Data Governance Policy

Document History:

Date	Revision	Comments
09-May-2023	2.0	Reviewed the policy and enhanced the data governance controls in line with the NDMO Guidelines

Approved by:

Name	Title	Date	Signature
Mohammed Alhakbani	CEO	09-May-2023	

Validated by:

Name	Title	Date	Signature
Richard Ltaif	CSGO	21-Mar-2023	
Saeed Alshehri	COO	13-Mar-2023	

Developed / Reviewed by:

Name	Title	Date	Signature
Teruyuki Ito	Data Analytics Lead Specialist	12-Feb-2023	

Distribution / Target Audience:

- TAWAL employees.

Revision History

Date	Revision Number	Description of change	Page Nos	Author
21-Jun-2020	1.0	Initial release.	All	QA
09-Sep-2022	1.1	Annual revision, no changes done.	All	QA
05-Feb-2023	2.0	The following change has been made: 1. Added a data classification matrix in topic 6.3.5 and defined the impact value as per NDMO Control guidelines.	23	QA (as a part of the Agility Project) Supported by the T&I team

Table of Contents

1. Objective

The objective of the Data Governance Policy is to provide guidelines on implementing, managing, and maintaining data as a valuable strategic asset across the Company. The policy ensures that data is accurate, consistent, complete, available, secure, and protected.

2. Scope

The scope of the Data Governance Policy includes all data processed and/or controlled by the company on all media and system platforms through any communication channel.

3. Definitions

- **Access**

  The user, system, or process is considered to have access to data if it has one or more of the following privileges:

  a) the ability to read or view the data.
  b) create new data.
  c) delete data or the ability to make a copy of the data.

  Access can be provided either continually or, alternatively, on a one-time or ad hoc basis.

- **Aggregation**

  Rare indirect identifiers (quasi) can be aggregated to provide better de-identification or anonymization.

- **Anonymization**

  A process that is intended to irreversibly remove the association between a subject and information that can identify the subject.

- **BRSD – Business Request Specification Document**

  It is the document that clearly defines business request specifications to cater to the business need. The business request specification document defines the requirements related to the project, product, or system. It is a document that details business requirements.

- **BU**

  Business Units of TAWAL – like Operations, Finance, Commercial, Human Resources, and Network. etc.

- **Business Glossary**

  Business Glossary is a dictionary that provides the names and definitions of all data elements within TAWAL.

- **Business Metadata**

  Business metadata is information about the data used for business assets i.e., business definitions, business terms, KPIs, formulas, business rules, usage, purpose, impact, etc. Business metadata includes the definition, examples, business rules, and policies for the business taxonomies used by TAWAL. It defines the semantics of a business concept.

- **Change Data**

  Change Data means any changes requested that have an impact on data in the following ways:

  a) Data Structure changes.
  b) Data Content changes.
  c) System changes that may directly or indirectly impact data (structure or content).

- **Communication Channels**

  Communication channels are the ways one can access, transmit, exchange, or share data within or outside the company.

- **Communications, Space & Technology Commission (CST)**

  The Saudi Communications and information technology commission regulates communications and information technology in Saudi Arabia to provide advanced telecommunication services by licensed companies in Saudi Arabia.

- **Company**

  In this document, we refer to TAWAL as a Company.

- **Conceptual Data Model**

  A conceptual data model defines what the system contains. Business stakeholders and data architects typically create models to organize, scope, and refine business entities and their attributes, and their relationships.

- **Corporate Analytics & Data (CAD)**

  The CAD is a centralized team of data experts who are able to develop and execute analytics efforts across the company.

- **Confidential Data**

  Data to which access is controlled, protected, and prohibited to use outside of TAWAL. This type of data is shared with a limited audience and poses a high risk if shared with unauthorized users.

- **CR – Change Request**

  A change request in consideration of Data management is a formal proposal that can be submitted by a Data Owner to make the desired changes in Data.

- **Critical Data Element – CDE**

  Critical Data Elements (CDEs) are the data elements that are determined to be vital to the successful operation of the company. These data elements may also be used in reports/dashboards (both internal and external) and are critical for decision-making or for measuring organizational performance. CDEs are defined as “the data that is critical to success” in a specific business area (line of business, shared service, or group function). CDE Category is a high-level categorization of CDEs, in which similar sets of CDEs are combined under the same group. CDE is the criteria that represent the identifiable criticality rule that highlights why a specific data element is critical to the company. CDE Dimension is the classification of CDE that identifies a particular set of data.

- **Data Acquisition**

  The process of procuring data that has been produced by a company outside of TAWAL. Examples are data collected from third-party vendors’ sources like credit card agencies, marketing companies, and other service platforms.

- **Data Architecture**

Data Architecture describes how data is collected, stored, transformed, distributed, and consumed. It includes rules governing structured formats, such as databases and file systems, and the systems for connecting data with the business process that consumes it.

- **Data Archiving**

  Defined as the secured storage of data such that data rendering is inaccessible by authorized users in the ordinary course of business, however, it can be retrieved by an administrator designated by the data owners.

- **Data Classification Levels**

  Logical grouping of data according to data access levels (Public, Internal, Confidential and Restricted types of data).

- **Data Collection**

  The systematic gathering of data for a specific purpose from various sources, including manual entry into an information system, questionnaires, interviews, observation, existing records, and electronic devices. This includes both operational data collections and data repositories.

- **Data Consumer**

  An individual or entity that receives and uses data sets to carry out certain business activities. Data consumers do not make changes to data in source systems.

- **Data Custodian**

  Responsible for data-related process management and coordination from a system-level perspective. The role exists within Technology & Innovation and is aligned with Data Stewards and Stewardship Leads. Examples: Project Managers with vendors of the Business Support Systems and Operations Support Systems.

- **Data Demand**

  The request for specific data made by any authorized consumer of the data processed and controlled by TAWAL from any of the systems in the analytical application landscape.

- **Data Destruction**

  The physical or electronic data destruction is sufficient to render it unusable and irretrievable by ordinary commercially available means.

- **Data Domain**

  The business grouping of data belonging to a specific business purpose.

- **Data & Analytics Governance Council**

  Data & Analytics Governance Council (DAGC) is a cross-functional leadership team that provides direction and support to the overall Data Governance function and resolves any internal data governance dispute across the company. The council will review and approve cross-domain level strategies and data decisions related to data governance. The Data & Governance Council is formed by the Data Governance Executive Committee. Members of the Data & Analytics Governance Council are:

  a) GM of the Technology and Innovation General department.

  b) Manager of the data office.

  c) All data owners.

- **Data Governance Council Chairman**

  The chairman of the Data Governance Council is represented by the GM – Technology & Innovation Department who is assigned by the data governance official sponsor. In addition to their role as a council member, the chairman takes a lead in accelerating decisions, resolving disputes, and escalating issues (when applicable) to avoid business disruptions. Additionally, the chairman performs oversight of the Data Governance business as usual activities and ensures issues are effectively resolved.

- **Data Governance Official Sponsor**

  The Data Governance Official Sponsor is TAWAL CEO (or his delegate) who ensures that data governance is implemented and executed within TAWAL. He operationalizes and supports the Data Governance Executive Committee.

- **Data Governance Executive Committee**

  The Data Governance Executive Committee (DA Steerco) is formed by the data governance official sponsor. Data Governance Executive Committee consists of TAWAL CxOs who assign data owners and provide direction support, and recommendations to improve the overall Data Governance function in coordination with the data owners to implement the controls. The Data

Governance Executive Committee is responsible also for forming the Data & Analytics Governance Council.

- **Data Governance Community**

  Data Governance Community is the collection of ALL roles defined in TAWAL's Data Governance Model that are required to perform some responsibilities to achieve an overall data governance e.g., Data Stewards, Data Custodians, etc.

- **Data Lifecycle**

  Is the sequence of stages from its initial generation or capture to its eventual archival and/or deletion at the end of its useful life.

- **Data Model**

  A data model is a set of data specifications and related diagrams that reflect data requirements and designs. The data model is a framework for business re-engineering and the development of new or enhanced applications to fulfill business requirements and processes.

- **Data Modelling**

  Data Modelling is an analysis and design method used to define and analyze data requirements, and design logical and physical data structures that support enterprise requirements. Data Modelling describes the types of interactions and information exchanges that occur within and between business units and/or data domains.

