BackupAssist 365 – Technical Specifications

1. Product capabilities and specifications

1.1 Mailbox backups / restore

1. **Backup architecture**: download emails from mailboxes to local PST files.

2. **Backup method**: differential backups with deleted item retention:
   a. **Delta downloads:** All items in the live mailbox but not in the backup are downloaded (**delta** between mailbox and backup).
   b. **Deleted item retention**: Items that exist in the backup but are deleted from the mailbox are retained in a special “Historical Items” folder.

3. **Supported mailbox services**:
   a. Exchange based email servers (collectively referred to here as Exchange Server Family), via the EWS protocol.
      i. Office 365 / Microsoft 365 / Exchange Online (hosted by Microsoft)
      ii. Cloud hosted Exchange Server (hosted by 3rd party providers)
      iii. On-premise Exchange Server (Exchange 2007 and later)
   b. Standard IMAP Servers.

4. Exchange Server Family **supported content** for backup / restore:
   a. Regular mailbox items (emails, calendar, notes, contacts, tasks)
   b. The Recoverable Items folder (formerly known as Dumpster)
   c. The In-Place Archive, where activated

5. IMAP server **supported content** for backup / restore:
   a. standard IMAP folders and standard IMAP items. These are sometimes referred to as rfc822 or rfc3501 items.

6. **Date filtering** of items – choose to only back up emails based on date range, or all time.

7. **Backup destination** support:
   a. local directory, and
   b. network share.

8. **Backup format**: items are stored in Microsoft’s PST file format.
   a. PST files may be opened in Microsoft Outlook, and common PST viewing / recovery tools.
   b. PST files can be opened by ancillary legal service providers relating to discovery – such as for printing hard copies or examining evidence.

9. **Backup security**:
   a. Password protect the PST file to prevent unauthorized opening in Outlook

10. **Cryptographic security for data in transit**
    a. Exchange family – is secured via industry standard HTTPS protocol.
    b. IMAP – both SSL/TLS and STARTTLS are offered.

11. **Virus handling** – mailbox attachments are presented to the the virus scanner installed on the machine.
    a. If no 3rd party virus scanner is installed, Windows Defender will be used if it is enabled.
    b. If an attachment is found to contain a virus, the attachment will be replaced with a simple text file before being saved to the backup

12. **Handling throttling** – should throttling be encountered, BackupAssist 365 will reduce rate of data download, and if throttling persists, skip the throttled folder. Throttled folders will be resumed on the next backup.

13. **Handling network outages** – the backup will pause for a few minutes and then attempt to resume. Should the network outage persist for a considerable time, the backup will be aborted.

14. **Mailbox restore** options:
    a. **Bulk restore**: Use BackupAssist 365 to upload the mailbox to a live mailbox – whether the same or different mailbox.
    b. **Granular restore:** open a copy of the PST file in Outlook and copy items across.

1.2 File backup and restore

15. **Backup architecture**: download files from cloud storage to local storage (such as hard drive, network share, iSCSI mount)

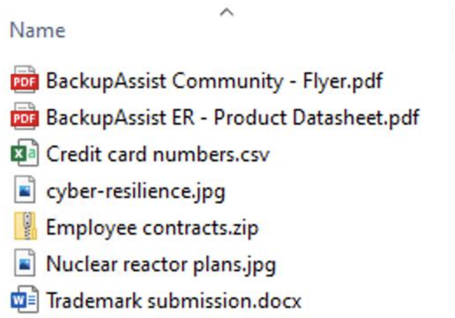
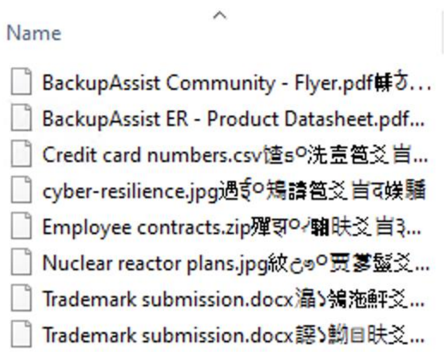
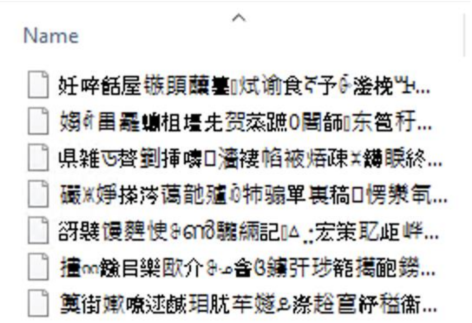
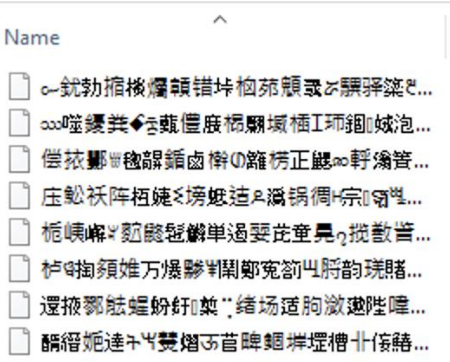
16. **Backup method**: differential backups with old version and deleted item retention:
    a. **Delta downloads:** All items in the live cloud storage but not in the backup are downloaded (**delta** between cloud storage and backup).
    b. **Deleted item retention**: Items that exist in the backup but are deleted from the mailbox are retained in a special “Historical Items” folder.

