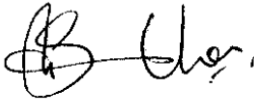




Document Title:	Institutional Data Policy		
Department / Division:	Information Communications Technology (ICT)		
Approved By:	Document Reference / Policy No.:	ADM-P-004	
Chief Information Officer		Issuance Date:	01 February 2015
		Revision Date:	25 May 2024
		Revision No.:	4.0
		Number of Pages:	6

**1.0 Policy Statement:** This policy outlines the principles and guidelines governing the collection, storage, access, and use of data to ensure compliance with legal and regulatory requirements.

**2.0 Purpose:** The purpose of this policy is to establish a framework for the management of Aga Khan University's (AKU) Institutional Data and the responsibilities for the protection of those data. To ensure the protection of the university's institutional data from accidental or intentional unauthorized access, damage, alteration, or disclosure while preserving the ability of authorized users to access and use institutional data for appropriate university purposes. AKU members require access to institutional data in support of the university's teaching, research, patient care and administration.

**3.0 Scope:** This policy covers all AKU's data including administrative, patient care data, research data and teaching material across all departments and systems, irrespective of the data location or the type of device it resides on. This policy is applicable to all users accessing institutional data in any way which includes all students, faculty members, employees, third parties, donors, and other staff (the members).

**4.0 Responsibilities:** University members act in one or more specific roles when collecting, maintaining, accessing, or using institutional data and must understand and fulfill the responsibilities associated with their roles.

4.1. Data Trustees: Senior university executives with management responsibility for areas of institutional data. Data Trustees work with the Chief Information Officer to ensure that the

appropriate resources (staff, technical infrastructure, etc.) are available to support the data needs of the entire university.

4.1.1. Their responsibilities include but not limited to:

- i. Assigning and overseeing Data Stewards.
- ii. Overseeing the establishment of data policies in their areas.
- iii. Determining legal and regulatory requirements for data in their areas.
- iv. Promoting appropriate data use and data quality.

4.1.2. Institutional Data covered by this policy include but are not limited to:

<b>Institutional Data Segment Type</b>	<b>Data Trustee</b>
Research Data	Dean of Research and Graduate Studies
Teaching data and material	Provost
Administrative data	Vice President, HR
Patient care data	Vice President, Health Services

4.2. Data Stewards: University officials with direct operational responsibility for one or more types of institutional data.

4.2.1. Their responsibilities include but not limited to:

- i. Develop a data access plan.
- ii. Create and perform processes to capture and fix inconsistent or erroneous data.
- iii. Certify data stored in University's Data Repository.
- iv. Participate in security access audits.
- v. Interpreting and assuring compliance with university policies and regulations regarding the release of, responsible use of, and access to institutional data.
- vi. Developing, implementing, and maintaining a Business Continuity Plan for institutional data under their control.
- vii. Providing communications and education to data users on appropriate use and protection of institutional data.

4.3. Data Custodian: University units or employees responsible for the operation and management of systems and servers which collect, manage, and provide access to institutional data.

4.3.1. Their responsibilities include but not limited to:

- i. Maintaining physical and system security and safeguards appropriate to the classification level of the data in their custody.
  - ii. Complying with applicable university policies.
  - iii. Maintaining Disaster Recovery plans and facilities appropriate to business needs and adequate to maintain or restart operations in the event systems or facilities are impaired, inaccessible, or destroyed.
  - iv. Managing Data User access as prescribed and authorized by appropriate Data Stewards.
  - v. Complying with all laws, regulations, and policies applicable to the institutional data in their custody.
- 4.4. Data Users: University units or members using institutional data in the conduct of university business.

4.4.1. Their responsibilities include but not limited to:

- i. Complying with laws and regulations as well as university policies, procedures, and standards associated with the institutional data used.
- ii. Using institutional data only as required for the conduct of university business within the scope employment.
- iii. Implementing safeguards prescribed by appropriate data stewards for confidential data.
- iv. Ensuring the appropriateness, accuracy, and timeliness of institutional data used for the conduct of university business.
- v. Reporting any unauthorized access, data misuse, or data quality issues to the appropriate data steward for remediation.

**5.0 Data Classification:** Data classification provides a basis for understanding and managing institutional data based on the level of criticality and required confidentiality of the data. Accurate classification provides the basis for an appropriate and cost-effective level of security and protection. Consistent with AKU's data classification scheme, the university's Institutional Data must be assigned to one of four classifications:

- 5.1. Public: covers information that may be disclosed to any person inside or outside the University. Although security mechanisms are not needed to control disclosure and dissemination, they are still required to be protected against unauthorized modification and/or destruction of information.
- 5.2. Internal: covers information that requires protection against unauthorized disclosure, modification, destruction, and use, but the sensitivity of the information is less than that for confidential information.
- 5.3. Confidential: covers sensitive information about individuals and sensitive information about the University. Information received under this classification requires a high level of protection against unauthorized disclosure, modification, destruction, and use.

