# Performance Specification
# 365 Total Backup

365 Total Backup is a reliable, intuitive, and easy-to-manage backup and recovery solution for Microsoft 365 Mailboxes & In-Place Archive mailboxes, OneDrive, SharePoint document libraries, Teams chats, Planner, OneNote and Endpoints.

The current requirements for using the service can be found: https://www.hornetsecurity.com/en/365-total-backup-information/

*In order to use the 365 Total Backup service, Customer must have Microsoft Cloud Licenses with either Exchange, Teams, SharePoint and / or OneDrive functionality, activated by Microsoft.*

*All entities within the entire Microsoft tenant that are assigned with a Microsoft 365 License granting functionality for either Exchange, Teams, SharePoint or OneDrive, regardless of their active use, are subject to 365 Total Backup licensing.*

*The highest usage amount of the month will be reported and charged.*

1) 365 Total Backup allows you to perform backups of the customer's specified data. The following functionality is included:
   a. **Multi-Tenancy:** Manage and monitor all Customer's Microsoft 365 Organizations and Windows endpoint backups through a web based multi-tenant console. Different settings can be set per organization.
   b. **GDPR Compliance:** Data retention policies facilitate compliance with the General Data Protection Regulation (GDPR). Backup versions can be automatically deleted on a rolling basis, or completely deleted after a set amount of time from a User/Group detected as removed from an organization. Additionally, backups can be manually deleted for a selected User or Group and site.
   c. **Data Encryption** - Backed up data is being protected by using AES 256-bit encryption for data at rest. All data transmission that occurs is done over a TLS encrypted channel which ensures protection of data sent over the internet or a computer network. A TLS encrypted channel is used during each user authentication interaction, meaning on login, setting changes, subscription management and accessing backed up data.
   d. **Four-Eye Approval** - Enable an additional layer of security that would allow you to mitigate risks of losing valuable data. This optional feature will allow organizations to select specific administrators as approvers for sensitive operations such as: data deletion for Users/Groups, tenant deletion, changes to retention settings and changes to Four-Eye Approval settings. If Four-Eye Approval is enabled, any of the aforementioned operations would need to be approved by a second administrator who is listed as one of the selected approving administrators.
   e. **Dashboard:** Through widgets, authorized administrators can get a clear overview of backup and restore activity, backup health status and recent restore history. When the authorized administrator adds an organization, they can choose which Users and M365 items the authorized administrator wants to back up. The authorized administrator can also configure which directories to back up from User's Endpoints that are either on-premise or roaming, without requiring a VPN connection.

f. **Auto provisioning:** 365 Total Backup automatically detects newly created User content, Group content, and SharePoint sites, and can be automatically backed up without the authorized administrator's intervention.
g. **Backup Frequency:** Microsoft 365 Backups are fully automated and attempted up to 4 times per day. Without prejudice to the generality of the aforesaid, any data that is created and deleted between Backup Snapshots will not be Backed up.
h. **For endpoints**, authorized administrators can choose the backup frequency for specific machines.
i. **Endpoint Backup Policies**: Configure settings for large groups of Windows endpoints by setting up policies to define backup directories, cloud storage, frequency, and retention.
j. Authorized administrators can manually back up specific Users, Groups, SharePoint files, document libraries and endpoints at any time.
k. **Bulk user management:** Enabling backups, disabling backups, and deletion of backup data can be performed for multiple Users at once. Despite the backup being disabled, the backups can be retained and restored even if the User has been deleted from Microsoft 365 tenant.
l. B**ackup Mailbox:** Backups for e-mail Users contain email calendar entries, and contact addresses.
    a. Backup In-Place Archive mailboxes: Possibility to backup all or selected; Users and Shared Mailboxes that have In-Place Archives.
m. **Backup OneDrive:** All files stored in OneDrive are backed up.
n. **Teams Chats Backup:** Backups Teams Chats for Users and Groups within Customer's Organizations, including any files that are shared during the conversations.
o. **SharePoint Backup:** Files and communication in SharePoint document libraries are backed up, including access permissions.
p. **Microsoft Planner Backup:** This feature backs up the plans and tasks that belong to Groups in your Microsoft 365 Organization, along with the comments and attachments in the tasks.
q. **OneNote Backup**: OneNote notebooks owned by Users and Groups are being backed up and can be restored directly to OneNote service.

r. **Endpoint Backup:** Policy driven File-Level backup for Windows desktops and laptops. Endpoint Backup is made up of:

    i. **Endpoint Manager** - is a server software that an authorized administrator installs on its premises or on a cloud virtual machine (VM) that an authorized administrator manages and that must be connected to an Azure Storage account. Endpoint Manager must be used in conjunction with Endpoint Agent(s) (which establish connection to it) to manage backup operations and configure Endpoints.
    ii. **Endpoint Agent** - installed on Endpoints that need to be backed up. Endpoint Agent connects to Endpoint Manager that backs up files and folders according to the backup policy being set up.

