

SERVICES

Customer may request any of specific services that falls under Exhibit A (A.1 – A.4) to be provided by Service Provider and/or any third party.

A.1: Managed Multi-Cloud Services (Managed MCS)

1. **Managed Multi-Cloud Services (Managed MCS) consist of providing:**

- a. Access to hyperscaler cloud services, including but not limited to Amazon Web Services, Microsoft Azure, or Google Cloud Platform (“MCS Third-Party Provider”), as selected by Customer from time to time.
- b. Third party services

The Service Level Agreement (“SLA”) for Managed MCS is to be provided by the MCS Third-Party with the agreement to be agreed upon between MCS Third-Party and Customer.

2. Managed MCS is hosted on the infrastructure of a third-party cloud provider (“MCS Third-Party Provider”) & applies to the use of our Services with the following supported cloud providers’ platforms or MCS Third-Party Providers.

3. **Cloud service integration and interoperability.** Service Provider does not control the development or operation of these third-party platforms. Service Provider will use commercially reasonable efforts to rectify issues within its own service that hinder integration, however, we are not responsible for resolving issues solely attributable to changes or incompatibilities within other MCS Third-Party Providers’ APIs or services or for providing support or troubleshooting for third-party platforms themselves.

4. **Troubleshooting interoperability issues.** Service Provider support team will assist Customer in identifying and diagnosing interoperability problems within our service’s integration with other cloud providers. However, the extent of Service Provider’s involvement depends on the nature of the issue:

- i. Issues within Service Provider service: Service Provider will provide best-effort troubleshooting and potential solutions within our control.
- ii. Issues within other platforms: Service Provider will assist in identifying the potential cause and suggest possible workarounds. However, Customer may need to contact the respective cloud provider for further support.

5. **Data portability and migration.**

- i. *Export formats and tools.* Customer retains the right to export their data in supported formats using Service Provider provided tools or API access. Certain limitations may apply based on data types and technical constraints.
- ii. *Data export and Migration Fees.* Standard service fees apply to cover associated data storage, retrieval, network egress, and administrative costs for export and migration. A detailed fee schedule will be provided upon request.
- iii. *Data migration limitations.* While Service Provider strives for seamless migration, limitations may exist for extremely large datasets, requiring potential additional time, resources, and costs. Data transformation or third-party dependencies may necessitate further effort or services at an additional cost. Customer acknowledges compatibility with other cloud providers cannot be guaranteed due to technical or external factors.

6. **Customer security responsibilities in MCS.** Configuration, access control, encryption, and vulnerability patching within Customer’s cloud resources are Customer’s purview. Additionally, compliance with each platform’s security policies and terms of service is Customer’s obligation.

