TELSTRA BUSINESS SYSTEMS PRODUCTS AND SERVICES SECTION

CONTENTS

TELSTRA BUSINESS SYSTEMS PRODUCTS AND SERVICES SECTION

1 ABOUT THIS SECTION

1.1 This is the Telstra Business Systems (**TBS**) Products and Services section of Our Customer Terms.

1.2 If you are a small business customer, these General Terms of Our Customer Terms apply. If you are a corporate customer, these General Terms of Our Customer Terms apply.

Inconsistencies

1.3 If the General Terms of Our Customer Terms are inconsistent with something in this section, then this section applies instead of the applicable General Terms of Our Customer Terms to the extent of the inconsistency.

1.4 If a provision of this section gives us the right to suspend or terminate your service, that right is in addition to our rights to suspend or terminate your service under the General Terms of Our Customer Terms.

2 WHAT ARE TELSTRA BUSINESS SYSTEMS PRODUCTS AND SERVICES?

Description

2.1 TBS products or services are comprised of some or all of the following:

(a) TBS Equipment and Services (including associated installation and professional services);

(b) Telstra Business Systems Care (see existing product terms at Our Customer Terms Telstra Business Systems Care);

(c) Network Device Installation;

(d) Cyber Security Audit;

(e) Cyber Security Remediation;

(f) Network Device Management;

(g) Telstra Install – Microsoft 365 Business; and

(h) Managed Microsoft 365.

(i) Managed Cyber Security – Check Point Harmony;

(j) Telstra Data Protect Installation

(k) T-Rooms Videoconferencing (see existing product terms at Our Customer Terms - Internet Direct and Business Broadband)

2.2 Your solution under Telstra Business Systems comprises the TBS Products and Services set out in your Application Form.

3 GENERAL

Term

3.1 Our agreement with you for your solution under TBS begins on the date that we accept your signed Application Form for your solution under TBS (‘**Start Date**’) and continues until it is terminated in accordance with these terms or all of your TBS Products and Services have either expired or have been terminated in accordance with these terms.

3.2 Unless otherwise set out in your Application Form or these terms, each of your TBS Products and Services will continue to be billed on a month to month basis on the existing terms (including price) at the end of the applicable minimum term set out in the relevant Application Form, unless either party notifies the other (at least 30 days before any automatic extension) that it does not want the service to extend automatically.

Services and Payment

3.3 The TBS Products and Services must be ordered, supplied and billed against the nominated accounts agreed by the parties.

3.4 If you dispute an invoice, you need not pay the disputed amount until the dispute is resolved, however you must pay all undisputed amounts by the due date.

3.5 If you do not pay any amount due under this Agreement on time, we may:

(a) on 7 days' notice, decrease or withdraw any off-tariff or discounted pricing for those Services until all unpaid amounts are paid; and

(b) charge you interest (calculated on a daily basis) at an annual rate equivalent to the Official Cash Rate set by the Reserve Bank of Australia plus 5%, on any unpaid amounts.

3.6 If your Application Form specifies a minimum volume or amount for one or more of the TBS Products and Services (‘**Relevant Services**’) in a Quarter, and you do not achieve at least 90% of that minimum volume or amount, we may on 7 days’ notice decrease or withdraw any off-tariff or discounted pricing for the Relevant Services for any subsequent Quarters until you achieve in a subsequent Quarter 100% of the minimum volume or amount for the Relevant Service (based on the previous off-tariff or discounted pricing in the relevant Application Form). For the purposes of this Agreement, "Quarter" means 3 calendar months beginning on the first day that your off-tariff or discounted pricing is implemented into our billing systems and each 3 calendar month period after that.

Annual CPI Adjustment

3.7 This clause applies if you sign up for or recontract your TBS Products and Services on or after 21 February 2024 and you purchase managed services with a minimum contract term of 12 months or longer:

(a) The prices for the managed services will remain fixed during the first 12 months from the commencement of the contract term (“**Start Date**”).

(b) At any time after the first 12 months, we may, by giving you reasonable advance

notice, increase the prices for a managed service by a percentage amount no greater than CPI (rounded to the nearest dollar), provided that we only exercise this price increase right no more than once in any 12-month period.

(c) In this clause, **CPI** means the percentage annual change in the Consumer Price Index All Groups weighted average for the 8 capital cities as published by the Australian Bureau of Statistics (ABS) immediately before the date of our price increase notice.

Invoicing

3.8 Subject to clause 3.8, the TBS Products and Services you order will be invoiced from the completion date specified on the signed Customer Acceptance Certificate, which confirms your acceptance of the work completed by us in the engagement. If a minimum term applies, the minimum term begins on the completion date specified in the Customer Acceptance Certificate.

3.9 We reserve the right to invoice you for your TBS Products and Services before you sign a Customer Acceptance Certificate if you do not sign and return one within a reasonable period of us completing the applicable Service Deliverables. In this instance, if a minimum term applies, the minimum term will begin upon commencement of billing for your TBS Products and Services.

Termination

3.10 If for any reason our agreement with you for any of the TBS Products and Services expires or is terminated:

(a) you must pay us all outstanding invoices by the due date and within 30 days of request for payment, all other amounts outstanding as at the date of, or arising as a result of, expiry, termination or cancellation (including any applicable early termination charges); and

(b) all rights a party has accrued before expiry, termination or cancellation continue.

3.11 If for any reason our agreement with you for any of the TBS Products and Services expires or is terminated, clauses 3.10 and 3.12 - 3.17 continue in full force and effect.

General

3.12 You must not disclose any of our technical, operational, billing, pricing or other commercially confidential information to any third party without our consent.

3.13 You agree that we may send commercial electronic messages (including information about our products and services) to each of the electronic addresses for which you are the account holder, unless you tell us otherwise.

3.14 You and we agree to use best endeavours to resolve in good faith any disputes or claims concerning our agreement with you for the TBS Products and Services. If the parties cannot resolve the dispute, the parties must try to resolve it by mediation administered by the Australian Commercial Disputes Centre according to its Mediation Guidelines before starting court proceedings (except for urgent injunctive or declaratory relief).

3.15 Our agreement with you for the TBS Products and Services is governed by the laws of the Australian State or Territory in which your principal place of business is located. Each party submits to the non exclusive jurisdiction of the courts of that place and the courts of appeal from them.

3.16 We may sub-contract any or all of the services to be performed in connection with the TBS Products and Services without your prior consent.

3.17 If you lease customer premise equipment ('**CPE**') through a financier approved by us your nominated account invoice may include a rental component for a specific period for that CPE which you agree to pay us. By paying us the rental component your obligations for that rental component is satisfied for that period. Our right under the General Terms of Our Customer Terms to terminate your Service if you don't pay an invoice includes a failure to pay any finance charges included in the invoice.

CallN Service

3.18 If you acquire the CallN Service from us, in connection with your solution under TBS or otherwise, the terms and conditions set out at www.telstra.com.au/customer-terms/business-government, Other Services, CallN section will govern the provision of your CallN Service.

4 SALE AND INSTALLATION OF EQUIPMENT AND SERVICES

Sale of Equipment

4.1 We will provide you with the Telstra Supplied Equipment as detailed in your Application Form (if any), on the terms and conditions in this clause 4.

4.2 We agree that:

(a) we will deliver the Telstra Supplied Equipment in accordance with the delivery conditions set out below;

(b) on the later of:

(i) you signing a Customer Acceptance Certificate as contemplated in clause 4.40; or

(ii) payment of the Equipment Purchase Price and the Installation Price to us,

we will transfer title and ownership of the Telstra Supplied Equipment to you free from any mortgage, charge, lien, pledge or other encumbrance; and

(c) you accept that all responsibility and risk in the Telstra Supplied Equipment passes from us to you on Delivery.

4.3 You agree that:

(a) we reserve the right to repossess the Telstra Supplied Equipment or suspend any Installation and TBS Professional Services you are also receiving from us (and reconnection fees may apply) if you do not pay the Equipment Purchase Price or the

Installation Price in full in accordance with your agreement with us for your solution under TBS; and

(b) you grant us an irrevocable licence for our employees, agents or contractors to enter the Sites or other premises where the Telstra Supplied Equipment is located with reasonable notice (and you must obtain permission for us to enter such premises) in order to repossess that Telstra Supplied Equipment pursuant to clause 4.3(a).

4.4 It is your obligation to ensure the adequacy of the security of the Telstra Supplied Equipment on your premises including preventing fraudulent intrusions into and/or unauthorized use of the Telstra Supplied Equipment and to take all reasonable steps to prevent unauthorised disclosure of any passwords.

4.5 You acknowledge that if we require you to pay part of the Equipment Purchase Price and Installation Price prior to the Start Date you have paid that amount. If so, you will only be required to pay us the remainder of the Equipment Purchase Price and the Installation Price.

4.6 Unless specified otherwise, if the terms set out in this section of Our Customer Terms allow us to impose extra charges for services we will only perform such services after obtaining your agreement to pay the extra charges. You must pay any extra charges properly incurred.

4.7 If you cancel an order for Telstra Supplied Equipment after we have ordered it for you but before Delivery (unless you are terminating your agreement with us for your TBS Products and Services for our material breach), in addition to any other rights we may have, we may, at our sole discretion, require you to pay for the Telstra Supplied Equipment that has been ordered for you or the reasonable expenses we have incurred up to the date that you cancel your order. If we require you to pay for the Telstra Supplied Equipment that has been ordered, you will be entitled to keep the Telstra Supplied Equipment that you have paid for.

Lease or Rent of Telstra Supplied Equipment and Services

4.8 We acknowledge that you may enter into financing or leasing arrangements with respect to the Equipment Purchase Price and Installation Price.

4.9 In connection with any financing or leasing arrangements made by you, you can procure the financier to pay us the Equipment Purchase Price and Installation Price for Telstra Supplied Equipment you acquire from us and we agree to accept such payment from your financier. If the financier fails to pay us, you agree to pay any amount not paid.

TBS Repayment Option

4.10 Under the TBS repayment option ('**TBSRO**'), you must pay us for the Telstra Supplied Equipment by monthly instalments as set out in your Application Form on the terms and conditions in this section of Our Customer Terms.

4.11 To be eligible for the TBSRO:

(a) your application must be approved by us; and

(b) if we have requested it, you must enter into a managed services agreement with us for the relevant site.

4.12 You must make a separate application to us if you wish to apply the TBSRO to further equipment or services. The eligibility criteria in clause 4.11 will apply. If we approve an application for further equipment or services, a new TBSRO Charge will apply.

4.13 Title to the equipment supplied to you under the TBSRO will pass to you when you have paid the whole of the TBSRO Charge but not before.

4.14 You acknowledge and agree that, if you apply for the TBSRO, we or our agents will perform investigations of your credit worthiness.

4.15 You understand and acknowledge that the total TBSRO Charge for eligible equipment and services will be greater than if you paid for the same equipment and services upfront.

4.16 You must seek independent advice concerning:

(a) the matters in clause 4.15; and

(b) which payment option for the Telstra Supplied Equipment (sale, lease, rent or TBSRO) is best for you, and you acknowledge that you have not relied on any opinion or advice that we or our dealers may have given you concerning payment options.

4.17 The terms and conditions of the TBSRO apply in addition to those of any other agreement that you have entered into with us.

4.18 If this agreement is terminated for any reason or you do not pay any monthly instalment of the TBSRO Charge in accordance with your agreement with us, you must pay us the TBSRO Early Termination Charge within 30 days of our invoice.

Installation and TBS Professional Services

4.19 We will provide you Installation and TBS Professional Services (if any) as detailed in your Application Form on the terms and conditions in this section of Our Customer Terms. A description of the TBS Professional Services that we will provide (if any) is set out in clauses 4.20 - 4.38 below.

Delivery

4.20 You acknowledge that the supply of the Telstra Supplied Equipment is subject to availability from the Supplier.

4.21 We will use all reasonable endeavours to deliver the Telstra Supplied Equipment to you within a reasonable timeframe and inform you of any delays in the delivery and Installation of the Telstra Supplied Equipment.

4.22 You may request special delivery or Installation of the Telstra Supplied Equipment and we will use our reasonable endeavours to comply with any such requests which may incur extra costs that we will advise you of.

4.23 You must ensure the working environment is safe for us.

Preparation for Installation

4.24 Prior to the Installation of any Equipment, you must provide or ensure that your employees,

contractors, or agents provide (where relevant): i) information necessary for us to configure the Equipment; and ii) a clean, dry operating environment for the Equipment within 3 metres of 240VAC General Purpose Outlet.

4.25 You are responsible for preparing the Site for Installation of the Equipment. If you have not done that work by the time we come to install the Equipment (on a date that is agreed with you), you agree that you will be charged a visit fee and Installation will be re scheduled.

4.26 You are responsible for getting any council or other approval needed for that work or the Installation work.

4.27 We may cancel our agreement with you for Installation and TBS Professional Services by written notice to you if you have not enabled Installation of the Equipment to take place within 60 days of the Start Date. In that event, you will pay us damages for our reasonable storage, handling, re scheduling and other administration costs as determined by us.

Timing of performance

4.28 We will endeavour to perform the Installation and TBS Professional Services within a reasonable timeframe.

4.29 We only have to perform the Installation and TBS Professional Services during Business Hours. If you want us to perform the Installation and TBS Professional Services at another time, there will be extra charges that we will advise you of.

4.30 You acknowledge that the performance of the Installation and TBS Professional Services is subject to provisioning of your carriage telecommunications services. If such provision is delayed, the performance of the Installation and Professional Services may also be delayed.

Installation of the Equipment

4.31 Standard Installation covers (where relevant): i) the installation and mounting of the Core Equipment at the Site and connection of the Core Equipment to a General Purpose Outlet; ii) any installation involving Internet Protocol (‘**IP**’) Telephone Handsets or IP Trunks; iii) the programming, acceptance testing and commissioning of the Core Equipment; iii) patching of Equipment to the existing cabling infrastructure; iv) connection of Equipment handsets to existing cabling; v) installation of Equipment rack; vi) DECT base stations; and (vii) connecting telecommunications services within the same room as the Core Equipment.

4.32 **Non-Standard Installation** of the Equipment includes but is not limited to: i) any additional cabling (including cable terminations) of the Equipment; ii) any variation to the standard configuration; iii) installation involving a heritage Site; and iv) any installation of Equipment not set out in 4.31 above.

4.33 If the installation of your Equipment is a Non-Standard Installation we reserve the right to charge additional fees to the Installation Price. Such additional charges will be the standard charges for such services at that time as advised to you at the time by us. We will tell you what these charges are before providing the Installation to you. If you do not agree with the additional charges for the Non-Standard Installation, we will not perform (and we are not otherwise required or obligated to perform) the Installation.

4.34 Subject to the Australian Consumer Law provisions in the General Terms of Our Customer

Terms, we are not responsible for any problem during an Installation unless we caused the problem or the problem is in the Telstra Supplied Equipment. If a problem occurs which we did not cause, and we have to fix it, there may be extra charges which we will advise you of. If you do not agree with the additional charges to fix the problem that we did not cause, we will not perform (and we are not otherwise required or obligated to perform) the Installation.

4.35 It may be necessary to change the Equipment because of a problem which we did not cause. In that case, the Installation Price may also change which we will advise you of. If you do not agree with the additional charges due to the change in Equipment, we will not perform (and we are not otherwise required or obligated to perform) the Installation.

TBS Professional Services

4.36 The TBS Professional Services we will provide to you are detailed in your Application Form. We may, from time to time, agree to add or remove a TBS Professional Service from the available TBS Professional Services (but this will not affect any TBS Professional Services that we have already agreed to provide to you).

4.37 Prior to the performance of the TBS Professional Services, you must provide or ensure that your employees, contractors, or agents provide (where relevant) information necessary for us to perform the TBS Professional Services. You must also provide us, our employees, agents or contractors with access to the Site (or any other place) to provide the TBS Professional Services.

4.38 For the purposes of the performance of the TBS Professional Services, you acknowledge that we own all Intellectual Property Rights in respect of any Developed Material and you assign to us all Intellectual Property Rights you may have in the Developed Material.

Limitation of Liability

4.39 Subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms:

(a) we are not responsible for any loss or damage to software, firmware, information or memory data of yours contained in, stored on, transmitted to or integrated with the Equipment while it is the subject of the Installation and TBS Professional Services, except to the extent caused by our (or our contractors') negligence; and

(b) we are not responsible for any other problem during performance of the Installation and TBS Professional Services unless we caused the problem.

Completion

4.40 At the completion of the Installation and TBS Professional Services you must sign a Customer Acceptance Certificate which will constitute your acceptance of the Installation and TBS Professional Services.

Our warranties

4.41 If you are a consumer as defined in the Australian Consumer Law, our goods and services come with guarantees that cannot be excluded under the Australian Consumer Law. For major failures with the service, you are entitled: (a) to cancel your service contract with us:

and (b) to a refund for the unused portion, or to compensation for its reduced value. You are also entitled to a replacement or refund for major failures with goods. If a failure with the goods or a service does not amount to a major failure, you are entitled to have the failure rectified in a reasonable time. If this is not done you are entitled to a refund for the goods and to cancel the contract for the service and obtain a refund of any unused portion. You are also entitled to be compensated for any other reasonably foreseeable loss or damage from a failure in the goods or service.

4.42 Other than clause 4.41 the benefits under clauses 4.43 - 4.48 are in addition to the rights and remedies you may have under the Australian Consumer Law or other laws.

4.43 We warrant that the Telstra Supplied Equipment will perform in accordance with the Supplier's Specifications for 12 months from the date that you sign a Customer Acceptance Certificate as contemplated in clause 4.40. This warranty will not apply if the Telstra Supplied Equipment has:

(a) been altered, repaired or maintained by a person other than us;

(b) not been operated in a suitable environment in accordance with its specifications; or

(c) been subjected to abnormal physical or electrical stress, misuse, negligence, or accident.

4.44 If any Telstra Supplied Equipment does not perform in accordance with clause 4.41 we will within 10 Business Days of identification of the fault repair or replace (at our option) the Telstra Supplied Equipment.

4.45 We will pay the cost of any parts needed to repair or replace the Telstra Supplied Equipment but, unless you have a Telstra Business Systems Care plan (as described in the Managed Voice Service – Part C – Telstra Business Systems Care section of Our Customer Terms), you will be responsible for additional costs such as labour and travel time calculated by reference to our standard MAC rates at that time as advised to you, or the cost of returning the Telstra Supplied Equipment to us. If you have a Maintenance Contract, those costs will be charged in accordance with the Maintenance Contract.

4.46 Telstra Supplied Equipment presented for repair may be replaced by refurbished goods of the same type rather than being repaired. Refurbished parts may be used to repair the Telstra Supplied Equipment.

4.47 If Telstra Supplied Equipment you send to us for repair is capable of retaining user-generated data (e.g. telephone numbers stored on a phone), some or all of your stored data may be lost during the process of repair. Please ensure that you have saved this data elsewhere prior to sending to us for repair.

4.48 To make a claim under this warranty, please contact us at 1800 181 329.

4.49 Subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, clauses 4.44 and 4.45 are your sole remedies for a breach of clause 4.43.

4.50 Other than the warranty in clause 4.43 and subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we make no additional warranties or representations in relation to the Telstra Supplied Equipment including warranties or

representations as to performance, fitness for purpose and the ability of the Telstra Supplied Equipment to operate with other items of equipment.

Your Warranty and Use of Equipment

4.51 You represent and warrant to us that you have full power to own property and have the power to enter into and perform your agreement with us for the TBS Products and Services and have obtained all necessary consents to enable you to do so.

4.52 You are solely responsible for any use of the Equipment on your premises, or any Installation and TBS Professional Services connected to the Equipment, by you or any third party, whether authorised or not.

MACS and Non-contracted Maintenance Services

4.53 If you request us to provide you with: a) a MAC or maintenance services or any additional services and you do not have Maintenance Contract with us; or b) where you do have a Maintenance Contract with us, a MAC or maintenance services or any additional services not covered by the Maintenance Contract, we will provide you with the MAC or maintenance services at our standard rates (for parts and labour) for such maintenance services or MAC at that time as advised by us. You must pay us for all charges properly incurred for the maintenance services or MAC performed by us in accordance with this clause 4.53.

4.54 You must provide us our employees, agents or contractors with:

(a) access to the Site (or any other place) to provide the maintenance services or MAC; and

(b) all assistance which is reasonably required to provide the maintenance services or MAC.

4.55 Subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we are not responsible for any loss or damage to software, firmware, information or memory data of yours contained in, stored on, transmitted to or integrated with the Equipment while it is the subject of a MAC, except to the extent the event giving rise to the loss or damage is caused or contributed to by our (or our contractors') negligence.

4.56 At the completion of the maintenance services or MAC you must sign a Customer Acceptance Certificate which will constitute your acceptance of the maintenance services or MAC.

5 NETWORK DEVICE INSTALLATION

Service Summary

5.1 Telstra's Network Device Installation service is ideal for customers needing assistance in setting up Network Devices. A Network Device is a physical piece of hardware enabling communication between different pieces of hardware within a computer network. An example of a Network Device is a router that connects a laptop to the internet as well as to a printer in the office.

5.2 Customers get access to an expert local Telstra technician to set up and install Network Device(s) enabling businesses to connect with their customers and provide connectivity to

their employees in the office or at home. This can be done on site or remotely. This service is for the **installation and configuration** of standard network devices, and does not include the supply, delivery, or post-provision support of devices.

What is included?

5.3 The service includes planning for the right hardware to use and its placement, physical setup, and configuration of the device such as security settings and testing. This installation service covers hardware purchased through Telstra. We may install your own device subject to a **Hardware Readiness Assessment** which is included in the service.

5.4 The service can be used to switch from an old network device or network provider where alternatives are available. We minimise the service interruption during this type of change as well as providing post installation testing to help maintain a working service.

