



Service Level Agreement (Leistungsbeschreibung) **M365 Backup as a Service**

Code: FS-C-M365B
Version: 3.0
Gültig ab 01.01.2025

CANCOM Austria AG // Wienerbergstraße 53 // 1120 Wien // Österreich // T +43 50 822 0 // info@cancom.com

HG Wien FN 178368g // Firmensitz Wien // UID ATU46276408 // InterzeroNr. 155219

Raiffeisenlandesbank Oberösterreich // BIC: RZOOAT2L // IBAN: AT35 3400 0000 0009 7899 // Creditor-ID: AT17ZZZ00000029797

www.cancom.at

Leistungen des Auftragnehmers

Dieses Dokument beschreibt die Serviceleistungen des Servicemoduls, welche im Rahmen des zwischen dem Auftraggeber und Auftragnehmer abgeschlossenen Vertrages erbracht wird.

Die Verantwortlichkeiten der beschriebenen Leistungen sind auf Basis eines RACI-Modells abgebildet.

Begriffserklärungen sowie Kontakt Informationen des Customer Service Center sind unter folgendem [Link](#) zu finden.

Sofern nichts Gegenteiliges vereinbart ist, gelten standardmäßig folgende Serviceziele: Servicezeit „SNAZ“ mit einer Reaktionszeit von 4 Stunden.

M365 Backup as a Service

M365 Backup as a Service für ein sicheres Offsite Backup Ihrer Microsoft Office 365-Daten.

Initiale Leistungen	AN	AG
Einrichtung der Authentifizierung vom Service "M365 Backup as a Service" zu Office 365 in der Umgebung des Auftraggebers	R/A	C/I
Einrichtung der Backup-Jobs	R/A	C/I
Einrichtung Entra ID Backup	R/A	C/I
Installation des "Veeam Backup & Replication"-Servers (wenn nicht vorhanden) auf der vom Auftraggeber bereitgestellten Infrastruktur	R/A	C/I
Installation des Veeam Explorers	R/A	C/I
Einrichtung der Authentifizierung zum Service "M365 Backup as a Service"	R/A	C/I
Einrichtung Restore Portal	R/A	C/I
Restore-Test	R/A	C/I
Schulung für Administratoren, Dokumentation	R/A	C/I
Einrichtung Immutable Backup Speicher	R/A	C/I
Einrichtung zweiter Backup Speicher (Backup Copy)	R/A	C/I

Wiederkehrende Leistungen	AN	AG
Bereitstellung Shared Infrastruktur inkl. der Veeam Backup für O365 Lizenzen		
Der Auftragnehmer stellt dem Auftraggeber eine Shared Infrastruktur sowie die dazugehörige „Veeam Backup for Office 365“ Lizenz für M365 Backup zu Verfügung. Im Speziellen werden damit Microsoft Exchange, SharePoint, OneDrive for Business und Teams gesichert. Die Backupdaten werden in einem Rechenzentrum in der „Region EU-West“ auf einem Object Storage gespeichert.	R/A	C/I

