OUR CUSTOMER TERMS
TELSTRA BUSINESS MANAGED SERVICES

CONTENTS

TELSTRA BUSINESS MANAGED SERVICES

1 ABOUT THIS SECTION

1.1 This is the Telstra Business Managed Services (**TBMS**) section of Our Customer Terms.

1.2 The General Terms of Our Customer Terms at https://www.telstra.com.au/customer-terms/business-government also apply, unless you have entered into a separate agreement with us which excludes the General Terms of Our Customer Terms.

1.3 In addition to the terms set out in this TBMS section of Our Customer Terms, service specific details for each component of your TBMS are set out in:

(a) the individual Application Form(s) for Solutioned Services and Professional Services; and

(b) your Order.

1.4 The "Common Terms" part of this TBMS section of Our Customer Terms set out in PART A contains the general terms applying to all of the services available as part of the TBMS.

1.5 The individual Managed Services sections set out in PART B set out the terms that apply specifically to each individual Managed Service, and your Order contains details of the particular Managed Services that you acquire from us.

1.6 If there is any inconsistency between:

(a) the General Terms of Our Customer Terms;

(b) this Common Terms part of this TBMS section of Our Customer Terms;

(c) the individual Managed Service sections of this TBMS section of Our Customer Terms (to the extent relevant to the services you actually acquire from us, as set out in your Order);

(d) the individual Application Form(s) for Solutioned Services and Professional Services; and

(e) your Order,

then the document listed later prevails to the extent of the inconsistency.

PART A – COMMON TERMS

2 TELSTRA BUSINESS MANAGED SERVICES

2.1 TBMS is a collection of services designed to assist you with management of your Approved Environment.

2.2 TBMS is made up of the following services:

(a) **Managed Services**: these services provide for management of an agreed scope of your Approved Environment;

(b) **Professional Services**: these are services with a defined scope, features and inclusions delivered on a project basis; and

(c) **Solutioned Services:** these are customised services, designed by a solution architect.

2.3 Unless otherwise stated, all TBMS are delivered remotely.

Eligibility

2.4 To be and to remain eligible to acquire TBMS, you must (unless we advise you otherwise):

(a) be a Telstra Business customer;

(b) have and maintain current access to the Telstra Apps Marketplace;

(c) comply with any Customer Pre-Requisites and any particular eligibility criteria set out in the applicable individual sections of this TBMS section of Our Customer Terms; and

(d) nominate us as your Microsoft Cloud Solution Provider (CSP).

2.5 TBMS is not available to Telstra Wholesale customers or for resale.

Activation

2.6 Your TBMS will be considered ‘active’, and we will commence charging for them, in accordance with the applicable individual Managed Services sections of this TBMS section of Our Customer Terms.

3 SERVICE COMPONENTS AND SERVICE TIERS

Managed Services

3.1 The Standalone Managed Services available as part of TBMS are:

(a) Managed Endpoint;

(b) Managed Collaboration;

(c) Managed Cloud Virtual Machine;

(d) Managed Cloud Services Backup;

(e) Managed Microsoft Defender; and

(f) Network Management.

3.2 The Standalone Managed Services are available to order individually. Further detail about each is set out in the respective Managed Services sections of this TBMS section of Our Customer Terms.

3.3 You can also acquire the Managed IT Services Bundle, which comprises:

(a) Managed Endpoint;

(b) Managed Collaboration;

(c) Managed Cyber Security;

(d) Managed OneDrive Backup; and

(e) Network Management.

Professional Services

3.4 You may request that we provide certain Professional Services relevant to your TBMS.

3.5 In certain circumstances, we may require you to add Professional Services in order to receive Managed Services. If this applies, we will inform you as part of the ordering process for the relevant Managed Services.

3.6 If we agree to provide Professional Services, these will be described in a separate Application Form, which may include terms in addition to this TBMS section of Our Customer Terms.

Solutioned Services

3.7 You may request that we provide certain Solutioned Services relevant to your TBMS.

3.8 If we agree to provide Solutioned Services, these will be described in a separate Application Form, which may include terms in addition to this TBMS section of Our Customer Terms.

Service Tiers

3.9 Certain individual Managed Services are available with Service Tiers. Unless we agree otherwise, any Service Tier you select applies to all Users of that Managed Service (that is, it is only possible to choose one Service Tier per Managed Service). For these purposes, the Managed IT Services Bundle is treated as a single Managed Service, so that one Service Tier will apply to the entire bundle.

4 TERM

4.1 Your TBMS will start on the Activation Date and continue on the basis of one of the following Initial Terms:

(a) a month-to-month basis (**Casual Term**); or

(b) either:

(i) a 12 monthly basis; or

(ii) as otherwise agreed in your Application Form,

(**Fixed Term**).

4.2 If the Initial Term is a Fixed Term, it will automatically renew at the end of the Initial Term on a month-to-month basis (**Renewal Term**), unless otherwise agreed or unless terminated earlier in accordance with Our Customer Terms (or your separate agreement with us).

5 FEES AND CHARGES

5.1 The fees for your TBMS are set out in the applicable Application Form and/or Order.

5.2 Further terms for fees and charges:

(a) for Managed Services, are set out in each of the individual Managed Services sections of this TBMS section of Our Customer Terms; and

(b) for Professional Services and Solutioned Services, are set out in the applicable Application Form.

5.3 Without limiting any other provision of Our Customer Terms, we may increase the fees and charges for one or more TBMS, by giving you reasonable advance notice from time to time. However:

(a) the change will only take effect at the expiry of the Initial Term or then-current Renewal Term for that service; and

(b) if you do not agree to the increased rates, you may terminate the relevant Managed Service(s) with effect from the expiry of the Initial Term or then-current Renewal Term for that Managed Service(s), by giving us written notice.

Other applicable fees

5.4 If you decide to take TBMS on a Casual Term basis, a Customer Onboarding Fee, equal to one month’s charges will be charged, as set out in the applicable Application Form and/or Order. The Customer Onboarding Fee does not apply to Fixed Term subscriptions.

5.5 If we agree to on-site delivery of the Professional Services, we will charge a Call Out Fee, as set out in the applicable Application Form and/or Order, or as otherwise notified to you.

6 SERVICE CONFIGURATION MANAGEMENT

6.1 All Managed Services and Solutioned Services include service configuration management.

6.2 Based on the information supplied to you at the commencement of your Managed Services and/or Solutioned Services, we will:

(a) set up a monitoring and alerting system;

(b) if applicable, supply, configure, and install monitoring tools or software agents as required by our IT Service Management (**ITSM**) tools to remotely monitor and manage any TBMS that require those tools;

(c) document and update service-related information about your Approved Environment, as well as configuration of our alerting system;

(d) validate the monitoring tools and processes for your Approved Environment; and

(e) implement or activate Remote Monitoring and Management (**RMM**) tools, linking them to your Approved Environment. These tools may include admin access and the associated management portal and, if we determine it is needed, installation of local software agents to allow increased visibility and control.

7 CUSTOMER EXPERIENCE MANAGER

7.1 As part of the TBMS we will provide you with access to a dedicated Customer Experience Manager (**CEM**), as further set out in this section.

7.2 The CEM will be responsible for the following:

(a) **Account Management**: including optimising your TBMS, being the primary point of contact for your TBMS, and reviewing the performance of your TBMS;

(b) **Service Management:** including providing support in relation to your TBMS to capture, co-ordinate, prioritise or escalate and communicate the resolution of Service Tickets within the Service Level; and

(c) **Onboarding Management**: including validating the Pre-Requisite Order Form and ensuring that all necessary pre-onboarding technical steps are completed by you.

7.3 The CEMs will not be responsible for:

(a) change management activities beyond your onboarding activities or changes to TBMS;

(b) internal customer adoption efforts for self-help portals or chatbots for third party applications, other than directing you to those applications;

(c) legal, regulatory, or audit documentation production;

(d) training activities;

(e) technical resolution of Service Tickets assigned to the Service Desk;

(f) business support outside of Business Support Hours; and

(g) billing enquiries (for which your Telstra Account Manager will remain your key contact).

8 SUPPORT REQUESTS

8.1 If you require our support with your Approved Environment, you can submit a request for us to provide it (**Support Request**). You can initiate a Support Request by phone, email, Service Portal or Chatbot, which is then a "**User-Initiated Request**".

8.2 When initiating a Support Request, you must:

(a) ensure that it is only lodged by an Authorised User for your business; and

(b) provide us with any reasonable information we request from you.

8.3 The Service Desk will perform troubleshooting through reactive and proactive alerting as raised through System-Initiated Requests and actively monitor your Approved Environment in accordance with this TBMS section of Our Customer Terms.

8.4 All User-Initiated Requests and System-Initiated Requests reported will be logged as a 'Service Ticket'.

8.5 We will respond to Service Tickets through:

(a) the CEM, during Business Support Hours; or

(b) the Service Desk, either outside of Business Support Hours or during Business Support Hours as directed:

(i) by the CEM; or

(ii) by you.

8.6 The Business Support Hours and other details regarding the CEM and the Service Desk are set out below:

	Customer Experience Manager (CEM)	Service Desk
Business Support Hours	8AM-6PM	24 Hours
Business Days	Monday – Friday Australian National Public Holidays excluded	Monday – Sunday Australian National Public Holidays included
Time Zone	Across all Australian time zones	
Monitoring	Only During Business Support Hours	24/7

8.7 You acknowledge and agree that:

(a) it is your responsibility to work with your Users to store information to enable backup;

(b) version updates and urgent security related updates may be applied to the Supported Technology at any time;

(c) monitoring alerts may require your action or escalation;

(d) remediation may require disabling services or removing software;

(e) any software or firmware update involves risk, and rollbacks and restarts may be required to restore service; and

(f) we are not responsible or liable for any loss or damage you incur or suffer in connection with our implementation of any third-party update, patch or fix into your Approved Environment, except to the extent such loss or damage was caused by our negligence, or our breach of Our Customer Terms (or your separate agreement with us) (and in on the event of such negligence or breach, subject to the terms of Our Customer Terms or your separate agreement with us).

Service Ticket resolution

8.8 In order to help you resolve a Service Ticket, we will:

(a) log and provide a Service Ticket reference number for the Service Ticket;

(b) classify the Service Ticket as appropriate;

(c) manage the Service Ticket until the Service Ticket is resolved;

(d) provide regular status updates for the Service Ticket; and

(e) advise you of the resolution and closure of the Service Ticket.

8.9 We will provide you with three reminders if we require your response to a Service Ticket. Service Tickets will be marked as resolved if you do not respond within 5 Business Days following our reminders. Any subsequent opening of such Service Ticket will be treated as a new Service Ticket.

8.10 If we reasonably believe the Service Ticket does not fall within the scope of the TBMS, we will promptly advise you. If, after discussing the Service Ticket with you, we reasonably believe the Service Ticket cannot be resolved, we will provide you with a reason and mark the ticket as closed.

8.11 In cases where Incidents are caused by a service or product in which we cannot control and/or support (such as third-party products and services), we will direct you to third-party vendor support processes. We will not be responsible or liable for issues or Incidents caused by third party products or third-party vendors, except to the extent such issue or Incident was caused by our negligence, or our breach of Our Customer Terms (or your separate agreement with us) (and in on the event of such negligence or breach, subject to the terms of Our Customer Terms or your separate agreement with us)..

Service Ticket classification

8.12 When processing a Service Ticket, we will classify it as either:

(a) an Incident Request; or

(b) a Service Request.

8.13 Once we have classified the Service Ticket, the CEM or Service Desk team will assign one of the Priority Levels set out in Table 1, using the Impact and Urgency matrix in Table 2:

Table 1

Priority Level	Definition
P1 - Critical	A critical Incident causing a complete system outage or unavailability of a major business function.
P2 - High	A high-priority Incident significantly impacting business operations but with a workaround available.
P3 - Medium	A medium-priority Incident affecting a single user or minor functionality, without major disruption.
P4 - Low	A low-priority Incident or with minimal impact on business operations.

Table 2

		URGENCY			
		Critical *No work can be performed, and your service is down at either a major site or multiple sites.*	**High** *Significant impact to work being performed, work around available, but not sustainable.*	**Medium** *Unable to perform some work tasks, but most business operations can continue.*	**Low** *Information requests / low priority work tasks.*
IMPACT	**Critical** *Entire Approved Environment inoperable across the total user population, severe impact on business operations; no workaround available; immediate attention required.*	Priority 1 - Critical	Priority 1 - Critical	Priority 2 – High	Priority 3 - Medium
	High *Major functionality impaired; workaround available but not sustainable long-term.*	Priority 1 - Critical	Priority 2 - High	Priority 2 – High	Priority 3 - Medium
	Medium *Limited impact on business operations; manageable inconvenience.*	Priority 2 - High	Priority 3 - Medium	Priority 3 – Medium	Priority 3 - Medium
	Low *No significant impact on business operations; cosmetic or non-urgent issues.*	Priority 3 - Medium	Priority 4 - Low	Priority 4 - Low	Priority 4 - Low

Service Request

8.14 If we classify a Service Ticket as a Service Request, it will be considered Priority 3 - Medium by default, unless we reasonably believe it should be a higher priority (applying the Impact and Urgency matrix in Table 2 above).

Service Level Targets

8.15 We aim to meet the Response and Restoration Service Level Targets for the TBMS as set out in this clause and clause 8.17, respectively:

Service Level Measure	Response Time Target	Minimum Service Level (MSL)	Description
Call Answered Rate	within 60 seconds	80%	Measures the % of calls answered within 60 seconds of reaching the appropriate queue. During periods of high call volume: 1) you will be offered a Callback option; or 2) your call will be routed to the Service Desk.
Call Abandonment Rate	After 60 seconds	5%	
Email Response	Within 2 hours	65%	Acknowledgement of issue and response with a tracking details.
Incident – First contact to Technical Contact	Priority 1 = 30 min	50%	This is a technical response metric.
	Priority 2 = 2 hrs	50%	
	Priority 3 = 6 hrs	50%	
	Priority 4 = 35 hrs	50%	

8.16 Response Times are calculated either:

(a) for an Incident Request, using the Priority Level set out in the table in clause 8.15; and

(b) for a Service Request, using the time we issue the Service Ticket to you.

8.17 The Table below sets out the Service Restoration Time Target that applies to your Service for Incidents only.

Service Level Measure	Service Restoration Time Target
Priority 1	4 hours
Priority 2	24 hours
Priority 3	4 Business Days
Priority 4	8 Business Days

Service Level Credits

8.18 If we fail to meet the MSL targets for a Service Level Measure (**Service Level Default**), you must notify us in writing if you wish to claim Service Credits.

8.19 If a response event is any of the SLA events under clause 8.15:

(a) a minimum of 10 response events per month; or

(b) where events are calls-related, a minimum of 10 calls per month,

are required for the calculation of Service Credits.

8.20 If we receive a notice from you under clause 8.18, we will investigate the issue, and if we agree (acting reasonably, based on the evidence available to us on our systems) that there has been a Service Level Default, we will pay you the corresponding Service Credit amount (**Service Credit Payable**) in accordance with clause 8.22.

8.21 Service Credits are only applicable to Managed Services and Solutioned Services, not to Professional Services.

8.22 Any Service Credit Payable is calculated in the following way:

Service Credit Payable = A x B x C

where:

A = **Capped Monthly Service Fee**, being the Monthly Service Fee in respect of the relevant Managed Service multiplied by twenty percent (20%).

B = **Service Level Credit Percentage** (%), being the number of transactions within the measurement period, which has achieved the MSL as a proportion of overall transactions expressed as a percentage divided by the Minimum Service Level, as set out in the table below (**Service Level Performance Rate**).

The Service Level Performance Rate will sit in one of three threshold bands each of which has a Service Level Credit Percentage (%) that is payable to the Customer for a Service Level Default, as detailed in the table below:

Service Level Performance Band	Service Level Credit Percentage %
Band 1: >95%	0%
Band 2: 90 – 95%	50%
Band 3: <90%	100%

C **= Service Credit Weighting** (%) the percentage weighting applied to the SLA Group, as set out in the table below under the column titled “Service Credit Weighting”. The highest weighting has been applied to the SLA requirements to prioritise the shortest response time to you.

SLA Group	SLA Requirement	Minimum Service Level (MSL)	Service Credit Weighting
Phone Call	Call Answer Rate within 60 seconds	80%	15%
	Call Abandonment Rate after 60 seconds	5%	5%
Email Response	Response within 2 hours	65%	15%
Incident	First contact to technical contact measurement. This is a technical response metric	P1 = 50%	20%
		P2 = 50%	20%
		P3 = 50%	15%
		P4 = 50%	10%
Total Weighting			**100%**

8.23 Subject to clauses 8.18 and 8.20, we will include any applicable Service Credits accruing as a credit against the Monthly Service Fees on the invoice issued by us within 90 days of the date the Service Credit accrued. If no more Monthly Service Fees are payable in relation to the relevant Managed Service, we will pay the Service Credits to you in the two months after the Service Credits are incurred.

8.24 The total amount of Service Credits credited or paid to you in respect of all Service Level Defaults occurring under a Managed Service in any one month must not exceed the capped Monthly Service Fee.

8.25 If a single Incident results in the failure of us meeting more than one Service Level, you may select only one of the relevant Service Level Defaults for which you will receive a Service Credit.

