ANYCLOUD BACKUP FOR 365 ENTERPRISE

Service description

Version1.0 March 2025

any.cloud

Table of contents

Introduction to Anycloud backup for Microsoft 365 – Enterprise

This document provides a detailed functional and technical description of Anycloud backup for Microsoft 365 – Enterprise and features available in the Anycloud backup for Microsoft 365 – Enterprise portals. The service is created with the intent to safely backup Microsoft 365 data in a separate cloud dissociated by Microsoft and enable restore functionality. Providing users with the data security needed which is not ensured in Microsoft 365 by default.

Anycloud backup for Microsoft 365 - Enterprise is a highly scalable solution suited for larger enterprises with a minimum of 1500 Microsoft licenses to back up. The solution is cost-efficient by combining Anycloud backup for Microsoft 365 and Anycloud object storage for backup. In essence the solution offers secure and compliant backup of your entire Microsoft 365 environment and data is safely stored in an object storage solution built natively on IBM Cloud making Anycloud backup for Microsoft 365 – Enterprise a robust, highly secure and cost-effective solution for enterprise businesses.

OBJECT STORAGE
SEATS
ENTERPRISE

Microsoft has hundreds of millions of users every day accessing their data from their M365 platform. The purpose of Anycloud backup for Microsoft 365 – Enterprise is to provide a secure backup of the data stored within Exchange, OneDrive for Business, SharePoint, and Teams. Microsoft is responsible for the infrastructure and the availability of the Microsoft 365 Cloud Service. Users are responsible for the access and control of the data residing in the Microsoft 365 environment. Therefore, it is the users' responsibility to backup and recreate any lost data.

The simple-to-use and intuitive interface of Anycloud backup for Microsoft 365 – Enterprise, is built on advanced technology from market leading software. The backup data is stored in object storage with military grade encryption within highly secured and certified IBM datacenters. This allows administrators to easily and securely backup their data outside of Microsoft while ensuring maximum security and compliance.

About any.cloud

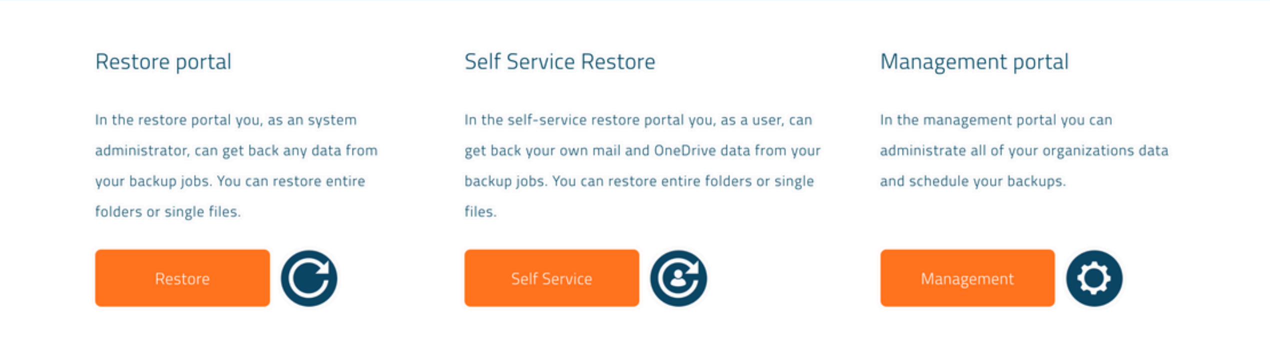
any.cloud guides innovation forward for over 210,000 leading technology manufactures and service providers. any.cloud develops technology solutions that help improve business and daily life. any.cloud broad portfolio that spans the entire technology landscape helps customers create, make, and manage forward-thinking products that make the benefits of technology accessible to as many people as possible.