- **Data Owner**

  Data Owners are leads for specific functional units' (Operations, Commercial, Finance, HR…) data with the responsibility of assigning their Data Stewards. They have the authority for decisions related to their data including the approval, enforcement of and adherence to those decisions as per business needs.

- **Data Privacy**

  Data Privacy is the practice that restricts unauthorized access to private data that applies to collecting personal information, such as customer records, enterprise financial data, business-related information, etc.

- **Data Quality Assessment (DQA)**

  This is the process of scientifically and statistically evaluating data to determine whether they meet the quality required for projects or business processes and are of the right type and quantity to be able to support their intended use. It is the process of identifying technical and business data quality issues in order to take remedial action and to plan data cleansing and data enrichment strategies.

- **Data Quality Health Index (DQHI)**

  DQHI is an index used to evaluate data quality across TAWAL for a specific data domain. It is calculated to measure the data quality in a proactive and traceable manner.

- **Data Retention**

  Defined as the period for which data must be kept and not be deleted. Data can be retained in any format in any system as agreed and can be accessed by all authorized users in the ordinary course of business.

- **Data Sourcing**

  The process of extracting data from internal and external sources including third-party vendors to fulfill business requirements related to data demand.

- **Data Steward**

  They represent the business and function units in data governance as business subject matter experts (SMEs) within their data domains. They also ensure that data governance policies, processes, standards, and tools are understood and utilized in organizational units.

- **Data Usage**

  The term data usage is defined in the context of data governance as the reasons for using data or information belonging to TAWAL. It dictates the purposes for which an individual may use the data. It is not to be confused with the data usage by TAWAL customers for their respective plans.

- **De-identification**

  Any process that removes the association between a subject’s identity and the subject’s data elements. Anonymization and pseudonymization are types of de-identification.

- **Direct Identifiers**

  Direct identifiers are data that directly identify a single individual or data subject, without additional information or with cross-linking through other information that is in the public domain.

- **External Data**

  Any data that is consumed or acquired from external sources by TAWAL for business purposes. Examples of such data include social media data, data for address validations, MOI data for verification of Iqama ID etc.

- **Indirect Identifiers**

  Indirect or quasi-identifiers are data that can identify a single person only when used together with other indirectly identifying data. Indirect identifiers can reduce the population to which the person belongs, possibly down to one if used in combination.

- **Internal Data**

  Data that could be subject to release is legally protected and must not be made public. It must only be disclosed under limited circumstances.

- **Issue Raiser**

  An issue raiser is a party (individual or department) that identifies and logs a data-related issue in the central Data Issue Log. The issue raiser will receive notifications regarding the issue status and resolution from the Data Steward.

- **KPI - Key Performance Indicator**

  A measurable value that evaluates the success of the company in engaging processes, policies, or projects.

- **Logical Data Model**

  A logical data model is a fully attributed data model that is fully normalized. Fully attributed means that the entity types have all the attributes and relationship types for all the data that is required by the application(s) it serves. It may include:

  a) Restrictions on the data that can be held.

b) Rules and derived data that are relevant to the processes of the application(s) the logical data model serves.

- **Masking**

  The process of removing a variable or replacing it with pseudonymous or random characters.

- **Master Data**

  Master data is the consistent and uniform core data within TAWAL that describes entities in which business is conducted. Master Data includes hierarchical or dimension data that categorizes core objects of business for analytical or reporting purposes. Examples of Master Data are:

  a) Customer Hierarchy.

  b) Customer Master Record.

  c) Supplier Master Record etc.

- **Master Data Categorization**

  Master data categorization encompasses people, process, and technology to create a consistent, sustainable, and enterprise-wide view of TAWAL data. Categorization is done by type and usage.

- **Master Data Management**

  Refers to the control over master data values to enable consistent, shared, contextual use across systems. Master Data Management (MDM) consolidates the different components of a data term into one accurate, timely and relevant version of truth.

- **Metadata**

  Metadata is data that describes other data and generally defines the content of a data object. Metadata describes the characteristics of a data set to establish a common understanding of the meaning of the data and to ensure its correct interpretation and use.

- **Metadata Management**

  Metadata management refers to the activities associated with ensuring that metadata is created/captured at the point of creation and that it is documented and maintained effectively.

Metadata management ensures that the broadest possible portfolio of metadata is collected and stored in a central repository for use by different stakeholders throughout the company.

- **Metadata Repository**

A structured repository that stores information about data collected in TAWAL's systems. A metadata repository will enable TAWAL to:

a) Support the long-term management of descriptive information about TAWAL's data.

b) Ensure that metadata is accessible, fit for purpose, and sustainable.

c) Foster a common understanding of the nature and types of data collected across TAWAL.

- **Non-curated Data**

Data that is not archived by TAWAL's data repository. For example, excel sheets or documents obtained from third parties.

- **Operational Metadata**

Operational metadata is the information about the data used for administrative and operational purposes, i.e., logs, data, and time of jobs executed, etc. Operational metadata comprises information such as the execution of a job, including time, date, number of records processed and rejected, login details, errors, and exceptions. It defines the semantics of the administrative and operational tasks involved with the data.

- **Physical Data Model**

A physical data model consists of the table's structure, column names and values, foreign and primary keys, and the relationships among them. It is a representation of a data design as implemented, or intended to be implemented, in a database management system.

- **Partner PII**

All Personal Identifiable Information (PII) data that is related to business partners of TAWAL.

- **PII**

Personal identifiable information (PII) is data that can potentially be used to identify or locate a specific individual. A single data attribute or in conjunction with other data attributes that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data must be considered.

- **Pseudonymization**

  A type of anonymization that removes the association between data and a subject and introduces a new identifier that establishes a bidirectional mapping between that subject and the new identifier.

- **Public Data**

  Data explicitly or implicitly approved for distribution to the public without restriction.

- **RCA – Root Cause Analysis**

  An approach for identifying the underlying causes of any issue so that the most effective solutions can be identified and implemented.

- **Recovery**

  The retrieval of the data, business processes and systems to bring them to a working and consistent state as required by the business.

- **Reference Data**

  Reference Data is data that defines, classifies, and categorizes a pre-defined set of values. Users will have the ability to use it as part of their interactions but will not have the authority to change them. For example, gender types, countries, states etc.

- **Re-Identification**

  A process by which the de-identified/anonymized data will be converted such that it reverts to its original state.

- **Restricted Data**

  Restricted data is any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit.

- **Sensitive Data**

  Defined as information that is protected against unwarranted disclosure. Access to sensitive data should be safeguarded. Leakage of this data can lead to lawsuits, negative business impact, financial impact, or customer privacy violation.

- **TAWAL Data Governance Operating Model (DGOM)**

  TAWAL Data Governance Operating Model (DGOM) refers to Data Governance roles and responsibilities, interaction model, standards, and metrics. The operating model is reviewed for efficiency and effectiveness periodically and is the ongoing mechanism to operationalize Data Governance within TAWAL.

- **Stewardship Lead**

  They are members of the CAD, who ensure corporate data is properly defined and used throughout the enterprise. They define and monitor the data governance compliance, metrics and objectives endorsed by the Data Governance Executive Committee and Data Governance Council as well as support, coordinate with and educate Data Stewards and Data Custodians.

- **Surrogate Keys**

  Refers to the unique identifier for either an entity in the modeled world or an object in the database.

- **Technical Metadata**

  Technical metadata is the technical information about the data used for business, i.e., column, table, data type, etc. Technical metadata consists of the technical description of the data assets, including information about schema, table, column, and physical attributes of data. It also contains mapping, and specifications of transformation jobs. It defines the semantics of physical data assets and their effect on management and business planning decisions. Technical metadata must be expressed to show key lifecycle events of the data assets, including mapping, lineage, and transformation rules.

- **VIP Data**

  Information of individuals or organizations there is classified as the top-secret Kingdom of Saudi Arabia.

4. Roles and Responsibility

The T&I Department in coordination with QA is responsible for developing and updating this policy.

The following are responsible to enforce the policy:

- Data Governance Official Sponsor.

- Data and analytics governance council.
- Data Governance Executive Committee.

