IIUM DATABASE GUIDELINES - DRAFT

IIUM ICT GUIDELINES

PREPARED FOR:
International Islamic University Malaysia

PREPARED BY:
Information Technology Division

IIUM ICT Guidelines

Document Change Log

Release Version	Date	Pages Affected	Remarks/Change Reference
Version 1.0	September 2025	-	*Initial Submission*
Version 1.1	October 2025	5	

Responsibility and Activity Log

Requestor	Description	Submission Date	Approval Date
Abu Hurairah A. Manaf	Endorsement from ITD Management	09/09/25	11/09/2025
Abu Hurairah A. Manaf	Add clause 4.1 and 4.2	28/10/2025	

IIUM ICT Guidelines

1. OBJECTIVE

The objective of this document is to outline the responsibilities for managing IIUM databases, including standards for access requests, authorisation procedures, user rights and responsibilities, revocation processes, and documentation requirements, ensuring compliance with University policies.

2. SCOPE

The scope of this document covers the management, access, and maintenance of institutional data critical to the University's administrative, academic, and operational functions. It applies to both production and non-production database environments, and is intended for system implementers, software engineers, and developers managing applications that interact with multi-user databases, as well as database programmers and administrators responsible for updates and maintenance.

This guidelines exclude data primarily used for academic research, which is governed by separate University policies. This framework ensures the integrity, security, and effective utilisation of the University's database resources.

3. TERMS AND DEFINITIONS

Term	Definition
IIUM	The International Islamic University Malaysia, otherwise known as the "University".
ITD	Information Technology Division
CIO	Chief Information Officer
Data Owner	Centre of Studies or Administrative Offices that owns and manages the assigned institutional data. Data Owner is also responsible for processes that relate to the data.
Database Administrator	One or more IT personnel assigned to manage University centralized databases.
Data Administrator	One or more IT personnel assigned by ITD to manage data and application systems of the data owners.
Data Users	University individuals who need and use University data as part of their assigned duties or in fulfillment of their roles in the University community.

Data	Pieces of information on the University which resides in the University Data Centre and other authorized electronic data repositories of the University.
Data Element	Any unit of data defined for processing, for example, staff number, name, address and student matric number.

4. GUIDELINES

4.1. This guideline shall be implemented in compliance with the IIUM's Anti-Bribery Management System (ABMS) in accordance with ISO 37001:2025 requirements, to ensure transparency, integrity, and accountability in all processes. All procurement activities shall reflect a commitment to fostering an anti-bribery culture, recognizing and managing conflicts of interest, and applying enhanced due diligence to third parties and sustainability-related aspects. Any actual or suspected bribery, corruption, or conflict of interest shall be reported through secure and protected channels, with whistle-blower protections in place.

4.2. This guideline shall be implemented in accordance with IIUM's ICT Security Procedure in compliance with ISO/IEC 27001:2022 requirements to ensure confidentiality, availability and integrity in all processes. All processes, decisions, and activities under this guideline must uphold the principles of confidentiality, availability and integrity as to protect the information data and assets.

4.3. DATA/DATABASE ACCESS AND AUTHORISATION

4.3.1. Access to protected University data and databases shall be authorised and managed to ensure appropriate usage and compliance with relevant policies.

4.3.2. Access may be granted for various purposes, including:

- New system development (e.g. creation of new schemas),
- System integration (via database tables, views, or APIs),
- Data access for other authorised purposes.

4.3.3. New system development (new schema):

- Complete the ***Request/Revoke Access to Database/System form*** and submit it to the Database Administrator.
- Submit the required documentation as specified in section 4.3: ***Standard Database Documentation***.

4.3.4. System Integration (via database tables, views or APIs):

- Obtain approval from the relevant Data Owner (refer to the ***Guideline on Electronic Data Management*** for the list of Data Owners) and

complete the ***Data Integration Request Form.***

- Authorisation shall be granted only for specific database tables or views within the relevant application, limited to what is necessary for system integration.
- Refer to the ***Guideline for IIUM API*** for integration using APIs.