5.5 Network Device Installation is available in three different packages (Basic, Standard, and Advanced) which each have different service deliverables, as set out in the table below and further described in clauses 5.7 – 5.27 (‘**Service Deliverables**’).

Service Deliverables	Basic	Standard	Advanced
Hardware Readiness Assessment	●	●	●
Equipment Setup & Installation (Remote or Onsite*)	●	●	●
Commissioning – General	●	●	●
Commissioning – Configure Neighbouring Connections	●	●	●
Commissioning – User Access Profiles		●	●
Commissioning – VPN services		●	●
Commissioning – Backup Carriage		●	●
Commissioning – Multi-Zone, Advanced Routing, Advanced Switching, Geo-Zoning			●
Commissioning – Security; Malware and AV Protection			●
Commissioning – Security; Firewall Policy, Content Filtering			●

*** Call Out Fees may apply**

Service Deliverables

5.6 Customers have the choice of three (3) Engagement Plans, with different services allowing for increasing levels of complexity to meet customer's needs.

Service	Basic	Standard	Advanced
Engagement Plan	Basic: Install and Set Up of Your Device	Standard: Everything in Basic plus Network Management Configuration	Advanced: Everything in Standard plus Network Security Configuration
Cost Incl GST	$660	$1,870	$2,640

 # See appendix for a detailed comparison on various service packages

All Engagement Plans include the following Service Deliverables:

Basic: Install and Set Up of Your Device

5.7 **Hardware Readiness Assessment**

(a) Audit of the Network Device including the vendors make, model, firmware version and maintenance agreement.

(b) Hardware must be supported by the vendor and not be at the end-of-life (EOL).

(c) Required for non-Telstra procured devices.

(d) Not required if Network Device has been procured and installed by the customer's Telstra Dealer using this package.

(e) Additional checks can include:

(i) Remote access management interface accessibility;

(ii) Recording details of equipment;

(iii) Recommendation for the replacement for EOL or unsupported BYOD;

(iv) Power suitability assessment;

(v) Cabling assessment to ensure suitability for network device installation. If not, quotation for suitable cabling to be provided, as an additional cost to the Network and Device Installation; and

(vi) Completing checklist assessment PS-030 – Pre-Service Checklist

5.8 **Equipment Setup and Installation**

(a) Subject to the below, all packages include on-site attendance for metro locations at a

scheduled time (within business hours) and includes unpacking, rack mounting, standard cabling to hardware, power on test, verify port-interface status and basic configuration of the named devices.

(b) See **Customer Responsibilities Equipment Setup and Installation** section for installation at locations with difficult access.

(c) See **What is not included** section for installation outside Metro areas.

5.9 **Commissioning – General**

(a) This provides checks to ensure the hardware installed meets your functional requirements, such as testing of IP connectivity, administration login, and end user connectivity.

5.10 **Commissioning – Configure Neighbouring Connections on the device**

(a) We will perform configuration required to connect existing neighbouring nodes such as connecting printers, Wi-Fi devices and smart devices to link to the network device. Where an existing network is being utilised, existing IP address configuration will be used to reduce change impact wherever practical.

(b) **Basic**: includes configuration of the new network device and successful testing of connectivity up to 3 different device types on the customer network (e.g. Firewall, PC, Printer).

(c) **Standard**: includes configuration of up to 5 existing devices (nodes).

(d) **Advanced**: includes configuration of up to existing 10 devices (nodes).

(e) The **Standard and Advanced** packages include connecting devices via trunking, switch port VLAN tagging, router connecting to a firewall and setup of DMZ (Demilitarized Zone) segments.

Standard: User Access Controls and Network Management

In addition to the Basic Plan Services Deliverables, the Standard Plan includes Network Controls and Management, which refers to making sure all your Wi-Fi connected devices e.g. printers are connected to the Network Device being installed.

5.11 **Commissioning – User Access Profiles**

(a) This adds another level of security to the customer network to determine which users and devices have authorized permissions to connect to the installed device. Access is either accepted or rejected based on a set of parameters and policies that are configured on the network device to be installed. The additional advanced configuration parameters for a policy-based access control may include:

(i) User access control, authentication to a third party (Active Directory / Radius / TACACS integration) to a primary and standby host, if applicable;

(ii) Determine who has access to what areas of the network;

(iii) Location access control;

(iv) Remote access profiles;

(v) Configure the allowed connected device limits per user; and

(vi) How third-party partners that interact with each other.

User Access Profiles for standard and advance packages allow up to **five** group access profiles.

5.12 **Commissioning – VPN (Virtual Private Network) Services**

(a) This Service Deliverable comprises defining, establishing and testing a new VPN on network hardware (router or security appliance):

(i) Multisite LAN - LAN VPN – Setup and integration into a private network (see clauses 5.17 – 5.27 below for **what is not included**);

(ii) Client VPN access point - Service includes setting up a VPN access point for client VPN access.

(b) Setup and testing of VPN client software not in scope. The Service Delivery Partner will provide the connection details that can be used to set up a VPN client later. If further assistance is required with VPN clients, customers can request Prepaid Support.

5.13 **Commissioning – Failover Carriage**

(a) This Service Deliverable includes configuration for internet or private WAN failover as well as the configuration and testing of carriage backup via external port/interface for failover if available. Testing for automated failover and failback to your primary carriage is included. The Advanced package includes failover between devices.

Advanced: Network Security Configuration

In addition to the Standard Plan Service Deliverables, the Advanced Plan includes network security configuration.

5.14 **Commissioning – Multi-Zone, Advanced Routing, Advanced Switching, Geo-Zoning**

(a) This Service Deliverable offers complex network configuration for multi-site, and customer unique security configuration on the single device. It includes:

(i) VLAN trunk/port configuration on the included device(s);

(ii) Additional zones configured with inter-zone security;

(iii) Split tunneling;

(iv) Advance switch port configuration. e.g. security, minimise port span, restrict no max addresses;

(v) Failover between devices for greater network redundancy. E.g. dual routers and switch stacks; and

(vi) A maximum of five VLANs, Groups, Zones and DMZ.

5.15 **Commissioning – Security: Malware and AV Protection**

(a) This Service Deliverable includes additional security configuration beyond basic stateful firewall protection configuration and includes:

(i) Applying scanning to nominated interfaces;

(ii) Installing security license add-ons,

(iii) Applying AV/malware configuration signature updates applied as requested - Auto or manual.

5.16 **Commissioning – Security, Firewall Policy, Content Filtering**

(a) This Service Deliverable provides additional security configuration beyond basic stateful firewall protection and out of box settings. (e.g. Vendor whitelist filters) and includes:

(i) Configuration of up to 20 custom firewall policies;

(ii) Configuration of up to 20 Internet content filtering policies; and

(iii) Defining up to 100 objects (objects that are referenced within a policy).

(b) If additional configurations are required, we recommend customers use Pre-Paid Support.

What is not included?

5.17 Complex configurations such as QoS (Quality of Service), ToS, CoS, traffic shaping, complex routing are not included. Our service delivery partner will identify any out-of-scope requests. You may request, and we may agree to provide, bespoke installations on separate terms and pricing.

5.18 Call Out Fees may apply:

- for travel to a customer site if more than 1 visit to the installation site is required, and
- where the installation site is located outside a metro area.

Additional information about these fees is specified in the Critical Information Summary and the call out fees page on our website (**telstra.com.au/small-business/online-support/business-software/call-out-fee**). The applicable fee may vary depending on the distance from the Business Technology Centre to the customer premises.

5.19 Onsite installation may not be possible for sites with difficult access, in which case installation will be performed remotely.

5.20 The approved list of network devices includes all current Telstra approved network devices. If a device is not on this list, then our service delivery partner must be provided with the details of the intended hardware prior to proceeding, to confirm that they have the capability to successfully install the device.

5.21 Dead-on-Arrival (DOA) parts and Return to Manufacturer (RMA) parts must be managed by you unless our service delivery partner supplies the device for this installation. BYOD DOA must be managed by the customer.

5.22 Supply and delivery of network devices is not included within this service.

5.23 Unforeseen cabling issues not in scope will be POA.

5.24 Authentication of devices to a third-party server (such as Active Directory / Radius / TACACS integration) is not in scope for the Basic package. The Basic package includes statically defined local user authentication.

5.25 Commissioning of network segments/VLANs is limited to 3 for the Basic package, up to 5 for the Standard package and up to 10 for the Advanced package.

5.26 IPSec tunnels between different makes of network devices is not recommended. Configuring the remote VPN endpoint is considered an additional service (POA).

5.27 Configuration of failover between devices, e.g. dual routers and switches (High Availability) is included in the Advanced package only if the hardware supports it.

Telstra Responsibilities

5.28 The following are Telstra's responsibilities in the delivery of the Network Device Installation service offering. We must:

(a) Complete the deliverables as detailed in this clause 5; and

(b) Collaborate with you to schedule dates and times for the installation of hardware.

Customer Responsibilities

5.29 You must:

(a) Please reference the Standard Terms for Small Business Professional Services Fixed Packages.

(b) Complete Service Checklist: A pre-service checklist will need to be signed off by the customer before the installation (to confirm requirements)

(c) Provide accurate high-level detail on your internal IT environment and objectives during pre-sale including:

(i) Customer data is available and profile role groups are defined;

(ii) Connection details to connect to an ISP;

(iii) Common infrastructure details that are required to install network hardware,

DHCP, neighbouring nodes etc.; and

(iv) Site photos, confirmation of staging area to setup area, correct cabling and shelving are available etc.

(d) Ensure that the network device that needs to be installed is available at the installation location and can be powered up and plugged into an active network port;

(e) Ensure backup/failover carriage is ready for service; and

(f) For installation in areas that are challenging to attend on-site (e.g. due to a natural disaster, customer visitor policy, occupational health & safety, etc.), the customer is required to have a resource available to provide remote support and an active internet service to assist in the installation of the network device(s). The Service Delivery Partner will provide remote assistance for the customer to install and connect the device to its network.

Illustrative Example of Supported Devices installed and associated Services.

5.30 The table below lists which features are included per package as well as the class of devices installed per package tier. This is illustrative only and any requirements can be discussed with your technician.

Note – this service is for the installation and configuration of standard network devices of the types described above, and do not include the supply, delivery or post-provision support any devices.

Size	Very small to small branch office use	Small branch office use	Enterprise level branch offices
Customer Sizing (Employees)	1-5	1-19	20-49. >49 POA
Carriage	NBN - TBB, 4G/5G, Fiber Connect 50/20	NBN – TBB, Telstra Internet Direct (TID), 4G / 5G, Fiber Connect 100/40	TID – BIP – CIP, 4G/5G, Fiber Connect 250/100, 500/200, 1000/400
Access Points	Cisco Meraki MR (MR28, MR36, MR78, MR86, etc) Basic Setup, SSID, standalone, WPA2,	Cisco Meraki MR (MR28, MR36, MR78, MR86, etc) SSID, mesh, WPA2, Bridge, VLAN, Mac filtering	Cisco Meraki MR (MR28, MR36, MR78, MR86, etc) SSID, mesh, WPA2, Bridge, VLAN, NAT, Geo-Zoning, Heatmaps, security filtering, Point-to-Point

Switches	Cisco Meraki MS (MS120, MS130, etc) Basic Setup Hub (unmanaged)	Cisco Meraki MS (MS120, MS130, etc) VLAN, Trunks, SNMP, Smart Switches	Cisco Meraki MS (MS120, MS130, etc) L2/L3 Managed, VLAN, Trunks, Advanced Switching & Switch Port Security, Add Expansion module
Routers	Cisco Meraki MX (MXZ4, MX68, MX64W, MX67, MX68, etc) Basic Setup. Single Internet Gateway, DHCP, Default route	Cisco Meraki MX (MXZ4, MX68, MX64W, MX67, MX68, etc) SNMP, VPN, Carriage Failover, Basic Routing, Port Redirection	Cisco Meraki MX (MXZ4, MX68, MX64W, MX67, MX68, etc) VPN, Advanced Routing, ACL Policy, QoS, Carriage Failover, Add Expansion module
Firewalls	N/A	N/A	FW Polices, Content Filtering, Software blades (add-on functions)
Location	Onsite/ Remote	Onsite/ Remote	Onsite/ Remote
Vendors	Cisco Meraki (MX, MS, MR)	Cisco Meraki (MX, MS, MR)	Cisco Meraki (MX, MS, MR)

More complex scenarios

5.31 Where a mixed package install with different levels of complexity is required, multiple orders can be placed with our service delivery partner to meet your requirements. For example, two basic switches and a small branch router could be serviced by Basic x 2 + Standard x 1 at the same installation engagement.

Invoicing

5.32 Services will be invoiced upon completion of the agreed deliverables and customer acceptance of the engagement.

Service Pricing

5.33 The charges for your Network Device Installation service (and where relevant, limitations on service inclusions) are set out in your Application Form and the Network Device Installation Critical Information Summary, a copy of which will be provided to you by your Telstra Dealer.

Special meanings

5.34 In this clause 5, the following words have the following special meanings:

TELSTRA BUSINESS SYSTEMS PRODUCTS AND SERVICES SECTION

BYOD has the meaning given to it in clause 5.7(a).

EOL has the meaning given to it in clause 5.7(a).

LAN has the meaning given to it in clause **Error! Reference source not found.**.

Service Deliverables has the meaning given to it in clause **Error! Reference source not found.**.

WAN has the meaning given to it in clause **Error! Reference source not found.**.

Appendix

Service Deliverable	Service Description	Basic	Standard	Advanced
Pre-Service Assessment	Over the phone or in store environment & device assessment	✓	✓	✓
Network Devices installed	Included number of network devices (routers, switchers, etc) installed	1	1	1
Readiness Assessment	Check hardware, device, and network are ready for this service	✓	✓	✓
Onsite installation	Equipment Setup and Onsite Installation during business hours to metro installation locations	✓	✓	✓
Configure upstream	Configuring upstream (neighbouring) devices for connection	✓	✓	✓
Commissioning	General (Configured for environment)	✓	✓	✓
	Authentication of devices to a third party		✓	✓
	Authentication to other networks or VLANs	3	Up to 5	Up to 10
	User Access Profiles		✓	✓
	VPN services (Telstra to Telstra)		✓	✓
	Backup Carriage: Failover between devices (e.g. dual routers & switches - High availability)			✓

	Multi-Zone, Advanced Routing, Advanced Switching, Geo-Zoning			✓
Security	Malware and AV Protection			✓
	Firewall Policy, Content Filtering			✓
Onsite visits	Included visits to a Metro site subject to suitable access	1 Metro onsite visit included		
Included Service Hours	Included hours of professional IT service work	1	2	3
Follow up service call	A 30 minute follow up call and check in to assess service performance	✓	✓	✓
Service minimum cost (per Network Device incl. GST)	**Pay upfront**	**$660**	**$1,870**	**$2,640**

For more complex business needs or more than five network devices, contact us for detailed pricing.

6 CYBER SECURITY AUDIT

Service Summary

6.1 The Cyber Security Audit is a strategic engagement with actionable deliverables for you to help you understand the existing integrity, confidentiality and availability of your business data.

6.2 The Cyber Security Audit leverages a methodology which is designed to examine your existing network as well as ICT hardware, software and connected devices to help mitigate cyber security incidents caused by various cyber threats.

6.3 The elements listed in the Service Description Deliverables Table in clause 6.7 are based on the Australian Cyber Security Centre (ACSC) "Essential Eight" mitigation strategies which help inform a roadmap for what and when elements need to be addressed.

6.4 As part of the Cyber Security Audit service we will provide a report which will deliver high-level findings to help identify compliance gaps and provide recommendations for improvement ('**Cyber Security Audit Report**'). It is designed for you to understand the strengths and weaknesses of your current cybersecurity posture.

Customer profile

6.5 The Cyber Security Audit service offering is ideal for customers who require a high-level report on their existing cyber-security setup and vulnerabilities.

6.6 The Cyber Security Audit may also provide recommendations and insights into your current cyber security posture and identify potential cyber security gaps for your with regulatory compliance requirements, particularly those that must secure personal client or customer information to comply with mandatory data breach notification laws or for customers looking to protect valuable business data by avoiding data breaches.

Service Description Deliverables Table

6.7 The Cyber Security Audit is available in three different packages (Basic, Essential and Advanced) which vary in their depth of analysis and level of customer facing time. The service deliverables in each package are set out in the table below ('**Service Deliverables**').

Deliverable	Basic	Essential	Advanced
Password Management Assessment	●	●	●
User Applications Settings Assessment	●	●	●
Trusted Application Review	●	●	●
Email Security Evaluation	●	●	●
Patching Assessment - Workstation	●	●	●
Data Protection - Malware & Virus	●	●	●
Report - PowerPoint Presentation	●		
Report - Comprehensive Full Assessment		●	●
Data Backups Check		●	●
User Access Management Assessment		●	●
Patching Assessment – Server and Network		●	●
Mobile and Smart Devices (BYOD) Review			●
Cloud Storage Review			●
Data Protection Assessment – Network & Data			●
Vulnerability Assessment – External & Internal			●
Onsite Assessment	POA	POA	POA

Service Deliverables

6.8 A description of each Service Deliverable is set out in clauses 6.9 - 6.23.

6.9 **Password Management Assessment:** A vital method of securing digital information in keeping businesses safe. The deliverables in this assessment include auditing the following:

(a) Are staff (including contractors) trained in the importance of strong passwords or passphrases and how to choose them?

(b) Are users advised to lock their computers when they leave their desks, even for short periods?

(c) Is password or passphrase complexity enforced? For example, including uppercase characters, lowercase characters, punctuation, length, symbols, and/or numbers.

(d) Are passwords or passphrases stored securely, such as in an 'encrypted' format?

(e) Is the sharing and reuse of passwords or pass-phrases forbidden?

(f) Are rules to change passwords regularly enforced?

(g) How quickly are passwords changed and accounts removed or suspended once someone leaves the business?

(h) Do accounts lock the user out after a specified number of failed logins? Do computers or programs automatically lock if left inactive or unattended for periods of time? Are accounts that are unused or inactive for some time suspended?

(i) If Wi-Fi is used in the network, is a suitable security protocol in place - (at least WPA2) and has the Wi-Fi gateway admin password been changed?

6.10 **User Application Settings Assessment:** This deliverable audits how your common office applications are configured from a security perspective, and includes Microsoft Office, web browsers & PDF viewers. Checks are made to see if these applications are limited to the manufacturer's recommended security settings to reduce the risk of abnormal tasks from being executed (e.g. noting high-risk plugins such as Flash, Java and web-advertisement content). These limitations reduce the chances of attack as plug-ins can sidestep standard antivirus monitoring. This includes an assessment of whether:

(a) Web browsers:

(i) web browsers block or don't support Adobe Flash content;

(ii) web browser Adobe Flash settings can't be changed by users; and

(iii) web browsers block web advertisements and Java from the Internet;

(b) PDF viewers:

(i) only required services are enabled; and

(ii) PDF viewers are hardened in line with vendor hardening guides;

(c) Adobe Flash;

(i) Adobe Flash is uninstalled from operating systems (i.e. NPAPI, PPAPI and ActiveX files are removed); and

(ii) Adobe Flash hardened in line with vendor hardening guides; and

(d) Microsoft Office:

(i) Microsoft Office macros can execute, but only after prompting users for approval;

(ii) users can change Microsoft Office macro settings; and

(iii) Microsoft Office is hardened in line with vendor hardening guides.

6.11 **Trusted Application Review:** Verifying only required applications are present and active on your computer system and or network. The goal of software control, application whitelisting, is to protect computers and networks from potentially harmful applications. The deliverables in this assessment include auditing the following:

(a) whether you have identified applications that are authorised to execute on a system;

(b) whether you have developed application whitelisting rules to ensure only authorised applications can execute;

(c) whether application whitelisting is implemented;

(d) whether you are using an approved whitelisting method covering executables, software libraries, scripts and installers;

(e) whether whitelisting is implemented on critical servers; and

(f) how often is testing of whitelisted application conducted.

6.12 **Email Security Evaluation:** Email is not a secure form of communication, and you should have policy or procedures in place to manage the transmission of business sensitive information via email. The deliverables in this assessment include auditing whether:

(a) systems are in place to protect your email from malware, spam and spoofing, including blocking spoofed email;

(b) you have a system or user policy in place that polices certain types of information being sent via unsecured email (for example sensitive data);

(c) email system logs are available for Administrator review; and

(d) SPF and or DMARC records for email verification have been implemented to prevent email spoofing.

6.13 **Patching Assessment - Workstation:** Many applications are regularly updated to address security vulnerabilities as they become apparent. These vulnerabilities can be a security hole or weakness found in a software program or operating system. Hackers can take advantage of the security hole by writing code (malware) to target the vulnerability. Regularly updating (or 'patching') the software will remove a critical means by which cyber-security attacks are carried out. The deliverables in this assessment review workstation and application patching including:

(a) application patching;

(b) how regularly patches are applied for extreme risk security vulnerabilities in Adobe Flash, web browsers, Microsoft Office, Java and PDF viewers for any of your

workstations;

(c) whether non-vendor-supported versions of Adobe Flash, web browsers, Microsoft Office, Java and PDF viewers used on any of your workstations;

(d) operating system patching:

(i) Identification of all operating system versions in use per workstation;

(ii) whether you are using only the latest vendor-supported operating system versions; and

(iii) how regularly patches for security vulnerabilities in operating systems are applied.

6.14 **Data Protection - Malware & Virus:** This deliverable inspects the current setup of software security controls (endpoint detection) and provide comparison commentary against current best practices. This service deliverable will include the following, for both key desktop and smart devices:

(a) whether you have antivirus installed with up-to-date definitions;

(b) whether installed antivirus is active on workstations and server(s);

(c) whether you are using only the latest vendor-supported antivirus application; and

(d) whether you are monitoring and controlling the use of removable media (e.g. hard drives and USBs).