Service Level exclusions

8.26 We are not responsible for a failure to meet a Service Level Target to the extent it arises as a result of:

(a) a breach of your obligations under this TBMS section of Our Customer Terms (or your separate agreement with us), or the terms of any Application Form or Order, or is otherwise caused by you;

(b) your negligent acts or omissions;

(c) any period of scheduled maintenance;

(d) any interference to your or your third party provides services or other technology that supports your Approved Environment that is out of our direct control;

(e) any unauthorised changes or misconfiguration made by you or a third party to your technology infrastructure, software or configurations;

(f) suspension or termination of your right to use or access the TBMS;

(g) failure by you to provide a Customer Pre-Requisite and / or perform a Customer Ongoing Responsibility, or provide information reasonably required by us to perform the TBMS;

(h) your breach of Law;

(i) a failure caused by a third party (other than our contractors);

(j) circumstances outside of our reasonable control;

(k) any third-party software or equipment used, operated or interfaced with your Approved Environment not provided by us;

(l) service or resource reductions requested or approved by you (in writing) provided that we previously notified you in writing that the implementation of such request would result in a Service Level Default;

(m) your failure to conduct repair on equipment that has been identified and agreed in writing to be unserviceable;

(n) not providing us with full and accurate information detailing any requests or relating to any Incident Request or Service Request reported to us;

(o) failing to follow our reasonable directions which directly impacts the Approved Environment;

(p) any failure which requires device/hardware replacement or on-site visits; and

(q) any device which is not connected on the network and is not remotely accessible, where sufficient troubleshooting has been done and demonstrated by us to your reasonable satisfaction.

8.27 We may not carry out all requests or rectify all Incident Requests as part of the Service Levels and may charge you for our reasonable costs incurred in identifying, examining and rectifying any of the following Incident Requests or Service Requests caused by you or any other party:

(a) where you breach:

(i) your obligations under this TBMS section of Our Customer Terms (or your separate agreement with us), or the terms of any Application Form or Order;

(ii) the responsibilities assigned to you in relation to the relevant products as part of the Approved Environment; or

(iii) any documents provided by us as part of the Approved Environment;

(b) due to a change, act or omission made by you, which causes damage and/or service degradation to physical or virtual environments supported under the TBMS;

(c) as a result of software (that is not provided by us or our contractors) being incompatible with a product, service or feature provided by us; or

(d) any support and maintenance outside our responsibilities.

Data Collection

8.28 You agree that we may collect and use your:

(a) system health data;

(b) change data;

(c) Service Ticket history; and

(d) any other relevant data necessary to carry out Support Requests,

in relation to your Approved Environment and as necessary to provide the TBMS.

Service Reports

8.29 We will provide you with a service report as set out in the individual Managed Service sections, in the format we determine from time to time, by making it available in the Service Portal.

9 ADDITIONAL SERVICE TERMS

9.1 We provide TBMS on the condition that you comply with the terms in this clause 9.

Your obligations

9.2 You must (unless we advise you otherwise):

(a) complete the Pre-Requisite Order Form that we provide to you, confirming your requirements and defining the design and layout within the Approved Environment to be covered by TBMS;

(b) have and maintain valid and current licences (or an alternative licence as notified by us from time to time in accordance with clause 9.8(c)) if required for each Managed Service;

(c) assess the applicability to your business and operations of the deliverables and TBMS and any recommendations, advice or instructions provided by us in the course of providing the TBMS;

(d) determine whether the TBMS and deliverables, including any revised business processes implemented:

(i) meet your business and compliance requirements; and

(ii) comply with your applicable internal policies and any related agreement;

(e) ensure that your appropriate business owners and technical staff can attend or participate in our scheduled meetings, workshops and remote support as needed for us to perform the TBMS;

(f) provide us with an accurate, up to date, high-level detail on your internal IT services and strategy;

(g) create, maintain and if required, delete the identity of Users of TBMS, unless we agree otherwise;

(h) provide us with appropriate administration credentials and remote access to hardware and systems, so that we can administer, manage and support the Approved Environment on your behalf, as per these Our Customer Terms;

(i) provide us with disaster recovery plans and business continuity plans;

(j) approve changes to cloud configurations required for Disaster Recovery;

(k) raise change requests for Disaster Recovery-related infrastructure updates;

(l) conduct application testing during annual Disaster Recovery failover exercises;

(m) provide site-to-site connectivity between your Approved Environment and our management platform as required;

(n) provide the user/group mappings and data classification required to configure policies;

(o) perform backups of all data contained in or available through the Devices connected to your Approved Environment (where we are managing your Approved Environment, we will provide sufficient access to allow you to perform backups of all data contained in or available through the Devices connected to your Approved Environment);

(p) ensure that Devices remain connected and capable of syncing and receiving updates;

(q) maintain and keep passwords up-to-date;

(r) ensure that your business internet connectivity is working and allow our remote monitoring and diagnostic tools to access and utilise your business Internet connectivity for delivering the TBMS (including obtaining any required consents or approvals and opening required network ports);

(s) take reasonable steps to notify us under clause 8, if a Device is lost or stolen;

(t) ensure timely provisioning of licences for any relevant licences; and

(u) comply with any other reasonable request we make in relation to your TBMS.

9.3 If you are unable to perform your responsibilities set out in clause 9.2, we may not be able to provide the TBMS you are seeking at all, or in full.

9.4 We may seek additional items and information from you as indicated in the individual Managed Services sections below, the Order or Application Form (if applicable).

Your responsibilities

9.5 You acknowledge that the performance of TBMS is dependent on your timely and effective performance of your responsibilities and that you make and communicate to us timely decisions.

9.6 You will provide us with access to your subject matter resources, to facilitate the provision of TBMS. Any security deliverables provided to you as part of TBMS are intended for your own internal use. These security deliverables are not intended for use in any legal proceedings.

9.7 You acknowledge and agree that we are not responsible or liable for:

(a) any unauthorised access to, loss or damage to data (including personal data stored on your Device);

(b) disruption you incur or suffer in connection with our implementation of your TBMS;

(c) any rollback, audit and coverage gaps or failures, performance and access issues, delays, administrative lockouts, unauthorised changes or errors in provisioning caused by your administration, unsupported models or account structures, Access Controls, misconfigured Multi Factor Authentication (**MFA**) or incorrect or incomplete data;

(d) any security events that occur due to delayed implementation of patching as part of these TBMS you have acquired for (unless we are responsible for undertaking patching and we delay implementing a patch made available to us in breach of these terms);

(e) malware infections resulting from User actions or third-party software;

(f) any delays in threat resolution due to third-party tool limitations or integration issues;

(g) service disruptions caused by outages, including missed or dropped calls;

(h) governance failures resulting from misconfigured tenant settings;

(i) failure by a third-party vendor to provide a patch that addresses new vulnerabilities,

except to the extent caused or contributed to by our negligence or breach of Our Customer Terms (or separate agreement with you).

9.8 You acknowledge and agree that:

(a) only supported Managed Services within the Approved Environment will be onboarded;

(b) only features in your licence will be supported, regardless of your selected Service Tier;

(c) if the inclusions in your underlying licences changes (for example, Microsoft 365 for Business), it may be necessary for you to acquire a different licence or different level of licence to continue to acquire your service from us and we will advise you if this is the case;

(d) patching may not prevent any or all security events, and that Device enrolment and policy application may create false positives, unintended restrictions and may affect settings, configuration, enrolment actions and User experience;

(e) any hardware or Devices must either be in warranty or still be eligible for limited or extended support by the vendor during the period of support, unless otherwise agreed in writing; and

(f) automatic enforcement actions (including DLP) may affect User experience and data access; false positives may occur and will be tuned as agreed. It is your responsibility to identify business-critical exceptions prior to enforcement.

9.9 Without limiting clause 9.10, with respect to existing security vulnerabilities as at the Commencement Date for the relevant TBMS, we will only be responsible for fixing such vulnerabilities to the extent included in the scope of the TBMS purchased by you.

Warranties

9.10 We do not represent or warrant to you that TBMS will:

(a) detect or identify all security or network threats to, or vulnerabilities of your networks or other facilities, assets, or operations;

(b) prevent all intrusions into or any damage to your networks or other facilities, assets, or operations;

(c) return control of your or third party systems where unauthorised access or control has occurred; or

(d) meet any particular industry standard or requirement (including the payment card industry data security standard), except for the ACSC Essential 8 applicable maturity level guidelines where specified, and in that case only provided that:

(i) you acquire that Managed Service from us;

(ii) you meet any applicable requirements, as set out in the relevant TBMS description and implement any relevant security controls; and

(iii) if you elect not to implement a security control applicable for a maturity level, we do not represent or warrant that the services will meet the relevant Australian Cyber Security Centre Essential 8 maturity level.

Required permissions and consent

9.11 You acknowledge that, in providing TBMS, we may access, monitor and interact with your or a third party's computer environment, network, equipment, software and related services (**Systems**) and data (including, but not limited to, logs and configurations).

9.12 You consent and must provide any necessary third party permissions, consents or authorisations necessary for us to access, store, process and use such Systems and data (including Personal Information) to perform and improve TBMS. This includes such consents and permissions as are necessary and appropriate to enable us:

(a) to collect, process, store or transfer any data (including Personal Information) through third party systems or cloud service providers for the purposes of the provision, support and improvement of TBMS;

(b) collect, store, use data (including the types and uses of Personal Information set out in our Privacy Policy) and share it with organisations that are located in Australia, Canada, United States, India and Malaysia for the purposes of the provision of TBMS;

(c) collect and analyse operational, usage, and performance data generated through the provision of TBMS, which may be used in an anonymised and aggregated form for service optimisation, analytics and development purposes;

(d) install and/or implement changes to configurations, systems, software, or network settings necessary for the provision and maintenance of TBMS, as authorised by you;

(e) gain management access for Devices and equipment as part of your Approved

Environment, as part of the TBMS purchased by the you;

(f) conduct security monitoring activities required for the protection and performance of your Systems covered by the scope of the TBMS purchased;

(g) obtain user administration access to your Microsoft Azure environment (where relevant), which may include Azure portal access with appropriate role-based Access Control (**RBAC**) permissions, Azure Resource Manager (**ARM**) APIs and templates, Azure Monitor, Log Analytics, and Security Centre, Azure Active Directory (**AAD**) integration, as required for identity and access management to the extent necessary to deliver the TBMS; and

(h) obtain any access to any other Azure services or tools necessary for us to fulfill our obligations.

You are also responsible for obtaining any necessary consents, permissions, or authorisations from your own Users, Authorised Users, employees, customers, or third parties whose data or systems may be impacted by the TBMS. You agree that we can rely on the authority of any of your personnel who tell us that they have authority to give consent on behalf of you.

Customer Tools

9.13 You acknowledge that, unless included in the Order and/or Application Form, you are responsible for:

(a) obtaining consent from any applicable third party for us to use or access the tools or software necessary for the provision of the TBMS purchased by the you (**Customer Tools**);

(b) unless included in the scope of the TBMS, designing, implementing and maintaining the Customer Tools;

(c) providing us with access to the Customer Tools, including without limitation, access to virtual or physical infrastructure required for the Customer Tools; and

(d) providing and ensuring adequate network bandwidth between the Customer Tools and your endpoints.

9.14 The TBMS is not designed to fulfil any particular legal or regulatory function or obligation, except expressly set out under this TBMS section of Our Customer Terms. You are fully responsible for ensuring that your security meets any specific regulatory requirements, industry self-regulatory codes, business requirements, and comply with your applicable internal guidelines and otherwise meets your business requirements.

WHS

9.15 If you purchase on-site Professional Services, you must:

(a) ensure that the serviced site does not pose risk to the health and safety of our personnel; and

(b) ensure that the personnel performing the TBMS on site are not exposed to risk to their health and safety as a result of your business or undertaking, including the conduct of your employees, contractors, subcontractors or other workers. We may remove personnel from a serviced site at any time, where, in our reasonable opinion, that personnel's health or safety is compromised.

9.16 If we become aware of information accessed through your System or provided by your personnel that reveals criminal activity, we will use all reasonable efforts to notify you without delay. You acknowledge that we may, notwithstanding any obligations of confidentiality under Our Customer Terms (or your separate agreement with us), notify applicable law enforcement agencies directly if we reasonably consider it is required by applicable Law to do so. We may provide such law enforcement agencies with all relevant information concerning such criminal activity, if required by applicable Law.

9.17 We may be required to disclose Personal Information in response to a request under a Law or perform mandatory reporting under a Law to governmental authorities in connection with information that comes to our attention while performing the TBMS.

Tools

9.18 You may receive access to some or all the following Tools:

(a) **ServiceNow**: This tool may be used to log Incidents as part of your use of the TBMS. You are, subject to compliance with clause 9.19 and 9.20, granted a non-exclusive, non-transferable right during the period you are paying for the TBMS to access the ServiceNow platform solely for the purpose of using and receiving the TBMS;

(b) **Google Chronicle**: Where you have ordered a premium tier Managed IT Services Bundle, you consent to perform the TBMS and to access and process any data related to the TBMS and represents that such access and processing does not violate any applicable Law or obligation you owe to a third party; and

(c) **Genwizard**: You may receive access to a dashboard generated by the AI Tool GenWizard during the period you are paying for the TBMS. GenWizard will not be deployed in your environments and any Gen-AI outputs would not be deliverables under your agreement. By using this service, you confirm you hold and provide all rights and consents necessary to access, host, process, modify, transfer, and otherwise use Customer Data in connection with the use of GenWizard (including any Gen AI product integrated with GenWizard) to perform the TBMS. You do not receive any Intellectual Property Rights in the Genwizard Tool. You will not and will not permit any other person to distribute GenWizard screenshots or GenWizard screen recordings to a third party, other than to Telstra, a Telstra Related Body Corporate, the Customer’s Telstra channel partner or any subcontractor for the purposes of using and receiving the TBMS,

together, **Tools**.

We will not provide any source code in relation to these Tools.

9.19 When using, or engaging with the Tools in relation to the TBMS, you must:

(a) comply with all applicable Laws;

(b) not knowingly post, distribute, or otherwise make available or transmit any software or other computer files that contain a virus, trojan horse, or worm or similar;

(c) not use any Tool or the TBMS for any purposes that breach any Laws;

(d) not maliciously interfere with or disrupt networks connected to the Tools or TBMS or knowingly cause the Tools to malfunction;

(e) not use the Tools or the TBMS to infringe any third party's copyright, patent, trademark, trade secret or other proprietary rights or rights of publicity or privacy; and

(f) not knowingly or negligently transmit in breach of any applicable Laws any materials that are abusive, deceptive, obscene, defamatory, offensive, threatening, harassing, hateful, indecent or pornographic, or otherwise contain materials that include child sexual exploitation material.

9.20 You must not (and must not permit others to):

(a) alter, enhance or otherwise modify any Tool or software used to provide TBMS;

(b) sublicense, sell, resell, rent, copy, lease, distribute, timeshare or otherwise transfer or make available to third parties any access or usage rights granted with respect to the Tools;

(c) disassemble, decompile, translate, reverse engineer or otherwise attempt to derive or extract any or all of the source code of any Tools or create derivative works or competing product or service based on the Tools (including by creating a custom application that replicates the exact automation by a Tool) or otherwise seek to modify the Tools; or

(d) remove, modify or destroy any copyright or proprietary markings, confidential legends or any trademarks or trade names placed upon or contained within the any Tools or documentation.

9.21 In addition to clauses 9.19 and 9.20, in relation to Google Chronicle, you must not and must not allow a third party to use Google Chronicle to:

(a) promote or encourage illegal activity or violate or promote the violation of the legal rights of others;

(b) gain unauthorised access to, disrupt, or impair the use of the Google Chronicle, or the equipment used to provide the Google Chronicle, by other customers, authorised resellers, or other authorised users;

(c) generate, distribute, publish or facilitate unsolicited mass email, promotions, advertisements, or other solicitations; or

(d) use the Google Chronicle or interfaces provided to access any other Google product or service.

9.22 You will be solely responsible for:

(a) maintaining your current maintenance and technical support contracts with your third-party vendors (**Vendors**) for any device(s) receiving Google Chronicle;

(b) ensuring any device(s) receiving the Google Chronicle conform to the version requirements we tell you about;

(c) interacting with Vendors to ensure that the device(s) are scoped and implemented in accordance with Vendors' recommended standards;

(d) interacting with Vendors regarding the resolution of any issues related to device(s) scoping, feature limitations or performance issues;

(e) remediation and resolution of changes to device(s) which negatively impact Google Chronicle or the functionality, health, stability, or performance of device(s); and

(f) assessing (and as applicable, implementing) any recommendations, advice and/or instructions provided in the course of providing the Google Chronicle.

9.23 You may ask us to provide assistance with remediation or resolution activities. If we agree, additional terms and conditions will apply.

9.24 You acknowledge and agree that:

(a) we retain, use and analyse information derived from your use of the Google Chronicle (in a de-identified manner), including indicators of compromise, malware, anomalies, or other information that may be found as part of, or related to the performance of the Google Chronicle for the purposes of gathering and compiling security event log data to look at trends and real or potential security threats, improving and developing security products and services, preparing and distributing statistical reports related to security trends and data patterns, internal research, and for providing general security related services;

(b) in the course of using Google Chronicle, we may become aware of issues such as data breaches, network intrusions, or the presence of malware, and that such issues may give rise to regulatory reporting obligations which you are subject to in one of more jurisdictions; and

(c) you will remain solely responsible for all such reporting requirements, and we shall have no liability in this regard, unless it is required by Law to report.

Solutioned Services

9.25 Where you request Solutioned Services, any proposal will include specific terms which apply to those services in the relevant Application Form.

Cyber Threat Intelligence

9.26 The following Cyber Threat Intelligence (**ACTI**) terms will apply if ACTI is used to provide the TBMS purchased by you:

(a) The TBMS proprietary ACTI Threat Intelligence content (**Content**) consists of:

(i) information about both public and unpublished zero day vulnerabilities derived from multiple public sources and internal research;

(ii) streams of threat indicators that assist in detecting cyber-attacks; and

(iii) other cyber intelligence information, alerts, analytical tools, and interactive visualisations.

(b) You may use such Content as may be provided to it solely for the purposes of management and protection of your networks, systems and assets through the TBMS. This right cease on expiry or termination of your TBMS.

(c) You will not remove any confidentiality, copyright or other markings from any Content or transfer or distribute the Content or any portion thereof to third parties. The Content is our confidential information and, to the extent permitted by Law, is provided to you on an "as is', "where is" and "as available" basis.

(d) You acknowledge and agree that the ACTI API will be disconnected by us upon expiration or earlier termination of the TBMS for any reason.

9.27 We may exercise or enforce any of the rights in this clause 9 through, or for the benefit of, any subcontractors or third party service providers we use in providing the TBMS (including by sublicensing rights to them).