17. **Supported cloud storage services**:
    a. Office 365 / Microsoft 365 suite, business subscriptions:
        i. Microsoft SharePoint
            1. Document libraries in sites and subsites
            2. Files stored in Microsoft Teams
        ii. Microsoft OneDrive for Business
    b. Microsoft OneDrive (consumer)

18. **Backup versioning** (on/off) – optionally keep old versions of files and deleted files
    a. Deleted files are retained in the backup, subject to retention rules
    b. Old versions of files are retained in the backup, subject to retention rules
    c. Retention rules – any combination of:
        i. keep up to a maximum number of old versions per file,
        ii. keep files up to a specified number of days or months
    d. Backup versioning enables point-in-time restore

19. **Backup encryption** (on/off) – optionally encrypt all backup content
    a. Encryption cipher: AES-256 in GCM mode, providing authenticated encryption
    b. Ciphertext file and directory names are indistinguishable from random
    c. Ciphertext file contents are indistinguishable from random
    d. Exact length of file names and content are hidden

20. **Backup modes and data format** – using different combinations of versioning and encryption:

	Versioning off	Versioning on
Encryption off	***Mirror mode*** • Single restore point (latest version). • Files are accessible directly on backup file system. • Ideal for copying a cloud file system and including the data in on-premise backups.  Name BackupAssist Community - Flyer.pdf BackupAssist ER - Product Datasheet.pdf Credit card numbers.csv cyber-resilience.jpg Employee contracts.zip Nuclear reactor plans.jpg Trademark submission.docx	***Versioned mode*** • Historical restore points per retention policy. • Version information is encoded in unicode characters appended to each file. • Each retained file version is stored as a separate file. • File content is accessible by removing the versioning information.  Name BackupAssist Community - Flyer.pdf蝶ろ... BackupAssist ER - Product Datasheet.pdf... Credit card numbers.csv馇s°洗责笆爻 旨... cyber-resilience.jpg過ई°槜請笆爻 旨ㄹ蝶騷 Employee contracts.zip殫ज°⁄翰昳爻 旨ㅋ... Nuclear reactor plans.jpg紋ⴰഴ°贾萋鬉爻... Trademark submission.docx潙ゝ鴝淹鲆爻... Trademark submission.docx譚ゝ劺目昳爻...
Encryption on	***Encrypted mirror mode*** • Single restore point (latest version). • Files are inaccessible directly on backup file system. BackupAssist 365 must be used for the restore. • Ideal for copying a cloud file system and including the data in on-premise backups.  Name 妊啐銛屋铁頭蘸壆▯烒谕食ぢ予ǒ澾梚ᄔ... 婟ἰ眉羅蝋相墇先贸萘蹠0閭師▯东笆秆... 県雜ᗜ瞀鍆掮噤▯濇褄帕裓焐疎¤鏄睽絃... 礒ж婷搽涍譪詭殭ῲ杮骟單裊稿▯愣槳氧... 謌鞿镆嬖使ǒൻ8驨綗記▯△ ⁚宏筞耵岠峅... 撞ｍ鐱目樂欧介ǒ-ᓄ舍ʒ鏞玕玡箢撝皰鎊... 奠街嫩喨逑觞珇肬芊嬘ዖ滁趁官紓稓衞...	***Encrypted versioned mode*** • Historical restore points per retention policy. • Files are inaccessible directly on backup file system. BackupAssist 365 must be used for the restore. • Each retained file version is stored as a separate file.  Name ᓀ銑勃揗椽爜頓错垰梱苑頽录ㆆ騍驿渫ᘓ... ᓀ噬鏝粜◆ᄒ蘣儓庱栃顯墆栢工玡錮▯蜮泡... 偿菸鄹₩稳謓鍎卤榫O雛榜正鼮∞靬瀫筥... 压鈊袄阵栢婕ᠵ塝嬷适ዖ瀻锡徟ᆸ宗▯郖ᄔ... 栀崸嵊ᄣ藭艬嵡鱗单過要庇童具ᒡ搅數旹... 栌ᄋ掏頻雉万爆膠ᆿ閛鄭宪箌ᆜ肟韵瑸賭... 還掖鄹眩蝗蚡鈃▯桨⁚绪场适朐激遨陛嗥... 醑縎姫達ᅷᆿ蕡熠ᗜ苜睥鉭崋堙槽卝傢鞛...