6.15 **Report – PowerPoint Presentation:** A high-level presentation to you covering the following:

(a) business purpose;

(b) scope and methodology;

(c) what was discovered: a summary of key findings with respective business risks and your expectations;

(d) a maximum of 5 key findings in the form of a traffic light report; and

(e) recommendations.

6.16 **Report – Comprehensive Full Assessment:** A detailed full report covering topics listed in the Report - PowerPoint Presentation, in addition to:

(a) an executive summary;

(b) a traffic light report;

(c) an extensive Cyber Security Audit report; and

(d) ICT supported documentation per Service Deliverable.

6.17 **Data Backups Check:** Security vulnerabilities can be used to corrupt computer hardware and the integrity of business data. Off-line and reliable backups that cannot be accessed by malware is a crucial corrective control that prevents malware from maliciously tampering with backed-up data. The deliverables in this assessment include auditing the following:

(a) whether you have a backup schedule in place for known business data, that is set to run at a business appropriate frequency;

(b) whether you have a backup schedule in place to store important new/changed data, software and configuration settings;

(c) whether your backups are stored for a minimum of three months or as appropriate for your business needs;

(d) whether your backups are stored offline, stored remotely to protect from natural disasters. The physical devices used to store your backup files to be kept in a secure location; and

(e) whether you test full data recovery at least once every 6 months and regularly tests to see if partial data is recoverable.

6.18 **User Access Management Assessment:** User administrator privileges should only be provided on an as-needs basis, as otherwise, third party exploits may use these administrator credentials to corrupt data or install malicious code. This deliverable will provide high-level analysis and risk assessment of current users' administrator privileges and the use of multi-factor authentication to systems. This assessment includes auditing whether:

(a) restrict administrative privileges:

(i) you have identified tasks which require administrative privileges and validated which staff members are required and authorised to perform those tasks as part of their duties;

(ii) you have systems to define and administer role-based access for data access;

(iii) role based accessed accounts are validated initially and on a monthly or more frequent basis or before they are required for a task and revoked immediately afterwards.

(b) multi-factor Authentication:

(i) you use multi-factor authentication for users using remote access (e.g. VPNs, remote desktops, corporate webmail);

(ii) you use multi-factor authentication for users performing privileged actions;

(iii) you use passphrases, security keys, physical OTP tokens, biometrics, smartcards, mobile apps, SMS messages, email and/or voice calls for authentication.

6.19 **Patching Assessment - Server and Network:** The deliverables in this assessment cover review of server and network patching. Network nodes include security appliance, routers,

switches and Wi-Fi access points. This assessment includes auditing:

(a) application patching:

(i) whether patches for high-risk security vulnerabilities in web server software, server applications that store essential business data, and other internet-accessible server applications are not applied or are applied on a greater than a monthly basis for any server; and

(ii) how often non-vendor-supported versions of web server software, server applications that store important data or other internet-accessible server applications are used.

(b) operating system patching:

(i) the identity of non-vendor-supported operating system versions used;

(ii) how regularly patches for security vulnerabilities in operating systems for all network devices and server are applied and verified; and

(iii) if you are using only the latest vendor-supported operating system versions.

6.20 **Mobile and Smart Devices (BYOD) Review:** The review is to document if you have control of smart devices connected to the business systems and if staff are permitted to use their own devices to access business data. This review includes auditing whether:

(a) your smart devices restrict application downloads;

(b) your smart devices have screen-lock enabled; and

(c) your smart devices are hardened e.g. developer options are disabled, devices are not rooted or jailbroken, or installation from unknown sources is disabled.

6.21 **Cloud Storage Review:** This deliverable provides a review of your cloud service provider regarding their availability, offering reliability, and security. This review includes auditing:

(a) whether you are using a reputable cloud storage provider that has been independently tested by security researchers;

(b) whether you retain legal ownership of your data and that your cloud vendor statement does not assume that you grant rights to do what they wish with their data and systems forever;

(c) if business data is accidentally deleted, the cloud vendor can quickly restore it;

(d) redundancy mechanisms and offsite backups prevent data corruption or loss; and

(e) whether you can quickly move data to another cloud vendor or on-premises.

6.22 **Data Protection Assessment - Network & Data:** This review will identify and analyse the existence or absence of security methods employed in protecting business data to minimise the risk of a cyber-attack. The deliverables include the following component level assessment:

(a) firewall: The audit will confirm the type of firewall(s) that are used whether they are appropriately configured. e.g. Is incoming and outgoing web traffic filtered?

(b) monitoring and event logging:

(i) Confirm what methods you use to monitor and identify unauthorised downloading, transferring or theft of business data, for example through the use of personal storage devices;

(ii) Confirm your methods of audit logging (or audit trail) enable actions to be linked to individuals, including both regular users and administrators. Do your audit logs or audit trail indicate when an individual has accessed, viewed, changed or destroyed business data, or unsuccessfully tried to obtain personal information?

(iii) What points of access (such as access to devices, files, networks, databases, and websites) do you audit?

(c) encryption:

(i) Identify where you have or have not employed encryption of any of the following:

(A) databases used to store confidential information;

(B) business data stored in third-party cloud servers;

(C) servers;

(D) backups;

(E) data in transit, for example, email or file shares (local or over the internet);

(F) end-user mobile devices, such as smartphones, tablets and laptops, including BYOD; and

(G) portable storage devices.

(ii) Confirm whether you have another unencrypted copy of your encrypted data.

(iii) Confirm whether you have enabled encrypted communications on your website (for example, for making payments)?

6.23 **Vulnerability Assessment – External & Internal:** Vulnerability Assessments provide a powerful tool to help proactively identify and assess potential cybersecurity risks by scanning vulnerabilities in data network and applications. The results will highlight any detected weaknesses to assist with prioritising remediation activities. This includes an assessment of whether your:

(a) external systems: provide external scans and reports with ranked threat results for specific, fixed public IP addresses; and

(b) internal systems: Provide a hardware-based or virtual scanning appliance inside the network, local area network, to scan one or more internal network segments.

What is not included?

6.24 Devices not connected to your network are excluded from the Cyber Security Audit.

6.25 Internet of Things (IoT) devices are excluded from the Cyber Security Audit.

6.26 This is not a compliance assessment or an asset audit.

6.27 Any changes to your current environment as at the date we conduct your Cyber Security Audit will be out of the scope of your Cyber Security Audit.

6.28 Any required changes to your network and systems due to our findings are out of scope of the Cyber Security Audit. You may request, and we may agree to implement those changes on separate terms and pricing.

6.29 The Cyber Security Audit does not include any legal advice on which standards or laws you need to comply with or the extent of your compliance with any such standards or laws.

Telstra Responsibilities

6.30 The following are Telstra's responsibilities in the delivery of the Cyber Security Audit service offering:

(a) we must complete all the Service Deliverables detailed under clauses 6.9 - 6.23, including producing and presenting relevant reports as specified per Cyber Security Audit package;

(b) we must collaborate with you to schedule the Cyber Security Audit and set the agenda for all workshops and presentations required; and

(c) we will work with our preferred service delivery partners to deliver the Cyber Security Audit to you.

Customer Responsibilities

6.31 You must:

(a) make sure the appropriate business owners and technical staff can attend or participate in our scheduled meetings and/or workshops as needed to perform the Cyber Security Audit;

(b) provide accurate high-level detail on your internal IT services and strategy to the Telstra IT consultant and our service delivery partner; and

(c) complete the 'PS-020 Cyber Security Audit Pre Work- Checklist' provided to you. You must complete and sign this pre-audit checklist before we conduct the Cyber Security Audit to confirm requirements.

6.32 Our services and Cyber Security Audit Report will be based on the information you provide to us and that we extract from your operating environment with remote tools. We will assume

all the information you provide is up to date and valid for your operating environment.

6.33 Our ability to complete the Cyber Security Audit depends on you providing the items and information outlined in clause 6.31 above. If you fail to comply with clause 6.31, such failure may result in extra charges or alteration to billing milestones for this service. We will let you know in advance in this occurs, and if you do not agree with the extra charges or alteration to billing milestones, we will not provide (and we are not otherwise required or obligated to provide) the service.

Service Pricing

6.34 Charges for your Cyber Security Audit (and where relevant, limitations on service inclusions) are set out in your Application Form and the Cyber Security Audit Critical Information Summary, a copy of which will be provided to you.

6.35 Additional charges will apply if we have to spend additional time on your Cyber Security Audit in order to comply with your specific requirements to complete an audit assessment (such as HSE inductions), provided that we tell you of those additional charges in advance. If you do not agree with those additional charges, we will not provide (and we are not otherwise required or obligated to provide) the service.

Location of Services

6.36 All packages are delivered remotely.

6.37 If on-site visits are requested, additional travel fees will apply. Fees for additional call outs are set out in the Cyber Security Audit Critical Information Summary, a copy of which will be provided to you, and your Application Form.

Special meanings

6.38 In this clause 6, the following words have the following special meanings:

Cyber Security Audit Report has the meaning given to it in clause 6.4.

Service Deliverables has the meaning given to it in clause 6.7.

7 CYBER SECURITY REMEDIATION

Service Summary

7.1 Cyber Security Remediation helps fix issues commonly uncovered following a Cyber Security Audit. Cyber Security Remediation is a pre-scoped professional service designed to implement, harden and configure your IT environment, per the recommendations previously documented under a "Basic", "Essential" or "Advanced" Cyber Security Audit.

7.2 Cyber Security Remediation provides a point in time mitigation of identified and agreed cybersecurity issues, by skilled IT personnel. The service does not include software licensing, hardware, ongoing management, processes and staff policies that may be recommended as part of a holistic managed security solution. These items would be procured separately.

7.3 The elements listed in the Service Description Deliverables Table in clause 7.6 are based on

the Australian Cyber Security Centre (ACSC) "Essential Eight" mitigation strategies and inform a priority of threat areas to focus on in a business' IT environment.

What is included?

7.4 Cyber Security Remediation is available in three packaged engagements (Basic, Essential and Essential+), which align to the assessment scopes from a previously performed Cyber Security Audit. Included in the engagements are the technical skills to implement and configure existing or newly procured security controls.

7.5 Please note that:

(a) the service inclusions are intended for environments operating predominantly on Microsoft systems. Where supported, equivalent remediation deliverables may be applied to Apple Mac workstations with known limitations documented.

(b) for customers operating in a Workgroup network (no central administration)

(i) the Basic and Essential packages are available for environments of up to ten (10) PC/workstations.

(ii) Customers with larger Workgroup networks are offered the Essential+ package, which additionally includes the setup and implementation of a new Microsoft Azure cloud based Active Directory server – with this in place, central administration and business wide policy deployment to your businesses PC/workstations is possible.

(c) for customers operating in a Domain network (central active directory), all service packages are available.

Service Description Deliverables Table

7.6 The inclusions in the Cyber Security Remediation service are set out in the table below and are further described in clauses 7.8 - 7.18 ('**Service Deliverables**').

Deliverable	Basic	Essential	Essential+
Antivirus & Malware Implementation	●	●	●
Patching Remediation – Workstations	●	●	●
Password Policy Implementation	●	●	●
User Applications Hardening	●	●	●
Trusted Application Control Implementation	●	●	●
Email Security Implementation	●	●	●
Post Implementation Document	●	●	●
Patching Remediation – Server & Network		●	●

User Access Management Implementation		●	●
Data Backups Optimisation		●	●
MS Azure Active Directory Service Implementation			●

Service Deliverables

7.7 A description of each Service Deliverable is set out in clauses 7.8 - 7.18.

7.8 **Antivirus & Malware Implementation:** This deliverable covers hardening against USB removable storage and the deployment, configuration and optimisation of licensed compatible antivirus and malware endpoint protection solutions, including those from Avast, McAfee, Malwarebytes, Bitdefender, ESET, Kaspersky, Symantec. If a 3rd party solution is not available, native controls (such as Security Essentials and Microsoft Defender) will be activated by default with known limitations documented. This deliverable includes:

(a) Antivirus and malware signature updates: where not yet configured, we will configure workstations and servers to automatically check for threat signature updates daily. Where supported by your selected solution, central distribution of the updates will be implemented so that updates are downloaded over your internet connection only once before being distributed locally by a server;

(b) Antivirus and malware notification of issues: where supported by your selected solution, email notifications of update failures and threat detection will be setup to your preferred destinations; and

(c) Removable storage risk prevention: where desired and compatible with your business processes, we will configure Domain Policy on your existing Windows network to block use of USB storage on workstations. This reduces the risk of commonly spread infection by way of USB storage sharing and company data loss via this means.

7.9 **Patching Remediation – Workstations:** This deliverable includes:

(a) Operating system patching: where automatic software updates have not completed, we will systematically troubleshoot impediments and attempt to bring workstation systems up to the latest security and system updates, as available at the date of remediation. Configuration of automatic update scheduling will be implemented where available, however future support is beyond the scope of and is not included in Cyber Security Remediation; and

(b) Application patching: where automatic software updates have not completed for MS Office (Office 2010 or newer), Java, PDF Viewers, licensed antivirus and malware applications, we will troubleshoot impediments and attempt to bring systems up to the latest updates as available at the date of remediation. Configuration of automatic software updates will be implemented where available, however future support is beyond the scope of and is not included in Cyber Security Remediation.

7.10 **Password Policy Implementation:** This includes:

(a) Configuring policy on your existing Windows network (where available central directory or individual workstations with limitations) to:

(i) automatically screen lockout workstations after 15 minutes of inactivity;

(ii) enforce user use of complex passwords (which includes a password length (no less than 8 characters), use of uppercase characters, lowercase characters and a number) in line with Microsoft guidance;

(iii) enforce regular change of user passwords, twice a year, or per other business preference;

(iv) prevent re-use of old passwords;

(v) automatically suspend accounts where there are 10 consecutive failed logins, or per other business preference; and

(vi) remove accounts of former employees as advised;

(b) Setting network device passwords: setting and documenting non-default administration passwords for identified network devise that have been left in the known factory default configuration, including firewalls, routers and Wi-Fi access points.

(c) Setting Wi-Fi keys and protocols: configuring wireless access points protocols and authentication keys to a secure setting available, per recommendation of the manufacturer.

7.11 **User Applications Hardening**: This deliverable covers the configuration hardening of common office applications, where they are in use in your network, by Attack Surface Reduction (less areas that can be attacked) by using Microsoft Defender. It also covers implementing configurations from application vendors' recommended security settings, for example reducing the risk of execution of malicious tasks and limiting macros (e.g. noting and restricting high-risk plugins such as ActiveX, Flash, Java and web-advertisement content). Before implementation, we will advise on changes made, to confirm any impact that they may have on your employees' normal use of the applications. This deliverable includes:

(a) Web browser(s) hardening:

(i) configuring blocking of Adobe Flash content, with administrator override only;

(ii) configuring blocking of Java, with administrator override only;

(iii) configuring blocking of ActiveX if not needed, with administrator override only; and

(iv) removing unwanted plugins/extensions.

(b) PDF viewer hardening:

(i) implementing vendor hardening guidelines for common PDF readers, such as Adobe Acrobat Reader, Nitro Reader and CutePDF.

(c) Adobe Flash hardening:

(i) if no known required use is confirmed, confirm required use before uninstalling from workstations (i.e. NPAPI, PPAPI and ActiveX files are removed); and

(ii) if known required use, implementing hardening in line with vendor guides.

(d) Microsoft Office Suite hardening: Microsoft Office applications can execute macros to automate regular tasks. However, macros can contain malicious code resulting in unapproved access to sensitive information as part of cyber intrusion. This deliverable includes:

(i) configuring restriction of macro execution by default within Microsoft Office suite (only after prompting users for approval can macros be executed);

(ii) configuring hardening in line with vendor guides; and

(iii) blocking file types.

7.12 **Trusted Application Control Implementation:** this deliverable covers implementation of Application Whitelisting, to provide control over the applications that are allowed in your network or installed and run on your employee workstations. This deliverable includes:

(a) providing a list of currently installed applications across your workstations, and seeking input on which applications should be set as trusted and which should be blocked; and

(b) implementing application whitelisting based on this input using available native Microsoft controls such as App Locker and Software Restriction Policies.

Note that to extend this deliverable to Apple Mac workstations, a separately procured subscription to Apple Profile Manager may be required.

7.13 **Email Security Implementation**: this deliverable includes:

(a) Email domain authentication: generating DMARC and SPF records for your email domain to be verifiable against email spoofing (spammers pretending to be your business). Where domain hosting credentials are readily available, we will implement DMARC and SPF records in your domain's public DNS. Where hosting details are not available, we will provide generic instructions that you can pass onto your service provider to request them to setup the DNS records.

(b) Office 365 Admin and multi-factor authentication: where your email is serviced by Office 365, we will set up a dedicated administrator account for you to use for future adds, moves and changes. We will also implement multi-factor authentication for your new administrator only account.

(c) Office 365 email attachment protection implementation: where your email is serviced by Office 365, we will implement increased malware and ransomware protections by blocking filetypes commonly used by malicious senders.

(d) Office 365 Advanced Threat Protection implementation: where your email is serviced by Office 365 and you have Advanced Threat Protection licensing, we will implement

anti-phishing and Advanced Threat Protection Safe Attachment controls.

7.14 **Post Implementation Document**: this deliverable includes providing you with post-implementation documentation which records the remediation works performed, implemented configuration details and any credentials created or reset for you to handover to your nominated technical party.

7.15 **Patching Remediation – Server & Network:** This deliverable includes:

(a) Server operating system patching: where automatic software updates have not completed, we will systematically troubleshoot impediments and attempt to bring a single Windows domain controller/server up to the latest security and system updates, as available at the date of remediation. Configuration of automatic update scheduling will be implemented where available, however future support is beyond the scope of and is not included in Cyber Security Remediation.

(b) Network device patching: where active vendor maintenance is in place, our team will attempt to upgrade device firmware on up to three devices (switch, firewall/router, Wi-Fi access point) to the latest security updates, as available at the date of remediation.

7.16 **User Access Management Implementation:** this deliverable covers the implementation of user groups for file shares based on roles and required access privileges and the restriction of administrator privileges within a network. Where requested, we will work with you on deploying user groups across your company data so that sensitive information (e.g. employee payroll) is restricted to only users whose role requires access to it.

7.17 **Data Backups Optimisation:** this deliverable covers the optimisation and configuration of your existing data backup solution, including policy configuration and testing those from: Acronis, Commvault, Datto, QNAP, Synology, Veeam or Veritas. This deliverable includes:

(a) Schedule, retention and policy: where absent, backup schedules will be implemented by mapping backup suitable data per business use to suitable destination data store(s) per business needs. We will confirm the frequency that the different types of your business data changes and will configure appropriate backup policies to help accommodate business needs.

(b) Offline and offsite: where available, we will configure the replication of backup data to offline (external/portable media) or offsite (online/cloud) data stores per the business' requirement. In all cases, the backup target media and tools must be supplied by you.

(c) Restoration test: testing of backup effectiveness will be performed in consultation with you. We will request you to nominate a group of files, directories or machines to test restoring from. The procedure of restoration will be documented in detail in the provided Post Implementation Documentation referred to in clause 7.14.

(d) Data backups notification of issues: where supported by your selected solution, email notifications of backup job failures and storage exhaustion will be setup to your preferred destination.

7.18 **MS Azure Active Directory Service Implementation:** this covers the implementation of a

new cloud-based Azure Active Directory service, to centralise user authentication and policies for staff workstations. The subscription and licensing of MS Azure Active Directory is to be priced and procured separately. This deliverable includes:

(a) deploying new Active Directory service on customer specific Azure instance;

(b) assign user licenses > setup user profiles;

(c) configuring user access policy, per your requirements;

(d) setting up groups, per your requirements;

(e) assigning users to admin roles, per business requirements;

(f) assisting with connection of workstation profiles; and

(g) walking through documentation for self or 3rd party management of staff adds, moves and changes.

What is not included?

7.19 Any legal or other advice on which standards a customer needs to comply with or extent of compliance.

7.20 Any software licensing, hardware or ongoing maintenance of an implemented solution.

7.21 The facilitation of user training.

7.22 Any changes to the current environment will be out of the scope of security audit.

7.23 Any other item or responsibility not expressly included in this document as part of Cyber Security Remediation service offering.

Telstra Responsibilities

7.24 The following are Telstra's responsibilities in the delivery of the Cyber Security Remediation service offering:

(a) We must complete all the Service Deliverables applicable to your service level detailed under clauses 7.8 - 7.18.

(b) We must collaborate with you to schedule the Cyber Security Remediation and set the agenda for any workshops or meetings.

(c) We will work with our preferred service delivery partners to deliver the Cyber Security Remediation to you.

Customer Responsibilities

7.25 You must:

(a) make sure that appropriate business owners and technical staff can attend or participate in our scheduled meetings and/or workshops as needed to perform the

Cyber Security Remediation.

(b) Complete a PS-020 Cyber Security Audit. The output of the PS-020 Cyber Security Audit generates critical input used to understand the environment and determine the correct remediation elements. For clarity, we will only deliver the Cyber Security Remediation if we have access to a recent (no more than 90 days old) PS-020 Cyber Security Audit Report and source data for the same customer and performed by the same nominated service provider.

(c) Complete the PS-050 Cyber Security Remediation Pre-Work Checklist provided to you. You must complete and sign this pre-work checklist before we conduct the Cyber Security Remediation to confirm requirements.

7.26 Cyber Security Remediation and the required and completed PS-020 Cyber Security Audit Report are or will be based on information you provide or have provided to us, and that we extracted from your operating environment with remote tools. We will assume all the information you provide is up to date and valid for your operating environment.

