updated regularly to ensure its alignment with its lifecycle and the changing external factors that affect its sensitivity.

- **Data Classification is done in a timely manner:**

  To ensure timely availability of data to the appropriate stakeholders, the classification should be performed upon creation of data in a timely manner. At the time of reception of the data from another entity, the receiving entity must respect the degree of classification determined by the originating entity.

- **Ensure compliance with regulatory requirements:**

  Data assets shall be classified to achieve compliance with the regulatory requirements and ensure lawful, ethical, and responsible handling of data across the business processes of the entities.

6.3 Policy Statements

CL.1 Data Classification Impact Assessment

Classification	Business Impact Level	Description	Examples
Top Secret	4	Data shall be classified as "Top Secret", if its unauthorized access, or disclosure can lead to exceptional and long-term damage to the government, national security, diplomatic relations and the reputation of the Sultanate.	● Plans and details of military operations or any information related to it. ● Information related to formal political relations and international agreements or treaties and all related discussions, studies and preparatory work. ● Information related to the works of management and formation of Security and Intelligence apparatus. ● Information related to weapons and ammunition or any source of the Defense powers.
Secret	3	Data shall be classified as "Secret", if its unauthorized access, or disclosure can lead to serious damage to the Sultanate and /or its interests.	● Information about the storage location of defense or economic materials. ● Information that has a security dimension and disclosure of it would make adverse effect on the morale of the citizens. ● Information about the movements of the armed forces or about public security. ● Information about the movements of police forces or details concerning public safety operations. ● Information affecting the dignity of the state.
Restricted	2	Data shall be classified as "Restricted", if its unauthorized access, or disclosure can cause harm to the organization's operations or reputation of a public personality.	● Information relating to administrative or public affairs. ● PII data of government employees. ● Documents of law enforcement agencies containing details of sensitive investigations.
Confidential	1	Data shall be classified as "Confidential" data, if its unauthorized access, or disclosure, can cause harm to an organization's competitive standing or reputation or reputation of an individual.	● Vendor contracts and quotations. ● Personally Identifiable Information (PII) data such as name, address, social security numbers, phone numbers, and account numbers, license numbers, biometric identifiers. ● Requests for proposals. ● Security protocols and access control lists ● Pending litigation documents ● Internal investigations and disciplinary records ● Employee performance evaluations.
Unclassified	0	Data shall be marked as "Unclassified", if it is assessed to not fall under any of the higher classification labels	● Inter or intra-agency memorandums. ● Information that provides competitive edge to a particular sector. ● Advisory reports for policy decision making. ● Data marked with the supplementary marker 'FOR PUBLIC RELEASE'. For e.g.: ○ Public announcements and press releases. ○ Information on public services provided to citizens by government. ○ Any information that is publicly available on entity websites. ○ Advertisements

CL.1.1 The entity shall prioritize its data assets to establish the order of classification.

CL.1.2 The data assets shall be classified into one of the primary data classification labels namely Top Secret, Secret, Restricted and Confidential as per the 'Royal Decree No. 118/2011- Issuing the Law Classifying the State's Documents and Regulating the Protected Places' or marked unclassified.

CL.1.3 The entity shall establish and follow approved processes for assigning the appropriate primary data classification label to its data assets. The process at minimum, shall include the following activities:

- Conduct impact assessment to identify the potential damage or impact that can be caused by the loss, misuse, or unauthorized disclosure of the data asset. The impact assessment shall at minimum cover the following dimensions:
  - Identification of potential impact arising from disclosure or unauthorized access to data.
  - Mapping of the identified potential impact to the business impact levels from 4 to 1.
  - Mapping of the data assets to the appropriate primary data classification labels namely Top Secret, Secret, Restricted, and Confidential as per the assessed business impact levels from 4 to 1 respectively. All data assets that are assessed to not fall under any of the primary data classification labels, shall be marked as 'Unclassified'.

CL.1.4 The entity shall obtain approval on the assigned data classification labels of its data assets.

CL.2 Supplementary Markers

CL.2.1 The entity shall define a list of entity specific supplementary markers (caveats and dissemination limiting markers) to be applied on top of the primary data classification labels to further limit the information dissemination as per its requirements.

CL.2.2 The entity shall evaluate and may apply one or more appropriate supplementary markers to its data assets that are classified as Top Secret, Secret, Restricted and Confidential to control the dissemination of data assets.

CL.2.3 The entity shall assess and mark its unclassified data assets with the supplementary marker 'FOR PUBLIC RELEASE' as per Article 28 of the 'National Data Strategy' for making them available as open data and contribute towards building a knowledge-based society. The assessment shall include at minimum the following:

- Potential conflict with the existing laws/policies.
- The benefits of applying the supplementary marker 'FOR PUBLIC RELEASE' versus the negative impact.

For examples of the supplementary markers (caveats and dissemination limiting markers), please refer to the table below:

Category	Description	Examples
Caveats	Caveats are warnings that the data asset has special requirements in addition to that of its primary data classification. Caveats are secondary markers to further limit the way in which data assets are handled and accessed. While every data asset may have only one primary data classification, it may have zero, one or more caveats as dictated by entity specific requirements.	- **PERSONAL-** Personal information (either fact or opinion) of an individual whose unauthorized disclosure may cause them some harm e.g., information relating to disciplinary proceedings, investigations of misconduct, medical information and similar. - **COMMERCIAL-** Information that are commercially sensitive e.g., bids, quotations, financial evaluations of bids. - **LEGAL-** Information that are legally sensitive e.g., contracts, agreements, litigation documents etc. - **CABINET-** Data assets relating to proceedings and decisions of the Cabinet of Ministers. - **OMANI ONLY-** Data assets only to be accessible to Omani employees of the agency and not to foreign nationals who are in the employment of the entity.
Dissemination Limiting Markers	Dissemination limiting markers are secondary markers to further limit the individuals or entities to whom the information/data may be disseminated. Such individuals or entities may be external to the agency. While every data asset may have only one primary data classification, it may have zero, one or more dissemination limiting markers as dictated by entity specific requirements.	- **INTERNAL USE ONLY-** Data assets that may only be accessible within the entity and is not to be shared with any external parties or the public. - **FOR PUBLIC RELEASE-** Data assets that have been approved for release to the public. - **OMAN GOVERNMENT ONLY-** Data assets that may be shared only with other government entities in the Sultanate of Oman. - **GCC ONLY-** Data assets that may be shared only with the other member countries of the Gulf Cooperating Council (GCC).

CL.2.4 The supplementary markers for all the data assets shall be defined as metadata within the entity's business glossary as defined in the Data Catalog Policy.

CL.3 Data Classification Review

CL.3.1 The entity shall define the criteria that can trigger the declassification or downgrade of the classification labels for each of its data assets.

CL.3.2 The entity shall develop and follow a process for reviewing and updating the assigned data classification labels to its data assets. The process at minimum shall include the following activities:

- Declassification or a downgrade of the data classification performed to reflect the change in the business impact levels of the data asset.
- The receiving entity challenging the data classification assigned by an originating entity in a scenario of conflict.

CL.3.3 The data classification labels for all the data assets shall be defined as metadata within the entity's business glossary as defined in the Data Catalog Policy.

CL.4 Data Classification Artefacts

CL.4.1 The entity shall maintain a data classification register containing the assigned primary classification labels and supplementary markers to its data assets. The entity can leverage its data catalog automated tool for this purpose. The register, at minimum, shall include the following:

- List of the entity's data assets.
- Primary data classification labels and supplementary markers assigned to the data assets along with dates of assignment.
- Duration for which the assigned primary data classification is valid. The duration of the primary data classification shall at maximum be the retention period defined for the data asset.
- The declassification or downgrade triggers for the data asset as defined by the entity during the assignment of primary data classification labels.
- A log of the data classification activities conducted on the data asset along with the details of primary classification labels and supplementary markers review.

6.4 Roles and Responsibilities Matrix

Key Activities	Data Governance and Management Head	Data Governance and Compliance Officer	Data Management Officer	Data Owner	Business Data Steward	IT Data Steward
Prioritize data assets for classification.	I	I	C/I	A	R	C
Conduct impact assessment and apply the primary classification labels.	I	C/I	C/I	A	R	-
Develop the process for data classification	A	R	I	C	C	C
Approve the process for data classification*	A/R	I	I	I	I	I
Approve the data classification labels	I	C/I	C/I	A/R	I	-
Review and update the primary classification labels.	I	C/I	C/I	A	R	I
Evaluate and apply supplementary markers to the data assets.	I	C/I	C/I	A	R	-
Create and maintain the data classification register.	I	C/I	C/I	A	R	I

R – Responsible, A – Accountable, C – Consulted, I – Informed

*Approval shall be provided by the Data Governance Committee.

