Aga Khan University Hospital

Document Title:	ICT Firewall Policy		
Department / Division:	Information Communications Technology (ICT)		
Approved By:		Document Reference/Policy No.:	ADM-P-019
Chief Information Officer		Issuance Date:	20 November 2016
		Revision Date:	24 May 2024
		Revision No.:	3.0
		Number of Pages:	4

1.0 **Policy Statement:** ICT firewall policy aims to secure AKUH (Aga Khan University Hospital) network by regulating firewall configurations to prevent unauthorized access and protect sensitive data. Regular updates will be conducted to adapt to evolving threats and maintain network security.

2.0 **Terms and Definitions:**

2.1. Firewall: Any hardware and/or software designed to examine network traffic using policy statements (ruleset) to block unauthorized access while permitting authorized communications to or from a network.

2.2. Firewall Configuration: The system settings that affect the operation of a firewall appliance.

2.3. Firewall Rule Base: A set of policy statements or instructions used by a firewall to filter network traffic.

2.4. NAT: When a packet traverses outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address.

2.5. Objects A firewall object refers to a specific entity configured within a firewall system, typically representing a network device, host, service, or user, and defining rules and settings to control traffic flow and access permissions for enhanced network security.

3.0 **Purpose:** Firewalls are defined as security systems that control and restrict both network traffic and services. Firewalls establish a perimeter where access controls are enforced and subsequently define how a network service is utilized. Typically, an organization may need to make firewall changes several times in a month, with each change requiring hours of evaluation time to assess potential impact to business continuity and security. This policy defines the essential rules regarding the management and maintenance of firewalls and establishes a standard for requests to add, modify and remove firewall policies. The document is applicable on all firewalls deployed at Aga Khan University Hospital, Pakistan (AKUH).

4.0 **Scope:** This policy is applicable to all users of AKUH including all faculty, students, staff, trainees, systems & applications.

5.0 **Responsibility:** AKUH ICT is responsible for maintaining, managing, and implementing firewalls into the network. All students, faculty members, staff and trainees need to be aware of this policy, their responsibility, and legal obligations.

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

6.1. Firewall Rules & Change Management

6.1.1. When modifying a firewall configuration, it is important to consider potential security risks to avoid future issues. The baseline of the firewall security is that the rules that you use to define network access should be as specific as possible and only those ports will be permitted which are necessary to run the services behind the firewall. By default, all the traffic is blocked, and only specific traffic is allowed to known services explicitly.

6.1.2. The table below shows how a recommended change management lifecycle applies specifically to firewall changes.

Phase	Behavior
Change request is issued	• Typically, by ICT or application owner. • The request is usually specified in network terms (example: access is needed from source A to destination B using port X) and may or may not relate to a specific firewall.
Plan the details of the change	• A network or firewall expert identifies the firewalls which should support the requested connectivity and addresses the change request. • Implementation details might be added to the request at this phase or later (e.g. rules or objects to be added or changed).
Assess the potential risk exposure	• Each planned change request is evaluated to assess its risk, compliance, and business justification. People from different disciplines might be involved in the process (dependent on risk). • The depth and formality of the process differs from requirement to requirement. Note: An initial assessment may be held even before planning, based on the end-to-end access requests.
Approval	• The request may be approved, rejected, or approved with modifications based on the assessment results. Manager Operations in consultation with Information Security Team (if required) may approve/modify/reject a change request.
Deploy the change	• Changes to the firewall rule base are implemented (Access rules, NAT rules and objects etc.)
Reconcile and verify	• Changes to firewall configuration are identified (change tracking). • Identified changes and approved change requests are compared. • It is verified that the identified changes correspond directly with approved requests and requests are implemented as specified. Deviations are highlighted. • The verified change requests are closed.

Inform ICT Service Desk / Application Owner / End User	• ICT Service Desk / Application Owner / End User will be informed about the changes which can have a potential impact, so that they are notified in case any related incident is raised over a period of weeks' time.

6.2. Firewall Physical Security:

   6.2.1. All firewalls must be in locked rooms accessible only to those who must have physical access to them to perform the tasks assigned by management. These rooms must maintain the log of all who gain entry to the room.

6.3. Regular Auditing:

   6.3.1. Because firewalls provide such an important barrier to unauthorized access to AKU networks, they must be audited on a regular basis. At a minimum, this audit process must include consideration of defined configuration parameters, enabled services, permitted connectivity, current administrative practices, and adequacy of the deployed security measures.

6.4. Logs:

   6.4.1. All changes to firewall configuration parameters, enabled services, and permitted connectivity must be logged. In addition, all suspicious activity which might be an indication of unauthorized usage or an attempt to compromise security measures must also be logged. These logs must be reviewed periodically to ensure the firewalls operate securely.

6.5. Disciplinary Actions:

   6.5.1. The failure by the users 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 criminal and/or civil penalties and to HR disciplinary action, up to and including termination.

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

8.0   Measures of Compliance: No specific measure of compliance for this policy.

9.0   Reference: No specific references provided.

10.0   Related Institutional Documents: Information Security Policy Manual.

11.0   Annexures: No additional documents provided.

12.0   Author: Kamran Mushtaq, Senior Manager Service Delivery.

13.0   Key Searchable Terms: Firewall, Network Security, Network Protection, Security Best Practices, Threat Detection.

14.0   Documents Change Record:

Review #	Review Date (dd-mm-yyyy)	Description Of Change	Identification of Change
3.0	24-05-2024	Reviewed and updated the document in accordance with the latest policy document template.	-