10 EXCLUSIONS

10.1 The TBMS does not include:

(a) inclusions, features or capabilities that are not expressly included in the TBMS or Service Tier(s) you have selected;

(b) underlying software plans or licences;

(c) initial setup of any software and licences;

(d) installation of software and support on out of scope Devices;

(e) training of any kind, including how to operate or use any software functionality;

(f) the supply and installation of hardware, applications or Devices and installation, cabling, or any other underlying requirements, equipment or infrastructure installation unless explicitly specified in the applicable Application Form and/or Order (this includes cabling or any other works requiring civil works and accreditations (such as electrical and plumbing));

(g) monitoring, alerting and reporting on devices not included in your Approved Environment;

(h) management or administration of any software other than as expressly set out in this section of Our Customer Terms, the applicable Application Form and/or Order;

(i) support in relation to any service outages or downtime caused by issues within the service operating systems or Microsoft platform (outside your direct tenancy);

(j) troubleshooting, support, and resolution activities for any ICT component impacting the M365 Services and application experience unless expressly included as part of a Managed IT Services Bundle or a separate related ICT Single Tier Service;

(k) asset inventory and tracking, including tracking or managing the inventory of hardware and software assets;

(l) creation, maintenance, or deployment of golden images for Devices;

(m) integration with non-Microsoft Intune RMM tools like System Center Configuration Manager (**SCCM**) or other Remote Monitoring and Management (**RMM**) tools, except for Microsoft Intune;

(n) non-Microsoft BIOS update/patching including BIOS updates, upgrades, or patching activities for hardware that are not Microsoft-based;

(o) unsupported, non-compliant, or custom-built Devices, or any operating system not listed as in-scope for TBMS;

(p) creation, deletion, or management of User accounts for platforms other than Microsoft; and

(q) any other item or work not expressly described in this section of Our Customer Terms (or your separate agreement with us), the applicable Application Form and/or Order, as being part of the TBMS.

11 TERMINATION

Termination

11.1 You may terminate your TBMS (in whole or in part):

(a) for a Casual Term or Renewal Term for TBMS, on at least 30 days' prior written notice; or

(b) for a Fixed Term, on at least 90 days' prior written notice.

We will charge you up to and including the last day of your notice period. Early Termination Charges may also apply, as set out in clause 11.3.

11.2 We can terminate any or all of your TBMS, if you:

(a) commit a material breach of Our Customer Terms (or your separate agreement with us), the applicable Application Form and/or Order;

(b) cause a defect or Incident by improper or negligent use of TBMS; or

(c) do not allow us access to your Approved Environment in order for us to maintain the TBMS,

and fail to remedy that breach, defect, Incident or access issue within a reasonable time of receiving a notice from us requiring you to do so.

11.3 You must pay Early Termination Charges if you have a Fixed Term Order and we terminate your TBMS under clause 11.2.

Migration

11.4 We may transfer you to a reasonably comparable alternative service during your then-current term (whether a Casual Term or Fixed Term) by giving you prior written notice. If we transfer you to a reasonably comparable alternative service and this has more than a minor detrimental impact on you, you may cancel that part of your TBMS without having to pay an Early Termination Charge for that service.

Early Termination Charges

11.5 Early Termination Charges for TBMS only apply to Managed Service Orders on a Fixed Term.

11.6 If you or we terminate or downgrade your TBMS during your Fixed Term for any reason other than our material breach, you have to pay us the Early Termination Charges for that TBMS.

11.7 The Early Termination Charges for the TBMS payable will be equal to one month’s charges for the terminated Managed Service, in addition to the charges payable under clause 11.1, or as set out in your Order.

11.8 You acknowledge the Early Termination Charges are a genuine pre-estimate of the loss we are likely to suffer if a Fixed Term Managed Service is terminated early.

11.9 Early Termination Charges do not apply to Professional Services or Solutioned Services.

PART B – MANAGED SERVICES

(A) MANAGED IT SERVICES BUNDLE

12 ABOUT MANAGED IT SERVICES BUNDLE

12.1 This is the Managed IT Services Bundle part of this TBMS section of Our Customer Terms.

12.2 Other terms also apply to the Managed IT Services Bundle. For more information about the other terms that apply and how they work together, see clause 1 of this TBMS section of Our Customer Terms.

13 MANAGED IT SERVICES BUNDLE

13.1 Managed IT Services Bundle provides you with end-to-end IT solutions across Network Management, Managed Endpoint, Managed Collaboration, Managed Cyber Security and Managed OneDrive Backup, as further set out in this section of Our Customer Terms, the individual Managed Service sections of Our Customer Terms and your Order.

13.2 If you elect to have a Managed IT Services Bundle, the service components will be aligned to the Essential 8 Controls. The Essential 8 Controls section of this TBMS section of Our Customer Terms describes the Essential 8 Controls.

13.3 The features vary between the Service Tiers of Basic, Standard, and Premium, as summarised in the following table:

Managed IT Services Bundle	Basic	Standard	Premium
Essential 8 Controls	Level 1	Level 2	Level 3
Network Management	Basic	Standard	Premium
Managed Endpoint	Basic	Standard	Premium
Managed Collaboration	Basic	Standard	Premium
Managed Cyber Security	Basic	Standard	Premium
Managed OneDrive Backup	Basic	Standard	Premium

Eligibility

13.4 To be and to remain eligible to acquire a Managed IT Services Bundle, you must:

(a) have and maintain a valid and current Microsoft 365 licence applicable to your Service Tier:

(i) **Basic and Standard**:

(A) less than 300 Employees: Microsoft 365 Business Premium licence and Microsoft Defender for Endpoint Plan 2: or

(B) 300 or more Employees: E3 licence with E5 Security Add-On;

(ii) **Premium**: an E5 licence; and

(b) maintain an Azure subscription with a storage account for service operations;

(c) comply with any Customer Pre-Requisites and any eligibility criteria indicated in the applicable individual Managed Services sections; and

(d) maintain all services included in the Managed IT Services Bundle.

14 FEES AND ACTIVATION

Fees

14.1 If you select a Managed IT Services Bundle, the applicable fees and charges for your service:

(a) will be charged on a per User basis;

(b) will be billed monthly in arrears; and

(c) are calculated on a daily basis for each day of the relevant month as follows:

A = B x C

where:

A is the fees and charges payable by you for your service for the relevant day;

B is the number of Active Users for that day; and

C is the applicable rate per Managed IT Services Bundle (as set out in the Telstra Business Managed Services Rate Card).

14.2 Fees will vary depending on the relevant Service Tier.

Activation

14.3 If you select Managed IT Services Bundle, it is considered active and charging commences, once all services included in the Managed IT Services Bundle are onboarded and active.

15 SERVICE COMPONENTS

15.1 The service components of your Managed IT Services Bundle will vary depending on the structure of your TBMS. For more information about the service components of your Managed IT Services Bundle, please see the individual Managed Services part of this TBMS section of Our Customer Terms.

15.2 The Service Tier for your Managed IT Services Bundle is set out in your Order.

Network Management Device Inclusions

15.3 Network Management, when purchased as part of a Managed IT Services Bundle, includes the management of the greater of:

(a) up to five Network Devices per customer; or

(b) one Network Device for every two Users (rounded down).

15.4 If you require more Network Devices under management (**Network Management Additional Device**), you can request Network Management Additional Devices from time to time.

15.5 You will be required to pay an additional fee for any Network Management Additional Devices, as set out in your Order.

16 EXCLUSIONS

16.1 Managed IT Services Bundle does not include:

(a) inclusions, features or capabilities that are not expressly included in the Service Tier you have selected; and

(b) any other item or work not explicitly described in the individual Managed Service section of Our Customer Terms as being part of Managed IT Services Bundle.

16.2 If you choose to acquire the Managed IT Services Bundle, you will not be able to take up Managed Endpoint, Managed Collaboration, Managed Microsoft Defender and Network Management service options as Standalone Managed Services.

17 YOUR OBLIGATIONS

You must comply with any obligations set out in the individual Managed Service sections and Common Terms of Our Customer Terms for TBMS.

(B) THE ESSENTIAL 8 CONTROLS

18 ABOUT THE ESSENTIAL 8 CONTROLS

18.1 This is the Essential 8 Controls part of this TBMS section of Our Customer Terms.

18.2 Other terms also apply to the Essential 8 Controls. For more information about the other terms that apply and how they work together, see clause 1 of this TBMS section of Our Customer Terms.

19 THE ESSENTIAL 8 CONTROLS

19.1 The Essential 8 Controls are aligned to the Australian Cyber Security Centre (**ACSC**) 'Essential Eight Framework' and provide a baseline of security strategies to help mitigate cyber security risk and/or data loss across your Managed IT Services Bundle.

19.2 The Essential 8 Controls are divided into four Maturity Levels, with each level adding a new level of security. The Maturity Levels provide a framework for assessing how you have implemented each baseline security strategy.

Eligibility

19.3 The Essential 8 Controls can only be acquired as part of a Managed IT Services Bundle and the eligibility criteria of the bundle apply. Please refer to the Managed IT Services Bundle part of this TBMS section of Our Customer Terms for eligibility.

20 FEES AND ACTIVATION

The applicable fees, charges and activation criteria for the Essential 8 Controls are set out in the Managed IT Services Bundle part of this TBMS section of Our Customer Terms.

21 SERVICE COMPONENTS

21.1 The features vary between the Service Tiers of Basic, Standard, and Premium, as summarised in the following table:

Service Tier		**Basic**	**Standard**	**Premium**
Aspect of Managed IT Services Bundle	**Essential 8 Controls**	**Maturity Level 1**	**Maturity Level 2**	**Maturity Level 3**
Managed Endpoint	Onboarding of Devices to Microsoft Intune.	✓	✓	✓
	Configuration policy set up of Microsoft Intune, Entra and Defender.	✓	✓	✓
	Microsoft Defender Antivirus Policy deployment.	✓	✓	✓
	Patch management of applications and operating systems.	✓	✓	✓
	Automation set up for enforcement, patching, scanning and alerting.	✓	✓	✓
	24/7 automated monitoring using the Microsoft Intune Console.	✓	✓	✓
	Inventory management of applications, endpoints and Users.	✓	✓	✓
	Access Control, including: • access allowlisting for approved executables; and • centrally managed allowlisting solution on workstations and servers.	✓	✓	✓
	Configuration of Microsoft Office Macros to block macros from the internet and allow only macros which are digitally signed or from trusted locations.	✓	✓	✓
	Hardening, including: • disable flash, ads and Java in web browsers; and • block web advertisements and access to risky sites.	✓	✓	✓
	Restrict administrative privileges, including: • restrict admin rights to specified Users; • enable separate accounts for admin and day-to-day work; and • review admin privileges on a quarterly basis.	✓	✓	✓
	Enable MFA for all remote access, including VPN, web apps, and cloud services.	✓	✓	✓
	Daily Backup.	✓	✓	✓
	Integration with Microsoft Defender for real-time detection and response.	✓	✓	✓
	Configuration of host-based firewalls and device-level DLP rules.	×	✓	✓
	Monthly threat and vulnerability management scan.	×	✓	✓
	Policy automation set up (based on User / Device risk posture).	×	✓	✓

Service Tier		**Basic**	**Standard**	**Premium**
Aspect of Managed IT Services Bundle	**Essential 8 Controls**	**Maturity Level 1**	**Maturity Level 2**	**Maturity Level 3**
Managed Collaboration	Patch Operation Systems (in 2 weeks).	×	✓	✓
	24/7 SOC and SIEM integration.	×	×	✓
	Application allowlisting using Windows Defender Application Control.	×	×	✓
	PowerShell logging, secure boot enforcement, vulnerability remediation workflows.	×	×	✓
	Level 3 policy enforcement for USB control, clipboard protection and browser hardening.	×	×	✓
	Centralised management of controls.	×	×	✓
	Logging and monitoring.	×	×	✓
	Tamper resistance implementation.	×	×	✓
	Backup, application controls and recovery process testing.	×	×	✓
	Mailbox provisioning and basic Microsoft 365 access.	✓	✓	✓
	MFA including enabling MFA and Microsoft Entra Conditional Access for all remote access, including VPN, web apps and cloud services.	✓	✓	✓
	Configure Exchange Online Protection on M365.	✓	✓	✓
	Incident and service request handling during Business Hours.	✓	✓	✓
	Configuration of Microsoft Entra Conditional Access Policies and DLP rules in Microsoft Exchange and Microsoft Teams.	✓	✓	✓
	Shared mailbox and distribution list administration.	✓	✓	✓
	Configuration and management of features in Microsoft Defender for Office 365 Plan 1, including: • Safe Links; • Safe Attachments; and • Microsoft Defender Anti-Phishing Policies.	×	✓	✓
	Configuration and management of features in Microsoft Defender for Office 365 Plan 2, including: • Automated Investigation and Response (AIR); • Microsoft Threat Explorer and Real-Time Detections; • Microsoft Defender Attack Simulation Training; and • Alerting and Hunting.	×	×	✓
	Access to compliance dashboards and audit logs.	×	✓	✓
	Integration with SOC and SIEM platforms for 24/7 alerting, analysis and containment.	×	×	✓
	VIP mailbox protection and tenant-wide governance.	×	×	✓

21.2 Once you have selected a Service Tier, the Essential 8 Controls will be applied across your Approved Environment during the onboarding of your selected Managed IT Services Bundle.

21.3 Once we have measured your implementation of each baseline security strategy, we will implement Mitigation Strategies as set out below.

Service Tier	Basic	Standard	Premium
Mitigation Strategy	**Maturity Level 1**	**Maturity Level 2**	**Maturity Level 3**
Strategy 1: Patch Applications	• Patch operating systems on a monthly basis. • Use automated tools to identify and deploy patches.	• Patch operating systems in 2 weeks and remove unsupported systems. • Perform threat and vulnerability management scans. • Perform monthly threat and vulnerability scan on your Approved Environment.	
Strategy 2: Patch operating systems			
Strategy 3: Multi-factor authentication (MFA)	• Enable MFA for all remote access, including VPN, web apps, and cloud services on Devices. • Enable MFA and Microsoft Entra Conditional Access for all remote access, including VPN, web apps and cloud services on Microsoft messaging and collaboration.		
Strategy 4: Restrict administrative privileges	• Perform the configuration required to restrict admin rights to specified Users. • Perform the configuration required to enable separate accounts for admin and day-to-day work. • Review admin privileges on a quarterly basis.		
Strategy 5: Application control	• Implement access to the application allow listing for approved executables (such as, .exe, .dll and scripts). • Use a centrally managed allowlisting solution on workstations and servers.		• Implement access to the application on your Approved Environment using Windows Defender Application Control (**WDAC**).
Strategy 6: Restrict Microsoft Office macros	• Configure Microsoft Office macros to block macros from the internet and only allow macros that are digitally signed or from trusted locations.		
Strategy 7: User application hardening	• Disable flash, ads and Java in web browsers. • Block web advertisements and access to risky sites.		• PowerShell logging, secure boot enforcement, and vulnerability remediation workflows.
Strategy 8: Regular Backups	• Perform daily backups of data and system configurations.		

Additional activities

21.4 As part of the Essential 8 Controls, and to help deliver the Mitigation Strategies, we will also undertake additional activities:

(a) To align with **Maturity Level 1**:

(i) onboard your Devices to Microsoft Intune;

(ii) configure rules and settings in Microsoft Intune, Entra and Defender to manage Users within your Approved Environment;

(iii) deploy Microsoft Defender Antivirus Policies into your Devices;

(iv) provide 24/7 automated monitoring of your Devices using the Microsoft Intune console;

(v) provision Users with Outlook mailbox and access to Teams and SharePoint as directed by your Authorised Customer Representative;

(vi) configure Exchange Online Protection in M365; and

(vii) Incident and Service Request handling during Business Support Hours.

(b) To align with **Maturity Level 2**:

(i) integrate your Devices with Microsoft Defender for near real-time detection and response;

(ii) configure host-based firewalls and DLP rules on your Devices;

(iii) configure rules and settings in Microsoft Intune, Entra and Defender to manage Users; and

(iv) implement automated policies based on the following risk signals:

Risk Signal	Automated Policy Action
Unpatched Device	Block access, enforce patch
Unknown location/Device	Enforce MFA or block
EDR detection	Isolate host, suspend account
Non-compliant Device	Prevent data sync or wipe
Excessive privilege use	Trigger alert or auto-downgrade

(v) for messaging and collaboration (Microsoft 365 – Outlook, Teams, SharePoint):

(A) configure Microsoft Entra Conditional Access Policies and Data Loss Prevention rules in Microsoft Exchange and Teams;

(B) implement the following controls in shared mailboxes and distribution lists:

Control	Control relevance to mailbox and DL administration
Restrict admin privileges	Limit who can manage mailboxes/DLs, use JIT access, audit changes
MFA	Enable MFA for access and delegation

Application hardening	Disable risky features (such as external sharing and anonymous sending)
Patch and logging	Ensure mailbox/DL platform is patched and access changes are logged

(vi) configure Safe Links, Safe Attachments and Microsoft Defender Anti-Phishing Policies features in Microsoft Defender for Office 365 Plan 1.

