


Policy Group	Data Governance and Management	Policy Number	UNI-DGM-201	 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 Classification

1. Introduction

These procedures provide guidelines to ensure information assets are classified according to the Data Classification Matrix, and the steps that need to be taken to ensure the correct handling of data in line with its data classification.

2. Identification of Information Assets and Data Owners

ACTIVITY	RESPONSIBILITY	STEPS
Identification of Information Assets and Owners	Data Owners / Data Stewards	<ol style="list-style-type: none"> 1. Create an inventory of the information systems for which the data classification needs to be applied in the University. 2. Identify data owners for all the information assets based on the data domains/subject areas. If the identified owners are not a single person but a group of people, DGC appoints a single point of contact and forms a hierarchy under that individual.

Example 2.1: Data Classification Form/Template

Data Domain	Data Sub-Domain	Public	Internal	Confidential	Restricted
Student	Student Statistical Information	Y			
Student	Scholarship / Sponsorship			Y	
Student	Personal Identifiable Information			Y	

Example 2.2: Data Classification Questionnaire

The higher the ratings the data receives, the more restrictive the data classification should be.

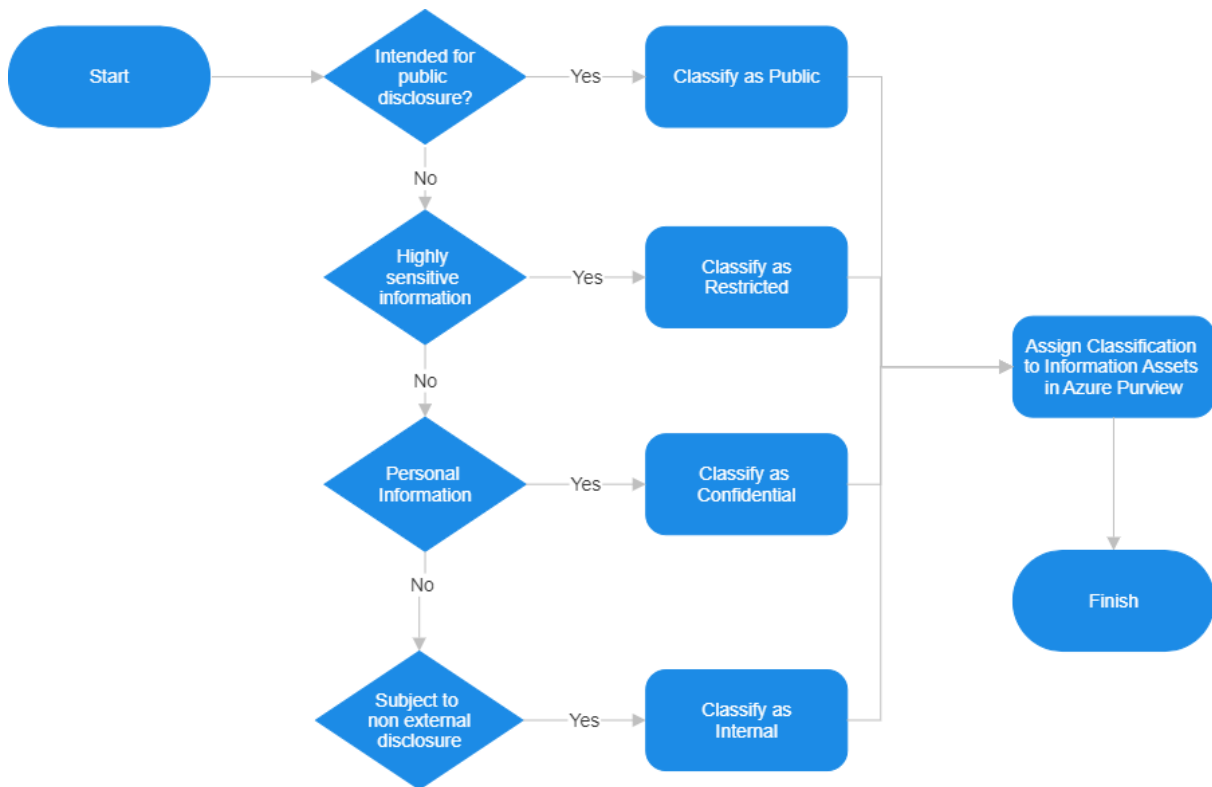
Answers to the questions listed below are provided to assist data owners in properly classifying their data. The importance of each of these items should be rated using a High (H), Medium (M), or Low (L) rating scale.

QUESTIONS	RATING
How important is it to the University that this data be known only by authorized people?	
How important is it to the University that this data be accurate?	
How important is it to the University that this data be available to authorized people only?	
How important is this data to regulatory guidelines compliance?	
How important is this data to privacy law compliance?	
How important is this data to regulatory compliance?	
How serious would the impact be if this data reached an unintended audience?	
How likely is it that this data could be used by someone to target employees, customers, shareholders, trading partners, facilities, or operations?	
How valuable would this data be to someone intent on causing harm to Zayed University?	
How likely is it that this data could be used in conjunction with public data to cause harm to Zayed University or its employees, customers, shareholders, or trading partners?	