7. **Data residency and regulations.** Service Provider offers regional deployment options within supported platforms, and resources outlining their data residency capabilities are provided. However, determining compliance with specific regulations and seeking legal advice are solely Customer's responsibility.
8. **MCS disclaimers.** Notwithstanding anything to the contrary in the Agreement, the Managed MCS:
 - i. Is not covered by any SLA, unless specifically identified under the terms of the SLA,
 - ii. Is not subject to any obligations for Service Provider [or its Affiliate(s)] to provide termination or transition assistance or other technical assistance after Suspension or termination, and
 - iii. Is not subject to any business continuity or disaster recovery commitments.
 - iv. Does not guarantee seamless interoperability with all features and functionalities of every supported cloud provider with regard to the integration of our service with their APIs and services.
 - v. Does not obligate Service Provider [or its Affiliate(s)] or the MCS Third-Party Provider to provide the MCS Third-Party Provider's services that are necessary for the Customer to use the Managed MCS.
9. **Limitations and exclusions applicable to Managed MCS.** Customer is solely responsible for determining whether the functionalities offered by Service Provider service on each supported cloud provider meets Customer's specific requirements. Due to technical differences in the underlying cloud environments that are beyond our control, certain features may have limitations or exclusions specific to each platform like:
 - i. Not all features of Service Provider service may be available on all supported cloud providers.
 - ii. Certain features may have limited functionality on specific platforms.
 - iii. Some features may be entirely excluded from use on specific platforms due to technical or security constraints.
 - iv. If the MCS Third-Party Provider makes a change to its services or terms, and Service Provider [or its Affiliate(s)] reasonably concludes that its provision of the Managed MCS is no longer commercially feasible as a result of the change, Service Provider (or its Affiliated Entities) may immediately suspend all or part of Customer's use of the impacted Managed MCS, or make any other discontinuance or backwards-incompatible change necessary to continue to provide the Managed MCS.
10. **Escalation and Change Management with MCS Third-Party Provider**
 - 10.1. In the event of third-party escalation the standard SLAs will be applied as agreed. The ticket will remain open in Service Provider's ITSM (Information Technology Services Management) system until we are informed of resolution status from the MCS Third-Party Provider. It is the responsibility of the Customer to inform the MCS Third-Party Provider of the managed service arrangement and to provide all necessary MCS Third-Party Provider contact information to the onboarding team at time of provisioning of the service.
 - 10.2. Tickets raised on the Service Provider service desk will remain open until closure once escalated to the MCS Third-Party Provider (principal third party vendor). Service Provider will provide necessary support on infrastructure changes to assist troubleshooting activities for the MCS Third-Party Provider to ensure back-to-back support is provided for the Customer.
 - 10.3. MCS Third-Party Provider can also raise change requests with Service Provider for assistance with a change or for information only purposes, during which time we can provide a change freeze and stop service desk alerts during the period of change. Service Provider is available on request to take part in activities that require changes to the infrastructure as per the terms of the agreement in section 3.5.

10.4. Scope of Change Management

- 10.4.1. Change management is inclusive of business-as-usual changes. These are defined as discrete activities on a single system or function that can be complete in a period of 8 hours or less. The change management function expressly does not include professional services, in the event a change requires professional services these must be scoped and priced accordingly using the standard man-day rate.
- 10.4.2. Professional services activities are defined as activities that exceed the 8-hour threshold and/or require changes to be applied across multiple systems. An example of this would be an operating system upgrade across several servers.

11. Payment for Customer multi-cloud consumption charges

- 11.1. Customer contract with MCS Third-Party Provider: The Customer acknowledges and agrees that they are responsible for paying all consumption charges incurred with the MCS Third-Party Provider (principal cloud vendors) as per the terms and conditions outlined in the respective MCS Third-Party Provider contracts. The Service Provider shall not be liable for any charges related to the Customer's usage of cloud services from these MCS Third-Party Provider.
- 11.2. Billing and payment responsibility: The customer is solely responsible for timely payment of all invoices related to cloud vendor consumption charges. The managed Service Provider will not be held liable for any late fees, interest, or penalties incurred due to the customer's failure to pay these charges on time.
- 11.3. Usage monitoring and reporting: The Service Provider may monitor and report on the Customer's usage of multi-cloud services to facilitate accurate billing. The Customer agrees to cooperate with any requests for usage data or reporting required by the Service Provider to fulfil this obligation.
- 11.4. Changes in MCS Third-Party Provider pricing: The Customer acknowledges that MCS Third-Party Provider pricing may change over time, and such changes will directly impact the consumption charges billed to the Customer. The Service Provider will not be responsible for any increases in pricing imposed by the MCS Third-Party Provider.
- 11.5. Dispute resolution: In the event of a dispute regarding MCS Third-Party Provider consumption charges, the Customer agrees to resolve the issue directly with the MCS Third-Party Provider according to the terms and conditions of the MCS Third-Party Provider's contract. The Service Provider may provide assistance in facilitating communication but is not obligated to mediate or resolve disputes related to pricing or billing.
- 11.6. Termination of services: Failure to pay MCS Third-Party Provider consumption charges may result in suspension or termination of services provided by the MCS Third-Party Provider and/or Service Provider. The Customer understands that continued use of cloud services is contingent upon compliance with payment obligations to the MCS Third-Party Provider.

