

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

CONTENTS

1	ABOUT THE TELSTRA ENTERPRISE MANAGED SERVICES SECTION	3
2	TELSTRA ENTERPRISE MANAGED SERVICES	3
3	SERVICE COMPONENTS	3
4	SERVICE CONFIGURATION MANAGEMENT (SCM).....	4
5	ONBOARDING.....	5
6	INFORMATION SECURITY MANAGEMENT.....	5
	Access Control to your Environment/Vendor Portal	5
	Permission Details	6
	Data Management	6
	Password and Credential Management.....	7
7	MONITORING AND EVENT MANAGEMENT	7
8	INCIDENT MANAGEMENT.....	8
	Service Request	10
	Escalation to Third Party Providers	10
	Escalation within Telstra	10
	Post Incident Review (PIR).....	10
	Your Responsibilities	11
9	PROBLEM MANAGEMENT.....	11
	Scheduled Maintenance	11
	Your Scheduled Maintenance.....	12
	Our Scheduled Maintenance	12
	Proactive Maintenance.....	13
	Vendor(s) Software Security Vulnerabilities	13
	Preventative Maintenance	13
10	SERVICE REQUEST MANAGEMENT.....	13
11	CHANGE ENABLEMENT	13
	Standard Changes	14
	Emergency Changes	14
	Normal Changes.....	14
12	RELEASE MANAGEMENT	15
13	DEPLOYMENT MANAGEMENT	15
14	CAPACITY AND PERFORMANCE MANAGEMENT.....	16
15	SERVICE LEVEL MANAGEMENT.....	16
	Service Level Commencement, Reporting and Application.....	16
16	MEASUREMENT AND REPORTING.....	17

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

17	RELATIONSHIP MANAGEMENT	17
	Service Transition	17
	Service Review	18
	Continual Service Improvement	18
18	TELSTRA ENTERPRISE HOSTING AND CONNECTIVITY SERVICES	19
	Pre-requisites and requirements	19
	Restrictions and limitations	21
	Agreed Data Locations	22
	Scheduled maintenance	22
19	DISENGAGEMENT SERVICES	22
20	PRE-REQUISITES	23
21	EXCLUSIONS	25
22	CHARGES	27
	Annual Rate Review	28
	Cost of Third Party Goods and Services	28
23	TERM, TERMINATION AND EARLY TERMINATION FEES	28
	Initial Term with a Commencement Date before 20 November 2023	28
	Initial Term with a Commencement Date on or after 20 November 2023	29
	Fixed Term Termination	29
	Minimum Commitment	29
	Early Termination Charges	29
24	YOUR RESPONSIBILITIES	31
25	DEFINITIONS AND INTERPRETATION	32

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

Certain words are used with the specific meanings set out in the General Terms of Our Customer Terms at <http://www.telstra.com.au/customer-terms/business-government/index.htm>

1 ABOUT THE TELSTRA ENTERPRISE MANAGED SERVICES SECTION

Applicable terms

- 1.1 In addition to this Telstra Enterprise Managed Services section of Our Customer Terms, unless we agree otherwise, the General Terms of Our Customer Terms (see <http://www.telstra.com.au/customer-terms/business-government/index.htm>) also apply.
- 1.2 See section one of the General Terms of Our Customer Terms for more detail on how the various sections of Our Customer Terms are to be read together.

2 TELSTRA ENTERPRISE MANAGED SERVICES

- 2.1 Telstra Enterprise Managed Services manage an agreed scope of your IT environments and associated components (**IT Environments and Components**) with comprehensive Information Technology Infrastructure Library 4 (**ITIL 4**) aligned services. Some of your IT environments and associated components may be hosted by us as part of the Telstra Hosting and Connectivity Services.
- 2.2 In addition to the terms set out in this section, service specific details for each component of your Telstra Enterprise Managed Service are set out in:
 - (a) the **Managed Service Description(s) (MSD(s))**; and
 - (b) where you purchase the Telstra Enterprise Hosting and Connectivity Service, the **Service Description (SD(s))**, attached to your Telstra Enterprise Managed Services Order.
- 2.3 Unless otherwise stated all Telstra Enterprise Managed Services are delivered remotely.
- 2.4 The features and functionality of the Telstra Enterprise Managed Services are dependent on the capabilities of the IT Environment and Components being managed and the ability of our systems to connect to the IT Environment and Components to obtain information.

3 SERVICE COMPONENTS

- 3.1 Subject to clause 3.3(a), the following ITIL 4 Practices are included as standard in your Telstra Enterprise Managed Services:
 - (a) Service Configuration Management;
 - (b) Monitoring and Event Management;
 - (c) Incident Management;
 - (d) Problem Management;
 - (e) Service Request Management;
 - (f) Change Enablement;

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

- (g) Release Management;
- (h) Deployment Management;
- (i) Capacity and Performance Management;
- (j) Service Level Management; and
- (k) Measurement and Reporting.

3.2 You can also apply for the following optional service component (for an additional charge):

- (a) Relationship Management.

3.3 If you require hosting and connectivity services in connection with your IT Environments and Components, you can also apply for the Telstra Enterprise Hosting and Connectivity Services. If you apply for, and we agree to provide, the Telstra Enterprise Hosting and Connectivity Services, then:

- (a) only the following ITIL 4 Practices are included as standard in your Telstra Enterprise Managed Services (unless otherwise set out in the applicable SD):
 - (i) Incident Management;
 - (ii) Service Request Management;
 - (iii) Problem Management; and
 - (iv) Change Enablement;
- (b) for clarity, all other ITIL 4 Practices identified in clause 3.1 do not apply to the IT Environments and Components that are subject to the Telstra Enterprise Hosting and Connectivity Services; and
- (c) we will provide the additional service components described in your Telstra Enterprise Hosting and Connectivity Services SD.

4 SERVICE CONFIGURATION MANAGEMENT (SCM)

- 4.1 Based on the information supplied by you and collected by the systems we utilise to manage ITIL 4 processes (**Service Management Systems**) or as agreed as part of an audit and within the capabilities of the Configuration Item (CI), we will store and update a Configuration Management System (**CMS**) of CI's relating to the managed IT Environment and Components.
- 4.2 Any Changes to the CI must be managed through the Change Enablement process to maintain the integrity of the CMS.
- 4.3 If you are making changes to your self-managed environments, which may impact any Telstra Enterprise Managed Services provided by us, you are responsible for ensuring all updates are supplied to us, for SCM.
- 4.4 We will maintain a register and copies of relevant documentation associated with the managed IT Environment and Components and their configuration.

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

5 ONBOARDING

- 5.1 Before your managed service can commence, any IT Environments and Components that are to be managed must be onboarded.
- 5.2 The following administrative activities are performed during the onboarding phase.
- (a) Your Company details, authorised contacts and signed contracts are registered within our systems.
 - (b) You will be assigned a Service Delivery Manager (If applicable).
 - (c) You will receive your Welcome Pack that includes vital information relating to your managed service. It will include:
 - (i) How to contact us to raise an incident, service request or general inquiry.
 - (ii) Access details to a Telstra provided Customer Management portal.
 - (iii) Access we require to administer your managed devices or environment.
 - (iv) Information relating to any tools or resources we will use to manage your devices or environment.
- 5.3 The following technical activities are performed during the onboarding phase Technical
- (a) Our Access: Our technical teams will work with you to obtain the relevant access to your IT Environments and Components. This will also include the secure sharing of any relevant passwords and account details.
 - (b) Monitoring: Our monitoring teams will work with you to setup monitoring for your IT Environments and Components. This will include the deployment of a virtual monitoring probe, credential configuration (API, SNMP, WinRM etc) and configuration of any thresholds.
- 5.4 Our Professional and Managed services technical teams will review all supplied technical documentation to confirm that all IT Environments and Components are accessible and are in a supportable state.
- 5.5 Onboarding Sign-off will be performed once all pre-requisite items have been satisfied and operational readiness has been confirmed. Your Managed Service and billing will then commence.
- 5.6 Please note that the onboarding experience and some of the above activities may not be required if you are already an existing customer.

