TABLE OF CONTENTS

Institutional Data Governance Policy

Article (1): Definitions

Institutional Data : Information created, collected, acquired, processed, stored, maintained, or published by the university in support of its academic, research, administrative, or operational functions, including but not limited to student records, faculty and staff data, research outputs, financial records, UAEU department level operational data, and UAEU or internal department policies or procedures, in any format i.e., digital, electronic, or physical and used for teaching, learning, research, compliance, institutional management, and service delivery.

Data Governance : A framework of policies, procedures, guidelines, roles, and responsibilities that ensures the effective management, protection, quality, and security of data across its lifecycle, aiming to maintain data accuracy, accessibility, consistency, security, and compliance with applicable laws and regulations, while establishing clear guidelines for ownership, stewardship, classification, access control, and accountability to support decision-making, operational efficiency, and compliance within UAEU.

Data Classification : The process of categorizing UAEU data based on its sensitivity, criticality, and regulatory requirements, ensuring that data is handled, stored, and protected according to its classification to support compliance, security, and risk management

Data Integrity : The assurance that UAEU data remains accurate, consistent, and unaltered during its lifecycle, protecting it from unauthorized changes, and ensuring its trustworthiness for decision-making and compliance.

Data Security : The implementation of controls to safeguard UAEU data from unauthorized access, alteration, loss, or disclosure, ensuring its confidentiality, integrity, and availability in line with information security and regulatory requirements.

Data Privacy : The management and protection of personal and sensitive data, ensuring its collection, processing, and storage comply with relevant or applicable privacy laws, regulations, and UAEU policies to uphold individuals' privacy rights.

Metadata : Descriptive information about UAEU data that provides context for its management, use, and retrieval, ensuring effective data governance, traceability, and compliance through clear identification of data attributes such as origin, format, and ownership.

Master Data	:	Core data essential for business operations, such as student records, faculty information, and organizational identifiers, that serves as the authoritative reference point for the organization and must be managed for accuracy, consistency, and accessibility
Data Lifecycle	:	The stages through which UAEU data progresses, from creation or acquisition to storage, use, sharing, and eventual deletion or archiving, with governance controls ensuring that data is properly managed and protected at every phase to meet regulatory, security, and operational requirements.
Data Access Control		The policies and technical measures that regulate and monitor access to data, ensuring that only authorized individuals or systems can access, modify, or share data based on roles and permissions, thereby enforcing security and compliance.

Article (2): Introduction

Overview

This policy establishes the framework for the governance, management, protection, and utilization of institutional data across the University to ensure its integrity, security, and accessibility.

Scope

1. This policy applies to all institutional data, regardless of the format, means, or location of storage, including electronic, print, audiovisual, backup, and archived data.

2. This policy applies to all members of the University community and any individuals or entities granted access to institutional data.

3. This policy does not apply to data generated exclusively for scientific research, which is governed by separate research policies and regulations.

Objectives

1. Establish a secure and well-structured data environment that ensures the accuracy, consistency, and reliability of institutional data to support data-driven decision-making and enhance operational efficiency.

2. Promote accountability and responsible data stewardship across all University units.

3. Improve data accessibility and usability while ensuring seamless integration of data systems to enhance efficiency and reduce costs.

4. Mitigate data security risks, including breaches of confidentiality, unauthorized access, and data loss.

5. Ensure transparency and consistency in data governance practices and procedures.

6. Safeguard the interests of all data stakeholders, including students, faculty, staff, and external partners.

7. Provide comprehensive training for staff and management on best practices in data governance.

8. Ensure compliance with all applicable data-related laws and regulations in the UAE, including those governing data protection, privacy, cybersecurity, and electronic transactions.

9. Establish clear data classification guidelines to facilitate proper data handling, storage, and protection within the University

Article (3): Stakeholders

1. Vice Chancellor:
   Holds executive authority over the University's data governance framework and ensures its strategic alignment with institutional objectives.

2. Data Trustees:
   Deputy Vice Chancellors, responsible for establishing strategic policies and overseeing data governance within their respective functional areas.

