OUR CUSTOMER TERMS
MANAGED CLOUD

CONTENTS

OUR CUSTOMER TERMS
MANAGED CLOUD

Certain words are used with the specific meanings set out in the General Terms part of the Cloud Services section of Our Customer Terms at http://www.telstra.com.au/customer-terms/business-government/cloud-services/, or in the General Terms of Our Customer Terms at http://www.telstra.com.au/customer-terms/business-government/index.htm

1 ABOUT THIS PART

1.1 In addition to this Managed Cloud section of Our Customer Terms, unless we agree otherwise, the following terms also apply:

(a) General Terms of Our Customer Terms (see http://www.telstra.com.au/customer-terms/business-government/index.htm); and

(b) General Terms of the Cloud Services section (see https://www.telstra.com.au/customer-terms/business-government#cloud-services); and

(c) other parts of the Cloud Services section, depending on the nature of the products and services that you receive from us.

1.2 For an explanation of the interrelationship between the various sections of Our Customer Terms see clause 1 of the General Terms of the Cloud Services section at the link above.

2 WHAT IS MANAGED CLOUD?

2.1 The Managed Cloud service provides a management layer for your chosen compatible infrastructure service. Save as set out in this Managed Cloud section, we do not monitor or manage any of your other services.

2.2 As part of your Managed Cloud 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.

Eligibility

2.3 You can apply for the Managed Cloud service on nominated virtual machines if you have one or more of the following cloud services ("**Approved Cloud Environment**"):

(a) Amazon Web Services

(b) Microsoft Azure

2.4 The Managed Cloud 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.

2.5 All virtual machines that you have requested management of must have a current back up and then be backed up regularly.

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

2.7 The Managed Cloud service is available for any virtual machines 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.

3 WHAT'S INCLUDED IN MANAGED CLOUD?

3.1 The Managed Public Cloud 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	Real-time monitoring combined with 24x7 proactive troubleshooting and escalation of Severity 1 and 2 alerts.
Service Availability Monitoring	Uptime monitoring of your Approved Cloud Environment & alerting sent directly to your dedicated contact point. End of month status & performance reporting.
Infrastructure Performance Monitoring	Monitor, highlight & alert on virtual server infrastructure.

OS Patch Management	Assess, test, schedule, deploy and manage patching on your Approved Cloud Environment.
Online Threat Protection	Antivirus and malware 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 remote 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.
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.

3.2 The following table sets out additional Managed Cloud service features specific to each Approved Cloud Environment:

AWS Platform Management	
AWS Services / Technologies	Amazon Services including: - EC2 instances - VPC - S3 - CloudWatch - CloudFormation - Management Console - RDS - Elastic Load Balancing

	- IAM - CloudFront - Other AWS services as required to provide management of the designed solution
Telstra Cloud Tracker*	Governance & Auditing of changes in your AWS Environment.
Telstra Cloud Advisor*	Optimisation of Cost, Performance, Security & Fault Tolerance.
Telstra Cloud Analytics*	Cost Management of AWS Environment.
Microsoft Azure Platform Management	
Microsoft Azure Services / Technologies	Microsoft Azure Services including: - Virtual Machines - Virtual Networks - Storage - Monitor - Resource Manager - Portal - Other Microsoft Azure services as required to provide management of the designed solution

* Available in a future release (estimated Q4 FY18)

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

3.4 We utilise a number of third party tools and software to deliver the Managed Cloud service, we may substitute alternative tools and software from time to time.

4 LIMITATIONS

4.1 The Managed Cloud service does not include:

(a) Configuration of any technology other than the Approved Cloud Environment or as otherwise set out in the Statement of Work;

(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 Statement of Work). 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.

4.2 If you require any services that fall outside of the scope of the Managed Cloud service, you can request these from us on a Time and Materials basis, which will be billed in addition to the Managed Public Cloud service charges.

5 CHARGES

5.1 The charges for your Managed Cloud services are set out in your Statement of Work.

6 TERM

6.1 Unless otherwise specified in your Statement of Work, managed services are available on a casual, month-to-month, basis.

7 YOUR RESPONSIBILITIES

7.1 You acknowledge that the Managed Cloud 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.

7.2 You must perform any testing we advise you is necessary in connection with your Managed Cloud service.

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

7.4 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.

