

Polyhose® Providing Flexible Solutions Globally	Data Management Policy	Doc. No.	PH/L3/IT/005		
		Issue No.	01		
		Rev. No.	00	Date	07.04.2022
		Page No.	1 of 6		

Data Management Policy and Procedures

Purpose

The unprecedented growth in data volumes has necessitated 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.

Scope

The intended coverage of this documentation is all critical electronic data stored on network-enabled devices. Any resources saved locally to machine hard drives or not in one drive folder will not be part of the backup process.

Policy

Backup policy provides the last line of defense against data loss and is sometimes the only way to recover from a hardware failure, data corruption, or a security incident. A backup policy is related closely to a disaster recovery policy, but since it protects against events that are relatively likely to occur, in practice it will be used more frequently than a contingency planning document.

The purpose of this policy is to provide a consistent framework to apply to the backup process. The procedure will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed.

This policy applies to all data stored on systems. The procedure covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

Procedure

Identification of Critical Data

Data is most critical in the organization. This is done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data is identified so that it can be given the highest priority during the backup process.

Polyhose® Providing Flexible Solutions Globally	Data Management Policy	Doc. No.	PH/L3/IT/005			
		Issue No.	01			
		Rev. No.	00	Date	07.04.2022	
		Page No.	2 of 6			

Data to be Backed Up

Data to be backed up will include:

- All data determined to be critical to the organization and/or employee job function.
- All information stored on the OneDrive and email server(s) (It is the user's responsibility to ensure any data of importance is moved to the One Drive folder.)
- All information stored on the cloud, which may include web servers, database servers, domain controllers, SDWAN, remote access servers, etc.

Data Not to be Backed Up

Data the IT Department will not be responsible for backing up is as follows:

- Users' personal data.
- Data stored on local hard drives of desktops and laptops (Except One Drive Folder).
- Data on removable media (i.e. DVDs, CDs, and Thumb Drives).
- Data stored on mobile devices.

Microsoft O365 Backup and Synchronization

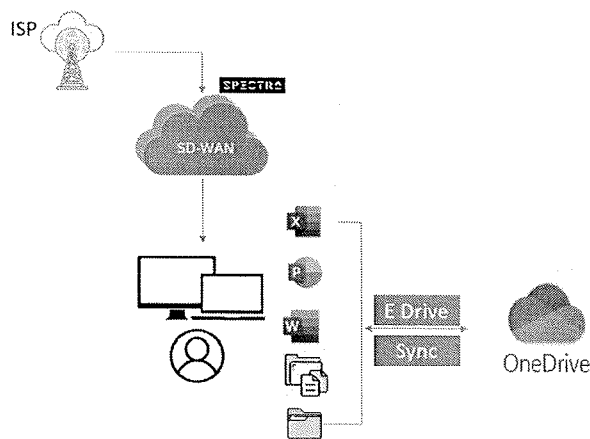
One Drive and Shared folders in cloud storage are provided to all users and polyhose have strict policies regarding the synchronization of one drive folder to the cloud.

Microsoft 365 comes with Microsoft's trusted security measures and data replication and recovery mechanisms. These ensure your data is as safe and available in the cloud as it was on-premises. This powerful system of protection is designed to guard against data loss caused by software malfunctions, hardware failure, power outages, and natural disasters.

	Data Management Policy	Doc. No.	PH/L3/IT/005		
		Issue No.	01		
		Rev. No.	00	Date	07.04.2022
		Page No.	3 of 6		

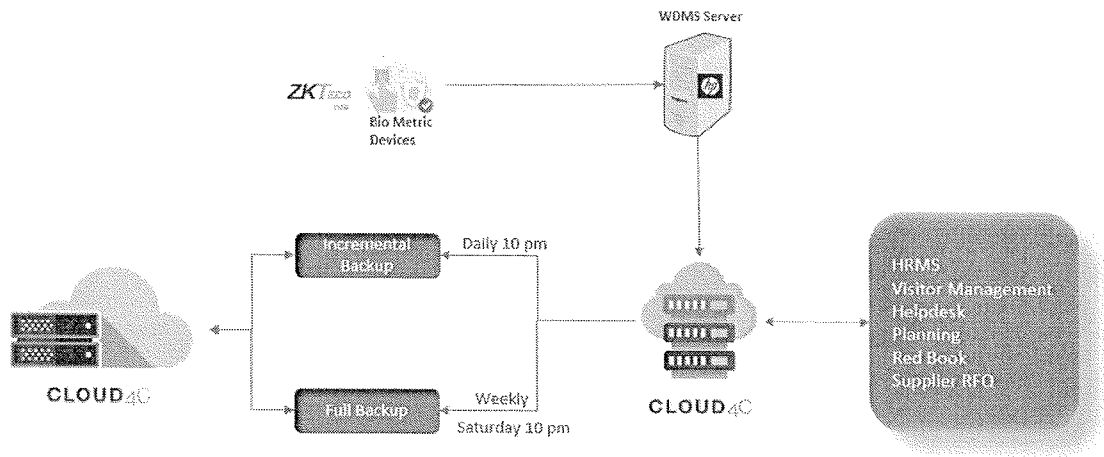
User Data:

Employees are not permitted to store data in C Drive. User Folders such as Documents and Downloads are configured to E Drive, and all Users have access only to E Drive. One drive Folder is configured to store and sync organizational data with the cloud.