5. References

- CST Cloud Computing Regulatory Framework
- National Data Management Office (NDMO) Data Management and Personal Data Protection
- TAWAL T&I Asset Management Policy
- TAWAL T&I Information Security Policy
- TAWAL T&I Compliance Policy

6. Policy description

6.1. Data Governance Compliance

Objective: Ensure compliance with Data Governance policies and processes adopted at the Company.

6.1.1. Commitment

a) Data Governance Council and Stewardship Leads shall conduct reviews to measure compliance across all policies, processes, and procedures.

b) The Data Governance Policy defined in this document and subordinate procedures and standards defined in other documents shall be reviewed at least annually or when significant changes to the Company's or its environment occur to ensure their continuing suitability, adequacy, and effectiveness, in accordance with the Data Governance mandate.

6.1.2. Non-Compliance

In the event of non-compliance, an analysis shall be conducted by Stewardship Leads under the guidance and direction of the Data Governance Council.

6.1.3. Issue Escalation & Resolution

a) Non-compliance issues are escalated as per their severity level and in alignment with the Data Governance Operating Model.

b) Stewardship Lead should seek clarification for non-compliance and receive a response within Service Level Agreement (SLA) from required stakeholders and escalate any non-responsiveness.

c) The data governance council is responsible for setting the SLA for the communication between the Stewardship Leads and the stakeholder.

d) Data Governance Council (DGC) is responsible for escalating any unsolved issue within SLA to the Data Governance Executive Committee (DG Steerco).

e) Stewardship Leads maintain issue description and status in a centralized log.

f) Data Governance Issue Escalation metrics must be defined, implemented, measured, and compliance reported regularly by the Data Governance Department.

6.1.4. Data Governance Resource Assignment

a) The Data Governance Sponsor must assign Data Governance Executive Committee members.

b) The Data Governance Executive Committee must assign Data Owners for relevant Data Domains.

c) Data Owners should appoint/replace Data Stewards for their respective Data Domains.

d) Technology & Innovation Council members should appoint/replace Data Custodians for all concerned systems.

e) Technology & Innovation Council members shall notify the CAD manager of any Data Custodians updates/changes.

f) All data-related roles and responsibilities shall be reviewed by Stewardship Leads and updated regularly to adjust to the changing business environment.

g) CAD creates and updates the directory with all Data Governance Community members' details (e.g., Employee details, roles, email id, contact number, department, office address etc.).

h) CAD should conduct periodic assessments to ensure all data governance roles are occupied.

i) Data Governance assignees should understand their responsibilities and comply with the Data Governance Operating Model.

Table 1: Roles and responsibilities for data governance compliance

Data governance role	Responsibility
Data Governance Council Chairman	• Accelerate decisions, facilitate dispute resolutions, and escalate issues. • (When applicable) to avoid business disruptions. • Oversight of Data Governance business as usual activities • Approved the Data Management Strategy.
Data Owner	• Data owners should be responsible for: a) Enforcing Data Governance compliance (activities and capabilities) across respective Data domains. b) Appointing Data Steward within the respective Data Domain.
Data Steward	• Responsible for enforcing Data Governance activities and capabilities across their respective data domain.
Stewardship Lead	• Monitoring Data Governance Policies and Processes metrics and investigating/analyzing non-compliance cases. • Data management strategy must be defined, documented, and reviewed on a timely basis.

6.2. Data Access and Usage

Objective: Ensure that proper secure data access is granted to protect all data processed and/or controlled by the Company from unauthorized access.

6.2.1. Data Access Authorization

a) Data consumers must clearly mention the data access request purpose. The data Owner must review the data access request before authorizing it. In the absence of the Data Owner the Data Steward shall review the access request before authorizing it. Data should not be accessed by data consumers unless it is clearly authorized by the data owner or data steward.

b) Even when authorized by appropriate Data Owner or Data Steward, Data Consumers should only access or use data when needed and as per the approved purpose.

c) The reasons for data access and the intended purpose of data usage must be defined and documented by the Data Steward.

d) Data must only be accessed through TAWAL's formal data access mechanisms after obtaining a data access request approval.

e) Data Stewards must ensure that Data Access Process is being followed for requesting and approving access.

f) Data Stewards review access if the consumer role changes and hence entitlement changes.

g) Data Consumers must stop using data in case of termination, closure of projects or change in roles, by putting necessary controls in place.

h) Data Consumer is obliged to report to data stewards revoking access in case of entitlement changes.

i) All TAWAL employees and contract employees who have been granted access to the data shall ensure data will not be used on public platforms and should be aware of relevant laws and regulations.

j) All data access must be logged across respective systems as per audit log retention rules by the Data Custodian.

k) Data Owners must ensure that Data Access and Usage entitlements are reviewed periodically.

l) Access control and procedures apply to all data lifecycle phases from creation to retirement to ensure protection.

m) All data consumers must ensure that no data (files like presentations, PDFs, etc.) is left on the unattended systems.

n) CRUD Matrix (Create, Read, Update and Delete) must be created and maintained for all data elements in the analytics platforms by Data Custodians.

6.2.3. Data Usage

a) Data consumers are accountable to use data fairly and lawfully for a limited and stated purpose.

b) Customer and Partners' PII data must be used as per the anonymization and pseudonymization mechanisms.

c) For frequently produced reports and analytical data, a footnote should state, "internal use of data is authorized by the Data Owner.'

d) Data must only be used by appropriate and authorized individuals and applications.

e) Data Owners must identify the legitimate business or commercial purpose for which their data is being processed and used.

f) Data Usage requests for non-TAWAL purposes (e.g.: - Compliancy and Regulatory) must be well documented and executed by Data Stewards as per the defined mechanisms.

g) All data usage standards and procedures apply to all data lifecycle phases – from creation to retirement – to ensure protection.

Table 2: Roles and responsibilities for Data Usage

Data governance role	Responsibility
Data Governance Council Chairman	• Accelerate decisions, facilitate dispute resolutions, and escalate issues (when applicable) to avoid business disruptions. • Oversight of Data Governance business as usual activities
Data Owner	• Accountable for approving / rejecting any data access and usage request for confidential or restricted data.
Data Steward	• Data Stewards ensure that the data access process is followed for granting data access requests. • Responsible to ensure data is classified as per Data. • Classification prior to approving data access to the requestor. • Responsible for managing notifications and communications for all data access requests.
Data Custodian	• Responsible for execution and implementation of access requests after the required approvals have been granted.

6.3. Data Classification

Objective: Ensures that all data processed and/or controlled by TAWAL are classified in accordance with the "National Data Management Office (NDMO) Data Management and Personal Data Protection Policy"

6.3.1. Data Classification Guidelines

The data classification system must:

a) Apply to data types rather than discrete data elements.

b) Determine the relative value of data including factors such as:

I. Statutory or regulatory requirements,
II. Impact on health, life, or personal safety,
III. Effects of data aggregation,
IV. Impact on TAWAL service plan from loss of information confidentiality, integrity, and availability,
V. Changes to information sensitivity over time.

6.3.2. Data Labeling Guidelines

a) Data Stewards and Data Custodians must document procedures to label data with its data classification standards as required by the TAWAL Data Classification System. Data labeling communicates the classification and protection requirements to employees.

b) Data types that must be considered for labeling include printed or electronic records, reports, files, on-screen displays, or messages. Data Custodians must select and document the appropriate label type for each data type.

c) Automatic data labeling must be used where possible (e.g., by use of document templates, standard report footers, printer watermarks, on-screen displays, or system-applied text).

d) Where direct data labeling is not possible, alternate methods must be used to communicate the data classification, such as marking storage media, description in data sharing agreements or system interface specifications, or use of metadata.

6.3.3. Data Classification & Sensitivity Categories

a) All data at the Company must be classified as sensitive or non-sensitive in accordance with the Company's "T&I Information security policy."

6.3.4. Assign Data Classification & Sensitivity

a) Data Owner is accountable to ensure that data in their data domain has the appropriate classification and sensitivity levels in accordance with the Company's "T&I Information security policy".

b) Confidential and Restricted data must go through appropriate Masking / De-identification techniques as per the Data Sharing section in this policy 6.13.