3. Assignment of Data Classification

ACTIVITY	RESPONSIBILITY	STEPS
Assigning Appropriate Data Classification to Identified Information Assets Data	Data Owners / Data Stewards	<ol style="list-style-type: none"> 1. Data Stewards are to fill Data Classification Form/Template and submit it to the data owner for approval. 2. Data Stewards classify data according to its value and risk for Zayed University as described in the Data Classification Policy. <ul style="list-style-type: none"> • Value refers to how much data contributes to business objectives. • Risk refers to how much the data exposes the University to potential threats, such as legal, regulatory, reputational, or operational issues. 3. Data Classification is to be applied in two stages. <ol style="list-style-type: none"> a. Apply at the domain/sub-domain level b. Based on sub-domain classification, apply it at the column level 4. Ensure that all required metadata fields are filled out in the form/template.
Reclassifying Classified Data (if applicable)	Data Owners/ Data Stewards	<ol style="list-style-type: none"> 1. If data confidentiality is altered or incorrectly classified, reclassify the data according to the Data Classification Matrix. 2. Update the respective labels in the Data Catalog to reflect the new classification. <p>NOTE: This step is particularly important when dealing with data that falls into the Confidential or Restricted classification.</p>
Implement the data classification for information assets in the Data Catalog.	Data Stewards	<ol style="list-style-type: none"> 1. Map the information assets in the Data Catalog with the data classifications as available in the form/template shared by the data owners. 2. Always keep the Data Catalog up to date with the relevant classification. In case of reclassification, ensure the changes are applied to the Data Catalog.

3.1 Data Classification Decision Tree



3.2 Changing or Downgrading Classifications

ACTIVITY	RESPONSIBILITY	STEPS
Reclassifying Data	Data Owners / Data Stewards	<ol style="list-style-type: none"> Perform regular audits of data classifications which may require changes in the following scenarios: <ol style="list-style-type: none"> When the original classification level for an information asset is no longer valid, downgrade/change the data classification level. When the data becomes inactive or is no longer in regular use. Obtain approval from the data owner/DGC to change, downgrade, or change classification with any classification category. Perform respective updates in the Data Catalog.

4. Data Handling Requirements

The following details data handling requirements (data access and data usage) for each classification level throughout the data lifecycle.

4.1 Data Access

Handling Control	Public	Internal	Confidential	Restricted
NDA	No NDA requirements	NDA or other contractual protection is recommended before data access by external entities	NDA is required before data access by external entities	NDA is required before data access by external entities
Access Controls Methods	No special requirements	<ul style="list-style-type: none"> A strong password is enforced Periodic access review and validation recommended 	<ul style="list-style-type: none"> Multi-factor authentication and strong passwords are recommended. Data access must be controlled by conditional access based on approval of the data owner/DGC. Access rights must be limited- to the least privilege. Periodic access review and validation required. 	<ul style="list-style-type: none"> Multi-factor authentication and strong passwords are recommended. Data access must be controlled by conditional access based on approval of the data owner/DGC. Access rights must be limited- to the least privilege. Periodic access review and validation required.
Authorization	Open access, no specific authorization required	Role-based access control (RBAC)	<ul style="list-style-type: none"> RBAC with detailed permissions restricting access to confidential information. Column-level security is to be implemented by methods of data masking/hashing for unauthorized users. 	<ul style="list-style-type: none"> RBAC with strict permissions and segregation of duties to minimize access to highly sensitive data. Column-level security is to be implemented by methods of data masking/hashing for unauthorized users.

4.2 Data Usage

Handling Control	Public	Internal	Confidential	Restricted
All Data	No monitoring is required. Can be used freely without restrictions.	<ul style="list-style-type: none"> • Periodic monitoring to ensure appropriate use. • Used for business purposes only. • Must adhere to University policies. 	<ul style="list-style-type: none"> • Frequent monitoring to ensure appropriate use. • Used for authorized purposes only. • Strict adherence to University policies. 	<ul style="list-style-type: none"> • Strict monitoring, with immediate alerts for any unauthorized access attempts. • Extremely strict usage policies; limited to specific authorized groups.
Websites	No special requirements.	Posting to publicly accessible internet sites is prohibited.	<ul style="list-style-type: none"> • Posting to publicly accessible internet sites is prohibited. • Posting to internal and external websites is prohibited unless approved by DGC, Security, and Legal teams. 	<ul style="list-style-type: none"> • Posting to publicly accessible internet sites is prohibited. • Posting to internal and external websites is prohibited unless approved by DGC, Security, and Legal teams.

5. 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.	
23 October 2024	Endorsed by the Data Governance Committee.	
17 October 2024	New Procedures drafted.	