

	POLICY		
	IT- BACK UP POLICY		
Document No. POL/IT/07	Rev:06	Date Of Issue: 16 September 2026	Page 1 of 8

Introduction:

This policy defines the backup policy for computers within the organization which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, the mail server, and the web server.

Purpose

This policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

Scope

This policy applies to all equipment and data owned and operated by the organization.

Definitions

1. Backup - The saving of files onto Data Cartridge or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
2. Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

About Backup System

"Aconis Backup Software" is the software used for automatic back up at the Centre. The software is installed on the Backup Server.

Microsoft One drive is activated for every user for automatic back up of file history in desktop, my documents and pictures folder.

Everyday back up shall be image back up only for servers and full back up shall be carried out on a monthly basis.

Storage Devices

A backup NAS is installed for taking monthly full backup, weekly differential backup and daily incremental backup using Acronis Cyber Protect Cloud.

			
	POLICY		
	IT- BACK UP POLICY		
Document No. POL/IT/07	Rev:06	Date Of Issue: 16 September 2026	Page 2 of 8

Responsibility

The IT executive shall perform regular backups and test restores. A schedule for back up of all servers/systems as outlined in this policy shall be maintained by the IT executive.

Test restore for the e-promis software shall be conducted by the service providers as may be required.

Testing

The ability to restore data from backups shall be tested at least once in 6 months.

Data Backed Up

Data to be backed up include the following information:

1. User data stored on the hard drive – includes E-promis, SCR datatbase, Accounts files, Quality Management System folder on the server, and user data is backing up every day to Microsoft cloud (one drive) decided by the management on the basis of criticality from time to time
2. System state data
3. The registry
4. E-RRRL folders

Systems to be backed up include but are not limited to:

1. File server
2. Database server
3. Domain controllers
4. User systems

				
	POLICY			
	IT- BACK UP POLICY			
Document No. POL/IT/07	Rev:06	Date Of Issue: 16 September 2026	Page 3 of 8	

Server Details at AL NOOR

Si. No	Server Name	IP Address	Details	BACK UP DETAILS
1	Noorportal	10.200.0.12	Antivirus installed on this server	Back up on backup NAS
2	noorprinter	10.200.0.15	Public folder shared from this server	Back up on backup NAS
3	Alnoor Domain	10.200.0.11	Domain controller and DHCP Server	Back up on backup NAS
4	Accounts	10.200.0.13	Sql server for E promis	Back up on backup NAS
5	ALNOOR243D ESK	10.200.0.18	Attendance system server	Back up on backup NAS
6	Apps Server	10.200.0.14	Application server	Back up on backup NAS
7	File server	10.200.0.16	Shared folders	Back up on backup NAS

Restoration

Users that need files restored must submit a request to the IT. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

Back up Storage Locations

Backup NAS used for backup is installed in Server room.

	POLICY		
	IT- BACK UP POLICY		
Document No. POL/IT/07	Rev:06	Date Of Issue: 16 September 2026	Page 4 of 8

PROCEDURE FOR BACKUP OF SERVERS

Monthly Backup of Al Noor Domain (10.200.0.11) is scheduled every last day of the month at 08:00 PM

Backup done using Acronis Cyber Protect agent to Backup NAS (10.200.0.19)

Daily backup of Al Noor Domain (10.200.0.11) is scheduled Monday to Friday at 08:00 PM

Backup done using Acronis Cyber Protect agent to Backup NAS (10.200.0.19)

Monthly Backup of Accounts Server (10.200.0.13) is scheduled every last day of the month at 09:00 PM

Backup done using Acronis Cyber Protect agent to Backup NAS (10.200.0.19)

Daily backup of Accounts Server (10.200.0.11) is scheduled Monday to Friday at 09:00 PM

Backup done using Acronis Cyber Protect agent to Backup NAS (10.200.0.19)

Monthly Backup of APP Server (10.200.0.14) is scheduled every last day of the month at 10:00 PM

Backup done using Acronis Cyber Protect agent to Backup NAS (10.200.0.19)

Daily backup of APP Server (10.200.0.14) is scheduled Monday to Friday at 10:00 PM

Backup done using Acronis Cyber Protect agent to Backup NAS (10.200.0.19)