6.3.5. Data Classification Matrix

Data Classification	Guidelines	Impact
Confidential	• Confidential data is data protected by statutes, regulations, TAWAL policies or contractual obligations. • Confidential data may be disclosed to employees on a need-to-know basis. • Confidential data has the potential to cause serious damage or distress to data subjects or serious damage to TAWAL interests if disclosed inappropriately. • Its unauthorized disclosure could seriously and adversely impact TAWAL and its stakeholders, leading to legal and financial repercussions and adverse public opinion.	Major
Restricted	• Restricted data is the information that is restricted to members of the TAWAL community who has a legitimate purpose for accessing such data and must be guarded due to proprietary, ethical, or data privacy considerations, and shall be protected from	Medium

	unauthorized access, modification, transmission, storage, or other use. • Restricted data has the potential to have a negative impact on data subjects or the Company's interests (but not falling into Confidential). • This information, if lost, could cause significant financial loss or reputational risk.	
Internal	• Internal data is the information that is available to all members of the TAWAL community. • Internal Data is the information that could be subject to release shall be legally protected and not be made public and must only be disclosed under limited circumstances	Low
Public	• Public data is information that is available to the general public on the TAWAL website, newsletters, and public forums. • Public data does not impact the business or data subjects.	No impact

TAWAL Information shall be classified in accordance with the Company's "T&I Information security policy" and the following classification schema:

6.3.6. Data Reclassification

Data Owner reclassifies or recertifies the classification categories of impacted data in accordance with the Company's "T&I Information security policy."

Table 3: Roles and responsibilities for data classification

Data governance role	Responsibility
Data Governance Council Chairman	• Accelerate decisions, facilitate dispute resolutions, and escalate issues (when applicable) to avoid business disruptions. • Oversight of Data Governance business as usual activities

Data Owner	• Data Owner reviews and approves the Data Classification and Sensitivity levels applied to the respective data domains.
Data Steward	• Responsible to assign the Data Classification and Sensitivity levels to the data for respective data domains.
Data Custodian	• Data Custodians assist the Data Stewards in applying the Data Classification and Sensitivity levels to the applicable system.
Stewardship Leads	• Confirm the consistency of assigned Data Classification and Sensitivity levels across all data domains and applicable systems.

6.4. Analytics Data Modelling

Objective: Ensures that consistent Analytics Data Modelling practices are followed across the Company.

6.4.1. Guiding Principles

a) Stewardship Leads are responsible for the development of the logical and physical data models to support Analytics data demand.

b) Stewardship Leads will review and monitor compliance and impact of the developed analytical data models against the planned impact.

c) Stewardship Leads will ensure appropriate alignment with the Enterprise Architecture domain.

d) Stewardship Leads participate and contribute to Enterprise Architecture activities related to the development and maintenance of data architecture.

e) Stewardship Leads to carry out analytics information flow analysis and ensuring data sourcing is aligned with data ingestion and sourcing guidelines.

f) Data Stewards will identify and review the key business goals, strategy, architecture and business requirements for analytics data modeling.

g) Data Stewards to develop and maintain the data domain’s analytics data system inventory and taxonomy.

h) Stewardship Leads will review outcomes of target analytics data models based on business requirements and will make iterative improvements as needed.

i) Shifts in technology, in addition to the emergence and adoption of new technology-related industries will be addressed as appropriate during periodic reviews.

j) Data Owners approve and publish business definitions used in information assets before releasing them, whether for business intelligence reports, dashboards, or analytical models.

6.4.2. Analytics of non-curated Data

a) Stewardship Leads to carrying out analytics information flow analysis and ensuring data sourcing is aligned with data ingestion and sourcing guidelines.

b) Data Governance Council must approve all data analytics activities that are conducted on noncurated data.

c) Approvals from the Data Owner and the head of the Data Governance Council are prerequisites to submitting the approval requests to the Data Governance Council.

d) Before using any non-curated data and to keep a single version of truth, the Metadata repository should be used by Stewardship Leads, to cross-check whether this set of data exists within sourced data.

e) Stewardship Leads to highlight and differentiate the design of the presentation of any data analytics insights driven from non-curated data and add the disclaimer “Data viewers use the presented insights driven from non-curated data and add the disclaimer “Data viewers use the presented insights at their own risk and responsibility.”

Table 4: Roles and responsibilities for Analytics Data Modelling

Data governance role	Responsibility
Data Governance Council Chairman	• Accelerate decisions, facilitate dispute resolutions, and escalate issues (when applicable) to avoid business disruptions. • Oversight of Data Governance business as usual activities. • To approve non-curated analytics demand.
Data Owner	• Steers on a high level the analytics models’ use cases. • Prioritizes business needs from data analytics. • To approve non-curated data analytics demand

Data Steward	• Ensures analytics models are serving business goals.
Stewardship Leads	• Development of analytics models • Ensure alignment with Enterprise Architecture • Responsible for reporting on analytics models' impact • Highlights insights derived from non-curated data requests

6.5. Metadata Management

Objective: Governs the management and documentation of metadata and business definitions of all data processed and/or controlled by the Company. Knowledge of data within different enterprise systems provides consistency to the information produced by the Company.

6.5.1. Guiding Principles

a) Data Stewards and Data Custodians clearly define Metadata in terms of three categories: business, technical and operational.

b) A central metadata repository must be used for the collection and maintenance of metadata, which will be used by all sectors and business units.

c) All business, technical and operational metadata need to include mandatory attributes for respective data elements.

d) Data Stewards must define the business metadata for their respective data domains.

e) Data Stewards must review and confirm the validity of business metadata (definitions, formulas, rules, usage, purpose, impact) for their respective data domains.

f) Data Custodians must define the technical and operational metadata.

g) Data Custodians must review and confirm the validity of technical and operational metadata.

h) Data Owners must approve new business terms and rules for their respective data domain.

i) Data Stewards and Data Custodians orchestrate the linkage of business and technical metadata. Which can be triggered by the Stewardship Leads.

j) Data Domain target state should be built and maintained to:

I. Utilize gaps previously identified in the current state.

II. Demonstrate formulating the target state analytical architecture signaling.

k) Leverage previously created/updated Data Dictionary by Data Custodians to build out the components of the analytics conceptual models.

6.5.2. Existing Enterprise Systems

a) Data Custodians must document database, schema, dataset, data attributes and data flow routines.

b) Data Custodians must integrate data assets into the central metadata repository.

c) Whenever possible, metadata is to be captured by the Data Custodian as soon as it is created.

d) Whenever possible, metadata within the source system generating and managing data assets is to be captured by the Data Custodian into the central metadata repository.

e) Capture metadata for all TAWAL data assets whenever it adds value or has a defined purpose.

f) Metadata containing classification information must be strictly aligned with the TAWAL Data Classification section in this policy 6.3.

g) Data Custodians must define data attributes at system level and integrate metadata information into the central metadata repository.

h) Data Custodians must make sure that all data assets such as schemas, datasets, data tables, data files, and data attributes (columns) are described to define the purpose and usage of the asset.

i) Data Custodians must create a data dictionary by defining the metadata, relationship and data lineage.

j) All metadata information must be documented by the data steward and integrated into the central metadata repository as part of the system rollout plan.

6.5.3. Business Glossary

a) Glossary terms and definitions must be collected, maintained and complied with by data stewards in a centralized business glossary across the Company.

b) A centralized business glossary shall be developed and should contain business terms, definitions, usage context and real-life examples if available.

c) Existing business definitions in silos must be migrated to the centralized business glossary and published for reference and usage across the Company.

d) Data Owners are accountable to maintain an updated business glossary for their respective data domains for day-to-day usage.

e) Relationships between business definitions and physical data elements must be defined and maintained by the data steward.

Table 5: Roles and responsibilities for Metadata Management

Data governance role	Responsibility
Data Governance Council Chairman	• Accelerate decisions, facilitate dispute resolutions, and escalate issues (when applicable) to avoid business disruptions. • Oversight of Data Governance business as usual activities
Data Owner	• Accountable for approving the business name and definition of all business terms for their Data Domain. • Accountable to have up to date business glossary with business terms used across TAWAL.
Data Steward	• Responsible for providing the correct business definition and formula for data elements belonging to their domains. • Responsible for keeping the business glossary up to date. Data Stewards are also responsible for linking technical metadata with business metadata and for integrating business and architectural relationships between objects.
Data Custodian	• Responsible for documenting the technical metadata for the data in the respective systems. • Responsible for identifying the required data elements for a specific Data Domain at the request of the Data Steward. • Data Custodians must ensure that the recipient of a data extract receives a copy of the business/technical metadata that corresponds to the extracted data.