7.27 You should also note that our ability to complete our service delivery depends on you providing the items and information outlined in clause 7.25 above. If you fail to comply with clause 7.25, such failure may result in extra charges or alteration to billing milestones for this service. We will let you know in advance in this occurs, and if you do not agree with the extra charges or alteration to billing milestones, we will not provide (and we are not otherwise required or obligated to provide) the service.

Service Pricing

7.28 Charges for your Cyber Security Remediation (and where relevant, limitations on service inclusions) are set out in the Cyber Security Remediation Critical Information Summary, a copy of which will be provided to you.

7.29 Additional charges will apply if we have to spend additional time on your Cyber Security Remediation in order to comply with your specific requirements to complete provision of deliverables (such as HSE inductions), provided that we tell you of those additional charges in advance. If you do not agree with those additional charges, we will not provide (and we are not otherwise required or obligated to provide) the service.

Location of Services

7.30 All Cyber Security Remediation services are delivered remotely.

7.31 If on-site work is required, additional travel and other fees will be quoted prior to commencement.

Special meanings

7.32 In this clause 7, the following words have the following special meanings:

Cyber Security Audit means the services outlined in clause 6.

Service Deliverables has the meaning given to it in clause 7.6.

8 NETWORK DEVICE MANAGEMENT

Service Summary

8.1 The Network Device Management service provides remote device management and support, related internet connectivity monitoring and device status alerting for your businesses' networking infrastructure, as agreed with us.

8.2 Network Device Management is suitable for administering remote management capable networking devices, such as compatible routers, switches, and Wi-Fi access points that we sell to you.

8.3 These network devices are remotely monitored and administered to help understand or mitigate the impact of network and connectivity issues as they occur to help reduce business disruption.

8.4 Network Device Management offers a choice of contract lengths and support hours.

8.5 As Network Device Management is a service delivered remotely via the internet, it is recommended that Network Device Management includes the management of your primary router per site.

8.6 During service take-on, we will link nominated devices to a remote monitoring and management system so that the devices can be monitored, supported and remotely managed and provide you with a mechanism to lodge support and service requests.

8.7 Supply and installation of network devices and related licencing is excluded from Network Device Management, and is available on separate terms and pricing.

What is included?

8.8 We (through our personnel and managed service providers ('**MSP**')) will deliver the Network Device Management service to you in accordance with clauses 8.8 - 8.14.

8.9 The Network Device Management service is available in two different service management classes (Standard and Advanced, as further described in clause 8.11) and is priced depending on the type of managed device and inherent service management complexity.

8.10 Network Device Management includes:

(a) router Management;

(b) switch management; and

(c) access point management.

8.11 Based on the specific make and model of the intended devices for service management, we will automatically class each Network Device Management service into one of the following two possible service management classes:

(a) **Standard Management** being the management of small and medium capacity, standard complexity devices, which have lower than 1Gbps throughput or deliver less

than 1000 concurrent VPN tunnels; and

(b) **Advanced Management** being the management of high capacity or high complexity devices, which have 1Gbps or higher throughput or deliver 1000 or more concurrent VPN tunnels.

(c) The MSP will offer service desk support during Local Business Hours unless Extended Business Hours is selected in your Application Form.

(d) **Local Business Hours** means the hours between 8:30 AM to 5 PM, Monday to Friday, excluding public holidays at the relevant site.

(e) Extended Business Hours may be offered on specific services and by certain MSP as an add-on service for an additional fee.

(f) **Extended Business Hours** means the hours between 8:30 AM to 8 PM, Monday to Friday + Saturday 9 AM to 12 PM, excluding public holidays at the relevant site.

8.12 You may request the same service desk support hours (being either Local Business Hours or Extended Business Hours) for all devices at a specific site. If you include more than one site in your Application Form and Extended Business Hours are available, the support hours may differ for each site.

8.13 All Network Device Management elements will be billed as separate line items.

8.14 The Network Device Management service, irrespective of the contract term, attracts a monthly fee, due monthly and billed in advance.

Service Description Deliverables Table

8.15 The following table summarises the service deliverables included in each of the service management classes ('**Service Deliverables**').

Item	Service Deliverables
Transition Service Process objective: To implement ITSM services. Transition services help make sure that changes to services and service management processes are carried out in a coordinated way.	**Remote management setup, configuration, and testing** • This service includes the setup of the monitoring and alerting system. • It includes the supply, configuration and installation of monitoring tools or needed software agents by which our IT Service Management ('**ITSM**') tools can remotely monitor and manage your network devices covered by your Network Device Management service. • Documenting and updating information about your Approved Environment, as well as the configuration of alerting and knowledge articles for your Approved Environment. • Includes validation of the monitoring tools and processes for your Approved Environment.
Service Operation Process objective:	**Monitoring & Alerting** [1] • This service includes automated remote monitoring of your network device/s as defined as the Approved Environment, for availability, network device latency, event logs, system information and performance counters – subject to device capability. • Includes real-time email alerts to you based on detected performance-related critical threshold breaches, faults and usage statistics.

Item	Service Deliverables
To help make sure that the IT services are delivered effectively and efficiently. The service operation process includes fulfilling user requests, resolving service failures, fixing problems, and carrying out routine operational tasks.	**Service Ticket Management** • Unlimited number of requests. • Proactive logging of detected service faults (we do it for you). • Access management. • 3rd party management (interacting with 3rd party vendors) including RMA (manufacturer's warranty claim) management of in-scope devices as listed as part of the Approved Environment.
	Incident Management • This service includes management of Incidents to restore normal operation to the Approved Environment through an incident management process.
	Monthly Service Reporting [2] • Monthly service tickets and requests summary. • Standard reporting as supported by the device (reporting capability varies per device model).
Continuous Improvement Process objective: To use methods from quality management to learn from past successes and failures. The continuous improvement process aims to continually improve IT processes and services' effectiveness and efficiency, in line with the concept of continual improvement adopted in ISO 20000.	**Service Asset & Configuration Management** • Tracking and reporting on ownership of network devices in the Approved Environment throughout the asset lifecycle (from procurement through to disposal). • Maintaining related information about the Approved Environment's network devices, their relationships to each other, and other customer-relevant or service management-related data.
	Patch Management • This service includes patch management of the Approved Environment. It is the process of finding, testing, distributing and applying updates to device software when required to help correct or prevent errors (also referred to as "vulnerabilities" or "bugs") in the network device software whilst helping reduce business impact.
	Service Improvement • Continuous improvement activities include identifying, performing, or recommending actions for the availability, reliability, and performance of the managed network devices in the Approved Environment.

Note 1:

(a) The Approved Environment is specified in the Network Device Management (MS-030): Pre Service Checklist, agreed with you in writing, which will form part of our agreement with you for the Network Device Management service.

(b) It is recommended that this service's primary device be the main router per site and all devices must be included in the Approved Environment description.

(c) The Network Device Management service includes the configuration of remote monitoring of specified network devices in our ITSM and Remote Monitoring and Management (‘**RMM**’) systems. The Network Device Management service is limited to devices currently available and orderable through us.

(d) Different devices may offer varying remote management capabilities. Our service delivery partner will be able to advise on the features and remote management capabilities of your specific equipment.

Note 2:

(e) Reporting varies per device, make and model. We will optimise reporting based on available report sources.

Service Deliverables

8.16 Network Device Management is a proactive managed service and includes remote monitoring, alerting and incident management, as well as a proactive service desk that aims to maintain the performance and availability of your Approved Environment with preventative activities. Also, the service desk will respond to related change requests, service alerts and troubleshoot network issues on your behalf during the service hours set out in your Application Form, including fault lodgement with us regarding the device's carrier connectivity when needed.

8.17 The Service Deliverables for the Network Device Management service are further described in clauses 8.18 - 8.27 below.

8.18 **Remote management setup, configuration, and testing**

(a) This Service Deliverable consists of the following transition processes:

(i) setting up remote monitoring and administration of the Approved Environment, as specified in the Network Device Management (MS-030): Pre-Service Checklist agreed with you in writing;

(ii) infrastructure documentation/detailing;

(iii) probe setup and linking to our service management and monitoring systems, including probe agent licencing;

(iv) device alert configuration and testing; and

(v) remote monitoring validation.

(b) We will implement or activate relevant RMM tools, linking them to your specified Approved Environment. These tools may include opening two network ports on your firewall for SNMP/WMI based remote monitoring, plus admin access to your network device, its associated management portal and, where needed, installing software agents or probes on the specific network device.

(c) If your specific network device requires any additional licencing from its manufacturer to enable remote monitoring, those licences will be your responsibility and, where relevant, may be quoted before work commences.

8.19 **Monitoring & Alerting**

(a) We will:

(i) conduct automated remote monitoring of your Approved Environment for availability, network device latency, event logs, system information and performance counters, subject to device capability;

(ii) send you near real-time email alerts, which are based on detected performance-related critical threshold breaches, faults and usage statistics;

(iii) use RMM tools, device management platforms and your Internet connection, to remotely collect and interpret real-time device usage data and status

messages and aggregate the data to our remote monitoring system or interface;

(iv) this diagnostic data does not include any identifiable Internet traffic content. This diagnostic data includes non-personal metrics such as data volumes transferred over time, quality metrics such as latency, uptime, availability as well as system logs and error codes for diagnostic purposes where available. This usage reporting drives real-time alerts based on pre-set thresholds;

(v) track network and device health via our RMM system, keeping records of these activities/fault tickets for the Service's duration. All collected data will be deleted on termination of the Service (except for archival purposes or if the law requires that the data be kept);

(vi) systematically interpret the managed device's performance logs and associated network performance events and metrics as inputs to performance reporting, alerting, and diagnostic tasks;

(vii) recommend and agree to alerting thresholds, a suitable delivery mechanism for alerts (such as SMS or email) with you and provide the alerting service; and

(viii) maintain a record of the current device configuration in support of the devices under management in the Approved Environment.

8.20 **Service Ticket Management**

(a) All valid requests reported by you to the MSP service desk ('**Service Desk**') will be logged as a ticket ('**Service Ticket**') in our platform.

(b) A request will only be valid if you provide the Service Desk with the following information:

(i) customer account number, account name and service number;

(ii) details of the Service Request (for example, symptoms and degree of impact);

(iii) impacted areas of your business;

(iv) contact details (including any premises contact details where on-site attendance may be required);

(v) desired outcome required; and

(vi) any other related information.

(c) Upon receiving a valid Service Ticket, we will classify the Service Ticket as either a failure or degradation of the service we manage ('**Incident'**) or any other request not related to failure or degradation of the service we manage ('**Service Request'**).

(d) As part of Service Ticket resolution, the Service Desk will:

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

(ii) classify the Service Ticket;

(iii) manage the Service Ticket until it is resolved or closed;

(iv) provide status updates for the Service Ticket; and

(v) advise you of the closure of the Service Ticket.

(e) We will deliver Service Ticket resolution remotely unless on-site resolution is included in your Application Form.

(f) Where on-site attendance is required to resolve the Service Ticket, we will arrange a suitable time to attend the premises with you (additional fees may apply).

(g) If we reasonably believe the request does not arise from or relate to the Network Device Management service, we will promptly advise you and close the Service Ticket.

(h) If we reasonably believe the request cannot be resolved, we will communicate to you why the Service Ticket cannot be resolved and close the Service Ticket.

(i) During the support hours set out in your Application Form, the Service Desk will perform active monitoring for alert events and trends of your Approved Environment and proactively lodge needed service tickets on your behalf for remediation and management and inform you of any impacts as required.

8.21 **Incident Management**

(a) This Service Deliverable aims to manage Incidents to restore normal operation to the Approved Environment.

(b) If we classify a Service Ticket as an Incident, the Service Desk will determine a priority rating based on the Impact and Urgency matrix as listed in the table below:

		URGENCY		
		High	Medium	Low
IMPACT	High	Priority 1 - Critical	Priority 2 – High	Priority 3 - Medium
	Medium	Priority 2 - High	Priority 2 –High	Priority 3 - Medium
	Low	Priority 3 - Medium	Priority 3 – Medium	Priority 3 – Medium

(c) **Urgency**: We define 'Urgency' as the necessary speed of restoration of service, based on available information, and it is classified as follows:

(i) **High**: no work can be performed, and your managed service is down at either a major site or multiple sites;

(ii) **Medium**: unable to perform some work tasks, but most business operations continue; and

(iii) **Low**: information requests and low priority work tasks.

(d) **Impact**: We define 'Impact' as the measure of how business-critical the Service Ticket is, based on available information, and it is classified as follows:

(i) **High**: entire Approved Environment inoperable across the total user population, causing a critical impact on your business operations;

(ii) **Medium**: approved Environment partially inoperable, and managed service is severely degraded, impacting significant aspects of business operations; and

(iii) **Low**: any degradation in service to Approved Environment.

(e) We will aim to respond to Service Tickets within the target response times set out in the table below ('**Response Times**') based on their priority ranking:

Priority	Response Times	Service Level
Priority 1	1 Business Hour	Assign a Service Ticket to at least 95% of Incidents and communicated to customer within response times
Priority 2	4 Business Hours	
Priority 3	8 Business Hours	

(f) For the duration of a Priority 1-Critical Incident (as defined in the table in clause 8.21(b)), we will provide a named incident manager or implement a matrixed incident resolution team responsible for restoring your services while keeping you informed of developments and expectations.

(g) Subject to clause 8.20(b), Response Times will be calculated from the time we receive your request of the Incident to the time we issue the Service Ticket to you.

(h) Response Times will be calculated within the support hours set out in your Application Form.

(i) Unless a service level exclusion applies in clause 8.23, we aim, but do not promise to, meet the service levels set out in clause 8.21(e), and you are not entitled to any credit if we do not meet those service levels.

8.22 **Service Request Management**

(a) This Service Deliverable aims to manage the Service Requests for your Network Device Management service.

(i) Service Requests may relate to remotely delivered services such as:

(A) moves, adds, changes and Deletions;

(B) password changes;

(C) requests for information in response to "how to" questions.

(b) If we classify your Service Ticket as a Service Request, it will be considered Priority 3 as described below by default unless we reasonably believe it should be a higher priority. The priority of a Service Request will be assessed on the Impact and Urgency.

		URGENCY		
		High	Medium	Low
IMPACT	Low	Priority 3 – Low		

8.23 **Service Level Exclusions**

(a) The Response Time service levels will not apply and we will not be responsible for a failure to meet a service level resulting from:

(i) a fault or failure of your Network Device Management service that is caused by you;

(ii) a failure by you to comply with the terms of agreement with you for the Network Device Management service;

(iii) any period of a scheduled maintenance;

(iv) any interference to you or your third party's services, infrastructure, equipment, software (including operating or email systems), configurations or other technology that support your environment that is out of our direct control;

(v) any unauthorised changes made by you or a third party to your technology infrastructure, software or configurations that support the Network Device Management service; and

(vi) suspension or termination of your right to use or access the Network Device Management service.

8.24 **Monthly Service Reporting**

(a) Automated reporting will be set up on the Approved Environment managed network devices and remotely collected and stored via our ITSM tools.

(b) We will use this data to create and issue standard usage reporting, which will be sent via a monthly email to your nominated email account.

(c) This Service Deliverable includes a standard monthly emailed report and will include:

(i) **devices under management** (in the Approved Environment) and an indication of remaining service life;

(ii) **service history** including:

(A) service tickets: details of recent service tickets associated with your managed services, including those raised by your team and those proactively triggered by monitoring events such as outages or logged on your behalf by us; and

(iii) **usage reporting** including:

(A) traffic utilisation of top applications;

(B) client utilisation;

(C) device utilisation; and

(D) port utilisation

(d) Reporting capabilities will vary by device type, make and model. We will endeavour to provide additional reporting, subject to device data availability and any additional costs.

8.25 **Service Asset and Configuration Management**

(a) This Service Deliverable aims to maintain and update a record of information about the specific network devices under management in the Approved Environment and includes:

(i) monitoring and maintenance of a record of the specified device(s) under management's current software version and details of changes over time as performed;

(ii) maintaining configuration management information on the relationships of these managed network devices to each other and other customer relevant or service management related data, including:

(A) managed device location;

(B) managed device-specific configuration;

(C) authorised customer contacts;

(D) active user details per managed device;

(E) admin passwords per managed device; and

(F) maintaining device-specific management console and vendor information as needed to deliver ongoing network device management services.

(iii) tracking the ownership, purchase dates and age of devices in the Approved Environment throughout the asset lifecycle (from procurement through to disposal).

8.26 **Patch Management**

(a) This Service Deliverable includes patch management of the network devices within the Approved Environment. It is the process of finding, testing, distributing and applying updates to the device's internal software when required to help correct or prevent errors (also referred to as "vulnerabilities" or "bugs") in the network device software whilst helping reduce business impact.

(b) Remote firmware updates/ patching of nominated devices will only occur according to manufacturer recommendations and as mandated by us to mitigate specific issues and require your explicit approval.

(c) This Service Deliverable includes:

(i) monitoring and sourcing the device manufacturer's latest model-specific firmware versions as they become available, in-line with our and the device manufacturer's latest recommended version advice;

(ii) proactively and remotely installing the latest device software version at a change window time agreed to with you;

(iii) Agreed change window downtime is excluded from uptime calculations. Unless otherwise notified and agreed, the default change window is defined as every Sunday morning between 3.00 AM and 4.00 AM;

(iv) manufacturer or our recommended urgent security related device firmware updates may be applied at any time, outside the change window, taking cognisance of your current business needs into account;

(v) verifying that network connectivity is restored after the software update/patching; and

(vi) if the software update causes an issue, we will follow the manufacturer's rollback procedure, with the primary goal always to ensure connectivity uptime.

(d) Any software or firmware update involves risk and will be applied only at your direction and risk.

8.27 **Service Improvement**

(a) This Service Deliverable is the delivery of improvement activities identified through ongoing remote monitoring and management and analysis of past service management activities, as well as analysis of problems, incidents and service tickets to identify, implement or recommend actions or changes needed for improvement to the availability, reliability and performance of the managed network devices in the Approved Environment.

(b) Proactive problem avoidance activities may include logging faults with 3rd parties, such as Telstra, the NBN, or the device's manufacturer if required and managing the fault ticket to resolution.

(c) Service improvement activities that will materially and detrimentally impact your staff, business operations or require investment will be explicitly agreed upon with you before commencement.

(d) The service includes progress updates to your nominated contact.

What is not included?

8.28 The Network Device Management service does not include any network device supply and installation, cabling, or any other underlying device-specific licences, equipment or infrastructure installation unless explicitly specified in this Agreement.

8.29 Management of network devices not explicitly identified in the 'Network Device Management (MS-030): Pre-Service Checklist' agreed with you in writing is not covered in the Network Device Management service.

8.30 The Network Device Management service does not include support for changes made to devices under management by 3rd parties, such as your IT department or other providers.

8.31 Additional work not included in package Service Deliverables described above, including work outside of our standard business hours, are not included as part of the package Service Deliverables.

8.32 Additional charges apply in respect of site visits (except for our first Metro Site visit) and are dependant on the distance of your site from our service delivery partners' location. The applicable charges will be set out in your Application Form.

8.33 Before we perform any service outside the standard included Service Deliverables for a Network Device Management service, we will provide a quotation for the non-standard services for your confirmation.

8.34 The Network Device Management service and associated inclusions are not an insurance service and do not imply warranty or guarantees regarding service uptime.

8.35 Any other item or work not explicitly described in these terms or your Application Form as being part of the Network Device Management service, is not included as part of the Network Device Management service.

8.36 **Our Responsibilities**

8.37 The following are our responsibilities in the delivery of the Service. We must:

(a) collaborate with you to schedule the Network Device Management service's initial configuration and set the agenda for required workshops or meetings;

(b) complete the relevant Service Deliverables detailed under clause 8.15, as set out in your Application Form.

(c) In the event of a connectivity issue to a managed device, the MSP will contact the connectivity carrier (which must be us) on your behalf for fault lodgement, fault finding and rectification purposes.

(d) We will work with our preferred service delivery partners to deliver the Network

Device Management service to you.

(e) Our MSP will have access to an email alerting capable RMM tool (remote monitoring and management) or portal. This system will generate alerts based on telemetry data as received from your devices, with default service thresholds pre-defined for specific monitored elements. Examples of alerts may include time-out (device unreachable), usage, availability, and other performance statistics. The range of available telemetry data to drive monitoring and alerting based services will vary between different network device vendors and models.

(f) Any other Telstra responsibilities set out in these terms or your Application Form.

Your Responsibilities

8.38 To receive the Network Device Management service and access the service deliverables described above, you must promptly complete the following at your own cost:

(a) complete the 'Network Device Management (MS-030): Pre-Service Checklist' provided to you. You must complete and sign this pre-service checklist before the Network Device Management services commence to confirm your requirements and define the managed devices within the Approved Environment. Reporting contacts must be provided, including confirmation of reporting frequency and named customer contacts and email addresses for reports;

(b) participation: ensure that the appropriate business owners and technical staff will attend or participate in our scheduled meetings or workshops as needed for us to perform the Network Device Management service;

(c) accurate IT information: provide accurate high-level detail on your internal IT services and strategy to us. Please note that our services and the Network Device Management configuration and service design will be based on the information you provide to us and that we extract from your operating environment with remote tools. We will assume all the information you provide is up to date and valid for your operating environment;

(d) licencing: certain network device features require specific licencing, which must be obtained under a separate agreement. We may advise if your device requires additional licencing. It is your responsibility to ensure that your network devices are appropriately licenced including in line with any advice we provide;

(e) access to systems: make sure and assist in providing us with appropriate administration credentials and remote access to the management consoles of devices in the Approved Environment so that we can configure and activate the Network Device Management service and deliver the ongoing remote monitoring and service management as required. Administrator access to the device will be restricted to us and our MSPs only, to maintain service responsibility integrity.

