CANCOM

Service Level Agreement

(Service Description)

M365 Backup as a Service

Code: FS-C-M365B
Version: 3.0
Valid from 01.01.2025

Service of the contractor

This document describes the services of the service module, which are provided as part of the contract concluded between the client (CL) and the contractor (CO). The responsibilities of the services described are based on a RACI model. Explanations of terms and contact information for the Customer Service Center can be found under the following link.

Unless otherwise agreed, the following service goals apply as standard: Service time "SNAZ" (NWH) with a response time of 4 hours.

M365 Backup-as-a-Service

M365 Backup as a Service for a secure offsite backup of your Microsoft Office 365 data.

Initial Services	CO	CL
Setting up authentication from the "M365 Backup as a Service" service to Office 365 in the client's environment	R/A	C/I
Setting up backup jobs	R/A	C/I
Setting up Entra ID Backup	R/A	C/I
Installation of the "Veeam Backup & Replication" server (if not available) on the infrastructure provided by the client	R/A	C/I
Installation of Veeam Explorer	R/A	C/I
Setting up authentication for the "M365 Backup as a Service" service	R/A	C/I
Setting up Restore Portal	R/A	C/I
Restore test	R/A	C/I
Training for administrators, documentation	R/A	C/I
Setting up Immutable Backup Storage	R/A	C/I
Setting up a second backup storage location (Backup Copy)	R/A	C/I

Recurring Services	CO	CL
Provision of shared infrastructure including Veeam Backup for O365 licenses		
The contractor provides the client with a shared infrastructure and the associated "Veeam Backup for Office 365" license for M365 Backup. In particular, this is used to back up Microsoft Exchange, SharePoint, OneDrive for Business and Teams.	R/A	C/I

The backup data is stored on an object storage in a data center in the "EU West" region. The client is responsible for restoring changed or deleted data using the Veeam Explorer provided.		
System security of the shared infrastructure		
EWS mechanisms are used to secure the data. This means that exactly the same mechanism is used when an email is downloaded from the O365 server to your local computer/Outlook. The downloaded data is therefore encrypted using TLS. Servers are integrated into the virus protection management of Microsoft Azure Security Center. Contractor services are used to monitor the shared infrastructure, and alarms are forwarded directly to the contractor.	R/A	C/I
Troubleshooting shared infrastructure issues		
The malfunctions (errors or defects) in the backup infrastructure reported by the client or identified by the contractor are analyzed, processed and remedied by the contractor. The contractor sets up monitoring for proactive alerting. In the event of software errors, the contractor checks whether the respective manufacturer provides software updates or hotfixes that resolve the error. These software packages available from the manufacturer are implemented in the system and it is checked whether the error has been resolved. The contractor backs up the operating system as part of the service module and, in the event of an error, will restore data that may contain data that is up to one calendar day old. In the event of malfunctions, faulty system files or application files in system directories are restored. If restoration is not possible because a block is present by the running application or application services, the client is informed. If several system files are defective or there are other compelling reasons (e.g. in the event of a virus attack, they cannot be cleaned up), the contractor will re-implement the operating system of the affected server. Since this is associated with the loss of data in the applications (installations) installed by the client, this will be agreed with the client. If a server restart is necessary in the event of a malfunctions, this will be carried out without prior agreement. If it is not possible to rectify errors and faults immediately, the contractor will endeavor to minimize the effects of the malfunctions using a workaround. The rectification of malfunctions in the "Veeam Backup and Replication Server" at the client's site is not included, but can be carried out at the expense of the effort involved and for a separate invoice.	R/A	C/I
Regular implementation of patches, hotfixes and security updates		
The contractor carries out patch management for the operating system and the Veeam application. This includes the installation of security updates and required critical updates on the virtual server systems according to the contractor's standard specifications.	R/A	C/I