6.5 Dependencies

- Data Governance Policy.
- Data Catalog Policy.

6.6 Policy Enforcement and Compliance

- The Data Governance and Management Head shall be responsible for implementing and enforcing the data classification policy within their respective entities.
- MTCIT shall be responsible for assessing the compliance of the government entities to the data classification policy.

7.0

Data Quality Policy

7.0 Data Quality Policy

7.1 Policy Objective and Scope

The objective of this policy is to provide fit-for purpose data to the internal and external data consumers along with fostering trust and confidence in data driven decision making.

The policy provides necessary requirements for the government entities within the Sultanate of Oman to establish a Data Quality Framework, enable data quality checks at source and ensure the availability of high-quality data across the entity.

7.2 Policy Principles

- **Data is a national asset:**

  Develop practice that enable realization of the inherent value of data as a national asset to drive innovation and unlock economic growth through data integrity, monetization, transparency, and accountability.
- **Data is trusted by all stakeholders:**

  Establish practices for providing reliable, accurate and fit for purpose data to build data trust and confidence thereby, facilitating informed decision making.

7.3 Policy Statements

DQ.1 Data Quality Framework

DQ.1.1 The entity shall establish a data quality framework for operationalizing the entity specific data quality management initiatives. The framework, at minimum, shall include the following:

- Identification of the data quality dimensions to address the data quality issues. The dimensions[2], at minimum, shall include one or more of the following:

Data Quality Dimensions	Definition	Examples
Completeness	Extent to which desired data is available for use.	A citizen's record aged 15 years or older, without a civil identification number.
Consistency	Extent to which identical data has the same value across the systems.	Date of Birth for citizens shall be stored in DD-MM-YYYY format across all systems within the entity.
Accuracy	Extent to which data value matches with the real value.	Change in address of the citizens are updated.
Timeliness	Extent to which the up-to-date data is available.	Change in address of the citizens shall be updated in the systems within the same day of notification.
Uniqueness	Extent to which unique data is available without duplication.	Different citizens cannot have the same civil identification number across systems.

- Approach for calculating the data quality scores. The data quality scoring approach, at minimum, shall include the following:
  - ○ Threshold percentage for each of the Data Quality Dimensions for meeting business expectations and the business impact of exceeding the threshold. For example: For assessing data quality completeness, metrics may include the percentage of missing values. A threshold of 4% or less indicates that the data is considered complete.
  - ○ Formula to calculate the data quality score.
- Data quality index to showcase the change in the data quality score over a time period.

DQ.1.2 The entity shall develop and obtain approval on the process for monitoring and identifying the data quality issues.

DQ.1.3 The entity shall define and obtain approval on the process for remediating the data quality issues. The process, at minimum, shall include the following:

- Root cause analysis to identify the cause of the issue.
- Remediation options to address the root cause.
- Plan to implement the selected remediation option.
- Implementation and validation of the selected remediation option.

DQ.1.4 The entity shall develop and obtain approval for the data quality Service Level Agreements (SLAs) which, at minimum, shall include the following:

- Timeline for developing plans to fix data quality issues.
- Timeline for implementing and reviewing data quality changes.
- Escalation actions for SLA violations.

DQ.2 Data Quality Operations

DQ.2.1 The entity shall develop and document the data quality rules for the business-critical data elements based on the data quality dimensions.

DQ.2.2 The entity shall conduct data quality profiling as per the data quality execution plan to monitor the data quality health.

DQ.2.3 The entity shall evaluate the data profiling result to analyze the requirement of rule change or threshold reconfiguration to refine the data quality monitoring inputs.

DQ.2.4 The entity shall conduct root cause analysis for the identified data quality issues and prepare data quality remediation report. The report shall include, at minimum the following:

- Description of the data quality issues.
- Impact of the data quality issues (business unit level/ entity level).
- Root cause analysis results of the identified issues.
- Recommended activities for issue resolution.

DQ.2.5 Data quality remediation plan shall be developed by the entity to implement the activities recommended for the resolution of the issues. The plan, at minimum, shall include the timeline and milestones for implementation of the recommended activities.

The entity shall obtain approval on the developed data quality remediation plan.

DQ.2.6 The data quality issue remediation shall be monitored as per the entity's data quality Service Level Agreements.

DQ.2.7 The entity shall maintain a data quality issues log. The log shall include, at minimum the following:

- Data quality issue description.
- Corrective or Preventive actions performed on the issue.
- Degree of data quality improvement.
- Number of data quality issues resolved vs the number of data quality issues identified.
- Number of SLA breaches.

DQ.3 Data Quality Automation Tool

DQ.3.1 The entity shall onboard and adopt a tool for implementing the processes of data quality management within the tool as automated workflows. The workflows at minimum shall include the following:

- Workflows for automated discovery of data quality issues as per the data quality rules defined across the data quality dimensions.
- Workflow for automated routing of the identified data quality issues to the relevant stakeholders.
- Workflows for generating standardized reports and dashboards summarizing key data quality metrics and trends within the entity data.

7.4 Roles and Responsibilities Matrix

Key Activities	Data Governance and Management Head	Data Governance and Compliance Officer	Data Management Officer	Data Owner	Business Data Steward	IT Data Steward
Develop the Data Quality Framework.	A	R	I	C/I	C/I	I
Develop the processes for Data Quality monitoring, issues identification and remediation	A	R	I	C	C	C
Approve the processes for Data Quality monitoring, issues identification and remediation*	A/R	I	I	I	I	I
Identify data quality dimensions.	A	R	I	C/I	C/I	I
Develop data quality service level agreements.	A	R	I	C/I	C/I	I
Develop data quality rules.	-	-	C/I	A	R	I
Conduct data quality profiling.	A	C/I	R	C/I	R	R
Develop data quality remediation plan.	-	I	C/I	A	R	I
Approve data quality remediation plan.	-	I	C/I	A	R	I
Execute data quality remediation plan.	-	I	I	A	R	R
Maintain data quality issues log.	A	R	R	C/I	C/I	I

R – Responsible, A – Accountable, C – Consulted, I – Informed

*Approval shall be provided by the Data Governance Committee.

7.5 Dependencies

- Data Governance Policy.

7.6 Policy Enforcement and Compliance

- The Data Governance and Management Head shall be responsible for implementing and enforcing the data quality policy within their respective entities.
- MTCIT shall be responsible for assessing the compliance of the government entities to the data quality policy.

8.0

Data Operations Policy

8.0 Data Operations Policy

8.1 Policy Objective and Scope

The objective of this policy is to enable governance of data storage operations while effectively managing the data lifecycle within the entity.

The policy provides requirements for the government entities within the Sultanate of Oman to enhance their data lifecycle operations including storage, retention, archival, backup, disposal, and recovery operations along with efficient disaster management mechanism.

8.2 Policy Principles

- **Data is managed across its lifecycle as per business needs:**

  Develop practices that help collect, store, archive, and dispose data as per its relevance and purpose along with delivering it to the data consumers.

8.3 Policy Statements

DO.1 Data Storage

DO.1.1 The entity shall conduct periodic storage infrastructure utilization forecast of its information systems based on the future business requirements. The forecast, at minimum, shall include the following:

- Storage capacity needs as per the planned application initiatives.
- Estimated budget for the future storage requirements.

DO.1.2 The entity shall define a process and obtain approval for evaluating and selecting the database technology. The evaluation, at minimum, shall include the following:

- Total ownership cost.
- Data volume capacity of the technology.
- Security controls provided by the technology.
- Availability of skilled resources within and outside of the entity.

DO.1.3 The entity shall define and obtain approval for the process of using digital means for data collection and shall maintain a register to document the reason for not collecting data through a digital means.

DO.1.4 The entity shall define and obtain approval for the process of providing role-based access to the relevant employees and contractors to the entity's database. Access controls for employees and contractors of the entity shall be determined by their respective classification labels, which are based on the nature of their work performed within and for the entity.

DO.1.5 The entity shall regularly monitor and report the performance of the database.

DO.1.6 The entity shall define and obtain approval on the Service Level Agreements[4] of database performance requirements, data availability and recovery requirements.

DO.1.7 The entity shall define and implement the retention periods for data based on business, regulatory and legal requirements.

DO.1.8 The entity shall conduct periodic reviews and update the defined retention periods as per requirements.