TERMINOLOGY	
Anycloud backup for Microsoft 365 – Enterprise	The service provided by any.cloud allows customers to backup, manage, and restore their Microsoft 365 data.
Software	All data are processed and handled using IBM Cloud data centers.
IBM Cloud	The provider of the data centers, where backup data from Anycloud backup for Microsoft 365 – Enterprise will be located. The geographical location for the backup data can be selected by the customer in the onboarding process.
True cloud-to-cloud model – to meet highest compliance	The backup is air-gapped and follows the principle of segregation of duties (SoD). Backup data is 100% separated from Microsoft 365 tenant and transferred to the selected IBM data center.
any.cloud	The provider of the service Anycloud backup for Microsoft 365 – Enterprise.
Management portal	The Management Portal is where system administrators schedule backup jobs.
Self-Service Restore Portal	The market leading simple Self-Service Restore Portal is where employees can restore mail and OneDrive files in one click.
Restore Portal	The Restore Portal for System Administrators where you can restore all backup data.
Backup	The remote copy of Microsoft 365 data.
Restore	The process of replacing a lost or deleted item from a backup.
Microsoft 365	The provider of the online services Exchange Online, Teams, SharePoint, and OneDrive for Business.
Insider Threat Protection	Complete protection for Microsoft 365, Exchange, SharePoint, OneDrive, and Teams. Data cannot be overwritten, altered, or deleted for the duration of the retention period.

TERMINOLOGY CONTINUED..	
GDPR, ''Right to be forgotten''	A feature that allows a user to be completely deleted from the backup retention part.
Role Based Access Control (RBAC)	A feature that enables users within the same tenant to access multiple predefined roles ensuring secure and flexible permission management inherited from the users Microsoft environment.
Search Protection	Enables live search of backup data without creating an index copy preventing potential misuse. To ensure confidentiality and security, only subjects, titles, senders, recipients, and dates are visible, while message body content remains hidden during search and restoration.
Insider Threat Protection	Safeguards against malicious or accidental deletions by retaining all deleted data for 30 days.
Encryption	Ensures that data is accessible only to the customer and remains unreadable by service providers, guaranteeing privacy and security.
Resting state	Refers to data that is stored and inactive, ensuring it remains secure while not in use.
Transit	Refers to data that is actively being processed or transmitted, ensuring its integrity and security during transfer.
Tenant	Represents the customer's dedicated environment within Microsoft 365, encompassing all associated resources and user accounts.
RPO (Recovery Point Objective)	Defines the maximum acceptable amount of data loss, measured as the time interval between two backup sessions in the event of a disaster.
RTO (Recovery Time Objective)	Specifies the maximum amount of time required to restore services and to recover operations following a disaster.

Functional description of Anycloud backup for Microsoft 365 – Enterprise

Anycloud backup for Microsoft 365 – Enterprise consists of 3 portals:



Restore portal

In the restore portal you, as an system administrator, can get back any data from your backup jobs. You can restore entire folders or single files.

Self Service Restore

In the self-service restore portal you, as a user, can get back your own mail and OneDrive data from your backup jobs. You can restore entire folders or single files.

Management portal

In the management portal you can administrate all of your organizations data and schedule your backups.

The Management Portal serves as the administrative interface for managing all organizational data, including scheduling backups. It is also in the management portal where retentionperiods for data are chosen – 1, 2, 3, 5, 7, 10, or 25 years.

The Restore Portal is the interface used to retrieve and restore backups. It is possible to restore entire folders or single files as needed.

The Self-Service Restore Portal allows single individuals to independently restore their own mail and OneDrive data from backup jobs. Users can restore entire folders or single files as needed.

Before the backup process can begin the customer needs to choose the data location in the Management Portal of Anycloud backup for Microsoft 365 – Enterprise. Data security is our priority, and our backup service is delivered in 17+ IBM Cloud data centers across the globe, all of which meet at least Tier-3 standards. In the data centers data is air-gapped, which ensures data is divided into separate physical environments. Air-gapping is a simple and very efficient solution, that isolates backup data from the production data. This protects customer's data from ransomware, since data is protected not only by being a copy, but by being practically inaccessible to any virus/malware. In addition, for enhanced protection and compliance, the solution is fully managed through a web application removing the possibility for any user to access the storage directly and therefore preventing unauthorized data deletion out of processes and routines set by the customer.

Furthermore, the service creates a secure backup through Insider Threat Protection (ITP) ensuring complete protection of Microsoft 365, Exchange, SharePoint, OneDrive for Business, and Teams data. Data cannot be overwritten, altered/modified, or deleted during the retention period, except when using the "right-to-be-forgotten" feature in the portal.

