Aga Khan University Hospital

Document Title:	Access Control Policy		
Department / Division:	Information Communications Technology (ICT)		
Approved By:		**Document Reference / Policy No.:**	ADM-P-002
Chief Information Officer		**Issuance Date:**	14 July 2015
		Revision Date:	25 May 2024
		Revision No.:	4.0
		Number of Pages:	5

1.0 **Policy Statement:** This policy states the AKU's Access Control Policy, ensuring secure and controlled access to its information resources in support of teaching, research, and administrative functions. Users must accept ICT policies and requirements as a condition of use.

2.0 **Terms and Definitions:** No specific terms or definitions required for this document.

3.0 **Purpose:** This document outlines the Aga Khan University's (AKU or University) policy on Access Control. AKU is committed to the appropriate use of Information and Communication Technology (ICT) Resources and Services in support of its teaching, research, administrative and service functions. The purpose of this policy is to establish security requirements to have controlled access to the information resources of AKU. The users are required to accept the ICT policies and applicable requirements for the use of ICT facilities as a condition of use.

4.0 **Scope:** This policy is applicable to all users of AKU's ICT facilities. This includes all students, faculty members, employees, and other staff (the users). They need to be aware of this policy, their responsibility, and legal obligations. All users are required to comply with this policy to protect themselves and AKU from any legal actions.

5.0 **Responsibility:** All students, faculty, staff, authorized vendors and trainees.

6.0 **Process / Procedure / Policy Content and Guidelines:**

6.1. Authorization: Need to know:

6.1.1.Only authorized users should have physical, electronic, or other access to ICT Resources.

6.1.2. It is the shared responsibility of administrators and users to prevent unauthorized access to systems at AKU.

6.1.3. Administrators and managers are primarily responsible for establishing, documenting, and managing access control policies and processes for their ICT Resources.

6.1.4. Authorization of access to ICT Resources must be based on appropriate business uses.

6.1.5. Access privileges must be reviewed and revised as appropriate to asset or system risk.

6.1.6. If there are changes in job function, student status, transfers, referral privileges, etc., user authorization should be reviewed and revised.

6.1.7. Access to Confidential and/or Highly Confidential information should be provided only when the user requires the information to perform his or her job functions.

6.1.8. Access must be based on a "need to know" analysis conducted by appropriate systems management and must be reviewed regularly.

6.1.9. Access should not be provided automatically or as an adjunct to another process; for example, if a person needs access to an information system screen which contains Confidential and/or Highly Confidential data but does not need access to all or some of the Confidential and/or Highly Confidential data elements, only those data elements which are specifically needed should be visible.

6.1.10. As part of a system risk plan, there must be procedures for granting, logging, and monitoring emergency temporary user access to Confidential and/or Highly Confidential information.

6.1.11. User accounts are created, updated, and deactivated through an automated process. Scripts download data from PeopleSoft systems. This data is then synchronized with active directory through an automated process to create, deactivate or update the needed attributes.

6.1.12. Role based access control is used as a method to secure access to systems and applications.

6.2. Individual Accountability:

6.2.1. Access would be granted to users in such a manner as to provide individual accountability.

6.2.2. Generic or otherwise shared accounts should not be permitted for access to Confidential and/or Highly Confidential information.

6.3. Logging out

6.3.1. Users must log off from applications, computers, and networks when finished.

6.3.2. Users must not leave unattended personal computers with open sessions without locking office doors or locking the computer.

6.4. Prevention and detection of Unauthorized Access:

6.4.1. Users are to use only their own individual access authorization and not access ICT Resources through another user's account.

6.4.2. ICT Resources that handle Confidential and/or Highly Confidential information must maintain and review access logs. Such access logs should be used to

(i) Identify questionable data access.

(ii) Investigate possible breaches.

(iii) Respond to potential weaknesses (e.g., in coding and systems architecture); and

(iv) Access effectiveness of implemented security controls.

6.4.3. Audit logging should be deployed in layers: at the network, application and back-end database level and incorporate the following:

(i) Access logs – host and applications administrators must have a procedure in place to log and review administrative and user access to Confidential and/or Highly Confidential Information.

(ii) Activity logs – it is recommended that user activity (e.g., data insertions, revisions, or deletions) be logged and reviewed for high-risk data elements or systems.