DO.1.9 The entity shall define and implement archival period of the data as per the business and regulatory requirements.

DO.1.10 The entity shall define and obtain approval on the rules for disposal of the data based on the classification levels and tables of common and specific retention periods approved for each entity.

DO.1.11 The entity shall document a list of safe destruction methods and obtain approval to implement it on the archived data.

DO.2 Backup and Restore

DO.2.1 The entity shall establish and follow a process for data backup and restore. The process, at minimum, shall include the following:

- Backup frequency for each information system.
- Backup scope of each information system along with the data range.
- Backup location along with the storage medium.
- Backup validation.
- Restore through change request.

DO.2.2 The entity shall conduct periodic recovery testing to ensure successful restoration of the backup within a timeframe.

DO.2.3 The entity shall verify the validity of the restored data before transferring it to the production environment.

DO.3 Disaster Recovery

DO.3.1 The entity shall develop and obtain approval on the disaster recovery plan[5] to ensure limited-service disruption in case of prolonged system outage.

DO.3.2 The entity shall develop a list of information systems ranked based on their business criticality and potential monetary and reputational losses because of emergency or disaster. The list of systems, at minimum, shall include the following:

- Recovery Time Objective – Maximum permissible outage time of the information system without causing business damage.
- Recovery Point Objective – Maximum permissible data the entity can afford losing without causing business damage.

DO.3.3 In the event of permanent loss of large volume of highly valued data (Data Classified as Top Secret and Secret), the entity shall develop a data loss case report. The data loss case report, at minimum shall include the following:

- Lost data description.
- Criticality of the data.
- Data loss cause.
- Date and time of data loss.

DO.3.4 The entity shall draft a report on the data loss incident, outlining lessons learned and preventive measures. The report shall then be submitted to the data governance committee for approval and direction.

8.4 Roles and Responsibilities Matrix

Key Activities	Data Governance and Management Head	Data Governance and Compliance Officer	Data Management Officer	Data Owner	Business Data Steward	IT Data Steward	IT Head
Develop the process for evaluation and selection of database technology.	C/I	C	R	C/I	C	R	A
Approve the process for evaluation and selection of database technology*	I	I	I	I	I	I	A/R
Develop the process for data collection.	A	R	I	C	C	C	-
Approve the process for data collection*	A/R	I	I	I	I	I	-
Develop process of providing role-based access to the relevant employees and contractors to the entity's database	A	R	I	C	C	C	-
Approve process of providing role-based access to the relevant employees and contractors to the entity's database*.	A/R	I	I	I	I	I	-
Define the Service Level Agreements of database performance requirements, data availability and recovery requirements	-	I	C	C	R	R	A
Approve the Service Level Agreements of database performance requirements, data availability and recovery requirements	-	I	C/I	A/R	I	I	I
Documenting a list of safe destruction methods	-	I	I	C/I	C/I	R	A
Approve list of safe destruction methods		I	I	I	I	I	R/A

Developing and enforcing Data retention periods.	-	C/I	C	A	R	R	-
Developing and enforcing data archival periods.	-	C/I	C	A	R	R	-
Developing and enforcing data disposal rules.	-	C/I	C	A	R	R	-
Data backup and restore operations.	A	I	I	I	C	R	C/I
Development of disaster recovery plan.	A	R	I	I	C	I	C/I
Approve the disaster recovery plan*	A/R	I	I	I	I	I	I
Analysis and processing of accidental data loss.	A	R	I	C/I	C/I	R	C/I

R – Responsible, A – Accountable, C – Consulted, I – Informed

*Approvals shall be provided by the Data Governance Committee.

8.5 Dependencies

- Data Governance Policy.
- Data Classification Policy.

8.6 Policy Enforcement and Compliance

- The Data Governance and Management Head shall be responsible for implementing and enforcing the data operations policy within their respective entities.
- MTCIT shall be responsible for assessing the compliance of the government entities to the data operations policy.

9.0

Data Architecture Policy

9.0 Data Architecture Policy

9.1 Policy Objective and Scope

The objective of this policy is to ensure that the data is defined, structured, and managed to ensure consistent and transparent usage of data.

The policy provides requirements for the government entities to establish standardized practices for translating business needs into data requirements in terms of identifying, defining, and modeling to facilitate availability of data to the data consumers.

9.2 Policy Principles

- **Data is trusted by all stakeholders:**

  Establish practices for providing reliable, accurate and fit for purpose data to build data trust and confidence thereby, facilitating informed decision making.

9.3 Policy Statements

DA.1 Data Architecture

DA.1.1 The entity shall develop and document its current state data architecture[6] for outlining the existing structure, components and processes involved in managing and utilizing its data from source to the target applications. The current state data architecture, at minimum, shall include the following:

- Identification of data sources.
- Identification of processes involved in existing business operations.
- Data storage systems, data processing systems and data analytics platforms involved in the existing processes.
- Data Architecture patterns in terms of data ingestion and provisioning as per the existing processes.

The entity shall obtain approval on the current state data architecture.

DA.1.2 The business and technical requirements shall be identified and documented as per the entity's planned data initiatives. The requirements, at minimum, shall include the following:

- The data required along with their sources as per the purpose and scope of the data initiative.
- Requirements of the data platform in terms of data ingestion, storage, data processing and provisioning as per the objectives of the data initiative.

DA.1.3 The entity shall review its current state data architecture and develop its target state data architecture as per the activities identified to address the gaps. The target state architecture shall be developed in alignment with the overall enterprise architecture standards. The target state data architecture, at minimum, shall include the following:

- Identification of data sources.
- Identification of processes involved as per the planned data initiatives.
- Data storage systems, data processing systems and data analytics platforms involved in the business processes of the planned data initiatives.
- Data Architecture patterns in terms of data ingestion and provisioning as per the existing processes.

The target state data architecture shall be reviewed to ensure that it addresses the requirements of the entity's planned data initiatives. Additionally, the entity shall obtain approval on the target state data architecture.

DA.1.4 The entity shall establish data architecture checkpoints within its software development lifecycle to review and assess impact on its data architecture due to any system development initiative.

DA.1.5 The data architecture shall be monitored and updated in case of any changes to the entity's data systems which include the following cases:

- Change in the structure of the existing data within the systems.
- Changing the data integration methods for accessing or sharing data from multiple systems.
- Changing the data sources or data storage systems.

DA.1.6 The entity shall define the process to update the data architecture. The process, at minimum, shall have the following steps:

- Reviewing the data architecture change request.
- Conducting impact assessment to identify the affected architecture components.
- Updating the impacted architecture components.
- Obtaining approval, updating the data architecture, and publishing it.

The entity shall obtain approval on the process for its implementation.

DA.1.7 The entity shall adopt a suitable tool to design and maintain its data architecture. The tool, at minimum, shall support the following capabilities:

- Data Architecture design.
- Impact analysis to analyze the risk of changes to the data architecture components.

DA.1.8 The data architecture shall be stored in a central location with appropriate access rights assigned to the relevant stakeholders.

DA.1.9 All updates made to the data architecture shall be tracked through a version control mechanism.

DA.2 Data Models

DA.2.1 The entities shall develop and document data models to define the structures and relationships of the data within its system components. The data models, at minimum, shall include the following:

- The conceptual data model showcasing the involved data entities, their attributes and relationship between the data entities.
- The logical data model based on the conceptual data model along with the data constraints.
- The physical data model based on the logical data model and including the table and column level information for each of the data entities.

The entity shall obtain approval on the developed and documented data models.

DA.2.2 The entity shall define the naming convention standards to be used for developing the data models. The naming convention standards shall be documented as technical metadata within the entity's data dictionary as per its Data Catalog Policy.

DA.2.3 The entity shall establish a diagramming method to develop its data models.

DA.2.4 The entity shall establish checkpoints within its software development lifecycle to review and assess impact on its data models due to any system development initiative.

DA.2.5 The entity shall adopt a suitable tool to design and maintain its data models. The tool, at minimum, shall support the following capabilities:

- Graphical representation of the data model.
- Automated redrawing of relationships based on movement of entities.

DA.2.6 The data models shall be monitored and updated in case of any changes to the entity's data systems which include the following cases:

- Change in the structure of the existing data within the systems.
- Changing the data sources or data storage systems.

DA.2.7 The entities shall develop and obtain approval on a process to update and receive approval for any changes made to the data models. The process, at minimum, shall include the following steps:

- Reviewing the data model change request.
- Conducting impact assessment to identify the affected data model components.
- Updating the impacted data model components.
- Obtaining approval, updating the data architecture, and publishing it.

