### Policy on Institutional Data

1. **Purpose**
The purpose of this policy is to establish a framework for the management of Aga Khan University’s (AKU or University) Institutional Data (as defined below) and the responsibilities for the protection of those data. This is 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. The university’s institutional data is a valuable asset and must be maintained and protected as such.

2. **Organizational Scope**
This policy covers all AKU information, 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. This includes all students, faculty members, employees, third parties and other staff (the members). They need to be aware of this policy, their responsibility and legal obligations. All users are required to comply with this policy in order to protect themselves and AKU from any legal actions.

3. **Definition**
Institutional Data: All data created, collected, maintained, recorded or managed by the university, its staff, and agents working on its behalf. This may include but not limited to:

- Data used for planning, managing, operating, controlling, or auditing university functions;
- Research data and teaching material
- Patient care data

4. **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:

- 4.1.1.1. Assigning and overseeing Data Stewards.
- 4.1.1.2. Overseeing the establishment of data policies in their areas.
- 4.1.1.3. Determining legal and regulatory requirements for data in their areas.
- 4.1.1.4. Promoting appropriate data use and data quality.

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

<table>
<thead>
<tr>
<th>Institutional Data Segment Type</th>
<th>Data Trustee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research Data</td>
<td>Dean of Research and Graduate Studies</td>
</tr>
<tr>
<td>Teaching data and material</td>
<td>Provost</td>
</tr>
<tr>
<td>Administrative data</td>
<td>Vice President, HR</td>
</tr>
<tr>
<td>Patient care data</td>
<td>Vice President, Health Services</td>
</tr>
</tbody>
</table>

4.2. **Data Stewards**: University officials with direct operational responsibility for one or more types of institutional data. Their responsibilities include but not limited to:

- 4.2.1. Develop a data access plan.
- 4.2.2. Create and perform processes to capture and fix inconsistent or erroneous data.
- 4.2.3. Certify data stored in University’s Data Repository
- 4.2.4. Participate in security access audits.
4.2.5. Interpreting and assuring compliance with University policies and regulations regarding the release of, responsible use of, and access to institutional data.

4.2.6. Developing, implementing, and maintaining a Business Continuity Plan for institutional data under their control.

4.2.7. 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. Their responsibilities includes but not limited to:

- 4.3.1. Maintaining physical and system security and safeguards appropriate to the classification level of the data in their custody.
- 4.3.2. Complying with applicable university policies.
- 4.3.3. 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.
- 4.3.4. Managing Data User access as prescribed and authorized by appropriate Data Stewards.
- 4.3.5. 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. Their responsibilities includes but not limited to:

- 4.4.1. Complying with laws and regulations as well as university policies, procedures, and standards associated with the institutional data used.
- 4.4.2. Using institutional data only as required for the conduct of university business within the scope employment.
- 4.4.3. Implementing safeguards prescribed by appropriate data stewards for confidential data.
4.4.4. Ensuring the appropriateness, accuracy, and timeliness of institutional data used for the conduct of university business.

4.4.5. Reporting any unauthorized access, data misuse, or data quality issues to the appropriate data steward for remediation.

5. Data Classification

5.1. 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:

5.1.1. Public: covers information that may be disclosed to any person inside or outside the University.

5.1.2. 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.

5.1.3. Confidential: covers sensitive information about individuals and sensitive information about the University.

5.1.4. 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. 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. Procedures must be in place to guide appropriate data access, ensure the security of the data, and provide a means to address procedural exceptions.
6.3. 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 University’s Policy on Use of IT Resources.

6.4. The university’s Institutional Data must be assigned to one of four defined classification (Public, Internal, Confidential, and Highly Confidential) as per the university’s policy on Information Classification and handling.

6.5. Roles, including those both of individuals with data responsibilities and of eligible users, are necessary to support data integrity and security.

6.6. All computers and devices used with Institutional Data must be configured, operated, and maintained in accordance with university computer security policies.

6.7. Personal use of institutional data, including derived data, in any format and at any location, is prohibited.

6.8. All remote sites of AKU must access Institutional data following the same university policies.

6.9. Procedures must be developed to address those cases where an individual seeks permission to access data outside of the access plan and defined roles.

6.10. 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.

6.11. 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.

6.12. 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.

6.13. 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.
6.14. 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.

6.15. 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. Enforcement

7.1. The failure by the users to comply with these Policies may result in loss of access to some or all of 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. Related Policies

8.1. AKU’s Policy on Use of IT Resources: http://akuportal.aku.edu/IT/IT%20Policies/ADM-P-010%20(Use%20of%20IT%20Resources%20Policy).pdf

8.2. AKU’s Policy on Information Classifications and Handling: http://akuportal.aku.edu/IT/IT%20Policies/Policy%20on%20Information%20Classification%20And%20Handling.pdf

8.3. AKU’s Policy on Confidentiality: http://vportal.aku.edu/hrpolicies/pdf/HRER-06.pdf

9. References


<table>
<thead>
<tr>
<th><strong>Division:</strong></th>
<th>Information Technology</th>
<th><strong>Title:</strong></th>
<th>Policy on Institutional Data</th>
<th><strong>Number:</strong></th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Issue/Effective Date:</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>Issue/Effective Date:</strong></td>
<td>1st February 2015</td>
</tr>
<tr>
<td><strong>Department/Section:</strong></td>
<td>IT/All</td>
<td><strong>Approved by:</strong></td>
<td>Chief Information Officer</td>
<td><strong>Revision:</strong></td>
<td>1.0</td>
</tr>
<tr>
<td><strong>Revision Date:</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>Revision Date:</strong></td>
<td>1st February 2015</td>
</tr>
<tr>
<td><strong>Page:</strong></td>
<td>Page 7 of 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>