3. Data Governance Council:
   Chaired by the Vice Chancellor and composed of the Director of the Institutional Effectiveness Organizational Unit, the Chief Information Officer, and Data Trustees. Provides oversight, strategic direction, and policy recommendations on data governance matters.

4. Data Stewards:
   Designated by Data Trustees and are, generally, operational managers in a functional area with day-to-day responsibilities for coordinating data governance activities and for managing business processes.

5. Data Management Committee:
   Comprising the Director of the Institutional Effectiveness Organizational Unit, the Chief Information Officer, Data Stewards, and other members appointed by the Vice Chancellor. It oversees the development and implementation of the data governance strategy, ensuring alignment with UAEU's objectives and regulatory requirements while promoting a culture of data-driven decision-making across the institution.

6. Data Custodians:
   IT and Business specialists responsible for managing and maintaining institutional data within information and IT systems.

7. Chief Information Officer
   Provides strategic oversight for data governance initiatives, ensures data governance is integrated into IT operations, and aligned with IT strategy and enterprise architecture.

8. Information Technology Organizational Unit
   Implements security measures, data privacy controls, access controls, and encryption. Identify and mitigate technology risks associated with data governance and ensure secure handling and transfer of sensitive data.

9. Legal Affairs Organizational Unit
   Ensure data governance policies comply with relevant regulations (e.g., GDPR, UAE PDPL). Manage legal risks related to data privacy, security, and intellectual property and Work with IT and business teams to enforce regulatory standards.

10. Data Users:
    University community members or external individuals who have been granted access to institutional data.

Article (4): Data Governance Principles

1. Institutional data is a strategic asset solely owned and managed by the University.

2. Clear roles, responsibilities, and processes for managing institutional data shall be defined and maintained.

3. Institutional data shall be organized by functional areas that align with the University's strategic and operational activities.

4. Each functional area is responsible for implementing and maintaining procedures for managing institutional data, ensuring data quality, security, and compliance with this policy.

5. All data-related activities are guided by a centralized governance structure that promotes consistency, transparency, and compliance with UAE and international data management standards.

6. Data governance supports change management activities concerning data values, structure, and metadata while promoting standardization of enterprise data.

7. Data governance and stewardship processes ensure transparency, making it clear how and when data-related decisions and controls are introduced.

8. A structured approach to managing the data lifecycle, including creation, retention, archival, and disposal, shall be adopted. Compliance metrics and monitoring mechanisms shall be in place to track performance and address deviations.

9. Data risk management practices shall be implemented to assess, mitigate, and manage risks such as unauthorized access, breaches, and regulatory non-compliance. Incident management protocols shall ensure timely reporting, investigation, and resolution of data-related issues.

10. Data governance shall be aligned with key UAEU business processes, including strategic planning, risk management, and IT service management, in accordance with relevant ISO standards and UAE regulations.

11. Data-related decisions, processes, and controls shall be auditable. Regular audits shall evaluate data governance compliance and identify areas for improvement.

12. Institutional data shall be safeguarded according to the Data Classification framework, with appropriate access, storage, and disposal protocols.

13. Institutional data shall be accessible subject to security restrictions outlined in this policy and the IT Policy.

14. The Data Governance Policy and procedures shall comply with applicable UAE laws and institutional accreditation standards.

15. UAEU enforces strict data privacy and security measures, ensuring compliance with relevant regulations and industry standards such as ISO 27001. The Division of IT shall implement data protection processes to safeguard sensitive information.

16. Each functional area or department shall be responsible for identifying and ensuring compliance with applicable data governance requirements.

17. UAEU ensures the availability and seamless flow of data across systems to support decision-making, research, and operational efficiency while adhering to privacy and security protocols.

18. UAEU promotes open data initiatives by publishing non-sensitive datasets in machine-readable formats to foster transparency, innovation, and collaboration.

19. Ongoing data governance training programs shall be developed and implemented for various stakeholders, ensuring they have the necessary knowledge and skills to adhere to governance principles and practice.

Article (5): Procedures

Procedures of the Data Governance policy to be approved by the Vice Chancellor