Cloud Server Auto Backup (CORE Application):

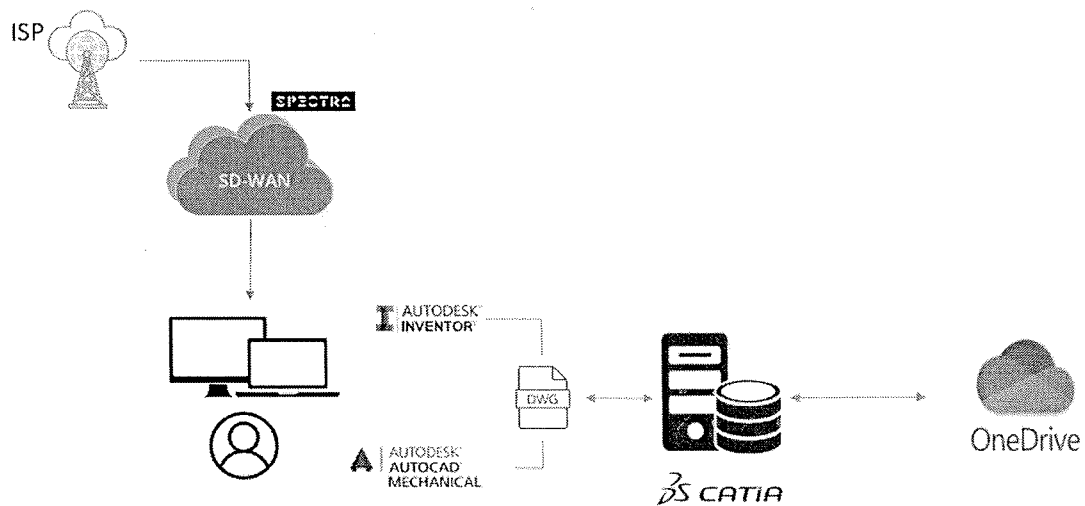
All web servers hosted on the cloud will be automatically backed up regularly. The cloud provider procures, installs, and maintains all hardware, software, backup, and other supporting infrastructure in its data centers.



Polyhose® Providing Flexible Solutions Globally	Data Management Policy	Doc. No.	PH/L3/IT/005		
		Issue No.	01		
		Rev. No.	00	Date	07.04.2022
		Page No.	4 of 6		

Design user Data Backup:

All design documents created by design users are backed up and the server is in sync with Cloud for regular backups. All the latest design documents are stored in One Drive and managed by Design Documents Incharge.



Polyhose® Providing Flexible Solutions Globally	Data Management Policy	Doc. No.	PH/L3/IT/005		
		Issue No.	01		
		Rev. No.	00	Date	07.04.2022
		Page No.	5 of 6		

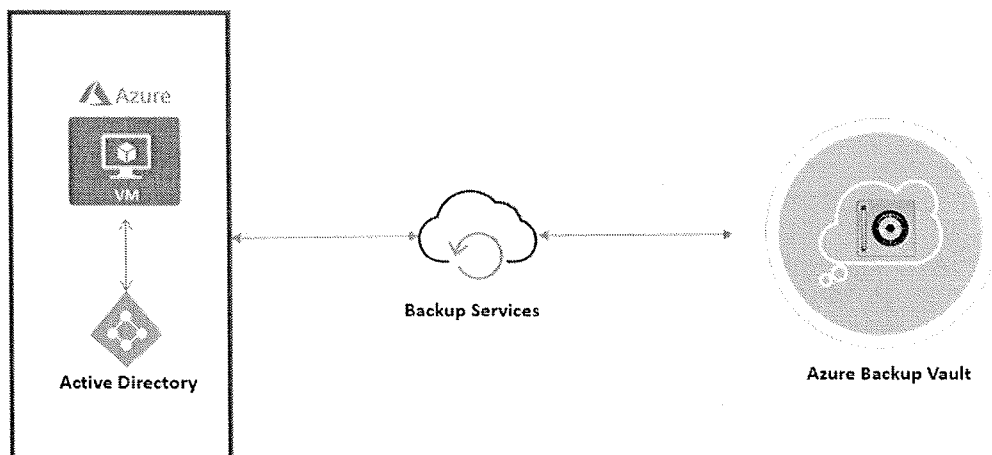
Azure AD Backup

Azure Backup is used for servers in Azure cloud infrastructure. It is a simple backup solution that doesn't require on-premises backup infrastructure and provides secure, long term and short-term storage of the data.

Azure Policy provides built-in policies for Azure Backup. These policies give us control over two main aspects of your backups:

Schedule: AD VM Backup is scheduled every day at 10 am.

Retention: Period during which backups are retained is 7 days.



	Data Management Policy	Doc. No.	PH/L3/IT/005		
		Issue No.	01		
		Rev. No.	00	Date	07.04.2022
		Page No.	6 of 6		

Rev No	Rev Date	Description	Remarks
00	07.04.2022	Initial release	-

Prepared by : Suriya A 	Reviewed By: Satish Babu B 	Approved by : Aliasger SJ 
--	--	---