6 INFORMATION SECURITY MANAGEMENT

Access Control to your Environment/Vendor Portal

- 6.1 We will require remote access and sufficient permissions to your environment and devices to perform the activities necessary to fulfill the managed service. Access to your environment must comply with your organisation's security policies, or should incorporate the following principles:

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

- (a) You should only provide us access the IT Environments and Components that are critical to the delivery of your Managed Service.
- (b) Remote access to your environment may be provided based on:
 - (i) any current methods your organisation uses today;
 - (ii) an alternate that can be negotiated with us and complies with your organisation's security requirements.
- (c) Our teams should be provided with individual user accounts that:
 - (i) follow the concept of "least privilege".
 - (ii) enforce strong hygiene such as 2FA/MFA, password complexity and length and require to be changed periodically, or as per your organisation's security policies.

6.2 Our staff will access your environment via their Telstra authorised devices (desktop/laptop/tablet) unless otherwise agreed.

Permission Details

- 6.3 The permissions required to administer your IT Environments and Components will vary based on your Managed Service.
- 6.4 Where we have configured accounts in your environment, they will be limited to providing support for services outlined in the applicable MSD. Details of permissions required can be provided upon request.

Data Management

6.5 Data Collection

- (a) You acknowledge and agree that as part of your Managed Service for your IT Environments and Components, Telstra Enterprise will:
 - (i) Collect device metrics and telemetry data using our monitoring tools.
 - (ii) Use collected data to observe, troubleshoot and diagnose issues.
 - (iii) Use for trending and/or recommendations
 - (iv) For reporting the purposes that will be presented or made available to you during service reviews.
- (b) Data collected will be retained for up to 12 months
 - (i) capture metrics from your managed devices as defined by the device servers and or monitoring tools. These metrics may be used (including after expiry or termination) as part of your Telstra Enterprise Managed Services.

6.6 Your Data

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

- (a) Backup and Disaster Recovery
 - (i) All data is exclusively protected and managed within the respective data protection or data replication product.
 - (ii) Telstra 's data management activities are expressly limited to data protection, data restore or virtual machine recovery activities within the respective data protection or replication product.
 - (b) Virtual Machines and Storage Systems
 - (i) All data held within your virtual machines or storage systems should not be accessible to Telstra Enterprise. Appropriate permissions should be applied to accounts used by Telstra Enterprise that prevent access to your information.
- 6.7 Telstra will provide to an authorised representative(s) within your organisation access to a Customer Management portal where you can view the services being managed by Telstra Enterprise and from where you can initiate a service request or incident.

Password and Credential Management

- 6.8 All local and service accounts related to the solution that are being managed by Telstra Enterprise are secured within a centralised credential repository.
- 6.9 All managed passwords adhere to Telstra Enterprise's standard password policies.
- 6.10 As part of our commitments to the security of your IT Environments and Components, passwords that we use to access your IT environment will not be shared with anyone for the duration of the managed service. Exceptions may apply only in extenuating or exceptional circumstances. Any passwords that have been shared in such circumstances will be rotated after an agreed period of time.

7 MONITORING AND EVENT MANAGEMENT

- 7.1 We will install a monitoring tool (supplied by us to be installed within your infrastructure which is required to perform remote monitoring of managed IT Environments and Components (**Monitoring and Event Management**)). The monitoring tool connects back to a central system using a secure encrypted connection, which allows for the delivery of system availability, performance, and capacity information back to our Managed Services Team (**Monitoring and Event Management System**). This information is then fed through our custom filters, and events are created via rules and agreed thresholds which are either automatically dealt with by our Service Management System or reviewed by our Managed Services Team to determine if an Incident should be raised.
- 7.2 The monitoring tool processes alerts and is combined with built-in call-home features that generate automated alerts and tickets within the Service Management System, unless otherwise specified in the MSD.
- 7.3 The monitoring provided with 24 x 7 x 365 support includes management of any P1 or P2 events after hours and we will contact you to confirm whether the incident requires investigation inside or outside of Business Hours.
- 7.4 The monitoring provided as part of your Monitoring and Event Management services is further detailed in the MSD(s) and is subject to the capabilities of the IT Environments and

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

Components being managed.

- 7.5 We will maintain the monitoring tool including patching, licensing and ongoing maintenance in line with our policies and procedures.
- 7.6 Each event collected by the monitoring tool and processed through the Service Management System is categorised as one of the three following types:
- (a) Informational – includes confirmation of a batch job or backup completion. This information is fed into the Managed Services Team's daily checks and on-going healthcare for managed IT Environments and Components;
 - (b) Warning – includes potential imminent failures or systems and processes that may have reached a predefined warning threshold, such as storage volume capacity reaching 80%. The Managed Services Team will then review and assess if any further preventative action is required in order to mitigate possible impact; and
 - (c) Critical – includes a system or process that has either reached a predefined critical warning level such as a storage volume capacity reaching 90%, or a system, service, environment or component down. The Managed Services Team will first assess the event to ensure that it is a genuine alert before initiating the Incident Management process.
- 7.7 All monitored metrics are dependent on the capabilities of the IT Environments and Components under management to present the information, which will be determined during the on-boarding of the managed IT Environments and Components. We will advise you if your IT Environments and Components do not have the capability to support a significant metric.

8 INCIDENT MANAGEMENT

- 8.1 All new Incidents will undergo an initial assessment of impact and urgency to determine the priority level using the matrix set out below. We will try to determine the number of users and/or systems affected and establish the impact to your managed IT Environments and Components. If a common position on the priority of the Incident cannot be agreed upon, your requested status will be used until an agreed priority status is met.
- 8.2 All Incidents will be recorded in our Service Management System under the incident management workflow.
- 8.3 The criteria for resolution are agreed as part of the initial impact assessment. Upon resolution, the Managed Services Team will contact the originator or your specified contact to advise of the resolution and confirm the criteria for resolution have been met prior to closing the ticket.
- 8.4 If the Managed Services Team are unable to contact the originator or your specified contact, a notification will be sent through to the Authorised Purchaser and the ticket automatically closed after 24 hours.
- 8.5 For Priority 1 Incidents we will facilitate, manage and co-ordinate the triage, escalation and notification functions in line with our Incident Management process for managed IT Environments and Components.
- 8.6 Below is the matrix we use to assess Incidents:

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

Business Impact	High	Significant P3	Major P2	Critical P1
	Medium	Minor P4	Significant P3	Major P2
	Low	Service Request	Minor P4	Significant P3
		Low	Medium	High
		Urgency		

8.7 The above priorities are defined as follows:

Priority 1 (P1)

- (a) To be classified as a P1 there must be an interruption impacting the whole organisation, a critical business application, or is causing a major commercial or publicity impact.
- (b) At this priority level both parties must commit to response times during Support Hours and involvement by all necessary and appropriate personnel until a mutually agreeable workaround is provided and the priority is no longer considered to be P1.
- (c) You must telephone through a P1 Incident for this to be accepted by us as a P1 Incident.

Priority 2 (P2)

- (a) To be classified as a P2, we must have lost access to a managed IT Environment or Component that is causing major impact to the business or in a state of degraded performance severely impacting business operations with no work around available.
- (b) At this priority level we are committed to provide a workaround and/or restore normal operations as quickly as possible during Support Hours.
- (c) You must telephone through a P2 Incident for this to be accepted as a P2 Incident by us.