(c) To align with Maturity Level 3:

(i) integrate SOC with SIEM to allow the SOC to:

(A) ingest and correlate logs from various sources (such as firewalls and identity platforms);

(B) detect anomalies or threats;

(C) trigger alerts in real time; and

(D) enable investigations and response to Incidents 24/7;

(ii) configure policy enforcement for USB control, clipboard protection and browser hardening as follows:

Control Area	Policy Enforcement Configuration
USB control	Encrypted, allow listed Devices; DLP rules; logging; just-in-time access
Clipboard control	Block between sessions/apps; DLP scanning; logs; restricted access in PAM

(iii) centrally enforce and monitor all controls;

(iv) use automation for enforcement, patching, scanning, and alerting;

(v) the system will log and refer correlation and response to security events to the Service Desk;

(vi) perform testing on backups, application controls, and recovery processes on an annual basis as part of disaster recovery exercises;

(vii) maintain up-to-date inventories of applications, endpoints, and Users;

(viii) configure Automated Investigation and Response, Microsoft Defender Threat Explorer and Real-Time Detections, Microsoft Defender Attack Simulation Training and Alerting and Hunting in Microsoft Defender for Office 365 Plan 2;

(ix) messaging and collaboration (Microsoft 365 – Outlook, Teams, SharePoint) - Integrate SOC with SIEM platforms for 24/7 alerting, analysis and containment by performing the following activities:

Category	Activities
Data ingestion	Connect all Microsoft Defender products to SIEM (Google Chronicle)
Alert management	Configure alert rules, severity, and routing
SOC response playbooks	Automate isolation, token revocation, and email quarantine
Monitoring and analysis	24/7 triage, correlation, threat hunting
Threat intel integration	Enrich alerts with TI feeds and MITRE ATT&CK mappings
Reporting and compliance	Dashboards, KPIs, audit logs, Incident response documentation

(x) messaging and collaboration (Microsoft 365 – Outlook, Teams, SharePoint) - VIP Mailbox Protection and tenant-wide governance.

(d) In order to receive the messaging and collaboration service, you must implement the following in your M365 environment:

(i) configure the VIP mailbox protection feature in Microsoft Defender for Office 365 Plan 2; and

(ii) configure a set of agreed governance controls to be applied across your Microsoft 365 in your Approved Environment.

22 SERVICE LIMITATIONS AND EXCLUSIONS

22.1 We do not guarantee that the Essential 8 Controls implemented through your Essential 8 Controls service will:

(a) detect or identify all security or network threats to, or vulnerabilities of your networks or other facilities, assets, or operations;

(b) in the event of changes or updates to the ACSC 'Essential Eight Framework', align with the current ACSC 'Essential Eight Framework'; or

(c) prevent all intrusions into or damage to your networks, including cyber security breaches or data loss.

22.2 If we identify remediations that are required as part of onboarding, and those remediations will take more than 30 minutes per Device, we will notify you. If you wish us to undertake the remediation, it will be scoped and invoiced for an additional fee as a Professional Services or Solutioned Services engagement.

22.3 You acknowledge and agree that, in the event an update or change to the ACSC 'Essential Eight Framework':

(a) you may be required to implement additional service pre-requisites and/or a Service Tier change;

(b) we may increase the fees or charges for your Essential 8 Control service(s) during your Initial Term or then Renewal Term to the extent necessary to cover the increase in cost to us in implementing such update or change. If you do not agree to the increased rates, you may terminate this service with immediate effect from the date of the fee or charge increase, by giving us written notice; and

(c) if we are unable to offer a pre-requisite or Service Tier change after using reasonable commercial efforts within six months after the relevant update or change to align to the updated or changed ACSC 'Essential Eight Framework', then either party may terminate this service by providing written notice to the other party.

No Early Termination Charges are payable as a result of termination under this clause 22.3.

23 YOUR OBLIGATIONS

You must comply with any Customer Ongoing Responsibilities.

(C) MANAGED ENDPOINT

24 ABOUT MANAGED ENDPOINT

24.1 This is the Managed Endpoint part of this TBMS section of Our Customer Terms.

24.2 Other terms also apply to Managed Endpoint. For more information about the other terms that apply and how they work together, see clause 1 of this TBMS section of Our Customer Terms.

25 MANAGED ENDPOINT

25.1 Managed Endpoint provides you with administration services, automated monitoring, management, and User support for your Devices, as further set out in this section of Our Customer Terms and your Order.

25.2 The features vary between the Service Tiers of Basic, Standard, and Premium, as summarised in the following table:

Managed Endpoint		Basic	Standard	Premium
Patch Management	Monitor OEM software for patches.	✓	✓	✓
	Apply patch updates as required.	✓	✓	✓
	Troubleshoot patch distributions.	✓	✓	✓
Antivirus Management	Define and deploy security policies.	✓	✓	✓
	Monitor and troubleshoot issues.	✓	✓	✓
	Provide quarterly health check reports.	✓	✓	✓
	Manage service level agreements and outbreak reports.	✓	✓	✓
Intune Administration	Manage alerts and notifications.	✓	✓	✓
	Monitor Microsoft Intune status.	✓	✓	✓

Managed Endpoint		Basic	Standard	Premium
	Device Enrolment in Microsoft Intune.	✓	✓	✓
	Create and modify Device configuration and enrolment policies.	✓	✓	✓
Mobile Device Management	Define compliance policies.	✓	✓	✓
	Set up and trigger remote wipe.	✓	✓	✓
	Monitor wipe status.	✓	✓	✓
	Configure and send lock commands.	✓	✓	✓
BIOS Update	Perform BIOS updates as delivered by Windows.	✓	✓	✓
Policy Enforcement	Define and set up compliance policies.	✓	✓	✓
	Assign policies to device groups.	✓	✓	✓
	Monitor policy deployment.	✓	✓	✓
	Ensure compliance and take corrective control using our Desired State Configuration.	✓	✓	✓
	Strict DLP rules with tracking of false positives/negatives.	×	×	✓
	Customize and deploy user- or group-specific security policies.	×	×	✓
	Generate compliance reports and alerts (frequency varies per Service Tier).	✓	✓	✓
Security & Compliance	Enabling and monitoring firewall configurations across endpoints.	×	✓	✓
	Implementing policies to prevent sensitive data exfiltration.	×	✓	✓
Threat Protection	Real-time threat detection and automated response using tools such as Microsoft Defender for Managed Endpoint.	✓	✓	✓
Automation	Dynamic policy application based on Device and User risk posture.	×	✓	✓
Monitoring	Perform 24x7x365 monitoring of all endpoints and mobile devices.	✓	✓	✓
Vulnerability & Threat Management	Scanning for and remediating endpoint vulnerabilities.	×	✓	✓
	Conduct onboarding vulnerability assessments for all new Devices.	×	×	✓
	Schedule and execute regular vulnerability scans.	×	×	✓
Remediation	Plan and implement remediation activities based on SOC/SIEM findings.	×	×	✓
Managed Endpoint Service Report	Compliance reporting.	Monthly	Weekly	Weekly

Additional Managed Endpoints

25.3 Managed Endpoint includes the management of up to two Devices per User (one Device with a desktop OS (Windows or MacOS) and one Device with a mobile OS (iOS, iPadOS, Android). If you require more than two Devices under management (**Additional Managed Endpoints**), you can request Additional Managed Endpoints from time to time.

25.4 You will be required to pay an additional fee for any Additional Managed Endpoints, as set out in the Telstra Business Managed Services Rate Card.

Eligibility

25.5 If Managed Endpoint is acquired as part of a Managed IT Services Bundle, the eligibility criteria of the bundle also apply. Please refer to the Managed IT Services Bundle part of this TBMS section of Our Customer Terms for eligibility criteria.

25.6 To be and to remain eligible to acquire Managed Endpoint, you must:

(a) have and maintain a valid and current Microsoft 365 for Business licence (or an alternative licence as notified by us from time to time), for each Managed Endpoint service:

(i) **Basic and Standard Tier:** Microsoft 365 Business Premium and Microsoft Defender for Endpoint Plan 2 or higher; or

(ii) **Premium Tier:** Either Microsoft 365 Business Premium or E3 with E5 security Add-On or Microsoft 365 E5 licence for each User; and

(b) ensure each Managed Endpoint remains enrolled in your Approved Environment;

(c) maintain an Azure subscription with a storage account for service operations (for example logs, automation and reporting); and

(d) have either:

(i) desktop or laptop Devices (Windows, MacOS); or

(ii) mobile / tablet Devices (Android, iOS, iPadOS).

26 FEES AND ACTIVATION

Fees

26.1 If you select Managed Endpoint as a Managed IT Services Bundle, the applicable fees and charges for Managed Endpoint are set out in the Managed IT Services Bundle part of this TBMS section of Our Customer Terms.

26.2 If you select Managed Endpoint as a Standalone Managed Service, the applicable fees and charges for Managed Endpoint:

(d) will be charged on a per User basis from the date of the relevant licence has been assigned to a User in the Approved Environment;

(e) will be billed monthly in arrears; and

(f) are calculated on a daily basis for each day of the relevant month as follows:

A = B x C

where:

A is the fees and charges payable by you for your Managed Endpoint service(s) for the relevant day;

B is the number of Active Users for that day; and

C is the applicable rate per Managed Endpoint service(s) (as set out in the Telstra Business Managed Services Rate Card).

26.3 Fees will vary depending on the relevant Service Tier.

Activation

26.4 If Managed Endpoint is acquired as part of a Managed IT Services Bundle, the activation criteria of the Managed IT Services Bundle part of this TBMS section of Our Customer Terms apply.

26.5 If you select Managed Endpoint as a Standalone Managed Service, Managed Endpoint will be considered 'active', and we will commence charging for the service when the Device(s) are enrolled in your Approved Environment and assigned to a User.

27 SERVICE COMPONENTS

27.1 The service components of your Managed Endpoint will vary depending on the structure of your TBMS. The service elements and the Service Tier for your Managed Endpoint are set out in your Order.

Managed IT Services Bundle

27.2 If you select your Managed Endpoint as part of a Managed IT Services Bundle, the service components listed under clause 27.4 will be aligned to the Essential 8 Controls.

27.3 The Essential 8 Controls section of this TBMS section of Our Customer Terms describes the Essential 8 Controls.

Managed Endpoint Service Components

27.4 Subject to the selected Service Tier, your Managed Endpoint will include the following elements and be subject to the following terms.

(a) **Patch Management**

(i) Patch management provides centralised management of all elements of the device patching lifecycle for Devices within your Approved Environment (**Patch Management).** This includes:

(A) monitoring OEM software for patches;

(B) defining and implementing a patch distribution schedule; and

(C) troubleshooting of patch distributions.

(ii) You acknowledge and agree that:

(A) software patches must be installed on all in-scope Devices and your Approved Environment;

(B) patching and reporting will only apply to Devices in the Approved Environment;

(C) Devices must remain connected, in vendor support and capable of receiving patches in order properly receive Patch Management; and

(D) any patch installation involves some risk and may require a restart or rollback to restore service.

(b) **Antivirus Management**

(i) Antivirus Management provides centralised control of antivirus software on Devices within your Approved Environment. This includes:

(A) defining and deploying security policies in line with the Desired State Configuration (subject to your specific restrictions in your Order, or as otherwise agreed with you); and

(B) using our ITSM systems to monitor and troubleshoot antivirus-related issues.

(ii) You acknowledge and agree that:

(A) antivirus software must be installed and supported on all in-scope Devices in your Approved Environment;

(B) monitoring and reporting will only apply to Devices in the Approved Environment;

(C) Devices must remain connected and capable of receiving updates in order properly receive Antivirus Management;

(D) where you request a deviation for a business application, you will provide us with accurate details of the impacted setting, the minimum change required, supporting vendor evidence, and a proposed review date; and

(E) we may reject or limit any requested deviation if, in our reasonable opinion, it materially increases security risk or may hinder alignment to recognised hardening frameworks (including the Essential 8 Controls).

(c) **Intune Administration**

(i) Intune administration provides Detective Controls across your Approved Environment (**Intune Administration**). This includes:

(A) the enrolment of Devices into Intune Administration;

(B) creating and modifying Devices configuration and enrolment policies in line with the Desired State Configuration;

(C) monitoring Intune Administration status; and

(D) managing alerts and notifications.

(d) **Mobile Device Management**

(i) Mobile Device Management is a feature that enforces compliance policies, enables remote actions, and maintains visibility over Device status within your Approved Environment. This includes:

(A) defining compliance policies using the Desired State Configuration;

(B) setting up and triggering remote wipe; and

(C) applying remote wipe actions, monitoring wipe status and configuring and sending lock commands when you report a lost or stolen Device to us.

(ii) You acknowledge and agree that if a Device is lost or stolen, you must raise a Support Request notifying us of the Incident.

(e) **BIOS Update**

(i) BIOS Update is a feature that helps maintain firmware currency and platform stability for Devices. This includes:

(A) performing BIOS updates as delivered by Windows using Microsoft Intune for eligible Devices; and

(B) initiating BIOS updates on Devices as delivered by Windows.

(ii) You acknowledge and agree that:

(A) BIOS updates only apply to Supported Technology within the Approved Environment where it runs on Windows 10/11, is Microsoft Intune-enrolled with an unlocked BIOS, meets hardware requirements indicated by us and supports OEM update tools; and

(B) any BIOS update involves risk and may require a restart or rollback to restore service.

(f) **Policy Enforcement**

(i) Policy enforcement provides support to Managed Endpoint compliance by defining, deploying, and monitoring security policies within your Approved Environment (**Policy Enforcement**). This includes:

(A) defining compliance policies using the Desired State Configuration to enforce security standards across Managed Endpoint;

(B) configuring and deploying user or group specific security policies;

(C) applying DLP policies;

(D) monitoring policy deployment;

(E) tracking DLP false positives or false negatives on an ongoing basis; and

(F) generating compliance reports,

as set out in the table in clause 25.2.

(g) **Security and Compliance**

(i) Security and compliance is a core feature that enforces Managed Endpoint protection within your Approved Environment, utilising our Desired State Configuration policy-driven automation, monitoring, and remediation (**Security and Compliance**). This includes:

(A) enabling firewall configurations across endpoints;

(B) monitoring firewall configuration status across endpoints;

(C) implementing policies to prevent sensitive data exfiltration; and

(D) applying Desired State Configuration DLP actions*,*

as set out in the table in clause 13.2.

(h) **Threat Protection**

(i) Threat protection is a feature that provides real-time detection and automated response to endpoint threats within your Approved Environment (**Threat Protection**). This includes:

(A) real-time threat detection and automated response; and

(B) monitoring of EDR alerts and telemetry,

as set out in the table in clause 25.2.

(i) **Policy Automation**

(i) Policy automation applies dynamic security policies to Managed Endpoint within your Approved Environment using the Desired State Configuration based on Device and User risk posture (**Policy Automation**). This includes:

(A) dynamic policy application based on Device or User risk posture (for example where malware, suspicious URLs are detected), in line with the Desired State Configuration;

(B) applying or revoking security policies automatically via the Desired State Configuration when risk posture changes; and

(C) providing alerts for automated policy changes,

as set out in the table in clause 25.2.

(j) **Monitoring**

(i) Monitoring is a feature that provides oversight of Managed Endpoint health and security within your Approved Environment. This includes:

(A) 24x7x365 monitoring of your Managed Endpoint service;

(B) generating alerts and notifications for detected issues; and

(C) escalating Incidents to you or your nominated contacts when action is required.

(k) **Vulnerability and Threat Management**

(i) Vulnerability and threat management identifies and helps remediate Managed Endpoint vulnerabilities through scheduled assessments and scans within your Approved Environment (**Vulnerability and Threat Management**). This includes:

(A) conducting onboarding vulnerability assessments for all new Device limited to 30 minutes per Device;

(B) scheduling and executing regular scans to identify and remediate endpoint vulnerabilities;

(C) generating remediation recommendations; and

(D) escalating critical vulnerabilities for immediate action,

as set out in the table in clause 25.2.

(ii) You acknowledge and agree that:

(A) not all Devices will be compatible due to factors such as age and capability of Device;

(B) if remediation is expected to exceed this timeframe, we will advise you of next steps, which may include replacing the Device or incurring Professional Service costs to remediate the impacted Device(s);

(C) remediation actions may affect Managed Endpoint performance or availability; and

(D) it is your responsibility to ensure that Users are available to support remediation actions if we require and that Managed Endpoint services are connected to the Approved Environment.

(l) **Remediation**

(i) Remediation is a feature that addresses security Incidents and vulnerabilities on Managed Endpoint within your Approved Environment when corrective control is required (**Remediation**).

(ii) This feature is only included with **Premium Tier** selection, as set out in the table in clause 25.2.

(iii) This includes:

(A) raising a Service Request on your behalf, informing you of any security Incidents and vulnerabilities identified by SOC/SIEM; and

(B) planning and implementing remediation activities based on the SOC/SIEM findings.

Managed Endpoint Service Report

27.5 We will provide you with a Managed Endpoint Service Report in relation to your Managed Endpoint service, as set out in the table in clause 25.2.

28 YOUR OBLIGATIONS

You must comply with any Customer Ongoing Responsibilities.

(D) MANAGED COLLABORATION

29 ABOUT MANAGED COLLABORATION

29.1 This is the Managed Collaboration part of this TBMS section of Our Customer Terms.

29.2 Other terms also apply to Managed Collaboration. For more information about the other terms that apply and how they work together, see clause 1 of this TBMS section of Our Customer Terms.

30 MANAGED COLLABORATION

30.1 Managed Collaboration provides you with administration services, proactive monitoring, lifecycle management, User support for Microsoft collaboration tools (such as chat, video, and file management) and voice technologies provided with your Microsoft 365 Business or Telstra Unified Communication plans, as further set out in this section of the Our Customer Terms and your Order.

30.2 Managed Collaboration is made up of the following:

(a) **MS Teams**: regular operational support for Users, including chat, file sharing, video conferencing, and integration with other Office 365 applications;

(b) **Outlook**: mailbox administration and operational support, including email backup and restore, message hygiene, and patch management;

(c) **One Drive:** One Drive management and support for Users, including secure cloud storage, file sharing, and synchronisation across Devices;

(d) **SharePoint**: administrative support for SharePoint sites, including document management, collaboration tools, and integration with Microsoft Teams; and

(e) **Unified Communications:** integration of voice services on supported Voice Solutions.

