ATTACHMENT – MANAGED CLOUD

This Attachment to the Telstra Cloud Services Service Schedule sets out the service description and service levels for Managed Cloud and applies in addition to the Telstra Cloud Services Service Schedule.

1 SERVICE DESCRIPTION

OVERVIEW

1.1 Managed Cloud provides a management layer on top of compatible cloud services (the "**Service**").

ELIGIBILITY

1.2 You can apply for the Service on nominated virtual machines on Approved Cloud Environment as notified by us.

1.3 The Service is only available with:

(a) Greenfield environments;

(b) Brownfield environments following assessment and approval by a Telstra engineer; and

(c) Standardised Windows and Linux ISO images. Please refer to the User Guide for more information on supported operating systems.

1.4 The Service is available for any virtual machine that we deploy on your behalf. Virtual machines that you have deployed will not be managed automatically; you need to request management for any virtual machines created by you.

FUNCTIONS

1.5 The Service includes the following:

Function	
Proactive Enterprise Management	We will monitor your servers 24x7x365 for any Severity 1 and 2 alerts and will proactively troubleshoot to help prevent potential issues. We will respond to monitoring alerts and proactively contact the end-user to triage support issues.
Authorised Contacts	Strict processes ensuring email or support liaison to confirmed authorised contacts only mitigates engineering security compromises.
Cost Optimisation	Review and optimisation of your spend on your Approved Cloud Environment. We will review and recommend right sizing options for your Approved Cloud Environment. You will also have access to infrastructure spend information on your Approved Cloud Environment.
Best Practice Deployment	Best practice deployment of your Approved Cloud Environment, including Role Based Access Control, Cloud Virtual Network Design, & Security Controls.
Monitoring	Agent based monitoring of services such as SMTP, HTTP/HTTPS, SSH on a real-time basis, combined with 24x7 proactive troubleshooting and escalation of Severity 1 and 2 alerts.

ATTACHMENT – MANAGED CLOUD

Server Uptime	Uptime monitoring of your Approved Cloud Environment & alerting sent directly to your dedicated contact point. End of month status & performance reporting.
CPU Utilisation	Monitor, highlight & alert on critical CPU utilisation metrics on server infrastructure.
Disk Space Utilisation	Monitor, highlight & alert on critical storage utilisation & I/O metrics on your server infrastructure.
Memory Utilisation	Monitor, highlight & alert critical memory usage metrics along with graphical insights on used memory & free memory, memory pages (in/out/fault) to assist in capacity planning.
OS Patch Management	Assess, test, schedule, deploy and manage patching on your Approved Cloud Environment.
Antivirus Management	Antivirus management and monitoring to maintain the health of your Approved Cloud Environment.
Security Hardening	We will apply security hardening settings to your virtual servers in accordance with best practice. Hardening the operating system disables functionality that is not required while maintaining the minimum functionality of the virtual server.
Advisory and Governance	We will provide a service delivery management function, vendor liaison, monthly reporting, change management, Service Request co-ordination and technical advice for in-scope technologies.
Change Management	Change Management will be carried out in line with your change management processes including attendance at Change Approval Board (CAB) as required. We will carry out assigned changes in relation to the Approved Cloud Environment
Maintenance	We will maintain the Approved Cloud Environment to minimise unplanned interruptions to services by way of regular reviews. We will also perform capacity planning and review performance metrics of the Approved Cloud Environment.
Availability Monitoring	Availability monitoring will be setup to monitor the OS layer and Approved Cloud Environments.
Reporting and Reviews	Monthly reports will summarise incidents and service requests logged for the month and proactive tasks undertaken. Any issues and opportunities to improve reliability and useability of the Approved Cloud Environment will be detailed. Regular reviews will help ensure the Approved Cloud Environment is maintained and incidents are minimised.

1.6 The following table sets out additional Service features specific to each Approved Cloud Environment:

AWS Platform Management

ATTACHMENT – MANAGED CLOUD

AWS Services / Technologies	Amazon Services for IaaS: - Amazon EC2 instances - Amazon VPC - AWS S3 Storage - Amazon CloudWatch - AWS CloudFormation - AWS Management Console - Other AWS services as required to provide management of the designed solution
Microsoft Azure Platform Management	
Microsoft Azure Services / Technologies	Microsoft Azure Services for IaaS: - Virtual Machines - Virtual Networks - Storage - Monitor - Resource Manager - Portal - Other Microsoft Azure services as required to provide management of the designed solution

1.7 We will allocate a Service Delivery Manager ("**SDM**") for your Service. The SDM is responsible for day-to-day service delivery and achieving the services levels.

1.8 We utilise a number of third party tools and software to deliver the Service, we may substitute alternative tools and software from time to time.