Right to be forgotten

To comply with the "right to be forgotten" -act, any.cloud have introduced a feature that allows end-customers to delete specific users and their associated data. When a deletion request is submitted through the portal, the designated administrators of Anycloud backup for Microsoft 365 – Enterprise tenants receive a notification. A 72-hour grace period then begins, marking the user for deletion. This delay ensures that accidental deletion requests can be withdrawn within the given 72-hours timeframe.

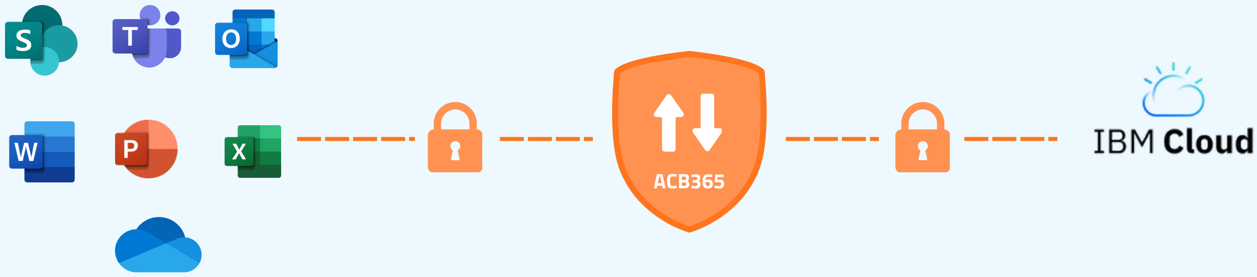
Accessing Support

Customers can access support for the solution through the integrated support feature within the Management Portal, ensuring direct and efficient assistance. Additionally, AI-powered support enables multilingual support for a streamlined user experience. All support services are provided remotely. All backup and restore activities are logged to provide documentation and audit trail visibility. Backup logs include who requested the backup. Restore logs include who requested the restore, of what and when.

True cloud-to-cloud

While Microsoft hosts the infrastructure for Microsoft 365 and other solutions, They are not responsible for the data stored in its platform. Without a backup, lost data cannot be recovered. Anycloud backup for Microsoft 365 – Enterprise is delivered in a cloud-to-cloud backup model, making sure data residing in Microsoft is safely backed up and transferred to another cloud. This ensures data availability and allows for restoration in case of lost or deleted data.

The Architectural Diagram – The backup & restore process



To initiate the backup process, access the Management Portal to configure your tenant account, then define and execute the backup jobs. The backup data is securely transferred directly from Microsoft 365 to IBM Cloud using Anycloud backup for Microsoft 365 – Enterprise service.

Anycloud backup for Microsoft 365 – Enterprise is built on industry-leading technology, ensuring end-to-end data security both in transit and at rest.

- Data in transit is encrypted with AES-256 bit.
- Data at rest is encrypted with AES-256 bit.

During the initial setup, customers select the data storage location from multiple available options. The chosen data center will be the permanent storage location for the customer's backups, and only the customer has the authority to delete their data. Once the location is selected, backup data is transferred to the designated IBM Cloud data center, where it remains in a secure resting state. The backups are performed at customer-defined intervals and retained according to the configured retention policy.

Within the Management Portal, users can customize their email notification preferences for Anycloud backup for Microsoft 365 – Enterprise. Options include receiving daily backup reports or only being notified in the event of an error or warning.

When restoration is required, the process is conducted through the Restore Portal of Anycloud backup for Microsoft 365 – Enterprise. For email restores, users have two options: restore to the original location or restore to an alternate location, both within the same tenant. For other Microsoft 365 data types, backups are restored exclusively to their original location.

Item level and indexing

The restore process in Anycloud backup for Microsoft – Enterprise includes a search tool designed to help users locate the data they need to restore. To ensure privacy and compliance, data is only indexed by the following: sender, receiver, subject, file type, file name, and date. Entire email contents are intentionally not indexed to uphold data integrity, compliance, and security across the service.