30.3 The features vary between the Service Tiers of Basic, Standard, and Premium, as summarised in the following table:

Managed Collaboration		Basic	Standard	Premium
User Lifecycle Management	User provisioning and deprovisioning.	✓	✓	✓
	Mailbox setup and password resets.	✓	✓	✓
	Access to Microsoft 365 apps (Word, Excel, PowerPoint, Outlook).	✓	✓	✓
IAM and Security Management	Exchange Online Protection (**EOP**), OneDrive and SharePoint access.	✓	✓	✓
	Native spam/phishing protection via EOP.	✓	✓	✓
	MFA enablement and basic Entra ID (Azure AD) integration.	✓	✓	✓
Teams Chat and Meeting Support	Microsoft Teams chat and meeting support.	✓	✓	✓
	Incident and service request handling during Business Hours.	✓	✓	✓
Voice Integration	Voice Integration (such as Adaptive Collaboration).	✓	✓	✓
	Configure User accounts with roles, permissions, phone numbers, and voicemail.	✓	✓	✓
	Set up call routing rules, dial plans, auto-attendants, and call queues.	✓	✓	✓
	Integrate telephony with collaboration tools, CRM, and SIP trunks.	✓	✓	✓
	Prioritise voice traffic using Quality of Service (**QoS**) settings and monitor call quality.	✓	✓	✓
	Enable encryption, firewalls, and secure access.	✓	✓	✓
Identity and Access Governance	Microsoft Entra Conditional Access Policy setup and enforcement.	✓	✓	✓
	Microsoft Teams and SharePoint policy enforcement.	×	✓	✓
	Shared mailbox and distribution list management.	×	✓	✓
Managed Collaboration Data Protection and Compliance	DLP configuration for Exchange Online Protection and Microsoft Teams.	×	✓	✓
	Compliance dashboard access and audit log review.	×	✓	✓
	Safe Links and Safe Attachments.	✓	✓	✓
	Microsoft Defender Anti-Phishing Policies.	✓	✓	✓
	Threat investigation dashboard.	✓	✓	✓
	Scheduled monitoring of collaboration services.	×	✓	✓
Advanced Threat Protection and Response	Microsoft Defender for Office 365 Plan 2.	×	×	✓
	Automated Investigation and Response (AIR).	×	×	✓
	Microsoft Defender Threat Explorer And Real-Time Detections.	×	×	✓
	Microsoft Defender Attack Simulation Training.	×	×	✓

Managed Collaboration		Basic	Standard	Premium
	Custom alert policies and advanced hunting.	×	×	✓
	Integration with Google Chronicle	×	×	✓
	Full SOC integration for triage and root cause analysis.	×	×	✓
Compliance and Governance	Real-time compliance and alerting.	×	×	✓
	Tenant-wide governance (such as geo-fencing and session control).	×	×	✓
Executive /VIP Support	VIP mailbox handling and proactive issue resolution.	×	×	✓
	Personalised configuration and User enablement.	×	×	✓

Eligibility

30.4 If Managed Collaboration is acquired as part of a Managed IT Services Bundle, the eligibility criteria of the bundle apply. Please refer to the Managed IT Services Bundle part of this TBMS section of Our Customer Terms for eligibility.

30.5 To be, and to remain eligible to acquire Managed Collaboration as a Standalone Service, you must:

(a) have and maintain a valid and current Microsoft 365 for Business licence (or an alternative licence as notified by us from time to time), for each Managed Collaboration service:

(i) **Basic and Standard Tier:** Microsoft365 Business Premium, E3 or E5 licence for each User; or

(ii) **Premium Tier:** Microsoft 365 E5 licence for each User; and

(b) maintain an Azure subscription with a storage account for service operations (such as logs, automation and reporting).

30.6 If the inclusions in your underlying licences changes (for example, Microsoft 365 for Business), it may be necessary for you to acquire a different licence or different level of licence to continue to acquire your service from us. We will tell you if this happens.

30.7 Microsoft 365 Business plans and licences within your tenancy that are assigned to an Active User will be considered 'under management'. Managed Collaboration is limited to Microsoft 365 Business plans and standalone licences listed above (or otherwise as notified by us from time to time), currently available and orderable through Telstra Apps Marketplace, Microsoft direct, or a licensed Microsoft Cloud Service Provider.

31 FEES AND ACTIVATION

Fees

31.1 If you select Managed Collaboration as a Managed IT Services Bundle, the applicable fees and charges for Managed Collaboration are set out in the Managed IT Services Bundle part of this TBMS section of Our Customer Terms.

31.2 If you select Managed Collaboration as a Standalone Managed Service, the applicable fees and charges for Managed Collaboration:

(a) will be charged on a per User basis from the date of the relevant licence;

(b) will be billed monthly in arrears; and

(c) are calculated on a daily basis for each day of the relevant month as follows:

A = B x C

where:

A is the fees and charges payable by you for your Managed Collaboration service for the relevant day;

B is the number of Active Users (chargeable units) for that day; and

C is the applicable rate per Managed Collaboration service (as set out in the Telstra Business Managed Services Rate Card).

31.3 Fees will vary depending on the relevant Service Tier.

Activation

31.4 If Managed Collaboration is acquired as part of a Managed IT Services Bundle, the activation criteria of the Managed IT Services Bundle part of this TBMS section of Our Customer Terms apply.

31.5 If you select Managed Collaboration as a Standalone Managed Service, it will be considered 'active', and we will commence charging for the service when our management tools are linked to your Approved Environment and when licences are active and assigned to a User.

32 SERVICE COMPONENTS

32.1 The service components of your Managed Collaboration will vary depending on the structure of your TBMS. The service elements and the Service Tier for your Managed Collaboration are set out in your Order.

Managed IT Services Bundle

32.2 If you select your Managed Collaboration as part of a Managed IT Services Bundle, the service components listed under clause 32.4 will be aligned to the Essential 8 Controls.

32.3 The Essential 8 Controls section of this TBMS section of Our Customer Terms describes the Essential 8 Controls.

Managed Collaboration Service Components

32.4 Subject to your selected Service Tier, your Managed Collaboration will include the following elements and be subject to the following terms.

(a) **User Lifecycle Management**

(i) User lifecycle management provides centralised control over User accounts within your Approved Environment (**User Lifecycle Management**). This includes:

(A) User provisioning and deprovisioning;

(B) mailbox setup;

(C) configuring mailbox settings such as display name, email aliases, and storage limits;

(D) assigning the mailbox to the correct User group or department;

(E) assisting Users to reset passwords; and

(F) configuring access to Microsoft 365 apps (such as Word, Excel, PowerPoint and Outlook).

(ii) You acknowledge and agree that:

(A) we create, enable, modify or disable access to Microsoft apps or services for joiners, changes or leavers when instructed by you; and

(B) unless agreed otherwise, you retain the responsibility for Active Users within your Microsoft 365 tenancy.

(b) **Identity Access Management and Security Management**

(i) Identity access management restricts access to Microsoft 365 services to authorised Users (**Identity Access Management**). Security management ensures that built-in security features reflect the Desired State Configuration (**Security Management**). This includes:

(A) support for Outlook (Exchange Online), OneDrive, and SharePoint team sites with no customisation;

(B) Desired State Configuration enabling and maintaining, native (built-in) spam/phishing protection via Exchange Online Protection, spam filtering and phishing detection;

(C) configuration and enforcement of MFA policies centrally;

(D) ensuring that MFA is enabled across all remote access points, including Outlook, Teams, SharePoint, VPNs, and web apps;

(E) configuring Safe Links and Safe Attachments, Microsoft Defender Anti-Phishing Policies and threat investigation dashboard; and

(F) Entra ID (Azure AD) SSO integration to manage User identities, access permissions, and authentication workflows.

(c) **Microsoft Teams Chat and Meeting Support**

(i) Microsoft Teams Chat and Meeting Support provides Users in your Approved Environment with access to support for Microsoft Teams. This includes:

(A) Microsoft Teams Chat and Meeting Support to trouble-shoot common issues such as audio/video problems and chat access; and

(B) guiding Users on basic features such as screen sharing, meeting recording, or using chat reactions.

(ii) You acknowledge and agree that:

(A) basic Microsoft Teams Chat and Meeting Support is limited to internal Users and Devices within your Approved Environment. You may elect to utilise Microsoft Teams' external communication features for other individuals but support for external Users or their Devices is not included; and

(B) there may be service disruptions caused by Microsoft Teams platform outages.

(d) **Voice Integration**

(i) Voice Integration allows Users to make and/or receive phone calls using Voice over Internet Protocol (VoIP) (**Voice Integration**). The Voice Integration features are available on supported Voice Solutions. This includes:

(A) configuration and support for voice integration features;

(B) configuration of User accounts with roles, permissions, phone numbers, and voicemail;

(C) set up call routing rules, dial plans, auto-attendants, and call queues;

(D) integration of telephony with collaboration tools, CRM, and SIP trunks;

(E) if available, prioritising voice traffic using QoS settings and monitoring of call quality; and

(F) enabling encryption, firewalls, and secure communication access (such as MFA).

(e) **Identity and Access Governance**

(i) Identity and access governance provides enforcement of policies across collaboration platforms and management of shared resources across the Microsoft tenancy (**Identity and Access Governance**). This includes:

(A) Microsoft Entra Conditional Access policy setup and enforcement;

(B) Microsoft Teams and SharePoint policy enforcement; and

(C) shared mailbox and distribution list management,

as set out in the table in clause 30.3.

(f) **Managed Collaboration Data Protection and Compliance**

(i) Data protection and compliance applies Microsoft 365 security and compliance controls to help safeguard sensitive data and support regulatory obligations across collaboration platforms (**Managed Collaboration Data Protection and Compliance**). This includes:

(A) DLP configuration for Exchange Online and Microsoft Teams;

(B) compliance dashboard and audit log review to support visibility into User and administrator activity;

(C) Safe Links and Safe Attachments;

(D) anti-phishing policies;

(E) threat investigation dashboard; and

(F) scheduled monitoring of Managed Collaboration services,

as set out in the table in clause 30.3.

(g) **Advanced Threat Protection and Response**

(i) Advanced Threat Protection and Response is a feature that helps detect and respond to cyber threats using Microsoft Defender and integrated security tools.

(ii) This feature is only included with **Premium Tier** selection, as set out in the table in clause 30.3.

(iii) This includes enabling the following inclusions within Microsoft Defender for Office 365 Plan 2:

(A) Automated Investigation and Response (**AIR**);

(B) Microsoft Defender Threat Explorer and near real-time detections;

(C) Microsoft Defender Attack Simulation Training;

(D) custom alert policies and advanced threat hunting across Microsoft 365 data sources;

(E) 24x7x365 proactive security monitoring and alerting;

(F) integration with Google Chronicle; and

(G) security events escalation to the SOC for triage and root cause analysis.

(h) **Compliance and Governance**

(i) Compliance and governance refers to the activities we undertake to enforce tenant-wide policies that restrict User access based on location and session behaviour (**Compliance and Governance**).

(ii) This feature is only included with **Premium Tier** selection, as set out in the table in clause 30.3.

(iii) This includes:

(A) continuous assessment of whether the tenant meets compliance benchmarks and triggers alerts when deviations are detected; and

(B) tenant-wide governance, including Geo-Fencing and Session Control.

(i) **Executive and VIP Support**

(i) Executive and VIP Support provides personalised assistance for high-priority Users, ensuring prompt resolution and tailored configuration.

(ii) This feature is only included with **Premium Tier** selection, as set out in the table in clause 30.3.

(iii) This includes:

(A) VIP mailbox handling and proactive issue resolution; and

(B) personalised configuration and User enablement.

(iv) You acknowledge and agree that, before Executive and VIP Support is implemented, you must confirm any specific configuration preferences or enablement requirements for VIP Users.

Managed Collaboration Service Report

32.5 We will provide you with a monthly Managed Collaboration Service Report in relation to your Managed Collaboration service.

33 EXCLUSIONS

Managed Collaboration does not include support for any on-premises deployments of Managed Collaboration, including Microsoft 365.

34 YOUR OBLIGATIONS

34.1 You must comply with any Customer Ongoing Responsibilities.

34.2 In addition to any Customer Ongoing Responsibilities, if you select the **Basic Tier**, you must:

(a) manage User identity lifecycle (such as onboarding and offboarding) unless delegated;

(b) maintain ownership of tenant-wide configurations and global admin roles;

(c) assist in validating basic security alerts (such as, login anomalies);

(d) perform manual reviews of audit logs and compliance reports;

(e) manage third-party integrations and unsupported apps;

(f) accept responsibility for data backup and retention policies (unless scoped separately);

(g) participate in security incident response activities as needed;

(h) maintain responsibility for User training on secure collaboration practices;

(i) provide access to internal stakeholders for escalations and approvals;

(j) validate and approve mailbox recovery, shared mailbox setup, and Microsoft Teams governance changes;

(k) collaborate on tenant-wide governance and policy lifecycle management;

(l) comply with any other reasonable request we make in relation to your Managed Collaboration service; and

(m) ensure timely licence provisioning for any relevant licences.

34.3 In addition to the responsibilities applicable to the Basic Tier, if you select the **Standard Tier,** you must:

(a) approve and validate Microsoft Entra Conditional Access and DLP policy designs before implementation;

(b) review and act on compliance dashboards and audit logs provided by the service provider; and

(c) coordinate with internal IT/security teams for integration with other enterprise systems.

34.4 In addition to the responsibilities applicable to the Basic and Standard Tiers, if you select the **Premium Tier**, you must:

(a) approve advanced security configurations (such as geo-fencing, session control and custom alert policies);

(b) participate in SOC-led incident response and remediation planning;

(c) provide access to SIEM/SOC teams for integration and alert correlation;

(d) validate and approve Microsoft Defender Attack Simulation campaigns and User training schedules;

(e) maintain executive sponsorship and stakeholder alignment for VIP support and governance; and

(f) participate in monthly service reviews, compliance scoring sessions, and roadmap planning.

(E) MANAGED CYBER SECURITY

35 ABOUT MANAGED CYBER SECURITY

35.1 This is the Managed Cyber Security part of this TBMS section of Our Customer Terms.

35.2 Other terms also apply to Managed Cyber Security. For more information about the other terms that apply and how they work together, see clause 1 of this TBMS section of Our Customer Terms.

36 MANAGED CYBER SECURITY

36.1 Managed Cyber Security provides you with whole of business cyber security coverage, designed to reflect the ACSC 'Essential Eight Framework'.

36.2 The features vary between the Service Tier of Basic, Standard, and Premium, as summarised in the following table:

Managed Cyber Security		Basic	Standard	Premium
Deploy Microsoft Defender antivirus	Install and configure Microsoft Defender with real-time protection and cloud-based updates.	✓	✓	✓
Apply patch management	Ensure operating systems and major applications are patched within 30 days.	✓	✓	✓
Enforce Microsoft security baselines via Microsoft Intune	Apply standard Microsoft security baselines to ensure consistent configuration across all managed Devices.	✓	✓	✓
Enrol Devices into Microsoft Intune	Register eligible Devices into Microsoft Intune for centralised policy and compliance management.	✓	✓	✓
Monitor alerts	Enable alerting for malware detections and policy violations, with basic visibility through the Microsoft 365 security portal.	✓	✓	✓
Configure windows defender firewall	Apply and enforce host-based firewall rules using Microsoft Intune.	×	✓	✓
DLP controls	Configure default DLP controls in the Approved Environment.	×	✓	✓
Implement endpoint-level DLP controls	Use Microsoft Defender and Microsoft Intune to block or restrict data transfers via USB, clipboard, or local file sharing.	×	✓	✓
Tighten Patch SLAs	Reduce patching timelines to within 14 days for critical vulnerabilities, improving resilience against known exploits.	×	✓	✓
Apply application allowlisting	Use Microsoft Defender Application Control (MDAC).	×	✓	✓
Monitor firewall & DLP events	Enable alerting and reporting for blocked connections and endpoint-level DLP violations, with escalation paths defined.	×	✓	✓
Integrate Defender XDR with SIEM	Stream telemetry and alerts into a centralised SIEM for correlation and analytics.	×	×	✓

Managed Cyber Security		Basic	Standard	Premium
Enable 24x7 SOC monitoring	Provide continuous monitoring, triage, and escalation of security Incidents by a dedicated SOC team.	×	×	✓
Conduct threat hunting & RCA	Perform proactive threat hunting and root cause analysis.	×	×	✓
Deliver monthly threat reports	Provide executive-level dashboards and detailed reports on threat trends, Incidents, and remediation actions.	×	×	✓
Run simulated attacks & recovery drills	Conduct monthly phishing simulations and backup restoration tests.	×	×	✓

Eligibility

36.3 Managed Cyber Security can only be acquired as part of a Managed IT Services Bundle and the eligibility criteria of the bundle apply. Please refer to the Managed IT Services Bundle part of this TBMS section of Our Customer Terms for eligibility criteria.

37 FEES AND ACTIVATION

The applicable fees, charges and activation criteria for Managed OneDrive Backup are set out in the Managed IT Services Bundle part of this TBMS section of Our Customer Terms.

38 SERVICE COMPONENTS

38.1 The service components for Managed Cyber Security will be aligned to the Essential 8 Controls. The Essential 8 Controls section of this TBMS section of Our Customer Terms describes the Essential 8 Controls.

38.2 In addition to clause 38.1, the **Basic Tier** for Managed Cyber Security includes the following:

(a) installation and configuration of Microsoft Defender with real-time protection and cloud-based updates;

(b) patch management operating systems and major applications patched within 30 days to reduce vulnerabilities;

(c) application of standard Microsoft security baselines using Microsoft Intune to ensure consistent configuration across all managed Devices;

(d) registration of eligible Devices into Microsoft Intune for centralised policy and compliance management;

(e) alerting for malware detections and policy violations, with visibility through the Microsoft 365 security portal; and

(f) monthly basic Incident reporting.

38.3 In addition to the Basic Tier, if you select the **Standard Tier**, your Managed Cyber Security will also include the following:

(a) application and enforcement of host-based firewall rules using Microsoft Intune to restrict unauthorised inbound and outbound traffic on endpoints;

(b) default DLP controls in the Approved Environment;

(c) endpoint-level DLP controls using Microsoft Defender and Microsoft Intune to block or restrict data transfers via USB, clipboard, or local file sharing;

(d) reduced patching timelines to within 14 days for critical vulnerabilities, improving resilience against known exploits;

(e) the use of Microsoft Defender Application Control to allow only approved applications to run on endpoints;

(f) enabling alerting and reporting for blocked connections and endpoint-level DLP violations, with escalation paths defined; and

(g) monthly Incident reporting and reporting on status of in-scope activities.