2) 365 Total Backup allows authorized administrators to restore backups. This includes the following functions:
    a. M365 Versioning and recovery: Backup data is stored indefinitely until deleted by the authorized administrators. Any version of the file, conversation, or mailbox that exists in the backup can be restored at any time.
    b. Endpoint recovery: Endpoint backup data is stored for the period as configured by the authorized administrator, and it can be restored anytime; back to the original endpoint or to a partner owned management server.
    c. Microsoft 365 Mailboxes and In-Place Archive mailboxes, OneDrive and SharePoint files and document libraries, Planner and OneNote can be:

i. Restored to the original account,
ii. Restored to another account within the same or alternate organization belonging to the same Customer,
iii. Downloaded as a .ZIP archive,
iv. In the case of mailboxes can be exported as a PST.
v. Microsoft 365 Teams Chats can be restored back to a new Team,
vi. Downloaded to HTML files.

d. Download and restore with 365 Total Backup can:
   i. Restore the Backup Data, or part thereof ("granular restore"), taken at any particular Snapshot directly to the original Backup Source or any other Backup Source within the Microsoft 365 Organisation and/or
   ii. Download the Backup Data (password protected), or part thereof taken at any particular Snapshot, and if the authorized administrator chooses this option, a download link to the restored content will be sent via email to the authorized administrator
e. Quick and Advanced Searches: Authorized administrators can search mailboxes and In-Place Archive mailboxes, Planner, OneNote, OneDrive and SharePoint filtered by multiple search criteria.
f. Granular file or email item recovery: Browsing into the contents of the backups allows authorized administrators to select specific files for recovery for mailbox and In-Place Archive mailboxes, OneDrive, SharePoint Document Libraries, Planner plans, OneNote notebooks and Endpoints.
g. Easy-to-use graphs show the monthly usage conveniently.
h. For successful, failed, or warning backup states, e-mail alerts or a daily summary digest notification can be set.
i. Account activity audit: All User account activities in 365 Total Backup are audited. This includes basic and security-relevant as well as data protection-relevant information such as browsing and recovery requests.
j. "Recover M365 data" - A self-service feature that enables the End Users within Microsoft 365 organization to independently recover their own backed up Mailbox, OneDrive and OneNote data without needing the intervention of an administrator. This is accessible via the Hornetsecurity User Panel for all customers onboarded through the Control Panel.

3. Client obligations: The client shall,
   a. Use and access the Service in accordance to the Acceptable Use Policy and adhere with the Fair Use Limits.
   b. Test the Backup Data on regular intervals to determine whether it is complete, accurate and restorable.

4. Limitations & Requirements
   a. Hornetsecurity provides support to authorized users as far as Hornetsecurity systems are concerned. The support of the client's systems is not part of the contract. Limitations and requirements for Microsoft 365 Total Backup can be found here: https://www.hornetsecurity.com/en/365-total-backup-information/

5. Disclaimers
   a. We may not be in a position to offer our Service if the features of Microsoft 365, the structure of the data that is to be backed up or any other technical specifications are modified by Microsoft or any other third party. If this occurs, we may terminate your Subscription but if we do so, we will refund you for any unused period of your Subscription on a pro-rata basis.
   b. Furthermore, we may not back up a Backup Source when this is corrupt, contains errors or is otherwise unreadable, or when we are otherwise precluded to do so by Microsoft or another party on which we rely to provide the Services.

6. Fair Use Limits
   a. The bandwidth, storage, infrastructure and resources that are required to use the Solution and which we make available in this respect are shared across all our clients. As a result, we have the right to take measures to ensure that all clients use the Solution reasonably and fairly so that such use does not interfere with or prevent normal service performance for other clients.
   b. We have decided not to set any pre-established benchmarks which determines excessive or unreasonable use, since, at our discretion, we may choose to preserve our normal service levels by reallocating resources reserved to other users that are at that particular moment not being utilized, or otherwise scale resources. You understand that if we decide not to actively enforce our Sensible Use policy, we shall not be considered as having waived our right to do so, nor have we consented to you continuing using our services at the same level that you are doing at any moment in time.
   c. To benefit from our Services, you are required to acquire Billable Units. The number of Billable Units that you require depend on a number of criteria, such as the size of your organization, the amount of users, data storage size of the particular Sources, etc.
   d. Irrespective of the amount of billable unit you have acquired, you must use our services sensi-bly, and specifically in a way which does not require us to allocate resources disproportionately. In determining this, we will benchmark your use of our resources (e.g., memory requirements, number of parallel connections) against that of the average client. We determine the average client by disregarding the 5% highest clients and the 5% lowest clients of the particular resource and averaging the amount between all our active clients.
   e. Any specific characteristics related to the industry that you operate in shall be disregarded in establishing whether the use thereof is considered to be reasonable.
   f. If we, acting reasonably and in good faith, consider your use of our Solution is not sensible or against this policy, we will, at our sole discretion take any of the following measures:
      i. Allow you to continue to use our Solutions but subject to payment of additional fees and complying with any terms that we may consider reasonable in the circumstances.
      ii. Notify you that your account will be terminated within a timeframe reasonably set at our discretion. During such time, all services and/or operations will be suspended.
   g. If we exercise our right to terminate your account as aforesaid:
      i. Any data (metadata, backup data, or otherwise) will be deleted at the end of the timeframe set out by us in the notification sent by us in this respect, notwithstanding anything to the contrary set out in the Terms and Conditions.
      ii. You will be provided with a refund of the fees paid in advance for the remaining days of your subscription period.