The Office 365 Shared Responsibility Model

	Primary Responsibility	Supporting Technology	Security	Regulatory
Microsoft's Responsibility Learn more from the <u>Office 365 Trust Center</u>	MICROSOFT GLOBAL INFRASTRUCTURE	Office 365 Data Replication DC to DC geo-redundancy	Infrastructure- Level Physical Security	Role as data processorData Privacy
	Uptime of the Microsoft Office 365 Cloud Service	Recycle Bin Limited, short term data loss recovery (no point-in time recovery)	Logical Security App-level Security User/Admin Controls	Regulatory Controls Industry certifications <i>HIPPA, Sarbanes-Oxley</i>
	Your office	Office 365 Backup	Data-Level Internal: Accidental Deletion Malicious Insiders	Role as data owner Answer to corporate
YOUR Responsibility	365 data Access and control of your data residing in Office 365	Stored in a different location Full Data Retention ST & LT retention filling any/all policy gaps granular & point-in time recovery options	Employee Retaliation Evidence Tampering External: Ransomware Malware Hackers Rogue Apps	and industry regulations Demands from internal legal and compliance officers

And Microsoft agrees...

Service Availability

6. 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.

Retention policies: What exactly does Microsoft back up?

1 mo 3 mo 1 wk 1 yr 2 yrs 5 yrs \bigcirc () Inbox or folder data In Office 365 Moved to archive Deleted items (recycle bin) In Office 365 Permanently deleted Auto-archived data (set at 1 month) Moved to archive In Office 365 Permanently deleted Deleted SharePoint Online sites and items 1st stage recycle bin 2nd stage Deleted OneDrive for Business files Permanently deleted 1st stage recycle bin 2nd stage Permanently deleted Employee leaves the company In Office 365

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?

Inbox or folder data Deleted items (recycle bin) Auto-archived data (set at 1 month) Deleted SharePoint Online sites and items Deleted OneDrive for Business files Employee leaves the company

1 wk O	1 mo 	3 mo 	1 yr 	2 yrs	5 yrs	>
Protected	with Veeam					
Protected	with Veeam					
Protected with Veeam						
Protected with Veeam						
Protected with Veeam						
Protected with Veeam						

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

