CANCOM

Service Level Agreement

(Service Description)

Data Resiliency Service

Code: MS-DRAAS
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.

Data Resiliency Service

The aim of using Data Resiliency Service (DRaaS) is to create an environment that enables reliable and rapid recovery in the event of a disaster.

Initial Services	CO	CL
Defining, setting up and testing remote maintenance access to the customer's systems	R/A	C/I
Installation and configuration of the Data Resiliency Service (VRO) on the provided hardware or virtual machine	R/A	C/I
Setting up and testing an exemplary recovery plan	R/A	C/I

Recurring Services	CO	CL
Checking the availability of new software packages and defining the updates to be installed		
Before the periodic updates are carried out, the contractor checks whether new software packages released by the manufacturer are available for the software solution used and checks the existing manufacturer documentation for these software packages (dependencies, corrected errors, manufacturer specifications, framework conditions and implementation instructions). The contractor informs the client about recommended updates to the Data Resiliency Service (DRaaS) solution.	R/A	C/I
Carrying out periodic updates of the Data Resiliency Service solution		
Before the periodic updates are carried out, the contractor checks whether new software packages released by the manufacturer are available for the software solution used and checks the existing manufacturer documentation for these software packages (dependencies, corrected errors, manufacturer specifications, framework conditions and implementation instructions). The contractor informs the client about recommended updates to the Data Resiliency Service solution.	R/A	C/I
Conducting periodic system checks of the Data Resiliency Service solution		
The agreed periodic system checks are coordinated by the contractor. The test dates are agreed with the client and carried out remotely.	R/A	C/I

The status of the systems and system components is checked according to the defined test plan (checklists). The functionality of the Data Resiliency Service environment is checked by recovering an exemplary VM.		
Comparison of the environment with the contractor's best practices		
As part of this service, we conduct regular reviews of the Data Resiliency Service to ensure that it meets the highest standards. During the system review, the focus is not only on the current status, but also on the contractor's recommendations for adjustments or optimizations of the service.	R/A	C/I
Preparation of a protocol, information to the client regarding any necessary measures		
A test report is created and sent to the client after completion of the test routine. The client is informed about the need for measures to improve the system.	R/A	C/I
Optional - Annual Review Emergency Manual		
When reviewing the emergency manual with a focus on ransomware recovery, the focus is on several aspects. This includes the structure and timeliness of the manual, the clear definition of responsibilities and effective communication channels. In addition, the precision of the recovery procedures, the quality of the backup strategies and their compliance with business requirements are checked. Security measures during and after recovery are analyzed, as is the frequency and effectiveness of emergency exercises and training for the client's employees. The documentation of all activities as well as regular internal or external audits round off the review to ensure that the emergency manual acts efficiently and reliably in the context of ransomware attacks.	R/A	C/I

Obligation of the client to cooperate	CO	CL
Existing licensing		
To provide the service, the products "Veeam Backup&Replication" and "Veeam Recovery Orchestrator" are required (valid license or ongoing manufacturer maintenance).	C/I	R/A
Remote access		
A prerequisite for carrying out the activities described is remote access to the Data Resiliency Service environment via VPN or screen-sharing solution. Active support in setting up remote access is one of the client's responsibilities.	C/I	R/A
Duty of care		
This service does not release the client from the ongoing, careful handling of the systems and system components. A tested system may exhibit problems with its functionality after or during the test. This may lead to data loss and similar consequences. The contractor therefore expressly advises the client that the data and systems must be backed up by the client before the contractor's services are carried out. The contractor accepts no liability for faults, defects or	C/I	R/A

| failures that occur during or after the test. The client must bear any disadvantage resulting from these circumstances. | | |

Framework conditions for service

For the software updates and periodic system checks, appropriate rights to the client's systems are required. These are provided, set up or commissioned by the client before the contractor provides the software updates or checks as a service.

Services not included

Measures to improve or optimize the system

Expenses for audit reports and protocols

Restore test of the entire infrastructure

Support services in response to inquiries (support, recovery tasks, design changes). These services are charged as required at the applicable hourly rate.

MS-DRAAS – Version 3.0