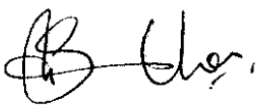




Aga Khan University Hospital

Document Title:	Information Classifications and Handling		
Department / Division:	Information Communications Technology (ICT)		
Approved By:		Document Reference / Policy No.:	ADM-P-003
Chief Information Officer		Issuance Date:	01 February 2015
		Revision Date:	25 May 2024
		Revision No.:	2.0
		Number of Pages:	9

1.0 Policy Statement: This policy establishes guidelines to ensure that information receives an appropriate level of protection in accordance with its importance to AKU.

2.0 Terms and Definitions:

- 2.1 ISO27001: International Organization for Standardization
- 2.2 AKU: Aga Khan University
- 2.3 ICT: Information Communications Technology

3.0 Purpose: The purpose of this policy is to establish a framework for classifying and handling Aga Khan University's (AKU or University) information based on its level of sensitivity, value, and criticality to the University. Classification of information will aid in determining associated rules for the handling of each class of information to ensure the appropriate level of security (confidentiality, integrity, and availability) of that information.

4.0 Scope: This policy covers all AKU information, irrespective of the data location or the type of device it resides on. The handling rules are applicable to all users of AKU's ICT facilities. This includes all students, faculty members, employees, and the users are required to comply with this policy and make third parties aware of this policy to protect themselves and AKU from any legal action. The scope of this policy is applicable for all AKU domestic and global locations. In case of any specific local country regulations not addressed by this information security policy, the local AKU local office will develop and maintain local policy to comply with the local regulatory requirements with the approval of Head of Information Security and Chief Information Officer (CIO).

5.0 Responsibilities:

- 5.1 Users: All users of AKU and third parties who handle information on behalf of AKU have a responsibility for ensuring that appropriate security controls are applied in respect of the information they are handling for the University. Appropriate security controls may vary

according to the classification of the information and the handling rules for the relevant category shall be followed. All users shall report issues of concern in relation to the application of this policy, including alleged non-compliance, to their manager as soon as possible.

- 5.2 Information Owners: Information Owners are responsible for assessing information and classifying its sensitivity accordingly. They are also responsible for applying the appropriate controls to protect that information.
- 5.3 ICT Services: ICT Services shall be responsible for providing the mechanisms and/or instructions for protecting electronic information while it resides on any AKU owned/controlled system.
- 5.4 Records Management Staff:
 - 5.4.1 Records Management Staff shall be responsible for providing the instructions to protect and preserve any physical or electronic records.
 - 5.4.2 All information held by or on behalf of AKU shall be categorized according to the Information Classifications. The categorization shall be determined by the originator of the information and all information falling into the classified categories shall be marked as such.
 - 5.4.3 Information shall be handled in accordance with the Information Handling policy and where information falls within more than one category, the higher level of protection shall apply in each case.
 - 5.4.4 Where a third party will be responsible for handling information on behalf of AKU, the third party shall be required by contract to adhere to this policy prior to the sharing of that information.

6.0 Information Classifications:

- 6.1 Public: This classification covers information that may be disclosed to any person inside or outside the University. It covers all the information that falls in either of the defined classes. 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. Data may include but is not limited to current courses and key information sets.
- 6.2 Internal: This classification 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. Examples use-only information include but not limited to internal memos, correspondence, and other documents whose distribution is limited as intended by the data owner.
- 6.3 Confidential: This classification covers sensitive information about individuals and sensitive information about the University. Such information has the potential to cause a negative impact on individuals' or the University's interests. Information receiving this classification requires a high level of protection against unauthorized disclosure, modification, destruction, and use. Specific categories of confidential information include personally identifiable information about:
 - 6.3.1 Current and former students including student academic, disciplinary, and financial records.

- 6.3.2 Current, former, and prospective employees, including employment, pay, benefits data, and other personnel information.
 - 6.3.3 Research information related to a potential or pending patent application.
 - 6.3.4 Certain University business operations, finances, legal matters, or other operations of a particularly sensitive nature.
 - 6.3.5 Information security data, including passwords. Information about security-related incidents.
- 6.4 Highly Confidential: This classification 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. This information includes but not limited to:
- 6.4.1 National Identity Card number
 - 6.4.2 Driver's license numbers.
 - 6.4.3 Medical records
 - 6.4.4 Investigations/disciplinary proceedings
 - 6.4.5 Bank details (sort code/account number)
 - 6.4.6 Credit Card Details (PAN/CVV2/Expiry Date/PIN)
 - 6.4.7 Passport Details
 - 6.4.8 University Strategies
 - 6.4.9 Donors, potential donors, and other University clients.
 - 6.4.10 Financial Data
 - 6.4.11 "On-going" and submitted Research Papers
 - 6.4.12 Access codes for higher risk areas
 - 6.4.13 Username and Passwords

