Guidelines on Electronic Data Management

International Islamic University Malaysia (IIUM)

Document Change Log

Version	Revision	Date	Pages Affected	Remarks/Change Reference
Version 01	00	18/01/2023	-	Endorsement from ITD Management
Version 01	01	25/06/2025	Page 10	Endorsement from ITD Management
Version 01	02	26/10/2025	Page 10 , Page 11	Endorsement from ITD Management
Version 01	03	27/03/2026	Page 5	Change OSIC name to OSIT

Responsibility and Activity Log

Requestor	Description	Submission Date	Approval Date
Nurmaliza Jumaat	Change of Electronic Data Management Committee to Guideline on Electronic Data Management	18/01/2023	18/01/2023
Abu Hurairah A. Manaf	Add Information and Data Deletion Clause (3.7)	23/06/2025	25/06/2025
Abu Hurairah A. Manaf	Add clause 3.8 , Section 7		
Abu Hurairah A. Manaf	Endorsement from ITD Management	20/11/2025	20/11/2025
Abu Hurairah A. Manaf	Endorsement from ITD Management	27/03/2026	15/04/2026

1. OBJECTIVE

This guideline serves as a reference for the management of IIUM data, including the responsibilities of those involved in electronic data management activities at the University, and outlines how electronic data should be treated and managed.

2. TERMS AND DEFINITIONS

Term	Definition
IIUM	The International Islamic University Malaysia, otherwise known as the "University".
ITD	Information Technology Division
CDO	Chief Digital Officer
Data Management Working Committee	A working committee that is responsible for the University data governance. The working committee is a sub- committee of the Information and Communication Sub Committee.
Information and Communication Sub Committee	A working committee that is responsible to determine web strategies, KM University-wide implementation, and formulation of university data management policy, procedure, and standards.
Data Owner	Centre of Studies or Administrative Offices that own and manage the assigned institutional data. The Data Owner is also responsible for processes related to the data.
Database Administrator	One or more IT personnel assigned to manage University centralised databases.
Data Administrator	One or more IT personnel assigned by ITD to manage the 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 fulfilment of their roles in the University community.
Data	Pieces of information on the University, which resides in the University Data Centre and other authorised 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.

Data Centre	Centrally managed facility that houses and maintains back-end IT systems, data stores, servers, and databases.
Data Repository	A set-up within the overall IT structure which keeps various kinds of university electronic data.
Application system	A computer program that is internally developed or procured and is designed to carry out specific tasks. It is typically used by data owners for work purposes.

3. GUIDELINES

3.1. Data Management Working Committee

3.1.1 The Director of OSIT (Office of Strategic Institution Transformation), who oversees data management, shall chair the Data Management Working Committee.

3.1.2 The Data Management Working Committee shall be comprised of data owners, data users, database administrators, data administrators, and other assigned University officers relevant to serving the function of the committee.

3.1.3 The secretariat of the Data Management Working Committee shall be an assigned officer(s) from the Office of Strategic Institution Transformation.

3.1.4 There shall be a Data Management Working Committee, which performs the following functions:

i. Review, formulate and oversee University data management policy, procedure, and standards

ii. Review, formulate and oversee the University data quality management process

iii. Handle University data sensitivity matters, which include validity, confidentiality, and security

iv. Manage user awareness and training in data management

3.2 Data Owners

Data Owners shall perform the following roles and responsibilities:

3.2.1 Responsible for the data quality, confidentiality, integrity, and availability

of data.

3.2.2 Promote and enhance the value of data for university-wide purposes and facilitate data sharing and integration

3.2.3 Determine the access levels of the data owned

3.2.4 Determine and authorise the access rights and privileges of the data owned.

3.2.5 Manage the operational matters of the assigned University data.

3.2.6 Responsible for ensuring that application systems developed shall use data according to the IIUM Standard Data Dictionary.

3.2.7 Responsible for data analysis of the assigned University data.

3.2.8 Provide management information to support University decision-making.

3.2.9 Fulfil external reporting requirements related to the assigned University data.

3.2.10 Resolve queries on the assigned University data.

3.3 Database Administrators

Database administrators shall perform the following roles and responsibilities:

3.3.1 Manage University centralised databases towards data security, confidentiality, integrity, and availability.

3.3.2 Maintain and manage the IIUM Standard Data Dictionary.

3.3.3 Develop and implement IIUM Standard Data Dictionary policy, procedures, and guidelines.

3.3.4 Develop and implement data retention and archiving policies, procedures, and guidelines.

3.4 Data Administrators

Data Administrators shall perform the following roles and responsibilities:

3.4.1 Manage the repositories where the assigned University data are stored.

3.4.2 Manage the applications and reporting systems that relate to the assigned University data.

3.4.3 Enhance his/her knowledge on the business of the data which he/she is managing.

3.5 Data Users

Data Users shall perform the following roles and responsibilities which include:

3.5.1 Access and use data only in the conduct of university business.

3.5.2 Respect the confidentiality and privacy of individuals whose records they may access.

3.5.3 Comply with the ethical, commercial, legal, security and other restrictions determined by the University that relate to the data in which they have access to.

3.6 Data

3.6.1 Every data source and dataset shall have a designated Data Owner.

3.6.2 Data shall be stored in an official University repository.

3.6.3 Data shall be defined consistently across the University.

3.6.4 Data element names, formats and codes shall be consistent across all repositories and application systems that use the data; and shall be consistent with the IIUM Standard Data Dictionary. In the absence of standards in the University Data Dictionary, the MAMPU Data Dictionary Sektor Awam shall be referred to.

