



WHITEPAPER

Why You Need to Back Up Microsoft 365 and How MSP360 Helps

You may have noticed that Microsoft has shifted to the cloud. Microsoft 365 is undeniably one of the world's most popular and most used business suites. It's so big, in fact, that anyone you know has at least once in their lifetime used some of its products. And the chances are that you are using Microsoft 365 in your company right now.

The fact that emails, calendars, spreadsheets, and presentations are now always in the cloud brings peace and tranquility into the minds of many people, who believe that their data is now always safe. But is it?

While, yes, your data is now managed by Microsoft in their huge and safe data centers, the company does not guarantee you that it will be 100% safe. Many security-related matters still need to be managed by the end users and corporate system administrators.

In this article, we will define the main misbeliefs about Microsoft 365 data protection, name the main reasons to back up Microsoft 365, and discuss other necessary protection methods.

Main Misbelief About Microsoft 365

As we've already mentioned, the main misbelief about Microsoft 365 services is that the company manages both the security of your data and its availability. However, it's not that simple.

As stated in the [official Services Agreement](#), the company ensures the physical security of your data and its automatic replication, provides you with instruments for identity and access management, and ensures service availability (although, according to the terms and conditions, the services might be unavailable "from time to time").

To put it in a nutshell, Microsoft won't help you if your password is too weak and your systems are breached, or if you shared your data to the web by accident. They also don't provide 100% uptime, since nobody can.

Why You Should Back Up Microsoft 365

So, let's get to the main reasons why you should regularly back up Microsoft 365 services:

- ▶ **To prevent data loss.** First of all, data backup will protect you from accidental and malicious data deletion. Your SharePoint or email data can be deleted on purpose by your employees, or malefactors who gain access to your corporate account. Without proper backup in place, such data would be permanently lost. This means lost email chains, spreadsheets, and other essential data that could cost your company tens of thousands of dollars.
- ▶ **Limited native recovery and retention.** A full-on backup suite will allow you to back up and recover your data according to your own schedule. By contrast, Microsoft's own recovery solution won't allow you point-in-time recovery of mailbox items.

- ▶ **Limited regulatory compliance.** A lot of businesses that work with personal data have to meet strict compliances, such as HIPAA or GDPR, to name but a few examples. These regulations force you to manage users' data with extreme care, to archive it for certain periods, and to delete it on request. Microsoft's Litigation Hold feature can be helpful in managing data that should not be deleted until further notice. However, that's still only one issue. The rest needs to be planned and managed by you.
- ▶ **Disable accounts of past employees.** When an employee leaves your company, you will typically have to archive their Microsoft 365 data. There are two ways to achieve this. Either natively archive their data and pay for the unused account, or back up all their data to low-cost storage and delete the account.
- ▶ **Access to data in the event of service outages.** Although they are a rare issue, data outages still happen with Microsoft services. Moreover, [according to Microsoft themselves](#), outages have been happening more often in recent years. A proper backup solution will allow you to at least access the data that you need in the event of an unforeseen issue with the service.

How to Protect Microsoft 365 Data

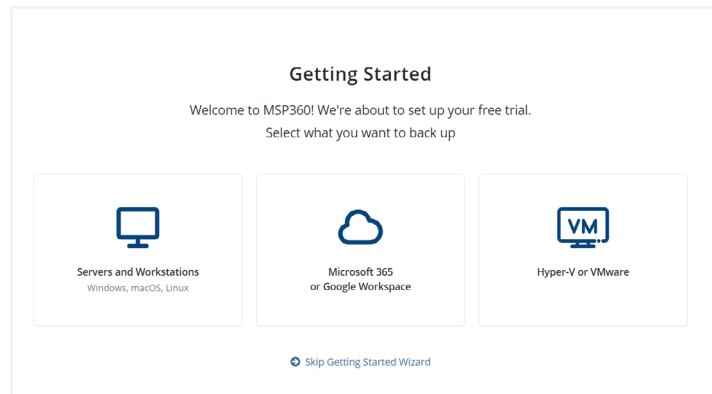
Here's a full list of what and how you should protect your Microsoft 365 account and data:

- ▶ **Review access policies.** First and foremost, to protect your Microsoft 365 data, you should recheck your access and identity policies. In many cases, a data breach starts with either a compromised administrator account or a weak password. Thus, you should employ a rule of least privilege, granting access to the needed resources only to the appropriate employees.
- ▶ **Create a backup schedule.** As we've already mentioned, Microsoft 365 won't fully protect your data. So you need to plan and schedule backups of your most valuable assets, such as emails, calendars, documents, SharePoint, and OneDrive data.
- ▶ **Test recovery.** There is a popular saying that a non-tested backup is as good as no backup at all. Hence, it is generally advisable to schedule all kinds of recovery tests to ensure that your data is recoverable and can be restored within a period of time defined by your corporate policies.
- ▶ **Plan your retention according to compliance.** Since compliance in many cases means that you need to store your data for long periods of time, you should think about creating a good retention policy. And while Microsoft doesn't have such a feature in place, there are advanced backup solutions that have.

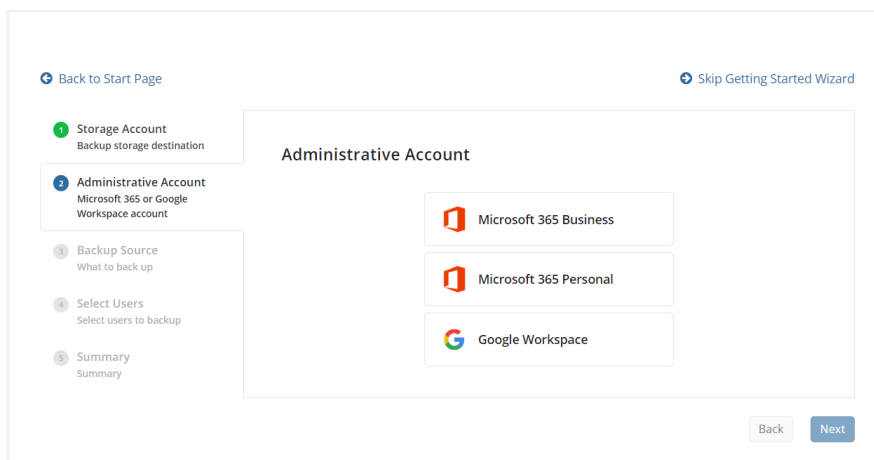
How to Create Microsoft 365 Email Backup with MSP360 Managed Backup

MSP360 Managed Backup for Microsoft 365 is a cloud-based tool, so you only need to connect it with your account and perform a basic configuration.

To start the free trial, go to the [MSP360 Managed Backup](#) product page and click the **Free Trial** button. Fill in the form and click the **Free Trial** button. You'll then be redirected to the Getting Started Wizard in the web control panel. Here, you need to select what you need to back up. Click the **Microsoft 365 or Google Workspace** button to start backing up M365 right away.



In the next step, you need to log in to your administrative account. Select the one you need from the list and click **Next**.



By default, you'll be granted 1 TB of MSP360 Storage powered by AWS with a 30-day free trial. However, MSP360 Managed Backup is a flexible and reliable backup solution that is natively integrated with all major storage providers, like AWS, Wasabi, Backblaze B2, Microsoft Azure, and Google Cloud.

MSP360 Managed Backup can protect your users' computers, production servers, and also everything within your Microsoft 365 account, including entire Outlook mailboxes, Calendar, Microsoft Exchange server, OneDrive, SharePoint, and Microsoft Teams data. For Microsoft 365 email backup, MSP360 Managed Backup also supports backup of online archives, shared mailboxes, and public folders.

Services	Users	Last Backup	Total	Items	
Mail	6	Mar 1, 2024, 10:44 AM GMT+1	1.1 GB	164885	On
Drive	6	Mar 1, 2024, 10:12 AM GMT+1	584.63 MB	49	On
Contacts	6	Mar 1, 2024, 9:31 AM GMT+1	5.96 MB	1526	On
Calendar	6	Mar 1, 2024, 10:35 AM GMT+1	2.11 MB	963	On
SharePoint		Mar 1, 2024, 12:06 AM GMT+1	36 MB	23	On
Teams		Mar 1, 2024, 8:11 AM GMT+1	2.81 MB	508	On

ⓘ The backup is scheduled to run at least twice a day automatically
Configure Backup

With MSP360 Managed Backup, you can also easily export user accounts to PST file format and ensure access to data in the event of future issues.