6.5 Summary Table:

	Public	Internal	Confidential	Highly Confidential
Example	Schedule of Classes	Memos and minutes	Academic records	Bank Account Numbers

Access	Minimal controls to prevent unauthorized modification/deletion	Determined by data owner	Limited based upon need to know, named users only, training and confidentiality agreement required	Provide access only when no alternative exists. Treat as toxic. Named users only, training and confidentiality agreement required
Use	Post as needed	Determined by data owner	No posting, limited reporting and copying.	Use only when no alternative exists. Treat as toxic. No posting, limited reporting and copying
Transmission	Minimal controls to prevent unauthorized modification	Determined by data owner	Confidential envelope; encrypted transmission	Hand deliver; encrypted transmission
Storage	Minimal controls to prevent unauthorized modification	Determined by data owner	Locked private office or cabinets; secure server room; should encrypt on desktops, laptops, media	Locked private office or cabinets; secure server room; should encrypt on desktops, laptops, media
Destruction	No Controls	Determined by data owner	Shred paper; secure delete files, wipe media	Shred paper; secure delete files, wipe media

7.0 Policy Content:

7.1 Asset Inventory: An inventory should be maintained of all the University's major information assets and the ownership of each asset must be clearly stated.

7.2 Equipment Disposal:

7.2.1 When permanently disposing the equipment containing storage media, all confidential and highly confidential data and licensed software must be irretrievably deleted before the equipment is moved off site.

7.2.2 Damaged storage devices containing confidential and highly confidential data must undergo appropriate assessment, to determine if the device should be destroyed, repaired, or discarded. Such devices must remain the property of the University

and may only be removed from the site with the permission of the information asset owner.

- 7.2.3 Any third party used for external disposal of the University's obsolete information bearing equipment or hardcopy material must be able to demonstrate compliance with the University's policies related to information security and also, where appropriate, provide a service level agreement which documents the performance expected and the remedies available in case of non-compliance.

7.3 Data Integrity:

- 7.3.1 The University advocates a clear desk and screen policy particularly when employees are absent from their normal desk and outside normal working hours. In addition, screens on which confidential and highly confidential information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorized persons.
- 7.3.2 Removal of the organization's confidential and highly confidential information assets, either printed or held on computer storage media, should be properly authorized by management. Prior to authorization, a risk assessment based on the criticality of the information asset should be conducted.
- 7.3.3 Service owners must ensure that appropriate backup and system recovery procedures are in place.
- 7.3.4 All users of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the confidentiality, integrity, and availability of such files. The degree to which software techniques and disciplined user procedures are necessary should be determined by management regarding the classification of the information in question.
- 7.3.5 Hard copies of Confidential and/or Highly Confidential material must be protected and handled appropriately.
- 7.3.6 All users should be made aware of the risk of breaching confidentiality associated with the photocopying, scanning or other duplication of Confidential and/or Highly Confidential documents. Authorization for copying should be obtained from the document owner where documents are classified as confidential or above.
- 7.3.7 All information used by the University must be stored appropriately.
- 7.3.8 All hard copies of Confidential and/or Highly Confidential documents are to be shredded or similarly destroyed when no longer required. The document owner must authorize or initiate this destruction.
- 7.3.9 Prior to sending Confidential and/or Highly Confidential information or documents to third parties, not only must the intended recipient be authorized to receive such information, but the procedures and information security measures adopted by the third party must also continue to assure the confidentiality and integrity of the information.
- 7.3.10 Confidential and/or Highly Confidential information may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be assured throughout the transfer.
- 7.3.11 Communication by Telephone, Fax, and Email.

- 7.3.12 Staff participating in telephone or video conferencing must be aware of the information security issues involved.
- 7.3.13 All parties are to be notified in advance whenever telephone conversations, meetings or events are to be recorded.
- 7.3.14 Email addresses and fax numbers should be checked carefully prior to sending, and a risk assessment conducted, especially where the information content is Confidential and/or Highly Confidential or where the disclosure of email addresses or other contact information to recipients is a possibility.
- 7.3.15 The identity of recipients or requesters of Confidential and/or Highly Confidential information over the telephone must be verified and they must be authorized to receive it.
- 7.3.16 Electronic commerce systems, whether to buy or to sell goods or services, may only be used in accordance with appropriate technical and procedural measures. Staff authorized to make payment by credit card for goods ordered over the telephone or internet are responsible for safe and appropriate use.
- 7.3.17 Information received via email must be treated with care due to its inherent information security risks. File attachments must be scanned for possible viruses or other malicious code.