Priority 3 (P3)

- (a) A P3 classification would include a degradation in performance with operational impact, however remains operational due to a workaround in place or an outage impacting a non-critical function or procedure.
- (b) At this priority level we will, during Business Hours, work towards a viable and mutually agreeable workaround or resolution or propose an upgrade or replacement to mitigate the problem.

Priority 4 (P4)

- (a) A P4 classification has minimal business risk and is isolated to a non-critical business

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

function. At this priority level we will, during Business Hours:

- (i) resolve the Incident; or
- (ii) provide advice on whether a workaround, upgrade or replacement to mitigate the Incident is available and work towards a viable and mutually agreeable workaround or resolution or propose an upgrade or replacement to mitigate the problem.

Service Request

- (b) A Service Request or request for information can be logged where there is no immediate impact to the business.
- (c) At this priority level we will, during Business Hours, respond to the request and provide the requested information or advice.

Escalation to Third Party Providers

- 8.8 We will escalate to a Vendor Incidents relating to managed IT Environments and Components in accordance with the agreed priority and the terms of the valid Vendor support agreement held by you and you acknowledge that we are authorised to act on your behalf for such escalation to a Vendor.
- 8.9 We will provide updates to you as they are made available to us by the Vendor. We will provide updates to you after Business Hours for Priority 1 Incidents only.
- 8.10 You acknowledge, we may be constrained by the level of Vendor support you have in place as we have no control of Vendor service levels or response obligations. Where you do not have an agreement in place with a Vendor, we cannot act on your behalf, and this will be your responsibility to engage the Vendor on any Incidents.

Escalation within Telstra

- 8.11 For an additional charge, where an Incident is raised by you, or detected by our Monitoring and Event Management System, relating to a Telstra service that is outside the Telstra Enterprise Managed Services, we will refer the incident to the relevant area and provide updates as per your support hours for that service. This is limited to impacted managed IT Environments and Components listed within the Order and MSD(s).
- 8.12 Service Levels for any Telstra services outside the Telstra Enterprise Managed Services apply to resolution of the Incident.
- 8.13 For escalation within Telstra please reach out to your Telstra Representative (available from Telstra Connect).

Post Incident Review (PIR)

- 8.14 On resolution of a Priority 1 Incident, we will conduct a PIR. Due to the complexities of root cause analysis this process can take time and may require support from you and Vendors, and there will be occasions where a root cause is not determined. Typically, a PIR will include a sequence of events from notification of a failure until resolution or a work around is put in place, any actions or changes implemented, determination of the root cause and any recommendations to help prevent the Incident from re-occurring.

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

Your Responsibilities

- 8.15 You must have an established first line support function that handles all contact with end users and carries out a technical triage of any issues reported.
- 8.16 You must undertake appropriate triage methods to ascertain the business impact of an Incident and confirm the Incident is related to the managed IT Environments and Components before contacting us.
- 8.17 Where requested, you must make available appropriately skilled persons while an Incident is being managed during Support Hours.

9 PROBLEM MANAGEMENT

- 9.1 Problem management is the determination of the root cause of an Incident to help reduce the chance of incident recurrence (**Problem Management**).
- 9.2 The Problem Management process will be instigated when a work around is put in place for an Incident where the root cause is either not known or requires further work to implement the final resolution. Problem Management for P1 Incidents is provided by default, whilst P2 Incidents require a request from you before analysis will be performed.
- 9.3 A Problem can be detected by several sources, including but not limited to:
 - (a) the Managed Services Team from a specific Incident;
 - (b) monitoring and alerting;
 - (c) Incident trend analysis;
 - (d) notification from vendor / security Incident;
 - (e) our known error records.
- 9.4 When a Problem is identified, we will gather all necessary information and perform root cause analysis.
- 9.5 If a Change is needed to fix a Problem, then a Request for Change will be initiated and put through the Change Management process.

Scheduled Maintenance

- 9.6 **Scheduled Maintenance** incorporates a period where works will be carried out that may or may not impact the managed IT Environment and Components.
- 9.7 You acknowledge that Scheduled Maintenance is required to keep systems working optimally and may require changes to a system and or an outage.
- 9.8 Scheduled Maintenance that will impact the managed IT Environment or Components must follow the Change Enablement process.
- 9.9 For the purposes of any availability calculation, systems that are unavailable for the duration of any Scheduled Maintenance will be deemed to be available and excluded from any Service Levels.

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

Your Scheduled Maintenance

- 9.10 **"Your Scheduled Maintenance"** incorporates Scheduled Maintenance to be undertaken by you that does not involve the Telstra Enterprise Managed Services or us.
- 9.11 You will advise us during Business Hours where it could be reasonably considered Your Scheduled Maintenance may impact the Telstra Enterprise Managed Services at least 24 hours prior to carrying out any such Scheduled Maintenance.
- 9.12 All notifications should be sent to the Telstra Service Desk via the Service Request process outlined in your Operations Manual.
- 9.13 You acknowledge that failure to comply with this section may result in Additional Service Charges should the Telstra Enterprise Managed Services be impacted.

Our Scheduled Maintenance

- 9.14 **"Our Scheduled Maintenance"** incorporates Scheduled Maintenance to be undertaken by us on our owned or operated systems that:
- (a) does not involve or impact the managed IT Environments and Components. This may include Proactive Monitoring, monitoring tools or Service Management Systems;
 - (b) where an outage is required on our owned system, we will follow an internal Change Enablement process with notifications published to you 72 hours prior to the scheduled start time.
- 9.15 We will endeavour to carry out Our Scheduled Maintenance that will impact the managed IT Environment and Components:
- (a) within the Scheduled Maintenance times referred to below,
 - (b) at other times with your agreement; or
 - (c) where it is needed to implement an Emergency Change.
- 9.16 We will advise you should the managed IT Environments or Components not be available during Our Scheduled Maintenance.
- 9.17 Unless otherwise stipulated in the applicable MSDs or SDs, the following table shows the agreed windows for Scheduled Maintenance implemented by us that impact your managed IT Environments and Components:

Service	System / Component	Primary Change Window	Secondary Change Window
All Services	All Environments	Second Wednesday each Month 6pm – 11pm	Second Sunday each Month 9am – 5pm
All Services	Systems that do not impact Environments	Any time at our discretion with 24 hours' notice	Any time at our discretion with 24 hours' notice

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

Proactive Maintenance

- 9.18 You will be notified of any issues which may affect availability or performance discovered during routine maintenance.

Vendor(s) Software Security Vulnerabilities

- 9.19 If vendor(s) environment is identified as having a Critical security vulnerability, then Telstra Enterprise will take action to remediate following the Vendor(s) recommendations; software releases and Change Management process.

Preventative Maintenance

- 9.20 Where recommended by us and in coordination with you, we will carry out regular and pre-scheduled checks to help maintain system operations, stability and security. Any findings will be reviewed and reported under the Service Request process.
- 9.21 Preventative maintenance tasks are further specified in the applicable MSDs and SDs.

10 SERVICE REQUEST MANAGEMENT

- 10.1 Service Request Management manages the lifecycle of all Service Requests.
- 10.2 We will record, respond and resolve Service Requests for managed IT Environments and Components, which could include:
- (a) request for general information,
 - (b) advice,
 - (c) procurement, and
 - (d) technical changes.
- 10.3 All Service Requests are listed in the Service Request Catalogue within the relevant MSD and/or SD.
- 10.4 If a Service Request requires Change Enablement, limits may apply and Additional Service Charges may be incurred. Refer to Section 11 Change Enablement for details.
- 10.5 Any Service Requests outside the Service Request Catalogue will incur Additional Service Charges.
- 10.6 We will provide you with information on the procedure for raising Service Requests during Onboarding.