Monthly Backup of File Server(10.200.0.16) is scheduled every last day of the month at 11:00 PM

Backup done using Acronis Cyber Protect agent to Backup NAS (10.200.0.19)

Daily backup of File Server (10.200.0.16) is scheduled Monday to Friday at 11:00 PM

			
	POLICY		
	IT- BACK UP POLICY		
Document No. POL/IT/07	Rev:06	Date Of Issue: 16 September 2026	Page 5 of 8

Backup done using Acronis Cyber Protect agent to Backup NAS (10.200.0.19)

Monthly Backup of Biometric Server (10.200.0.18) is scheduled every last day of the month at 03:00 PM

Backup done using Acronis Cyber Protect agent to Backup NAS (10.200.0.19)

Daily backup of Al Noor Domain (10.200.0.18) is scheduled Monday to Friday at 03:00 PM

Backup done using Acronis Cyber Protect agent to Backup NAS (10.200.0.19)

Monthly Backup of Server BK (10.200.0.17) is scheduled every last day of the month at 02:30 PM

Backup done using Acronis Cyber Protect agent to Backup NAS (10.200.0.19)

Daily backup of Al Noor Domain (10.200.0.17) is scheduled Monday to Friday at 02:30 PM

Backup done using Acronis Cyber Protect agent to Backup NAS (10.200.0.19)

Monthly Backup of Noorportal (10.200.0.12) is scheduled every last day of the month at 06:00 PM

Backup done using Acronis Cyber Protect agent to Backup NAS (10.200.0.19)

Daily backup of Al Noor Domain (10.200.0.12) is scheduled Monday to Friday at 06:00 PM

Backup done using Acronis Cyber Protect agent to Backup NAS (10.200.0.19)

Monthly Backup of Al Noor Domain (10.200.0.15) is scheduled every last day of the month at 07:00 PM

Backup done using Acronis Cyber Protect agent to Backup NAS (10.200.0.19)

AL NOOR REHABILITATION & WELFARE ASSOCIATION FOR PEOPLE OF DETERMINATION  النور جمعية النور للرعاية وتأهيل أصحاب الهمم			
POLICY			
IT- BACK UP POLICY			
Document No. POL/IT/07	Rev:06	Date Of Issue: 16 September 2026	Page 6 of 8

Daily backup of Al Noor Domain (10.200.0.15) is scheduled Monday to Friday at 07:00 PM

Backup done using Acronis Cyber Protect agent to Backup NAS (10.200.0.19)

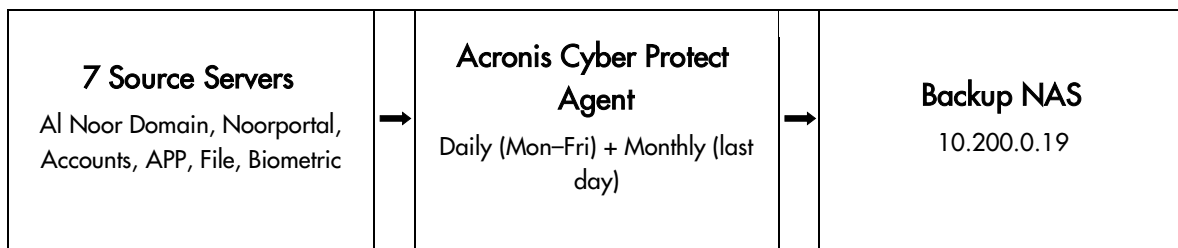
PROCEDURE FOR BACKUP OF USER DATA

All user data is backed up to OneDrive in real-time

Backup Procedures & Schedule

All servers are protected using Acronis Cyber Protect, with Daily and Monthly backup jobs replicated to the central Backup NAS.

