ANYCLOUD BACKUP FOR ENTRA ID

Service description

Version 1.0 September 2025

any.cloud

Table of contents

About Anycloud 1

Introduction to Anycloud Backup for Entra ID 1

Terminology 2

Functional description of Anycloud Backup for Entra ID 5

Terms and termination 13

Service levels & support 13

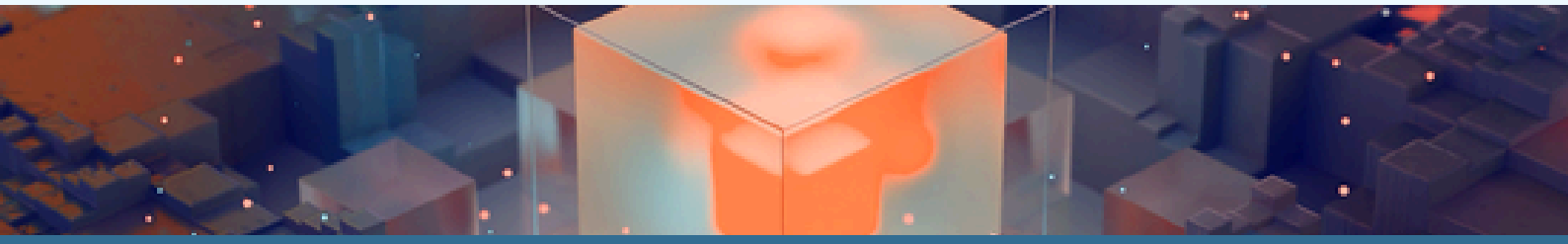
Customer obligations 16

Combining Anycloud backup for Microsoft 365 and Entra ID 16

Document references 17

About Anycloud

Anycloud is a leading provider of innovative cloud solutions for businesses through distribution worldwide with more than 25 years on the market. We continuously progress to fit the IT landscape, while delivering innovative offerings, to our distributors and their partners and customers, built with scalability and simplicity. We collaborate with our distributors to deliver security and data management. Our portfolio of cloud solutions each has an individual focus and expertise for data protection and digital security, delivering market leading technology.



Introduction to Anycloud Backup for Entra ID

This document provides a detailed functional and technical description of Anycloud Backup for Entra ID and features available in the Anycloud Backup for Microsoft 365 portals. Anycloud Backup for Entra ID is a full-featured SaaS-based backup and recovery solution designed to safeguard the identity and access infrastructure in Microsoft Entra ID (formerly Azure Active Directory). The service is the critical entry point to thousands of cloud and SaaS applications and ensures continuity, visibility, and compliance by protecting against misconfiguration, deletion, or attack.

Microsoft Entra ID is under constant attack, with over 600 million identity-related threats detected daily. The combination of cyberthreats, accidental deletions, policy misconfigurations, and strict regulatory frameworks (e.g. GDPR, DORA) increases the urgency to secure Entra ID. Microsoft's Shared Responsibility Model confirms that the protection of identity data is the customer's responsibility. Anycloud backup for Entra ID closes this gap with proactive monitoring, secure backups, and lightning-fast recovery options.

The following additional definitions apply:

TERMINOLOGY	
Partner	The company entering into the agreement with Anycloud.
Customer	A business that purchases the service from the partner. Also known as an "end user" in the agreement.
User	Anyone permitted by the customer to use the service and who may be granted access to Anycloud Backup for 365 and the web portal.
Anycloud backup for Entra ID	The backup service provided by Anycloud that protects identity objects and configurations in Microsoft Entra ID, including users, groups, roles, applications, and policies. It enables secure, automated backups and fast recovery to ensure continuity, visibility, and compliance.
Supplier	any.cloud A/S, having its principal place of business located at Hedegaardsvej 88, 2300, Copenhagen S Denmark.
Portal	The portal is where management and restore of Entra backup is happening.
Restore	The process of replacing a lost or deleted item from a backup.
Backup	Customer data stored in the service for the selected retention period.
Microsoft 365	The provider of the onlineservices Exchange Online, Teams, SharePoint, and OneDrive for Business.
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 – Entra ID will be located. The geographical location for the backup data can be selected by the customer in the onboarding process.