11 CHANGE ENABLEMENT

- 11.1 All Standard and Normal Changes for each service are listed in the Service Request Catalogue within the relevant MSD and/or SD.
- 11.2 Service Requests that require the Change Enablement process to be followed are considered as either a Standard or Normal Change

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

11.3 All Changes are subject to the following minimum lead times:

- (a) Standard changes are up to five (5) business days
- (b) Normal changes are up to ten (10) business days

Standard Changes

11.4 **"Standard Changes"** are low risk, pre-approved Changes that can be implemented without additional authorisation.

11.5 To meet the "Standard" classification the Change must:

- (a) be low risk;
- (b) be relatively common and recurring;
- (c) be following an established standard operating procedure; and
- (d) not require any planning or consultancy effort.

11.6 We will action Standard Changes on managed IT Environments and Components during Business Hours.

11.7 These Standard Changes are provided on the basis that you accept them as pre-approved changes and no additional approvals or CAB processes are required for their implementation, and

11.8 You can raise an unlimited number of Service Requests that require the Change Enablement process to be followed and are defined as a Standard Change. Refer to the Service Request Catalogue outlined in the relevant MSD and/or SD.

11.9 Multiple Standard Change requests may be determined by us as a Normal Change.

11.10 A request to implement a Standard Change outside Business Hours will incur Additional Service Charges which will be advised and must be accepted in writing prior to works commencing.

Emergency Changes

11.11 An **"Emergency Change"** is a Change required in order to resolve or implement a tactical workaround for a P1 or P2 Incident. All Emergency Changes are subject to approval by both parties before implementation.

Normal Changes

11.12 **"Normal Changes"** are all Changes that are not classified as Standard Change or Emergency Change

11.13 Once assessed, the change will then be submitted for further technical review by us.

11.14 You can raise an allotted number of Service Requests per month that require the Change Enablement process to be followed and are defined as a Normal Change. Refer to the Service Request Catalogue outlined in the relevant MSD

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

- 11.15 We may, in our discretion, define high impact/high risk Normal Changes as a discrete bundle of related IT project activities that is completed in accordance with an agreed statement of work outside this agreement (**Project Service(s)**).

12 RELEASE MANAGEMENT

- 12.1 Software patch or firmware releases covering managed IT Environments and Components are reviewed by us frequently. Advice and recommendations are provided to you as to which releases should be considered for installation.
- 12.2 Minor releases that can, in our discretion, be completed as a Standard Change will be completed by us during Business Hours.
- 12.3 Minor releases required to resolve a P1 or P2 Incident will follow the Emergency Change process.
- 12.4 Major software upgrades (or otherwise subsequent major upgrades where listed in specific MSD) or upgrades classified as a Normal Change or Project Services will be reviewed and incur Additional Service Charges.

13 DEPLOYMENT MANAGEMENT

- 13.1 There are three classifications of patching:
- (a) **Urgent Release** – A patch release supported by the Vendor which is a dot release and addresses a known security issue which is applicable to the managed IT Environments or Components covered by the Telstra Enterprise Managed Services.
 - (b) **Minor Release** – A patch release supported by the Vendor that is a dot release and is recommended by us to overcome an issue impacting the managed IT Environments or Components or provide additional functionality that would be beneficial to you.
 - (c) **Major Release** – A patch or firmware release supported by the Vendor that will implement changes and/or add new functionality to the managed IT Environments or Components.
- 13.2 Remediation of any dependant services that are required to perform upgrades remain your responsibility unless the dependant services are provided by us.
- 13.3 Patching will be in accordance with Change Enablement processes and Scheduled Maintenance as follows:
- (a) Minor Releases that are Standard Changes will be completed by us during Business Hours.
 - (b) If Minor Releases cannot be completed as a Standard Change during Business Hours, then such Minor Releases will be applied by us in Support Hours as a Normal Change.
 - (c) Urgent Releases deemed applicable to your managed IT Environments or Components will be applied within 72 hours of such release being made available by the Vendor, using either the Standard or Emergency Change process as required.
- 13.4 Major software upgrades (or otherwise subsequent major upgrades where listed in specific MSD) are classified as a Normal Change, or Project Services, and will incur Additional

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

Service Charges.

14 CAPACITY AND PERFORMANCE MANAGEMENT

- 14.1 Capacity and Performance Management, where applicable for the managed IT Environments and Components, assesses current performance of the managed IT Environments and Components. We will provide current capacity and performance information, with recommendations, for your consideration of future business requirements on the managed IT Environments and Components.
- 14.2 We will provide Capacity and Performance Management information as part of Reporting, or this will be managed under the Incident Management process if there is a material impact on service.

15 SERVICE LEVEL MANAGEMENT

- 15.1 Service Level Management maintains and improves service quality through monitoring, reporting and reviewing IT service achievements.
- 15.2 The following table outlines the Service Level Targets and performance indicators associated with Incident and Change Enablement events associated with the managed IT Environments and Components.

Category	Service Level Target
P1 Incidents	98% of incidents responded to within 15 minutes
P2 Incidents	98% of incidents responded to within 30 minutes
P3 Incidents	98% of Incidents responded to within 4 hours during Business Hours
P4 Incidents	98% of Incidents responded to within 8 Business Hours
Normal Change	100% of Changes completed within CAB approved timeslot*
Standard Change	100% of Changes completed within approved timeslot*

** Completion of a Change does not indicate success or failure. A failed Change must be rolled back within the allocated timeslot as per approved rollback plan unless otherwise agreed with you.*

- 15.3 The Incident response service level target (or “incidents responded to” in table above) measures the time interval between the notification of an incident either from your notification by phone, an automated proactive alert, or manual discovery is identified by the Managed Services Team, and the time taken to issue a service ticket acknowledging the issue.

Service Level Commencement, Reporting and Application

- 15.4 Service Levels will commence the date we commence monitoring each IT Environments or Components using Proactive Monitoring.

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

- 15.5 Service Level reporting will commence from the first of the month subsequent to commencement of service levels and delivered on or around the second Thursday of the following month.

16 MEASUREMENT AND REPORTING

- 16.1 We will provide a report to you, detailing work completed. This will typically include the below:
- (a) all incidents, requests, problem records and changes logged during the month;
 - (b) performance reports (as outlined in the MSD(s)); and
 - (c) your managed IT Environments and Components availability statistics (as outlined in the MSD(s)).
- 16.2 Additional information may be reported on dependent on the Telstra Enterprise Managed Services we are providing to you. These reporting elements will be listed within the related MSD(s).

17 RELATIONSHIP MANAGEMENT

- 17.1 The Relationship Management process, if selected, will include the introduction of a Service Delivery Manager (**SDM**) to manage the service levels of your Telstra Enterprise Managed Services and your relationship with us.
- 17.2 If an SDM is selected and included in your Telstra Enterprise Managed Service, they will be responsible for the following:
- (a) customer on-boarding (pack and workshop)
 - (b) contract management
 - (c) quarterly or monthly service review meeting and report with additional content, including:
 - (i) service delivery minutes/actions
 - (d) escalation management
 - (e) Continual service improvement
- 17.3 A schedule of Service Review Reports & Meeting is agreed with you as part of onboarding.
- 17.4 In addition, the SDM will drive further Relationship Management functions as described below.
- 17.5 No governance meetings will be provided unless SDM is selected and included in the agreement.

Service Transition

- 17.6 The Managed Services Team will be responsible for transitioning systems and IT Environments and Components into the Telstra Enterprise Managed Services. This includes

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

confirming all required information is collected and the Service Management System, Proactive Monitoring and CMS are updated. The SDM will support the Managed Services Team during this process.

- 17.7 The SDM will provide an Operations Manual which provides important information covering the details of the Telstra Enterprise Managed Services and how to work with us.
- 17.8 If SDM is not selected the Operations Manual will be provided by the Telstra Enterprise Managed Service onboarding team.

