



Service Level Agreement

(Service Description)

Azure Config Backup as a Service

Code: FS-AzCBaaS

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.

Azure Config Backup as a Service

With Azure Config Backup as a Service, the client can quickly get back on track after a security-relevant event.

Initial Services	CO	CL
Onboarding the desired number of subscriptions in our backend system	R/A	C/I
Carrying out a test backup	R/A	C/I
Transmission of information for a possible restore	R/A	C/I
Documentation	R/A	C/I

Recurring Services	CO	CL
Provision of shared infrastructure including service for securing configuration data		
The contractor provides the client with a shared infrastructure and an automated system with which the client's configuration is backed up. In particular, this backs up the most important configurations, but not data, of the existing Azure environment. For security reasons, access to the backed up files is currently not possible.	R/A	C/I
System security of the shared infrastructure		
Native Microsoft Service Connections are used to secure the data, so every backup is encrypted with TLS. Servers are integrated into the virus protection management of Microsoft Azure Security Center. Azure Native 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 backup infrastructure faults (errors or defects) reported by the client or identified by the contractor are analyzed, processed and resolved 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	R/A	C/I

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 faults, 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 will be 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 for the server. Since this involves loss of data and 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 fault, 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 fault using a workaround.		
Patches, hotfixes and security updates		
The contractor carries out patch management for the operating system. 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

Framework conditions for service
Change requests will be invoiced based on the client's detailed requirements and based on the actual effort at the applicable hourly rate.
The restoration of changed or deleted configurations is not part of the service and will be charged at the currently valid hourly rate.
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
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)
Regular restore tests in the client's environment
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
Option of data restore directly by the client.

