



Service Level Agreement

(Leistungsbeschreibung)

Secure-Offsite Backup as a Service

Code: FS-C-SOB

Version: 3.0

Gültig ab 01.01.2025

Leistungen des Auftragnehmers

Dieses Dokument beschreibt die Serviceleistungen des Servicemoduls, welche im Rahmen des zwischen dem Auftraggeber (AG) und Auftragnehmer (AN) 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“ (NWH) mit einer Reaktionszeit von 4 Stunden.

Secure-Offsite Backup as a Service

Mit diesem Service erhalten Siemittels Veeam Cloud Connect eine zusätzliche Backupkopie an einem externen Speicherort.

Initiale Leistungen	AN	AG
Onboarding in die durch den Auftragnehmer bereitgestellte Shared Infrastruktur für dieses Service	R/A	C/I
Einrichtung der Authentifizierung vom Service "Secure Offsite Backup as a Service" in der Umgebung des Auftraggebers	R/A	C/I
Herstellung der Verbindung zum "Secure Offsite Backup as a Service"	R/A	C/I
Einrichtung eines Backup-Jobs für einen Server	R/A	C/I
Restore-Test	R/A	C/I
Einführung für Administratoren in das Service "Secure Offsite Backup as a Service"	R/A	C/I

Wiederkehrende Leistungen	AN	AG
Bereitstellung Shared Infrastruktur inkl. der Veeam Cloud Connect Lizenzen		
Der Auftragnehmer stellt dem Auftraggeber eine Shared Infrastruktur und sofern benötigt die dazugehörigen „Veeam Cloud Connect“ Lizenzen für Veeam Backup & Replication zur Verfügung. Dazu übermittelt der Auftragnehmer dem Auftraggeber die entsprechenden Informationen (wie IP-Adresse und Port Nummer) damit beim Auftragnehmer das Cloud-Repository in seinem Backup & Replication Portal vor Ort eingerichtet werden kann. Optional stellt der Auftragnehmer dem Auftraggeber die Veeam Cloud Connect Funktionalität „Insider Protection“ bereit. Durch Aktivierung dieser Funktionalität wird, wenn das Backup oder spezifische Wiederherstellungspunkte in der Backup Kette vom Cloud Repository gelöscht werden, von Veeam Backup & Replication nicht sofort gelöscht, sondern in den "Papierkorb" verschoben. In diesem Bereich verbleiben die Daten für den vom Auftraggeber vorgegebenem Zeitraum von x-Tagen. Backup Daten im „Papierkorb“ beeinflussen die Backup Quota nicht, es wird jedoch Speicherplatz benötigt, die dem Auftraggeber zusätzlich in Rechnung gestellt werden.	R/A	C/I

Diese Funktionalität unterliegt den Voraussetzungen von Veeam Backup & Replication für Insider Protection. Das Restore von veränderten oder gelöschten Daten obliegt dem Auftraggeber. Der Auftragnehmer kann den Auftraggeber bei einem Restore nach gesonderter Beauftragung unterstützen. Die Verrechnung erfolgt nach tatsächlichem Aufwand zum gültigen Stundensatz.		
System Sicherheit der Shared Infrastruktur		
Die Infrastruktur ist in einem Rechenzentrum in Österreich das nach international anerkannten Informationssicherheitsnorm ISO/IEC 27001 zertifiziert ist, untergebracht. Das Rechenzentrum weist die Einhaltung der Normvorgaben im Hinblick auf die Implementierung eines Information Security Management Systems (ISMS) auf. Die Internet Verbindung zur Backup Infrastruktur wird durch eine redundant angebundene Firewall abgesichert. Ein Zertifikat wird vom Auftragnehmer zur Verfügung gestellt, mit dem die Verbindung eingerichtet wird. Die Datenübertragung vom Veeam Backup Repository in das Rechenzentrum erfolgt verschlüsselt mit SSL. Die Backup Infrastruktur ist in sich redundant ausgelegt. Für das Monitoring der Shared Infrastruktur werden Services des Auftragnehmers verwendet, Alarme werden direkt an den Auftraggeber 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 von den Betriebssystemen der Shared Infrastruktur durch und wird im Fehlerfall jene Betriebssystem-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.	R/A	C/I