Supported backup types within ACB365 – Enterprise

Microsoft Exchange Online

User mailboxes, including:

- Emails
- Calendar
- Contacts
- Tasks
- Notes
- Shared mailboxes
- Resource groups
- Archive mailboxes

Microsoft OneDrive for Business

- Any files and folders stored within Microsoft OneDrive

Microsoft SharePoint Online and Microsoft SharePoint Personal sites

- Sites
- Document libraries
- Document lists
- Documents
- List items

Microsoft Teams

- Channels
- Tabs
- Posts
- Files

Recovery Time Objective (RTO)

Backup Recovery Time Objective(RTO) is a critical factor in ensuring business continuity. In restore scenarios, Microsoft allows temporarily removal of throttling to facilitate faster data recovery from Exchange. With Anycloud backup for Microsoft 365 – Enterprise, restores are perfomed quickly and securely back into Microsoft 365 environments, ensuring a low RTO.

Frequency and retention

Backup jobs are initiated automatically based on the defined scheduler settings, which determine how often Microsoft 365 data is backed up. The available frequency options include:

Daily: The backup job will create restore points repeatedly throughout a day on specific days.

Supported retention are:

1 year
2 years
3 years
5 years
7 years
10 years
25 years

API

Certain API calls and integration such as job status, consumption, seat counts etc. is available to retrieve and implement into customers own back-office systems.

The Enterprise billing model

Anycloud backup for Microsoft 365 – Enterprise pricing is structured around:

Minimum commit on Enterprise model

- 1.500 seats
- 10 TB storage (ACOSB)
- Commit model is 3 years
- Prepaid model per year (annual billing)

Overage on minimum commit Enterprise model

- Seat overage are invoiced monthly in arrears
- Storage overage are invoiced in full TB's monthly in arrears

Seat licenses

Seat licenses beyond the Enterprise Commit model are determined based on the number of users included in the backup jobs. These jobs can be configurated to target specific Azure Active Directory Groups, limiting the scope of users. Alternatively, an exclusion group can be defined in web portal, ensuring that users within this group are excluded from backups and the licensing counts. Backup jobs can also be configured to include the entire customer organization, backing up all user accounts within the Microsoft365 tenant. In this case, the number of licenses utilized will match the total number of users in the tenant.

Licenses enable daily backups and remain active until the license is terminated, as the service operates on an ongoing basis. Additionally, it is possible to set a cap on the number of licensed seats – any new users beyond this limit will not be backed up.

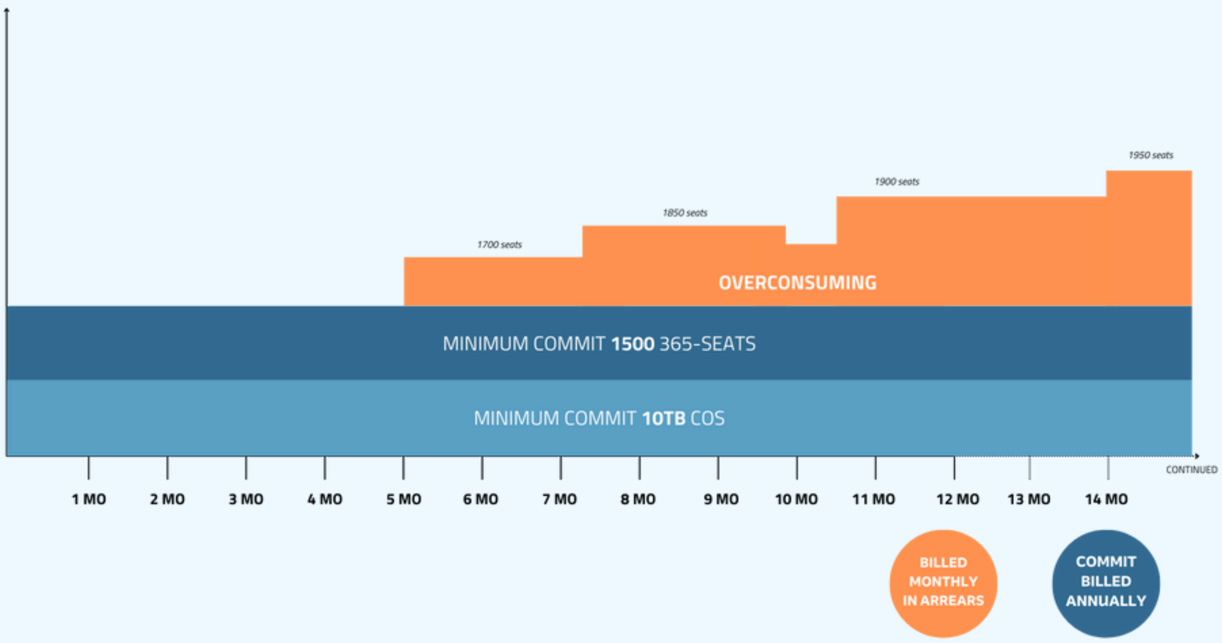
To determine the required number of seat licenses:

- Count the total number of users within Microsoft 365 who have an active subscription.
- A user is counted only once, even if they use multiple Microsoft 365 services (e.g., Exchange Online, SharePoint Online, and OneDrive for Business).
- 1 user = 1 Anycloud backup for Microsoft 365 – Enterprise license.

Examples

*Consumption overage is added on a per seat basis. The below example is based on a **1500 seat** commit*

- *Accumulated 1505 seats for one month – additional 5 seats invoiced, monthly in arrears*
- *Accumulated 1805 seats for one month – additional 305 seats invoiced, monthly in arrears*



A user account consists of:

- Microsoft Exchange Online: Such mailbox can be a personal mailbox, an Online Archive mailbox or both.
- Microsoft SharePoint and Microsoft SharePoint personal sites: Each Microsoft 365 user with access to Teams, communication, collaboration, and other non-personal SharePoint sites intended for back up must be licensed.
- Microsoft Teams: Each Microsoft 365 user with access to Microsoft Teams objects designated for backup requires a license. The license is consumed by any object (mailboxes, OneDrive for Business accounts, or SharePoint personal sites) for which at least one restore point has been created within the past 31 days. If an object is not backed up for 31 days, the license is automatically revoked.

The ACB365 – Enterprise license is not required for:

- Shared, Resource and Group mailboxes: Shared and resource mailboxes do not consume units in the license if such mailboxes do not have a Microsoft Office 365 license assigned.
- External SharePoint users: An external SharePoint user is a user outside of the customer's Microsoft 365 subscription who has been granted access to one or more sites, files, or folders. External authenticated users are limited to basic collaboration tasks, and external anonymous users can edit or view specific documents when granted explicit permissions.

Licensing model beyond 10 TB

The monthly storage overage rate is divided by the number of days in the current month to determine the daily rate. The daily charge is calculated based on the rounded-up TB used each day per storage account exceeding **10 TB**. At the end of each month, all daily charges are summed to generate the monthly invoice.

Examples

Consumption is added in full TB levels, examples for 10 TB commit

- *10.2 TB equals 11 TB – 1 TB additional invoiced, monthly in arrears*
- *20.9 TB equals 21 TB – 11 TB additional invoiced, monthly in arrears*

Consumption is added in full TB levels, examples for 30 TB commit

- *35.1 TB equals 36 TB – 6 TB additional invoiced, monthly in arrears*
- *49.5 TB equals 50 TB – 20 TB additional invoiced, monthly in arrears*

Customer Data Encryption

Customer data is encrypted with AES-256 bit in flight and at rest in IBM data centers.

Compliance

The Anycloud backup for Microsoft 365 – Enterprise service is created by any.cloud, who is an ISO 27001 certified company with an SLA formed by the regulations and requirements based on ISO 27001 and has an GDPR ISAE 3000 assurance report made by an independent external auditor every year.

The service complies with the General Data Protection Regulation and standards mentioned above. In addition, the technologies used are also compliant as all backup data is encrypted, – once you have placed your data in one of the datacenters it stays there. Data security is highly valued, and the data belongs only to the customer that owns the data even if the customer should decide to stop using Anycloud backup for Microsoft 365 - Enterprise. The future proof of the data is ensured thanks to software from market leading vendors, which is the foundation for the service. Our cloud backup for 365 services is delivered utilizing 17+ IBM Cloud data centers globally. All data centers have minimum. SOC2 reports, and the EU data centers are all GDPR compliant.

IBM data centers

Anycloud backup for Microsoft 365 – Enterprise is delivered through IBM data centers, which are all minimum tier-3 data centers. Meaning data centers have multiple paths for power and cooling, including redundant systems that allow maintenance without the services being offline. This tier has an expected uptime of 99.982% per year according to IBM SLA.

