



# Top 5 Reasons to Backup Office 365

The adoption of Microsoft 365, formerly known as Office 365, has grown exponentially in recent years. In 2022, it is one of the leading cloud-based business platforms worldwide, garnering [nearly 345 million paid seats](#) globally, a 17% year-over-year increase in commercial revenue.

Despite this progress, many businesses fail to realize that Microsoft 365 still has its limitations. In particular, the fact that Microsoft 365 does not come with a backup or archiving option leaves a gap that businesses need to fill.

You may be asking: “Do I really need to backup Microsoft 365? Surely Microsoft takes care of that themselves?” The answer is: yes, you do need to back it up. Read on for the five key reasons why.

## The Truth About Microsoft 365

Microsoft (the company) may host the infrastructure of their M365 solution, but this doesn't supersede the user's responsibility to maintain an active backup for Microsoft 365 data. In fact, ownership of your data in the cloud — being able to set up, access, recover or move it — is your obligation, not Microsoft's. According to Microsoft Services Agreement (Sec.2):

*“Many of our Services allow you to store or share Your Content or receive material from others. We don't claim ownership of Your Content. Your Content remains Your Content and you are responsible for it.”*

There is a false impression that data created and stored in cloud ecosystems such as Microsoft 365 do not need to be backed up beyond the native offerings.

This isn't true.

The fact is, businesses actually need to establish a Microsoft 365 backup & recovery plan for their data. Here are the top five reasons why businesses should backup Microsoft 365.

### 1. Ensure Business Continuity.

Data backup for Microsoft 365 ensures business continuity. This is the ability of an organization to continuously function during and after adverse events: natural disasters, outbreaks, fires, cyberattacks, and other internal or external threats.

Key to laying out a business continuity plan is establishing the risk management procedures that will assist in preventing the interruptions of critical services. Business continuity plans also consider how to reestablish full function to the department affected, or the entire organization, as smoothly and quickly as possible. A good plan answers the following questions:

- How can you keep your organization's vital functions running when disaster strikes?
- How can you ensure minimal downtime?
- How fast can you recover from the disaster?

Ensuring access to full and accurate records of your data is a vital piece of a complete business continuity policy. In a way, data backup and archiving is good insurance against the risk of data loss. The out-of-the-box tools that come with Microsoft 365 should not be your only tool to ensure your business has full and complete records in the event of data loss.

### 2. Microsoft Doesn't Actually Backup Your Data.

Microsoft is a great provider, but they don't actually have users completely covered. The company guarantees the infrastructure, but not the customer's data. According to Microsoft's Service Agreement (Sec.6b):

*“Microsoft is not liable for any disruption or loss you may*

*suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services."*

Moreover, if you're thinking about using the Recycle Bin as a data repository, think again: Microsoft 365 only keeps deleted documents and emails in the Recycle Bin for up to 90 days. This is extremely risky because the Recycle Bin doesn't have the same security features as a SaaS backup solution, exposing your Microsoft 365 data to ongoing threats.

Moreover, deleting data without backing it up first means potentially destroying records that may be required for legal or regulatory compliance, should your firm ever be audited. A dedicated Microsoft 365 backup and recovery solution is a more appropriate tool.

### 3. Alleviate Data Location Uncertainties.

Microsoft 365's variety of applications and data structures all store your data in the cloud. But where? Where exactly is your data? And if you did have to retrieve it, how would you find it?

According to the Microsoft Trust Center:

*"Customer data may be replicated within a selected geographic area for enhanced data durability in case of a major data center disaster, and in some cases, will not be replicated outside it."*

Many people don't realize that their data (Outlook emails, OneDrive documents, SharePoint files, Teams conversations, etc.) are separate, and sometimes stored separately. So the only way to backup it all up, and restore all of it, is with a system designed to find it all, store it all, and restore it all. This is not an easy task, and sometimes nearly impossible to do with the native Microsoft 365 tools.

### 4. Meet Compliance and Regulatory Requirements.

Regulated industries (like Financial Services, Healthcare, Legal, etc.) have stricter backup regulations. If your firm

is under one of these regulated industries, you may have regulations and requirements to provide access to data that goes well beyond typical backup methods.

[HIPAA](#), [GDPR](#), [Can-Spam](#) and other regulations often require firms to keep complete and accurate records of email, attachments, files and related information for several years. Compliance with these regulations, however, is not guaranteed with the out-of-the-box tools that come with Microsoft 365. The platform does have optional backup / archiving tools available for purchase, but this is additional cost, and likely with a more difficult user experience versus other solutions.

Certain backup solutions provide the ability to set retention rates that are as long as is necessary to legally maintain compliance. This allows your company, no matter which industry, to address lawsuits and discovery processes smoothly. Enabling legal or time-based holds in Microsoft 365 allows quick, safe, and tamper-proof access to pertinent data stored there.

### 5. Protect Your Data from Digital Threats

Data loss is prominent in this new world of hackers and data hostage viruses. It isn't just outsiders that are the issue, either. Employees are prone to accidentally deleting or misplacing files. In addition, disgruntled and rogue employees can intentionally delete or damage business-critical data.

Many firms have faced increasing instances of ransomware attacks in the past two decades. According to [Verizon's annual Data Breach Investigations Report \(DBIR\)](#), ransomware is responsible for 25% of all data breaches across various industries. The average cost of a data breach? [\\$4.24M](#).

The only way to truly protect your business from a ransomware attack is by having a full and complete backup and archive of all your data. Anything less, and your business is in danger of being severely impacted by the loss of data. Microsoft 365 does not keep full and complete backups and archives of all your data that goes back months, even years. Only a backup and archiving solution specifically made for this kind of process can handle that task easily and quickly.



## Backup Microsoft 365 with Dropsuite

These are the top five reasons to backup Microsoft 365, and are proof of how necessary a Microsoft 365 backup and recovery solution is, especially one that goes well beyond what Microsoft offers.

Dropsuite provides an industry-leading [Microsoft 365 Backup and Archiving](#) solution. Our solutions include many features specifically designed to make backup fast, easy and secure.

To find out more, [contact](#) our Dropsuite Microsoft 365 data backup specialists and see a demo of our best-in-class solution.

## CONTACT US

For more information, please contact us:  
[www.dropsuite.com](http://www.dropsuite.com) | [sales@dropsuite.com](mailto:sales@dropsuite.com)