	• With the support of the designated Data Stewards, Data Custodians must create a data journey by mapping technical data objects to business definitions. • Data Custodians populate the central metadata repository to include all metadata information for data objects and information assets.
Stewardship Leads	• Stewardship Leads must certify the accuracy, completeness and timeliness of the metadata content.

6.6. Reference and Master Data Management

Objective: Establish golden records, define and maintain hierarchies, manage changes to reference and master data and achieve a unified 360-degree view of foundational data.

6.6.1. Guiding Principles

a) Lifecycle of Reference and Master Data - from data creation to data retirement – across all applicable systems, must be fully documented by Data Stewards and Data Custodians.

b) Approval and validation procedures for creating, reading, updating and deleting (CRUD Matrix) Reference and Master Data must be documented by Data Stewards and Data Custodians.

c) Reference and Master Data must be categorized, labeled and documented for new and existing data by Data Stewards.

d) Manual processing and workarounds on Reference and Master Data must be mitigated, and documented and results should be monitored by Stewardship Leads to ensure consistency.

e) Data Stewards assess and update Reference and Master Data processes regularly to improve efficiencies, increase data quality or adapt to new business needs.

f) Data Stewards defines CDE to be monitored using a data quality tracking procedure.

g) Data Stewards conducts Data Quality Assessments for new and existing Reference and Master Data.

h) New and existing Reference and Master Data elements must be classified by Data Stewards as per Data Classification.

i) Data Stewards must classify new and existing Reference and Master Data elements as Critical Data Elements and proactively monitor their quality.

j) To ensure compliance, Data Owners must appoint Data Stewards of Reference and Master Data Management as per the Data Governance Operating Model.

k) Reference and Master Data Management metrics must be defined, implemented and measured, and compliance reported regularly by data stewards.

6.6.2. Data Hierarchy Definitions and Core Capabilities

a) Data hierarchy must be defined to properly define and document Master Data.

b) Core capabilities of Master Data must be considered when identifying Master Data. The core capabilities are:

i. **Matching**: The process of properly identifying and linking two or more records to each other.

ii. **Merging**: The process of combining multiple records' information and eliminating duplicate records.

iii. **Survivorship**: The set of rules defining the trusted hierarchy across various data sources to indicate which source is more trustworthy for creating a golden record.

iv. **External Match**: The process of matching an incoming record with the master records in the system before loading them into the master database.

6.6.3. Data Lookups

Reference data lookups must be properly documented, and details should be uploaded to the central metadata repository as per Metadata Management

Table 6: Roles and responsibilities for Reference and Master Data Management

Data governance role	Responsibility
Data Governance Council Chairman	• Accelerate decisions, facilitate dispute resolutions, and escalate issues (when applicable) to avoid business disruptions. • Oversight of Data Governance business as usual activities
Data Steward	• Responsible to identify, define and manage Reference and Master Data.
Stewardship Leads	• Stewardship Leads certify the accuracy, and completeness of defined Master Data and drive the coordination between Data Stewards from different Data Domains for consistency.

6.7. Data Demand

Objective: Govern the demand for data, reports and dashboards processed and/or controlled by the Company, for all analytical purposes.

6.7.1. Guiding Principles

a) Data Consumers must formally log analytical data demand requests at the Company.

b) Data Owners must approve analytical data demand requests for their respective data domains.

c) Data must only be accessed and shared if formally authorized by the Data Owner

d) Data Consumers should provide the intended purpose of data usage for each analytical data demand request and approved by the Data Owner.

e) Data Consumers and digital ambassadors must raise analytical data demand requests only through the formal demand mechanisms and communication channels.

f) Analytical data demand requests, internal or external, must mitigate any business risk or violation.

g) Data should be defined by the Data Stewards in the business metadata repository before executing the demand.

h) Data elements used and/or created as part of the analytical data demand requests, must be updated in the centralized Metadata Repository by Data Steward of the respective data domain.

i) Stewardship Leads ensure that all data demand requests are executed only for data already defined in the business metadata repository.

Table 7: Roles and responsibilities for Data Demand

Data governance role	Responsibility
Data Governance Council Chairman	• Accelerate decisions, facilitate dispute resolutions, and escalate issues (when applicable) to avoid business disruptions. • Oversight of Data Governance business as usual activities
Data Owner	• Data Owner is accountable for the proper governance of data demand requests for all data processed and controlled in respective data domains.
Data Steward	• Responsible for providing additional details for BRSD. • Responsible for supporting finalizing FDD. • Responsible to provide feedback and validating data demand request completion.
Data Custodian	• Data Custodian ensures that the Data Demand request is properly executed and deployed within and across systems.
Stewardship leads	• Stewardship Leads review and analyzes the data demand request based on the BRSD. • Stewardship Leads prepares draft FDD and validates the implementation of data demand requests as per FDD. • Stewardship Leads initiate Data Sourcing Process. • Stewardship Leads communicate the closure of the request to the requestor

6.8. Data Quality

Objective: Define the acceptable standards of data quality for all data processed and/or controlled by the Company and provide an effective framework for data quality management and assurance under the Data Governance Console.

6.8.1. Guiding Principles

a) Data Owners are accountable for maintaining high-quality and accurate data that results in effective data-driven decisions.

b) Data Owners will set the crucial strategic imperative to produce robust and high-quality data.

6.8.2. Existing Data

a) Data quality processes/procedures must always be applied when recording and storing data.

b) The quality of all Critical Data Elements (CDE) must comply with the applicable data quality dimension set by Data Governance.

c) Data Owners are accountable to provide rules to measure the Data Quality Health Index (DQHI) for their respective Data Domains.

d) Applying data cleansing & monitoring routines (manual or systematic) to existing data should be conducted whenever sufficient added value is presented to the Company, as per the Data Quality processes (Reactive and Proactive).

e) Data owner is responsible for planning and executing data quality improvement initiatives whenever needed with the assistance of the data custodian.

6.8.3. New Services / Data Exchanges

a) Data Owner is accountable to ensure that newly created or updated data is accurate and complete to sustain high-quality standards.

b) Data Quality Assessment (DQA) must be completed by the Data Steward and custodian and reviewed by the Data Owner prior to implementing new services, computer-based information management tools, and manual or systematic data exchanges/interfaces.

c) Data Quality Assessment (DQA) must be completed and reviewed prior to the disclosure of data to a third party, as per the Data Quality Assessment Process.

d) Data Stewards must always implement Data Quality processes at the point of recording and storing original and existing data.

6.8.4. Data Quality Dimensions

Data quality tracking activities should follow the following data quality dimension definitions.

a) **Accuracy**: Data Accuracy refers to the degree that the data refers to the “real-life” entities they model. In many cases, measure accuracy by how the values agree with an identified reference source of the correct information, such as comparing values against a database of record or a similar corroborative set of data values from another table, checking against dynamically computed values of perhaps applying a manual process to check value accuracy.

b) **Completeness**: One expectation of completeness indicates that certain attributes always have assigned values in a data set. Another expectation of completeness is that all appropriate rows in a dataset are present. Assign completeness rules to a data set in varying levels of constraint mandatory attributes that require a value, data elements with conditionally optional values and inapplicable attribute values. See completeness as also encompassing usability and appropriateness of data values.

c) **Consistency**: Consistency refers to ensuring that data values in one data set are consistent with values in another data set. Consistency can include an expectation that two data values drawn from separate data sets must not conflict with each other or define consistency with a set of predefined constraints. Encapsulate more formal consistency constraints as a set of rules that specify consistency relationships between values of attributes, either across a record or message, or along all values of a single attribute. Consistency must not be confused with accuracy or correctness. Consistency may be defined between one set of attribute values and another attribute set within the same record (record-level consistency) between one set of attribute values and another attribute set in different records (cross-records consistency), or between one set of attribute values and the same attribute set within the same record at different points in time (temporal consistency).

d) **Currency**: Data currency refers to the degree to which information is current with the world that it models. Data currency measures how “fresh” the data is, as well as its correctness in the face of possible time-related changes. Measure the currency as a function of the expected frequency rate at which different data elements refresh, as well as verify that the data is up to date. Data currency rules define the “lifetime” of a data value before it expires or needs updating.

e) **Integrity**: Integrity (or referential integrity) is the condition that exists when all intended references from data in one column of a table to data in another column of the same or a different table are valid. Integrity expectations include specifying that when a unique identifier appears as a foreign key, the record to which that key refers exists. Integrity rules also manifest as constraints against duplication, to ensure that each entity occurs once, and only once.

f) **Uniqueness**: Uniqueness states that no entity exists more than once within the data set. Asserting the uniqueness of the entities within a data set implies that no entity exists more than once within the data set and that a key value relates to each unique entity, and only that specific entity, within the data set.

g) **Timeliness**: Timeliness refers to the time expectation for accessibility and availability of information. As an example, measure one aspect of timeliness as the time between when information is expected and when it is readily available for use.

h) **Conformity**: The degree to which data is stored in a defined format.

i) **Range**: Data must be within the defined value ranges.