DA.2.8 The data models shall be stored in a central location with appropriate access rights assigned to the relevant stakeholders.

DA.2.9 All updates made to the data models shall be tracked through a version control mechanism.

9.4 Roles and Responsibilities Matrix

Key Activities	Data Governance and Management Head	Data Governance and Compliance Officer	Data Management Officer	Data Owner	Business Data Steward	IT Data Steward	Enterprise Data Architect
Define the entity specific data architecture standards.	I	I	I	I	I	C	A/R
Develop the Current and Target State Data Architecture.	I	I	R	I	C	C	A
Approve the current and target state data architecture	I	I	I	-	-	I	A/R
Develop the process to update the data architecture	A	R	I	C	C	C	-
Approve the process to update the data architecture*	A/R	I	I	I	I	I	-
Identify the business and technical requirements for the target state data architecture.	A	I	R	C	R	R	C/I
Monitor and review data architecture.	-	I	C/I	C/I	C/I	R	A
Develop the process for updating the data models	A	R	I	C	C	C	-
Approve the process for updating the data models*	A/R	I	I	I	I	I	-
Develop and updating the data models.	-	I	I	C/I	C/I	R	A
Approve the data models (including any updates made to them)	-	I	I	C/I	C/I	I	A/R
Define the data modeling diagramming method.	A	R	C/I	I	I	R	R

R – Responsible, A – Accountable, C – Consulted, I – Informed

* Approvals shall be provided by the Data Governance Committee

9.5 Dependencies

- Data Governance Policy.
- Data Classification Policy.

9.6 Policy Enforcement and Compliance

- The Data Governance and Management Head shall be responsible for implementing and enforcing the data architecture policy within their respective entities.
- MTCIT shall be responsible for assessing the compliance of the government entities to the data architecture policy.

10.0

Data Sharing and Integration Policy

10.0 Data Sharing and Integration Policy

10.1 Policy Objective and Scope

The objective of the Data Sharing and Integration policy is to foster seamless internal and external data sharing among the information systems while establishing measures for ensuring the protection of data being shared.

The policy provides the necessary requirements to the government entities for establishing standard data sharing methods along with setting expectations in the form of agreements between the parties exchanging the data. Additionally, the policy provides requirements for automating the data sharing methods using a data sharing automation tool.

10.2 Policy Principles

- **Data is shared and is accessible on time:**

  Develop practices to facilitate seamless internal and external sharing of data, ensuring that data users obtain information in a timely manner, thereby improving the quality and efficiency of decision-making processes.

- **Systems are integrated with a focus on compatibility and streamlined data exchange:**

  Establish robust methodologies and infrastructure to seamlessly integrate diverse technology systems, prioritizing secure and reliable access to data for authorized users.

10.3 Policy Statements

DSI.1 Data Sharing Methods

DSI.1.1 The entity shall detail the functional and non-functional requirements into an integration requirements document as per its planned and approved data analytics business cases. The requirements, at minimum, shall include the following:

- The purpose and scope of the use case for data collection/sharing.
- Data availability requirements.
- Regulatory requirements, if any, governing the collection, storage, retention and archival of data.
- Implementation Timeline.
- Cost Estimate.

DSI.1.2 The entity shall assess its current integration architecture to identify the gaps with respect to the data integration requirements.

DSI.1.3 A target integration architecture shall be created to bridge the identified gaps. The target integration architecture, at minimum, shall include the following:

- The data sources, intermediary systems, and data platforms along with target systems (internal/external).
- Data Integration patterns (ETL – Extract transform and load, ELT – Extract load and transform, event streaming, API - Application Programming Interface and data virtualization) as per the data availability requirements.
- Technical standards for data and information exchange outlined in the "Systems Integration Policy for Government Entities – Published by MTCIT."

DSI.1.4 The entity shall develop a solution integration design as per its target integration architecture. The solution integration design, at minimum, shall include the following:

- Overview of the integration solution supported by the solution integration diagram.
- Data flow diagram representing the flow of data between the systems sharing data.
- Mapping specifications for all the intermediary staging areas where the data is being transformed between the source and the target systems.
- Security requirements to be considered.

DSI.1.5 The entity shall test the developed integration solution prior to its deployment to the production environment to verify its alignment to the solution integration design. The testing, at minimum, shall consist of the following:

- **Integration testing:** verifying the correctness of data flows between integrated technology components (systems, applications, data stores) to identify and resolve any data quality issues.
- **Functional testing:** verifying that the system meets both functional and non-functional requirements and satisfies purpose of the data collection/sharing.

Each of the above shall, at minimum, include the following:

- Defining the test cases.
- Setting up the test environment.
- Executing the test cases in a test environment and documenting test results.

DSI.1.6 The entity shall monitor and maintain the solution integration design to incorporate any changes in the integration requirements. The monitoring and maintenance shall at minimum include the following:

- Reporting on any identified issues.
- Documenting change requests on the integration requirements from the end users.

DSI.2 Data Sharing Agreements

DSI.2.1 The entity shall develop and implement a Data Sharing Agreement Template for creating a contractual agreement with parties for internal (in case the data providers and consumers are from different departments of the same entity) and external data sharing. The template, at minimum, shall include the following fields:

- Purpose of the data sharing request.
- Legal basis (statute or royal decree) for data sharing request allowing the entity to share data or signed agreements).
- Declaration of the technical and security measures available at the requestor's end for ensuring data protection.
- Minimum volume of data required to achieve the purpose of the data sharing request.
- Requirements for data to be shared namely, data format, data accuracy, level of detail, data structure, data type, masking, anonymization (in case of Personally Identifiable Information (PII) data) and aggregation.
- Liability Provisions in case of non-compliance with the provisions of the data sharing agreement.
- Restrictions on data usage and sharing with third parties.

DSI.2.2 The entity shall ensure that it is the producer of the requested data to establish that the data is being requested from the right source.

DSI.2.3 The entity receiving the data shall comply with the data classification level stipulated by the originating entity.

DSI.2.4 The entity shall ensure that data is appropriately classified among Top Secret, Secret, Restricted, Confidential, Unclassified before sharing it internally or externally.

DSI.2.5 The data sharing agreement shall include a clause that prohibits data requestors from making copies of shared data or sharing the data received without the consent of the producer of the data. Exceptions (if any) shall be explicitly mentioned in the data sharing agreement.

DSI.2.6 The data sharing agreement shall be signed by the relevant executives before data is shared.

DSI.2.7 The entity shall give priority to approved and secure sharing media for exchanging data

DSI.2.8 In case of sharing of personal data, the identity of the data subjects shall be anonymized, unless the identity is necessary for the purpose of sharing. Necessary controls shall be maintained to protect the privacy of the data subjects in accordance with the 'Personal Data Protection Policy'.

DSI.2.9 A process shall be developed and followed as per the SLA stipulated in the 'National Data Strategy' for the assessment and fulfillment/rejection of the external data sharing requests. The entity sharing the data may stipulate the conditions for agreeing to the data sharing request such as the data retention rules for the data being shared etc.

DSI.2.10 A record of data sharing requests received, and the decisions made against them shall be developed and maintained.

DSI.2.11 The entity shall periodically review and update the data sharing agreements to incorporate any changes in the contractual requirements.

DSI.2.12 A mechanism shall be created and followed for receiving and routing the internal and external data sharing requests to the appropriate roles as per the responsibilities outlined in the 'Data Governance and Management Office Establishment Guidelines'.

DSI.3 Data Sharing Automation Tool

DSI.3.1 The entity shall evaluate and adopt a tool as per its solution integration design to automate the internal and external data sharing as workflows. The workflows at minimum, shall include the following:

- Assessment and fulfillment/rejection of the data sharing requests as per pre-defined rules.
- Automated routing of the data sharing requests to the appropriate roles.
- Data Sharing tool access management.

10.4 Roles and Responsibilities Matrix

Key Activities	Data Governance and Management Head	Data Governance and Compliance Officer	Data Management Officer	Data Owner	Business Data Steward	IT Data Steward	Enterprise Data Architect
Develop the integration requirements document.	I	I	R	I	C	R	A
Create the target integration architecture.	I	I	C/I	I	C	R	A
Develop the solution integration design.	I	I	C/I	I	C	R	A
Test the developed integration solution.	I	I	R	A	C	R	C/I
Monitor and maintaining the developed integration solution.	I	I	R	A	C	R	C/I
Develop the data sharing agreement template.	A	R	I	C/I	C/I	-	-
Develop a process for the assessment and fulfillment/rejection of the external data sharing requests.	A	R	C	C/I	C/I	I	-
Approve process for the assessment and fulfillment/rejection of the external data sharing requests*.	A/R	I	I	I	I	I	-
Review and update the data sharing agreements.	I	C/I	I	A	R	I	-
Data sharing integration.	I	I	I	A	R	R	C/I

R – Responsible, A – Accountable, C – Consulted, I – Informed

* Approval shall be provided by the Data Governance Committee

10.5 Dependencies

- Data Governance Policy.
- Data Classification Policy.