For data resilience there are several options to choose from:

- Single: Data stored in a single geographical data center is distributed in many physical storage appliances.
- Regional (recommended): Backups in regional geographical datacenters distribute the data across 3 independent IBM Cloud data centres spread across a metropolitan area 10 km apart. Any one of these data centers can suffer an outage or even destruction without impacting availability and data resiliency.
- Climate friendly sites: Several IBM data centres are climate friendly, which is shown by a green leaf in the onboarding process.

Import of existing retention data

In case the customer wishes to import retention data from a compatible environment before initiating the service, the following conditions applies:

- The customer must first purchase Anycloud backup for Microsoft 365 – Enterprise and authenticate their tenant in the portal. At this stage, no backup jobs may be created.
- The customer must provide access to the existing (or a copy of) Veeam-compatible version backup retention data stored in a cloud object storage location. The data must be encrypted with a password using Veeam Backup for 365 software. The encryption passwordmust be supplied securely to us. Note: We only accept imports from data encrypted with Veeam Backup for 365.
- The backup data must be sourced from a Veeam backup for 365 version that is compatible with the version currently used by us, typically the latest version.
- While copying the data, the backupdata must not be altered in any way, as any changes will cause the import to fail.
- Once the import is completed, the customer may proceed to set up their backup jobs.
- NOTE: Only users included in the backup jobs created within Anycloud backup for Microsoft 365 – Enterprise will be entitled to use the supplied retention data. It is not possible to restore or transfer users who are no longer part of the backup/tenant, even if they are present in the supplied retention data.

Data retrieval following the termination of the service

In the event of data retention export after termination of the service, the following terms applies:

- No seat/license requirement is needed to use the the export service. However, there is a 1.500 EUR fee per tenant to be exported.
- The receiving party must use Veeam Backup for 365 in the same version as Anycloud backup for Microsoft 365 – Enterprise. The version number in use will be provided upon export request.
- The customer must provide access to a cloud object storage location within IBM cloud. If the object storagelocation is outsideof IBM Cloud, an additional fee of 100 EUR per TB of data will be applied.
- The encryption key/password will be provided to the receiving party of the backup retention data.
- No assistance will be provided for adding the data to the receiving software or creating jobs etc.
- Due to limitations in Veeam backup for 365, only users included in the new backup jobs will have the supplied retention applied. Users in the retention data but not part of the new backup jobs will not be able to be restored.
- We do not offer assistance adding the data to the receiving software or creating jobs etc.

Choosing Anycloud backup for Microsoft 365 – Enterprise

- Protect your data with a true cloud-to-cloud backup
- Flexible pricing through the Enterprise billing model
- Quickly overcome data loss
- Simplified management via one platform

Anycloud backup for Microsoft 365 – Enterprise differs from other backup services available on the market, because of the deep focus on compliance. The service has built-in Insider Threat Protection (ITP) making sure that all backup and restores are logged and that if data is deleted by an insider or by accident, it is safely stored for 30 days after deletion.

The unique portal and its built-insecurity make Anycloud backup for Microsoft 365 – Enterprise a solution, easily integrated in any organization that needs backup of Microsoft365 data. Providing data security and data protection by storing a copy of data, physically separated and away from both Microsoft and the organization. The service allows IT administrators to use their time wisely, as backups are scheduled and carried out automatically in the system. Anycloud backup for Microsoft 365 – Enterprise is for companies in need of data protection, that require easy and secure backup operations.

Service levels and support

Availability:

Anycloud backup for Microsoft 365 – Enterprise ("the Solution") shall be available 99.999 percent of the time, calculated in accordance with these Terms over the previous calendar month ("Availability Time").

Availability shall be calculated as follows:
(Availability / (Totaltime – Planned downtime)) x 100

Where:

Availability refers to the total number of hours during the previous calendar month period when the service was available for the partner.

Total time denotes the total number of hours within the previous calendar month.

Planned downtime is defined as the number of hours in the previous calendar month during which the service unavailable to the partner due to planned services and maintenance as outlined in the section "Service and Maintenance".