(f) usage of your Internet connectivity: you must 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 Network Device Management service (including obtaining any required consents or approvals and opening required network ports);

(g) reasonable care: if a loan device is provided at any time, it is your responsibility to keep it in the original condition as received and make it available for removal by our MSP when required to do so;

(h) access to the site: provide reasonable access to the site by our technician if needed;

(i) sign, date, and return the Customer Acceptance Certificate we provide to you once the Network Device Management service has been deployed and testing shows it is working;

(j) where we or our MSP incur costs due to your negligence, fault, act, or omission, you must pay us additional fees, which we will confirm on request; and

(k) any other responsibilities agreed under our agreement with you for the Network Device Management service or reasonably requested by us or our MSP to perform our obligations under our agreement with you for the Network Device Management service.

8.39 Our ability to provide the Network Device Management service depends on you promptly providing the items and information outlined in clause 8.38. If you fail to comply with your obligations in clause 8.38, such failure may result in extra charges or alteration to billing milestones for this service. We will let you know in advance in this occurs, and if you do not agree with the extra charges or alteration to billing milestones, we will not provide (and we are not otherwise required or obligated to provide) the service.

Service pricing

8.40 Charges for the Network Device Management service (and where relevant, limitations on service inclusions) are set out in your Application Form.

8.41 An additional service fee will apply if we have to spend additional time on your Network Device Management service in order to comply with your specific requirements (such as HSE inductions). The additional service fee may include reinstallation charges, charges for extra time-on-site, as well as travel fees. We will inform you of those additional charges in advance. If you do not agree with those additional charges, we will not provide (and we are not otherwise required or obligated to provide) the service.

Location of services

8.42 All Network Device Management services are delivered remotely.

Hardware assessment

8.43 The Network Device Management service is available only for the current compatible devices we supply to you. As devices and capabilities differ, we might not be able to manage your devices remotely. We will assess each of your device make and model, and if we cannot control and monitor it, we will let you know that the device is not eligible for the Network Device Management service.

Total minimum service cost

8.44 Minimum costs for each Network Device Management service are set out in your Application

Form and is billed monthly in advance. The minimum cost you pay depends on the package you select, the support option you choose, and any additional services you need.

Term and termination

8.45 Your Network Device Management service begins from the completion of the relevant deliverables, as specified on the Customer Acceptance Certificate, and continues for the minimum term, as set out in your Application Form, unless terminated or renewed in accordance with these terms.

8.46 Either party can terminate a Network Device Management service at any time by giving the other party at least 30 days' prior written notice. If you choose to terminate a Network Device Management service within the minimum term set out in your Application Form (where the minimum term is greater than one month) or we terminate your Network Device Management service as a result of your material breach, we may charge you an early termination charge calculated as the lesser of:

(a) the monthly charges payable for the relevant terminated Network Device Management service x the number of months remaining in the applicable minimum term; and

(b) 35% of A x B where A is the monthly charges payable for the relevant terminated Network Device Management service and B is the total number of months contained in the applicable minimum term minus one month.

You acknowledge that this is a genuine pre-estimate of our loss.

8.47 We may terminate or suspend your Network Device Management service immediately by notice to you if:

(a) you fail to comply with your obligations in clause 8.38 and you fail to remedy the non-compliance within 14 days of being notified of the non-compliance; or

(b) our agreement with our third-party supplier for the Network Device Management service expires or is terminated such that we are unable to continue to provide the Network Device Management service under our agreement with you. If this happens, may migrate you to a reasonably comparable alternative service on reasonable notice to you. If we transfer you to a reasonably comparable alternative service and this has more than minor detrimental impact on you, you may cancel your service without having to pay any early termination charges for that service.

8.48 On termination, cancellation or expiry of the Network Device Management service:

(a) you must cease using or accessing the Network Device Management service; and

(b) you must pay us all outstanding invoices for the Network Device Management service by their due date.

8.49 On expiry of the minimum term for your Network Device Management service as set out in your Application Form, your Network Device Management service will automatically renew on a month-to-month basis, unless either party cancels the Network Device Management service by notifying the other party at least 30 days prior to any automatic extension.

Payment options

8.50 Apart from the Network Device Management service setup fees, if applicable, which will appear as a once-off amount on your first Telstra bill after service activation, the Network Device Management service is only available as a monthly subscription payment option for the duration of your agreement with us.

8.51 Usual credit terms apply to the payment of these amounts.

Special meanings

8.52 In this clause 8, the following words have the following special meanings:

Approved Environment means the devices covered under your Network Device Management service, as identified in the in the 'Network Device Management (MS-030): Pre Service Checklist' referred to in clause 8.15. For the purposes of this definition, 'device' refers to IP manageable network devices such as a router, switch or Wi-Fi access point with SNMP v3 or WMI remote monitoring capability that are compatible with the Network Device Management service.

Extended Business Hours means the hours between 8:30 AM to 8 PM, Monday to Friday, and Saturday 9 AM to 12 PM, excluding public holidays at the relevant site.

Impact has the meaning given to it in clause 8.21(d).

ITSM has the meaning given to it in the table in clause 8.15.

Local Business Hours means the hours between 8:30 AM to 5 PM, Monday to Friday, excluding public holidays at the relevant site.

MSP has the meaning given to it in clause 8.8.

Response Times has the meaning given to it in clause 8.21(e).

RMM has the meaning given to it in clause 8.15(c).

Service Deliverables has the meaning given to it in clause 8.15.

Service Desk has the meaning given to it in clause 8.20(a).

Service Request means a Service Ticket classified by us as a Service Request, as contemplated in clause 8.20(c).

Service Ticket has the meaning given to it in clause 8.20(a).

Urgency has the meaning given to it in clause 0.

9 TELSTRA INSTALL – MICROSOFT 365 BUSINESS

Service Summary

9.1 The Telstra Install - Microsoft 365 Business service is a professional service to remotely

install, configure, verify and handover a new Microsoft 365 Business environment and customer tenancy, based on Telstra's policies for Microsoft 365 Business.

9.2 The service is delivered remotely, and is limited to installing the applicable components, features, and capabilities offered within the Microsoft 365 Business platform. Onsite options are available for additional charges, and are priced on application.

9.3 Remote installation requires matching time commitments from your elected administrator for orientation, remote hand assistance or training. This is your responsibility.

Eligibility requirements

9.4 The Telstra Install – Microsoft 365 Business service requires a separate paid subscription to Microsoft 365 Business plans purchased directly from Microsoft, an authorised Microsoft Cloud Service Provider (CSP), or via the Telstra Application Marketplace (TAM). You need one applicable Microsoft 365 Business licence for each user type you would like to deploy. Our Account Manager or our service delivery partner can help order this on your behalf, using the information you provide.

Customer Profile

9.5 The Telstra Install – Microsoft 365 Business service is offered to Telstra customers who have ordered Microsoft 365 Business applications and services and require professional installation and activation.

What is included?

9.6 The Telstra Install - Microsoft 365 Business service is dependent on Microsoft 365 Business plan subscriptions (M365 Business Basic, M365 Business Standard, and M365 Business Premium), which are sold separately.

9.7 We will deploy and install each of these licences, and/or their standalone components as per Microsoft standards and policies.

Service Description Deliverables Table

9.8 The inclusions in the Telstra Install – Microsoft 365 Business service are set out in the table below and are further described in clauses 9.10 - 9.15 ('**Service Deliverables**').

	Service Deliverables
ALL SERVICES INCLUDE	- Transition planning and support (as per clause 9.10) - Change Management (as per clause 9.11) - Service Asset configuration management (as per clause 9.12]) - Release and deployment management (as per clause 9.13]) - Service Validation and Testing (as per clause 9.15)
OPTIONAL SERVICE ADD-ON	- MS365 Apps for Business – Device Installation - Microsoft Endpoint Manager - Microsoft Defender P1 (Cloud)

Service Deliverables:

9.9 A description of each Service Deliverable is set out in in clauses 9.10 - 9.15.

9.10 **Transition planning and support:**

(a) This comprises:

(i) the coordination of the service delivery activities that are required for a successful installation, such as verifying an efficient service delivery mechanism, coordinating licence purchase if needed, and arranging the installation appointment with your nominated representative that will act as remote hands and be set up as your admin user; and

(ii) validating required information for success. This includes confirming in Telstra Application Marketplace (TAM) and your customer Telstra account that the specified Microsoft 365 Business plans and/or subscription are available to support the required installation service and policies defined in the 'PS-011 – Presales Checklist – Telstra Install-Microsoft 365 Business' provided to you.

(b) Services are delivered via scheduled remote appointments within our business hours (Monday to Friday, 9 am-5 pm in the State or Territory in which we or our service delivery partner are located).

9.11 **Change Management:**

(a) Using the information you provide when you complete the 'PS-011 – Presales Checklist – Telstra Install-Microsoft 365 Business' form we provide to you, we will review your hardware environment, and Microsoft 365 Business licence subscriptions, to help ensure compatibility and to help optimise the user experience for Microsoft 365 Business.

9.12 **Service Asset and Configuration Management:**

(a) Using the information you provide when you complete the 'PS-011 – Presales Checklist – Telstra Install-Microsoft 365 Business' form we provide to you, we will configure your user accounts as per your licence subscription requirements and align your users to the latest Telstra policy as set out in clause 9.13.

9.13 **Release and Deployment Management**

(a) Using the information you provide when you complete the 'PS-011 – Presales Checklist – Telstra Install-Microsoft 365 Business' form we provide to you, we will install the requested Microsoft 365 Business service as per the latest Telstra policy.

(b) This Service Deliverable includes deployment services associated with each component of the Microsoft Business 365 service, as detailed in the table below. Certain deployment services are only available if you purchase the relevant Telstra Microsoft 365 Business Service package or Optional Service Add-On.

Microsoft Business 365 Service Component	Deployment Services	Telstra Install – Microsoft 365 Business Service Type		
	Note: Feature availability is based on your MS365 licence	M365 Essential – Customer Setup	M365 Essential – User Setup	Service Add-on

M365 Admin Portal	Setup M365 customer tenancy including Administrators Create or Import users Setup DNS (as per clause 9.14) Add customer logo Service Validation and Testing (as per clause 9.15)	✓		
User Setup	General setup of end users including: - Set up of Multi Factor Authentication (MFA) - Email migration of 1 email box per user up to 50GB - Set up Gmail, Apple Mail or Windows Mail (as applicable on up to 3 devices per user)		✓	
Exchange Online	Configure & deploy malware policy Configure & deploy spam policy Configure & deploy safe attachments policy Configure & Deploy DMARC & DKIM policy Append standard terms and conditions disclaimer to emails Configure alerting rules to support	✓		
Azure Active Directory	Multiple security groups created for permission management Approval processes for consenting to apps which request access to company data Remove the ability for Azure AD users to consent to apps they own Enable multifactor authentication for all users Enable registration methods to include, app, phone, email, and SMS	✓		

	Enable self-password reset			
SharePoint Online	Guest access to expire after 60 days Enforcing MFA verification Guests must use the same account for sign-ins	✓		
Security & Compliance	Enable unified auditing with 10-year retention Configure & deploy safe links profile Enable administrator auditing	✓		
M365 Apps for Business	Installation of M365 apps for business to local devices. Note: Maximum 3 devices per user at time of installation			✓
Microsoft Endpoint Manager	Setup Microsoft Intune tenancy including MDM policies for "Bring your own device" User / Mobile Device enrolment Note: Maximum of 3 mobile devices per user at time of installation.Desktop/Laptop PCs not included			✓
Email Migration	Per mailbox service option Migration of email data from other service providers into the M365 environment Note: Maximum 50GB email data. Additional charges may apply for larger data sets.		✓	
Onsite Installation	Onsite services as required - POA			

9.14 DNS Setup & Domain Setup

(a) We will set up Microsoft 365 DNS record as required for custom domain.

(b) You must promptly provide a suitably qualified technical resource with access to your DNS zone, or provide the information from our technical resource to a service provider who can update records on your behalf.

(c) The records below will be added and validated to help ensure a suitable Microsoft 365 experience:

(i) CNAME records;

(ii) MX record;

(iii) DMARC record;

(iv) DKIM record;

(v) TXT records; and

(vi) SFP record.

(d) Requirements for these records may change depending on the current implementation / deployment of your existing Microsoft 365 environment.

9.15 **Service Validation and Testing**

(a) We will confirm deployment is complete based upon deployment guidelines outlined in these terms. We will test the deployment by running a validation tool to check the environment has been deployed successfully and is in line with our policies.

(b) The validation tool will return any detected errors or missed configuration, which will then be reviewed and/or rectified before handover. Points of validation include, but are not limited to, the following:

(i) test email and email security configuration;

(ii) test platform security policy configuration;

(iii) external sharing; and

(iv) blueprint output test.

What is not included?

9.16 The Telstra Install – Microsoft 365 Business service does not include:

(a) any equipment installation, application licencing, connectivity, or anything else not set out in these terms;

(b) ongoing monitoring or management of the Microsoft 365 Business environment and your tenancy;

(c) Windows 10/11 installation;

(d) onsite installation. This is a remote service only. Onsite installation and support can

be purchased separately for an additional charge and is priced on application;

(e) work outside standard packages. Additional hours of work above the relevant packaged inclusion (to meet your specific requirements) is not included (e.g. Teams phone system integration, Teams App, and Telstra Calling for Office 365). Separate charges will apply for any such work;

(f) software updates on your device such as Windows updates, iOS update on iPhone, or any other software or firmware updates required before the Telstra Install – Microsoft 365 Business service can commence;

(g) enterprise licencing. The Telstra Install - Microsoft 365 Business service is available in connection with Microsoft 365 Business plans only, as outlined in clause 9.6. It is not available in connection with Microsoft 365 Enterprise licences;

(h) email migrations over 50GB per inbox and migration of shared and central inboxes. If you require these services, further charges may apply; and

(i) data migration or usability testing of SharePoint and OneDrive. SharePoint and OneDrive is limited to activation of the services as per the relevant Microsoft licence subscription. Copying of data from source to destination is your responsibility or can be purchased separately on a time and materials basis.

Telstra Responsibilities:

9.17 The following are Telstra's responsibilities in the delivery of the Telstra Install – Microsoft 365 Business service:

(a) collaborate with you to schedule a date and time for the service to be delivered;

(b) complete the deliverables as detailed in these terms;

(c) complete all requirements as detailed in our 'PS-011 – Presales Checklist – Telstra Install-Microsoft 365 Business' document.

Customer Responsibilities

9.18 You must promptly ensure the following for the successful delivery of the Telstra Install - Microsoft 365 Business service:

(a) Microsoft 365 Business: you have a new or existing Microsoft 365 Business plan or standalone licence subscription purchased directly from Microsoft, an authorised Microsoft Cloud Service Provider (CSP), or via the Telstra Application Marketplace (TAM);

(b) Compatible devices: your devices are compatible with Microsoft 365 Business;

(c) Maintain your subscription: you maintain an up to date subscription for relevant licences and applications so the services, features and components of Microsoft 365 Business continue to function;

(d) Provide a technical resource: you provide a suitably qualified technical resource with access to your DNS zone, or provide the information from our technical resource to a

service provider who can update records on your behalf. If you do not have this information, further charges may apply;

(e) Complete Pre-Checklist: you complete and sign the pre-checklist form: 'PS-011 – Presales Checklist – Telstra Install-Microsoft 365 Business' we provide to you, to confirm your requirements. The accuracy of the information in this checklist is critical. The accuracy is your responsibility and the information provided will facilitate this service delivery. Any inaccurate information may incur further charges;

(f) Accuracy: you provide accurate detail on the existing IT & network environment and any specifically requested information about the relevant users, groups and policies that are needed within the Microsoft 365 Business environment;

(g) Agree to and keep installation appointments: you keep any installation appointments. As this is a professional service, we reserve the right to charge for missed service appointments. Please provide at least two business days' notice if you wish to reschedule an appointment;

(h) Access to systems: you provide relevant admin access credentials and access to existing systems to allow us to complete the required configuration, deployment and testing of the environment, including, but not limited to, activation of remote management, automation, and access tools (where necessary);

(i) Act as remote hands: you act as "remote hands" where necessary. In some instances, and with specific technologies, remote tools cannot be used. In these cases, you may be asked to provide "remote hands," e.g. act on our instructions to perform specific needed functions, such as downloading and activating specific applications on a mobile device;

(j) Sign the Customer Acceptance Certificate ('**CAC**'): you sign the CAC upon successful completion of the Telstra Install – Microsoft 365 Business service. Our technician or account manager will request that you sign the CAC upon successful completion of the relevant Service Deliverables.

Service Pricing

9.19 Charges for your Telstra Install – Microsoft 365 Business service (and where relevant, limitations on service inclusions) are set out in your Application Form and Telstra Install-Microsoft 365 Business Critical Information Summary, a copy of which will be provided to you. We may update these charges from time to time. If any changes are made to the pricing after you have taken up the service and those price changes apply to your service and have more than a minor detrimental impact on you in relation to that service, you may terminate your service by written notice to us without having to pay any early termination charges for that service.

9.20 Where required, an additional fee will apply if additional hours are required to comply with your specific requirements to complete the engagement, such as HSE inductions. We will inform you of those additional charges in advance. If you do not agree with those additional charges, we will not provide (and we are not otherwise required or obligated to provide) the service.

Special meanings

9.21 In this clause 9, the following words have the following special meanings:

Customer Acceptance Certificate or **CAC** means the document you must sign upon completion of the relevant Service Deliverables, as contemplated in clause 9.18(j).

Service Deliverables has the meaning given to it in clause 9.8.

10 MANAGED MICROSOFT 365

Service Summary

10.1 Telstra's Managed Microsoft 365 service provides customers with administration, proactive monitoring, management, and user support of their Microsoft 365 Business plans (Basic, Standard and Premium). Telstra's Managed Microsoft 365 service aims to ensure that your Microsoft 365 tenancy is always performing at its best by minimising downtime and vulnerabilities through utilising the latest policies and updates from Microsoft.

10.2 Our service delivery partners are your local trusted experts highly certified in Microsoft cloud services, helping to deliver a best practice approach to managing your services and helping you to get the most from your software investments.

10.3 Our service delivery partners can also help support your network and communications services, providing holistic, end-to-end support for your ICT environment; increasing stability and security of your Microsoft 365 tools and applications, and providing a great user experience.

10.4 Managed Microsoft 365 provides customers with the following:

(a) modular pricing;

(b) no lock in contracts;

(c) monitoring and alerting;

(d) proactive Service Desk;

(e) choice of support hours; and

(f) locally supported by our service delivery partners, backed by Telstra.

What is included?

10.5 The support included in your Managed Microsoft 365 service is dependent on your underlying Microsoft 365 Business plan subscriptions (Microsoft 365 Business Basic, Business Standard, and Business Premium). For customers with Enterprise plans within their Microsoft 365 Business tenancy the Business Premium inclusions will apply. Microsoft 365 plan subscriptions are sold separately.

10.6 We will administer and manage, and provide user support for each of these licences, in accordance with Microsoft standards and policies. Management will be provided at a tenancy

level, and across all Microsoft 365 Business plans within the Microsoft 365 Business tenancy.

* The Managed Microsoft 365 service is available to existing Microsoft 365 tenancies only. Setup, Installation, and deployment of new Microsoft 365 Business and Enterprise tenancies is not included in this service and is available separately.

Supported Microsoft 365 Business Plans and Features			
Microsoft Package Supported	**Business Basic**	**Business Standard**	**Business Premium**
Exchange Online	✓	✓	✓
Azure Active Directory	✓	✓	✓
Teams	✓	✓	✓
Office Web Apps	✓	✓	✓
SharePoint Online	✓	✓	✓
OneDrive	✓	✓	✓
Office Apps for Business		✓*	✓
Endpoint Manager (Mobile Device Only)			✓
Defender for 365			✓

10.7 The Managed Microsoft 365 service is limited to the administration, management and support of the Microsoft 365 platform and applications as per the table below. Troubleshooting, support, and resolution activities for associated ICT components impacting the Microsoft 365 platform and applications will be at Telstra's our discretion.

Supported	**Business Basic**	**Business Standard**	**Business Premium**
Microsoft Application / Platform	Web Browser + M365 Apps*	Web Browser + M365 Apps*	Web Browser + M365 Apps* + Defender for Endpoint
User Device	-	-	iOS, Android, Intune Enrolment
Microsoft 365 Cloud Services	Azure AD, Exchange Online, SharePoint Online, Teams	Azure AD, Exchange Online, SharePoint Online, Teams	Azure AD, Exchange Online, SharePoint Online, Teams, Intune
On-Premise hardware & 365 deployments	-	-	-
Peripheral / Printer	-	-	-

Network / Switch/ Router / Firewall	-	-	-
Internet/ Wifi / Cabling	-	-	-
Security hardware and applications, data management and backup (Outside M365 Platform)	-	-	-
3rd Party / LoB Applications	-	-	-

10.8 Microsoft 365 Business plans and licences within your tenancy that are assigned to an active user will be considered under management. The service is limited to Microsoft 365 Business plans and standalone licences listed above, currently available and orderable through Telstra, Microsoft direct, or a licenced Microsoft Cloud Service Provider

10.9 Standard licence features and inclusions" refers to the Microsoft 365 Business Service Descriptions found here: https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-service-descriptions-technet-library

10.10 Support is provided by phone, email and remote access where required. The Managed Microsoft 365 service does not include onsite support.

10.11 Our service delivery partner will offer service desk support during Local Business Hours unless you are receiving Extended Business Hours support. Support hours are set across the entire Microsoft 365 Business tenancy, and only one option can be selected and applied across each tenancy.

(a) Local Business Hours means only the hours between 8:30 AM to 5 PM, Monday to Friday, excluding public holidays, in the State or Territory in which our service delivery partner is located.

