Meridian IT Australia

Service Description – mCompute Flex

1. Service Description – mCompute Flex

The Parties Meridian IT ("Provider") and the Client being an entity subscribing to Meridian IT for cloud services; agree that by accessing Meridian IT's cloud services, you (hereinafter referred to as "The Customer", "you" and "your") accept, without limitation or qualification, the terms and conditions contained within this Agreement or Service Description.

2. What is a Service Description

The Provider's mCompute Service Description defines the services offered and specific terms and conditions for each of these Services. This document forms part of our agreement, in conjunction with the master contract.

3. Services

The Provider will deliver the following Services

3.1 Infrastructure as a Service

- The Provider will provide the customer with the ability to consume a private cloud infrastructure service, whereby the customer consumes virtual machines or virtual instances for their own dedicated use
- mCompute Flex service provides the customer with a managed or self-managed operating system with an agreed allocation of virtual CPU's (vCPU), RAM, Disk capacity.
- The infrastructure service will be provided to as part of a multi-tenant service.
- Resources to be allocated based on a client by client basis, through provisioning of Virtual Machines (VM) resources.
- The mCompute service will be located in Australia in geographically dispersed datacentres. The Equinix Tier III operated datacentres will be located in Sydney (SY5) and Melbourne (ME2)
- The infrastructure will be available on a 24 x 7 basis with an availability Service Level Target of 99.99%, assuming the client has opted for the Disaster Recovery as a Service (DRaaS) option.
- This service is eligible for service rebates where the Service is unavailable as per the General Terms and Conditions. The following rebates apply for this service:

Service	Service Credit
Less than 43 minutes unavailable per calendar month.	No credit
More than 43 minutes but less than 360 minutes during a calendar month.	5% of the Monthly Service Charge
More than 360 minutes during a calendar month.	10% of the Monthly Service Charge

3.2 Software

a. The Provider will license the software as required based on the Providers **"Service Provider License Agreement"** with Microsoft or **"Red Hat Certified Cloud Service Provider"** program with Red Hat

b. Clients with active Microsoft Software Assurance (SA) or Subscription licenses (Windows Server) or the Red Hat Cloud Access Program may be eligible to utilize License Mobility features to transfer licenses to the MITA platform.

c. The Provider reserves the right to include additional software and licenses upon request from the tenant. This includes but not limited to Anti-Virus software and software from the Microsoft SPLA program (SQL, Exchange etc)

3.3 Monitoring & Reporting

a. **Reporting:** The Provider will provide monthly reports to the Client. The report structure will include:

- Per client abbreviation
- Capacity Consumption
- VM Monitoring: Reports on CPU, Memory, IOPS.
- General IPC & SLA
- BAU
- Network Utilisation Reporting

b. **Monitoring:** The Provider will be responsible for Remote monitoring which takes place on a 24 x 7 basis:

Service	Description	Managed Service
Platform Console	Centralised console for management of platform	Provider will manage the Platform console and manage the alters and messages, advising the tenant of any impact to Workload performance or platform availability.
Hardware Monitoring	Hardware across the platform will be monitored.	Provider will manage the "trigger points" informing the tenant of the appropriate action required to maintain the system within the thresholds and carry out rectification work
Performance Monitoring	Monitor system, workload performance.	Provider will monitor all aspects of the system performance informing tenant of the appropriate action required to maintain the system within the thresholds and carry out rectification work.
Backup as a Service Monitoring (BaaS)	Monitor the backup policies, schedules and (optional) replication status for secondary copies	Where BaaS has been purchased, the Provider will monitor and manage the backup devices and ensure that the backups are working in accordance with the schedule, policies and retention.
Disaster Recovery Monitoring (DRaaS)	Monitor the replication policies, schedules, and status	Where DRaaS has been purchased, the Provider will monitor the DR process and the

		infrastructure to ensure that a DR invocation can be successfully managed.

3.4 Support and Maintenance

a. The Provider will provide 24x7 support of the platform infrastructure. This service includes platform incident detection, escalation to the vendor if necessary, and issue resolution. Platform availability remains the responsibility of the Provider.
b. Where the Client purchases additional services such as Operating Systems or Application support, this will incur an additional Managed Service cost.
c. Technical Support by the Provider is based on Australian Eastern Standard time zones.