TERMINOLOGY CONTINUED..	
Customer data	Includes any data, text, drawings, diagrams, images, or sounds (together with any database made up of any of these) embodied in any electronic, magnetic, optical, or tangible media and stored in the customer's Microsoft Entra ID tenant, including identity objects such as users, groups, policies, and applications.
Incident	Any reported event not part of the standard operation of the Service and which causes disruption to or a reduction in the quality of the service.
License	Required for each customer who wishes to use the service. Licenses are more fully described in section 4 of this document.
Retention period	The amount of time each selected backup is stored for within the service.
Cloud-to-cloud model	The backup is air-gapped and follows the principle of segregation of duties (SoD). Backup data is 100% separated from the Microsoft 365 environment and transferred to the selected IBM data center.
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.
Insider Threat Protection	Safeguards against malicious or accidental deletions by retaining all deleted data for 30 days.
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.
Encryption	Ensures that data is accessible only to the customer and remains unreadable by service providers, guaranteeing privacy and security.

TERMINOLOGY CONTINUED..	
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 Entra ID

Anycloud Backup for Entra ID operates as a fully managed SaaS platform. Customers connect their Entra ID tenant securely and begin protection with minimal setup and consist of 1 portal:

Anycloud Backup for Entra ID offers complete flexibility in retention management. Customers can define retention policies from a day to unlimited, ensuring compliance with internal policies, industry standards, or regulatory requirements. Unlike fixed retention models, the service allows administrators to adapt retention settings dynamically, giving full control over how long identity data is stored and ensuring recoverability without unnecessary limitations.

The restore function within the portal is the interface used to retrieve and restore backups. This portal allows administrators to recover Entra ID objects such as users, groups, applications, and policies.

The portal also provides access to:

- Configure and manage backup jobs
- Select retention period
- Monitor job status and configure notifications
- Restore Entra ID objects such as users, groups, roles, applications, conditional access policies, administrative units, audit logs, and change history
- View a security overview including a dashboard with security score, personalized recommendations, and direct links to best-practice guides for improvement
- Access a full audit trail of login and sign-in logs, including error codes for quick diagnostics
- Compare changes in users and groups between the current and the last backup
- View detailed information for individual users and groups
- Review backup and restore logs for complete traceability

Data security is our priority, and our backup service is delivered in 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.

The service includes protection against insider threats by retaining deleted identity data for a defined period, ensuring recoverability of users, groups, and other Entra ID objects. Data cannot be overwritten, altered/modified, or deleted during the retention period.

Supported backup types

The following identity-related components in Microsoft Entra ID are included in the scope of Anycloud Backup for Entra ID service:

- Azure AD/Entra ID users (including attributes and group memberships)
- Security and Microsoft 365 groups
- Administrative units and rirectory roles
- Application registrations and Enterprise apps
- Conditional access policies
- Audit logs and change history

Recovery Time Objective (RTO)

Recovery Time Objective (RTO) is a critical factor in ensuring business continuity. Anycloud Backup for Entra ID enables rapid object-level restore through an optimized workflow. Impacted objects can be recovered quickly and securely, with minimal disruption to business operations. With Anycloud Backup for Entra ID, restores are performed quickly and securely back into Microsoft 365 environments, ensuring a low RTO. Automated identification of impacted items and one-click restore ensure that services are returned with minimal downtime. In most scenarios, recovery is completed within minutes. Throttling can be bypassed temporarily to accelerate bulk recovery, where permitted by Microsoft.