Table 8: Roles and responsibilities for Data Quality

Data governance role	Responsibility
Data Governance Council Chairman	• Accelerate decisions, facilitate dispute resolutions, and escalate issues (when applicable) to avoid business disruptions. • Oversight of Data Governance business as usual activities
Data Owner	• Data Owners approve or reject data quality-related requests for their data domain, prioritize and take actions on data quality improvements. • Defines the data health index by data domain

Data Steward	• Data Stewards conducts the business RCA, designs business solutions, and improves business data quality. • Responsible for ensuring high quality within their data domains and responsible for the data quality monitoring of Critical Data Elements (CDE. • Responsible for implementing Data Quality business fixes and/or business recommendations based on the RCA or DQA.
Data Custodian	• Data Custodians execute the technical RCA and provide data samples when requested to do so by Data Stewards. • Responsible for implementing Data Quality system fixes and/or technical recommendations based on the RCA or DQA
Stewardship leads	• Stewardship Leads govern the data quality initiatives and communicate results regularly via DQ scorecards

6.9. Critical Data Element

Objective: Govern the identification and documentation of Critical Data Elements that are vital to the success of the Company's operations.

6.9.1. Guiding Principles

a) Data Stewards must identify, define, document and label CDEs for their respective data domains.

b) Single database column should represent a single Critical Data Element (CDE).

c) Data Stewards and Data Custodians tag any security or privacy constraints that a CDE might have.

d) Data Stewards documents all CDEs according to metadata standards defined in Metadata Management.

e) Data Stewards categorize each CDE as per the approved CDE categories - Personal Information, Operational Information, Management, Financial, Data Sharing, and Compliance.

f) Data Owners must approve the definition and categorization of CDE within their Data Domain.

g) Data Stewards ensure proper alignment between all CDEs and Data Governance policy.

h) Data Steward must assess the quality of identified CDEs through the Data Quality Assessment (DQA) process.

i) All CDE's Data Quality must be continuously monitored by the appropriate Data Steward.

6.9.2. Categorization of Critical Data Elements

CDE Category	Definition	Example
Category 1 (Corporate/Personal information)	Those elements which distinctly identify an individual or company.	• Iqama/Passport Name • Credit card details • Tax number • Company registration number
Category 2 (Operational Information)	Elements which describe the assets of TAWAL, and the operations data which are related to operating and maintaining the sites.	• Site coordinates • TOC tickets • Alarms • MSP activities
Category 3 (Management)	Elements which are part of the KPIs of the business which is used by the management to track the performance of TAWAL	• Colocation ratio • Number of orders from customers • New MSA agreements with MSPs and customers
Category 4 (Financial)	All elements related to financial data	• Total revenue, costs, net income, etc.

Category 5 (Data sharing)	Data that is shared from external entities as well as data shared with external entities	• 3rd party data from maps • Customer survey data
Category 6 (Compliance)	Mandatory elements that must be stored to comply with either internal regulations (data governance policy) or external regulations	• Business glossary • CST restrictions

Table 9: Roles and responsibilities for Critical Data Element

Data governance role	Responsibility
Data Governance Council Chairman	• Accelerate decisions, facilitate dispute resolutions, and escalate issues (when applicable) to avoid business disruptions. • Oversight of Data Governance business as usual activities.
Data Owner	• Accountable to make sure that their data is properly identified as Critical Data Elements
Data Steward	• Responsible for identifying, defining and documenting the CDEs based on the CDE criteria. Data Stewards must categorize each CDE according to its criticality to the company, per the approved CDE categories.

6.10. Data Lifecycle Management

Objective: Ensure that data processed and/or controlled by the Company is compliant with the standard lifecycle of data and respective regulations. All data processed and/or controlled by the Company must follow the Data Lifecycle phases. Data Lifecycle Management should be carried out in accordance with requirements set by the Company's "Data Lifecycle Policy."

6.10.1. Data Creation

Is the process of extracting loading and transforming data into a golden source of trust given that the data architecture modeling principles are in line with NDMO. T&I dept shall ensure proper governance controls. Audits shall be in place for corporate data acquisition, data entry and derived data as per Data Collection methodology.

6.10.2. Data Storage

Data Storage activities must be aligned with Enterprise Architecture policies, which define format and applications for storage. Proper governance, controls and audit must be considered by the related department as per Data Archiving and Retention.

6.10.3. Data Management

Data Management includes Data Quality, Metadata Management, Reference, and Master Data Management for the Company's data. All data processed and/or controlled by the Company shall be aligned with Data Quality, Metadata Management and Reference and Master Data Management.

6.10.4. Data Access and Usage

To be aligned with Data Access and Usage for its all-lifecycle phases in section 6.2.

6.10.5. Data Archiving and Retention

To be aligned with Data Archiving and Retention for retention activities section in this policy

6.10.6. Data Destruction

To be aligned with Data Archiving and Retention for destruction activities section in this policy

6.10.7. Change Data

a) Data Owner is accountable for all data changes in their respective data domain. They must review, approve, reject and prioritize any data change requests that affect his/her data domain.

b) Data Governance Council must review, approve and prioritize the change data request if the request affects multiple data domains across different BUs/FUs.

c) Data Steward and Data Custodian assesses, documents and guides business and technology impacts for all data change and data acquisition requests across data domains, business processes and systems.

d) Data Stewards must compile specific recommendations and perform a cost/benefit analysis of all data change requests.

e) Data Steward must prioritize data change requests based on the impact assessment and level of importance.

f) Data Stewards shall update the required documentation for business metadata as per Metadata Management.

g) Data Custodians shall update the required documentation for operations and technical metadata as per Metadata Management.

Table 10: Roles and Responsibilities for Data Lifecycle Management

Data governance role	Responsibility
Data Governance Council Chairman	• Accelerate decisions, facilitate dispute resolutions, and escalate issues (when applicable) to avoid business disruptions. • Oversight of Data Governance business as usual activities
Data Owner	• Accountable for Data Governance compliance to ensure high-quality data throughout its lifecycle. • Accountable to approve or reject change data requests whenever they request their Data Domain.
Data Steward	• Responsible to manage & control change data requests that include fast-track escalation, impact assessment, formulating business recommendations and performing cost/benefit analysis.
Data Custodian	• Responsible for technical assessment, recommendation and implementation of change data requests based on inputs from the Data Steward.
Stewardship leads	• Responsible for reviewing the technical and business recommendations and checking if the request impacts multiple or single data domain(s).

6.11. Data archiving and retention

Objective: Provides guidelines for retrieval, storage and retention of data processed and/or controlled by the Company, and to enable identification and destruction of data where there is no business, legal or historical significance or any financial or legal impact on the company. Scope of Data Archiving and Retention is the Company's digital data that exists in the Company's systems and databases. Documents governance should be carried out in accordance with Company's "T&I Asset Management policy".