Service Review

- 17.9 The Service Review and associated reports will provide an overview of your specific Telstra Enterprise Managed Services over a given period including a documented action register which is tracked and managed by the SDM. A standard Service Review will include:
- (a) reviewing report and content;
 - (b) discussing any identified risks to the Telstra Enterprise Managed Services;
 - (c) review existing operations meeting minutes and actions; and
 - (d) a customer business update.
- 17.10 Additional details of the items to be included in the Service Reviews for your Telstra Enterprise Managed Services are in the MSD/s and Operations Manual.
- 17.11 Service Review documents are either sent or presented to you during the second full calendar week of the following month based on the frequency established during the Telstra Enterprise Managed Service onboarding.
- 17.12 If SDM is not selected reports will be sent to you automatically. You must keep the customer recipient details up to date.

Continual Service Improvement

- 17.13 If selected, the SDM will take responsibility for making sure that information outlining the Telstra Enterprise Managed Service is available to all parties, meeting your reasonable expectations, and continuing to enhance value for you. To achieve this, the SDM will take responsibility for:
- (a) *P1 Incident Management* – the SDM will take a proactive approach to driving any major incidents and managing the outcomes of a P1 Incident;
 - (b) *Problem Management* – checking all Problem Management processes are followed and information and recommendations including PIR provided back to you;
 - (c) *Satisfaction Survey* – The SDM will present a bi-annual survey to allow you to provide impartial feedback and comments on Telstra Enterprise Managed Services performance; and
 - (d) *Continual Service Improvement* – A Service Improvement Plan (SIP) will be developed and managed by the SDM with you.

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

- 17.14 If SDM is not selected you can, via a Service Request, request the review of an Incident, Problem or service improvement initiatives.

18 TELSTRA ENTERPRISE HOSTING AND CONNECTIVITY SERVICES

What are the Telstra Enterprise Hosting and Connectivity Services?

- 18.1 Telstra Enterprise Hosting and Connectivity Services provide the underlying physical and virtual infrastructure for hosted virtual services which:
- (a) enables you to cost-effectively extend your corporate network and securely connect to multiple cloud service providers;
 - (b) includes a multi-tenancy network platform which spans datacentres across Australia; and
 - (c) are able to provide secure connectivity to various Software as a Service (**SaaS**) providers.
- 18.2 Telstra Enterprise Hosting and Connectivity Services can be provided as one of the following:
- (a) shared virtual resources;
 - (b) reserved virtual resources; or
 - (c) dedicated hardware.
- 18.3 Your selection, and the other details of your Telstra Enterprise Hosting and Connectivity Service, are set out in your Order.

Pre-requisites and requirements

The following is not considered complete or exhaustive and all Telstra Enterprise Managed Services sections of Our Customer Terms should be consulted:

- 18.4 In order to receive and use the Telstra Enterprise Hosting and Connectivity Services, you will need to enter into a separate professional services agreement with us for the integration of your network and cloud services on the terms set out in the [Professional Services section of Our Customer Terms](#) or your separate agreement with us, as applicable. The charges for that integration work will be set out in your separate agreement with us.
- 18.5 For each component of your Telstra Enterprise Hosting and Connectivity Service, you must order, and maintain for the term of that service, a corresponding Telstra Enterprise Managed Service.
- 18.6 You must:
- (a) order, and maintain for the term of your Telstra Enterprise Hosting and Connectivity Service at your own cost, any carriage services required in order to receive and use the Telstra Enterprise Hosting and Connectivity Services; and
 - (b) ensure that any components of your network and/or systems not provided by us, support any configuration needed to integrate the Telstra Enterprise Hosting and

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

Connectivity Services without extensive remediation or configuration. In particular, the following capabilities may be required:

- (i) port-channel feature on switching;
 - (ii) dynamic routing capability; and
 - (iii) spare switch ports for integration scenarios; and
- (c) provide us with any access we require in order to provide the Telstra Enterprise Hosting and Connectivity Service and any other related Telstra Enterprise Managed Services; and
- (d) obtain all relevant third party consents to:
- (i) provide us with the access contemplated in clause 18.6(c); and
 - (ii) allow us to access your IT Environments and Components, and integrate the Telstra Enterprise Hosting and Connectivity Service with your environment, without breaching any third party rights.

18.7 If you do not comply with clauses 18.4 to 18.6 then:

- (a) your Telstra Enterprise Hosting and Connectivity Services and associated Telstra Enterprise Managed Services may be adversely affected;
- (b) we are not responsible for any failure to comply with our obligations in respect of your Telstra Enterprise Hosting and Connectivity Services and associated Telstra Enterprise Managed Services to the extent we cannot do so because of your failure to comply with clauses 18.4 to 18.6; and
- (c) we may terminate your Telstra Enterprise Hosting and Connectivity Services and associated Telstra Enterprise Managed Services.

18.8 You indemnify us against any loss or damage that we suffer or incur and that arises naturally (that is, according to the usual course of things) as a result of any third party claim against us in relation to your breach of clause 18.6(d), except to the extent that the loss or damage arises from our negligence, breach of contract or breach of applicable law. We will also take reasonable steps to mitigate our loss or damage that we suffer or incur in connection with such a claim.

18.9 Additionally, if we or our third party service providers host your devices in our data centre racks or our third party service provider's data centre racks then:

- (a) you remain responsible for any such devices, including in relation to any required maintenance of those devices;
- (b) access to rackspace for the purposes of maintaining your devices or otherwise can be provided on separate terms and pricing, which will be notified to you on request; and
- (c) notwithstanding anything to the contrary in your agreement with us for the Telstra Enterprise Hosting and Connectivity Services, we accept liability arising from our breach of contract or negligence for any damage to those devices resulting from our supply of the Telstra Enterprise Hosting and Connectivity Services, but we limit our

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

liability to our choice of repairing or replacing those devices or paying the cost of repairing or replacing them.

18.10 If you do not comply with clause 24 then:

- (a) your Telstra Enterprise Hosting and Connectivity Services and associated Telstra Enterprise Managed Services may be adversely affected; and
- (b) we are not responsible for any failure to comply with our obligations in respect of your Telstra Enterprise Hosting and Connectivity Services and associated Telstra Enterprise Managed Services to the extent we cannot do so because of your failure to comply with clause 24.

Restrictions and limitations

18.11 You must not, and must ensure that your Authorised Users do not:

- (a) resupply, resell, sublicense or otherwise allow any other person to access or use the Telstra Enterprise Hosting and Connectivity Services;
- (b) modify, adapt, change, decompile, disassemble, reverse compile or otherwise reverse engineer all or any portion of the Telstra Enterprise Hosting and Connectivity Services, including any source code, object code, algorithms, methods or techniques used or embodied therein; or
- (c) use the Telstra Enterprise Hosting and Connectivity Services:
 - (i) to engage in any fraudulent or unlawful behaviour, or to defame, menace or harass any third party;
 - (ii) to gain unauthorised access to or interfere with any online resources or systems of any third party, including by any form of hacking;
 - (iii) to distribute unsolicited emails to third parties, including bulk unsolicited emails;
 - (iv) in any manner that is likely to result in our systems, or that of any other person, being affected by any virus, worm, Trojan or similar computer program;
 - (v) in a way that infringes the Intellectual Property Rights or any other rights of any person;
 - (vi) in a way that disrupts, misuses or excessively uses the hardware, bandwidth access, storage space or our other resources or the resources of our third-party service providers or other customers;
 - (vii) use any data mine, scrape, crawl, email harvest or any other process that sends automated queries;
 - (viii) for the purposes of accessing, storing, distributing, providing (including to us) or otherwise transmitting any information, data, materials or content that:
 - (ix) infringes the Intellectual Property Rights of any third party;

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

- (x) is unlawful, misleading, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;
- (xi) promotes unlawful violence;
- (xii) depicts sexually explicit images; or
- (xiii) is discriminatory or promotes discrimination based on race, gender, colour, religious belief, sexual orientation or disability.