10.6 Policy Enforcement and Compliance

- The Data Governance and Management Head shall be responsible for implementing and enforcing the data sharing and integration policy within their respective entities.
- MTCIT shall be responsible for assessing the compliance of the government entities to the data sharing and integration policy.

11.0

Data Analytics Policy

11.0 Data Analytics Policy

11.1 Policy Objectives and Scope

The objective of this policy is to enhance the decision-making capabilities of the entities along with improving their efficiency and productivity.

The policy provides the requirements for the government entities to systematically adopt practices aimed at deriving actionable insights from raw data such as analytics business case identification, implementation, and adoption of tools for automating analytics activities which are as follows:

11.2 Policy Principles

- **A data-driven culture is encouraged:**

  Establish processes and develop skills required for entities to utilize their data, derive meaningful insights, and leverage technology to improve their decision making and operational efficiency.

11.3 Policy Statements

AN.1 Business Cases

AN.1.1 The entity shall identify and create an exhaustive list of its analytics business cases (including potential business cases for advanced analytics) across the entity's business functions. The business case definition shall at minimum include the name, description and the business functions involved in implementing the business cases.

AN.1.2 A business case prioritization matrix shall be created to prioritize the exhaustive list of analytics business cases. The matrix shall at minimum have the following criteria:

- Alignment to the business objectives of the entity.
- Feasibility of implementation.
- Financial impact due to implementation.
- Business benefits due to implementation including the targeted Return On Investment (ROI).
- Technical complexity of implementing the business case.

AN.1.3 The business cases shall be shortlisted based on their feasibility and validity as determined from the technical complexity (including the needed tools), required skillset etc.

The entity shall obtain approval on the shortlisted business cases for their implementation.

AN.1.4 The exhaustive list of analytics business cases shall be periodically reviewed and updated.

AN.2 Data Analytics Implementation

AN.2.1 The entity shall document the requirements for the approved business cases. The requirements, at minimum, shall include the following:

- The objective of the business case.
- The required data and its sources.
- The required quality of data.
- The expected business value through the development of the business case.
- The type of analytics (prescriptive, descriptive, diagnostic, predictive) to be utilized.
- Performance, usability, and workflow requirements.
- Technologies required for implementing the business case including the data storage, processing, and integration requirements.
- Criteria for successful implementation of the business case.

AN.2.2 The entity shall develop a plan and obtain approval for implementing the approved analytics business cases. The plan shall at minimum, include the following activities:

- Detailing the functional and non-functional requirements for translating the business case objectives into analytics requirements including the scope and acceptance criteria.
- High-level conceptual design of the analytics solution
- The environments for hosting the analytics solution during and after the development.
- Developing the functional and non-functional requirements to meet the high-level conceptual design.
- Testing the developed solution as per the defined scope and acceptance criteria.
- Deployment timeline/schedule for establishing a pilot and/ or delivery of the business case.
- Required personnel within the entity that possess the necessary skills to execute the business case.
- Availability and quality of the required data.
- The data management activities (acquisition, integration, quality check, enrichment, storage, processing etc.) required to deliver the analytics business case.

AN.2.3 The entity shall implement and validate the outcomes of the implemented analytics business cases. The validation activities, at minimum, shall include the following:

- Functional and non-functional requirements.
- Personal Data Protection considerations.
- Validation of business impact including the ROI as per the target set.

AN.2.4 The outcomes shall be documented, and the benefits delivered shall be socialized to all the relevant stakeholders.

AN.3 Data Analytics Tools

AN.3.1 The entities shall adopt and onboard a data analytics tool for automated insight generation and reporting. The features of the tool, at minimum, shall include the following:

- Automated visualization and reporting of metrics as per defined frequency.
- Support integration with a variety of data sources. The data sources, at minimum, shall include databases, data warehouses, data lakes, cloud storage, data streams and files.
- Capability to support creation of workflows for data collection, transformation and enrichment, analysis and reporting to enable collaboration among the data analytics roles.

AN.4 Data Platforms

AN.4.1 The entity shall onboard and adopt data platforms that support implementation of advanced analytics initiatives. The platforms, at minimum, shall support the following features:

- Integration with various data sources namely, databases, data warehouses, data lakes, data lakehouses, cloud storage, data streams and files.
- Data profiling and remediation workflows to handle missing values along with identification of the data quality dimensions.
- Data enrichment capabilities through integration with third-party tools.
- Capabilities for advanced statistical analysis namely, regression, clustering, time series analysis and predictive modeling.
- Self-service reporting that enables users to create custom reports as per requirements.
- Capability to handle large data volumes along with high performance ability.
- Capability to support creation of workflows for data collection, transformation and enrichment, analysis and reporting to enable collaboration among the data analytics roles.

11.4 Roles and Responsibilities Matrix

Key Activities	Data Governance and Management Head	Data Governance and Compliance Officer	Data Management Officer	Data Owner	Business Data Steward	IT Data Steward
Development and maintenance of the analytics business cases.	A	C/I	R	C/I	R	I
Prioritization and shortlisting the Analytics business case.	A	C/I	R	C/I	R	C/I
Approving the shortlisted analytics business case*.	A/R	I	C/I	C/I	C/I	I
Detailing the requirements of the analytics business case.	C/I	C/I	R	A	R	R
Development of the business case implementation plan.	A	I	R	C/I	C/I	R
Approval on the business case implementation plan*.	A/R	I	C/I	C/I	C/I	I
Implementing and validating the outcomes of the analytics business cases.	A	I	R	I	C/I	R
Onboarding the data analytics tools and data platforms.	A	C/I	C/I	C/I	C/I	R
Implementing the data analytics tools and data platforms.	A	C/I	R	C/I	C/I	R

R – Responsible, A – Accountable, C – Consulted, I – Informed

* Approvals shall be provided by the Data Governance Committee

11.5 Dependencies

- Data Governance Policy.
- Data Catalog Policy.
- Data Quality Policy.
- Data Architecture Policy.
- Reference and Master Data Policy

11.6 Policy Enforcement and Compliance

- The Data Governance and Management Head shall be responsible for implementing and enforcing the data analytics policy within their respective entities.
- MTCIT shall be responsible for assessing the compliance of the government entities to the data analytics policy.

12.0

Open Data Policy

12.0 Open Data Policy

12.1 Policy Objective and Scope

The objective of the policy is to foster informed decision making by encouraging usage of public data, establish a knowledge-based society and create an environment of data trust and transparency.

The policy provides requirements for government entities to establish standardized practices for identifying and publishing their public data for the general public's usage.

12.2 Policy Principles

- **Unmodified**

  Open data assets shall be provided from the source without modification or summarization.

- **Up to date:**

  Open Data assets released by the government entities shall be periodically updated (semi-annually or at least annually), depending on the nature of the data asset and shall be published immediately upon collection.

- **Permanent**

  Open data assets shall be made available permanently with appropriate version tracking and archiving the older versions over time. An indication that an alteration has been made shall be marked on the open data asset.

- **Accessible**

  Open data assets shall be easily accessible and shall be easily downloadable. The interface shall allow users to bulk download and provide a means to request additional data through Application Program Interface (API).

- **Trusted**

  Open data assets shall be digitally signed or include an attestation of publication/creation date, authenticity and integrity.

- **Documented**

  Open data assets shall be documented with sufficient information to make the data assets meaningful and useful to the users. This information shall be provided on the entity's websites.

- **Non-discriminatory**

  Open-data assets shall be available to anyone, at any time without having to identify themselves or provide any justification for accessing open datasets.

- **Non-proprietary**

  Open data assets shall not have any restrictions on their usage and shall not be subject to copyright, trademark, patent or trade secrets provided the government entities use the open government license to clarify the terms of use.

- **Machine readable**

  Open data assets shall be available in widely used machine readable formats (XML, JSON, XLS, CSV) or any format that is consistent with the international requirements for open data.

- **Free of charge**

  All open data assets shall be published free of charge.

12.3 Policy Statements

OD.1 Open Data Identification

OD.1.1 The entity shall identify all its 'Unclassified' data assets marked 'FOR PUBLIC RELEASE' as Open Data, in alignment with its data classification policy and the Article 28 of the 'National Data Strategy'.

