Category	Data Governance and Management	**Policy Number**	UNI-DGM-101
Classification	Public	**Version**	1.0
Responsible Office	VP-CEO	**Policy Owner**	SFD Director
Date Approved	3 June 2025	**Effective Date**	3 June 2025
Date Last Reviewed	New Policy	**Due Date for Next Review**	3 June 2028

جـــامـعـة زايـــد
ZAYED UNIVERSITY

POLICY
Data Governance Policy

1. Purpose

This policy addresses the data governance framework which governs policies on data sharing, data classification, open data, data retention and continuity, and data quality. It outlines data management definitions, and the roles and responsibilities involved in data governance at Zayed University.

2. Scope of Application

This policy applies to all Zayed University faculty, staff, consultants, service provider contractors, and temporary employees.

3. Definitions

Data Catalog	A Data Catalog helps the University organize, manage, and access its data assets. It provides a centralized repository for metadata, improves data governance, and enhances collaboration by making data discovery and utilization easier for researchers, faculty, and administrators.
Data Classification Matrix	The document that gives information about the data classification (Restricted, Confidential, Internal, Public) applied to an information asset.
Data Domain	A specific area of data related to a particular business function or process, such as registration, research, finance, or procurement.
Data Governance Committee (DGC)	A data-related decision-making body that sets priorities for data governance objectives, standards, and policies, and resolves issues escalated from other levels of the University and external stakeholders.
Data Owner	Anyone who holds responsibility for data quality, and ensures that all necessary security measures are taken to protect data from unauthorized access and data leakage for their University unit.

Data Recipient	Any user with whom the data is being shared, or the receiver of the data
Data Requestor	Government Ministry, Government Entity, University employee, third-party contractor, service provider, consultant, University partner, or anyone authorized to access the University Information Systems and/or University data
Data Steward	A person who is a subject area expert and has technical knowledge of a particular University unit, and who is given this role by a Data Owner
Data Sub-Domain	A specialized area within a broader data domain, like student GPA or faculty workload.
Data User	University employee, contractor, third-party agent, or anyone authorized to access the University's Information Systems and/or University data
External Stakeholder	A person or organization that is not a university employee or student
Information Assets	Personal data, sensitive data, research data, and other types of data that are collected, stored, and processed by the University
Internal Stakeholder	A University employee or student
Metadata	Information provided about specific data (such as where and when the data was collected, created, organized, transmitted, and updated; and the person responsible) so that the data can easily be found, retrieved, and used
NDA	Non-Disclosure Agreement
Open Data	Any data which can be shared with the public without any restrictions through the University's website
PII	Personally Identifiable Information such as Emirates ID, Passport Number, Visa details, etc.
SFD	Strategy and Future Department
University	Zayed University
VP-CEO	Vice-President and Chief Executive Officer

4. Policy

4.1 Zayed University ("**University**") understands the role of data in achieving strategic and operational objectives and the need to govern it through well-defined roles and responsibilities.

4.2 For data to be a strategic asset, it requires strong governance practices and structure. At the University, a Data Governance Framework has been established with the vision of ensuring secure access to accurate, and reliable data that can enable the University to achieve its objectives.

4.3 The Data Governance Framework consists of core elements that include the Data Governance Committee ("**DGC**"); policies and procedures on data sharing, data classification, data retention and continuity, data quality, and open data; the implementation of a centralized data catalog consisting of information about data in the systems being used at Zayed University, and the creation and maintenance of an accurate and accessible data archive.

4.4 The DGC will oversee the overall Data Governance Framework and the development of policies and procedures for the management of data across the University.

5. Roles and Responsibilities

5.1 Data Governance Committee

The DGC is appointed by the Vice-President and Chief Executive Officer ("**VP-CEO**") and is the main decision-making body for data policies at the University. DGC responsibilities include but are not limited to:

a) Identifying Data Owners and Data Stewards for each department and communicating/assigning the roles and responsibilities of individuals involved in data governance.

b) Ensuring the effective implementation, enforcement, and periodic reviews of all the policies and procedures covered under this policy.

c) Ensuring that employees are aware of the content of this policy and are trained appropriately.

d) Ensuring all policy owners are required to review their policies at least once every three years and kept relevant.

e) Taking appropriate action for any data breaches such as accidental or deliberate exposure of data to unauthorized parties, data theft, misuse of data, or insufficient data protection, reported by any member of the University.

f) Making decisions about whom to share data with, including internal and external stakeholders.

g) Providing approval on Data Classifications on the data domain and data sub-domain levels.

h) Ensuring only authorized users have access to analytical reports (datasets created using student, faculty, procurement, finance, research, etc.) and security is correctly implemented.

j) Overseeing and approving data quality rules defined by Data Owners.

k) Making appropriate decisions for any system discontinuity and the retention of its data by validating the potential implications.

5.2 Data Owners

Data owners' responsibilities include but are not limited to:

a) Establishing rules for the appropriate use and protection of data.

b) Providing input to information system owners regarding security requirements and security controls for the information systems where their data resides.

c) Deciding who is authorized to access information assets and defining the type of privileges and/or access rights to grant.

d) Conducting an annual review and assessment of data classifications, and adjusting them as required.

e) Ensuring that the data for which they are responsible is properly classified throughout its lifecycle from creation, through modification, to destruction; including recognizing and downgrading the data classification when protection is no longer needed at the original level; and that all required metadata fields are completed.

f) Ensuring that the data for which they are responsible is stored appropriately, either on the University's servers or on a University-approved cloud storage service, in line with its data classification.

g) Ensuring that any violations of this policy are reported, particularly those that are subject to privacy laws or other regulated disclosure notifications.

h) Granting access and officially assigning custody of an information asset.

j) Verifying that relevant measures are in place to guarantee the proper accessibility of data.

k) Ensuring that access rights are reviewed when a user's data access requirements change (e.g., due to job reassignment).

m) Ensuring business terms and the data dictionary are correctly populated on the Data Catalog for other departments' usage.

5.3 Data Stewards

Data Stewards' responsibilities include but are not limited to:

a) Overseeing and managing data sharing requests received from anyone, ensuring the request is aligned with policy guidelines and that procedures are applied correctly.

b) Obtaining approval from Data Owners before sharing data whenever a new request is received from any individual (internal or external).

c) Managing agreements and setting guidelines with internal and external stakeholders to fulfill any data-sharing requests.

d) Ensuring data quality strategy execution, defining and monitoring rules for data quality, and making necessary updates in the source systems to improve the quality of data.

e) Identifying data issues using data profiling results, manual analysis by exploring data and finding any issues detected in data (such as incorrect data values, missing values, etc.), escalating issues when necessary, and developing a root cause analysis.

f) Ensuring clear and consistent business and data definitions are defined on the Data Catalog for the data assets.

g) Ensuring data classifications are correctly defined on the Data Catalog for all the columns of their data.

h) Updating descriptions, classifications, etc., on the Data Catalog as and when changes have occurred.

j) Maintaining detailed records of all data-sharing requests and activities, including requests, and approvals from DGC, NDAs, etc., on the Zayed University network drive.

6. Related Policies and Laws

- UNI-DGM-201 Data Classification
- UNI-DGM-202 Data Sharing
- UNI-DGM-203 Open Data

7. Administration

This policy is administered by SFD.

8. Revision History

Date	Revision	Ver.
23 June 2025	Chair of the Board Decision issued (PD#22 of 2025).	
3 June 2025	Approved by FAIAC.	1.0
22 May 2025	Endorsed by UPSC.	
23 October 2024	Endorsed by the Data Governance Committee.	
3 October 2024	New policy drafted.	