- 5.4. Highly Confidential: covers sensitive information which, if it becomes available to unauthorized users, creates risk for identity theft and has the potential to cause serious damage or distress to individuals or serious damage to the University's interests if disclosed inappropriately.

## **6.0 Policy Content:**

- 6.1. All institutional data is owned by AKU and, as such, all members of the University are responsible for appropriately respecting and protecting the asset.
- 6.2. University members working with or using institutional data in any manner must comply with all applicable university policies, procedures and standards, and all applicable contracts and licenses. Examples include the University's Policy on Use of ICT Resources.
- 6.3. The university's Institutional Data must be assigned to one of four defined classifications (Public, Internal, Confidential, and Highly Confidential) as per the university's policy on Information Classification and handling.
- 6.4. Roles, including those both of individuals with data responsibilities and of eligible users, are necessary to support data integrity and security.
- 6.5. All computers and devices used with Institutional Data must be configured, operated, and maintained in accordance with university information security policies.
- 6.6. Personal use of institutional data, including derived data, in any format and at any location, is prohibited.
- 6.7. All remote sites of AKU must access Institutional data following the same university policies.
- 6.8. Procedures must be developed to address those cases where an individual seeks permission to access data outside of the access plan and defined roles.
- 6.9. Institutional Data must be safeguarded and protected to maintain the confidentiality and privacy of personally identifiable information. It must be protected from deliberate, unintentional, or unauthorized alteration, destruction and/or inappropriate disclosure or use in accordance with established university policies and practices and laws.
- 6.10. Each functional area must develop and implement processes for identifying and correcting erroneous or inconsistent data. When and if erroneous or inconsistent data has been identified, the Data Steward from the corresponding functional area shall within five business days either correct the data or escalate the issue to the appropriate Data Trustee.
- 6.11. Access to the institutional data should be based on the business needs of the organization and as per the policies. It must be available to authorized users only.
- 6.12. Before individuals will be allowed to access University data, training in the use and attributes of the data, functional area data policies, and University policies regarding data is mandatory.

- 6.13. Breaches, losses, or unauthorized exposures of confidential data must be immediately reported to the area specific data trustees or the Chief Information Officer for investigation and must be handled in accordance with the University Policy on Confidentiality.
- 6.14. Data Trustees, Data Stewards, Data Custodians, or specific university units may have additional policies for institutional data within their areas of operational or administrative control.

**7.0 Disciplinary Actions:** The failure by the users to comply with these policies may result in loss of access to some or all institutional data and/or loss of access privileges to institutional data. In addition, violators of these policies may be subject to criminal and/or civil penalties and to disciplinary action, up to and including termination.

**8.0 Compliance Reference:**

- 8.1. ISO27001:2013 International Standard
- 8.2. General Data Protection Regulation (GDPR)
- 8.3. Data Protection Act, Kenya

**9.0 Measures of Compliance:** Compliance with this policy will be verified through internal and external audits.

**10.0 Reference:** This policy satisfies the following requirements:

Clause Reference	Name of the Clause	Control reference	Name of control	Name of the Standard / Regulation
-	-	-	-	ISO/IEC 27001:2013
-	-	-	-	GDPR
-	-	-	-	Data Protection Act, Kenya

**11.0 Institutional Documents Policies:**

- 11.1. Acceptable Use of ICT Assets Policy
- 11.2. AKU's Policy on Information Classifications and Handling
- 11.3. AKU's Policy on Confidentiality

**12.0 Annexure:** No additional documents provided.

### 13.0 Author(s)

Name	Designation
Suneel Kumar Panjwani	Head of Information Security
Saad Ameen	Information Security Specialist
Atif Ali	Information Security Analyst
Samra Sabir	Information Security Analyst

**14.0 Key Searchable Terms:** Institutional data, classification, data stewards, trustees, Data User, Data Custodian

**15.0 Revision History:** This policy is subject to review and revision every two (2) years to ensure its effectiveness and alignment with changing organizational requirements and regulatory obligations.

### 16.0 Documents Change Record:

Review #	Review Date (dd-mm-yyyy)	Description Of Change	Identification of Change
04	25-05-2024	Reviewed and updated the document in accordance with the latest policy document template.	-