The Office 365 Shared Responsibility Model

Microsoft’s Responsibility
- MICROSOFT GLOBAL INFRASTRUCTURE
  - Uptime of the Microsoft Office 365 Cloud Service
- Recycle Bin
  - Limited, short term data loss recovery (no point-in time recovery)
- Office 365 Data Replication
  - DC to DC geo-redundancy

Your Responsibility
- 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

Supporting Technology
- Office 365 Data Replication
- Recycle Bin

Security
- Infrastructure-Level
  - Physical Security
  - Logical Security
  - App-level Security
  - User/Admin Controls
- Data-Level
  - Internal: Accidental Deletion, Malicious Insiders, Employee Retaliation, Evidence Tampering
  - External: Ransomware, Malware, Hackers, Rogue Apps

Regulatory
- Role as data processor
  - Data Privacy
  - Regulatory Controls
  - Industry certifications
    - HIPPA, Sarbanes-Oxley
- Role as data owner
  - Answer to corporate and industry regulations
  - Demands from internal legal and compliance officers

© 2019 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.
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 re-acquire 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?

- 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

- In Office 365
- Permanently deleted
- Moved to archive

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

Barriers to Modernize
- Data at Risk
- Slow to Cover
- Unclear Path to Cloud

Accelerate Digital Transformation
- Hybrid Cloud Success
- Modernize Data Protection
- Accelerate Cloud Adoption

Limited IT Budget
- Labor Intensive
- Reduce Hardware
- Legacy Tape

Drive Efficiencies
- Simple & Automated
- Shift to Software & Cloud
- Modernize Backups

Growing Risks
- Retention + Data Growth
- Gap in O365 Coverage

Lower Cost & Risk
- Affordable Long-term Storage
- Fully Protect O365

Peace of Mind
24x7x365

Customer Pain

Business Outcome