38.4 In addition to the Standard Tier, if you select the **Premium Tier**, your Managed Cyber Security also includes the following:

(a) integrated Defender XDR with SIEM to stream telemetry and alerts into a centralised SIEM for correlation and analytics;

(b) 24x7 SOC monitoring;

(c) proactive threat hunting and root cause analysis to identify and contain persistent threats;

(d) executive-level dashboards and detailed reports on threat trends, Incidents, and remediation actions; and

(e) monthly phishing simulations and backup restoration tests to validate Incident response readiness.

39 EXCLUSIONS

39.1 Managed Cyber Security does not include:

(a) if you select **Basic** or **Standard Tier**:

(i) custom DLP pattern development (such as custom regex, fingerprinting or advanced data classification rules) for precise data loss prevention;

(ii) integration with non-Microsoft third-party firewall or DLP tools for enhanced security measures; or

(iii) advanced forensics for in-depth investigation and analysis of security Incidents; and

(b) in addition to the exclusions for Basic or Standard Tier, for **Premium Tier**:

(i) customised threat intelligence feeds or specific proprietary detection rules; or

(ii) legal or regulatory breach notification services.

40 YOUR OBLIGATIONS

40.1 You must comply with any Customer Ongoing Responsibilities.

40.2 In addition to any Customer Ongoing Responsibilities, if you select the **Basic Tier**, you must:

(a) comply with defined data classification schema and acceptable use policies; and

(b) approve pathing windows and any exceptions to standard update policies.

40.3 In addition to the responsibilities applicable to the Basic Tier, if you select the **Standard Tier,** you must:

(a) review and approve standard firewall rule sets and endpoint-level DLP policies before deployment;

(b) provide definitions and examples of sensitive data identification types to guide endpoint-level DLP configuration;

(c) support timely patching by approving patch windows and ensuring Devices remain online and reachable; and

(d) participate in change control processes for updates to firewall rules or DLP enforcement policies.

40.4 In addition to the responsibilities applicable to the Basic and Standard Tiers, if you select the **Premium Tier**, you must:

(a) participate in onboarding workshops to define escalation paths, SLAs, and response workflows;

(b) grant SOC access to Defender, Google Chronicle and relevant logs for monitoring and investigation;

(c) engage in incident collaboration response activities and approve remediation actions as needed;

(d) ensure internal policies align with SOC recommendations and Essential 8 Control Level 3;

(e) conduct internal awareness programs to support phishing simulations and response readiness; and

(f) ensure backup systems are in place and accessible for testing and recovery validation.

(F) MANAGED ONEDRIVE BACKUP

41 ABOUT MANAGED ONEDRIVE BACKUP

41.1 This is the Managed OneDrive Backup part of this TBMS section of Our Customer Terms.

41.2 Other terms also apply to Managed OneDrive Backup. For more information about the other terms that apply and how they work together, see clause 1 of this TBMS section of Our Customer Terms.

42 MANAGED ONEDRIVE BACKUP

42.1 Managed OneDrive Backup is a component of the Managed IT Services Bundle that uses Microsoft 365 capabilities to automate backup processes, apply Access Controls and deliver reporting and monitoring features. This requires each User’s Device to be enrolled and managed using Desired State Configuration. Once enabled, files in the designated folders are automatically redirected and synced to the User's OneDrive account in the Cloud.

42.2 The features vary between the Service Tier of Basic, Standard, and Premium, as summarised in the following table:

Managed OneDrive Backup		Basic	Standard	Premium
Enable OneDrive Backup	Configure OneDrive Known Folder Move (KFM) to back up desktop, documents, and pictures folders.	✓	✓	✓
Schedule Weekly Sync	Ensure weekly synchronisation of user data to OneDrive cloud storage.	✓	✓	✓
Monitor Backup Status	Use Microsoft 365 admin centre to monitor backup health and sync issues.	✓	✓	✓
Reporting	A backup summary report will be provided on a monthly basis.	✓	✓	✓
Enforce OneDrive Access Policies	Apply Microsoft Entra Conditional Access and MFA to secure access to backup data.	✓	✓	✓
Configure Retention & Versioning	Enable file versioning and retention policies to support rollback and compliance.	×	✓	✓
Monitor Access Logs	Track access to backup data using Microsoft Purview Audit or Defender for Cloud Apps.	×	✓	✓
Weekly Backup Continuity Checks	Validate that weekly backups are completing successfully and alert on failures.	×	✓	✓
Automate DR Playbooks	Integrate OneDrive recovery with SOC or Logic Apps to trigger DR workflows.	×	×	✓
Simulate Backup Failover	Conduct quarterly disaster recovery simulations to validate restore readiness.	×	×	✓
Validate Backup Integrity	Perform automated checks to ensure backup data is complete, accessible, and uncorrupted.	×	×	✓
Integrate with Incident Response	Link backup alerts to SOC or IR teams for rapid containment and recovery.	×	×	✓
Weekly Backup Continuity Checks	Validate that weekly backups are completing successfully and alert on failures.	×	×	✓

Eligibility

42.3 Managed OneDrive Backup can only be acquired as part of a Managed IT Services Bundle and the eligibility criteria of the bundle apply. Please refer to the Managed IT Services Bundle part of this TBMS section of Our Customer Terms for eligibility criteria.

43 FEES AND ACTIVATION

The applicable fees, charges and activation criteria for Managed OneDrive Backup are set out in the Managed IT Services Bundle part of this TBMS section of Our Customer Terms.

44 SERVICE COMPONENTS

44.1 The service components of Managed OneDrive Backup will be aligned to the Essential 8 Controls. The Essential 8 Controls section of this TBMS section of Our Customer Terms describes the Essential 8 Controls.

44.2 In addition to clause 44.1, the **Basic Tier** for Managed OneDrive Backup includes the following:

(a) OneDrive 'Known Folder Move' to back up desktop, documents, and pictures folders;

(b) monitoring backup health and sync issues via Microsoft 365 admin center to monitor;

(c) configuration for weekly synchronisation of User data to OneDrive cloud storage;

(d) configuration of Microsoft Entra Conditional Access and MFA to secure access to backup data; and

(e) a monthly backup summary report.

44.3 In addition to the Basic Tier, if you select the **Standard Tier**, your Managed OneDrive Backup will also include the following:

(a) enabling of file versioning and retention policies;

(b) tracking access to backup data using Microsoft Purview Audit or Defender for Cloud Apps;

(c) validation that monthly backups are completed successfully;

(d) testing restoration of data in a test environment; and

(e) alerts on failures.

44.4 In addition to the Standard Tier, if you select the **Premium Tier**, your Managed OneDrive Backup will also include the following:

(a) automated DR playbooks and integrated OneDrive recovery with SOC or Logic Apps to trigger DR workflows;

(b) annual backup failover simulations to validate restore readiness;

(c) automated checks to test that backup data is complete, accessible and not complied;

(d) linked backup alerts to SOC or IR teams;

(e) legal hold or eDiscovery custom configurations; and

(f) a weekly backup summary report.

45 EXCLUSIONS

45.1 Managed OneDrive Backup does not include:

(a) if you select **Basic Tier**:

(i) back up of non-user folders or external drives for comprehensive data protection;

(ii) backup of mobile Devices or shared drives to safeguard all User data; and

(iii) onsite support or recovery for immediate assistance and data restoration;

(b) in addition to the exclusions of the Basic Tier, for **Standard Tier**:

(i) manual backup of custom folders or third-party apps to ensure data protection; and

(ii) integration with third-party backup tools for enhanced backup capabilities; and

(c) in addition to the exclusions of the Standard Tier, for **Premium Tier**:

(i) backup of non-Microsoft third-party SaaS platforms;

(ii) custom DR scripting outside Microsoft ecosystem for tailored disaster recovery solutions;

(iii) legal or regulatory breach notifications; and

(iv) physical media recovery to restore data from damaged or corrupted storage devices.

46 YOUR OBLIGATIONS

46.1 You must comply with any Customer Ongoing Responsibilities.

46.2 In addition to any Customer Ongoing Responsibilities, if you select the **Standard Tier,** you must:

(a) approve and maintain Access Control policies; and

(b) participate in quarterly backup policy reviews.

46.3 In addition to the responsibilities applicable to the Standard Tier, if you select the **Premium**

Tier, you must:

(a) participate in DR simulations and post-mortems;

(b) maintain licensing and access for automation tools; and

(c) approve integration with SOC/IR workflows.

(G) NETWORK MANAGEMENT

47 ABOUT NETWORK MANAGEMENT

47.1 This is the Network Management part of this TBMS section of Our Customer Terms.

47.2 Other terms also apply to Network Management. For more information about the other terms that apply and how they work together, see clause 1 of this TBMS section of Our Customer Terms.

48 NETWORK MANAGEMENT

48.1 Network Management provides remote Network Device management and support, related internet connectivity monitoring and Network Device status alerting for your business's networking infrastructure, as further set out in this section of Our Customer Terms and your Order.

48.2 Subject to your selected Network Devices, Network Management includes the management of:

(a) Routers;

(b) Switches; or

(c) Wireless Access Points.

48.3 The features vary between the Service Tiers of Basic, Standard, and Premium, as summarised in the following table:

Network Management		Basic	Standard	Premium
Network Infrastructure Management	VLAN segmentation and static routing configuration.	✓	✓	✓
	Access Control List management.	✓	✓	✓
Network Security and Access Control	Firewall rule setup and port management.	✓	✓	✓
	Access Control enforcement.	✓	✓	✓
Maintenance and Configuration Management	Firmware updates and patching for supported Network Devices.	✓	✓	✓
	Backup and restore of Device configurations.	✓	✓	✓
	Patch management for Network Devices.	✓	✓	✓
	Configuration backup validation and version control.	×	✓	✓

Network Management		Basic	Standard	Premium
	Quarterly Network Device audits.	×	×	✓
Monitoring and Incident Response	Network monitoring (such as availability and uptime).	✓	✓	✓
	Incident response for connectivity issues.	✓	✓	✓
	Logging and manual review.	✓	✓	✓
Load Balancing and Availability	Configuration and management of L4/L7 load balancers.	×	✓	✓
	Health checks and failover setup for load-balanced services.	×	✓	✓
	SSL certificate management on load balancers.	×	✓	✓
Network Governance and Change Control	Change management and impact analysis for network changes.	×	✓	✓
	Network segmentation and micro-segmentation support.	×	✓	✓
	Enforced segmentation and traffic filtering.	×	✓	✓
Network Security and Threat Management	Firewall policy tuning and threat filtering.	×	✓	✓
	Real time traffic and threat logging.	×	✓	✓
	Regular vulnerability assessments and remediation planning.	×	✓	✓
SD-WAN Tenancy and Policy Management	Management of SD-WAN tenancy.	×	×	✓
	Centralised policy enforcement across branch networks.	×	×	✓
	Automated failover and link remediation.	×	×	✓
Network Performance and Optimisation	Real-time traffic analytics and optimisation.	×	×	✓
	Traffic shaping and bandwidth reservation.	×	×	✓
Security and Monitoring Integration	Integration with SIEM/SOC for network event correlation.	×	×	✓
	24x7 proactive monitoring.	✓	✓	✓
	MFA for admin access.	✓	✓	✓
	24x7 proactive monitoring and incident response for critical links.	×	×	✓

48.4 The features of Network Management will also vary depending on the Network Device you select in your Order, as summarised in the following table:

Wireless Access Points	Basic	Standard	Premium
Provisioning and configuration of Wireless Access Points (such as Meraki and Cisco).	✓	✓	✓
SSID setup and Access Control.	✓	✓	✓
WPA2/WPA3 security enforcement.	✓	✓	✓
Zero-touch provisioning via Meraki Dashboard or DNAC.	✓	✓	✓
Role-based Access Control (RBAC) for Wireless Access Point Users.	×	✓	✓
Integration with identity platforms (for Azure AD, Okta).	×	×	✓
PMF (Protected Management Frames) enforcement.	×	×	✓
Switches			

Wireless Access Points	Basic	Standard	Premium
Provisioning and configuration of L2/L3 switches (Cisco/Juniper/Meraki).	✓	✓	✓
Access validation.	✓	✓	✓
Configuration versioning and rollback.	×	✓	✓
Switch configuration (for example STP tuning, QoS, port security).	×	✓	✓
Routers			
Provisioning and configuration of Routers.	✓	✓	✓
Backup and restore of Router configurations	✓	✓	✓
Creating and maintaining documentation for network infrastructure.	✓	✓	✓
Router configuration (for example dynamic routing and QoS).	×	✓	✓

Eligibility

48.5 If Network Management is acquired as part of a Managed IT Services Bundle, the eligibility criteria of the bundle apply. Please refer to the Managed IT Services Bundle part of this TBMS section of Our Customer Terms for eligibility criteria.

48.6 To be and to remain eligible to acquire Network Management as a Standalone Managed Service, you must:

(a) have and maintain a valid and current Network Device(s) that has passed the hardware assessment; and

(b) maintain an Azure subscription with a storage account.

49 FEES AND ACTIVATION

Fees

49.1 If you select Network Management as a Managed IT Services Bundle, the applicable fees and charges for Network Management are set out in the Managed IT Services Bundle part of this TBMS section of Our Customer Terms.

49.2 If you select Network Management as a Standalone Managed Service, the applicable fees and charges for Network Management:

(a) will be charged on a per Network Device basis from the date the Network Device has been assigned to an Active User;

(b) will be billed monthly in arrears; and

(c) are calculated on a daily basis for each day of the relevant month as follows:

A = B x C

where:

A is the fees and charges payable by you for your Network Management service for the relevant day;

B is the number of Network Devices (chargeable units) for that day; and

C is the applicable rate per Network Management service (as set out in the Telstra Business Managed Services Rate Card).

49.3 Fees will vary depending on the relevant Service Tier.

Activation

49.4 If Network Management is acquired as part of a Managed IT Services Bundle, the activation criteria of the Managed IT Services Bundle part of this TBMS section of Our Customer Terms apply.

49.5 If you select Network Management as a Standalone Managed Service, it will be considered 'active', and we will commence charging for the service when our ITSM and RMM tools are linked to your environment and when licences are active and assigned to a Network Device as applicable.

50 SERVICE COMPONENTS

50.1 The service components of Network Management will vary depending on the structure of your TBMS, the Network Devices and Service Tier you have selected. The service elements and the Service Tier for Network Management are set out in your Order.

Managed IT Services Bundle

50.2 If you select your Network Management as part of a Managed IT Services Bundle, the service components listed under clause 50.4 will be aligned to the Essential 8 Controls.

50.3 The Essential 8 Controls section of this TBMS section of Our Customer Terms describes the Essential 8 Controls.

General Network Management Service Components

50.4 Subject to your selected Service Tier, your Network Management will include the following elements and be subject to the following terms.

(a) **Network Infrastructure Management**

(i) Network infrastructure management provides provisioning and configuration of your Network Devices to ensure they are correctly deployed, segmented, and secured as part of your Approved Environment (**Network Infrastructure Management**). This includes:

(A) implementing VLAN Segmentation to isolate traffic and optimise network performance;

(B) implementing Static Routing by manually configuring the fixed network path or paths between Network Devices where required, to support predictable and controlled data flow between network segments; and

(C) the application of Access Control Lists to restrict unauthorised access to protected network resources and services.

(ii) You acknowledge and agree that we are not responsible for misconfigurations caused by network design inputs you provide.

(b) **Network Security and Access Control**

(i) Network security and Access Control applies foundational preventative controls to your Network Devices to restrict unauthorised access and maintain essential security configurations across your Approved Environment (**Network Security and Access Control**). This includes:

(A) firewall rule and port management applied at the Network Device level to allow or block specific network traffic based on IP addresses, communication protocols and service ports used by applications; and

(B) Access Control enforcement.

(ii) You acknowledge and agree that:

(A) you must nominate Authorised User(s) who may request a network change;

(B) we may request maintenance windows for policy deployments to avoid user impact; and

(C) third-party carrier/firewall services outside the Approved Environment remain out of scope for direct changes.

(c) **Maintenance and Configuration Management**

(i) Maintenance and configuration management is focused on preventative controls (**Maintenance and Configuration Management**). This includes:

(A) monitoring and sourcing the manufacturer's latest model-specific firmware versions as they become available;

(B) deploying firmware updates and patching for Switches, Routers, firewalls and applying vendor-recommended software updates;

(C) verifying that connectivity is restored after the Supported Technology update/patching;

(D) configuration backup and restore to maintain versioned backups and perform configurations; and

(E) quarterly audits that validate Network Device configuration integrity and compliance.

(ii) You acknowledge and agree that if a maintenance window is required, you will be responsible for approving the maintenance window and notifying impacted staff and other relevant stakeholders.

(d) **Monitoring and Incident Response**

(i) Monitoring and incident response provides proactive monitoring of Network Devices within the Approved Environment and priority response to network incidents, troubleshooting and resolution of critical issues (**Monitoring and Incident Response**). This includes:

(A) monitoring Network Device availability, uptime, and network connectivity to detect disruptions or degraded performance across the Approved Environment;

(B) responding to connectivity-related Incidents by investigating alerts, reviewing Network Device and path status, and performing diagnostics to support service restoration;

(C) enabling minimal logging on managed Network Devices to capture essential system events, configuration changes, and basic security alerts required for operational awareness and Incident triage; and

(D) reviewing logs manually in response to alerts or Incidents, rather than performing continuous or automated log analysis.

(ii) You acknowledge and agree that:

(A) monitoring is limited to Network Device availability, uptime, and basic connectivity status; and

(B) logging is minimal and reviewed manually in response to alerts or Incidents. Real-time analysis, long-term retention, or forensic investigation are not included unless specified otherwise in your Order.