10.12 Extended Business Hours may be offered by some of our service delivery partners as an add-on service and is applicable for all services within your Microsoft 365 Business tenancy. Please contact your service delivery partner to confirm availability of Extended Business Hours support.

(a) Extended Business Hours means only the hours between 8:30 AM to 8 PM, Monday to Friday and Saturday between 9 AM to 12 PM, excluding public holidays, in the State or Territory in which our service delivery partner is located.

10.13 A change to either Extended Business Hours support or Local Business Hours support must be requested via an authorised service ticket and can only be requested once per month. Changes will take affect within 24 hours after authorisation is received.

Service Deliverables tables

10.14 The following tables summarise the service deliverables for the core components of the Telstra Managed Microsoft 365 service platform ('**Service Deliverables**') and outlines our

service responsibilities. More detailed descriptions of the Service Deliverables are included in clause 10.15 - 10.27.

Item	Deliverable
Transition **Service** *Process objective:* *To implement ITSM services.* *Transition services help make sure that changes to services and Service Management processes are carried out in a coordinated way.*	**Policy configuration and Self-healing (as per clause 10.18)** This service includes deployment of Telstra's policy blueprint and desired state configuration across the customers Microsoft 365 business tenancy and includes: - Active Directory - Exchange - SharePoint **Remote management setup, configuration, and testing (as per clause 10.19)** - This service includes the setup of the monitoring and alerting system. - It includes the supply, configuration, installation and validation of monitoring tools or necessary software agents by which our ITSM tools can remotely monitor and manage your Microsoft 365 Business tenancy - Documenting and updating service information about your Microsoft 365 Business tenancy including common tickets and software utilisation, as well as the configuration of alerting and knowledge articles
Service Operation *Process objective:* *To help make sure that the IT services are delivered effectively and efficiently.* *The Service Operation process includes fulfilling user requests, resolving service failures, fixing problems, and carrying out routine operational tasks.*	**Monitoring and Alerting (as per clause 10.20)** - This service includes automated remote monitoring of your Microsoft 365 Business tenancy for availability, event logs, system information and policy configuration according to your plan - Includes real-time automated ticketing and response based on detected policy changes and security issues, faults, and usage statistics.
	Proactive Service Desk (as per 10.21) - Unlimited number of service requests relating to your Microsoft 365 Business tenancy. - Proactive logging of detected service faults (we do it for you). - 3rd party vendor management (limited to Microsoft) including: - Licence & Contract management - Level 4 Vendor support escalations
	Incident and Problem Management (as per clause 10.22) - This service includes management of unplanned issues or degraded service experience or capability of the Microsoft 365 Business tenancy through an incident management process that includes: - Detection

	- Investigation - Diagnosis - Resolution - Recovery - End user support
	Monthly Service Reporting (as per clause 10.25) - Monthly service tickets and requests summary. - includes Microsoft telemetry data
Continuous Improvement *Process objective: To use methods from quality management to learn from past successes and failures.*	**Licence and Configuration Management (as per clause 10.26)** - Monthly reporting and tracking on ownership of licences and plans within the Microsoft 365 Business tenancy throughout the asset lifecycle (from procurement through to disposal). - Maintaining service-related information about the Microsoft 365 Business tenancy such as data volumes, licence usage and platform availability.
The Continual Service Improvement process aims to continually improve IT processes and services' effectiveness and efficiency, in line with the concept of continual improvement adopted in ISO 20000.	**Service Improvement (as per clause 10.27)** Continuous improvement activities such as identifying, performing, or recommending actions for the availability, reliability, and performance of the Microsoft 365 business tenancy.

Service Deliverables in detail

10.15 Telstra Managed Microsoft 365 is a proactive managed service and includes remote monitoring of incidents against our policy blueprint, alerting and incident management, as well as a proactive service desk that aims to maintain the performance and availability of your Microsoft 365 business tenancy with preventative activities.

10.16 The Service Desk will also respond to change requests, service alerts and troubleshoot issues within the Microsoft 365 Business tenancy on your behalf during service hours as outlined in section two of this document, including fault lodgement with the vendor when deemed necessary by our Level 3 support team.

10.17 The service includes the following Service Deliverables.

10.18 **Policy Configuration and Self-Healing**

(a) Your Microsoft 365 Business tenancy will be managed in accordance with current Microsoft policies using a Telstra managed Desired State Configuration policy blueprint. This blueprint will enable proactive management, automated ticketing, real time monitoring, and self-healing of your tenancy through our IT Service Management (‘**ITSM’**) platform (subject to available telemetric data).

(b) Should these policies within your tenancy be changed, we will reverse the changes, bringing your tenancy back to our desired state configuration ensuring a consistent and secure experience. Any existing policies we consider appropriate will continue to

remain unchanged (and unmanaged) and will not be affected by the Telstra policy blueprint.

(c) The below list is an example of some of the Microsoft 365 Policies which we will deploy and administer into Microsoft 365 tenancies. We will ensure these policies remain up to date in accordance with new service updates and feature releases from Microsoft.

Microsoft 365 Service Component	Deployment Inclusions & Deliverables			
	Specific Feature availability is based on your Microsoft 365 Business licence	Business Basic	Business Standard	Business Premium
Exchange Online	• Configure & deploy malware policy • Configure & deploy spam policy • Configure & deploy safe attachments policy • Configure & Deploy DMARC & DKIM policy • Append standard terms and conditions disclaimer to emails • Configure alerting rules to support	✓	✓	✓
Azure Active Directory	• Security groups created for permission management • Approval processes for consenting to apps which request access to company data • Remove the ability for Azure AD users to consent to apps they own • Enable multifactor authentications for all users • Enable app, phone, email, and SMS registration methods. • Enable self-password reset	✓	✓	✓
SharePoint Online	• Guest access to expire after 60 days • Enforcing MFA verification • Guests must use the same account for sign-ins	✓	✓	✓
Security & Compliance	• Enable unified auditing with 10-year retention • Configure & deploy safe links profile • Enable administrator auditing • Configure security alerts	✓	✓	✓
Microsoft Apps for Business	• Installation & Support of Microsoft Apps for Business on local devices.		✓	✓
Microsoft Endpoint Manager	• Support Microsoft Intune mobile device tenancy including MDM policies for "Bring your own device" including: - Compliance policy - Configuration policy - Update policy • User / Mobile Device enrolment • *Endpoint Manager support is for mobile Devices only. • *Only available to Microsoft Business Premium plan customers			✓
Microsoft Defender P1	• Enable minimum security policies available to Microsoft Defender P1, including - Advanced Anti-Phishing policy - SafeLinks email policy			✓

	- Safe Attachments policy - Enable Microsoft Defender Endpoint integration • *Only available to Microsoft Business Premium plan customers			

10.19 **Remote management setup, configuration, and Testing**

(a) This Service Deliverable includes the setup of the monitoring and alerting system as follows:

(i) the supply, configuration, and installation of monitoring tools or software agents within your Microsoft 365 Business tenancy as required by our ITSM tools to remotely monitor and manage your in-scope Microsoft 365 Business plans and licences;

(ii) documenting and updating service-related information about your Microsoft 365 Business tenancy, as well as configuration of our alerting system; and

(iii) includes validation of the monitoring tools and processes for your Microsoft 365 Business tenancy.

(b) We will implement or activate RMM tools, linking them to your specified Microsoft 365 Business tenancy. These tools may include admin access to your Microsoft 365 Business tenancy, its associated management portal and, if we determine it is needed, installation, installation of local software agents to allow increased visibility and control.

(c) Remote management and monitoring capabilities are subject to available telemetric and analytical data available from Microsoft. Available data will differ between tenancy, licence, and tenancy types.

10.20 **Monitoring and Alerting**

(a) Per clause 10.21, the Service Desk will perform active monitoring during your chosen support hours. This includes monitoring for alert events and common trends of your Microsoft 365 Business tenancy and lodging services tickets on your behalf for remediation. The Service Desk will also inform you of any impacts on your Microsoft 365 Business tenancy as required.

(b) This Service Deliverable includes the following:

(i) automated remote monitoring by our service delivery partner of your Microsoft 365 Business tenancy for availability, event logs, system information and performance counters – subject to plan and licence capability;

(ii) reports on performance-related critical threshold breaches, faults and usage statistics sent to you monthly;

(iii) using RMM tools, we will remotely collect and interpret real-time usage data and status messages, aggregating the data to our remote monitoring system or interface;

(iv) Usage data collected includes non-personal metrics such as data volumes, licence usage, availability, and uptime, as well as system logs and error codes

for diagnostic purposes where available. These metrics drive real-time alerts based on policy thresholds;

(v) we will track platform health and usage via our RMM system and keep records of these activities/fault tickets for the duration of your service. All collected data will be deleted on termination of the service (except for archival purposes or otherwise required by law);

(vi) we will systematically interpret the managed licence logs and associated performance events and metrics as inputs to performance reporting, alerting, and diagnostic tasks; and

(vii) we will maintain an ongoing record of your Microsoft 365 platform configuration in support of the licences under management in your Microsoft 365 Business tenancy.

(c) Remote management and monitoring capabilities are subject to available telemetric and analytical data from Microsoft. Available data will differ between tenancy, licence, and tenancy types.

(d) Diagnostic data does not include any identifiable internet traffic.

10.21 **Service Desk**

(a) The Service Desk will provide support during nominated support hours (via email & phone queues) for standard low risk and low-cost service requests. The Service Desk will also troubleshoot problems as raised through service tickets and actively monitor your Microsoft 365 Business tenancy in accordance with these terms. We will also provide proactive automated ticketing for issues within your Microsoft 365 Business tenancy based on our policy blueprint as per clause 10.18.

(b) All Service Requests reported to the Service Desk will be logged as a '**Service Ticket**' in our ITSM platform and will be the single source of truth for Service Ticket resolution.

(c) As part of Service Ticket resolution, the Service Desk will:

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

(ii) classify the Service Ticket as appropriate;

(iii) manage the Service Ticket until it is closed;

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

(v) advise you of the closure of the Service Ticket.

(d) When reporting a non-automated Service Ticket, you must provide the Service Desk with the following information:

(i) customer account number or account name and service number;

(ii) details of the relevant service request (for example, symptoms and degree of

impact);

(iii) impacted areas of your business;

(iv) contact details (including any premises contact details where on-site attendance may be required);

(v) outcome required; and

(vi) any other related information that you believe is pertinent.

(e) We will deliver Service Ticket resolution remotely unless attending on-site is a pre-requisite and included in our agreement with you. Where on-site attendance is required to resolve the Service Ticket, we will arrange a suitable time to attend the premises with you, which may incur an additional fee set our service delivery partner's discretion. This will be communicated to you with as much notice as is reasonably practical. We will not perform any billable activity without your confirmation and agreement to proceed.

(f) Where we reasonably believe a Service Ticket cannot be resolved or does not appear to arise from or relate to the in-scope services in your Managed Microsoft 365 service, we will promptly advise you and suggest alternative paths to resolution where possible before closing the Service Ticket.

(g) Non-standard requests are changes to the Microsoft 365 tenancy that require negotiation of timeframes to complete, due to size or complexity. These may be free of charge, or quoted separately as chargeable project work, which we can confirm. We will not perform any billable activity without your confirmation and agreement to proceed.

10.22 **Incident and Problem Management**

(a) This Service Deliverable aims to manage incidents to restore normal operation to your approved environment.

(b) If we classify a Service Ticket as an '**Incident'**, the Service Desk will determine a priority rating based on the Impact and Urgency matrix as listed in the table below:

		URGENCY		
		High	Medium	Low
IMPACT	High	Priority 1 - Critical	Priority 2 – High	Priority 3 - Medium
	Medium	Priority 2 - High	Priority 2 –High	Priority 3 - Medium
	Low	Priority 3 - Medium	Priority 3 – Medium	Priority 3 – Medium

(c) **Urgency**: We define Urgency as the necessary speed of restoration of service, based on available information, and it is classified as follows:

(i) **High**: No work can be performed, and your service is down at either a major

site or multiple sites.

(ii) **Medium**: Unable to perform some work tasks, but most business operations can continue.

(iii) **Low**: Information requests / low priority work tasks.

(d) **Impact**: We define Impact as the measure of how business-critical the Service Ticket is and is classified as follows:

(i) **High**: Entire approved environment inoperable across the total user population, causing a critical impact on your business operations.

(ii) **Medium**: Approved environment partially inoperable, and service is severely degraded, impacting significant aspects of business operations.

(iii) **Low**: Any degradation in service to approved environment.

(e) We will aim to respond to Service Tickets within the target response times ('**Response Times**') based on their priority ranking:

Priority	Response Times	Service Level
Priority 1	1 Business Hour	Assign a Service Ticket to at least 95% of Incidents and communicated to customer within response times
Priority 2	4 Business Hours	
Priority 3	8 Business Hours	

(f) For the duration of a **Priority 1 - Critical Incident** (see the **Impact and Urgency matrix** in clause 10.22(b)), we will provide a named incident manager or implement a matrixed incident resolution team responsible for restoring your services while keeping you informed of developments and expectations.

(g) Subject to clause 10.22(h), Response Times will be calculated from the time we receive your request of the Incident to the time we issue the Service Ticket to you.

(h) Response Times will be calculated within the Local Business Hours or the Extended Business Hours (as applicable).

(i) Unless a service level exclusion applies in clause 10.24, we aim to, but do not promise, to meet the Service Levels above and you are not entitled to any credit if we do not meet the Service Levels.

10.23 **Service Ticket priority and classification:**

(a) This Service Deliverable aims to manage the Service Requests of your Service.

(b) Service Requests may relate to remotely delivered services such as:

(i) Moves / Adds / Changes / Deletions (MACD)

(ii) Password changes

(iii) Requests for information in response to "How to" questions.

(c) If we classify your Service Ticket as a Service Request, it will be considered Priority 3 as described below by default unless we reasonably believe it should be a higher priority. The priority of a Service Request will be assessed on the Impact and Urgency Matrix defined in clause 10.22(b).

		URGENCY		
		High	Medium	Low
IMPACT	Low	Priority 3 – Low		

(d) We will aim to respond to Service Tickets within the target Response Times based on their priority ranking:

Priority	Target Response Times	Service Level
Priority 1	1 Business Hours	Assign a Service Ticket to at least 95% of Service Requests and communicated to customer within response times
Priority 2	4 Business Hours	
Priority 3	8 Business Hours	

(e) Subject to clause 10.23(f), Response Times will be calculated from the time we receive your Service Request to the time we issue the Service Ticket to you.

(f) Response Times will be calculated within the Local Business Hours or the Extended Business Hours (as applicable).

(g) Unless a service level exclusion applies in clause 10.24, we aim to, but do not promise, to meet the Service Levels above and you are not entitled to any credit if we do not meet the Service Levels.

10.24 **Service Level Exclusions**:

(a) The Response Time Service Levels will not apply, and we will not be responsible for a failure to meet a Service Level resulting from:

(i) a fault or failure of your Microsoft 365 service that is caused by you;

(ii) a failure by you to comply with the terms of our agreement with you for your Managed Microsoft 365 service;

(iii) any period of a scheduled maintenance;

(iv) any interference to you or your third party's services, infrastructure, equipment, software (including operating or email systems), configurations or

other technology that support your tenancy that is out of our direct control;

(v) any unauthorised changes made by you or a third party to your technology infrastructure, software or configurations that support your Microsoft 365 service; and

(vi) suspension or termination of your right to use or access your Microsoft 365 services.

10.25 **Monthly Service Reporting**

(a) Automated reporting will be set up on your Microsoft 365 Business tenancy. This will remotely collect and store data via our ITSM tools.

(b) Our team will use this data to report on your standard usage, which will be sent via a monthly email to your nominated email account.

(c) This Service Deliverable includes a standard monthly emailed report and will include information on:

(i) metrics on plans and licences under management within your tenancy, and notification of any changes in the last month;

(ii) users and user activity;

(iii) risky events;

(iv) storage quota;

(v) service history including but not limited to:

(A) Service Tickets: details of recent service tickets associated with your managed services, including those raised by your team and those proactively triggered by monitoring events such as outages or logged on your behalf by us;

(B) Availability: the availability of your Microsoft 365 plans and licences, detected between the internet and our monitoring systems as measured during the reporting period; and

(C) changes made to desired state configuration policy blueprint

(d) Reporting capabilities will vary by plan and licence type. Wherever possible, we will endeavour to provide additional reporting, subject to data availability.

10.26 **Licence and Configuration Management**

(a) This Service Deliverable is about maintaining and updating a record of service-related information about the specific users and licences under management in the Microsoft 365 Business tenancy and includes:

(i) monitoring and maintaining a record of the specified plans and licences under management's current software version and details of changes over time as

performed;

(ii) maintaining a record of configuration information on the Microsoft 365 tenancy and other customer relevant or service management related data, including:

(A) managed licence type;

(B) authorised customer contacts;

(C) active user details per managed licence;

(D) admin passwords per managed licence;

(E) maintaining licence management console and vendor information as needed to deliver ongoing Managed Microsoft 365 services; and

(F) tracking the ownership, purchase dates and age of licences in your Microsoft 365 Business tenancy throughout the asset lifecycle (from procurement through to disposal).

10.27 **Service improvement**

(a) This Service Deliverable is the delivery of improvement activities identified through ongoing remote monitoring and management and analysis of past service management activities. It also includes analysis of problems, Incidents, and Service Tickets. These are used to identify, implement, or recommend actions or changes needed for improvement to the availability, reliability, and performance of the Microsoft 365 plans and/or standalone licences in your Microsoft 365 Business tenancy. The Service Deliverable includes:

(i) proactive problem avoidance activities may include logging faults with 3rd parties, such as Telstra, or the software vendor if required, and managing the fault ticket to resolution;

(ii) any service improvement activities that will materially and detrimentally impact your staff, business operations or require investment will be explicitly agreed upon with you before commencement; and

(iii) progress updates to your nominated contact.

What is not included?

10.28 The Managed Microsoft 365 service does not include:

(a) the Microsoft 365 software plan/licence costs and is only available to Microsoft licences listed within these terms. If you have Enterprise plans within your tenancy, the Business Premium inclusions will be provided for those plans;

(b) initial setup of new Microsoft 365 licences. Please refer to the Telstra Install – Microsoft 365 service (as set out in clause 9 of these terms] for assistance with deployment of new Microsoft 365 tenancies, plans and licences;

(c) Software functionality support and training is not included and will incur further costs.

User supported is limited to the software packages set out in these terms. Support of any additional features, functions, or applications outside the Microsoft 365 platform will be at our discretion. The Managed Microsoft 365 service does not include hardware or device supply and installation, cabling, or any other underlying requirements, equipment or infrastructure installation unless explicitly specified in these terms or your Application Form;

(d) management or administration of any software outside the Microsoft 365 Business tenancy not set out in these terms.

(e) work outside standard packages: Additional hours of work required above the relevant packaged inclusions and to meet your specific requirements (e.g. project work) is not included. Separate charges will apply;

(f) support for on-premises deployments of Microsoft 365 in any form. The Managed Microsoft 365 service is suitable for Microsoft 365 cloud services only;

(g) site visits: the Managed Microsoft 365 service is remotely delivered. Any site visits must be agreed with our service delivery partner, and additional charges may apply;

(h) management of Cloud based PABX systems like Telstra Calling for Office 365;

(i) any warranties or guarantees regarding uptime. The Managed Microsoft 365 service and associated inclusions are not an insurance service and do not imply or include any warranty or guarantees regarding service uptime;

(j) any service outages or downtime caused by issues within the Microsoft platform (outside your direct tenancy). This is out of our control and falls outside the scope of the Managed Microsoft 365 service;

(k) troubleshooting, support, and resolution activities for associated ICT components impacting the Microsoft 365 software and application experience. We may (but are not required to) agree to perform such activities for additional charges. The Managed Microsoft 365 service is limited to the administration, management and support of the Microsoft 365 platform including Microsoft 365 Business plans and their associated applications as listed in clause 10.7 of these terms;

(l) website management; and

(m) any other item or work not explicitly described in these terms as being part of the Managed Microsoft 365 service, is not included as part of that service.

Our Responsibilities

10.29 The following are our responsibilities in the delivery of the Managed Microsoft 365 service offering:

(a) Our service delivery partner will collaborate with you to schedule the Managed Microsoft 365 service's initial configuration and set the agenda for required workshops or meetings;

(b) we will complete the Service Deliverables detailed under “Service Deliverables Table”

in clause 10.14;

(c) we will provide support within the support boundary, being the specified Microsoft 365 Business licences and plans within your active production Microsoft 365 Business tenancy;

(d) we will have access to an email alerting capable RMM tool or portal. Our system will generate alerts based on data as received from your tenancy, with default service thresholds pre-defined for specific monitored elements. Examples of alerts may include usage, availability, and other performance statistics. The range of available data to drive monitoring and alerting based services will vary between different Microsoft 365 plans and licences;

(e) we will keep best practice policies updated, and rollout any feature updates released by the vendor as per included licence types and active subscriptions;

(f) before we perform any service outside standard included Service Deliverables, we will provide a quotation for the non-standard services for your confirmation and acceptance;

(g) we reserve the right to reverse any change requests we feel fall outside our fair use policies available on our website;

(h) any other Telstra responsibilities set out in these terms or your Application Form.

Your Responsibilities

10.30 To receive the Managed Microsoft 365 service and access the Service Deliverables described above, you must:

(a) Pre-service checklist: complete the Managed Microsoft 365 Pre-Service Checklist we provide to you. This checklist will need to be signed off before the Managed Microsoft 365 service commences confirming your requirements and defining the managed licences within your Microsoft 365 Business tenancy. Reporting contacts must be provided, including confirmation of reporting frequency, and named contacts and email addresses for reports;

(b) Participation: ensure that the appropriate business owners and technical staff can attend or participate in our scheduled meetings or workshops as needed for us to perform the Managed Microsoft 365 service.