OD.1.2 A process for identification of Open Data assets from among the inventory of data assets shall be developed and followed by the entities. The process, at minimum, shall include the following steps:

- Prioritization of the data assets as per their importance to be published as open data.
- Identification of data sources for the data assets including the associated metadata. The entity's data catalog may be leveraged for this purpose.
- Impact assessment on the data assets (along with related metadata) for identifying their potential to be classified as open data.
- Evaluating alignment of the open data assets with the outlined policy principles.
- Certification of the identified open data assets.

The entity shall obtain approval on the process for identifying its open data assets.

OD.1.3 A list of all the identified and certified open data assets shall be created. The list, at minimum, shall include the following information:

- Name of the open data asset.
- The data sources for the open data asset.
- Log of open data publishing and modification activities on the corresponding open data assets.
- The executive role within the entity responsible for certifying the open data.

OD.2 Open Data Publishing

OD.2.1 The entity shall publish all its identified open data assets within their official websites as per the specifications under the Open Government License while adding the © symbol with the entity's name on the website page without using the phrase "All rights reserved".

OD.2.2 The entity shall develop a standard structure for publishing[7] its open data assets. The structure, at minimum, shall have the following attributes:

- Name of the open data asset.
- Descriptive information necessary to describe the open data for the understanding of the public.
- Department responsible for the open data.
- The date on which the open data asset was last reviewed and updated.

OD.2.3 The entity shall develop a register of the open data that is published. The register shall at minimum include the following information:

- Name of the open data asset
- Information about the open data asset i.e., metadata
- Name of the person or department responsible for the data asset within the government entity
- Format of the published data asset (XML, JSON, XLS, CSV)
- Schedule for updating the data asset.

OD.2.4 The entity shall periodically evaluate the possibility of marking data as 'Unclassified' to make additional data available for public release as open data.

OD.2.5 A channel shall be developed on the websites of the entities and operationalized for receiving public requests of sharing additional data.

OD.2.6 A process shall be developed for assessing and responding to the public requests of sharing additional open data assets. The process, at minimum, shall include the following steps:

- Receipt and acknowledgement of the open data sharing request.
- Communication of the assessment outcome (accepted/rejected) to the requestor along with justification within 15 working days.
- Making the requested additional open data available to the requestor in case the request is accepted.

OD.2.7 Open data assets shall be published by adhering to the standard formats consistent with the principles of open data policy.

OD.2.8 Periodic review and maintenance of the published open data assets shall be carried out by the entities to ensure adherence to the relevant regulatory requirements.

OD.2.9 An automated tool shall be leveraged by the entities to implement the processes of open data identification and publishing as automated workflows.

OD.2.10 Processes for open data identification and publishing shall be implemented as automated workflows within the automated tool.

12.4 Roles and Responsibilities Matrix

Key Activities	Data Governance and Management Head	Data Governance and Compliance Officer	Data Management Officer	Data Owner	Business Data Steward	IT Data Steward
Identifying open data assets.	I	C/I	C/I	A	R	I
Developing the process for open data identification.	A	R	I	C/I	C/I	I
Approve open data identification process*.	A/R	I	C/I	C/I	C/I	I
Developing and maintaining the list of open data assets.	I	C/I	C/I	A	R	I
Developing the plan for publishing the open data assets.	A	R	R	C/I	C	I
Approving the plan for publishing the open data assets*.	A/R	C	I	I	I	I
Developing standard structure for publishing open data assets.	A	R	C/I	C	C	I
Publishing the open data assets.	A	R	R	C/I	C/I	R
Developing register of published open data assets	A	R	R	C/I	C/I	R
Developing a process for receiving additional open data public requests.	A	R	I	C/I	C/I	I
Reviewing and maintaining the published open data assets.	A	R	R	C/I	C/I	R
Implementing workflows for open data identification and publishing in the automated tool.	A	C/I	R	I	C/I	R

R – Responsible, A – Accountable, C – Consulted, I – Informed

* Approvals shall be provided by the Data Governance Committee

12.5 Dependencies

- Data Governance Policy.
- Data Classification Policy.

12.6 Policy Enforcement and Compliance

- The Data Governance and Management Head shall be responsible for implementing and enforcing the open data policy within their respective entities.
- MTCIT shall be responsible for assessing the compliance of the government entities to the open data policy.

13.0

Reference and Master Data Policy

13.0 Reference and Master Data Policy

13.1 Policy Objective and Scope

The objective of this policy is to enable the data consumers access a single authoritative version of all the data that is shared or duplicated across the entity's systems.

The policy provides requirements for the government entities to establish processes and systems for creating and orchestrating the authoritative version of all the data that provides context to business activities.

13.2 Policy Principles

- **Data is trusted by all stakeholders:**

  Establish practices for providing reliable, accurate and fit for purpose data to build data trust and confidence thereby, facilitating informed decision making.

13.3 Policy Statements

RMD.1 Reference Data Management

RMD.1.1 The entity shall identify and create a list of reference data objects that are utilized within its business processes based on the analysis of the data catalog and existing data models.

RMD.1.2 The entity shall review its existing information system landscape and identify the systems where the reference data objects are read.

RMD.1.3 Processes for creating, updating, and deleting/archiving the reference data shall be developed and followed. The entity shall obtain approval on the processes for their implementation.

RMD.1.4 Ownership and stewardship roles shall be assigned to the relevant stakeholders for managing the reference data within the entity.

RMD.1.5 The reference data shall be added as metadata within the entity's business glossary.

RMD.1.6 The entity shall periodically review and update the list of reference data objects as per their usage status within the entity's business processes.

RMD.1.7 The entity shall maintain a version control to ensure traceability of all the updates made to the list of reference data objects.

RMD.2 Master Data Management

RMD.2.1 The entity shall identify and create a list of master data objects that are utilized within its business processes based on the analysis of the data catalog and existing data models.

RMD.2.2 The entity shall review its existing information system landscape and identify the systems where the master data objects are created, read, updated, or deleted.

RMD.2.3 Processes for creating, updating, and deleting/archiving the master data shall be developed and followed. The entity shall obtain approval on the processes for their implementation.

RMD.2.4 Ownership and stewardship roles shall be assigned to the relevant stakeholders for managing the master data within the entity.

RMD.2.5 The master data shall be defined as a metadata attribute within the entity's business glossary.

RMD.2.6 The entity shall periodically review and update the list of master data objects as per their usage status within the entity's business processes.

RMD.2.7 The entity shall maintain a version control to ensure traceability of all the updates made to the list of master data objects.

RMD.3 Reference and Master Data Automation Tool

RMD.3.1 The entity shall identify the requirements for creating and provisioning the authoritative data to the target systems. The requirements, at minimum, shall include the following:

- Data sources to be integrated.
- Target systems consuming the authoritative data.
- Data quality rules to be enforced.
- The required integration and orchestration patterns.

RMD.3.2 The entity shall, based on its requirements, evaluate, and select a suitable reference architecture pattern from among Consolidation, Registry and Coexistence architecture patterns for designing the Reference and Master Data hub (RMD hub).

RMD.3.3 The entity shall design a solution architecture based on the reference architecture pattern selected. The solution architecture, at minimum, shall include the following:

- The Create, Read, Update, and Delete (CRUD) matrix for defining the master data sources.
- Master data records between the data sources and the RMD hub.
- Authoritative records between the data hub and target systems.
- Reference data between data hub and consuming applications.
- The conceptual, logical, and physical data models including hierarchy and relationships between the master data tables reference and Master Data hub (RMD hub). List of reference data tables.
- The data dictionary containing the description of the master data elements along with the source to target transformation logics and Delete (CRUD) matrix for defining the master data sources.

RMD.3.4 The entity shall evaluate and onboard a reference and master data automation tool to implement the solution architecture design and provide authoritative records to the target systems. The tool implementation, at minimum, shall include the following requirements:

- Data quality rules to be enforced to ensure data accuracy and up to date data.
- Technical and security controls to monitor the access to the authoritative data.

RMD.3.5 A version control shall be implemented in the tool for maintaining an audit trail of all the updates made to the reference and master data records.