18.12 The Telstra Enterprise Hosting and Connectivity Services are not designed or intended for use in on-line control of aircraft, air traffic, aircraft navigation or aircraft communications, or in the design, construction, operation or maintenance of any nuclear facility, or in the operation or in maintenance of any direct life support system, or in other hazardous environments or life threatening operations. Subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we disclaim any express or implied warranty, or statutory guarantee of fitness for such uses and are not liable for any costs, liabilities or damages resulting from the use of the Telstra Enterprise Hosting and Connectivity Services in such environments or operations, except to the extent such costs, liabilities or damages resulting from the use of the Telstra Enterprise Hosting and Connectivity Services in such environments or operations are caused or contributed to by our (or our contractors') negligence or breach of contract. You agree that you will not use the Telstra Enterprise Hosting and Connectivity Services for such purposes.

Agreed Data Locations

18.13 Your Data will be stored at the Agreed Data Locations. We will only move Your Data:

- (a) at your request or at the request of one of your Authorised Users;
- (b) if we are required to do so under applicable law; or
- (c) temporarily in emergency situations that require the data to be moved, such as emergency maintenance or to contain a cyber attack.

Scheduled maintenance

18.14 The Scheduled Maintenance provisions in clauses 9.6 to 9.21 apply in respect of the Telstra Purple Hosting and Connectivity Services.

19 DISENGAGEMENT SERVICES

19.1 If you notify us of your intention to terminate your agreement with us for the Telstra Enterprise Managed Services, or allow that agreement to expire, then subject to clause 19.6 and on written request we will:

- (a) develop a plan (**Disengagement Plan**) detailing the steps for and an agreed time period of disengagement (**Disengagement Period**), within 30 days of that written request;
- (b) continue to provide the Telstra Enterprise Managed Services during the Disengagement Period, in accordance with the terms of your agreement with us for those services;

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

- (c) provide all reasonable information and assistance you request in relation to the transfer of the Telstra Enterprise Managed Services to you or your nominated third party service provider (**Successor Service Provider**); and
 - (d) transfer your data access and account credentials back to you or a nominated third party in a reasonable format.
- 19.2 You may terminate the disengagement services described in clause 19.1 at any time on 5 Business Days written notice to us.
- 19.3 You must continue paying the applicable charges for your Telstra Enterprise Managed Services during the Disengagement Period, in accordance with the terms of your agreement with us for those services;
- 19.4 Unless otherwise agreed with you in writing (including in the Disengagement Plan), we will charge you for the disengagement services described in clause 19.1, and as set out in the Disengagement Plan, at our then current standard hourly rates, but only to the extent that those disengagement services do not form part of the Telstra Enterprise Managed Service.
- 19.5 Nothing in clause 19.1 requires us to disclose or transfer any of the following to you or any third party:
 - (a) our proprietary technology;
 - (b) our Intellectual Property Rights; or
 - (c) our technical, operational, billing, pricing or other commercial information.
- 19.6 Nothing in clauses 19.1 to 19.4 requires us to provide:
 - (a) the disengagements services described in those clauses; or
 - (b) any Telstra Enterprise Hosting and Connectivity Services or related Telstra Enterprise Managed Services, including during any Disengagement Period,

if you do not pay us the applicable charges for those services in accordance with our agreement with you for those services.

20 PRE-REQUISITES

- 20.1 Before the Services can start, the following prerequisites (and any prerequisites included in the Order) must be met by you to allow for a transition and delivery of the Telstra Enterprise Managed Services and prior to Service Levels commencing.
- 20.2 You may engage us to assist with these prerequisites as part of Project Services.
- 20.3 You acknowledge that we are the sole administrators of environments managed by us.
- 20.4 You must provide, at your expense:
 - (a) the following documentation and information (which must be current and an up to date reflection of the IT Environments and Components to be managed at time of handover):

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

- (i) a completed information gathering questionnaire/s as provided by us in advance of scheduled implementation work (if being provided);
 - (ii) a completed managed services provisioning template as provided by us covering the full list of IT Environments and Components; and
 - (iii) access to documentation representing the current build and architecture of the environment including connectivity diagrams and configuration covering all IT Environments and Components;
- (b) remote access to all IT Environments and Components to be managed to deliver the Telstra Enterprise Managed Services;
 - (c) credentials with appropriate level of access to all managed IT Environments and Components, including access to consoles and management interfaces;
 - (d) user accounts required by us and created and tested by you to verify appropriate access;
 - (e) details of the relevant Vendor contracts relating to managed IT Environments and Components;
 - (f) access to the relevant Vendor acting on your behalf to log and manage Incidents and escalations; and
 - (g) named User account creation for our staff.

20.5 You must:

- (a) provide infrastructure resources to be used for the monitoring tool(s) based on our recommendations;
- (b) provide secure access to allow monitoring tool communications via the internet back to our Proactive Monitoring systems;
- (c) allow us access to internet resources to obtain required monitoring software for the monitoring tools;
- (d) enable connectivity throughout the infrastructure for monitoring tools to access every IT Environment and Component; and
- (e) configure in-scope IT Environments and Components to allow monitoring tool access to management information. This includes the monitoring systems for your IT Environment to be configured to forward system alerts into our managed services environment. If it is not possible to forward system alerts into the Service Management Systems, then this may invalidate any service level agreements.

20.6 You agree that we remain the owner and administrator of the monitoring tool(s). Any changes or requirements to alter, move or otherwise modify the monitoring tool(s) will require our prior approval. Failure to do so may result in the inability to deliver the Telstra Enterprise Managed Services.

20.7 To enable us to provide the Telstra Enterprise Managed Services, you agree that you will (at your expense) perform certain tasks which include, but are not limited to:

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

- (a) where a monitoring tool is installed on your infrastructure, ensuring the server is maintained and has access to in-scope IT Environments and Components and we have access to manage;
- (b) ensuring an on-going availability of suitable connectivity for us to the IT Environments and Components located on your controlled premises for the purposes of performing the Telstra Enterprise Managed Services;
- (c) ensuring all managed IT Environments and Components owned by you and supported under these Telstra Enterprise Managed Services are licensed at the appropriate level and have the required support in place to enable escalations to the Vendor, and that we have authority to access this support;
- (d) maintaining IT Environments and Components managed as part of the Telstra Enterprise Managed Services based on Vendor or Telstra Enterprise's recommendations particularly when known bugs or issues exist;
- (e) ensuring we retain full 'administrative' access to in-scope IT Environments and Components and monitoring tool(s);
- (f) unless otherwise stipulated in your Order, ensuring that valid data and configuration backups are managed, including where applicable deploying a SFTP server to enable us to forward backups for your environment. These backups should be available should the need arise to reinstate data or configuration on an environment or a system not covered by the Telstra Enterprise Managed Services;
- (g) advising us of any changes or outages controlled by you that may impact the Telstra Enterprise Managed Services; and

20.8 Any IT Environments or Components found to be end of support and not under Vendor support or a third party managed contract during the Service Term will be supported on a Best Efforts basis, and will exclude us from service level obligations, Release Management, Problem Management, Change Enablement and managed IT Environments and Components repair or replacement management obligations. If you require us to perform these services, such service will be provided subject to Change Enablement stipulations and Additional Service Charges may apply.