LIMITATIONS

1.9 The Service does not include:

(a) configuration of any technology other than the Approved Cloud Environment or as otherwise set out in the Service Order Form;

(b) end user support and training. We can provide this option if required at an additional cost;

(c) interstate or international travel and onsite support (unless specifically stated in the Service Order Form). Travel fees may apply where travel is required;

(d) migration of data, databases or content from an existing system to the Approved Cloud Environment;

(e) support of the applications that are installed on the virtual machines within the Approved Cloud Environment;

(f) testing or deployment outside of the scope of this service;

(g) software licences for both antivirus and backup. This will be charged against your Telstra Approved Cloud Environment bill;

(h) the backup service. You may request a backup service from us, subject to additional terms and conditions and charges;

(i) storage costs for backup. This will be charged against your Telstra Approved Cloud Environment

bill; and

(j) the Approved Cloud Environment. This is subject to separate terms and conditions and charges.

1.10 If you require any services that fall outside of the scope of the Service, you can request these from us on a time and materials basis, which will be billed in addition to the Service charges.

2 SERVICE LEVELS

2.1 The available service levels for the Service are set out in the table below.

Service levels		
Severity	**Response Time**	**Resolution Time**
Severity 1	15 Mins	4 Hours
Severity 2	30 Mins	8 Hours
Severity 3	1 Hour	1 Day
Severity 4	2 Hours	2 Days
Service Requests	1 Day	3 Days

("**Service Levels**")

2.2 The timeframes set out in clause 2.1 above are suspended for any period during which we are waiting for your response or confirmation.

2.3 Response Time is calculated from the time of which the ticket was logged to when we have responded to your contact identified in the ticket.

2.4 Resolution Time is calculated from the time of which the ticket was logged to when we have changed the status of the ticket to 'resolved'.

2.5 Severity 1 and 2 incidents are calculated on a 24-hour basis.

2.6 Severity 3 and 4 incidents and Service Requests are calculated during Business Hours only.

CLASSIFICATION OF SEVERITY

2.7 We will use Impact and Urgency to set the severity level.

2.8 Urgency is the necessary speed of restoration of the Service, which is determined as follows:

(a) High: Preventing a core business function or service from being performed;

(b) Medium: Prevents or restricts the effectiveness of a day-to-day function or service; or

(c) Low: Minor impact to day-to-day tasks.

2.9 Impact of the ticket is the measure of how business critical it is, which is determined as follows:

(a) High: Impacts an entire site or all users;

(b) Medium: Impacts an entire team or small group of users; or

(c) Low: Impacts a single user or limited number of users.

2.10 The following table set out how we calculate Severity levels based on Urgency and Impact.

		URGENCY		
		High	Medium	Low
IMPACT	High	Severity 1 - Urgent	Severity 2 - High	Severity 3 - Medium
	Medium	Severity 2 - High	Severity 3 - Medium	Severity 4 - Low
	Low	Severity 3 - Medium	Severity 4 - Low	Severity 4 - Low

ESCALATION PROCEDURES

2.11 We follow a standard escalation process to resolve tickets which will be documented in the service delivery manual. You may escalate tickets when the level of Impact or Urgency increases.

SERVICE REQUESTS

2.12 Service Requests are any Install, Move, Add or Change to the Approved Cloud Environment.

2.13 All standard service request tickets will be classified as a Severity 4. You can request re-assignment to a higher priority on a case by case basis based on business priorities. In such a case, we will assign resources to assess and implement a high priority service request on a best efforts basis into the above priorities, and will be actioned within the corresponding Response Time service level. Service Requests will be either as per defined and agreed Service Catalogue items (as set out in your Service Order Form) or on a time and materials basis.

SERVICE LEVELS – REPORTING

2.14 Agreed reporting will be made available to your primary contact following the end of the prior month as agreed in the Service Order Form.

ACTIVATION TIMEFRAMES

2.15 The following table sets out the activation timeframes:

Deliverable	Target timeframe
Request for Assessment	3 Business Days from receipt of the request
Scoping	mutually agreed in the Service Order Form
Onboarding	mutually agreed in the Service Order Form
Activate Managed Cloud	mutually agreed in the Service Order Form

SERVICE LEVEL EXCLUSIONS

2.16 We are not responsible for a failure to meet a Service Level where:

(a) the failure is caused by you or as a result of your breach of contract;

(b) you fail to follow our reasonable directions;

(c) you do not provide us with full and accurate information detailing any requests or relating to any incidents that you report to us;

(d) the failure is caused by an outage of the infrastructure platform. The infrastructure service is subject to separate terms and conditions (including service level and service level credits); or

(e) it is caused by something outside our reasonable control.

(f) services offered by 3rd parties that directly affect the platform, that are not provided or managed by Telstra.