7.5 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.

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

7.7 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.

7.8 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 your cloud services or the Managed Cloud services 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.

7.9 If your Managed Cloud 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.

8 INTELLECTUAL PROPERTY RIGHTS

8.1 Except as provided in this clause 8, nothing in this Agreement transfers ownership in, or otherwise grants any rights in, any Intellectual Property of a party.

8.2 For the purposes of this clause 8:

Background Material means any material (other than Contract Material) owned or licensed by us (or our licensors) and made available to you for the purposes of this Agreement;

Contract Material means all material created by us or by the parties jointly after the Start Date that is delivered or required to be delivered to you in relation to the Managed Cloud Services, but excludes Customer Material and Background Material.

Customer Material means all material that is provided by you to us for the purposes of this Agreement and performing the Managed Cloud Services, but excludes Contract Material.

Our Material

8.3 We grant you a non-exclusive, non-transferable, royalty free licence to use the Background Material for the sole purpose of using and receiving the benefit of the Managed Cloud Services during the Term. You must not sub-licence, assign, share, lease or otherwise transfer any right to use the Background Material to any third party.

Your Material

8.4 You grant to us a non-exclusive, royalty-free licence (including the right to sub-licence for the purposes of providing the Managed Cloud Services) to use, reproduce, modify, adapt and otherwise exercise all Intellectual Property Rights in the Customer Material to the extent necessary for us to perform our obligations under this Agreement.

Contract Material

8.5 Unless otherwise agreed, we (or our licensors) own all intellectual property rights in the Contract Material.

8.6 We grant you a, non-exclusive, non-transferable and royalty free licence to use the Contract Material for the sole purpose of using and receiving the benefit of the Services during the Term. You must not sub-licence, assign, share, lease or otherwise transfer any right to use the Contract Material to any third party.

9 SERVICE LEVELS

Premium Service Levels

9.1 The Premium Service Level is an enhanced 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 Premium Service Level to your Approved Cloud Environment is subject to our approval.

9.2 If we approve the Premium Service Level for your Approved Cloud Environment, we will use commercially reasonable efforts to maintain Highly Available Solution availability of 99.99% each month.

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

9.4 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

9.5 If in any month the actual Highly Available Solution availability does not meet the Premium 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% – 99.99%	50%
Less than 99.9%	75%

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

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

9.8 The Premium 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.

9.9 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.

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

Standard Service Levels

9.11 The standard service levels for Managed Cloud are set out in the table below.

Managed Cloud – Standard SLA		
Severity	**Response Time**	**Resolution Time**
Severity 1	15 Mins	2 Hours
Severity 2	30 Mins	6 Hours
Severity 3	45 Mins	8 Hours
Severity 4	120 Mins	24 Hours

9.12 The timeframes are suspended for any period during which we are waiting for your response or confirmation.

9.13 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.

9.14 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'.

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

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

Classification of Severity - Incidents

9.17 We will use impact and urgency to set the priority level. Urgency is the necessary speed of restoration of Managed Cloud service. Impact of the ticket is the measure of how business critical it is.

9.18 The speed at which restoration is required (Urgency) 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;

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

9.19 The impact the incident has on the Organisation ("**Impact**") is determined as follows:

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

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

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

9.20 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

9.21 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

9.22 Service requests are any Install, Move, Add or Change to the Approved Cloud Environment. All standard service request tickets will be classified as a Severity 4. Customers 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 SLA. Service Requests will be either as per defined and agreed Service Catalogue items (as set out in your Statement of Work) or on a time and materials basis.

Service Levels – Reporting

9.23 Agreed reporting will be made available to your primary contact following the end of the prior month as agreed in the Statement of Work (SOW).

Activation Timeframes

9.24 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 Statement of Work
Onboarding	mutually agreed in the Statement of Work
Activate Managed Cloud service	mutually agreed in the Statement of Work

Service Level Exclusions

9.25 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 SLA targets and credits) and

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

10 DEFINITIONS

10.1 **Business Day** means Monday to Friday excluding the following Australian public holidays: New Year's Day, Australia Day, Good Friday, Easter Monday, ANZAC Day, Christmas Day and Boxing Day.

10.2 **Business Hours** means 8:30am to 5:30pm (Australian Eastern Standard Time) on a Business Day.

10.3 **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).