


<b>Category</b>	Data Governance and Management	<b>Policy Number</b>	UNI-DGM-201	 مَامعة زَايد ZAYED UNIVERSITY
<b>Classification</b>	Public	<b>Version</b>	1.0	
<b>Responsible Office</b>	VP-CEO	<b>Policy Owner</b>	SFD Director	
<b>Date Approved</b>	3 June 2025	<b>Effective Date</b>	3 June 2025	
<b>Date Last Reviewed</b>	New Policy	<b>Due Date for Next Review</b>	3 June 2028	

## POLICY

### Data Classification

#### 1. Purpose

This policy outlines the steps taken to identify, classify, label, and protect data that has been created and is owned by Zayed University.

#### 2. Scope of Application

- 2.1** Unless specifically exempted in writing by the Data Governance Committee, all Zayed University data, regardless of format, is covered by this policy.
- 2.2** The responsibilities for data classification, protection, and handling as stated in this policy apply to all Zayed University faculty, staff, consultants, service provider contractors, and temporary employees.

#### 3. Definitions

<b>CAFO</b>	Chief Administration and Finance Officer
<b>Data Classification Framework</b>	An approach that is used to categorize data elements based on their sensitivity, value, and criticality to the University. It helps the University identify and manage its data effectively, ensuring proper handling, protection, and compliance with regulations.
<b>Data Classification Matrix</b>	A document that gives information about the data classification (Restricted, Confidential, Internal, Public) applied to an information asset.
<b>Data Owners</b>	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 department
<b>Data Users</b>	University employees, contractors, third-party agents of the University, or anyone authorized to access the University's Information Systems and/or data.
<b>DGC</b>	Data Governance Committee
<b>Executive Management</b>	VP-CEO, Provost, and CAFO
<b>External Party</b>	A person or organization that is not a part of the University community

<b>ITD</b>	Information Technology Department
<b>PII</b>	Personally Identifiable Information such as Emirates ID, Passport Number, Visa details, etc.
<b>Provost</b>	Provost and Chief Academic Officer
<b>Senior Leadership</b>	Associate Provost, Assistant Provosts, Deans, Directors, Registrar, and equivalent
<b>SFD</b>	Strategy and Future Department
<b>University</b>	Zayed University
<b>University Community</b>	University students and employees
<b>VP-CEO</b>	Vice-President and Chief Executive Officer

#### 4. Policy

**4.1** Zayed University (“**University**”) will develop, implement, and apply standards, controls, and procedures to ensure information assets are properly classified and protected from unauthorized access, disclosure, or loss.

**4.2** The University is committed to ensuring that all University members including staff, faculty, contractors, temporary employees, etc. are aware of the importance of data protection and the importance of acting in a way that ensures appropriate data use.

**4.3** All University data must always be handled and processed (data usage, encryption, sharing, authorization), according to applicable laws and regulations.

##### **4.4 Classification and Labeling**

Data must be classified based on its sensitivity and risk by the Data Classification Matrix. This in turn will indicate the security measures that must be taken and the requirements for data handling.

**4.4.1** A data classification framework has been established to protect University data and to minimize any risk that could negatively impact the University’s operations or its ability to fulfill its mission.

**4.4.2** The default classification for all data will be “Internal” unless labeled or explicitly defined otherwise by the data owner in line with the University Data Classification Matrix.

##### **4.5 Declassification and Downgrade**

The University will establish a sensitivity and downgrading process that supports a downgrading mechanism used to reduce the classification and control of data. The downgrading process must be limited to the data owners authorized to change the data classification level governed by the Data Governance Committee (“**DGC**”).

**4.5.1** The classification of University data will be reevaluated annually to ensure the assigned classifications are still relevant according to any changes to the legal and contractual obligations as well as changes to the use of data and its value to the University.

**4.5.2** This evaluation must be carried out by the respective data owners identified for the information assets.

- 4.5.3** If a data owner determines that the classification of a specific data set has changed, an in-depth analysis must be performed by the relevant data owners to determine whether existing controls are consistent with the new classification, and the matter must be discussed in a DGC meeting. If gaps exist, they must be corrected as soon as possible.

#### **4.6 Data Breach Reporting**

Any suspected breach of this policy or compromise of confidential and restricted data by an unauthorized party must be reported immediately to the DGC. Upon receiving the report, the DGC Information Security lead will be responsible for conducting and coordinating an investigation (under the advice of legal counsel, if appropriate) in line with the University Incident Management and Response process. The investigation must include conducting a careful analysis of the situation, making recommendations for corrective action, and submitting a report of the incident to appropriate members of the Executive Management, Senior Leadership, and relevant University units as needed.

### **5. Data Classification Matrix**

<b>Classification Category</b>	<b>Description</b>	<b>Potential Impact</b>
Restricted	<ul style="list-style-type: none"> <li>• Data that is highly sensitive and should only be accessed by authorized personnel on a need-to-know basis.</li> <li>• Explicit approval of the DGC is required to access this data, even for those with a need to know.</li> <li>• Restricted data and devices with restricted data must be stored in a secure (locked) location.</li> <li>• Restricted data must always be encrypted.</li> </ul>	<ul style="list-style-type: none"> <li>• Restricted data is information whose loss, corruption, or unauthorized disclosure would be catastrophic or severely damaging to the University's reputation or business position, resulting in significant financial, reputational, and/or legal loss.</li> <li>• Impact includes violating regulatory requirements and contractual requirements.</li> </ul>
Confidential	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Explicit approval of the DGC is required to release this data outside its originating unit, even to those with a need to know.</li> <li>• Access to confidential data requires authentication and password protection.</li> </ul>	<ul style="list-style-type: none"> <li>• Confidential data is data whose loss, corruption, or unauthorized disclosure would seriously harm the University's reputation or business position, resulting in severe financial, reputational, and/or legal loss.</li> <li>• Impact includes violating contractual requirements, damaging the University's reputation and exposing high to very high-risk information.</li> </ul>

Internal	<ul style="list-style-type: none"> <li>• Data that is generated and owned by the University. This may include student information, employee data, financial records, and other sensitive information not intended for public usage.</li> <li>• Internal data requires the data owner's approval for accessing the data inside or outside the University.</li> </ul>	<ul style="list-style-type: none"> <li>• Internal data is data whose loss, corruption, or unauthorized disclosure is of importance only inside the University and, therefore, would not result in a tangible business, financial, or legal loss.</li> <li>• Impact includes violating contractual requirements and damaging the University's reputation.</li> </ul>
Public	<ul style="list-style-type: none"> <li>• Data that is freely available and accessible to the public. This type of data can include government publications, open-access research papers, census data, open data, and other freely available datasets.</li> <li>• Dissemination of this data does not require specific approval from the data owner.</li> <li>• Public data can be viewed or copied without restriction and can be accessed by external parties from any location.</li> <li>• The decision to make a piece of data public should be deliberate and approved by the data owner.</li> </ul>	<ul style="list-style-type: none"> <li>• No damage would occur if public information were available to unauthorized parties either external or internal.</li> <li>• The impact would not be damaging or a risk to the University's business operations.</li> </ul>

## 6. Related Policies and Laws

- Telecommunications Regulatory Authority (TRA) Regulations for Information Technology Security in Federal Entities
- National Electronics Security Authority Security Controls
- UNI-GOV-303 Definition of Senior (Top) Positions

## 7. Administration

This policy is administered by SFD in coordination with ITD.

## 8. Revision History

Date	Revision	Ver.
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.	