Commvault Remote Managed Services Description

Our Remote Managed Services offering ("RMS") is a managed service that monitors, manages, and optimizes our Solutions and provides 24x7 remote monitoring, remediation, reporting, and annual health checks.

- **Remote Monitoring:** 24x7 remote monitoring of Customer's Commvault environment through its connection to the RMS monitoring platform.
- **Reporting:** Monthly operational report with details on health and service level of Customer's Commvault environment delivered by the 7th business day of each calendar month ("Monthly Operational Report").
- **Strategic Business Reviews:** Strategic business reviews to assess RMS status, evaluate key initiatives, and address service concerns up to four times annually.
- **Feature Release Updates:** Scheduled remote deployment of the Solutions' feature releases within Customer's environment, including long-term support releases, through mutually agreed change management.
- **Media Agent Software Configuration:** If required to address capacity or performance limitations, Commvault will deploy and configure additional Commvault media agent software in support of the In-Scope Environment.in accordance with mutually agreed schedule and change management. Deployment, configuration, or migration of media agent hardware, Commvault Hyperscale-X, and installation of Commvault client(s) or CommServe are excluded.
- **Commvault Hyperscale:** Management of Customer's Hyperscale X appliances and/or Hyperscale X Reference Architecture solutions in support of the In-Scope Environment, including firmware and operating system and vendor escalation for hardware failures.
- **Administration and Planning:** Perform administrative tasks relating to configuration within In-Scope Environment and conduct planning activities during Regional Business Hours, including developing and maintaining backup procedures following Commvault best practices, performing capacity management and performance trending, or configuring new clients within Commvault policies. "Regional Business Hours" means the standard business days and hours of Commvault's business operation in a specific geographic region, typically 8 a.m. to 5 p.m.
- **Incident Management:** 24x7 remote triage and troubleshooting of In-Scope Environment for incidents detected by the RMS or reported by Customer, including remediation of issues related to any in-scope backup failures and restore operations as required to support Customer during self-service restore operations and performance of restore operations per Customer requests. If the cause of any issue is within Customer's server, storage, or network infrastructure, Customer will be responsible for corrective action.
- **Problem Management:** Remotely perform probable cause analysis of Severity Level 1 incidents (as defined below) pertaining to In-Scope Environment during Regional Business Hours. If the cause of any issue is within Customer's server, storage, or network infrastructure, Customer will be responsible for corrective action.
- **Vendor Callout:** Contact up to two third-party vendors identified by Customer during activation. Callouts will be performed for media management or In-Scope Environment hardware failures to report incidents and coordinate resolution of incidents and issues affecting In-Scope Environment and clients. If additional vendor support is required for support of the Commvault environment, additional charges will be incurred by Customer.
- **Access Management:** 24x7 access to the RMS ticketing portal.
- **Change Management:** Participation in mutually agreed to change management process to address changes pertaining to In-Scope Environment. Commvault will evaluate and approve changes to In-Scope Environment, pro-actively alert Customer regarding production changes in the managed environment and execute approved change requests as agreed to by the defined stakeholders. Commvault resources will not directly access Customer's ticketing system. Standard changes will be addressed during Regional Business Hours while emergency changes will be addressed 24x7.
- **Restore Verification:** Every 6 months, measure the ability of Customer to restore up 10% of the "critical" Commvault clients within the In-Scope Environment. "Critical" clients are those systems identified by Customer as essential to core business operations. This measurement will include restores processed during the course of business-as-usual. In the event that Customer does not initiate restores from at least 5% of the client environment, Commvault will notify Customer of the gap.
- **Service Delivery Manager:** Provide an assigned service delivery manager during Regional Business Hours for program administration and escalation management activities.
- **Monthly Backup SLA Service Level:** Target a 98% or higher monthly backup success service level for clients across the aggregate In-Scope Environment. The monthly backup service level will be reported via the Commvault Cloud Backup Success Report. Failure by Commvault to meet the monthly backup service level may entitle Customer to service credits as set forth below.
- **Monthly Restore Success Rate Service Level:** Target a 100% monthly restore success service level for clients across the aggregate In-Scope Environment. Restore success is defined as the Solution restoring data from successful backups in its original format. The restore success rate service level will be measured and included in the Monthly Operational Report. Failure by Commvault to meet the monthly restore service level may entitle Customer to service credits as set forth below.
- **Restore Request Response Time Service Level**: For Severity Level 1 (as defined below) restore requests, Commvault will target to acknowledge and respond within one (1) hour of receiving the request from Customer. Severity Level 1 Restore Requests must be initiated by Customer via direct call to the Commvault designated contacts. For non-Severity Level 1 restore requests, Commvault will target to acknowledge and respond within four (4) hours of receiving the request from Customer. Commvault's obligation to meet the restore request response time set forth herein is subject to the following: (a) Customer submission and Commvault acceptance of a formal restore request ticket with sufficient detail and authorization; (b) For Severity Level 1 restore requests, Commvault has received call from Customer requesting such restore; and (c) Customer contact must be available to address Commvault questions before and during the restore process. Failure by Commvault to meet the Severity Level 1 restore request response time within a given month may entitle Customer to service credits as set forth below.