Backup Flow Overview



Backup Schedule Summary

#	Server / System	IP Address	Daily Backup (Mon–Fri)	Monthly Backup (Last Day)
1	Al Noor Domain (Primary DC)	10.200.0.11	08:00 PM	08:00 PM
2	Noorportal	10.200.0.12	06:00 PM	06:00 PM

				
	POLICY			
	IT- BACK UP POLICY			
Document No. POL/IT/07		Rev:06	Date Of Issue: 16 September 2026	Page 7 of 8

#	Server / System	IP Address	Daily Backup (Mon–Fri)	Monthly Backup (Last Day)
3	Accounts Server	10.200.0.13	09:00 PM	09:00 PM
4	APP Server	10.200.0.14	10:00 PM	10:00 PM
5	Noorprinter	10.200.0.15	07:00 PM	07:00 PM
6	File Server	10.200.0.16	11:00 PM	11:00 PM
7	Biometric Server	10.200.0.18	03:00 PM	03:00 PM

Key Points

- Backup Agent: Acronis Cyber Protect agent installed on each server.
- Backup Destination: Backup NAS (10.200.0.19) for all servers.
- Daily Backups: Run Monday to Friday for every server, at its designated time.
- Monthly Backups: Run on the last day of every month, at its designated time.
- Time Spacing: Jobs are staggered across the day (03:00 PM – 11:00 PM) to avoid resource contention on the Backup NAS.

			
POLICY			
IT- BACK UP POLICY			
Document No. POL/IT/07	Rev:06	Date Of Issue: 16 September 2026	Page 8 of 8

Appendix – Amendment History & Authorisation

Revision No	Description of Change	Issue Date	Authorised By
00	First Issue	4 Nov 2012	Director
01	Included back up of user data and offsite back up	30 June 2013	Director
02	New Al Noor logo	01 Feb 2016	Director
03	Replace the Centre's logo in all QMS documents and revision of document codes	12 Aug 2020	Director
04	Various Sections of the Policy. Based on audit recommendations	28 December 2023	Director
05	- Changes in department names & designations - Changes in server name - Deleted back up external storage location, monthly back up schedule and offsite storage of back up.	26 November 2024	Director
06	Why this change was made: The Centre upgraded its backup infrastructure from a tape/data-cartridge based system to a centralized, cloud-managed NAS solution (Acronis Cyber Protect) to reduce reliance on manual tape handling, lower the risk of missed/failed backups, simplify the backup schedule, and keep the policy aligned with the current server hardware and network addressing. Removed from the Policy: - Backup Server + Data Cartridges (weekly/monthly tape rotation) as the primary backup device — physical tapes were prone to media degradation/failure and required manual swapping, increasing the risk of missed or failed backups - Old server IP address range 15.100.1.x — the network was re-addressed as part of the server/infrastructure refresh - Mail Server (Alnoorexch) and stand-alone Noorsql server listed as separate backed-up systems — these systems were decommissioned/consolidated and no longer exist as standalone servers	16 September 2026	Director

	 POLICY IT- BACK UP POLICY		
Document No. POL/IT/07	Rev:06	Date Of Issue: 16 September 2026	Page 9 of 8

	• Weekly / duplicate-weekly / monthly (set-I & set-II) backup rotation schedule, and Data Cartridge as a backup device — the multi-step tape rotation was complex to manage and verify, and is unnecessary with automated NAS backups • Weekly Back Up Plan and Monthly Back Up Schedule figures illustrate the tape-based rotation, which no longer applies • Detailed per-department OneDrive backup-time table (Admin, SCR, Special Educators, Program Leaders/HODs/Accounts & Director) and duplicate weekly/monthly backup of Data Backup server to hard disk — replaced by continuous, real-time OneDrive sync, removing the need for scheduled department-specific backup times Added to the Policy: • Backup NAS (10.200.0.19) using Acronis Cyber Protect Cloud, with an Acronis Cyber Protect Agent installed on each server — provides centralized, automated and monitored backups with better reliability and reporting than manual tape backups • New server IP address range 10.200.0.x — reflects the current network addressing after the infrastructure refresh • Biometric Server added as a new backed-up system — a new attendance/biometric system was introduced to the network and needs to be protected by backup • Simplified backup schedule: Daily (Mon–Fri) + Monthly (last day) job per server — reduces complexity and administrative overhead compared to the previous multi-tier tape rotation • New Backup Flow Overview diagram, Backup Schedule Summary table, and Key Points summary section — improves clarity and auditability of the backup process for IT staff and auditors • Statement that all user data is backed up to OneDrive in real time — reduces the data-loss window (recovery point objective) compared to fixed daily backup times		
--	--	--	--