13.4 Roles and Responsibilities Matrix

Key Activities	Data Governance and Management Head	Data Governance and Compliance Officer	Data Management Officer	Data Owner	Business Data Steward	IT Data Steward	Enterprise Data Architect
Identifying, developing and maintaining the list of reference and master data objects.	-	I	C/I	A	R	C	-
Developing processes for creating, updating, deleting/archiving the reference and master data objects.	A	R	C/I	C/I	C/I	I	-
Approve processes for creating, updating, deleting/archiving the reference and master data objects*.	A/R	C/I	C/I	C/I	C/I	I	-
Documenting requirements for creating and provisioning authoritative data.	-	I	C/I	A	R	I	-
Evaluating and selecting suitable reference architecture pattern.	A	C/I	C/I	C/I	C/I	R	R
Designing the solution architecture diagram for reference and master hub.	A	I	C/I	I	I	R	R
Evaluating and onboarding a reference and master data automation tool.	A	C/I	R	I	I	R	C/I
Implementing the reference and master data management processes as automated workflows.	A	C/I	R	C/I	C/I	R	-

R – Responsible, A – Accountable, C – Consulted, I – Informed

*Approvals shall be provided by the Data Governance Committee

13.5 Dependencies

- Data Governance Policy.
- Data Quality Policy.

13.6 Policy Enforcement and Compliance

- The Data Governance and Management Head shall be responsible for implementing and enforcing the reference and master data policy within their respective entities.
- MTCIT shall be responsible for assessing the compliance of the government entities to the reference and master data policy.

14.0

Data Monetization Policy

14.0 Data Monetization Policy

14.1 Policy Objective and Scope

The objective of Data Monetization policy is to create tangible economic benefits within the government entities in terms of revenue generation or cost optimization through their data assets.

The policy provides requirements for the government entities within the Sultanate of Oman to identify and leverage business cases aimed at creating new revenue streams or optimizing operational costs.

14.2 Policy Principles

- **Data is a national asset:**

  Develop practice that enable realization of the inherent value of data as a national asset to drive innovation and unlock economic growth through data integrity, monetization, transparency, and accountability.

- **A data-driven culture is encouraged:**

  Establish processes and develop skills required for entities to utilize their data, derive meaningful insights, and leverage technology to improve their decision making and operational efficiency.

14.3 Policy Statements

DM.1 Revenue Streams Creation

DM.1.1 The entity shall conduct a data monetization opportunity assessment to identify and document an exhaustive list of data products for revenue streams creation by leveraging its data.

DM.1.2 Business cases shall be developed for the identified data products. The business case, at a minimum, shall include the following:

- Targeted segment/s and market size.
- Benchmarking analysis on the associated trends.
- Estimated costs and revenue.

The entity shall obtain approval on the business cases for implementation.

DM.1.3 The entity shall develop data product designs for the approved business cases. The data product designs, at a minimum, shall include the following:

- Functional and non-functional requirements.
- Data and technical architecture of the data products.
- Data product business model including identification of the targeted customers, partnership for development of data product, data product sale model (subscription based, freemium, one-time payment etc.).

DM.1.4 The entity shall determine the price for each of the designed data products. The price of the data products shall only be charged from non-government entities that are using the data products. The following, at minimum, shall be considered for determining the product price:

- Expected demand for the data product.
- Benchmark price as per the market analysis.
- Expected cost.

The entity shall get the pricing model reviewed and obtain approval for its implementation.

DM.1.5 A financial plan shall be developed for estimating the commercial feasibility of developing and operationalizing the data product. The plan shall at minimum, include the following:

- Addressable market size.
- Expected revenue.
- Return on Investment (ROI) and Payback period.

The entity shall get the financial plan reviewed and obtain approval for its implementation.

DM.1.6 The entity shall define a charging model for each of the shortlisted data products intended to generate revenue. The charging models shall be selected from the following:

- Consumption-based model: Charging dependent on consumer's usage of data products.
- Freemium/premium model: Offering basic features free and charging for the premium features.
- Subscription model: Charging based on monthly recurring fees.
- One-time free model: Charging one-time fee from consumers for the data products.

The entity shall get the charging model reviewed and obtain approval for its implementation.

DM.1.7 The implemented data products shall be periodically monitored and enhanced to achieve the required ROI within the calculated payback period.

DM.2 Cost Optimization

DM.2.1 The entity shall identify the opportunities to leverage its data to streamline its operations across functions. For example:

- Automating workflows to limit repetitive operations and avoiding errors.
- Optimizing service delivery, reducing bottlenecks, and enhancing citizens satisfaction.

DM.2.2 The entity shall leverage its data to identify opportunities for enhancing its strategic decision making. For example:

- Optimizing resource allocation across operations.
- Energy consumption optimization in public places.
- Optimizing procurement and contract costs.
- Route optimization and fleet management for public transportation.

DM.2.3 The outcomes from the implementation of the identified opportunities shall be periodically monitored and enhanced.

14.4 Roles and Responsibilities Matrix

Key Activities	Data Governance and Management Head	Data Governance and Compliance Officer	Data Management Officer	Data Owner	Business Data Steward	IT Data Steward
Identify revenue streams creation opportunities.	I	I	C/I	A	R	-
Approve data products for revenue streams creation*.	A/R	-	I	C/I	I	-
Development of business cases.	I	I	I	A	R	C/I
Development of data product designs.	I	I	I	A	R	I
Determine price of the data products.	C/I	I	I	A	R	-
Development of financial plan for the data products.	C/I	I	I	A	R	-
Approve financial plan for the data products*.	A/R	I	I	C/I	I	-
Development of charging models for the data products.	C/I	I	I	A	R	-
Approve the price and charging model of the data products*.	A/R	I	I	C/I	I	-
Identify the cost optimization opportunities.	I	I	C/I	A	R	-

R – Responsible, A – Accountable, C – Consulted, I – Informed

*Approvals shall be provided by the Data Governance Committee.

14.5 Dependencies

- Data Governance Policy.
- Data Analytics Policy.
- Data Architecture Policy.

14.6 Policy Enforcement and Compliance

- The Data Governance and Management Head shall be responsible for implementing and enforcing the data monetization policy within their respective entities.
- MTCIT shall be responsible for assessing the compliance of the government entities to the data monetization policy.

15.0

Freedom of Information Policy

15.0 Freedom of Information Policy

15.1 Policy Objective and Scope

The objective of this policy is to set forth fundamental requirements for governing the accessibility of unpublished official information to public, with the aim of promoting transparency and fostering growth.

The policy establishes standardized requirements for government entities within the Sultanate of Oman to grant access to unpublished official information to the public. It outlines the mechanism for the citizens to request such information along with addressing grievances in the event of disputes.

15.2 Policy Principles

- **Data is a national asset:**

  Develop practice that enable realization of the inherent value of data as a national asset to drive innovation and unlock economic growth through data integrity, monetization, transparency, and accountability.

15.3 Policy Statements

FOI.1 Information Request Management

FOI.1.1 The entity shall develop and obtain approval for the process of managing the request to access entity's unpublished official information.

FOI.1.2 The entity shall establish methods including both paper-based and electronic formats, for requesting access to or obtaining unpublished official information.

FOI.1.3 Identity of the individuals shall be verified before granting access to the requested unpublished official information.

FOI.1.4 The entity shall make the information request forms available on its official website, for requesting access to the entity specific unpublished official information. The request form shall include, at minimum, the following:

- Name of the Requestor.
- Civil Identification Number of the Requestor.
- Contact information of the requestor.
- Purpose of the information request.

FOI.1.5 The entity shall review the requested information within a month of its receipt and notify its decision to either approve, deny or intimate an extended timeline for the response. The entity shall obtain approval on the notification before being sent to the requestor.

FOI.1.6 Charges for processing information requests, shall be standardized.

FOI.1.7 In case of denial of a request, the requestor shall be notified of the reasons for denial along with instructions to initiate grievance, if any.

FOI.1.8 The entity shall ensure a balance between right to access information and considerations such as national security and the protection of personal data while responding to public requests for accessing unpublished official information.

FOI.2 Issue and Grievance Management

FOI.2.1 The entity shall develop a process for handling the issues and grievances raised by the requestor based on the received information. The process shall include an activity to review the decisions on issues and grievances by the data governance committee to ensure they are transparent, and free from undue influence or bias.

FOI.2.2 Decisions on issue and grievance shall be communicated to the requestor in writing, providing reasons for the decision and information on further recourse, if available.

FOI.2.3 The entity shall maintain a register to document the information requests along with the corresponding information or responses shared.