(iii) System monitoring – the frequency and scope of access monitoring should be appropriate to the system's level of risk. It should be coordinated with other monitoring tools and practices including, for example, monitoring of systems performance, network traffic, and intrusion detection.

(iv) All Audit logs must be reviewed monthly.

6.5. Vendor and third-party access:

6.5.1. Vendor access can only be provided after signing a non-disclosure agreement.

6.5.2. Vendor access to ICT Resources is conferred to specific identifiable persons. Access must be limited to specific resources, tasks, and functions only for the period required to accomplish approved tasks. There must be procedures for terminating individual access upon completion of or removal from approved tasks.

6.5.3. Vendors are required to comply with AKU policies regarding the confidentiality of Confidential and Highly Confidential information to which they have access. They must take all reasonable steps to protect AKU ICT Resources from corruption, tampering, or other damage.

6.5.4. It is prohibited to share accounts even if individuals share certain administrative or support responsibilities.

6.5.5. Upon request the vendor must be prepared to do the following:

(i) Identify ICT Resource(s) and information to which the vendor will be granted access.

(ii) Identify the business purpose for which access is to be granted and limitation of access to that purpose.

(iii) Provide access logs that capture individual identity and timing and duration of access and be maintained for no less than 90 days.

(iv) Provide descriptions of security policies and practices.

6.5.6. Violations of this policy may result in the loss of vendor access to AKU ICT Resources and/or other legal or contractual recourse.

6.6. Remote Access:

6.6.1. It is the responsibility of users with remote access privileges to AKU's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to AKU.

6.6.2. To access University information remotely with personal equipment, users must understand that their machines are a de facto extension of the AKU network, and as such are subject to the same rules and regulations that apply to AKU owned equipment, i.e., their machines must be configured to comply with the University Information Security Policies.

6.6.3. Secure remote access must be strictly controlled. Control must be enforced via password authentication or public/private keys with strong passphrases.

6.6.4. At no time should any user provide their login or email password to anyone, not even family members.

6.6.5. Devices configured for access to the University network must have strong authentication.

6.6.6. All hosts that are connected to the University network(s) via remote access technologies must use the most up-to-date antivirus software, this includes personal computers. Personal equipment that is used to connect to the University's networks must meet the requirements of the University-owned equipment when used for remote access.

6.6.7. Organizations or individuals who wish to implement non-standard Remote Access solutions to the University production network must obtain prior approval from Information Services.

6.7. Software Application:

6.7.1. Application support personnel will have view only access to systems/ modules supported, together with access to system monitoring pages, application configurations and interfacing parameters on the live instances. To resolve system issues, relevant access may be granted on a temporary basis.

6.7.2. Developers will not have access to deploy changes or make changes to access security in live environment. These deployment and application security privileges will remain with designated team members in the software team.

6.7.3. Access to program source code is given to authorized personnel as per the sheet maintained by the department after the approval of department lead and ICT security.

6.7.4. Regularly maintain version control over source code to support recovery from prior versions. It is the responsibility to regularly perform file check in and check out.

6.7.5. Access to the production database is provided to the application developer only when the database team receives an approved DB-SRF (special request form) by the application owner or the department head. The access is given for the decided date and time after which the rights are revoked.

6.7.6. Formal periodic review of user access rights should be carried out by User coordinators/ functional leads, to ensure that system privileges are maintained in line with current job responsibilities of the end user.

6.8. All exceptions must be approved by the management and recorded.

7.0 **Disciplinary Actions:** The failure by the users to comply with these Policies 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 these Policies may be subject to criminal and/or civil penalties and to disciplinary action, up to and including termination.

8.0 **Compliance Reference:** No specific regulatory reference is provided for this policy.

9.0 **Measures of Compliance:** No specific measures of compliance.

10.0 **Reference:** No specific references provided.

11.0 **Related Institutional Documents:** No related documents applicable.

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

13.0 Author: Shumail Khalid, Senior Manager Service Delivery

14.0 Key Searchable Terms: Access control

15.0 Documents Change Record:

Review #	**Review Date** (dd-mm-yyyy)	**Description Of Change**	**Identification of Change**
4.0	25-05-2024	Reviewed and updated the document in accordance with the latest policy document template.	-