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 Komponenten“ beim Auftraggeber vor Ort ist nicht inkludiert, kann aber gerne nach Aufwand gegen gesonderte Verrechnung durchgeführt werden.		
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. Regelmäßige notwendige Wartungsarbeiten an der Infrastruktur können zu kleineren Ausfällen führen. Der Auftraggeber wird über Wartungsfenster im Ausmaß von ca. 8 Stunden proaktiv informiert, an denen der Service nicht oder nur sehr eingeschränkt zur Verfügung steht. Vorgehen bei Notfallwartungsmaßnahmen (Ungeplante Wartungsfenster): Unter ungeplanten Wartungsfenstern versteht der Auftragnehmer Unterbrechungen von Servicezeiten, welche durch Notfallwartungsmaßnahmen hervorgerufen werden. Diese Maßnahmen sind zur Vermeidung von unvorhersehbaren Ausfällen von Services oder Servicekomponenten notwendig. Die Notfallwartungsmaßnahmen werden dem Auftraggeber mitgeteilt und unabhängig von den definierten Wartungsfenstern durchgeführt.	R/A	C/I
WAN Accelerator		
Der Auftragnehmer stellt auf Wunsch des Auftraggebers die Veeam Cloud Connect Funktionalität „WAN Accelerator“ zur Verfügung. Durch Aktivierung dieser Funktionalität wird die Datenübertragung optimiert und speziell bei einer Internetverbindung mit geringer Bandbreite wesentlich verbessert. Diese Funktionalität unterliegt den Voraussetzungen von Veeam Backup & Replication für WAN Accelerator, insbesondere der korrekten Veeam Backup & Replication Edition.	R/A	C/I

Mitwirkungspflichten des Auftraggebers	AN	AG
System Mindestanforderungen		
Der Veeam Backup und Replication Server muss die Mindestanforderung seitens Veeam erfüllen (siehe auch Veeam Technical Dokumentation).	R/A	C/I
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. Um die volle Funktion des Services zu gewährleisten, muss beim Auftraggeber die gleiche Version wie beim Auftragnehmer installiert sein.	R/A	C/I

Backup Kontrolle		
Die Backup- bzw. Backup Copy-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 Zertifikatsprobleme) und der geplanten Sicherungs- und Kopieläufe durchführt. Die Unterstützung durch den Auftraggeber bei der Analyse von Fehlermeldungen sowie das Treffen von notwendigen Maßnahmen erfolgt nach Aufwand, welcher gesondert zum gültigen Stundensatz verrechnet wird.	R/A	C/I

Rahmenbedingungen für die Leistungserbringung
Der Auftraggeber verfügt über eine umfassende Veeam Backup und Replication Infrastruktur, die alle für die Erbringung des Services erforderlichen Rollen beinhaltet.
Der Auftraggeber verfügt über eine entsprechende Internetanbindung, um das Service zu nutzen. Die Internetanbindung und die Internetverbindung ist nicht Teil dieses Services und liegt im Verantwortungsbereich des Auftraggebers.
Optional kann das Initial Backup (Initial Seeding) vor Ort beim Auftraggeber durchgeführt werden. Dazu wird das Initial Backup auf einem Datenträger, welchen der Auftragnehmer zur Verfügung stellt, durchgeführt. Dieses Initial Backup wird danach in die Shared Infrastruktur des Auftragnehmers eingespielt. Voraussetzung sind die erfüllten technischen Voraussetzungen beim Auftraggeber vor Ort. Dieses Service und eventuell notwendige Komponenten werden dem Auftraggeber nach tatsächlichem Aufwand gesondert in Rechnung gestellt.
Optional kann dem Auftraggeber im Disaster Recovery Fall die Backupdaten des Auftraggebers oder Teile davon, die auf der Shared Infrastruktur zur Verfügung stehen, auf einem Datenträger, welchen der Auftragnehmer bereitstellt, kopiert und dem Auftraggeber zur Verfügung gestellt werden. Dieses Service wird dem Auftraggeber nach tatsächlichem Aufwand in Rechnung gestellt.
Change Requests werden auf Basis detaillierten Anforderungen des Auftraggebers nach tatsächlichem Aufwand gesondert 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.
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.
Es ist erforderlich die beim Onboarding benötigten Verbindungen für den SSL Zertifikats Status Check dauerhaft zu gewährleisten.

Nicht enthaltene Leistungen
Konfigurationsarbeiten der Auftraggeber-Firewall für die Anbindung

Dedizierte Datenleitungen (WAN-Anbindungen) vom und zum Auftraggeber
Einrichten von neuen Funktionalitäten (Features)
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
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