12. Billing terms

- 12.1. *Billing relation:* To make use of the Managed MCS, Customer must maintain an independent agreement, account and billing relationship with the applicable MCS Third-Party Provider eg. Microsoft Azure, Amazon Web Service (AWS), Google Cloud Platform (GCP) etc. Service Provider is only an intermediary in this case.
- 12.2. *Consolidated billing:* Service Provider will bill 100% of fee as per the start date of billing by MCS Third-Party Provider (principal cloud provider). Service Provider will directly pass-through all platform usage costs associated with the Managed MCS to the Customer. A markup of certain percentage will be applied to the direct platform usage costs for managing the platform infrastructure of MCS Third-Party Provider. This markup will be clearly stated in the Service Order Form and subject to periodic review and potential adjustment upon mutual agreement.

- 12.2.1 Upfront billing: Customer will make an upfront commitment for the amount that Customer agrees to spend for the services. Accordingly, Customer will be billed in annually/semi-annually/quarterly (whichever is applicable) in advance for the committed amount. The minimum term of services is 3 years with the period beginning on the day that Customer receives activation email, unless otherwise specified in the agreement.
- 12.2.2 Arrear billing: In addition to committed charges for the minimum term which is billed under upfront billing, Customer may be liable for overage charges. For purposes of this Section, “overage” is defined as the amount of usage of the service during the relevant period that exceeds the usage covered by Customer’s active committed term of service. Any usage above the monthly commitment is incurred as overage and billed monthly in arrears separately as per the prevailing pricing.
- 12.2.3 Amount forfeited: The monthly committed amount or credits must be used within the monthly commit period. Any unused amount or credits within that period are forfeited.

13. Non-applicability of certain clauses or terms of ANNEX (1): SLAs:

The following clauses/terms of Annex (1): SLAs shall not be applicable for Customer who have subscribed for A.1: Managed Multi-Cloud Services (Managed MCS) under Exhibit A:1.2.7: Uptime Guarantee

1.2.8 Disaster Recovery,

1.1 Service Credits

1.2 & 1.4.7

SERVICES

Infrastructure as a Service (IaaS)

1. **Infrastructure as a Service (IaaS):** Under IaaS, compute platforms supply a virtual server instance and storage and APIs that let Customers migrate workloads to a virtual machine. Customers will have allocated compute power & resources. The virtual networks connect and manage cloud resources.
2. **Disaster Recovery as a Service (DRaaS):** Under DRaaS, Service Provider manages server image and production data replication to the cloud, disaster recovery run book creation, automated server recovery within the cloud, automated server failback from the cloud, and network element and functionality configuration, as needed.
3. **Backup as a Service (BaaS):** Instead of performing backup with a centralized, on-premises IT department, BaaS connects systems to a private, public or hybrid cloud managed by the Service Provider.

The performance standards for the above-mentioned Services are determined into the Service Level Agreement ("SLA") attached hereinafter as Annex (1).

SERVICES

Managed Services

Cloud Managed Services:

Cloud managed services refer to outsourced IT services. The key features of cloud managed services include Monitoring and maintenance, Infrastructure management, Security and compliance, Support and troubleshooting, Cost optimization, Scalability, and performance optimization.

These services shall be subject to the Service Level Agreement Attached herein after as Annex (1).