Availability shall not include:

- Faults, deviations, delays, changes or similar events on hardware, software, network systems and equipment's delivered by a third party (except for any.cloud's subcontractors), and which are outside of the control of any.cloud.
- Faults, deviations, delays, changes, or similar events caused by the customer or on the customers equipment which communicates with the data center(s).
- Other matters which are caused by the customer, customer's hardware, software, network systems and equipment's, customer's employees or persons or entities engaged by the customer ("customer's IT environment") except when such matter has been caused by the customer following the instructions of any.cloud or its sub-contractors.

Service and Maintenance

any.cloud shall, always, be entitled to carry out planned service, repair, and maintenance of the solution and will be presented in the portal. any.cloud shall always ensure that any planned service, repair, and maintenance is undertaken at a time which will have the least business interruption on the partner and its customers. Such planned service, repair and maintenance of the solution shall be regarded as planned downtime and shall be disregarded when calculating the availability of the solution.

If the partner wish to change, amend, or upgrade the solution, the partner shall submit written request to any.cloud. any.cloud shall carry out the requested change within a period of fifteen (15) working days after the receipt of the request, unless any.cloud, at its discretion, prior hereto notifies the partner that the requested changes cannot be made. any.cloud shall pay for the changed services in accordance with any.cloud's price list, always. The time used by any.cloud in connection with the change of the solution, shall be considered extra work and shall be paid separately by the partner.

The partner shall, on reasonable request from any.cloud, assist any.cloud where reasonably possible with error tracing and diagnostics related to incidents the partner has reported.

The partner shall keep any.cloud informed on the technical and administrative contact persons at the partner and their contact information.

any.cloud shall commence error tracing as soon as possible after any.cloud has received information regarding the error in such a manner that, in the reasonable opinion of any.cloud, enables any.cloud to identify the nature of the error or any.cloud becomes aware of an error through any.cloud's surveillance of the solution ("Required Information"). any.cloud shall aim at commencing error tracing within one hour after receipt of Required Information (two hours outside of any.cloud's normal business hours as determined by any.cloud). If, in the reasonable opinion of any.cloud, a material event occurs regarding any.cloud's infrastructure (and not related to the partner's IT environment), any.cloud shall aim at commencing error tracing within 15 minutes after receipt of required information (30 minutes outside of any.cloud's normal business hours as determined by any.cloud).

Re-establishment Time

Re-establishment time means the time, which it takes for any.cloud to re-establish the partner's solution in the event of interruption ("Re-establishment Time").

The Re-establishment Time depends on the solution, the customer, the customers' IT environment, and therefore the Re-establishment Time depends on the specific circumstances. any.cloud shall, however, aim at re-establishing customer data within three (3) working days hereinafter. This shall, however, not apply in the event of intentional act of the customer or in the event of a Force Majeure event.

Service Levels and Ongoing Contact Agreements

Priority	Initial contact SLA	Progress updates
P1	30 minutes	4 hours
P2	2 hours	8 hours
P3	4 hours	8 hours

Service Levels and Ongoing Contact Agreements

P1 – Mission Critical Incident – Service is down causing critical impact to business operations if service is not restored quickly, and no workaround is available.
Example of scale can be partner cannot access service; customers cannot access service.

P2 – Problematic Incident - The service performance is degraded. Service functionality is noticeably impaired, but most business operations continue.

P3 – Informative Incident – It is used for general requests for information regarding supported products, and in cases when the supported product's performance is inconsistent with documentation but causing no disruption or degradation to IT systems.

Accessing support

Support as a direct consequence of the customer's use of the solution should be accessed by the partner using an integrated supportfeature within the Management Portal, providing direct and immediate access to assistance. In addition, the support feature incorporates AI enabling support in multiple different languages ensuring a simplified user experience.
All support is carried out remotely.

Support hours

Standard support is delivered during normal working hours which are Monday – Friday, 8-16 CET. Extended support offerings are available.

Customer obligations

To access the service, the customer must provide connection details to their Microsoft 365 tenant, and this should be done by an individual with Microsoft 365 global administration rights. This can be done either via the partner or inputted directly by the customer. The customer is also required to identify the groups they would like to backup or the user count if the entire organization is required. This should be agreed between the partner and the customer.

LET'S STAY CONNECTED

Anycloud A/S
Hedegaardsvej 88
2300 Copenhagen S
Denmark

CVR: DK31161509
E-mail: sales@anycloud.dk

any.cloud