7.4 Data Transmission:

- 7.4.1 Highly Confidential, Confidential, and Internal information must not be distributed or made available to users who are not authorized to access the information. This applies to originals, copies, and new materials that contain all or part of the information, and to oral communication of information. When such information is distributed, it must be distributed in such a manner that the restrictions on its future distribution are clear.
- 7.4.2 When distributing documents in electronic form, precautions should be taken against distributing files and disks with viruses and other forms of malicious code. Users should not forward e-mail messages with attachments without some level of confidence that the attachments do not carry malicious code.
- 7.4.3 Confidential and/or Highly Confidential information should not be transmitted across public networks (i.e., the Internet) in clear text.
- 7.4.4 Confidential and/or Highly Confidential information sent via e-mail or as e-mail attachments must be encrypted.
- 7.4.5 Confidential and/or Highly Confidential information should only be shared on local file servers if access is appropriately limited.
- 7.4.6 All file transfers to third party organizations containing Confidential and/or Highly Confidential information should be encrypted. Mail should be appropriately sealed and marked.

7.5 Encryption:

- 7.5.1 Users are required to follow the University's policy on encryption to provide appropriate levels of protection to Confidential and/or Highly Confidential information whilst ensuring compliance with statutory, regulatory, and contractual requirements.
- 7.5.2 Users will ensure that confidential and highly confidential data on their PCs (laptops and desktops) are encrypted. User will generate a ticket at ICT Service Desk for encryption of hard drives if it contains confidential and highly confidential data.
- 7.5.3 Confidential and/or Highly Confidential data should only be taken for use away from the University in an encrypted form unless their confidentiality and security can otherwise be assured.
- 7.5.4 Procedures should be established to ensure that authorized staff may gain access, when needed, to any important business information being held in encrypted form.
- 7.5.5 The confidentiality and security of information being transferred on portable media must be protected using appropriate encryption techniques.
- 7.5.6 Encryption should be used whenever appropriate on all remote access connections to the University's network and resources.
- 7.5.7 A procedure for the management of electronic keys, to control both the encryption and decryption of Confidential and/or Highly Confidential documents or digital signatures, must be established to ensure the adoption of best practice guidelines.

7.6 Electronic Information Backup, Recovery and Disposal:

- 7.6.1 Backup, recovery, and disposal procedures are required for business-critical systems at AKU and recommended for any system.
- 7.6.2 Backup of the University's information assets and the ability to recover them is an important priority.
- 7.6.3 Management is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the business needs of the University.
- 7.6.4 System administrators and managers of business-critical systems or those related to Confidential and/or Highly Confidential information must have documented procedures to create a retrievable, exact copy of critical information and must evaluate data and systems recovery regularly.
- 7.6.5 Backup media must be removable and stored in a fireproof safe that is remote from the physical system that has been backed up.
- 7.6.6 In the case of critical information systems where 24/7 service is required, consideration must be given to deploying equipment such as redundant power supplies for recovery from any disaster.

- 7.6.7 Management must ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of data files; especially where such files may replace files that are more recent.
- 7.6.8 Confidential and/or Highly Confidential information must be disposed of in such a manner as to ensure it cannot be retrieved or recovered.
- 7.6.9 When donating, selling, transferring, or disposing of computers or removable media, care must be taken to ensure that Confidential and/or Highly Confidential data is rendered unreadable by, for example, defacement or other standard techniques.
- 7.6.10 It is insufficient to simply “delete” information (or reformat) from most storage media as that information is often easily recovered.

8.0 Disciplinary Actions: Failure to comply with this policy may result in loss of access to some or all of ICT resources and/or loss of access privileges to ICT resources. In addition, violators of this policy may be subject to disciplinary action, up to and including termination as well as to civil and/ or criminal penalties.

9.0 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.

10.0 Compliance Reference:

10.1 ISO/IEC 27001:2013 standard, Clause A.7.2 - Information Security Policy.

10.2 ISO/IEC 27001:2013 standard, Clause A.8 - Asset Management

11.0 Measure of Compliance: Compliance with this policy will be verified through internal and external audits.

12.0 Reference: This policy satisfies the following requirement of the standard:

Clause Reference	Name of the Clause	Control reference	Name of control	Name of the Standard
-	-	A.7.2	Information Security Policy	ISO/IEC 27001:2013
-	-	A.8	Asset Management	ISO/IEC 27001:2013

13.0 Related Institutional Documents: [Information Security Policy Manual \(ADM-P-024\).](#)

14.0 Annexure: None

15.0 Author(s):

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

16.0 Key Searchable Terms: Assets, Information handling, classification, data, internal use.

17.0 Documents Change Record

Review #	Review Date (dd-mm-yyyy)	Description Of Change	Identification of Change
2.0	25-05-2024	Reviewed and updated the document in accordance with the latest policy document template.	-