The Office 365 Shared Responsibility Model

Primary Responsibility

Supporting Technology

Security Regulatory

Microsoft's Responsibility

Learn more from the Office 365 Trust Center

MICROSOFT GLOBAL INFRASTRUCTURE

Uptime of the Microsoft Office 365 Cloud Service

Office 365 Data
Replication
DC to DC geo-redundancy

Recycle Bin

Limited, short term data loss recovery (no point-in time recovery)

Infrastructure-Level

Physical Security Logical Security App-level Security User/Admin Controls

Role as data processor

Data Privacy Regulatory Controls Industry certifications HIPPA, Sarbanes-Oxley

YOUR Responsibility

Your office 365 data

Access and control of your data residing in Office 365

Office 365 Backup

Copy of your data stored in a different location

Full Data Retention

ST & LT retention filling any/all policy gaps *granular & point-in time recovery options*

Data-Level

Internal:
Accidental Deletion
Malicious Insiders
Employee Retaliation
Evidence Tampering

External:
Ransomware
Malware
Hackers
Roque Apps

Role as data owner

Answer to corporate and industry regulations

Demands from internal legal and compliance officers



And Microsoft agrees...

Service Availability

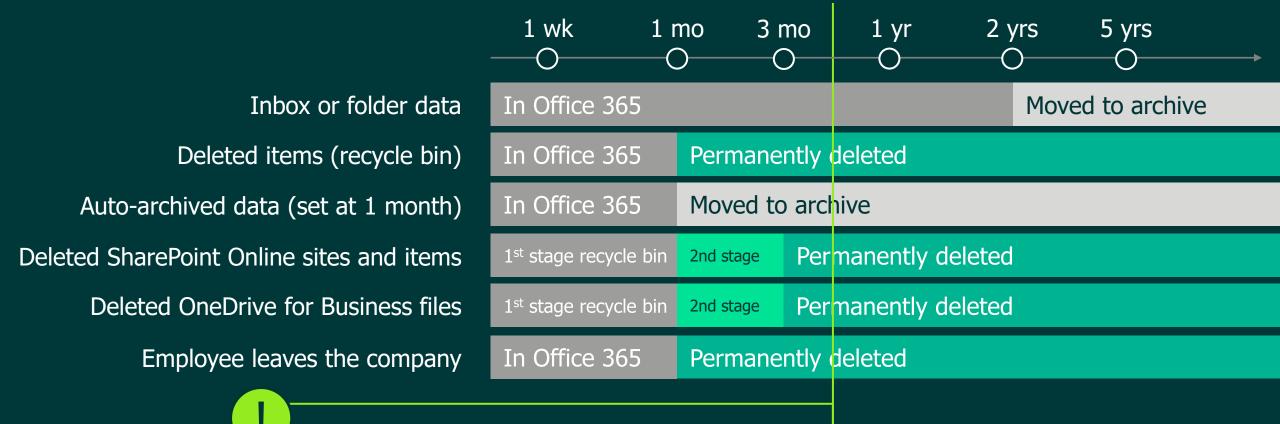
Service Availability.

a. The Services, Third-Party Apps and Services, or material or products offered through the Services may be unavailable from time to time, may be offered for a limited time, or may vary depending on your region or device. If you change the location associated with your Microsoft account, you may need to reacquire the material or applications that were available to you and paid for in your previous region.

b. We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and 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.

Source: https://www.microsoft.com/en-us/servicesagreement, 8/17/2020

Retention policies: What exactly does Microsoft back up?



The average length of time from data compromise to discovery is over 140 days, yet default settings only protect for 30-90 days.

Source: Microsoft Office 365, 6 steps to holistic security, chapter 1



Retention policies: What exactly does Microsoft back up?

	1 wk	1 mo	3 mo	1 yr 	2 yrs ——O—	5 yrs ——O——	
Inbox or folder data	Protected	with Veeam	1				
Deleted items (recycle bin)	Protected	with Veeam	1				
Auto-archived data (set at 1 month)	Protected	with Veeam	1				
Deleted SharePoint Online sites and items	Protected	with Veeam	1				
Deleted OneDrive for Business files	Protected	with Veeam	1				
Employee leaves the company	Protected	with Veeam	1				

Veeam Backup for Microsoft Office 365 is more than simply filling gaps.

It's about providing access and control to ALL

Exchange Online, SharePoint Online and OneDrive for Business data and storing it in one location, making recovery fast, easy and reliable.

Microsoft + Veeam: Better Together