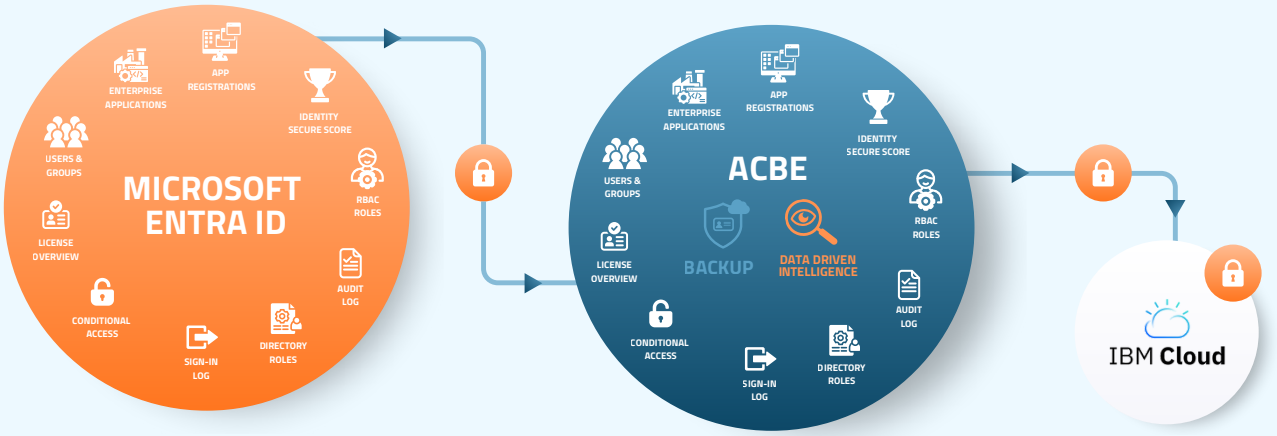
Right to be forgotten

Anycloud Backup for Entra ID supports GDPR-compliant data deletion. Admins can initiate a 72-hour grace period to delete user backup data permanently, offering organizations full compliance with "right to be forgotten" mandates.

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 Entra ID 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 Entra ID service.

Anycloud Backup for Entra ID 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 Entra ID. Options include receiving daily backup reports or only being notified in the event of an error or warning. The Management portal is available to the partner and can also be made available to customers. Key features of the module include but are not limited to the following:

- Track user
- Different retention periods
- Add new customers and users
- Add new administrators
- All activities are logged
- Setup and monitor backup jobs
- Multiple users can receive job reports and warnings via email
- Geo location can be chosen for the backup data

When restoration is required, the process is conducted through the Restore portal of Anycloud Backup for Entra ID. The Restore portal allows system administrators to restore customer data back to their Microsoft 365 account. Key features of this portal include – but are not limited to the following:

- Restore Entra ID objects such as users, groups, applications, and policies to the tenant with full audit tracking and conflict detection.
- Restore replace existing data only if it is actually missing
- Adaptive restore option view for faster restore
- Administrator(s) restore capabilities Extensive logging
- Restore objects in-place or to a different environment
- Restore single objects, collections of objects, or entire configuration sets
- Restore with overwrite or merge options
- Preview changes before restore

Change comparison
Side-by-side comparison of backed-up objects with their current state is available, enabling quick identification of modifications, deletions, or additions.

Administrative roles in Anycloud Backup for Entra ID
Partners and customers can set up different access roles in the three portals to control whether users have limited or full access using Role-Based Access Control (RBAC).

3.7. Item level and indexing

The restore process in Anycloud Backup for Entra ID includes a search tool that allows administrators to locate specific users, groups, applications, or policies for recovery. To ensure compliance and privacy, only metadata such as object names, creation dates, and modification dates are indexed – not the full object content.

Frequency and retention

Backups are generated automatically at fixed intervals, typically ranging from once an hour to daily. This ensures that data is continuously protected without the need for manual intervention. The system uses so-called incremental backups, where only the changes made since the last backup are stored. This strategy makes both time and storage use more efficient by eliminating unnecessary copies of unchanged files. Additionally, the method contributes to faster and easier data recovery while ensuring optimal utilization of resources.

Underlying technology

The service is built on IBM Cloud technology and delivered exclusively from IBM Tier-3+ data centers. IBM Cloud technology is certified for ISO 27001, ISO 27017, ISO 27018, SOC 1 Type 2, SOC 2 Type 2, and SOC 3. All EU data centers are GDPR-compliant. The customer selects the data location during onboarding, after which backup data is permanently stored in the selected region.

Retention periods

Backups are kept according to the customer's chosen retention policy, which can range from a day to unlimited. The retention setting is defined directly in the web portal, and backups will automatically be managed according to the selected policy. This ensures that organizations can align retention precisely with internal guidelines or regulatory requirements.

If needed, the retention period can be changed at any time through the Management portal.