(e) **Load Balancing and Availability**

(i) Load balancing and availability optimises the distribution of network traffic and supports high availability for your applications (**Load Balancing and Availability**).This includes:

(A) configuration and management of Layer 4 (transport-level) and Layer 7 (application-level) load balancers;

(B) implementing health checks using defined probes; and

(C) managing SSL certificates on load balancers to support secure traffic termination and encryption for web-facing services,

as set out in the table in clause 48.3.

(ii) You acknowledge and agree that:

(A) you will be required to provide the applicable SSL certificate materials as indicated to you by us, or alternatively, delegate authority for us to manage them;

(B) application owners must supply health-check URLs and acceptable failover behaviors;

(C) you may be required to coordinate testing with application teams;

(D) load balancing will be limited to supported Layer 4 and Layer 7 configurations on Approved Environment;

(E) health checks and failover mechanisms are configured based on standard capabilities and custom logic or integration with external systems are not included; and

(F) SSL certificate management is limited to installation and renewal on load balancers and certificate procurement, and lifecycle tracking remain your responsibility.

(f) **Network Governance and Change Control**

(i) Network governance and change control is an enhanced service layer that provides structured oversight of network changes, segmentation enforcement, and policy alignment beyond infrastructure provisioning and configuration (**Network Governance and Change Control**). This includes:

(A) performing change management and impact analysis for network modifications;

(B) the provision of support for network segmentation and micro-segmentation strategies; and

(C) enforcing segmentation and traffic filtering rules to control communication paths and reduce exposure across your network,

as set out in the table in clause 48.3.

(ii) You acknowledge and agree that:

(A) you will be required to nominate change approvers and provide business blackout dates;

(B) on-site changes attract additional costs, if required (and we will notify you of these charges at the time); and

(C) segmentation scope depends on accurate application and data-flow maps you provide.

(g) **Network Security and Threat Management**

(i) Network security and threat management provides advanced preventative and detective controls (**Network Security and Threat Management**). This includes:

(A) firewall policy tuning and threat filtering;

(B) real-time traffic and threat logging; and

(C) regular vulnerability assessments and remediation planning,

as set out in the table in clause 48.3.

(ii) You acknowledge and agree that:

(A) backlog vulnerabilities that existed prior to onboarding will be addressed on a per Network Device basis. If the network remediation is significant, it will be addressed under Professional Services; and

(B) you must approve maintenance windows for policy changes.

(h) **SD-WAN Tenancy and Policy Management**

(i) SD-WAN Tenancy and Policy Management is a feature that enables centralised, policy-driven control of your Approved Environment across multiple sites. This includes:

(A) management of SD-WAN tenancy;

(B) centralised policy enforcement across branch networks; and

(C) automated failover and link remediation,

as set out in the table in clause 48.3.

(ii) You acknowledge and agree that:

(A) you will maintain SD-WAN licences and provide controller access;

(B) we require Internet service Provider (ISP) circuit details (such as provider, circuit/service ID, access type, bandwidth and hand-off) and DEMARC (demarcation) contacts for escalations (such as site contact, building management/landlord if applicable and after-hours access instructions), and keep these details current; and

(C) some advanced features may depend on specific edge models and software support.

(i) **Network Performance and Optimisation**

(i) Network performance and optimisation controls improve network efficiency, prioritise critical traffic, and ensure optimal use of available links (**Network Performance and Optimisation**).

(ii) This feature is only included if you select the **Premium Tier**, as set out in the table in clause 48.3.

(iii) This includes:

(A) real-time traffic analytics and optimisation;

(B) traffic shaping; and

(C) bandwidth reservation.

(iv) You acknowledge and agree that:

(A) accurate classification may require coordination with application owners;

(B) certain reports depend on Network Device telemetry exports, and your Approved Environment must support and allow these exports; and

(C) business-critical application lists and priorities must be provided and maintained by you.

(j) **Security and Monitoring Integration**

(i) Network performance and optimisation provides detective and corrective controls by integrating network telemetry with external platforms for event correlation, proactive monitoring, and Incident response (**Network Performance and Optimisation**).This includes:

(A) integration with SIEM/SOC for network event correlation;

(B) 24x7 Proactive Monitoring;

(C) MFA for admin access for Network Device configuration interfaces (where available); and

(D) Incident response for critical links,

as set out in the table in clause 48.3.

(ii) You acknowledge and agree that:

(A) you will provide SIEM endpoints, ingest specifications and retention policies;

(B) integration scope is limited to the Approved Environment and supported log types; and

(C) response actions requiring third-party providers are coordinated but are outside our direct control.

Individual Network Device Service Components

50.5 Subject to your selected Network Device, your Network Management will also include the following elements and be subject to the following terms.

(a) **Wireless Access Points**

(i) Subject to your selected Service Tier, management of Wireless Access Points includes:

(A) provisioning and configuring your Router to enable the deployment and setup of your supported Routers within your approved environment post initial installation and configuration;

(B) SSID setup and basic Access Control to enable wireless network identifiers;

(C) WPA2/WPA3 security enforcement using modern encryption and authentication standards;

(D) role-based Access Control for Wireless Access Point Users that enforces differentiated access to wireless network based on User roles;

(E) integration with identity platforms (such as Azure AD and Okta) enabling wireless authentication to be centrally managed using enterprise identity platforms; and

(F) protecting the management traffic exchanged between Wireless Access Point and Devices.

(ii) You acknowledge and agree that we are not responsible for:

(A) connectivity issues resulting from unsupported or misconfigured wireless endpoints;

(B) initial installation and configuration services of Wireless Access Points;

(C) authentication failures or access delays caused by misconfigured identity platforms or unsupported integration methods;

(D) configuration delays or operational impacts caused by your administration restrictions or unsupported access models;

(E) identity management when wireless authentication is not integrated with enterprise identity platforms;

(F) unauthorised access or access-related issues resulting from shared credentials, unmanaged devices, or your controlled authentication settings;

(G) access issues caused by your Devices that do not support WPA2 or WPA3 protocols;

(H) delays or deployment failures caused by platform misconfiguration or access restrictions; or

(I) access conflicts or policy enforcement issues resulting from your managed role definitions or identity platform misalignment,

except to the extent caused or contributed to by our breach of these Our

Customer Terms.

(b) **Switches**

(i) Subject to your selected Service Tier, management of Switches includes:

(A) provisioning and configuration of configure Switches to secure and manage traffic within the same network (Layer 2) and route traffic across different networks or business sites (Layer 3) post initial installation and configuration;

(B) VLAN setup and port configuration to segments traffic and enforces access boundaries across shared infrastructure;

(C) access validation that verifies authorised access to Switch interfaces and administrative functions;

(D) Switch configuration (such as STP tuning, QoS and port security) applying advanced settings to optimise switching performance and security; and

(E) Switch configuration audits that validates Switch configuration integrity and compliance.

(ii) You acknowledge and agree that we are not responsible for:

(A) initial installation and configuration services of Switches;

(B) monitoring gaps or delayed response caused by customer-imposed alert thresholds or unsupported telemetry;

(C) failover limitations or remediation delays caused by unsupported hardware, incomplete link definitions, or customer-managed routing policies; or

(D) performance issues or switching conflicts caused by customer-imposed configuration overrides or unsupported Switch models,

except to the extent caused or contributed to by our breach of these Our Customer Terms.

(c) **Routers**

(i) Subject to your selected Service Tier, management of Routers includes:

(A) provisioning and configuring your Router to enable the deployment and setup of supported Router within your Approved Environment post initial installation and configuration;

(B) firewall rule setup, port management, basic traffic filtering and port control to supported Routers;

(C) static routing and VLAN segmentation including configuration of static routes to control how traffic flows between segments and apply VLANs to isolate traffic across shared infrastructure;

(D) backup and restoration of Router configurations to support recovery in the event of Router failure or misconfiguration;

(E) monitoring supported Routers for connectivity Incidents;

(F) creating and maintain documentation for network infrastructure including configuring records and access policies;

(G) Router configuration to enable the application of advanced routing protocols and traffic prioritising settings;

(H) Router based failover and link remediation; and

(I) Router configuration audits on a quarterly basis to detect configuration drift, confirm alignment with approved standards, and support defensibility.

(ii) You acknowledge and agree that we are not responsible for:

(A) initial installation and configuration services of Routers;

(B) audit failures caused by your own managed changes or unsupported configuration formats;

(C) routing conflicts or segmentation issues resulting from your network design inputs;

(D) Incident resolution delays caused by third-party dependencies or unsupported monitoring configurations;

(E) gaps in documentation resulting from your own changes or unapproved configuration updates;

(F) routing conflicts or performance degradation caused by your own imposed configuration overrides or unsupported Router models; or

(G) resolution delays caused by third-party dependencies or your own escalation pathways,

except to the extent caused or contributed to by our breach of these Our Customer Terms.

Network Management Service Report

50.6 We will provide you with a Network Management Service Report either:

(a) for **Basic** and **Standard Tiers**, monthly; or

(b) for **Premium Tier**, weekly,

in relation to your Network Management service.

51 EXCLUSIONS

51.1 As Network Devices and capabilities differ, we might not be able to manage your Network Devices remotely.

51.2 We will assess the make and model of each of your devices, and if we cannot control and monitor it, we will let you know that the device is not eligible for the Network Management service.

52 YOUR OBLIGATIONS

52.1 You must comply with any Customer Ongoing Responsibilities.

52.2 In addition to any Customer Ongoing Responsibilities, you must:

(a) ensure physical access and power availability for all Network Device hardware;

(b) approve any baseline configurations;

(c) review and approve firewall rule changes and port access requests;

(d) maintain responsibility for ISP/carrier relationships and SD-WAN links;

(e) maintain hardware warranty and licensing;

(f) participate in Incident resolution by providing on-site access or context;

(g) ensure timely firmware licensing and hardware warranty renewals;

(h) monitor and report any physical or environmental issues affecting Network Devices;

(i) provide escalation contacts for change approvals and emergency access;

(j) for Switches, provide network topology and documentation; and

(k) for Routers, provide load balancer configuration, advanced routing protocols (for example, BGP and OSIF) and integration with SIEM/SOC tools.

52.3 In addition to the responsibilities in clause 52.2, if you select the **Standard Tier**, you must:

(a) for Wireless Access Points, enable Firewall policy tuning, participate in change advisory board reviews and approve wireless segmentation and guest access polices;

(b) for Switches, participate in change advisory board reviews, provide escalation contracts for emergency access and approve Switch configuration changes; and

(c) for Routers, ensure you maintain load balancer health checks or SSL management, custom automation or scripting, on-premises cabling or physical installation and third party Router vendor support.

52.4 In addition to the responsibilities in clause 52.3, if you select the **Premium Tier**, you must:

(a) approve load balancer configurations, SSL certificates, and health check parameter;

(b) provide application-level context for load balancing rules and failover logic;

(c) participate in change management reviews for network segmentation and QoS policies;

(d) provide any relevant documentation for custom Network Device policies;

(e) validate and approve advanced firewall policies and threat filtering rules;

(f) coordinate with internal application teams for traffic prioritization and routing logic;

(g) approve SD-WAN architecture, policies, and application-aware routing rules;

(h) provide access to cloud security platforms for integration;

(i) participate in SLA reviews, quarterly security reviews and SD-WAN optimisation planning;

(j) collaborate with SOC/SIEM teams for alert correlation and Incident response;

(k) review and approve traffic shaping, bandwidth reservation, and prioritization policies;

(l) provide escalation paths for critical link remediation and failover testing; and

(m) ensure licensing and support contracts for SD-WAN appliances and cloud controllers.

(H) MANAGED CLOUD VIRTUAL MACHINE

53 ABOUT MANAGED CLOUD VIRTUAL MACHINE

53.1 This is the Managed Cloud Virtual Machine (**VM**) part of this TBMS section of Our Customer Terms.

53.2 Other terms also apply to Managed Cloud VM. For more information about the other terms that apply and how they work together, see clause 1 of this TBMS section of Our Customer Terms.

54 MANAGED CLOUD VM

54.1 Managed Cloud VM provides operational support and lifecycle management for Virtual Machines hosted in a supported cloud environment, including monitoring, patching, antivirus, and infrastructure oversight, as further set out in this section of Our Customer Terms and your Order.

54.2 The features of Managed Cloud VM are summarised in the following table:

Managed Cloud VM	Description
OS Administration	Perform daily maintenance of operating system and managing Incidents related to the virtual server operating system.
OS Patch Management	Perform operating system patching process, patches, and other updates associated with the Supported Operating Systems.
Antivirus Management	Antivirus protection for the Supported Operating System.
Availability Management and Monitoring	Monitor virtual machine elements and other cloud services using defined metrics.
Power-control policy	Implement power-control policy based on utilisation.
Virtual Machine Management	Commissioning and decommissioning of Virtual Machines.
Deployment	Template-based deployments and tagging standards.
Infrastructure Monitoring	24x7 monitoring of compute, storage, and network components.
Incident Management	Alert triage and Incident resolution. Escalation to cloud providers for platform-level Incidents.
Customer Usage Report	Report on your usage of supported Virtual Machines and rightsizing recommendations.

54.3 Managed Cloud VM can only be purchased as a Standalone Managed Service. You can purchase Managed Cloud VM with other Standalone Managed Services or in addition to the Managed IT Services Bundle.

Eligibility

54.4 To be and to remain eligible to acquire Managed Cloud VM, you must maintain an Azure subscription with a storage account for service operations (such as logs, automation and reporting).

55 FEES AND ACTIVATION

Fees

55.1 The applicable fees and charges for Managed Cloud VM:

(a) will be charged on a per Virtual Machine basis from the date of the relevant licence;

(b) will be billed monthly in arrears; and

(c) are calculated on a daily basis for each day of the relevant month as follows:

A = B x C

where:

A is the fees and charges payable by you for your Managed Cloud VM service for the relevant day;

B is the number of Virtual Machines (chargeable units) for that day; and

C is the applicable rate per Virtual Machine (as set out in the Telstra Business Managed Services Rate Card).

Activation

55.2 Managed Cloud VM will be considered 'active', and we will commence charging for Managed Cloud VM, when a Virtual Machine(s) has been onboarded into your Approved Environment.

56 SERVICE COMPONENTS

56.1 Your Managed Cloud VM will include the following elements and be subject to the following terms:

(a) **OS Administration**

(i) OS Administration is a feature that provides daily maintenance of the virtual server operating system. This includes:

(A) daily maintenance of the operating system; and

(B) managing Incidents related to OS Administration health and performance.

(ii) You acknowledge and agree that:

(A) OS Administration maintenance may require scheduled downtime; and

(B) we are not responsible for application-level issues resulting from OS updates, except to the extent that they are caused or contributed to by our breach of these Our Customer Terms.

(b) **OS Patch Management**

(i) OS Patch Management is a feature that applies vendor supported firmware updates. This includes performing OS patching processes, including patches and service updates.

(c) **Antivirus Management**

(i) Antivirus management is a feature that provides antivirus protection for Supported Operating Systems. This includes antivirus protection for the Supported Operating System through configuration and monitoring antivirus tools.

(ii) You acknowledge and agree that Antivirus Management coverage is limited to Supported Operating Systems.

(d) **Availability Management and Monitoring**

(i) Availability Management and Monitoring is a feature that monitors Virtual

Machine availability using defined metrics. This includes monitoring Virtual Machine elements and other cloud services using defined metrics.

(ii) You acknowledge and agree that Availability Management and Monitoring is based on standard metrics and thresholds.

(e) **Power-Control Policy**

(i) Power-Control Policy is a feature that manages power usage based on utilisation thresholds. This includes implementing power-control policy based on utilisation.

(ii) You acknowledge and agree that:

(A) power-control actions may affect availability of non-critical workloads; and

(B) you must notify us of any workloads that require continuous uptime.

(f) **Virtual Machine Management**

(i) Virtual Machine Management is a feature that manages the lifecycle of Virtual Machines. This includes the commissioning and decommissioning of Virtual Machines.

(ii) You acknowledge and agree that:

(A) Virtual Machine Management is provisioning is subject to available capacity and licensing; and

(B) decommissioning will follow agreed retention and archival policies.

(g) **Deployment**

Deployment is a feature that standardises Virtual Machine deployment. This includes template-based deployments and tagging standards.

(h) **Infrastructure Monitoring**

(i) Infrastructure monitoring is a feature that monitors core infrastructure components (**Infrastructure Monitoring**). This includes 24x7 monitoring of compute, storage, and network components.

(ii) You acknowledge and agree that:

(A) monitoring is limited to supported infrastructure components; and

(B) logging retention is subject to your cloud subscription limits.

(i) **Incident Management**

(i) Incident Management is a feature that manages alerts and incidents across the Approved Environment (**Incident Management**). This includes:

(A) alert triage and Incident resolution; and

(B) escalation to cloud providers for platform-level Incidents.

(j) **Customer Usage Report**

We will provide you with a monthly Customer Usage Report in relation to your Managed Cloud VM usage of supported Virtual Machines and rightsizing recommendations.

57 EXCLUSIONS

57.1 Managed Cloud VM does not include:

(a) cloud solutions, including the development of tailored cloud solutions, custom scripting or automation (such as Terraform and Ansible) and cloud-native app modernisation (such as containerisation and PaaS migration); or

(b) application level support, including PAAS service, middleware, databases or management of third-party services or platforms not hosted in the supported cloud environment.

58 YOUR OBLIGATIONS

You must comply with any Customer Ongoing Responsibilities.

(I) MANAGED CLOUD SERVICES BACKUP

59 ABOUT MANAGED CLOUD SERVICES BACKUP

59.1 This is the Managed Cloud Services Backup part of this TBMS section of Our Customer Terms.

59.2 Other terms also apply to Managed Cloud Services Backup. For more information about the other terms that apply and how they work together, see clause 1of this TBMS section of Our Customer Terms.

60 MANAGED CLOUD SERVICES BACKUP

60.1 Managed Cloud Services Backup provides operating system-level backup and recovery for on-premise and Virtual Machines in your Approved Environment, as further set out in this section of Our Customer Terms and your Order. We will install and manage backup agents or integrations to capture system state and data in accordance with our policies, store it in an approved cloud repository, and provide recovery options for supported workloads. Managed Cloud Services Backup utilises Azure Backup as the backup platform which is deployed in your Approved Environment.