RMS Exclusions:
Architectural design or revision; disaster recovery or business continuity planning and testing, major operational recoveries resulting from a ransomware attack on Customer or disaster recovery event beyond 10% of protected systems under management in a month; administration and implementation of Customer-side issue resolutions, ongoing maintenance, patching and upgrades of existing Commvault clients; installation of Solutions on new clients; implementation of new hardware or software not identified as part of the infrastructure at the time of activation; management of Commvault applications within Commvault CommCells outside the scope of the In Scope Environment; general system administration of operating systems such as patch management of the operating system related to any CommServe, media agent, or client included in the delivery of RMS unless deployed on a Hyperscale X appliance or Hyperscale X Reference Architecture solution; physical rack-and-stack and/or cabling of appliances and deployment and configuration of new appliances; server hardware maintenance management; non-Commvault security management; hardware fault rectification for non-Commvault appliances or infrastructure; provisioning of new hardware including servers, storage, tape drives and others; physical management of media; non-Commvault patch application; desktop end user support; desktop/client installation or upgrades.

Changes to In-Scope Environment:
Changes to In-Scope Environment will incur additional fees.

Customer Responsibilities
Commvault's performance is contingent on Customer fulfilling its responsibilities as set forth in herein and requires coordination with appropriate Customer personnel. Commvault's nonperformance of its obligations will be excused to the extent that Commvault's failure to perform results from Customer's failure to fulfill its responsibilities or provide prompt and reasonable assistance. Customer shall:

- **Customer Contacts**: assign Customer contacts to support delivery of RMS, including (a) a primary contact to manage change management and Customer-internal resources, including its third party resources, and act as the focal point for issue resolution; (b) named, authorized contacts to interface on a day-to-day basis with Commvault ; and (c) a Customer Project Executive who can provide exclusive oversight and has the authority to make decisions for Customer regarding changes, budget, scope, resources, and other RMS related issues if they cannot be resolved by Customer's primary contact.
- **Customer Infrastructure**: provide the infrastructure necessary for deployment of RMS management utilities, including but not limited to metrics reporting utility that provides Customer the ability to display customizable, multi-level views of backup resources and customizable business level reports.
- **Non-Commvault Environment**: procure, install, and service all elements of Customer's non-In Scope Environment, including minimum OS installation and patching, server hardware, client hardware, storage, SAN fabric, networking, cabling, and power. The servers running the Solutions shall be maintained by the Customer unless Customer has purchased and deployed Hyperscale X appliances or Hyperscale X Reference Architecture solutions. For the avoidance of doubt, Customer is solely responsible for the management and maintenance of any non-Commvault data protection platforms.
- **Installation**: perform installation of Commvault client software on production systems.
- **Access**: provide Commvault with reasonable cooperation, information, access, and support necessary for the delivery of RMS, including access to suitably configured computers, software products, and applicable passwords; install and maintain deployed software on Customer systems; materials and resources related to Customer's technical environment; Customer operating systems, network, and computing environments; and Customer's In-Scope Environment. If onsite presence is required and mutually agreed, Customer must provide access to a suitable conference room for meetings, interviews, and facilitated sessions. Customer shall be responsible for travel related expenses for any onsite services.
- **Commvault Procedures and Requests**: follow the appropriate operating procedures during submission of RMS requests and perform changes to Customer's environment as requested by the Commvault to resolve failures or performance issues with the Solutions. Failure to make such changes will results in forfeiture of any service credits.
- **Notification**: notify Commvault in writing at least twenty-four (24) hours in advance of any scheduled maintenance, network, or system administration activity that would affect Commvault's ability to deliver RMS.
- **Data Management Policy:** establish and implement a data management policy that meets the Customer's business requirements. and ensure such policy meets any compliance and/or privacy requirements that apply to Customer or its customers.
- **Other Requirements**: ensure, at all times, : (a) Commvault has been correctly licensed for all appropriate platforms, and the same are made available in a timely manner to Commvault. Customer may only receive RMS for versions of the Solutions within the In-Scope Environment that are currently supported by Commvault.; (b) all maintenance and support contracts of required systems, software, and hardware are provided to Commvault. All such contracts are active and in good standing, and all support contract numbers, or identifications have been provided.; (c) contact information, and relevant contract numbers for third-party hardware vendors are supplied to Commvault. Customer must notify these vendors that it authorizes Commvault to open incidents with and receive status updates from these vendors relating to the Commvault environment.; (d) all appropriate servers, computers and storage configurations will be running in a supported configuration; (e) the technical environment, including application and database, will be kept under change management ; (f) Customer's physical environment is stable and provides a viable environment for Commvault to deliver RMS; (g) a test environment is provided for Commvault to use for tasks such as test restores and patch verification. If a test environment is not available, then production servers will be used with the Customer's consent for such purposes.; (h) Customer has or maintains active maintenance and support for all Solutions within the In-Scope Environment. Failure to do so may result in a suspension or termination of RMS; and (j) Customer activates and maintains Commvault cloud reporting.