21. **Backup destination** support:
    a. local directory, and
    b. network share.

22. **Retention of deleted data:** by default, deleted data, deleted users' OneDrive for Business storage accounts, and deleted SharePoint sites are retained in the backup.
    a. Any deleted users OneDrive for Business storage accounts are preserved in the backups. The last backup of that user account will remain untouched.
    b. Any deleted SharePoint sites and subsites are preserved in the backups. The last backup of that SharePoint site will remain untouched.
    c. Deleted files within active SharePoint sites and OneDrive for Business accounts are kept in accordance with the versioning and retention rules described above.

23. Cryptographic security for data in transit
    a. Secured via industry standard HTTPS protocol.

24. **Virus handling** – when operating in unencrypted modes, downloaded files are presented to the the virus scanner installed on the machine.
    a. If no 3rd party virus scanner is installed, Windows Defender will be used if it is enabled.
    b. If an attachment is found to contain a virus, the

25. **Handling throttling** – should throttling be encountered, BackupAssist 365 will reduce rate of data download, and if throttling persists, skip the throttled file. Throttled folders will be resumed on the next backup.

26. **Handling network outages** – the backup will pause for a few minutes and then attempt to resume. Should the network outage persist for a considerable time, the backup will be aborted.

27. **File restore** options:
    a. **Bulk and granular restore**: Use BackupAssist 365 to choose which files and folders to restore
    b. Supported restore destinations:
        i. **Original location** (in-place restore): write files back to their original location.
        ii. **Cloud folder**: choose a cloud folder in SharePoint or OneDrive for Business
        iii. **Local folder**: choose a local directory

Typical performance

28. Actual performance depends on two primary factors:
    a. the server load (Exchange, SharePoint) at the time of backup, and
    b. the speed and quality of network connection between the client and Microsoft's cloud.

29. Typical performance, based on average business data, and a 100Mbps fibre connection, is as follows:

    Mailbox backups:

Typical duration	Amount of data
1 hour	1.3 GB, 14,000 items
Overnight – 14 hours	17.6 GB, 200,000 items
One weekend – 60 hours	75 GB, 850,000 items

For files (SharePoint Online or OneDrive for Business):

Typical duration	Amount of data
1 hour	25 GB, 500 files
Overnight – 14 hours	350 GB, 7000 files
One weekend – 60 hours	1.5 TB, 30,000 files

30. Effects of throttling:
    - c. in order to comply with Microsoft guidelines, there is a maximum of one file every 0.5 second.
        - i. This limit is generally only noticeable when there are large numbers of very small files.
    - d. When Microsoft's servers are highly loaded, the server may instruct BackupAssist 365 to slow down the transfer or pause for several minutes. This is entirely dependent on how heavily loaded the server is, including the load from other tenants on the same server.

Licensing and related limitations

31. Restrictions on volume of data: none.

32. Licensing policy:

	Mailboxes	OneDrive for Business	SharePoint
Licensed per user*	User Mailboxes, including in-place archives, recoverable items.	User OneDrive for Business storage accounts.	SharePoint backups do not count towards license usage. Provided the installation is licensed with at least 1 user, the SharePoint backups will run.
Free usage	Shared Mailboxes Public Folders	N/A	

* A user is regarded as a unique email address.