15.4 Roles and Responsibilities Matrix

Key Activities	Data Governance and Management Head	Data Governance and Compliance Officer	Data Management Officer	Data Owner	Business Data Steward	IT Data Steward
Develop information request process along with the form.	A	R	C/I	C/I	C/I	I
Approve information request process along with the form*.	A/R	I	I	I	I	I
Manage freedom of information requests.	A	C	C	R	R	I
Review and approve freedom of information requests responses.	A/R	I	I	C/I	C	-
Develop a process for handling the issues and grievances raised by the requestor	A	R	C/I	C/I	C/I	I
Approve the process for handling the issues and grievances raised by the requestor*.	A/R	I	I	I	I	I
Manage freedom of information requests issues and grievances.	A	C	C	R	C/I	I

R – Responsible, A – Accountable, C – Consulted, I – Informed

*Approvals shall be provided by the Data Governance Committee.

15.5 Dependencies

- Data Governance Policy.
- Data Classification Policy.

15.6 Policy Enforcement and Compliance

- The Data Governance and Management Head shall be responsible for implementing and enforcing the freedom of information policy within their respective entities.
- MTCIT shall be responsible for assessing the compliance of the government entities to the freedom of information policy.

16.0

Personal Data Protection Policy

16.0 Personal Data Protection Policy

16.1 Policy Objective and Scope

This policy aims to achieve a number of objectives, including:

- Benefiting from the value of data as an economic resource that helps innovation and contributes to supporting economic transformations.
- Improving the data subject's confidence in the ability of government entities to act and deal with personal data by maintaining it in accordance with the provisions of relevant laws and policies.
- Applying international best practices for personal data protection policies and controls and enhancing the value derived from it in improving performance, productivity, and ease of providing public services.
- Creating a framework that balances mechanisms for individuals' rights to protect their personal data, with permission to process and retain data in cyberspace, and the spread of the concepts of big data and artificial intelligence.

This policy seeks to establish a set of controls to protect personal data, including its processing, storage, disclosure, access, modification, and access to it. This policy applies to the units of the state's administrative apparatus.

16.2 Policy Principles

- **Data practices are compliant with regulatory requirements:**

  Develop data governance and management practices that uphold the regulatory requirements to ensure lawful, ethical, and responsible handling of data across the business processes of the entities.

16.3 Policy Statements

PDP.1 Controlling Entity Obligations

PDP.1.1 The controlling entity shall commit to protect all the information and personal data in its possession, including the information and data received from other units, or those that have been disclosed to other units.

PDP.1.2 When processing personal data, the controlling entity shall at minimum consider the following:

- Data is collected through legitimate and fair means and that the collection is limited to what is necessary to meet its legal requirements or related to its direct business activity.
- Data processing is fair and lawful.
- Data is true and accurate and is updated when necessary.
- Data does not remain in a form that allows the data subject to be identified after the purpose for which it was collected or for which subsequent processing is carried out has been exhausted.

PDP.1.3 The controlling entity shall request to obtain the minimum amount of data and documents from the data subject to complete service transactions, in the event that they are not available electronically or are not available for electronic circulation with any other government unit.

PDP.1.4 The controlling entity shall implement security and organizational measures to protect data from accidental or unauthorized destruction or accidental loss, or from unauthorized alteration, disclosure, hacking, or any other form of processing.

PDP.1.5 The controlling entity shall establish adequate security precautions for all systems and storage media involved in dealing with data to prevent any type of hacking.

PDP.1.6 In cases where the processing unit or any third party assigned to process personal data, the controlling unit shall at minimum ensure the following:

- The processing unit/third party provides adequate guarantees regarding the application of the technical and organizational measures that must be considered when processing data and takes the necessary steps to verify compliance with them.

- The processing shall be carried out in accordance with a written contract concluded between the controller and the processing unit/third party that processes the data on its behalf or under its supervision.
- Clear stipulations are included in the contract regarding retention periods and arrangements for deleting data sent or received.

PDP.1.7 The controlling unit shall disclose acquired or updated data with the third-party processing unit - as long as there is a clear and valid purpose for the disclosure in accordance with legal obligations and privacy considerations.

PDP.1.8 The controlling entity shall display a privacy notice on its website to provide the data subjects with information on their personal data collection, its processing. The privacy statement shall at minimum include the following:

- The purpose of collecting personal data.
- Whether collecting all or some of it is mandatory or optional.
- Information to the data subjects that their personal data will not be processed in a way that is inconsistent to the purpose of collecting it.
- The types of personal data that will be collected.
- The means used to collect, process, store and dispose the personal data.
- The unit or units to which the personal data will be disclosed, its description, and whether the personal data will be transferred, disclosed, or processed outside the Sultanate.
- Potential consequences and risks of not completing the personal data collection procedure of the entity.

PDP.1.9 The privacy notice shall inform the data subjects of their rights over their personal data collected by the entities. The following rights shall be included in the privacy notice:

- The right to information, including being informed of the purpose of collecting data.
- The right to access their personal data available to the controlling entity in accordance with the relevant regulations and policies.
- The right to request access to their personal data available to the controlling entity in a legible and clear format.
- The right to request the correction, completion or updating of personal data available to the controlling entity.

PDP.1.10 The controlling entity shall establish mechanisms to ensure the safe destruction of personal data in order to prevent unauthorized parties from accessing the data.

PDP.1.11 The controlling entity shall notify the Electronic Defense Center in the event of any leakage, damage or hacking of personal data.

PDP.1.12 The controlling entity shall process the personal data within the geographical borders of the Sultanate to ensure national sovereignty over personal data and the protection of privacy of the data subjects. Exceptions to the transfer or processing of personal data if any, shall be only for the following cases:

- Execution of a contract outside the geographical borders of Oman to which the data subject is a party.
- Initiating procedures to claim or defend legal rights.
- Protecting the vital interests of the data subject.

PDP.1.13 The controlling entity shall obtain the approval of the Electronic Defense Center before transferring personal data outside the geographical borders of the Sultanate of Oman for the purpose of processing it.

PDP.2 Third Party Processing Unit Obligations

PDP.2.1 The third-party processing unit shall at minimum, commit to the following:

- Protecting all the information and personal data in its possession, including information and data received from other units, or those that have been disclosed to other units.
- The processing unit or third party shall not undertake any processing except in accordance with the instructions of the controlling entity.

16.4 Roles and Responsibilities Matrix

Key Activities	Data Governance and Management Head	Data Governance and Compliance Officer	Data Management Officer	Data Owner	Business Data Steward	IT Data Steward	Data Protection Officer
Develop the consent statement and privacy notice.	I	C	C/I	I	I	I	A/R
Develop the process for notifying leakage, damage or hacking of personal data.	I	C	C/I	C/I	C/I	I	A/R
Developing the contract for third party personal data processing.	I	C/I	I	C/I	C/I	I	A/R
Developing mechanism of ensure the safe destruction of personal data	-	C/I	I	C/I	C/I	I	A/R

R – Responsible, A – Accountable, C – Consulted, I – Informed

16.5 Dependencies

- Data Governance Policy.
- Data Catalog Policy.
- Data Classification Policy.
- Data Operations Policy.

16.6 Policy Enforcement and Compliance

- The policy will come into effect 24 months after the date of its adoption and circulation by the Ministry of Transport, Communications, and Information Technology.
- The Ministry of Transport, Communications and Information Technology is responsible for monitoring the compliance of the government entities to the policy and presenting the results of compliance to the Council of Ministers.

17.0

Appendices

17.0 Appendices

17.1 Appendix 1 – Document and Content Management related policies

Domain	Policy/Law Name	Policy/Law Summary	Publishing Entity	Published Date
Document and Content Management	Documents and Archives Law pursuant to the amendment issued pursuant to Royal Decree No. 52/2022	Describes the various stages of the document lifecycle- **current, intermediate, and final fate** based on the entity specific document retention periods for each stage.	National Records and Archive (NRAA)	2nd July 2007

17.2 Appendix 2 - References

The following references shall be consulted wherever applicable for the policy statements within this document:

- **National Data Strategy:** For aligning to the responsibilities of the Data Governance and Management Office.
- a) **National Data Strategy:** For data quality dimensions of accuracy, completeness, availability (coverage) and timeliness.

  b) **Open Government Data Policy:** For the data quality dimensions of completeness and timeliness.
- **Database Security Standards:** For defining the database access process.
- **IT Governance Charter:** For defining the SLAs for tracking database performance.
- **ICT Service Continuity Policy:** For developing the disaster recovery plan.
- **IT Governance Charter:** For the design principles to guide the development of the data architecture.
- **Open Government Data Policy:** For the specifications on the attributes, principles, and file formats for publishing open datasets.
- **National Procedures Guide for Document and Electronic Document Management:** For specifications related to metadata of the data catalog and data architecture policy.