MSP360 Managed Backup for Microsoft 365 and Google Workspace 2.0 with Export to PST

While backing up your data, it's extremely important to meet regulatory compliance, and MSP360 Managed Backup can help you with custom retention policies available for Microsoft 365. You can create retention policies for Mail, Drive, Contacts, Calendar, and SharePoint. You can either delete all objects that were modified or created before a specified date, or specify a number of versions for objects you want to keep in backup storage.

Create Retention Policy

Name *
Mail

For Service *
Mail

Delete Older Than
30 Days From: Date Modified Date of Backup

Purge Delay
1 Days

Disable

Create Cancel

Create Retention Policy

Name *
Drive

For Service *
Drive

Delete Older Than
30 Days From: Date Modified Date of Backup

Always Keep the Latest Revision

Revisions to Keep
1

Purge Delay
1 Days

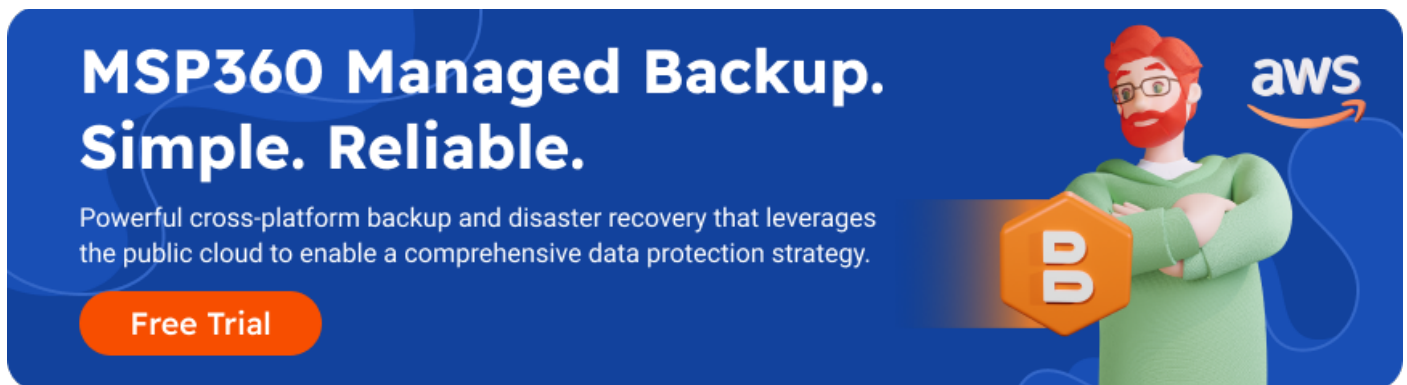
Disable

Create Cancel

MSP360 Managed Backup offers advanced security features to help users fully protect their data. For instance, you can grant users limited permissions or remove them completely. Also, MSP360 Managed Backup offers the highest-possible level of backup protection with [Object Lock \(immutability\)](#).

Immutable backups are not vulnerable to ransomware, unattended access, or human factors. Even if you lose all your data, an immutable backup will help you to rebuild everything from scratch, using clean, uncorrupted data.

The other great feature is granular recovery; you can recover single emails, individual files, and folders. This makes data recovery after an accidental data deletion easier.



MSP360 Managed Backup.
Simple. Reliable.

Powerful cross-platform backup and disaster recovery that leverages the public cloud to enable a comprehensive data protection strategy.

[Free Trial](#)

aws

Conclusion

When it comes to Microsoft 365 backup, you don't need to compromise on efficiency or speed in order to gain peace of mind and flexibility. MSP360 Managed Backup is as flexible as you or your customer need and will provide you with robust Microsoft 365 data protection.

About MSP360

Established in 2011 by a group of IT professionals, MSP360™ (formerly CloudBerry Lab) provides cutting-edge SaaS solutions that are simple, cloud-based, and profitable for Managed Service Providers.