Das Restore von veränderten oder gelöschten Daten über den zur Verfügung gestellten Veeam Explorer obliegt dem Auftraggeber.		
System Sicherheit der Shared Infrastruktur		
Es werden EWS- Mechanismen zur Sicherung der Daten verwendet. Das bedeutet, dass genau der gleiche Mechanismus zum Einsatz kommt, wenn eine E-Mail vom O365-Server auf Ihren lokalen Computer/ Outlook heruntergeladen wird. Die heruntergeladenen Daten werden also durch die Verwendung von TLS verschlüsselt. Server sind in das Virenschutz Management von Microsoft Azure Security Center eingebunden. Für das Monitoring der Shared Infrastruktur werden Services des Auftragnehmers verwendet, Alarmer werden direkt an den Auftragnehmer weitergeleitet.	R/A	C/I
Behebung von Störungen an der Shared Infrastruktur		
Die vom Auftraggeber gemeldeten oder von Auftragnehmer erkannten Störungen (Fehler oder Mängel) der Backupinfrastruktur, werden durch den Auftragnehmer analysiert, bearbeitet und behoben. Seitens des Auftragnehmers wird ein Monitoring zum proaktiven Alerting eingerichtet. Der Auftragnehmer prüft bei Softwarefehlern, ob vom jeweiligen Hersteller Software Updates oder Hotfixes zur Verfügung gestellt werden, welche den Fehler beheben. Diese vom Hersteller verfügbaren Softwarepakete werden im System implementiert und es wird geprüft, ob der Fehler behoben ist. Der Auftragnehmer führt im Rahmen des Servicemoduls die Sicherung des Betriebssystems durch und wird im Fehlerfall jene Daten wiederherstellen, welche einen bis zu einem Kalendertag alten Datenbestand enthalten können. Bei Störungen werden fehlerhafte Systemdateien oder Dateien von Applikationen in Systemverzeichnissen wiederhergestellt. Ist die Wiederherstellung nicht möglich, da eine Sperre durch die laufende Applikation oder durch Applikationsdienste gegeben ist, so wird der Auftraggeber informiert. Sind mehrere Systemdateien defekt oder bestehen andere zwingende Gründe (z.B. im Falle eines Virenbefalls kann nicht bereinigt werden), so wird vom Auftragnehmer das Betriebssystem des betroffenen Servers neu implementiert. Da dies mit Verlust von Daten bei den vom Auftraggeber installierten Applikationen (Installationen) verbunden ist, wird dies mit dem Auftraggeber abgestimmt. Ist im Störungsfalle ein Neustart des Servers notwendig, so wird dieser ohne Absprache durchgeführt. Sollte eine sofortige Behebung von Fehlern und Störungen nicht möglich sein, ist der Auftragnehmer bestrebt, mithilfe eines Workarounds die Auswirkungen der Störung zu minimieren. Die Behebung von Störungen des „Veeam Backup und Replication Servers“ beim Auftraggeber vor Ort ist nicht inkludiert, kann aber gerne nach Aufwand gegen gesonderte Verrechnung durchgeführt werden.	R/A	C/I
Regelmäßige Durchführung von Patches, Hotfixes und Security-Updates		
Der Auftragnehmer führt das Patch-Management für das Betriebssystem und die Veeam Applikation durch. Dies beinhaltet die Installation von Security-Updates und erforderlichen kritischen Updates auf den virtuellen Serversystemen nach Standardvorgaben des Auftragnehmers.	R/A	C/I

Entra ID Backup		
Der Auftragnehmer führt ein tägliches Backup (alle 24 Stunden) der Entra ID Objekte durch, laut Funktionsumfangs des Produktes „Veeam Backup und Replikation“ in der jeweils eingesetzten Version des Auftragnehmers. Es können keine Exklusions der zu sichernden Entra ID Objekte definiert werden. Im Fall eines benötigten Restore der Entra ID Daten, muss der Auftraggeber den Auftragnehmer über ein Supportticket kontaktieren, der Aufwand des Restore wird dem Auftraggeber nach tatsächlichem Aufwand gesondert in Rechnung gestellt.	R/A	C/I
Immutable Backup Speicher		
Der Auftragnehmer richtet einen zeitlich unveränderbaren Backupspeicher ein. Die Sperrzeit entspricht der vom Kunden beim Onboarding genannten Aufbewahrungsfristen. Wichtig: Diese Option kann nur beim initialen Onboarding zu diesem Service gewählt werden und <u>nicht nachträglich erweitert werden</u>.	R/A	C/I
Zweiter Backup Speicher (Backup Copy)		
Der Auftragnehmer richtet zum Primären Backup Speicher einen zusätzlichen Backupspeicher ein. Die Daten werden immer nach durchgeführten Backup auf den zusätzlichen Speicher kopiert. Die Aufbewahrungsfrist der Backup Copy entspricht der Aufbewahrungsfrist des Primären Backup. Diese Option der Backup Copy erhöht (verdoppelt) die benötigten Backup Ressourcen (TB).	R/A	C/I

Mitwirkungspflichten des Auftraggebers	AN	AG
Bereitstellung Veeam Backup und Replication Server - Bei Nutzung der lokalen Restore Applikation		
Der Auftraggeber stellt einen „Veeam Backup und Replication Server“ zur Verfügung. Der Server muss die Mindestanforderung seitens Veeam erfüllen (siehe auch Veeam Technical Documentation): • 4 CPU Cores, • 8GB RAM, • 30 GB HDD, • von Microsoft supportete Windows 64-bit Version Der notwendige „Veeam Backup und Replication Server“, falls nicht schon vorhanden, kann als kostenfreie Community Edition zur Verfügung gestellt werden	C/I	R/A
Einrichtung des Entra ID Backup		
Der Auftraggeber muss bei der Einrichtung des Entra ID Backups dem Auftragnehmer die Anmeldung durch einen Globalen Administrator des Auftraggebers im zuge einer Remote Session ermöglichen.	C/I	R/A
Backup Defaults		
Es gelten die Funktionen bzw. Einschränkungen der aktuell eingesetzten Version der Software „Veeam Backup für Office365“.	C/I	R/A