21 EXCLUSIONS

21.1 The following service level components are excluded from the Telstra Enterprise Managed Services:

- (a) data restoration on managed IT Environments and Components (unless covered by a service as described in relevant attached MSD(s) or SD; and
- (b) end user support or technical advice to any persons not listed as a named contact in our systems.
- (c) all costs and activities associated to external auditing or compliance;
- (d) remediation actions to resolve identified issues as a result of an audit or compliance assessment;
- (e) On site support;

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

- (f) Attendance to customer change meetings.
- (g) Any solution design changes or custom development;
- (h) Sourcing, financing, or providing any technical training;
- (i) The implementation of service improvement initiatives will be presented to you during scheduled service review (If Applicable) governance meetings and confirmation as to whether Additional Service Charges apply, for subsequent implementation[N

21.2 Unless otherwise agreed in writing, we are not responsible for a failure to meet a Service Level to the extent that you cause the failure as a result of:

- (a) a breach of your obligations under these terms or the terms of an Order,
- (b) misconfiguring a platform which directly impacts the managed IT Environments and Components
- (c) causing a catastrophic equipment failure due to an undocumented bug introduced on an application or IT system,
- (d) negligent acts or omissions,
- (e) incidents arising from you or your personnel's lack of training;
- (f) implementing changes which directly impacts the managed IT Environments and Components,
- (g) failing to follow our reasonable directions which directly impacts the managed IT Environments and Components,
- (h) not providing us with full and accurate information detailing any requests or relating to any Incidents reported to us; or
- (i) failing to comply with a request from us to maintain sufficient capacity or performance levels including but not limited to:
 - (i) sufficient storage capacity for virtual disks,
 - (ii) network bandwidth,
 - (iii) compute capacity; or
 - (iv) such failure which directly impacts the managed IT Environments and Components.

21.3 Unless otherwise agreed in writing, we are not responsible for a failure to meet a Service Level due to:

- (a) a failure caused by a third party (other than our contractors);
- (b) limitations of your Vendor or third-party support agreement;
- (c) circumstances outside of our reasonable control; or

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

- (d) any third-party software or equipment used, operated or interfaced with your IT Environments and Components not provided by us.

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

- (a) where there is a breach by you of:
 - (i) these terms or the terms of an Order;
 - (ii) the responsibilities assigned to you in relation to the relevant products as part of the managed IT Environments and Components; or
 - (iii) any documents provided by us as part of the managed IT Environments and Components;
- (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 Telstra Enterprise Managed Services;
- (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 unless a Change Request has been formally raised and accepted by all parties; or
- (d) any support and maintenance outside our responsibilities.

22 CHARGES

22.1 The charges for your Telstra Enterprise Managed Services are set out in your Order.

22.2 Billing for the Monthly Recurring Charges (**MRC**) of your Telstra Enterprise Managed Services will begin on the earlier of:

- (a) the date we start monitoring the first IT Environment or Component;
- (b) the date we start supporting your IT Environments and Components;
- (c) if you take up the Telstra Enterprise Hosting and Connectivity Service, the date on which it is provisioned;
- (d) on completion of onboarding activities; or
- (e) a date in time which we mutually agree in writing with you,

the "**Billing Commencement Date**".

22.3 Where pricing for the Telstra Enterprise Managed Service is based on a per unit model, unless otherwise detailed and agreed in writing, as IT Environments or Components are deployed, and supported MRC's will be based on a pro-rata basis.

22.4 Some components of the Telstra Enterprise Managed Services may be completed post Billing Commencement Date.

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

22.5 If Services are unable to be onboarded, or utilised by you due to a delay caused by:

- (a) your failure to complete your responsibilities or obligations under your agreement with us for the Telstra Enterprise Managed Services; or
- (b) any other third-party reason where the third party is acting on your behalf and which we are not directly responsible for,

we will advise you in writing of the Billing Commencement Date which will be no later than 45 days from the Commencement Date.

Annual Rate Review

22.6 Subject to clause 22.8, for Telstra Enterprise Managed Services on a Fixed Term, the charges will remain fixed for the first twelve (12) months from the Commencement Date. Upon the completion of each annual anniversary of the Commencement Date, the then current pricing as set out in the Order may be adjusted in accordance with the clause below.

22.7 We may adjust the charges annually to reflect any fluctuations due Consumer Price Index (CPI) provided that:

- (a) we notify you of any revised charges as soon as practicable following the annual review; and
- (b) the revised charges do not exceed the amount of the CPI increase.

Cost of Third Party Goods and Services

22.8 We rely on third party goods or services in order to provide the Telstra Enterprise Hosting and Connectivity Services to you (**Third Party Goods and Services**). If the cost of acquiring or procuring such Third Party Goods and Services from the relevant third party provider increases (other than based on an increase in CPI), then we may increase our charges to you in respect of those Third Party Goods and Services by a reasonable amount corresponding to the increase in the cost of acquiring or procuring such Third Party Goods and Services from the relevant third party provider. We will provide you with reasonable advance written notice of any such increase.

22.9 Unless otherwise stated in your agreement with us, if the increased charge which we notify to you under clauses 22.7 and 22.8 is more than 20% of the charges immediately prior to the date of our notification you may cancel the Services and/or Deliverables by notice to us within 5 business days of the date we notify you of the increased charges. Where you exercise this right to cancel, you must pay us for all Services and Deliverables provided up to the date of cancellation and must pay any additional charges specified in your agreement with us, except you are not required to pay any other early termination charges.

23 TERM, TERMINATION AND EARLY TERMINATION FEES

Initial Term with a Commencement Date before 20 November 2023

23.1 Your Telstra Enterprise Managed Services will start on the Commencement Date and continue for the period specified in your Order (**Initial Term**).

23.2 Unless otherwise set out in an applicable MSD or SD:

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

- (a) if the Initial Term is longer than one month (**Fixed Term**), it will automatically renew at the end of the Initial Term on a month-to-month basis (**Renewal Term**) unless terminated earlier in accordance with the termination clause below; and
- (b) if your Initial Term is one month or less (**Casual Term**), it will automatically continue until terminated by either party by giving the other party at least 7 days prior written notice.

Initial Term with a Commencement Date on or after 20 November 2023

- 23.3 Your Telstra Enterprise Managed Services will start on the Commencement Date and continue for an initial period and subsequent renewal period specified in your Order or separate agreement with us (being the **Initial Term**, **Renewal Term** and **Casual Term** as applicable).
- 23.4 We will provide you with reasonable advance notice that your Fixed Term is about to be renewed. If we fail to provide you with reasonable advance notice, you may terminate your Telstra Enterprise Managed Services at any time after your service has renewed by giving us not less than 30 days' prior written notice without having to pay any early termination charges.

Fixed Term Termination

- 23.5 Your Telstra Enterprise Managed Services will terminate at the end of the Initial Term or the then-current Renewal Term (as the case may be) if either party notifies the other in writing not less than 60 days prior to the end of the Initial Term or then current Renewal Term (as the case may be) that they do not wish to renew the Telstra Enterprise Managed Services for a further Renewal Term.

Minimum Commitment

- 23.6 If you have a Fixed Term, you may request in writing, in accordance with this clause, a variation of the Telstra Enterprise Managed Services to meet your changing requirements and demands. When such variations result in a reduction to the Monthly Recurring Charges (MRC), the resulting MRC total may not be lower than 75% of the higher of:
 - (a) The MRC as at the Billing Commencement Date; or
 - (b) The average MRC over the previous 3 months.