SERVICE LEVELS CREDITS

2.17 The Service Level is a standard offering, allowing you to use a Telstra certified highly available solution for your Approved Cloud Environment ("**Highly Available Solution**") to achieve availability-based service levels. The application of the Service Levels to your Approved Cloud Environment is subject to our approval and we will advise you of any revised Service Level targets if this is relevant to your Approved Cloud Environment.

2.18 If we approve the Service Level for your Approved Cloud Environment, we will use commercially reasonable efforts to maintain Highly Available Solution availability of 99.95% each month.

2.19 Availability excludes any outages or downtime related to maintenance or management work, scheduled downtime or customer initiated downtime (including downtime due to Change Requests).

2.20 Highly Available Solution availability is calculated as:

Monthly Availability Percentage = ((total minutes in a calendar month – total minutes Unavailable) / total minutes in a calendar month) x 100

2.21 If in any month the actual Highly Available Solution availability does not meet the Service Level you will be eligible to receive a service level credit as described below ("**SLA Credit**"):

Monthly Availability Percentage	**SLA Credit Percentage**
99.9% – 99.95%	50%
Less than 99.9%	75%

2.22 The SLA Credit is calculated as a percentage of the monthly Managed Cloud charge paid by you.

2.23 Measurement of the Service Level is based on the Highly Available Solution regions being Unavailable.

2.24 The Service Level does not include any credit for your underlying public cloud infrastructure. Your public cloud provider will, in accordance with its terms and conditions, pay any applicable service level credits for the unavailability of your underlying public cloud infrastructure.

2.25 To receive an SLA Credit you must submit a request to your Account Executive or Service Delivery Manager within 2 months including the following information:

(a) the dates and duration of each unavailability incident you are claiming; and

(b) details of the affected virtual machines within your Approved Cloud Environment.

2.26 If we approve your claim, we will apply the SLA Credit to a future bill.

3 CHARGES

3.1 The charges for the Service will be billed monthly in arrears.

3.2 As part of your Service, we may give you access to certain tools and applications to monitor performance of your cloud environment. Please note that any bill history, usage and cost metrics are only estimates. The estimated totals may not correspond to the totals shown on your Telstra bill, due to misalignment of billing periods or lag in displaying information in the current month. We do not guarantee that the information on the tools or applications will be accurate or complete. If you require the exact totals, you must refer to your Telstra bill. You must ensure that you pay the total shown on your Telstra bill.

4 YOUR RESPONSIBILITIES

4.1 All virtual machines of your Approved Cloud Environment must have a current back up and then be backed up regularly.

4.2 You will need to provide us with administrative access to the virtual machines you nominate to be managed as part of the Service. You will also need to allow deployment of management agents and security scripts on your virtual machines to be managed by us.

4.3 You are responsible for ensuring that you comply with the licence terms of any software (such as application software or operating system) which you install or use in connection with your Approved Cloud Environment.

4.4 Even though we are providing you with managed services for your Approved Cloud Environment, you will be given a high degree of control over your Approved Cloud Environment. If you configure and manage your Approved Cloud Environment in such a manner that causes disruption to those services or the Service and/or deletion of any of your data, you will be responsible for any loss that you suffer as a result and you may need to pay us an additional charge to fix any problems on a best efforts basis.

4.5 If your Service includes management of third party hardware and/or software not provided by us, you warrant that you have obtained the appropriate consents or hold the necessary licences to enable us to manage that hardware or software on your behalf.

4.6 You acknowledge that the Service relies on you providing us with accurate information on your Approved Cloud Environment, including but not limited to details on applications, user locations and application usage profiles, storage, peripherals, network topology and security requirements.

4.7 You must perform any testing we advise you is necessary in connection with your Service.

4.8 You are responsible for all internal stakeholder communications in connection with your Approved Cloud Environment (for example outages for patches or upgrades).

4.9 You must identify your personnel that are responsible for working with us and define the roles of the identified personnel. You must also ensure your identified personnel are available to provide information, and participate in scheduled information gathering sessions, interviews, meetings and conference calls with us.

4.10 You will use reasonable endeavours to investigate and try to identify whether or not the Approved Cloud Environment is the likely root cause before contacting us for support.

4.11 You must have a backup service for every virtual machine that we are managing.

ATTACHMENT – MANAGED CLOUD

5 DEFINITIONS

5.1 In this Attachment, unless otherwise stated:

Business Hours means 8.30am to 5.30pm (local time in the jurisdiction of where the Service is supplied) on a Business Day.

Cloud Virtual Network means VPC for AWS and Virtual Network for Microsoft Azure.

Unavailable means when your virtual machines have no external connectivity but excluding any outages or downtime related to maintenance or management work, scheduled downtime or customer initiated downtime (including downtime due to Change Requests).