Entra ID Backup		
The contractor performs a daily backup (every 24 hours) of the Entra ID objects in accordance with the functional scope of the "Veeam Backup and Replication" product in the version used by the contractor. No exclusions of the Entra ID objects to be backed up can be defined. In the event that a restore of the Entra ID data is required, the client must contact the contractor via a support ticket. The cost of the restore will be invoiced to the client separately based on the actual effort involved.	R/A	C/I
Immutable Backup Storage		
The contractor will set up a backup storage location that cannot be changed over time. The lock-in period corresponds to the retention periods specified by the customer during onboarding. Important: This option can only be selected during the initial onboarding process for this service and cannot be added later.	R/A	C/I
Second backup storage (Backup Copy)		
The contractor sets up an additional backup storage location alongside the primary backup storage. Data is always copied to this additional storage location after a backup is performed. The retention period for the backup copy is the same as for the primary backup. This backup copy option increases (doubles) the required backup resources (TB).	R/A	C/I

Obligation of the client to cooperate	CO	CL
Deployment of Veeam Backup and Replication Server - When using the local Restore application		
The client provides a "Veeam Backup and Replication Server". The server must meet Veeam's minimum requirements (see also Veeam Technical Documentation): • 4 CPU cores, • 8GB RAM, • 30 GB HDD, • Windows 64-bit version supported by Microsoft The necessary "Veeam Backup and Replication Server", if not already available, can be made available as a free community edition	C/I	R/A
Setting up Entra ID Backup		
When setting up the Entra ID backup, the client must enable the contractor to log in via a global administrator of the client during a remote session.	C/I	R/A
Backup Defaults		
The functions and restrictions of the currently used version of the "Veeam Backup for Office365" software apply.	C/I	R/A

The contractor's default backup settings are as follows: • Daily incremental backup • Entire M365 organization (mailboxes, Sharepint, OneDrive, and teams) Retention periods must be specified by the client during onboarding (default = 90 days)		
Backup Control		
Backup control on the client's side is always the responsibility of the client. It is recommended that the client regularly checks the system configuration (e.g. permissions of the service account, problems with paths or certificates) and the planned backup runs. The contractor's support in analyzing error messages and taking necessary measures is based on the effort involved, which is billed separately at the applicable hourly rate.	C/I	R/A
Veeam Backup & Replication Server Compatibility		
The client is responsible for the compatibility of the Veeam Backup & Replication Server on site with the infrastructure provided by the contractor. The contractor will proactively inform the client about version changes.	C/I	R/A

Framework conditions for service

The functions and limitations of the currently used version of the "Veeam Backup for Office365" software apply.
Change requests will be invoiced based on the client's detailed requirements and based on the actual effort at the applicable hourly rate.
Expenses for support for the restoration of modified or deleted data by the Contractor will be charged separately according to the actual expenditure at the applicable hourly rate.
Regular, necessary maintenance work on the infrastructure can lead to minor outages. The client will be proactively informed about quarterly maintenance windows of around 8 hours during which the service will not be available or will only be available to a very limited extent.
As part of the service module, the contractor carries out regular checks of the configured and planned backup runs. Error messages are analyzed, and necessary measures are developed and initiated.
At the end of the contractual relationship, the client's data will be deleted by the contractor within one month. If requested, the client's existing data can be copied to media and handed over for a fee before deletion.

Services not included

Configuration work on the client's firewall for the connection
Dedicated data lines (WAN connections) from and to the client

Setting up new functionalities
Preparing security reports
Reports with security-relevant information from the logs
Evaluation of the network environment and analysis of application performance (end-to-end monitoring)
Export of media/backup tapes
Regular restore tests in the client's environment
Backup control, analysis and diagnosis of the backup log (on the client's side)
For monitoring and alerting the Veeam Backup and Replication server at the client's site
Backup of client applications that are not serviced by the contractor as a service provider
Client-side work (maintenance, firmware updates, configurations...)
Integrating additional applications or changes into the backup system after initial setup
Restoration of system data or individual files
Backup of hybrid environments
Additional costs incurred by Microsoft when backing up Teams chats and Teams channel chats using the Microsoft Graph API (as Microsoft charges fees for API usage). These fees are charged by Microsoft per tenant and per message.
Additional acceptance tests besides the primary backup storage
With the Backup Copy option, the required backup resources (TB) are included in the total backup storage and are not shown separately.

FS-C-M365B – Version 3.0