Annexure 1: Policy Template

Aga Khan University Hospital

Document Title:	Server Backup Policy		
Department / Division:	Information and Communications Technology		
Approved By: Chief Information Officer		**Document Reference/Policy No.:**	ADM-P-008
		Issuance Date:	15th July, 2015
		Revision Date:	May 14, 2024
		Revision No.:	4.0
		Number of Pages:	3

1.0 Policy Statement:

This policy outlines AKU's backup and recovery process to protect critical data stored in AKU-managed data centers.

2.0 Terms and Definitions:

None

3.0 Purpose: The exceptional growth in data volumes has compelled an efficient approach to data backup and recovery. This document is intended to provide details on the stipulations of data backup and retrieval operations to the client.

4.0 Scope: The intended recipients of this policy are the business units and the application owners for which the servers are housed in the AKU data center.

5.0 Responsibility:

All business units and application owners are expected to adhere to this policy.

6.0 Process / Procedure:

Information Technology recognizes that the backup and maintenance of data for servers are critical to the viability and operations of the Hospital and University. It is essential that standard practices be followed to ensure that data files are backed up on a regular basis.

The University's data center is equipped with an enterprise backup solution which is comprised of backup software, tape library and disk-based backup appliance attached to it. The backup software used for the management of the backup process is EMC's Networker. The disk-based appliance provides a fast method to perform disk-based backups which are quick to restore. While encrypted

tape backups are used for disk-to-tape backups for off-site storage. The backup solution is compatible for both fiber channel and LAN based backups.

The Data Center team ensures that all backups are completed successfully and reviews the backup process for all servers daily. In an event of unsuccessful/failed scheduled backup the data center team informs the application owners and takes appropriate measures to initiate a manual backup immediately.

6.1. Backup Content

The content of data backed up varies from server-to-server. The primary data that will be backed up are: Data files designated by the respective owners of the servers and in some instances System Data (Applications files for the server and other selected software installed on the server). Data to be backed up will be listed by location and specified data sources. This will be stipulated in a separate document called "Data Source Manifest". Data Center team is responsible to backup and provide restoration wherever required for the data mentioned in "Data Source Manifest".

6.2. Backup Type

Backup of servers are scheduled to occur every day in off- peak hours.

Daily Full Backup: This is a full backup which takes place daily for all files and folders selected for backup. The retention of this backup is seven (07) days.

Monthly backup: This is a full backup which takes place monthly for all files and folders selected for backup. The retention period for these backups' ranges from quarterly to three years.

6.3. Offsite Storages of Tapes

Daily backups are replicated to disaster recovery sites through disk-based replication.

Monthly tapes are placed in a locked fireproof cabinet at off-site campus (Secondary Hospital) and remain there according to pre-defined retention policy.

Only designated/authorized staff are responsible for the movement of tapes between the data center and off-site locations. Proper logs are maintained for tape rotation.

6.4. Restorations

In case where restoration is required for any data, the application owners request the data center team to initiate restore by mentioning date of backup, source and destination for the backup to be restored. It is further the responsibility of the application owner to bring the system to its normal state using the restored data.

Also, the data center team does random restores every month to ensure the integrity of the backups being taken along with the media it is being taken on.

7.0 Compliance Reference:

None

8.0 Measures of Compliance:

None

9.0 Reference:

None

10.0 Related Institutional Documents:

None

11.0 Annexures:

None

12.0 Author:

Shumail Khalid, Senior Manager Service Delivery

13.0 Key Searchable Terms:

Server Backup

14.0 Documents Change Record:

Review #	Review Date (dd-mm-yyyy)	Description Of Change	Identification of Change	Approved By
4	15-Dec-23	Change the policy format into hospital policies	All Format	Manager