Service Level Agreement

(Service Description)

Secure-Offsite Backup as a Service

Code: FS-C-SOB
Version: 3.0
Valid from 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

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.

Secure-Offsite Backup as a Service

With this service, you receive an additional backup copy in an external storage location via Veeam Cloud Connect.

Initial Services	CO	CL
Onboarding to the shared infrastructure provided by CANCOM for this service	R/A	C/I
Setting up the authentication of the CANCOM service "Secure Offsite Backup as a Service" in the customer's environment	R/A	C/I
Establishing the connection to "Secure Offsite Backup as a Service"	R/A	C/I
Setting up a backup job for a server	R/A	C/I
Restore test	R/A	C/I
Introduction for administrators to the service "Secure Offsite Backup as a Service"	R/A	C/I

Recurring Services	CO	CL
Provision of shared infrastructure including Veeam Cloud Connect licenses		
The contractor provides the client with a shared infrastructure and, if required, the associated "Veeam Cloud Connect" licenses for Veeam Backup & Replication. To do this, the contractor provides the client with the relevant information (such as IP address and port number) so that the cloud repository can be set up on site in the contractor's Backup & Replication portal. Optionally, the contractor provides the client with the Veeam Cloud Connect "Insider Protection" functionality. By activating this functionality, if the backup or specific recovery points in the backup chain are deleted from the cloud repository, Veeam Backup & Replication will not delete them immediately, but will move them to the "trash can". The data will remain in this area for the period of x days specified by the client. Backup data in the "trash can" does not affect the backup quota, but storage space is required, which will be billed to the client additionally. This functionality is subject to the Veeam Backup & Replication requirements for Insider Protection. The client is responsible for restoring changed or deleted data. The contractor can support the client with a restore after a separate order has been placed. Billing will be based on actual expenditure at the applicable hourly rate.	R/A	C/I
System security of the shared infrastructure		

The infrastructure is housed in a data center in Austria that is certified according to the internationally recognized information security standard ISO/IEC 27001. The data center complies with the standard requirements with regard to the implementation of an Information Security Management System (ISMS). The Internet connection to the backup infrastructure is secured by a redundant firewall. A certificate is provided by the contractor with which the connection is set up. The data transfer from the Veeam backup repository to the data center is encrypted with SSL. The backup infrastructure is designed to be redundant. The contractor's 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 correct the error. These software packages available from the manufacturer are implemented in the system and it is checked whether the error has been corrected. As part of the service module, the contractor backs up the operating systems of the shared infrastructure and, in the event of an error, will restore the operating system 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 done 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 Components" at the client's site is not included, but can be carried out at the expense of the effort and for a separate invoice.	R/A	C/I
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. Regular, necessary maintenance work on the infrastructure can lead to minor outages. The client is proactively informed about maintenance windows of around 8 hours during which the service is not available or only available to a very limited extent.	R/A	C/I

Procedure for emergency maintenance measures (unplanned maintenance windows): The contractor defines unplanned maintenance windows as interruptions to service times caused by emergency maintenance measures. These measures are necessary to avoid unforeseeable failures of services or service components. The emergency maintenance measures are communicated to the client and carried out independently of the defined maintenance windows.		
WAN Accelerator		
At the request of the client, the contractor will provide the Veeam Cloud Connect functionality "WAN Accelerator". By activating this functionality, data transfer is optimized and significantly improved, especially with an Internet connection with low bandwidth. This functionality is subject to the requirements of Veeam Backup & Replication for WAN Accelerator, in particular the correct Veeam Backup & Replication Edition.	R/A	C/I

Obligation of the client to cooperate	CO	CL
System minimum requirements		
The Veeam Backup and Replication Server must meet Veeam's minimum requirements (see also Veeam Technical Documentation).	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. To ensure the full functionality of the service, the client must have the same version installed as the contractor.	C/I	R/A
Backup Control		
The backup or backup copy 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. service account authorizations, path problems or certificate problems) and the planned backup and copy runs. The client'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

Framework conditions for service
The client has a comprehensive Veeam backup and replication infrastructure that includes all roles required to provide the service.
The client has an appropriate internet connection to use the service. The internet connection and internet connection are not part of this service and are the responsibility of the client.
Optionally, the initial backup (initial seeding) can be carried out on site at the client's premises. The initial backup is carried out on a data storage device provided by the contractor. This initial backup is then imported into the contractor's shared infrastructure. The prerequisite is that the technical requirements are met on site at the client's premises. This service and any necessary components will be invoiced to the client separately based on the actual effort involved.

Optionally, in the event of a disaster recovery, the client's backup data or parts thereof that are available on the shared infrastructure can be copied to a data storage device provided by the contractor and made available to the client. This service will be invoiced to the client based on the actual costs incurred.
Change requests will be invoiced separately at the applicable hourly rate based on the client’s detailed requirements and actual effort.
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.
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.
It is necessary to permanently ensure the connections required for the SSL certificate status check defined during onboarding.

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 (features)
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
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