3.5 IP Addressing

The Provider will assign IP addresses for client use. All IP addresses remain the property of the Provider and cannot be transferred out of the network.

- Public IP Allocation: For workloads that require internet-facing access, the Provider offers a pool of public IP addresses, ensuring secure, reliable connectivity to external networks and customers. Each Pool of Public IP addresses is available in blocks of 2, 6 and 14 contiguous IP addresses

3.6 Security Posture

The Provider adheres to security and data management practice ISO27001 and ISO9001.

- The Provider (MITA) will be responsible for providing hosting facilities in a Tier III secure environment that operate on a 24 x 7 basis.
- The Provider (MITA) will be responsible for maintaining the security posture in accordance with ISO27001 – Information security, ISO9001 – Quality Assurance
- **Network Traffic Isolation:** The platform includes advanced networking and security services that enable and support multi-tenancy. Each tenant will be isolated from other tenants by firewall policies and via custom traffic rules and isolated virtual networks.
- **Data Encryption:** The Provider will provide encryption of data in transit and at rest on Infrastructure provided as part of the service.
- **Data-in-transit:** data in transit is encrypted using SSL/TLS protocols
- **Data-at-rest**: data at rest is encrypted with AES-256 encryption algorithms

3.7 Platform High Availability

- **Local Replica:** By default, the Provider will ensure that a local copy of each data block is stored within each cluster.
- **Local Snapshots:** The platform provides the option for the Client to use point-in-time snapshots of data. Snapshots can be stored locally on the same platform as the VM or can be replicated along with the source data to a replicated copy at the secondary site (if the DRaaS option is selected). Snapshot capacity is counted towards the consumed capacity for each tenant.
- **Disaster Recovery (DRaaS): The Provider includes an option for Disaster Recovery.**
    - **RPO:** The DRaaS supports a default Recovery Point Objective (RPO) of 1 hour. For specific use cases an RPO of 15 minutes is available under the discretion of the Provider. *Note: RPO is the amount of data loss that can be tolerated.*
    - **RTO:** The DRaaS supports a Recovery Time Objective (RTO) of 1 hour.
    - **Protection Domains:** The Provider can provide **Protection Domains** for workloads. Protection Domain is a logical construct that groups workloads together for the purposes of data replication and failover.

- **DR Resources:** The Provider will provide the technical assistance required to invoke and carry out the DR processes, bringing platforms into production. DR can be initiated by the tenant on request (maximum of one failover & failback event every 12 months) or due to an unplanned event. The Provider will inform the client of failover events within 1 hour of unplanned failover.
- **DR Failover Testing:** The Provider will be responsible for any DR test as requested by the Client.

- **Backup as a Service (BaaS): The Provider includes an option for BaaS.**
  - **RTO:** The BaaS supports a Recovery Time Objective (RTO) of 24 hours.
  - **Encryption:** The Provider will provide AES-256 Encryption
  - **Immutability:** The Provider will provide Write-Once-Read-Many (WORM) capabilities on request

3.8 Storage Traffic Input Output Quality of Service (QoS):

The Provider reserves the right to set specific limits and prioritizations on Input Output (IO) operations based maintaining a balanced platform for all tenants. The limit will be based on workload type.The Provider reserves the right to qualify any **High Performance Application** workload before the workload is transitioned to the platform.

Workload Type	Max IOPS (IO per Second)
Standard Business Application	500
Database Applications	1000
High Performance Applications	Available upon qualification

3.9 Contract Term

The contract term will be agreed between the Provider and the Client.

Termination fees will apply if the contract is ended before the contract term is reached

3.10 Scheduled and Maintenance and Outage Window

To ensure the stability, security, and performance of the Meridian IT Private Cloud, regular maintenance activities will be conducted. During these windows, the Provider apply critical updates, security patches, and system improvements to their infrastructure.

Maintenance windows are scheduled to minimize disruption to your services and are typically conducted during off-peak hours. Notifications will be provided in advance to keep you informed about the timing and nature of the maintenance.

Scheduled maintenance requiring service downtime is reserved for the following standard outage window but may not be utilized if not required:

Day: 2nd Sunday of the month

Time: 6:00 AM to 2:00 PM (local time)

Emergency maintenance may occasionally occur outside of this window to address critical issues, with prior notice provided where feasible.