6.11.1. Data archiving

a) Data must always be archived whenever practical, to satisfy business requirements and improve the cost-effectiveness of data retention. Even when authorized by appropriate Data Owner or Data Steward, Data Consumers should only access or use data when needed and as per the approved purpose.

b) Data Custodians communicate data storage, archival and retention costs to the data owners when determining retention and archival requirements.

c) Data Steward should ensure that archiving activities are aligned with the data retention type matrix defined in this policy.

d) Data Stewards must ensure that archived data is not altered, and accessibility is provided throughout the retention period only to authorized users.

e) Restoring data from backups or archives should be done only for a valid business justification, disaster recovery or legal/regulatory requirements.

f) Data must be archived as per the retention policy and needs to be destroyed after the agreed retention period expires.

g) Data archiving and storage location must follow KSA regulations (CST Cloud Computing Regulatory Framework).

h) Data Access and Usage applies to all data archived, backed up and restored to ensure data protection.

6.11.2. Data retention

a) Data must be retained whenever there are needs, to satisfy business requirements and improve cost-effectiveness.

b) Data that is adequate, relevant and controlled by business / legal requirements must be retained for prescribed periods as per the data retention type matrix as detailed in section 6.11.3.

c) Data Owners must specify and approve retention and archiving periods for their respective Data Domains.

d) Data retention must be appropriate in duration, media, level of accessibility, ownership and location to satisfy business requirements.

e) Retained electronic data must be machine-readable and accessible at any time during the retention period.

f) The Mandatory Service Level Agreement (SLA) must control the availability of retained data for the Company.

g) Audit files and log entries associated with processed and/or controlled data, must be retained to ensure data is stored and processed lawfully.

h) Data backups should always be available to effectively restore data in case of any future failure.

i) Data owners can extend the retention period beyond the data retention matrix type period as per business needs.

j) Data Owners can seek legal advice before deciding on an exception request to avoid imposing legal concerns.

6.11.3. Data retention types-matrix

6.11.3.1. Short-Term Data

a) Data that is updated regularly would have to be ingested at high-frequency periods to ensure that data is reasonably up to date.

b) Data which does not need to be retained for extended periods of time (less than 6 months) and early destruction would not compromise the availability and abundance of data.

c) Data that is needed for short periods of time and is commonly accessed and referenced over a short period (less than 6 months) and not referred to as historical data.

6.11.3.2. Medium-Term Data

a) Data that is updated more often than short-term data would not have to be ingested at periods of such high frequency to ensure that data is reasonably up to date.

b) Data that needs to be retained for longer periods (between 6 months and 5 years) and early destruction would compromise the availability and abundance of data.

c) Data that is needed for medium periods and may be accessed and referenced again later (between 6 months and 5 years).

6.11.3.3. Long-Term Data

a) Data that is not updated often and would not have to be ingested at periods of high frequency.

b) Data which must be retained for periods of time (more than 5 years) and early destruction would compromise the availability and abundance of data.

c) Data that is needed for long periods of time and is commonly accessed and referenced over a long period and is referred to as historical data (more than 5 years).

6.11.4. Data Backup and Restoration

a) Data Owners and Data Custodians must define and document backup and recovery processes that reflect the security classification and availability requirements of information and information systems.

b) Data Custodians must conduct a Security Threat and Risk Assessment to identify safeguards for backup facilities and media that are commensurate with the value and sensitivity of the information and information systems.

c) Data custodians must test and document the data restoration procedure periodically.

6.11.5. Data Destruction

a) Data must be deleted as permitted or required and that is sufficient to the type of data, its sensitivity, and future usage of the storage.

b) Data must not be destroyed if there are legal or financial concerns.

c) Data must not be destroyed if it results in the loss of any historical information affecting institutional analysis or institutional memory.

d) Data storage medium must be destroyed when the re-usage of that medium is not possible or required.

e) Depending on the data's sensitivity, deleting data must be authorized by the appropriate Data Owner.

f) Data deletion/destruction should not create, transfer, modify or terminate any right.

g) Data deletion standards and requirements must be defined and documented.

h) Destroy data at the end of its legally designated retention period.

i) The Data Custodian shall maintain and enforce a detailed list of approved destruction methods for each type of data archived whether in physical storage media, in database records or backup files.

Paper records

a) The Company shall utilize an onsite shredding machine to dispose of all paper materials.

b) The Company, if possible, shall use a service provider for large disposals and confidential data should be disposed of appropriately in the presence the of Data Retention Officer or Company's representative.

Electronic records

a) The deletion of electronic records shall be organized in conjunction with the IT Department who will look after the removal of all data from the medium so that it cannot be reconstructed.

b) When records or data files are identified for disposal, their details shall be provided to the designated business Owner.

c) The Company shall sanitize systems/electronic media/storage media before their Disposal.

d) The designated data owners from the respective departments shall prepare and update the Register for Records Disposed of.

e) The electronic records stored on CD or DVD are deleted by completely destroying or breaking them.

f) Soft copies of paper-based records should be kept as long as paper-based records are kept.

Table 11: Roles and Responsibilities for Data Archiving and Retention

Data governance role	Responsibility
Data Governance Council Chairman	• Accelerate decisions, facilitate dispute resolutions, and escalate issues (when applicable) to avoid business disruptions. • Oversight of Data Governance business as usual activities
Data Owner	• Data Owner confirms the archiving periods, data retention type and rules for data that belong to their data domain. • Data Owners are accountable for enforcing the retention, archiving and destruction of data, and communicating these periods. • Submit approvals, and clarifications and seek legal advice for resolution
Data Steward	• Data Steward defines the archiving periods, data retention type and rules for data that belong to their respective data domain.
Data Custodian	• Data Custodian ensures that the Data Archiving is properly executed within and across systems. • Responsible for enforcing the retention periods confirmed by Data Owner or by regulatory compliance. • Data Custodian maintains and enforces a detailed list of approved destruction methods appropriate for each type of data archived.
Stewardship leads	• Ensure that there are no conflicts between the data archiving rules and retention periods. • Ensure that data retention must be followed as per the data retention matrix defined in the policy.

6.12. Data protection

Objective: Ensure that data receives an appropriate level of protection in accordance with its importance to the Company.

6.12.1. Guiding principles

a) Data Protection ensures that sensitive data is in accordance with the Company's "T&I Information security policy."

b) The following data domains are of high importance and must receive the appropriate level of data protection:

i. Personally Identifiable Information (PII).

ii. VIP Data.

iii. Customer agreement data

iv. Governmental Agencies Data

v. TAWAL Sensitive Corporate Data

c) Data Owner and Data Stewards are responsible to comply with the Company's "T&I Information security policy," and Customer agreement data handling procedures (section 6.12.4 in this policy) and adopting the "T&I asset management policy."

Data Owner is responsible to ensure all Personally Identifiable Information (PII), VIP data, Governmental Agencies Data, and TAWAL Sensitive Corporate Data are aligned with policies, standards, and guidelines provided by all regulatory bodies. **Domain**	**Classification**			
	Confidential	**Restricted**	**Internal**	**Public**
Personally Identifiable Information (PII)		✓		
VIP data	✓			
Customer agreement data	✓			
Governmental agencies data	✓			
TAWAL sensitive corporate data	✓			

6.12.2. Personally Identifiable Information (PII)

a) Data Owner is accountable for identifying and protecting Personal Data belonging to their data domain throughout its lifecycle phases.

b) Data Owner and Data Steward are responsible to classify Personal Data as the Data Classification section of this policy.

6.12.3. VIP Data

a) Data Owner is accountable for identifying and protecting VIP Data belonging to their data domain.

b) Data Owner and Data Steward are responsible to ensure VIP Data is classified appropriately as per the Data Classification section in this policy.