Incident Response and Service Level Agreement (SLA)

Commvault will undertake reasonable efforts to meet the following responses to incidents and backup service levels, subject to the exclusions set forth below. Commvault reserves the right to reassign severity levels based on the surrounding circumstances and nature of the incident.

Level and Targeted Response Time	Severity Definition and Incident Response
Severity 1- Critical (1-hour response)	Customer's system is inoperable or is at a severely reduced level of functionality resulting in an adverse impact on normal business operations and no immediate workaround or resolution is available. Customer agrees the incident will be worked continuously until resolved.
Severity 2- Severe (4-hour response)	Customer is experiencing intermittent failure or performance degradation which has limited Customer's normal business operations. These incidents are time sensitive and critical to productivity, but do not cause an immediate work stoppage. No workaround is available, and operations can continue in a limited capacity.
Severity 3 – Medium (1 business day response)	Conditions are defined as a minor and can be worked around without major impact to Customer's normal business operations.

Backup and Restore Targets and Credits

Metric	Service Level Monthly Target	Monthly Metric	Service Credit (% based on monthly recurring fees)
Backup SLA Service Level: As measured by the Commvault Cloud Dashboard	98%	<98% and >95% <95% and >90% <90% and >80% <80%	5% 10% 15% 20%
Restore Success: Defined as the Solutions restoring data from successful backups in its original format to the specified location.	100%	<100% and >95% <95% and >90% <90% and >80% <80%	10% 20% 30% 40%
Restore Request Response Time	Severity Level 1: 1 Hour	1 occurrence 2 – 5 occurrences > 5 occurrences	5% 10% 20%

The foregoing targets (the "Targets") shall only apply to Customer's In-Scope Environment and are not applicable where the failure to meet such target is due to any factor beyond Commvault's reasonable control, including but not limited to: (a) any emergency or planned maintenance, repair and upgrade; (b) issues or failures within Customer's or its service providers' services, environment, hardware, software, or other components not supplied by Commvault; (c) third party attacks, intrusions, distributed denial of service attacks or force majeure events, including those at Customer's or any third-party sites or data centers; or (d) Customer's acts or omissions in violation of the Terms. The aggregate maximum service credit in any given month is capped at 50% of the total monthly recurring fees for RMS. Customer will not be eligible for any service credits if the In-Scope Environment contains less than an aggregate total of 100 terabytes of licensed capacity or 500 protected servers.

In the event Commvault fails to meet the Targets, it shall (a) use commercially reasonable efforts to provide Customer with an error correction or work-around

that corrects the reported non-conformity; and (b) provide Customer a service credit as set forth above, provided such service credit is approved by Commvault, such approval not to be unreasonably withheld. Commvault will report on service level incidents detected by RMS in its Monthly Operational Report. Within 10 days of Customer receiving a Monthly Operational Report that includes a purported incident, Customer must submit a claim to Commvault with all information following the claim submission process described in the fifth sentence of section 3.2 of the Terms for the SaaS Solution. The remainder of the same section following such sentence applies to any failure to meet the RMS Service Level Monthly Targets. During activation of RMS, the Targets and service credits do not apply.

Activation Deliverables:

Deliverable	Description
Project Kick-off	Commvault will conduct a remote meeting with the Customer to kick-off the RMS project, including: • Contract review • Activities and responsibilities review • Team and project plan review • Initiate connectivity process
Infrastructure Readiness	Commvault will work with the Customer to establish technical requirements of RMS including: • Connectivity to managed backup infrastructure • Access to Customer CommServe and media agents • Metrics reporting utility (as applicable)
Environment Discovery	Commvault will perform environment discovery to review and document the following: • Business requirements of the Customer • Customer's backup infrastructure • Incident management process • Change Management process
Transformation Workbook	Commvault will develop a transformation workbook that includes the following: • Identification of top risks affecting Commvault performance • Customer health-check and benchmarking • Review of naming conventions • Gap analysis of Commvault best practices and tuning standards; policy review and recommendations

Optional Services:

Customer may purchase the below additional services, subject to additional fees.

Commvault Customer Success Engineer

If purchased, Customer will have access to an identified Commvault Customer Success Engineer during Regional Business Hours, not to exceed 220 workdays per year, who serves as a technical escalation point and assists Customer with planning exercises or implementation of best practice methodologies.

Customer Success Engineer responsibilities may include:

- Assisting Customer with the development of backup policies.
- Coordinating Commvault-related issues escalations.
- Researching and providing technical advisement to help Customer optimize product performance, based on Customer's specific environment and operating objectives.
- Assisting with the technical aspects of RMS
- Reviewing the initial health-check of Customer's existing archiving environment in connection with RMS and helping to identify any areas that need to be improved.
- Assisting the Commvault team, in upgrade/patching processes in connection with RMS.
- Perform technical escalation management to Commvault when required.
- Creating root cause analysis documentation when applicable.
- Participating in RMS reviews
- Participating in issue management inclusive of multi-vendor collaboration in connection with RMS.