(c) Accurate IT information: provide accurate high-level detail on your internal IT services and strategy to the us. Please note that the Managed Microsoft 365 service and the Managed Microsoft 365 configuration and service design will be based on the information you provide to us and that we extract from your operating environment with remote tools. We will assume all the information you provide is up to date and valid for your tenancy.

(d) Licencing: hold an active, valid Microsoft 365 tenancy with paid subscriptions for licences for us to deliver the Managed Microsoft 365, which must be obtained under a separate agreement, either through Telstra or Microsoft. It is your responsibility to ensure that your Microsoft 356 tenancy is appropriately licenced;

(e) Access to systems: make sure and assist in providing us with appropriate administration credentials and remote access to the Microsoft 365 Business tenancy and management, so that we can administer and manage the tenancy on your behalf as per clauses 10.18 - 10.27. Administrator access to the Microsoft 365 tenancy will be restricted to Telstra and vendor parties only, to maintain service responsibility integrity;

(f) Usage of your Internet connectivity: 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 Managed Microsoft 365 service (including obtaining any required consents or approvals and opening required network ports);

(g) sign, date, and return a Customer Acceptance Certificate ('**CAC**') we issue to you (once the Managed Microsoft 365 service has been deployed and tested as working); and

(h) any other responsibilities set out in these terms or your Application Form, or reasonably requested by us to perform our obligations in respect of your Managed Microsoft 365 service.

10.31 Our ability to complete our ongoing service delivery obligations depends on you promptly providing the items and information outlined above. If you do not comply with your obligations in clause 10.30 above, or if we incur costs due to your negligence, fault, act, or omission, you may incur extra charges or alteration to your billing cycle for the Managed Microsoft 365 service as a result.

Invoicing

10.32 The Managed Microsoft 365 service is offered as a month-to-month service, calculated daily. Service usage data will be collected from the policy deployment date, based on daily usage rates for user assigned licences within the applicable Microsoft 365 Business tenancy. Fees will be billed monthly in arrears until expiration or termination of your agreement with us for your Managed Microsoft 365 service (whichever is earlier).

Service Pricing

10.33 Charges for the Managed Microsoft 365 service are set out in your Application Form and in the Managed Microsoft 365 Critical Information Summary, a copy of which will be provided to you. We may update these charges from time to time and notify you of any changes to service pricing. If any changes are made to the pricing after you have taken up the service and those price changes apply to your Managed Microsoft 365 service and have more than a minor detrimental impact on you in relation to that service, you may terminate your Managed Microsoft 365 service by written notice to us without having to pay any early termination charges for that service.

10.34 The Managed Microsoft 365 service will be matched to your Microsoft 365 Business tenancy, and any changes (e.g., additions, cancellations, upgrades, downgrades) made to the underlying Microsoft licences will be automatically reflected in the amount we charge you for your service.

10.35 Charges will only apply to active licences that have a user assigned.

Location of services

10.36 All packages are delivered remotely.

10.37 Additional fees will apply if on-site visits are requested.

Software and Licence Eligibility

10.38 The Managed Microsoft 365 service is available only for current compatible Microsoft 365 Business cloud licences, purchased through Telstra, Microsoft, or an authorised third party cloud service provider.

Early termination and other charges

10.39 You may cancel your Managed Microsoft 365 service at any time before we start to work on your instructions. You may cancel at any time before we commence work on setting up your Managed Microsoft 365 service.

Other fees

10.40 As per 10.28, any work outside the Service Deliverables will incur extra costs. Examples of these are on-site visits, new tenancy setup, data migrations, SharePoint site creation, and new licence installations.

10.41 Any additional services costs considered as non-standard service requests will be communicated to, and agreed by you, before we commence work.

Special meanings

10.42 In this clause 10, the following words have the following meanings:

Customer Acceptance Certificate or **CAC** means the document you must sign upon completion of the relevant Service Deliverables, as contemplated in clause 10.30(g).

Extended Business Hours has the meaning given to it in clause 10.12(a).

Incident means a Service Ticket that we classify as an Incident, as contemplated in clause 10.22(b).

Impact has the meaning given to it in clause 10.22(d).

ITSM has the meaning given to it in clause 10.18(a).

Local Business Hours has the meaning given to it in clause 10.11(a).

Response Times has the meaning given to it in clause 10.22(e).

RMM means remote monitoring and management.

Service Deliverables has the meaning given to it in clause 10.14.

Service Desk means the service desk as described in clause 10.15.

Service Level means the service levels set out in clauses 10.22(e) and 10.23(d).

Service Request means a Service Ticket that we classify as a Service Request, as contemplated in clause 10.23(c).

Service Ticket has the meaning given to it in clause 10.21(b).

Urgency has the meaning given to it in clause 10.22(c).

11 MANAGED CYBER SECURITY – CHECK POINT HARMONY

Service Summary

11.1 Telstra's Managed Cyber Security – Check Point Harmony ("Managed Service") provides ongoing support and management of Check Point Harmony cyber security products (Endpoint, Mobile and Email & Collaboration), subscribed by you through Telstra. This may include service management, adds, moves and changes, policy, service or client updates, reporting and other features as available on the product or service under management, and agreed to with us.

11.2 The Managed Service is suitable for administering cyber security protection for devices and platforms, ongoing maintenance and security alerts, and the creation of policies to suit the needs of the business. Products and services are remotely administered and monitored utilising our remote monitoring tools to help understand and or mitigate the impact of any potential business risks as they occur.

11.3 The Managed Service offers a core management service and a choice of service desk hours for management. Supply and installation of the underlying product licencing, including establishing any administration portal for the product, is excluded from this Service; however, it is available separately.

11.4 As the Managed Service is delivered remotely, management access of any administration portal for the cyber security product must be delegated to our personnel.

What is included?

11.5 Products Managed as part of this service

(a) The Managed Service is dependent on Telstra provided Check Point Harmony subscriptions (Endpoint, Mobile and Email & Collaboration) which are sold separately.

(b) Telstra will administer and manage, and provide user support for each of these licences, as per Check Point's standards and policies. Management will be provided at a tenancy level, and across the whole licence environment. *Installation and deployment of new Check Point Harmony tenancies is excluded from this service and is available separately.

(c) The following table details the features delivered as part of each product.

Feature	Endpoint	Mobile	Email & Collaboration

Anti-Phishing for incoming and internal emails	✔	✔	✔	
Malicious URL prevention (URL Protection)	✔	✔	✔	✔
Device and OS Protection – Protects devices with real-time risk assessments detecting attacks, vulnerabilities, configuration changes, and advanced rooting and jailbreaking		✔		
On Device Network Protection - Anti-Bot: Detects and blocks bot-infected devices, allows control of DNS preferences, protects end-users privacy, prevents MiTM attacks	✔	✔		
URL Click-Time Protection (URL Re-writing)			✔	
Account takeover prevention (Anomalies)			✔	
Unauthorized applications detection (Shadow IT)			✔	
Known malware prevention (Anti-Virus)	✔	✔	✔	✔
Complete zero-day malware prevention (Sandboxing)	✔	✔	✔	✔
Attachment sanitization (CDR, Threat Extraction)	✔		✔	
Reduce Attack Surface: Endpoint Firewall, Application Control, Compliance, Port Protection, VPN	✔			
Attacks Prevention: AV, Static Analysis, File Reputation, NGAV, Anti-Malware	✔			
Secure Internet Browsing: Zero Phishing, Corporate password reuse protection, URL Filtering, SSL Visibility, Malicious site protection	✔	✔		
Continues Protection: Anti-Ransomware, Behavioral Guard, Anti-Bot, Anti-Exploit	✔			
Threat Intelligence: Powered by ThreatCloud™, Automated IoC and IoA cloud sharing	✔	✔		
Content Disarm & Reconstruction (CDR): Threat Emulation (Sandbox), Threat Extraction	✔			

11.6 Support levels

(a) We (through our personnel and Managed Service Providers (MSP)) will deliver the Managed Service to you in accordance with this Agreement and description

(b) The Managed Service is available in a proactive service management tier and priced according to the volume of Check Point Harmony licences , as specified in the

Managed Cyber Security - Check Point Harmony – Critical Information Summary.

(c) Service Desk support hours is by default Business hours only.

- **Business Hours** means the hours between 8:30 AM to 5 PM, Monday to Friday, excluding public holidays at the relevant site

(d) Extended Business Hours may be selected, if made available our MSP, as an add-on and is applicable for all services under the Managed Service:

(i) **Add-on: Extended Business Hours** (means the hours between 8:30 AM to 8 PM, Monday to Friday + Saturday 9 AM to 12 PM, excluding public holidays at the relevant site)

(e) All Managed Service elements will be billed as separate line items. The service is offered as a monthly fee, with a fee due monthly, billed in arrears. The services and contract terms for the Managed Service will automatically continue on a month-to-month basis under the existing terms and conditions, including price. For any changes to the terms and conditions, including price, we will provide you with at least 30 days' notice.

(f) Any administration portal that is required to administer the cyber security services will be restricted to read-only access for customers while under Managed Service. If the Managed Service is terminated at any point by us or the customer, administrator access will be transferred back to the customer.

Service Deliverables table

11.7 The following table summarises the service deliverables available for each feature package. More detailed descriptions of the various deliverables are included in the following pages.

Item	Deliverable
Transition Service *Process Objective:* *To implement ITSM services.* *Transition services help make sure that changes to services and Service Management processes are carried out in a coordinated way.*	Remote management setup, configuration, and testing • This service includes the setup of the monitoring and alerting system for Check Point Harmony services • Documenting and updating information about your services Alert configuration and testing. • Remote monitoring validation.
Service Operation	Monitoring & Alerting[1]

Process Objective: *To help make sure that the IT services are delivered effectively and efficiently.* *The Service Operation process includes fulfilling user requests, resolving service failures, fixing problems, and carrying out routine operational tasks.*	• This service includes automated remote monitoring of the device protection for Cyber Security incidents, offline devices, event logs and system information – subject to capability of device, endpoint or platform. • Includes real-time email alerts to you based on security related critical incidents, faults and usage statistics.
	Proactive Service Desk • Unlimited number of requests • Proactive logging of service faults (we do it for you) • Access Management • 3rd Party management (interacting with 3rd party vendors) incl. escalation to vendor where required.

	Incident and Problem Management
	
	• Management of Incidents and Problems that impact the effective operation of the Check Point Harmony software in providing Cyber Protection for the devices and/or applications on which it is installed
	• Management of Incidents and Problems where the service detects a cyber security incident that requires action by the customer. This will include the management of the Cyber Security through an incident management process that includes:
	  ○ Detection
	  ○ Investigation
	  ○ Diagnosis
	  ○ Communication with the customer of any urgent action required to alleviate a Cyber risk associated with the Incident or Problem.

	Monthly Service Reporting • Monthly service tickets and requests summary • Standard reporting as supported by the device (reporting capability varies per device model)
Continuous Improvement	Service Asset & Configuration Management • Tracking and reporting on active licences and historic security events.

Process Objective: To use methods from quality management to learn from past successes and failures. *The Continual Service Improvement process aims to continually improve IT processes and services' effectiveness and efficiency, in line with the concept of continual improvement adopted in ISO 20000.*	• Updating and enhancing security policies based on your requests or based on best practice.
	Client software updates • This service includes management monitoring of devices to ensure they're running the minimum client version of Check Point Harmony Email & Collaboration, Mobile and Endpoint, as recommended by the vendor. • As the minimum client version is increased by the vendor, automatic updates should ensure devices are updated within an client updates based on the minimum recommended client version. • Also includes alerting of when minimum client versions are not maintained by end users.
	Service Improvement Continuous improvement activities include identifying, performing, or recommending actions for the security of the managed devices, SaaS environment or products.

Note - In-scope Check Point services under management are specified in a **Pre Service Checklist**, which will form part of this Agreement.

Service Deliverables in detail

11.8 This is a proactive managed service that includes remote monitoring, alerting, incident management, and a proactive service desk that aims to maintain the security of device or SaaS environment security through preventative activities. Also, the Service Desk will respond to change requests, service alerts and troubleshoot security alerts on your behalf during service hours, including escalation to the relevant vendor where required.

11.9 The service includes the following Service Deliverables:

11.10 Remote management setup, configuration, and testing. This service deliverable consists of the following transition processes:

(a) Setting up and confirming our access to the relevant administration portal to ensure we can remotely monitor and maintain administration of your services.

(b) Includes the configuration of monitoring tools or needed software agents by which our IT Service Management (ITSM) tools can remotely monitor and manage your in-scope services.

(c) Documenting and updating information about your services, as well as configuration of alerting and knowledge articles for your environment including how to access the Check Point Harmony read only portal.

(d) Includes validation of the monitoring tools and processes for your Approved

Environment

11.11 We will implement or activate relevant Remote Monitoring and Management (RMM) tools, linking them to administration portal for the cyber security product. This will include maintaining administrator access to the portal and restricting any access you have to read-only.

11.12 **Monitoring and Alerting:**

(a) During nominated support hours, the Service Desk will perform active monitoring for alert events and trends of your services and proactively lodge needed service tickets on your behalf for remediation and management to resolution and inform you of any impacts as required.

(b) This service deliverable includes:

(i) Automated remote monitoring by the Telstra Business Technology Centre of your Telstra provided Check Point Harmony Endpoint, Mobile and Email & Collaboration services

(ii) Monthly emailed reports to you based on performance-related critical threshold breaches, faults and usage statistics.

(iii) Aggregating the data to our remote monitoring system or interface

(iv) We will systematically interpret the managed licence logs and associated performance events and metrics as inputs to performance reporting, alerting, and diagnostic tasks tickets on your behalf for remediation and management to resolution and inform you of any impacts as required.

11.13 **Proactive Service Desk**

11.14 The Service desk will provide priority support during nominated support hours (via email & phone queues) for standard low risk, low-cost service requests, troubleshoot problems raised by you as service tickets and monitor your devices remotely.

11.15 All Service Requests reported to the TBTC Service Desk will be logged as a Service Ticket in Telstra's ITSM platform and will be the single source of truth for Service Ticket resolution.

11.16 As part of Service Ticket resolution, the Service Desk will:

(i) Log and provide a Service Ticket reference number for the Service Ticket

(ii) Classify the Service Ticket as defined in Incident and Problem Management (below)

(iii) Manage the Service Ticket until it is closed

(iv) Provide regular status updates for the Service Ticket

(b) Advise you of the closure of the Service Ticket.

11.17 When reporting the Service Ticket, you must provide the Service Desk with the following information:

(a) Customer account number / account name and service number

(b) Details of the Service Request (for example, symptoms and degree of impact)

(c) Impacted areas of your business

(d) Contact details (including any premises contact details where on-site attendance may be required)

(e) Outcome required

(f) Any other related information that you believe is pertinent.

11.18 We will deliver Service Ticket resolution remotely unless attending on-site is a pre-requisite and included in the product service agreement. Where on-site attendance is required to resolve the Service Ticket, we will arrange a suitable time to attend the premises with you (which may incur an additional fee and be communicated to you with the most notice possible).

11.19 Where we reasonably believe the Service Ticket does not appear to arise from or relate to the in-scope services, we will promptly advise you.

11.20 If we reasonably believe the Service Ticket cannot be resolved, we will communicate why we believe the Service Ticket cannot be resolved

11.21 **Incident and Problem Management**

(a) This service deliverable aims to restore normal operation and/or resolve a cyber security incident.

(b) This service includes the management of cyber security incidents and alerts as detected by any services that we manage through an incident management process that includes:

(i) Detection

(ii) Investigation

(iii) Diagnosis

(c) Communication with the customer of any urgent action required to alleviate a Cyber risk associated with the Incident or Problem

(d) For the duration of a **Priority 1-Urgent incident** (see the **Incident Priority matrix** below), we will provide a named incident manager or implement a matrixed incident resolution team responsible for restoring your services while keeping you informed of

developments and expectations.

(e) Service Ticket priority and classification:

(i) The Service Desk will classify and prioritise support requests when logged using a combination of "Urgency" and "Impact" (both defined below) to determine the incident and ticket "Priority", which determines the sequence in which the MSP works on multiple issues.

(ii) Urgency: We define urgency as the necessary speed of restoration of service and is classified as follows:

(A) **High**: No work can be performed /time-sensitive/remedial activity to the Approved Environment can prevent a major incident

(B) **Medium**: Unable to perform some work tasks / multiple users affected

(C) **Low**: Information request / low priority or simple work tasks

(iii) The Service Desk will choose an appropriate Urgency category to assign to the ticket.

(iv) Impact: We define impact as the measure of how business-critical the incident impact is, classified as follows:

(A) **High**: All in-scope technology (Approved Environment) delivered functions are inoperable across the total user population, severe business impact

(B) **Medium**: Some in-scope technology (Approved Environment) delivered functions inoperable, modest business impact, during business hours

(C) **Low**: Any degradation in service from in-scope technology (Approved Environment), single-user impact

(v) Our Response to Service Tickets: We will aim to respond to Service Tickets within the target response times (Response Times) based on their priority ranking.

(vi) The Service Desk will choose an appropriate Impact category to assign to the ticket

Priority	Response times	Service level
Priority 1	1 Business Hours	Assign a Service Ticket to at least 95% of Incidents and communicated to customer within response times
Priority 2	4 Business Hours	

Priority 3	8 Business Hours	

(A) For the duration of a Priority 1 - Critical Incident, we will provide a named incident manager or implement a matrixed incident resolution team responsible for restoring your services while keeping you informed of developments and expectations

(B) Subject to our Service Ticket priority and classification above, Response Times will be calculated from the time we receive your request of the Incident to the time we issue the Service Ticket to you

(C) Response Times will be calculated within the Local Business Hours or the Extended Business Hours (as applicable)

(D) Unless a service level exclusion applies, we aim to, but do not promise, to meet the Service Levels above and you are not entitled to any credit if we do not meet the Service Levels.

(vii) Service Ticket Incident Priority matrix

(A) We will use the **Incident Priority matrix** below to define the incident priority based on the above urgency and impact classifications

(B) In the case of incidents, we strive to resolve the incident according to the following defined priorities:

Incident Priority / Severity		**Impact**		
		High	**Medium**	**Low**
Urgency	High	Priority 1 – High	Priority 2 - Medium	Priority 3 - Low
	Medium	Priority 2 - Medium	Priority 2 - Medium	Priority 3 - Low
	Low	Priority 3 - Low	Priority 3 - Low	Priority 3 - Low

(f) Service Level Exclusions

(i) The Response Time Service Levels will not apply, and we will not be responsible for a failure to meet a Service level resulting from:

(A) a fault or failure of your Service that is caused by you.

(B) a failure by you to comply with the terms of this Agreement;

(C) any period of a scheduled maintenance.

(D) any interference to you or your third party's services, infrastructure, equipment, software (including operating or email systems), configurations or other technology that support your environment that is out of our direct control;

(E) any unauthorised changes made by you or a third party to your technology infrastructure, software or configurations that support the Services; and

(F) suspension or termination of your right to use or access the Services

11.22 **Service requests:**

(a) Service requests may relate to deploying a new service, creating a new policy, modifying existing policies, Moves/Adds/Changes (MAC), or requests for information in response to "How to" questions.

(b) **Standard pre-approved service requests** apply to the services that we manage only. They may include "How to questions" relating to installations or deletions, Moves/Adds/Changes (MAC) or requests for information.

(c) If we classify your Service Ticket as a Service Request, it will be considered Priority 3 as described above by default unless we reasonably believe it should be a higher priority. The priority of a Service Request will be assessed on the Impact and Urgency as defined above.

(d) ***Note: Non-standard requests*** *are changes to the services that require negotiation of timeframes to complete, due to size or complexity. These may be free of charge (FOC) or quoted separately as a chargeable "change request", which we can confirm. We will not perform any billable activity without your explicit consent.*

11.23 **Monthly Service Reporting**

(a) Automated reporting will be set up on the services and events data will be remotely collected and stored via our ITSM tools. Our team will use this data to create and issue standard usage reporting, sent via a monthly email to your nominated email account.

(b) This service deliverable includes a standard monthly emailed report and will include:

(i) Licences/devices in use, including variations, quantities and changes.

(ii) Service Tickets History: details of recent service tickets associated with your

managed services, including those raised by your team and those proactively triggered by monitoring events such as security events or logged on your behalf by us.

(iii) Service Events History: details of events that occur on product technologies managed as part of your service.

(c) The following table illustrates the events that are monitored, their priority, and which events automatically raise a Service Ticket for investigation, and which are included in monthly reporting.