Early Termination Charges

- 23.7 If you have a Fixed Term and during the Initial Term you terminate the Telstra Enterprise Managed Services for any reason other than our material breach, we may charge you an Early Termination Charge (**ETC**) for the Telstra Enterprise Managed Services with the amount equal to the actual costs and expenses that we have incurred or committed to in anticipation of providing the service to you and that cannot be reasonably avoided by us as a result of the cancellation, which will not exceed an amount calculated as follows:

Number of Remaining Months	Early Termination Charge
37 – 60 months	18 months of Monthly Recurring Charges

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

25 – 36 months	12 months of Monthly Recurring Charges
13 – 24 months	8 months of Monthly Recurring Charges
5 - 12 months	4 months of Monthly Recurring Charges
0 – 4 months	50% of the remaining Monthly Recurring Charges

If you take up the Telstra Enterprise Hosting and Connectivity Service, in addition to the ETC calculated in accordance with the table above, we may also charge you an ETC for the Telstra Enterprise Hosting and Connectivity Service calculated as follows:

$$\text{ETC} = A + B + C$$

where

- A** = the unavoidable and unrecoverable cost of any fixed term third party licence that we purchase in respect of your Telstra Enterprise Hosting and Connectivity Service, prorated based on the number of months remaining in your Initial Term or Renewal Term (as applicable);
- B** = the unrecoverable cost of any hardware (corresponding to the decreased value of the hardware calculated based on Telstra's ability (using reasonable efforts) or inability to reuse the hardware within 60 days after the termination of your Telstra Enterprise Hosting and Connectivity Service) that we purchase specifically to provide your dedicated Telstra Enterprise Hosting and Connectivity Service; and
- C** = the unavoidable and unrecoverable costs of any third party service (other than third party licenses) we acquire for the purposes of providing the Telstra Enterprise Hosting and Connectivity Service, prorated based on the number of months remaining in your Initial Term or Renewal Term (as applicable).

- 23.8 During your Renewal Term, you can terminate your service at any time by giving us not less than 30 days' prior written notice but we may charge you an amount equal to the actual third-party costs and expenses that we have incurred or committed to in anticipation of providing the service to you and that cannot be reasonably avoided by us as a result of the termination.
- 23.9 You acknowledge that this amount is a genuine pre-estimate of the loss Telstra Enterprise are likely to suffer.
- 23.10 The ETC's will be in addition to any outstanding charges due pro-rated to last payment.
- 23.11 Any charges which have been incurred are non-refundable in event of early termination.
- 23.12 The ETC will be in addition to any charges associated with disengagement services.
- 23.13 ETC's may also apply for additional services as listed in any MSDs or SD.

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

23.14 There are no early termination fees for Telstra Enterprise Managed Services on a Casual Term.

23.15 If a Telstra Enterprise Managed Service is cancelled or terminated for any reason:

- (a) on and from the termination date you must remove our access to your systems and environment being managed by or in connection with that Service, and immediately cease using the relevant Telstra Enterprise Managed Services;
- (b) you must pay us all outstanding invoices for the Telstra Enterprise Managed Services by their due date; and
- (c) all rights a party has accrued before expiry, termination or cancellation continue.

24 YOUR RESPONSIBILITIES

24.1 Unless expressly identified otherwise in this section of Our Customer Terms or your Order (including any MSD(s) or SD(s)), you must:

- (a) notify us of any planned or scheduled maintenance and system downtime that either you or your third party suppliers instigate, which may affect your IT Environments and Components, including environmental changes;
- (b) obtain, maintain and manage any relevant third-party maintenance and support contracts;
- (c) give us adequate notice of any upgrade to, or modification of, your IT Environments and Components that may affect the availability, support or compatibility of the Telstra Enterprise Hosting and Connectivity Service with your IT Environment and Components;
- (d) pay any third party charges relating to your environment;
- (e) provide all necessary end user support and training to your Authorised Users;
- (f) ensure 24x7x365 availability of a suitable escalation contact who is authorised to approve emergency changes and engage other aspects of your support functions;
- (g) provide any project management required for your company specific activities. We do not provide any project management services as part of the Telstra Enterprise Hosting and Connectivity Services or any other related Telstra Enterprise Managed Services;
- (h) provide us with contact details and roles of personnel we may need to contact in connection with your Telstra Enterprise Hosting and Connectivity Services or any other related Telstra Enterprise Managed Services (such as Executive and Senior Management, Business Analysts, Architects, Systems Architects, Systems Engineers, and Network Engineers) and ensure those personnel are available to provide us with information, and participate in scheduled information gathering sessions, meetings and calls;
- (i) perform any testing we require;
- (j) coordinate the availability and assistance of any other third party suppliers or service

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

providers that may be required as part of any service integration testing; and

- (k) provide us with either process documentation or an authorised contact for user account administration activities such as account unlock, password reset and 2FA/MFA support.

25 DEFINITIONS AND INTERPRETATION

25.1 In this section unless otherwise indicated:

Authorised User means any person who you authorise to access or use the Telstra Enterprise Hosting and Connectivity Services.

Additional Service Charges means a charge or charges that are advised and must be accepted by you in writing before a chargeable service action can take place.

Agreed Data Locations means the data centre locations set out in your Order.

Best Efforts means we will do everything that can reasonably be done to help manage a service that is no longer supported by a Vendor and is without Service Levels from us.

Change/s means the addition, modification or removal of anything that could have a direct or indirect effect on the Telstra Enterprise Managed Services.

Change Enablement is an ITIL 4 Practice that has the purpose of maximising the number of successful service and product changes by checking that risks have been properly assessed, changes have been authorised to proceed and change schedules have been managed.

Commencement Date means the date set out in your Order or if no date is specified the date the first day that the Telstra Enterprise Managed Services are installed or provisioned and are ready-for use, as determined by us.

Configuration Management System (CMS) means a set of tools, data and information that is used to store information for configuration items (components that need to be managed) within the designated scope of the Telstra Enterprise Managed Services.

Incident(s) means an unplanned interruption to a service or a reduction in quality of a service in your managed IT Environments or Components.

Incident Management is an ITIL 4 Practice that defines the appropriate management of incidents based on their impact.

Intellectual Property Rights means all current and future registered rights in respect of copyright, designs, circuit layouts, trademarks, trade secrets, domain names, database rights, know-how and confidential information and any other intellectual property rights as defined by Article 2 of the World Intellectual Property Organisation Convention of July 1967.

IT Environments and Components has the meaning given to it in clause 2.1 of this section of Our Customer Terms.

Managed Services Team means the Telstra Enterprise team who manages your IT Environments and Components in accordance with your MSD(s) or SD.

OUR CUSTOMER TERMS

TELSTRA ENTERPRISE MANAGED SERVICES

Operations Manual means the document we provide once onboarding has been completed. It contains operating procedures, processes and environmental information pertaining to your managed IT Environments and Components which sets out the processes and procedures that together will be used in the day to day operational management of your Telstra Enterprise Managed Service.

Order means any application form, statement of work or other order placed by or on behalf of you for Telstra Enterprise Managed Services and accepted by Telstra Enterprise (in our discretion).

Proactive Monitoring refers to Telstra Enterprise's systematic observation of managed IT Environments and Components and includes recording and reporting on changes of state.

Request for Change means a request from a user or user's authorised representative for the addition, modification or removal of anything that could have a direct or indirect effect on the managed IT Environments and Components.

SaaS has the meaning given to it in clause 18.1(c) of this section of Our Customer Terms.

Scheduled Maintenance means activities or tasks that are which are scheduled in advance and performed so assets can remain functional for as long as possible without unplanned downtime. Scheduled Maintenance is determined by us based on maintenance triggers including time, usage, event and condition.

Service Description (SD) or Managed Service Description (MSD) has the meaning given to it in clause 2.2 of this section of Our Customer Terms.

Service Levels means the service levels (if any) for your Telstra Enterprise Managed Services specified in this Telstra Enterprise Managed Services section or MSD or SD.

Service Management System means platforms or applications we use to implement and deliver Telstra Enterprise Managed Services on behalf of customers.

Service Request means a request from a user or user's authorised representative for information, advice, a Standard Change or access to a service.

Term means the term of the Telstra Enterprise Managed Services as described in clause 20.

Vendor means a third party supplier of a platform, service or application in your IT Environments and Components where the relationship is owned by either you or us.

Your Data means the data that you store on, or transmit via, the Telstra Enterprise Hosting and Connectivity Services.