6.12.4. Customer Agreement Data

a) TAWAL will not use information about customer activities together with any information that would result in a customer being identified without his written consent.

b) TAWAL will not sell, trade, or disclose to third parties any customer identifiable information derived from the registration for or use of a TAWAL service including customer names and addresses without the consent of the customer (except as required by legal processes or in the case of imminent physical harm to the customer or others).

c) When TAWAL uses other agents, contractors, or companies to perform services on its behalf, TAWAL should protect the customer’s identifiable information consistent with this policy.

d) TAWAL will not read or disclose to third parties private e-mail communications that are transmitted using TAWAL services except as required to operate the service or as otherwise authorized by law.

e) TAWAL will implement technology and security features and strict policy guidelines to safeguard the privacy of the customer’s identifiable information from unauthorized access or improper use and will continue to enhance security procedures as new technology becomes available.

f) TAWAL may also use customer identifiable information to investigate and help prevent potentially unlawful activity or activity that threatens the network or otherwise violates the customer agreement for that service.

g) TAWAL honors requests from customers to review all customer-identifiable information maintained in reasonably retrievable form and will correct any such information which may be inaccurate. Customers may verify that appropriate corrections have been made.

h) Customer information shall be disclosed only to those people who have a legitimate business need for that information. The information classification scheme shall be used as the basis for the need to know so that information is protected from unauthorized disclosure, use modification, and deletion.

i) TAWAL should check that no confidential customer information is stored directly on its web servers such as bank account details etc.

6.12.5. Governmental Agencies Data

a) Data Owner is accountable for identifying and protecting Governmental Agencies' Data belonging to their data domain.

b) Data Owner and Data Steward ensure that Governmental Agencies Data are classified as restricted as per the Data Classification section in this policy.

6.12.6. TAWAL Sensitive Corporate Data

a) Data Owner is accountable for identifying and protecting TAWAL Sensitive Corporate Data belonging to their data domain.

b) Data Owner and Data Steward are responsible to ensure Sensitive Corporate Data is classified appropriately as per the Data Classification section in this policy.

6.13. Data Sharing

Objective: Defines the standards for sharing all data processed and/or controlled by TAWAL to ensure optimal data protection. Additionally, ensures that data processed and/or controlled by the company is only shared with authorized users and systems to prevent data misuse.

6.13.1. Data sharing and standard

a) Stewardship Leads ensure that data shared (both internally and externally) does not have any direct linkage to the personal identity of the Company's customers or any other entities.

b) Stewardship Leads identify direct and indirect identifiers for requested data sets, to prevent the identification of individuals, subsidiaries, and customers.

c) Data Classification identifies the type of data that can be shared and whether the appropriate encryption and security mechanisms are required.

d) The appropriate anonymization method must be secured, encrypted and aligned with Data Protection section 6.12 to minimize the risk of violating the privacy of sensitive data.

e) The most appropriate encryption method to secure data must be selected and applied.

f) Data Protection non-disclosure agreements must be included to prohibit third parties from sharing information randomly.

g) Data shared externally by the Company should not contain restricted or sensitive data and must have all appropriate approvals.

6.13.2. Intended Purpose and Time

a) Data Consumers clearly articulate the intended purpose of data sharing, usage reason, and usage time duration.

b) Data Stewards examine the purpose of data requests to deploy secured and encrypted deidentification and masking methodologies, as per the Data Protection section in this policy.

c) After the stipulated time of a data request expires, strict measures must be enforced to audit and stop data sharing.

6.13.3. Data Reclassification Exposure Risk Identification

a) To protect the company against the re-identification of shared data, required data identifiers should be anonymized or masked and documented for future reference.

b) Using replacement surrogate keys enhances the identification of the same subject across a dataset and leads to insightful data.

6.13.4. De-identify Data

a) Data custodians must de-identify critical data after the evaluation of critical identifiers by the data steward.

b) Data custodians must apply de-identification methods which are secured, encrypted, and aligned with the data protection section in this policy in order to minimize the risk of data exposure before it is shared with the requestor.

Table 12: Roles and responsibilities for data sharing.

Data Governance Role	Responsibility
Data Governance Council Chairman	• Accelerate decisions, facilitate dispute resolutions, and escalate issues (when applicable) to avoid business disruptions. • Oversight of data governance business as usual activities
Data Owner	• Accountable to identify potential risks to the company across all four data classification levels related to the Data Sharing section. • Data Owners will communicate the data-sharing requirements across their business units.
Data Steward	• Responsible for assisting Data Owners with the identification of potential risks across the datasets.
• Data Custodian	• Responsible for ongoing identification of potential risk with data within a dataset that is shared with the requestor
• Stewardship leads	• Responsible for monitoring compliance based on reported noncompliance issues by Data Stewards. • Responsible to raise the issues of non-compliance to Data Owners and report to Stewardship Leads for monitoring the compliance of Data Sharing.

6.14. Data Collection

Objective: Governs the collection and sourcing of all data processed and/or controlled by the Company.

6.14.1. Data Collection

a) Data must only be collected when there is a legitimate business purpose that is aligned with the strategic intent of the company.

b) All data collected must be classified by the Data Steward as per the Data Classification Matrix.

c) When external parties are collecting data on behalf of the company, data protection NDA between the company and external parties should be signed to ensure confidentiality and security.

d) The Data Governance Council must approve all new data collection mechanisms.

e) Business and/or technical metadata details of collected data elements must be captured and documented in the centralized metadata repository.

f) Data collected must go through the CDE Identification process to identify and tag any potential CDEs.

6.14.2. Data Sourcing

a) All data sourcing requests must be captured and documented in the BRSD.

b) All new data sourcing requests must be supported by a comprehensive business justification.

c) The pre-requisite for external data sourcing is to ensure that the company informs the external sourcing party that the company will use the data at its discretion unless otherwise stated.

d) Data Owner is accountable to coordinate with T&I to have suitable controls and formal communication for external data sourcing to avoid any legal actions against the company.

e) Business Glossary must contain the new terms and business definition for newly sourced data as per Metadata Management.

f) Before sourcing any data and keeping a single version of the truth, the metadata repository should be used by Stewardship Leads, to cross-check whether this set of data exists.

g) Sourced data elements must go through the CDE Identification process to identify and tag potential CDE.

h) All data sourced must be classified by the Data Steward as per the Data Classification Matrix.

i) Data Stewards assesses all data sourced through the Data Quality Assessment process to ensure high-quality data before making it available for consumption.

j) Data Sourcing exercises and environments must be aligned with Data Access and Usage to ensure that only appropriate individuals have adequate access.

k) Data sourced must be aligned with enterprise architecture policies and standards to ensure data lands in an appropriate environment.

Table 13: Roles and responsibilities for data collection.

Data Governance Role	Responsibility
Data Governance Council Chairman	• Accelerate decisions, facilitate dispute resolutions, and escalate issues (when applicable) to avoid business disruptions. • Oversight of Data Governance business as usual activities
Data Owner	• Data Owner is accountable for having Data Governance controls in place for external data sourcing to avoid any legal actions against TAWAL. • Data Owner is accountable to approve or reject data sourcing and collection requests related to their respective data domain.
Data Steward	• Responsible for ensuring that the data collection and sourcing exercise complies with data governance policies and processes. This includes metadata management (business definitions), data quality assessment and CDE identification. • Responsible for clarifying the business definitions for the requested Data Source.
Data Custodian	• Data Custodians formulate technical recommendations for Data Sourcing and how/where to source the data from • Responsible to adhere to the data governance policies and processes. This includes technical metadata management, data quality assessment and CDE identification.
Stewardship Leads	• Validate the outcome of data collection and sourcing requests as part of the closure activity.

7. Asset Labeling/Classification, Data Classification, Data Retention Mapping

<table>
<tr><th colspan="2">Asset Classification</th><th>Data Classification</th><th>Data Retention Types</th><th>Data Retention Duration</th></tr>
<tr><td colspan="2">Very High</td><td>Confidential</td><td>Medium Term Data</td><td>Between 6 months and 5 years</td></tr>
<tr><td colspan="2">High</td><td>Restricted</td><td>Long Term Data</td><td>More than 5 years</td></tr>
<tr><td>Significant</td><td>Moderate</td><td>Internal</td><td rowspan="2">Short Term Data</td><td rowspan="2">Less than 6 months</td></tr>
<tr><td colspan="2">Low</td><td>Public</td></tr>
</table>

8. Waiver Criteria

This policy is intended to address Cyber Security requirements. If needed, waivers shall be formally submitted to the TAWAL Cyber Security Steering Committee, including justification and benefits attributed to the waiver. The policy waiver period is a maximum of 4 months and shall be reassessed and re-approved, if necessary, for a maximum of three consecutive terms.

9. Monitoring and Review

This policy document shall be regularly monitored for compliance obligations and reviewed on an annual and requirement basis.