Licensing Model

Anycloud Backup for Entra ID is available as a standalone service or as part of a bundle with Anycloud Backup for Microsoft 365. Licensing and pricing are defined in the EULA. Please refer to the current EULA for applicable terms.

Customer data encryption

Customer data are encrypted with AES256 bit in flight and at rest.

Product features

Anycloud Backup for Entra ID provides a comprehensive set of operational and security-focused features designed to ensure continuity, visibility, and compliance for identity data.

Centralized management portal

- Single interface for configuration, monitoring, restore, and reporting
- Partner and customer management views for multi-tenant administration

Granular and full directory restore

- Restore individual objects, selected collections, or complete configuration sets
- Side-by-side preview of changes before restoration to prevent accidental overwrites
- Restore with overwrite or merge options for controlled recovery

Advanced change tracking

- Detailed, side-by-side comparison of changes between backup versions
- Historical insight into directory settings, policy changes, and security configurations
- Full traceability of object creation, modification, and deletion events

Security and compliance tools

- Security score dashboard displaying current security posture with a numeric score
- Contextual, personalized recommendations for security improvements
- Full audit trail of login and sign-in logs, including MFA events, conditional access results, and error codes
- Direct links to vendor-verified security hardening guides
- Exportable audit reports to support compliance audits and investigations

Security insights and governance from backup data

Anycloud Backup for Entra ID does more than preserve identity configurations and objects – it actively turns backup data into actionable security and governance insights within the portal. By continuously capturing and retaining detailed Entra ID state information, the service enables organizations to:

- Visualize security posture
  - View a security score summarizing the current risk level of the Entra environment
  - Receive prioritized recommendations for hardening configurations based on observed changes and best practices

- Audit and compliance validation
  - Analyze historical login and sign-in logs to detect anomalies, unauthorized access attempts, and MFA policy gaps
  - Cross-reference configuration changes against internal governance policies or external compliance frameworks
  - Export audit-ready reports for regulatory or internal review

- Change-driven governance
  - Compare current and previous backups to identify new, modified, or deleted security objects, policies, or role assignments
  - Detect and respond to high-risk changes such as removal of Conditional Access rules or addition of excessive admin privileges
  - Use object-level history to track when and by whom key security settings were altered

- Integrated operational view
  - Access all governance and security insights directly in the same portal used for backup and restore operations
  - Link directly from findings to Microsoft Entra admin actions, allowing quick remediation of identified issues

By combining immutable backup data with built-in analysis and reporting features, the service provides both the forensic depth needed for incident investigations and the day-to-day visibility required for ongoing governance.

Backup data security

- All data encrypted in transit and at rest with AES-256 encryption
- TLS 1.2+ enforced for all communications
- Immutable storage ensures backups cannot be altered or deleted within the retention period
- Logical air-gapping prevents direct access to the backup repository from production systems
- Segregation of duties so that no single account or role can both access backup data and control restore operations
- Hosted in IBM Cloud Tier-3+ data centers with ISO 27001, ISO 27017, ISO 27018, SOC 1 Type 2, SOC 2 Type 2, SOC 3 certifications
- Full compliance with GDPR for EU-hosted environments

Flexible backup and retention

- Automated incremental backups as frequently as every hour
- Retention options from a day to unlimited
- Automatic enforcement of retention expiry with verified deletion

Performance and reliability

- Redundant infrastructure in IBM Cloud to ensure high availability
- Backup job health monitoring with configurable alerts
- Designed for minimal API throttling impact on Microsoft Entra ID

3.15. Extended disaster recovery with Anycloud Backup for Microsoft 365

When combined with Anycloud Backup for Microsoft 365, organizations gain a complete disaster recovery solution that covers both the Microsoft Entra ID identity layer and the full breadth of Microsoft 365 content. This combined capability allows rapid restoration of:

- User accounts, security groups, roles, and identity-related policies from Entra ID
- Emails, calendars, contacts, and tasks from Exchange Online
- SharePoint sites, OneDrive for Business content, and Microsoft Teams data including channels, files, and conversations
- Security and compliance settings across the Microsoft 365 tenant

This integrated approach ensures that in the event of a cyberattack, accidental deletion, configuration corruption, or large-scale service outage, both identity services and business-critical collaboration content can be recovered in a coordinated and efficient manner. Recovery operations can be executed in parallel to reduce downtime, ensuring that users regain both access credentials and the associated productivity tools as quickly as possible.