- a. Secured Services: Security experts will perform security analysis and passive health monitoring.
 - i. Health and Performance Monitoring: Health monitoring using event trending technology to ensure that the SOC is receiving events from Customers monitored systems 24 hours a day, 7 days a week, and 365 days in a year.
 - ii. Security Event Monitoring: Monitoring of SEIM events by certified security experts to identify and respond to security threats 24 hours a day, 7 days a week, and 365 days in a year.
 - iii. SOC (Securities Operations Centre) Access: Non-metered access to Service Provider's security analysis staff across SOC via the ticketing system, email, and phone.
- b. Assured & Assist Services: Assured/Assist is a proactive Information Technology (IT) infrastructure managed service
 - i. The framework for services includes installation of proactive system monitoring software at the Customer site. The alerts generated by this system automatically raise tickets on the Service Provider's Assured/Assist helpdesk which are serviced by Network Operations Centre (NOC) engineers of Service Provider.
 - ii. Customers receives a proactive service tasks list which defines all the system checks Service Provider performs and the frequency of the checks.
 - iii. The service also includes reactive support with priority escalation based on severity for any issues that arise on systems supported by Service Provider's team of Assured/Assist engineers.
 - iv. On a periodic basis, Customer shall receive a management report that provides insight into the health of Customer's environment and a chronological list of issues and fixes found and provided by Service Provider.
 - v. Details of how the Service Provider delivers these services can be found in the Managed Service Handbook

Point C to U below details the Customer obligations:

- c. Where required, the Customer shall make available appropriately skilled employee of Customer while an Incident is being managed.
- d. Outside normal Business Hours, the Customer must undertake appropriate triage methods to ascertain whether an Incident is of P1 status before logging the Incident
- e. The Customer is required to undertake an initial impact assessment before logging the Incident with Service Provider. Such Impact Assessment is to include:
 - Affected Services
 - Business Impact
 - Number & Type of users affected
 - Recent changes on affected infrastructure (regardless of perceived impact)
- f. The Customer shall provide full physical access to all Customer Supported Assets at Customer Premises if/when required.
- g. The Customer shall provide full administrative access to Service Provider to all the services outlined in the Impact Assessment and any subsequently identified services.
- h. The Customer is required to ensure that all Customer supported assets are appropriately licensed and have Supplier recommended hardware and vendor support in place.
- i. The Customer shall provide Service Provider with suitable remote access to all supported systems.
- j. The Customer is responsible for completing change request form in accordance with Service Provider's change management process.

- k. The Customer shall ensure that all relevant Customer employees have access to and have read Service Provider's Managed Services Handbook.
- l. The Customer shall ensure an on-going availability of suitable internet connection
- m. The Customer shall ensure 24x7x365 availability of a suitable escalation contact should Service Provider need to gain approval for an emergency change or to engage other aspects of the Customers support functions.
- n. The Customer shall provide suitable notice to any planned/scheduled maintenance that could affect the Customer supported assets including environmental changes.
- o. All Customer supported assets within the demarcation zone within this Agreement are covered by a valid software maintenance and support agreement in line with SLA under this Agreement.
- p. All Customer supported assets are in a valid supported configuration
- q. All Customer specific pre-requisites have been completed before Agreement commencement
- r. Access to customer systems via WebEx will be granted for the following elements of the Service to be delivered by Service Provider:
 - Telephone and remote diagnostics for faults
- s. Customer VPN/remote management software connectivity will be maintained for the following elements of the Service to be delivered by Service Provider:
 - Telephone and remote diagnostics for faults
 - Enhanced monitoring of Customer supported assets
- t. Customer is responsible for appropriately maintaining the devices being monitored. In the event of a device failure or misconfiguration, Customer will be responsible for the actions necessary to bring the device back online.
- u. Customer should communicate any network or system changes that could impact service delivery to the SOC via a ticket in the Service Provider's customer portal. SLAs will not apply to devices that are experiencing health issues.

SERVICES

Professional Services

Cloud Professional Services:

Consist of providing cloud professional services, including but not limited to cloud consulting, cloud implementation, and cloud migration.

The scope of Professional Services activities under cloud may include the following:

1. Analysis of Customer IT environment, workloads etc. to develop a customized cloud environment followed by migration planning.
2. Designing secure & scalable cloud infrastructure like network topology etc.
3. Handling the migration of Customer's applications, data, email workloads (Office 365) etc. to the cloud platform with minimal disruption to ongoing operations.
4. Security services like threat detection & mitigation etc.
5. Providing ongoing technical support to address any issues that may arise.