


Policy Group	Data Governance and Management	Policy Number	UNI-DGM-XXX	 جامعة زايد ZAYED UNIVERSITY
Classification	Public	Version	1.0	
Responsible Office	VP-CEO	Policy Owner	SFD Director	
Date Approved	26 June 2025	Effective Date	26 June 2025	
Date Last Reviewed	New Procedures	Due Date for Next Review	3 June 2028	

PROCEDURES

Data Sharing

1. Introduction

These Procedures establish clear guidelines for responsible and secure information exchange with internal and external stakeholders and websites. Adherence to the Procedures ensures confidentiality, promotes accountability, streamlines processes, fosters collaboration, and maintains compliance with UAE Government and Zayed University (“**University**”) regulations, thus supporting the University's mission of academic excellence and integrity.

2. Definitions

DGC	Data Governance Committee
Least Data Sharing Principle	Users must ensure that only a minimal amount of data is shared (to share only what is needed) to protect privacy and still enable useful data access.
NDA	Non-disclosure Agreement
PII	Personally Identifiable Information such as Emirates ID, Passport Number, Visa details, etc.
SFD	Strategy and Future Department
University	Zayed University

3. Data Classification

The University classifies data into four (4) categories: public, internal, confidential, and restricted. Each category has different levels of access and sharing requirements, and users are required to comply with the Data Sharing Policy and Procedures when sharing data within the University or with external Stakeholders.

Classification Category	Risk	Description	Potential Impact
Restricted	High	Data that is highly sensitive and should only be accessed by authorized personnel on a need-to-know basis. It includes data that, if compromised, could cause significant harm to the University.	The impact of this data being revealed to the public can be devastating to the University.

Confidential	Medium	Data that is strictly protected and only accessible to authorized individuals. This may include PII, trade secrets, financial information, or any information that could cause harm if compromised.	The leakage of confidential data can result in several consequences.
Internal	Low	Data that is generated and owned by the University. This may include student information, employee data, financial records, and other sensitive information that is not intended for public usage.	The publication of this data may cause some inconvenience.
Public	No Impact	Data that is freely available and accessible to the public. This type of data can include government publications, open-access research papers, census data, and other freely available datasets.	A breach of public data will not harm individuals or the University.

4. Submission of Data Requests

ACTIVITY	RESPONSIBILITY	STEPS
Identify the required data	Data Requestor	1. Based on the use case for which data is required, identify the data using the least-data sharing principle.
Write a data request email to the Data Owner	Data Requestor	1. Identify the system and data owner of the data being requested through the Data Catalog on the Intranet. 2. Write an email to the data owner by specifying the relevant details of the request such as purpose, data requested, expected date to receive data, etc. For any ad-hoc data requests from external entities attach DGC approval (if applicable).

Sample Form to Submit Data Request:

Question	Answer
What is the Purpose of the Data Request?	
Which data is being requested? Mention the name of the Department (if applicable)	
What is the expected date to receive the data?	
Does the data request contain any Restricted or Confidential data?	
Comments/Special Instructions	

5. Review of Data Sharing Request

ACTIVITY	RESPONSIBILITY	STEPS
Review the data-sharing request details.	Data Owner	<ol style="list-style-type: none"> 1. Go through the data request in detail and understand the purpose for the data that has been requested. 2. DGC approval is required for any ad-hoc data requests submitted that are not already classified and approved. 3. A Non-Disclosure Agreement (NDA) must be signed for any data requests received from consultants and other external institutions unless already approved by DGC. 4. For ad-hoc requests, forward the request to the Data Steward for extracting and sending the data to the recipient/s. 5. If it's a periodic request, the report access should be given to the data requestor.
Perform authorization assessment	Data Steward	<ol style="list-style-type: none"> 1. Follow the Data Classification Matrix to verify if the data request contains any Restricted or Confidential data. 2. Verify if the requestor has permission to access any data that is Restricted or Confidential. 3. Individual or department requests for access to Restricted or Confidential data must be sent to DGC for approval.

6. Submission of Data to Recipient

ACTIVITY	RESPONSIBILITY	STEPS
Identify Information Assets	Data Steward	<ol style="list-style-type: none"> 1. Identify the systems and respective columns by using the Data Catalog. 2. Obtain approvals from Data Owners if applicable.
Extract data	Data Steward	<ol style="list-style-type: none"> 1. Extract specific columns from the datasets as per the data request to follow the least-data-sharing principle.
Prepare Data	Data Steward	<ol style="list-style-type: none"> 1. Apply data anonymization as per the Classification Matrix if the data contains any Restricted or Confidential data. 2. Format the data (as close as possible) as per the data sharing request. 3. Protect data files/documents using a password.

Share Data to Recipients	Data Steward	<ol style="list-style-type: none"> 1. Send password-protected documents when sharing data via email or uploading to any shared-drive location. 2. Include a confidentiality statement at the end of e-mails when sharing data to notify the recipient of the Restricted or Confidential data.
--------------------------	--------------	---

7. Recording of Data Sharing Requests

ACTIVITY	RESPONSIBILITY	STEPS
Track all data requests	Data Steward	<ol style="list-style-type: none"> 1. Maintain detailed records of all data-sharing requests and activities, including requests, approvals from DGC, NDAs, etc. in a Zayed University shared drive.

8. Revision History

Date	Revision	Ver.
30 June 2025	VP-CEO Decision issued (VPD#61 of 2025).	
26 June 2025	Approved by the VP-CEO.	1.0
22 May 2025	Approved by the UPSC.	
9 December 2024	Endorsed by the Data Governance Committee.	
17 September 2024	New procedures drafted.	