By maintaining separate but synchronized backup sets for identity and content, the combined solution delivers a layered defense against operational disruption, data loss, and compliance breaches, enabling organizations to meet stringent RTO and RPO targets across their Microsoft cloud environment.

Terms and termination

Pricing model & seat licenses

Anycloud Backup for Entra ID is available as a standalone service or as part of a bundle with Anycloud Backup for Microsoft 365. Licensing and pricing are defined in the EULA. Please refer to the current EULA for applicable terms.

Service levels & support

Availability

Anycloud Backup for Entra ID ("the solution") shall be available 99.9 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 shall mean the total amount of hours in the previous calendar month period, where the service has been available for the partner.

Total time shall mean the total amount of hours in the previous calendar month period.

Planned downtime shall mean the number of hours in the previous calendar month, where the service has not been available for the partner due to planned services and maintenance in accordance with 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 Anycloud's subcontractors), and which are outside of the control of Anycloud.
- Faults, deviations, delays, changes, or similar events caused by the customer or on the customers equipment which communicates with the Anycloud's 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 Anycloud or its sub-contractors.

Service and maintenance

Anycloud shall, always, be entitled to carry out planned service, repair, and maintenance of the solution. All such work is announced on the following link: https://status.anycloud.dk/. Anycloud 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 wants to change, amend, or upgrade the solution, the partner shall submit a written request to Anycloud. Anycloud shall carry out the requested change within a period of fifteen (15) working days after the receipt of the request, unless Anycloud, at its discretion, prior hereto notifies the partner that the requested changes cannot be made. Anycloud shall pay for the changed services in accordance with Anycloud's price list, always. The time used by Anycloud 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 Anycloud, assist Anycloud where reasonably possible with error tracing and diagnostics related to Incidents the Partner has reported.

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

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

Re-establishment Time

Re-establishment time means the time, which it takes for Anycloud 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. Anycloud shall, however, aim at re-establishing customer data within 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

***For ANZ, the targeted response time for P1, P2 and P3 are 2,4 and 8 business hours:**

Re-establishment Time

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

Standard support is delivered during normal working hours which are Monday–Friday, 8am to 4pm CET for countries in EMEA region. Extended support offerings are available.

Support hours

Standard support is delivered during normal working hours which are Monday-Friday, 8am to 4pm CET for countries in EMEA region. Extended support offerings are available.

Customer obligations

To access the service, the customer must provide connection details to their Microsoft 365 Entra ID 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.

Combining Anycloud Backup for Microsoft 365 and Entra ID

Anycloud Backup for Entra ID and Anycloud Backup for Microsoft 365 are complementary services that, when combined, provide organizations with complete coverage of both identity and collaboration data within the Microsoft cloud ecosystem.

Where Anycloud Backup for Microsoft 365 focuses on protecting productivity data – such as emails, files, Teams conversations, and SharePoint sites – Anycloud Backup for Entra ID safeguards the core identity and access infrastructure behind it. This includes users, groups, administrative roles, application registrations, conditional access policies, and audit logs.

Combining the two services creates a powerful duo including:

- Operational continuity: Organizations can quickly recover both collaboration content and identity configurations after accidental deletions or cyberattacks.

- Compliance coverage: Regulatory requirements like GDPR and DORA demand control over both user data and identity logs. The combination ensures full retention and restore capabilities across all Microsoft 365 services and Entra ID.

- Unified management: Both services are managed through dedicated portals with similar interfaces and cloud-to-cloud architectures, allowing IT administrators to operate efficiently across identity and content recovery.

- Enhanced security: Backup data from both services is encrypted, air-gapped, and stored in IBM Cloud data centers – isolated from the production environment and Microsoft's infrastructure.

By deploying both services together, organizations ensure that their collaboration data and access control infrastructure are equally protected – delivering true end-to-end resilience across the Microsoft cloud.

Document references

End user License Agreement Bundle

End user License Agreement standalone

Fair Usage Policy

Service status & maintenance announcements

LET'S STAY CONNECTED

Anycloud A/S
Hedegaardsvej 88
2300 Copenhagen S
Denmark

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

any.cloud