Die Default Backup Einstellungen des Auftragnehmers sind wie folgt: • Tägliches Inkrementell Backup • Gesamte M365 Organisation (Mailboxen, Sharepoint, OneDrive, und Teams) Aufbewahrungsfristen sind vom Auftraggeber beim Onboarding anzugeben (Default = 90 Tage)		
Backup Kontrolle		
Die Backup Kontrolle auf Seite des Auftraggebers obliegt immer dem Auftraggeber. Es ist empfohlen, dass der Auftraggeber eine regelmäßige Kontrolle der Systemkonfiguration (z.B. Berechtigungen des Service-Accounts, Probleme bei Pfaden oder Zertifikaten) und der geplanten Sicherungsläufe durchführt. Die Unterstützung durch den Auftragnehmer bei der Analyse von Fehlermeldungen sowie das Treffen von notwendigen Maßnahmen erfolgt nach Aufwand, welcher gesondert zum gültigen Stundensatz verrechnet wird.	C/I	R/A
Kompatibilität des Veeam Backup & Replication Server		
Der Auftraggeber ist für die Kompatibilität des Veeam Backup & Replication Server bei ihm vor Ort mit der vom Auftragnehmer zur Verfügung gestellten Infrastruktur verantwortlich. Der Auftragnehmer informiert den Auftraggeber proaktiv über Versionsänderungen.	C/I	R/A

Rahmenbedingungen für die Leistungserbringung
Es gelten die Funktionen bzw. Einschränkungen der aktuell eingesetzten Version der Software „Veeam Backup für Office365“.
Change Requests werden auf Basis detaillierten Anforderungen des Auftraggebers nach tatsächlichem Aufwand zum gültigen Stundensatz verrechnet.
Aufwände für Support-Unterstützung für das Restore von veränderten oder gelöschten Daten durch den Auftragnehmer werden nach tatsächlichem Aufwand zum gültigen Stundensatz gesondert verrechnet.
Regelmäßige notwendige Wartungsarbeiten an der Infrastruktur können zu kleineren Ausfällen führen. Der Auftraggeber wird über quartalsmäßige Wartungsfenster im Ausmaß von ca. 8 Stunden proaktiv informiert, an denen das Service nicht oder nur sehr eingeschränkt zur Verfügung steht.
Der Auftragnehmer führt im Rahmen des Servicemoduls eine regelmäßige Kontrolle der konfigurierten und geplanten Sicherungsläufe durch. Fehlermeldungen werden analysiert, notwendige Maßnahmen erarbeitet und eingeleitet.
Bei Ende des Vertragsverhältnisses wird die Löschung der Daten des Auftraggebers durch den Auftragnehmer innerhalb eines Monats durchgeführt. Auf Wunsch können vor der Löschung die bestehenden Daten des Auftraggebers kostenpflichtig auf Medien kopiert und übergeben werden.

Nicht enthaltene Leistungen
Konfigurationsarbeiten der Auftraggeber-Firewall für die Anbindung
Dedizierte Datenleitungen (WAN-Anbindungen) vom und zum Auftraggeber

Einrichten von neuen Funktionalitäten
Anfertigen von Security-Berichten
Reports mit sicherheitsrelevanten Informationen aus den Logs
Auswertung der Netzwerkumgebung und Analyse der Applikationsperformance (End-to-End-Monitoring)
Export von Medien/Backup-Bändern
Regelmäßige Restore-Tests in der Umgebung des Auftraggebers
Backup-Kontrolle, Analyse und Diagnose des Backup-Logs (Auf Seite des Auftraggebers)
Für das Monitoring und Alerting des Veeam Backup and Replicationsserver beim Auftraggeber
Sicherung von Applikationen des Auftraggebers die nicht vom Auftragnehmer als Dienstleister serviert werden
Auftraggeberseitige Arbeiten (Wartungen, Firmware update, Konfigurationen...)
Einbinden von zusätzlichen Applikationen oder Änderungen in das Backup-System nach erstmaliger Einrichtung
Wiederherstellung von Systemdaten oder einzelner Dateien
Backup von hybriden Umgebungen
Anfallende Zusatzkosten durch Microsoft beim Backup von Teams Chats und Teams Channel-Chats durch die Verwendung der Microsoft Graph API (da Microsoft Gebühren für die API-Nutzung erhebt) . Diese Gebühren werden durch Microsoft pro Tenant (Mandant) und pro Nachricht eingehoben.
Weitere Abnahmetest zusätzlich zum Primären Backupspeicher
Bei der Option Backup Copy werden die benötigten Backup Ressourcen (TB) im gesamt Backupspeicher inkludiert und nicht gesondert ausgewiesen.

