Annexure 1: Policy Template

Aga Khan University Hospital

Document Title:	Patch Management Policy		
Department / Division:	Information and Communications Technology (ICT)		
Approved By: Chief Information Officer		**Document Reference/Policy No.:**	ADM-P-021
		Issuance Date:	August 1, 2016
		Revision Date:	May 14, 2024
		Revision No.:	3
		Number of Pages:	

1.0 Policy Statement:

At AKUH this policy outlines the standard procedure for patching AKU servers, workstations, and databases to ensure security and facilitate functionality enhancements when needed.

2.0 Terms and Definitions:

No specific terms or definitions required for this document.

3.0 Purpose:

The purpose of this policy is to establish standard procedures for the identification of vulnerabilities, potential areas of functionality enhancements, as well as timely installation of patches and updates on university owned servers, computers and databases.

4.0 Scope:

The processes addressed in this document affect all servers, databases and desktops computer on campus connected to the AKU Pakistan network/ Domain.

5.0 Responsibility:

All students, faculty, staff, and trainees.

6.0 Process / Procedure / Policy Content:

6.1 **Patch Management Process**

6.2 **Server Patch Management Process**

6.2.1 Download patches from a trusted source before scheduled quarterly downtime.

6.2.2 Windows Servers patches test/validation is done by applying the patches initially to test systems. An email will be sent to relevant teams to check their testing servers and confirm proper functionality and post update status.

6.2.3 The application owner is responsible to approve the test patches.

6.2.4 Deploy patches on production servers during communicated downtime.

6.2.5 In case of a patch required urgently, the matter is to be discussed in the change control board along with its implications and upon required approvals, and after following all the test procedures, the security updates are rolled out to production without any further delay.

6.3 Desktop Patch Management Process

6.3.1 Download patches from a trusted source monthly.

6.3.2 Windows desktop patch is validated by applying the patches initially to test Desktop systems. Test desktop systems comprise of one to two systems from a critical area.

6.3.3 The owner who has been issued the desktop is responsible to approve the test patches.

6.3.4 In case of a patch required urgently, the matter is to be discussed in the change control board along with its implications and upon required approvals, and after following all the test procedures, the security updates are rolled out to production without any further delay.

6.4 Database Patch Management Process

6.4.1 The patch updates are applied on the databases after the recommendation from the vendors. These patches should fix the known and reported bugs of the current setup.

6.4.2 The recommended patches are to be first applied on test environment.

6.4.3 On successfully passing the tests, DB team is responsible to raise the request for downtime in the form of a change request (CR). If CR is approved, the tested patch is applied on the production environment.

6.5 Disciplinary Actions

6.5.1 The failure by the users to comply with these Policies may result in loss of access to some or all of IT Resources and/or loss of access privileges to IT Resources. In addition, violators of these Policies may be subject to 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 measures of compliance.

9.0 Reference:

No specific references provided.

10.0 Related Institutional Documents:

No related documents applicable.

11.0 Annexures:

No additional documents provided.

12.0 Author:

Shumail Khalid, Senior Manager Service Delivery.

13.0 Key Searchable Terms:

Patch Management

14.0 Documents Change Record:

Review #	**Review Date** (dd-mm-yyyy)	**Description Of Change**	**Identification of Change**	**Approved By**