60.2 The features of Managed Cloud Services Backup are summarised in the following table:

Managed Cloud Services Backup	Description
Backup Policy and Standards	• Define backup and restore standards and policies.

Managed Cloud Services Backup	Description
	• Recommend improvements for protection, efficiency, and cost.
Backup Operations	• Prepare operating systems for backup agent installation. • Perform initial backup and restore test during build/ORT. • Execute weekly full and daily incremental backups. • Monitor backup/restore processes. • Verify backup/restore status and take corrective actions.
Disaster Recovery Support	• Update Disaster Recovery Plans during transition for Disaster Recovery Plans testing. • Apply configuration changes to meet Disaster Recovery Plans requirements.
Managed Cloud Services Backup Service Report	Monthly back-up summary.

60.3 Managed Cloud Services Backup can only be purchased as a Standalone Managed Service. You can purchase Managed Cloud Services Backup with other Standalone Managed Services or additional to the Managed IT Services Bundle.

Eligibility

60.4 To be and to remain eligible to acquire Managed Cloud Services Backup, you must:

(a) maintain an Azure subscription with a storage account for:

(i) service operations (such as logs automation and reporting); and

(ii) Azure Backup components required for delivery of Managed Cloud Services Backup.

(b) have and maintain the following supporting systems:

(i) Windows Server (2016 or later) or supported Linux versions; or

(ii) physical servers or Virtual Machines (such as VMware vSphere, Hyper-V, or supported public cloud VMs).

61 FEES AND ACTIVATION

Fees

61.1 The applicable fees and charges for Managed Cloud Services Backup:

(a) will be charged on a per Gigabyte basis from the date of activation;

(b) will be billed monthly in arrears;

(c) are calculated on a daily basis for each day of the relevant month as follows:

A = B x C

where:

A is the fees and charges payable by you for your Managed Cloud Services Backup service for the relevant day;

B is the number of Backup Targets (chargeable units) for that day; and

C is the applicable rate per device (as set out in the Telstra Business Managed Services Rate Card).

Activation

61.2 Managed Cloud Services Backup will be considered 'active', and we will commence charging for Managed Cloud Services Backup, when each Backup Target we are managing is enrolled and active in the Approved Environment.

62 SERVICE COMPONENTS

62.1 Your Managed Cloud Services Backup will include the following elements and be subject to the following terms:

(a) **Backup Policy and Standards**

(i) Backup Policy and Standards is a feature that defines and maintains backup and restoration standards and policies for systems within your Approved Environment. This includes:

(A) defining with us backup and restoration standards and policies; and

(B) recommending improvements for protection, efficiency, and cost.

(ii) You acknowledge and agree that we are not responsible for compliance gaps or recovery failures caused by your failure to implement recommended policy changes or maintain required system configurations.

(b) **Backup Operations**

(i) Backup Operations is a feature that manages the execution and monitoring of backup and restore activities for supported systems within your Approved Environment. This includes:

(A) activities to set up Backup Operations, including preparing operating systems for backup agent installation and initial backup and restore test during build and Operational Readiness Testing; and

(B) ongoing activities to maintain Backup Operations, including executing scheduled backups comprising of weekly full and daily incremental backups, monitoring backup and restore processes to ensure data protection and verifying backup and restore status and taking corrective actions if necessary.

(ii) You acknowledge and agree that we are not responsible for missed backup windows, incomplete backups, or restore failures caused by insufficient network bandwidth, unsupported configurations, or customer-initiated changes that impact backup operations, except to the extent caused or contributed to by our breach of these Our Customer Terms.

(c) **Disaster Recovery Support**

(i) Disaster recovery support is a feature that supports the maintenance and execution of disaster recovery plans for systems within your Approved Environment (**Disaster Recovery Support**). This includes:

(A) defining and/or updating Disaster Recovery Plans for Managed Cloud Services Backup to support future Disaster Recovery testing activities; and

(B) applying configuration changes to meet Disaster Recovery requirements of Managed Cloud Services Backup.

(ii) You acknowledge and agree that we are not responsible for Disaster Recovery Plan failures or extended recovery times caused by incomplete information we have received by you, use of configuration changes not approved by us, or failure by you to follow our agreed change processes.

Managed Cloud Services Backup Service Report

62.2 We will provide you with a monthly Managed Cloud Services Backup Service Report in relation to your Managed Cloud Services Backup service.

63 EXCLUSIONS

63.1 Managed Cloud Services Backup does not include:

(a) Azure subscription containing Azure Backup components; or

(b) management of third-party backup tools.

64 YOUR OBLIGATIONS

You must comply with any Customer Ongoing Responsibilities.

(J) MANAGED MICROSOFT DEFENDER

65 ABOUT MANAGED MICROSOFT DEFENDER

65.1 This is the Managed Microsoft Defender part of this TBMS section of Our Customer Terms.

65.2 Other terms also apply to Managed Microsoft Defender. For more information about the other terms that apply and how they work together, see clause 1 of this TBMS section of Our

Customer Terms.

66 MANAGED MICROSOFT DEFENDER

66.1 Managed Microsoft Defender provides you with protection against cyber threats for Devices within your Approved Environment, as further set out in this section of Our Customer Terms and your Order.

66.2 The features of Managed Microsoft Defender are summarised in the following table:

Managed Microsoft Defender	Description
Provisioning and Configuration	Enable and onboard supported endpoints (such as Windows, MacOS and mobile) into Microsoft 365 Defender for Endpoint.
	Configure baseline security policies (such as antivirus, firewall and attack surface reduction).
	Integrate Managed Microsoft Defender with Microsoft 365 Defender portal and Microsoft Intune (if applicable).
Monitoring and Threat Protection	Monitor endpoint health and threat activity 24/7 using the Microsoft Defender Security Centre.
	Investigate and respond to alerts.
	Configure and manage threat indicators, exclusions, and custom detection rules.
Vulnerability and Exposure Management	Enable Threat and Vulnerability Management dashboard.
	Review exposure scores and recommend remediation actions.
	Coordinate patching and configuration changes.
Managed Microsoft Defender User Support	Assistance with security-related issues for Users.
Service Report	Generate and share reporting.

66.3 You acknowledge that certain features outlined in the table in clause 66.2 may vary depending on the capabilities and inclusions of your underlying Microsoft 365 license.

66.4 Managed Microsoft Defender can only be purchased as a Standalone Managed Service. You can purchase Managed Microsoft Defender with other Standalone Managed Services but will be unable to purchase it in addition to a Managed IT Services Bundle.

Eligibility

66.5 To be and to remain eligible to acquire Managed Microsoft Defender, you must:

(a) have and maintain an active Microsoft Defender for Endpoint Plan 2 licence or M365 E5;

(b) maintain an Azure subscription with a storage account for service operations; and

(c) have either:

(i) desktop or laptop Devices (Windows, MacOS); or

(ii) mobile / tablet Devices (Android, iOS, iPadOS).

67 FEES AND ACTIVATION

Fees

67.1 The applicable fees and charges for Managed Microsoft Defender:

(a) will be charged on a per licence basis;

(b) will be billed monthly in arrears; and

(c) are calculated on a daily basis for each day of the relevant month as follows:

A = B x C

where:

A is the fees and charges payable by you for your Managed Microsoft Defender service for the relevant day;

B is the number of assigned licences (chargeable units) for that day; and

C is the applicable rate per licence (as set out in the Telstra Business Managed Services Rate Card).

Activation

67.2 Managed Microsoft Defender will be considered 'active', and we will commence charging, when the licence is assigned to an Active User.

68 SERVICE COMPONENTS

68.1 Your Managed Microsoft Defender will include the following elements and be subject to the following terms:

(a) **Provisioning and Configuration**

(i) Provisioning and Configuration is a feature that enables supported endpoints to be onboarded into Microsoft Defender for endpoint and establishes baseline security policies across the Approved Environment. This includes:

(A) enabling and onboarding endpoints into Managed Microsoft Defender for endpoint;

(B) configuring and enforcing baseline security policies using Microsoft security technologies as described above;

(C) integrating Microsoft Defender with Microsoft 365 Defender portal and Intune;

(D) applying the standard Desired State Configuration for security policies to supported endpoints; and

(E) monitoring onboarding status and remediate failed enrolments where possible.

(ii) You acknowledge and agree that:

(A) you must provide access to identity and device management platforms (such as Entra ID, Intune);

(B) ASR rules and Windows Firewall apply only to Windows endpoints;

(C) equivalent protections for Apple devices (such as macOS and iOS) are limited to what Microsoft Defender for Endpoint supports on those platforms; and

(b) **Monitoring and Threat Protection**

(i) Monitoring and threat protection provides continuous monitoring of endpoint health and threat activity using the Microsoft Defender Security Centre (**Monitoring and Threat Protection**). This includes:

(A) monitoring endpoint health and threat activity through the Microsoft Defender Security Centre;

(B) investigating and responding to security alerts generated by Microsoft Defender for Endpoint;

(C) configuring and managing threat indicators, exclusions, and custom detection rules;

(D) responding to detected threats and alerts in accordance with agreed processes; and

(E) applying remediation actions as required to restore endpoint security.

(ii) You acknowledge and agree that:

(A) you must provide access to endpoint Devices and ensure supported OS versions are in place; and

(B) you must maintain endpoint patching cadence and OS health.

(c) **Vulnerability and Exposure Management**

(i) Vulnerability and exposure management provides threat and vulnerability management dashboards for endpoints (**Vulnerability and Exposure Management**). This includes:

(A) enabling and maintaining the Threat & Vulnerability Management dashboard for visibility of vulnerabilities and exposures;

(B) reviewing exposure scores and recommending remediation actions based on identified risks;

(C) coordinating patching and configuration changes with endpoint teams;

(D) identifying vulnerabilities and exposures on managed endpoints using the Threat & Vulnerability Management dashboard; and

(E) recommending and supporting remediation actions based on risk and exposure data.

(ii) You acknowledge and agree that you must review and act on any reasonable recommendations shared by the service team in the Managed Microsoft Defender Service Report.

(d) **Managed Microsoft Defender User Support**

(i) Managed Microsoft Defender User Support provides assistance to Users for security-related issues within the Approved Environment. This includes:

(A) assisting Users with security-related queries or Incidents (such as blocked applications, false positives, or alert notifications);

(B) providing guidance on safe practices and supported security features where relevant;

(C) log and investigate User-reported security issues through our ITSM system; and

(D) escalate unresolved or complex issues to the appropriate teams as required.

(ii) You acknowledge and agree that is limited to security-related issues within the Approved Environment and supported Microsoft Defender for endpoint features.

Managed Microsoft Defender Service Report

68.2 We will provide you with a monthly Managed Microsoft Defender Service Report in relation to your Managed Microsoft Defender service.

69 EXCLUSIONS

Managed Microsoft Defender does not include integration with third-party tools, custom security policies, or management of non-Microsoft security components (including Apple’s native firewall).

70 YOUR OBLIGATIONS

You must comply with any Customer Ongoing Responsibilities.

DEFINITIONS

In this TBMS section of Our Customer Terms, unless otherwise indicated:

(a) **Access Control** means the policies, processes and technologies used to authenticate Users and authorise their access to systems, applications, data or network resources.

(b) **Access Control Lists** means the rules to permit or deny traffic based on IP addresses, communication protocols or service ports used by specific applications (such as web or remote access).

(c) **Activation Date** means the date on which the activation criteria outlined in the respective individual Managed Service sections has been achieved.

(d) **Active User** means a User assigned to a licence or device and that has been authorised to use the TBMS.

(e) **Antivirus Management** means defining security policies, monitoring antivirus health, and providing regular reports to maintain visibility and compliance of Microsoft Defender within the Approved Environment.

(f) **Application Form** means the application form detailing the relevant Professional Services and/or the Solutioned Services, as applicable.

(g) **Approved Environment** means your technology components which are logged in your device inventory database maintained by us. This may include routers, switches, laptops, mobile devices and the M365 environment.

(h) **Authorised Customer Representative** means the designated representative for the customer, who acts as the primary point of contact.

(i) **Authorised Users** means the Users identified to us as such by the Authorised Customer Representative.

(j) **Backup Targets** means the appliance targeted for backup that is enrolled and active in Azure Backup in the Approved Environment.

(k) **Business Days** has the meaning given to it in clause 8.6.

(l) **Business Support Hours** has the meaning given to it in clause 8.6.

(m) **Call Out Fee** means the fees charged by us for on-premise visits, as described in your relevant Application Form and/or Order.

(n) **Casual Term** has the meaning given to it in clause 4.1(a).

(o) **Customer Onboarding Fee** means a one-time charge that covers the initial activities required to prepare, configure, and integrate a customer’s systems or environment into the managed service, ensuring readiness for ongoing management and support.

(p) **Customer Ongoing Responsibility** means the list of responsibilities that you must comply with, which we provide to you.

(q) **Customer Pre-Requisites** means the list pre-requisites that you must comply with under your selected TBMS, that will be provided to you by us during the ordering process.

(r) **Data Loss Prevention** or **DLP** means Microsoft Purview Data Loss Prevention.

(s) **Desired State Configuration** means a standard Telstra policy blueprint (which may change from time-to-time, including adapting to new versions or releases of Windows and MacOS) designed to enable proactive management, automated ticketing, real time monitoring of your Approved Environment through our IT Service Management (**ITSM**) platform (subject to available telemetric data).

(t) **Devices** means desktop, laptop, tablet or mobile devices enrolled within your Approved Environment.

(u) **Early Termination Charges** or **ETCs** has the meaning given in clause 11.7.

(v) **Executive and VIP Support** means personalised assistance for high-priority Users.

(w) **Fixed Term** has the meaning given to it in clause 4.1(b).

(x) **Incident** means an unplanned interruption to your Approved Environment, or reduction in the quality of your Approved Environment.

(y) **Incident Request** means a Support Request that relates to an Incident.

(z) **Initial Term** means the applicable period defined in clause 4.1.

(aa) **IR Teams** means the specialised Incident Response team responsible for containing and managing security Incidents.

(bb) **Law** means any law, including any common law, equity, statute, regulation, proclamation, ordinance, by-law, mandatory code of conduct, writ, judgment and any award or other industrial instrument.

(cc) **Managed IT Services Bundle** means the services identified in clause 3.3.

(dd) **Managed Services** has the meaning given to it in clause 2.2(a).

(ee) **Mitigation Strategy** has the meaning given to it in clause 21.3.

(ff) **Monthly Service Fee** means the monthly service fee as indicated in your Order.

(gg) **Network Devices** means the Wireless Access Point, Router and Switch devices, as set out in your Order.

(hh) **Order** means your proposed order, as approved by you through Telstra Apps Marketplace.

(ii) **Personal Information** has the same meaning given to it in the *Privacy Act 1988* (Cth).

(jj) **Pre-Requisite Order Form** means the document provided to you by us at the commencement of the ordering process.

(kk) **Professional Services** has the meaning given to it in clause 2.2(b).

(ll) **Renewal Term** has the meaning given to it in clause 4.2.

(mm) **Routers** means a router device(s) from Cisco, Juniper, Meraki or Zscaler that has passed a hardware assessment and is in warranty or still eligible for limited or extended support during the period of support by us.

(nn) **Service Credits** means the amount payable by us to you arising from a Service Level Default, as set out in clauses 8.19– 8.25.

(oo) **Service Desk** means the primary point of contact outside of Business Support Hours for 24/7 support but does not include engagement with third party support.

(pp) **Service Levels** means the service levels (if any) for your Managed Services, as specified in clause 8.

(qq) **Service Level Default** has the meaning given to it in clause 8.18.

(rr) **Service Level Targets** means the targets set out in clauses 8.15 and 8.17.

(ss) **Service Portal** means the portal provided by us, where you may access your Service Requests and service reports from time to time.

(tt) **Service Restoration Time Target** has the meaning given to it in clause 8.17.

(uu) **Service Request** means a Support Request that does not relate to an Incident and that relates to the services in relation to your Approved Environment.

(vv) **Service Ticket** has the meaning given to it in clause 8.4.

(ww) **Service Tier** means the Basic Tier, Standard Tier or Premium Tier, as specified in your Order or as otherwise agreed between you and us from time to time.

(xx) **Solutioned Services** has the meaning given to it in clause 2.2(c).

(yy) **Standalone Managed Services** means the services identified in clause 3.1.

(zz) **Support Request** has the meaning given to it in clause 8.1.

(aaa) **Supported Operating Systems** means a version of macOS or Windows that is currently supported by Apple or Microsoft (as applicable), and any other operating system determined by us acting reasonably, and as notified to you.

(bbb) **Supported Software** means a version of Microsoft 365 (including all Microsoft 365 applications) that is currently supported by Microsoft, and any other software determined by us acting reasonably, and as notified to you.

(ccc) **Supported Technology** means the Supported Software and/or the Supported Operating Systems (as applicable).

(ddd) **Switches** means a switch device(s) from Cisco, Juniper, Meraki or Zscaler that has passed a hardware assessment and is in warranty or still eligible for limited or extended support during the period of support by us.

(eee) **System-Initiated Requests** means automated alerts in response to monitoring activities we undertake.

(fff) **Telstra Apps Marketplace** means the ordering site used by us in order for you to approve your Orders, which may change from time to time.

(ggg) **Telstra Business Managed Services Rate Card** means the rate card setting out our fees for Managed Services, which is available on request.

(hhh) **User** means a user of your TBMS.

(iii) **User-Initiated Requests** has the meaning given to it in clause 8.1.

(jjj) **VIP Mailbox Protection** means personalised assistance for high-priority Users, ensuring prompt resolution and tailored configuration.

(kkk) **Voice Solution** means a voice solution as approved by us from time to time, such as Telstra Adaptive Collaboration, Microsoft Operator Connect and Telstra Calling for Office 365.

(lll) **Wireless Access Points** means a wireless access point device(s) from Cisco, Juniper, Meraki or Zscaler that has passed a hardware assessment and is in warranty or still eligible for limited or extended support during the period of support by us.