Service	Events	Description	Priority	Included in reporting	Automatically raises a ticket
Harmony Mobile	Application	Application which are on Risk, Removed, Installed, Noncompliant	Critical	✔	✔
	WIFi Network	Event and Threat found on Cellular network	Critical	✔	✔
	Network Security	Capital Portal Redirection, Botnets, Phishing, Spyware/Malicious sites	Critical	✔	✔
	OS Exploits	Malicious apps which use and exploit the OS vulnerability	Critical	✔	✔
	Device	Malicious text or links which use and exploit the OS vulnerability	Critical	✔	✔
	File	Malicious or unknown file downloaded	Critical	✔	✔
	IOS profiles	Maliciious threats using iOS profiles as the attack vector	High	✔	
Harmony Endpoint	Anti-Malware	Malware (short for "malicious software") is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behaviour an attacker wants.	High	✔	✔
	Anti-Ransomware	Ransomware is a type of malware designed to extort money from its victims, who are blocked or prevented from accessing data on their systems.	High	✔	✔
	Forensics	Harmony Endpoint Forensics analyses attacks detected by other detection features like Anti-Ransomware or Behavioural Guard, the Check Point Gateway and some third-party security products. On detection of a malicious event or file, Forensics is informed, and a Forensics analysis is automatically initiated. After the analysis is completed, the entire attack sequence is then presented as a Forensics Analysis Report	High	✔	✔
	Anti exploit	An anti-exploitation feature provides protection against exploits in a broad, generic manner. This is in contrast to antivirus or signature-based detection, which looks for known-bad pieces of code or malicious files. An example of an anti-exploitation feature is Data Execution Prevention (DEP), which stops an exploit by disrupting	High	✔	✔

		the methods by which an attacker can inject code into a running program			
	Threat extraction	Threat Extraction proactively protects against known and unknown threats contained in documents by removing exploitable content. This method is also known as file sanitization or CDR (content disarm and reconstruction	High	✔	✔
	Threat Emulation	Threat Emulation Appliance with inline deployment - The files are kept in the Threat Emulation appliance and after emulation, safe files go to the computer in the internal network.	High	✔	✔
	Zero Phishing	Phishing on Endpoint covers below: • Real-time protection from unknown phishing sites • Static and heuristic-based detection of suspicious elements across websites requesting private inf	High	✔	✔
	Behavioral Guard	Constantly monitoring of files and network activity for suspicious behavior.	High	✔	
	URL Filtering	A URL that the customer has identified as requiring to be blocked before entering the customer's network	High	✔	
	HTTPS Inspection	Detection of malicious content within HTTPS traffic.	High	✔	
	Firewall	When a security event is detected by the Endpoint firewall	High	✔	
	Anti-bot	Check Point Software Blade on a Security Gateway that blocks botnet behaviour and communication to Command and Control (C&C) centres. Acronyms: AB, ABOT.	High	✔	✔
Harmony Email and Collaboration	Threat Emulation	A malicious file attachment detected (in email, on cloud drive, in Teams msgs, etc...)	High	✔	✔
	Anti-Phishing	Phishing attempt detected in an email or msg (email is delivered but there is a warning) this really depends in the workflow defined in the policy (e.g. detect mode vs block mode)	High	✔	✔
	Compromised Accounts	Anomalies detected in the behaviour of an internal users (suspicious for Account take over) – for example sending phishing from employees' internal email or when the system see I logged in from one location then from other one (impossible travel situation) or I logged in from another device that is not recognized or that is using a different language then what I have	High	✔	✔
	Anti-Spam	Remediation of an email that has been identified as spam	High	✔	
	Click-Time Protection	Click-Time Protection allows to add exceptions to domains and URLs that need to be blocked, allowed, or ignored regardless of being malicious or not. Alerts when a user clicks on a link that is not permitted	medium	✔	

(d) *Reporting capabilities will vary based on data available from the underlying product technology. We will always endeavour to provide as much information as possible. Refer to the Appendices for the details of the reporting that will be made available with each product technology provided as part of your service.*

11.24 **Service Asset and Configuration Management**

(a) This service deliverable is about maintaining and updating a record of information about the licenses under management and includes:

(i) Monitor and maintain a record of the licences under management – including current licence type and details of security events over time.

(ii) Maintain information about the current security policies and best practices for the environment.

(b) Software updates

(i) This service deliverable includes any required updates to software where required to maintain a service. It is the process of ensuring any required minimum version of software is defined, ensuring any client updates are automated (as available) and monitoring all devices or SaaS environment for compliance with the defined minimum versions. This includes:

(A) Monitoring the latest client versions as they become available from any service under management, in line with our and any vendor's latest recommended version advice.

(B) Ensuring the minimum client version, as recommended by a vendor and us, is correctly applied in administration portals.

(C) Monitoring all devices and SaaS environments under management to ensure compliance with the minimum versions and alerting you when devices are not running the minimum version within an agreed threshold (e.g., within three days of release).

(c) Remote installation and deployment of client updates are not included. Any remote or onsite support for installing or updating the client version will be chargeable based on rates set out in Managed Cyber Security - Check Point Harmony – Critical Information Summary**.**

11.25 **Service improvement**

(a) This service deliverable is the delivery of improvement activities identified through ongoing remote monitoring and management and analysis of past service management activities, as well as analysis of problems, incidents and service tickets to identify, implement or recommend actions or changes needed for improvement to the security of the devices and the service provided.

(b) This may include updating, altering or enhancing the security policy based on improvements to best practice, updated features from the vendor, or specific recommendations from our Security experts.

(c) Telstra reserves the right to replace the underpinning tools or technology at any time to continue to offer device, software and endpoint protection with an alternate

vendor. This would only occur following significant notification and consultation with you and would not incur additional costs.

What is not included?

11.26 Activation of any software licences acquired from Telstra Apps Marketplace, and initial establishment of the cyber security service for the business. (This is available separately.)

11.27 Deployment of initial licences to any endpoints, devices, SaaS environments or any other platform – this is available separately as a professional installation service from Telstra

11.28 Management of any cyber security licences or products that are not purchased from Telstra Apps Marketplace.

11.29 Support for changes made to devices or platforms under management by 3rd parties, such as your IT department or other providers.

11.30 Work outside standard packages: Additional work, including out-of-hours work, is not included in the package Service Deliverables.

11.31 Site visits – additional fees will apply if any onsite visits are required (see below).

Other exclusions and notes

11.32 Before we perform any service outside standard included Service Deliverables for a management service, we will provide a quotation for the non-standard services for your confirmation.

11.33 The Managed Service and associated inclusions are not an insurance service and do not imply warranty or guarantees regarding service uptime or protection from cyber intrusions.

11.34 Any other item or work not explicitly described in this Service Schedule as being part of the Managed Service is not included as part of the service.

Our Responsibilities

11.35 The following are our responsibilities in the delivery of the Managed Service:

(a) Collaborate with you to schedule the Managed Service's initial configuration and set the agenda for required workshops or meetings.

(b) Complete the service deliverables detailed under 'What is Included'.

(c) **Support boundaries**: This Managed Service's support boundary is defined as the specified devices or SaaS environments, or other platforms only as defined in the **Pre-Service Checklist**

(d) We will work with our preferred service delivery partners to deliver this service to you.

(e) Our service provider will have access to a RMM tool (remote monitoring and management) or portal. This system will generate alerts based on data as received from your devices, endpoints or platforms, with default service thresholds pre-defined for specific monitored elements.

(f) Any other responsibilities agreed under this Agreement.

Your Responsibilities

11.36 To receive the Managed Service service and access the service deliverables described above, you must promptly complete the following:

(a) Complete the **Pre-Service Checklist**. This checklist will need to be signed off before services commence confirming your requirements and defining the devices, SaaS environments or other platforms. Reporting contacts must be provided, including confirmation of reporting frequency and named customer contacts and email addresses for reports.

(b) Participation: Ensure that the appropriate business owners and technical staff can attend or participate in our scheduled meetings or workshops as needed for us to implement the Managed Service.

(c) Accurate information: Provide accurate detail on your devices, SaaS environments, device and other platforms. Please note that the Managed Service configuration and service design will be based on the information you provide to us. We'll assume all the information you provide is up to date and valid for your environment.

(d) Licencing: All required licencing is to be purchased and correctly set up in your business's name. It is your responsibility to ensure that your devices, SaaS environments or other platforms are appropriately licenced including in line with any advice we provide. Check Point Harmony licencing must be purchased through the Telstra Apps Marketplace (TAM).

(e) Installation / establishment: Any administration portal or initial service establishment must be in place, with all licences and devices correctly set up. This can either be undertaken by yourself, a representative of your business, or by Telstra through our Install service, available separately.

(f) Access to systems: Assist in providing us with appropriate administration credentials and remote access to any administration portals so that we can configure and activate the service and deliver the ongoing remote monitoring and service management as required. Administrator access any administration portal will be restricted to agreed parties only to maintain service responsibility and integrity – this will generally be our MSP and Telstra's Security team (for any escalations). Access to any administration portal for you will be restricted to read-only while under this Managed Services agreement.

(g) Usage of your Internet connectivity: You must ensure that your business Internet

connectivity, including any mobile or other platform Internet connectivity, are working to allow the services to function correctly at all times within your control.

(h) Comply with the TBS Standard Terms for Small Business Professional Services Fixed Packages.

(i) Our ability to complete our ongoing service delivery obligations depends on you promptly providing the items and information outlined above – otherwise, you may incur extra charges or alterations to billing milestones for this service.

(j) Sign, date, and return the Client Acceptance Certificate (CAC) once the Services have been deployed and tested as working.

(k) Where we or our MSP incur costs due to your negligence, fault, act, or omission, you must pay us additional fees, which we will confirm on request.

(l) Any other responsibilities agreed under this Agreement or reasonably requested by us or our MSP to perform our obligations under this Agreement.

Invoicing

11.37 The service is offered as a monthly fee, calculated daily. Service usage data will be collected from the policy deployment date, based on daily usage rates for licence types within the applicable Check Point Haromy tenancy. Fees will be billed monthly in arrears until termination.

11.38 We may commence billing for the service if the CAC is not signed within a reasonable period (7 days), or where we can prove through standard reporting that the service is operational.

11.39 The monthly services fee for the Managed Cyber Security Service will automatically continue a month-to-month basis under the existing terms and conditions, including price, until the customer cancels their service. For any changes to the terms and conditions, including price, we will provide you with at least 30 days' notice

Service Pricing

11.40 Charges for this service offering (and, where relevant, limitations on service inclusions) are set out in the Managed Cyber Security - Check Point Harmony – Critical Information Summary. We may update these charges from time to time.

11.41 Where required, a service fee will apply if additional hours are required to comply with specific customer requirements not covered in the standard inclusions (such as HSE Inductions). The service fees may include reinstallation charges, extra time-on-site, and travel fees.

Location of services

11.42 All packages are delivered remotely. No site visits are included.

11.43 Additional travel and call-out fees will apply if onsite visits are requested. Charges for call-outs and travel can be supplied by your local TBTC.

Software and Licence Eligibility

11.44 This solution is available only for current compatible Check Point Harmony Endpoint, Mobile and Email & Collaboration licenses, purchased through Telstra.

Total minimum service cost

11.45 Minimum costs for each service are outlined in the Managed Cyber Security - Check Point Harmony – Critical Information Summary and is chargeable monthly in arrears. The minimum service cost you pay depends on the service you select, the support option you choose, and any additional services you need.

Early termination and other charges

11.46 You may cancel your service at any time before we start to work on your instructions. We do not charge you up to that point.

11.47 Once the service has been activated, it will automatically continue on a month-to-month basis on the existing terms (including monthly subscription fees) until either party cancels on 30 days written notice. Any changes in terms or fees will be notified to you with at least 30 days' written notice.

Other fees

11.48 Any work outside the pre-defined service inclusions listed under "Service Deliverables Table" **above** will incur extra costs. Examples of these are on-site visits, new tenancy setup and new licence installations. Any additional services costs considered as non-standard service requests will be communicated to, and agreed by you, before we commence work.

Payment Options

11.49 Apart from the service setup fees (which will appear as a once-off amount on the first Telstra bill after service activation), the service is only available as a monthly subscription payment option for the contract duration, commencing on the first Telstra bill you receive after successful service activation.

11.50 The Service will be automatically renewed after the initial contract duration as a monthly contract, billed monthly with 30-days' written notice if either party wishes to cancel. Usual credit terms apply to the payment of these amounts.

Billing

11.51 On the same day of each month, you'll be billed in advance for your monthly service fee.

11.52 Direct Debit is our preferred payment method, you can set it up anytime at telstra.com/direct debit

11.53 Electronic payments – Free

11.54 Payments made in person or cheque – Extra $2.50 (some exemptions apply).

11.55 Paperless bills are free. A paper bill can be issued for $2.20 per copy sent (some exemptions apply).

11.56 Paper bills are issued unless you set up paperless billing. Set up Email bill at telstra.com/emailbill or for more information on your billing options visit telstra.com/fees-on-payment-methods

12 TELSTRA DATA PROTECT INSTALLATION

Service Summary

12.1 The Telstra Data Protect Installation service comprises the installation, configuration, verification and hand over of the Service Software on Backup Target Devices.

12.2 The terms in this Clause 11 as well as the Other Services - Professional Services section of Our Customer Terms apply to our provision, and your receipt and use of the Telstra Data Protect Installation service.

12.3 Unless otherwise agreed with you in the order details in this agreement, the Telstra Data Protect Installation service will be delivered remotely during Business Hours.

12.4 Remote installation requires matching time commitments from your elected Administrator for orientation, remote hand assistance or training. On-site installation may be available to reduce your time commitment. However, additional charges may apply for on-site installation or installation outside of Business Hours.

12.5 The Service requires adequate storage capacity on the Backup Target Device/s to download and install the Telstra Data Protect agent software/app on the device.

12.6 This service requires a separate paid subscription to Telstra Data Protect storage available via the Telstra Application Marketplace. You need adequate storage for all the devices you wish to backup, which will grow over time. Your Telstra Business Technology Centre Representative or Telstra Client Partner can help order this on your behalf using the information you provide.

12.7 The Telstra Application Marketplace forms part of the Cloud Services section of Our Customer Terms (available at https://www.telstra.com.au/customerterms/business-government/cloudservices) governs your use of the Telstra Application Marketplace.

Customer Profile

12.8 This service is offered exclusively to Telstra customers who have separately purchased relevant Telstra Data Protect subscriptions and require professional installation and activation. Your Telstra Business Technology Centre Representative or Telstra Client Partner can recommend Telstra Data Protect subscription plan/s to you (and order this on your

behalf) based on the information you provide.

What is included?

12.9 Telstra Data Protect Installation is available with two standard offers as further described below. The main inclusions in the standard packages are:

(a) **Admin Portal** is the setup and handover of the Admin portal to manage the backup service as provided by your Telstra Data Protect subscription. This is essential for a new Telstra Data Protect service.

(b) **Essential 1** is a per device, remote installation of the Telstra Data Protect backup agent on Backup Target Devices and activating the backup service into the Telstra Data Protect provided cloud storage subscription.

12.10 Onsite installation is available however additional fees may apply.

Service Description Deliverables Table

Inclusions		Installation Service Inclusion	
		Admin Portal (optional one-off charge)	**Essential 1**
Inclusion limits	Activation of Backup Target Devices		Installation of Telstra Data Protect instance on 1 Backup Target Device
	Backup protection plan profiles[1] *Creation of backup protection plan profile(s) in the Telstra Data Protect Application*		1 backup protection policy
	Customer Admin User creation	1 Admin user	
Delivery coordination		✓	✓
Change Management		✓	✓
Setup Telstra Data Protect Admin portal and Admin user		✓	✗
Setup backup protection plans in Admin portal *Create backup protection policies including rules and schedules*		✓	✗
Setup Backup Target Devices[3]		✗	✓

Inclusions	Installation Service Inclusion	
	Admin Portal (optional one-off charge)	Essential 1
Deploy and activate the Telstra Data Protect plans that you bought from us to work with the identified device		
Release and Deployment Management[4] *To help ensure that these changes have reduced impact on the business operation*	✓	✓
Service Validation and testing	✓	✓

What is not included?

12.11 The Telstra Data Protect Installation service does not include any equipment installation, Telstra Data Protect licencing or connectivity.

12.12 Initial full backups may take a long time, ranging from minutes to days. This depends on the Backup Target Devices' total data volume for backup, your available bandwidth, any network limitations, and specific business rules built into the backup protection plan profiles. To help mitigate backup traffic impact on your ongoing business operation, you must ensure after-hours backup scheduling, and backup data stream throttling.

12.13 This service is deemed complete when we demonstrate, in the Telstra Data Protect administrative portal, that the backup service is operational and delivers measurable backup data payload into your Telstra Data Protect tenancy.

12.14 Ongoing monitoring or management of Telstra Data Protect is not included.

12.15 Anything else not explicitly described in clause 12.9.

Your Responsibilities

12.16 You must:

a) Ensure that you purchase a Telstra Data Protect subscription that includes enough data storage to complete an initial backup of all Backup Target Devices and a reasonable amount of unique data growth overhead;

b) Accurately complete the pre-service checklist form we provide to you before we can perform the Service;

c) Provide accurate detail on your existing IT and network environment and any other information we reasonably request in relation to the Backup Target Devices;

d) Provide at least 2 Business Days prior written notice to us if you wish to reschedule an

appointment for performance of the Service;

e) Provide any necessary Administrator access credentials and access to existing systems to allow our technician to perform the Service;

f) Act on the instructions of our installation technician to perform certain activities in relation to the Service (such as to download and activate specific applications on a mobile device) in circumstances where our technician cannot do this remotely;

g) Provide reasonable access to your sites if we have agreed to deliver the Service onsite; and

h) Promptly sign a Customer Acceptance Certificate once the Service has been performed and the Telstra Data Protect service is operating on your Backup Target Devices.

Service Pricing

12.17 Charges for your Telstra Data Protect Installation (and where relevant, limitations on service inclusions) are set out in your Application Form and the Telstra Data Protect Installation Critical Information Summary, a copy of which will be provided to you.

12.18 Additional service fees apply if we have to spend additional time on your Telstra Data Protect Installation in order to comply with your specific requirements to complete the engagement (such as HSE inductions). We will inform you of those additional charges in advance. If you do not agree with those additional charges, we will not provide (and we are not otherwise required or obligated to provide) the service.

Special Meanings

12.19 In this clause 10, the following words have the following meanings:

Administrator means an end user who is designated as an administrator in the Telstra Data Protect application form.

Business Hours means 9am – 5pm on Business Days.

Service Software means the Telstra Data Protect software.

13 SPECIAL MEANINGS

13.1 In this section of Our Customer Terms, the following words have the following special meanings:

Additional Equipment means that Equipment described as such in your Application Form and which we will not maintain under a Maintenance Contract you have with us, if applicable.

Application Form means an application form or order form used to order any of the TBS Products and Services.

Business Day means a day other than a Saturday, Sunday or a public holiday in the place where the Site is located.

Core Equipment means the part of the Equipment which centrally controls all of the other Equipment.

Customer Supplied Equipment means that Equipment which you supply, as set out in your Application Form and which we will not maintain under a Maintenance Contract you have with us, if applicable.

Customer Acceptance Certificate or **CAC** means the document you must sign upon completion of the relevant Service Deliverables

Cyber Security Audit means the service described in clause 6.

Delivery means your receipt of the Telstra Supplied Equipment.

DECT means Digital European Cordless Telecommunication.

Developed Material means all material in any form, including documents, reports, products, equipment, information, data, software, software tools and software development methodologies, created or developed by our employees, agents, contractors or representatives in the performance of the TBS Professional Services.

Equipment means all the equipment for a Site as detailed in your Application Form, as varied from time to time, including without limitation any software contained in that equipment. Equipment includes Core Equipment, Main Equipment, Additional Equipment, Customer Supplied Equipment and Telstra Supplied Equipment, except where otherwise specified.

Equipment Purchase Price means the GST exclusive price specified in your Application Form for each individual piece of Telstra Supplied Equipment.

Installation means the Standard Installation and the Non-Standard Installation or any special installation request made by you in accordance with clause 4.22.

Installation Price means the GST exclusive price specified in your Application Form for the installation for each individual piece of Telstra Supplied Equipment.

Intellectual Property Rights means all rights conferred under statute, common law and equity in and in relation to inventions, designs, trade marks, trade names, logos and get up, confidential information and copyright and any other intellectual property rights as defined by Article 2 of the World Intellectual Property Organisation Convention of July 1967.

MAC (moves, adds, changes) means a request to install, move, add, change, remove, upgrade, delete, reconfigure and relocate your Equipment, including changes to the configuration or programming of the Equipment, adding extra Equipment to an existing configuration, relocation of existing Equipment within the same Site and any additional cabling.

Main Equipment means that Equipment described as such in your Application Form which, if applicable, we will maintain under a Maintenance Contract with the exception of any exclusions to the Maintenance Contact as set out in your Application Form.

Maintenance Contract means a contract for the provision of Telstra Business Systems Care

in respect of the Main Equipment, as referred to in clause 4.45.

Managed Microsoft 365 means the services described in clause 10.

Metro Site means a Site that is within a 60km radius of a capital city of a State or Territory in Australia or the business premises of one of our service delivery partners.

Network Device Installation means the service described in clause 5.

Network Device Management means the service described in clause 7.

Non-Standard Installation means the installation services described in clause 4.32.

Site means the site/s described in your Application Form as varied from time to time.

Standard Installation means the installation services described in clause 4.31.

Start Date has the meaning given to it in clause 3.1.

Supplier means the person supplying the Equipment to us.

Supplier's Specifications means the specifications published by the Supplier for the Equipment and included with the Equipment upon Delivery.

Supplier's Warranties means any express warranties the Supplier gives for Additional Equipment.

TBS has the meaning given to it in clause 1.1.

TBS Products and Services means the TBS products and services described in clause 2.1.

TBS Professional Services means the services we will provide to you in relation to the TBS Products and Services as set out in your Application Form and as described in this clause 13.

TBSRO means the TBS repayment option described in clause 4.10.

TBSRO Charge means the total charge payable under the TSBRO, and is calculated by multiplying the monthly 'Total Site Charge' set out in your Application Form by the total number of months in the TBSRO term set out in your Application Form.

TBSRO Early Termination Charge is the total of the unpaid part of the TBSRO Charge.

Telstra Business Systems Care means the service described in the Managed Voice Services – Part C – Telstra Business Systems Care section of Our Customer Terms.

Telstra Install – Microsoft 365 Business means the services described in clause 9.

Telstra Supplied Equipment means that Equipment which we will supply to you as part of the TBS Products and Services, as set out in your Application Form, and excludes that Equipment which is Customer Supplied Equipment.

T-Rooms Videoconferencing means the service described in the Our Customer Terms - Internet Direct and Business Broadband section