3.6.5 Every data element shall be created by one data owner only and there shall be no subsequent creation of the same data element.

3.6.6 The structure of data shall be controlled to ensure minimal implications on business and systems.

3.6.7 Data shall be recorded in an auditable and traceable manner and comply with any agreed change control process.

3.6.8 Data shall be properly backed up and restored according to the University data back-up and restore procedure.

3.6.9 A data element shall be considered as university data if it is relevant to planning, managing, operating, or auditing a major administrative function of the University.

3.6.10 University data shall be subjected to data audit by the relevant University authority.

3.6.11 The data shall be stored in the University repository and accessible through the following application systems:

No	Category	Information	Application system
1	Employee data	Staff personal record, service record, appraisal, benefits, and payroll	IIUM Human Resource Information System (HURIS)
2	Financial data	Investment records, financial statements & Reports, Capital Construction Records	IIUM Financial Information System (IFIS)
3	Research data	Research funded by university grants & research funded by outside bodies -Research reports and research data -Patent, trademark, and other intellectual property records	Research Management System V2 (RMSV2)
4	Student data	Undergraduate and postgraduate student records. Student exam records and graduation records, Theses and dissertations records.	Student Information System (SIS)
5	Academic data	Records documenting the teaching and learning process, e.g. course outlines, curricula, syllabi, reading lists and other courseware objects. – Prospectus - Accreditation records	ECUREv2 system, OBEM system

6	Alumni data	Alumni Chapters, Newsletter, Publicity, Career development	IIUM Alumni Portal, Student Information System (SIS)
7	Publication data	Books, Book chapters, Journal articles, Conference papers - Newsletter	IREP, Student repository, IIUM Journal system
8	Electronic filing	HR Related Records and documents Administrative Records and documents	IIUM Document Management System (IDMS), Seascape
9	Online learning records	Learning materials, student assignments	Italeemc, italeem_archiv e
10	Legal records	MOU/MOA, Litigation, Debt Recovery, Disciplinary	IIUM Legal Monitoring System (ILMOS)
11	General Administrat ive Records	Includes minutes of meetings, reports, programmes of key events, photographs, Videos, Sound recordings, News clippings, Policies and Procedures, Manuals, Speeches and Presentations, Publications and Project file	Office Desktops, Personal Laptops, and External Storage equipment.
12	Physical Developm ent Records	Records include architectural blueprints, aerial photographs, planning drawings, changes to plans, and other graphic representations related to buildings, systems, and land. -Project construction records.	I-space – is on space management/facilities only. Upgrading Work System – for renovation and upgrading records.
13	Institutional Records	All types of university records fall into a range of categories including,	University databases and systems, IIUM Portal,

		but not limited to: administrative records, alumni records, environmental health and safety records, faculty records, financial/budget records, legal and regulatory compliance records, personnel records, operations records (facilities management), student academic records, student life records, university research data and compliance, and university statistics.	Office Desktops, Personal Laptops, External Storage equipment

3.7 Information and Data Deletion.

3.7.1 This applies to all electronic records, including but not limited to:

- Documents, emails, and databases
- System logs and backups
- Any other digital files stored on university-managed systems, cloud services, or external storage devices.

3.7.2 All data deletions must be approved by the designated data owner before execution.

3.7.3 Only authorised personnel may perform data deletion after receiving approval.

3.7.4 Data must not be deleted before the end of its defined retention period, except in cases of legal or regulatory exceptions.

3.7.5 Data must be securely deleted using an appropriate method based on its classification, ensuring it cannot be accessed, retrieved, or reconstructed. Techniques such as secure overwriting, cryptographic erasure, degaussing, or physical destruction should be applied as required. Additionally, all copies, including backups and temporary files, must be securely deleted or sanitised in accordance with university policies.

3.7.6 All data deletions must be recorded to ensure compliance and accountability.

Records should include details such as the date and time of deletion, the data type and classification, the approved requestor (Data Owner), the method used, and the authorised personnel responsible for the deletion. Documentation must be retained in accordance with university policies and may be subject to audit.

3.8. This guideline shall be implemented in accordance with IIUM's ICT Security Policy 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. IMPLEMENTATION AND NON-COMPLIANCE

4.1 The CDO holds the responsibility for the implementation of this guideline and shall take necessary action in the event of a violation of this guideline.

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

5. ENTITIES AFFECTED BY THIS GUIDELINE

This guideline shall apply to all staff.

6. MAINTENANCE AND MONITORING OF THE GUIDELINES

The Data Management Working Committee is responsible for the formulation and maintenance of this guideline.

7. RELATED POLICIES/STANDARDS/PROCEDURES/GUIDELINES

This guideline shall be read together with the following documents or any documents below:

7.1 IIUM ICT Policy
7.2 ICT Regulations
7.3 IIUM ICT Security Policy
7.4 IIUM Records Management Policy
7.5 Management of Data Backup
7.6 MAMPU Data Dictionary Sektor Awam (DDSA)

7.7 Personal Data Protection Act 2010 (PDPA)

7.8 IIUM Standard Data Dictionary (iPerform system)

7.9 IT Infrastructure Library (ITIL)

7.10 Control of Business IT (COBIT)

Title of Guideline	:	Guidelines on Electronic Data Management
Number of Guidelines	:	IIUM-ISMS-L3-015
Approving Authority	:	ITD Management
Approval Date	:	15/04/2026
Effective Date	:	15/04/2026
Version No.	:	01
Revision No.	:	03