4.3.5. Data access for other authorised purposes should follow the ***Data Request and Distribution Procedure****.*

4.4. DATABASE CREDENTIALS

Database authentication credentials are essential for authorising applications to access University databases. However, improper use, storage, or transmission of these credentials may compromise University data.

4.4.1. Each application or system serving a specific business function must have its own unique database credentials. Credential sharing between applications is strictly prohibited.

4.4.2. Database passwords must comply with established password best practices or University-defined password standards.

4.4.3. Access to database credentials must be strictly limited to individuals whose roles require such access.

4.4.4. Credentials must be securely stored in a configuration file that is:

- Separate from the source code,
- Located outside the web root,
- Protected with strict access permissions.

4.4.5. Files containing live or production database credentials must not be uploaded to Source Code Management (SCM) systems.

4.4.6. Database credentials must be restricted to accessing only the specific databases required. Development and production environments must use separate databases and credentials. The production database must be configured to accept connections only from the designated application server.

4.5. DATABASE DOCUMENTATION

Comprehensive database documentation is essential to ensure the proper, efficient, and sustainable use of databases. It serves as a valuable reference for administrators, developers, and stakeholders, helping them understand the

database structure, relationships, and constraints, and supporting maintainability throughout its lifecycle.

4.5.1. A complete **Database Design Document** must accompany all requests for new schemas. The creation of a new schema will proceed only after the documentation has been reviewed and approved by the Database Administrator.

4.5.2. The **Database Design Document** must include the following components:

- Table Descriptions – including the table name, purpose, list of columns with data types and constraints, primary key, foreign keys, and any relevant notes.
- Entity-Relationship Diagrams.
- Index Documentation
- Version Control
- Stored Procedures and Functions Documentation.
- Details of Data Access – including access from other schemas, whether through direct database tables or views.

4.5.3. The following forms must be completed and submitted to the Database Administrator, as applicable:

- Migration of Application System & Database from Development to Production Environment
- IT Change Request (Non-Standard Change)

4.6. DATABASE CHANGES MANAGEMENT.

Effective database change management is essential for preserving data integrity, security, and availability within the University. It involves tracking, controlling, and implementing changes to the database such as schema modifications, data updates, database views, functions, or stored procedures to ensure these changes are handled efficiently and do not compromise performance or functionality.

4.6.1. The Database Change Request form must be completed and submitted to the Database Administrator for all standard database changes.

4.6.2. The Database Design Document must be updated to reflect the changes, and the version control system should be revised accordingly.

4.6.3. All changes must be thoroughly tested in the development environment before deployment to the production environment.

4.6.4. Changes must be communicated via email or other formal channels to the relevant development teams to ensure they are informed and able to reflect the updates. This helps prevent disruptions to other applications or systems.

4.7. CENTRALISE REFERENCE CODE SCHEMA

To maintain consistency in reference codes and avoid the existence of multiple versions for similar data, a centralised reference code schema has been introduced.

4.7.1. The respective owner of each reference code table is responsible for ensuring that the data is kept up to date.

4.7.2. Replication of reference code tables is strictly prohibited to maintain data consistency.

5. IMPLEMENTATION AND NON-COMPLIANCE

The Director of ITD holds the responsibility for the implementation of this guideline and shall take necessary actions in the event of violation of this guideline.

6. ENFORCEMENT

This guideline is applicable to the University community and any infringement of the guideline may subject to disciplinary actions and any other actions deem necessary.

7. MAINTENANCE OF GUIDELINES

The Information Technology Division is responsible for the formulation and maintenance of this guidelines.

8. RELATED POLICIES/STANDARDS/PROCEDURES/GUIDELINES

8.1 This guideline shall be read together with the following or any documents which recently approved:

8.1.1 ICT Regulations
8.1.2 IIUM ICT Policy
8.1.3 IIUM ICT Security Procedure
8.1.4 Guidelines on Electronic Data Management
8.1.5 Guideline for IIUM API

8.1.6 Data Request and Distribution Procedure

8.1.7 Penggunaan Dan Pemakaian Data Dictionary Sektor Awam (Ddsa) Sebagai Standard Di Agensi-Agensi Kerajaan

8.1.8 RUU Perkongsian Data 2024