OUR CUSTOMER TERMS
MANAGED SECURITY SERVICES SECTION

CONTENTS

Certain words are used with the specific meanings set out in clause 23 and in the General Terms of Our Customer Terms at http://www.telstra.com.au/customer-terms/business-government/index.htm.

1 ABOUT THIS SECTION

1.1 This is the Managed Security Services section of Our Customer Terms.

1.2 The General Terms of Our Customer Terms also apply to your Services. See section one of the General Terms of Our Customer Terms at http://www.telstra.com.au/customer-terms/business-government/index.htm for more detail on how the various sections of Our Customer Terms are to be read together.

2 MANAGED SECURITY SERVICES

Our services

2.1 Our Managed Security Services can include design, monitoring and management of your digital and physical assets, depending on which service elements you choose.

2.2 We provide our Managed Security Services by way of shared infrastructure, dedicated infrastructure and virtualised applications, depending on what services you acquire.

2.3 Our Managed Security Services are made up of:

(a) Cyber Detection and Response (**CDR**) (formerly "Security Monitoring");

(b) Managed Next Generation Firewall bundle, which includes Security Intelligence;

(c) Managed Firewall, which includes Security Intelligence;

(d) Managed Intrusion Protection Service (IPS), which includes Security Intelligence; and

(e) Cyber Detection and Response – Endpoint ("**CDR - Endpoint**").

2.4 The details of each element of our Managed Security Services, and the other services we offer, are set out below.

Availability

2.5 The Cyber Detection and Response terms in this Managed Security Services section of Our Customer Terms only apply to services contracted before 30 August 2024. For Cyber Detection and Response services contracted or renewed on and from 30 August 2024.

2.6 On and from 2 March 2020, we withdrew Managed Firewall and Managed IPS from sale to new and existing customers. Customers with existing contracted Managed Firewall or Managed IPS services can request adds, moves, and changes as per the terms of their contract.

2.7 From 14 December 2020, Managed Gateway & Cyber Security Equipment will no longer be available with Cisco and Juniper hardware (managed and unmanaged) to new and existing customers (including no further adds, moves or changes to existing hardware or service).

2.8 To provide the Managed Security Services, we need to be able to connect to your device, application or service (as the case may be). We'll tell you when you apply for the Managed Security Services what the minimum connectivity requirements are.

2.9 There are elements of the Managed Security Services that we can only provide if you have certain devices, applications or services. If you don't have the minimum requirements needed for the service you want to acquire, we can't provide that service to you. We'll tell you the minimum requirements on request.

2.10 The Managed Security Services are not available to Telstra wholesale customers or for resale.

3 WHAT IS CYBER DETECTION AND RESPONSE (CDR)?

3.1 The CDR (formerly "Security Monitoring") service comprises the following services:

(a) logging – this service stores the log and event data we receive from you;

(b) event monitoring, correlation and classification – this service monitors logs and events for Incidents;

(c) incident notification – this service provides notification of Incidents and may include rating of these Incidents; and

(d) if included, vulnerability Management – this service scans for vulnerabilities in the IT assets that we've agreed with you.

How we provide CDR and what you must do

3.2 We provide the CDR service:

(a) using shared infrastructure and the public cloud, unless we otherwise think it's appropriate to use dedicated infrastructure; and

(b) through a method between your infrastructure and our infrastructure that we will confirm to you on request.

3.3 To receive the CDR service, you must at your own cost:

(a) separately obtain an appropriate carriage service;

(b) ensure the term of that carriage service does not end before the term of your CDR service; and

(c) complete changes to your network and resources as we require from time to time to allow log and event data to be passed to us from your infrastructure to our infrastructure using a means that we require.

3.4 Each element of the CDR service comprises one or more stages, depending on the service:

(a) the first stage is provided on a once-off basis at the start of your service;

(b) the second stage is provided on an ongoing basis during the term, once the first stage is completed; and

(c) the third stage is provided periodically during the term as we think necessary.

Service	First stage	Second stage	Third stage
Logging	Design the network connectivity to our infrastructure. Configure our infrastructure and create the required VPN tunnel to your infrastructure.	Capture your logs and events, often in near real time where we think necessary. Store your log data in a secure environment. Provide access to your log data via the Telstra Security Portal.	N/A
Event monitoring, correlation and classification	On-board the platform to accept your log and event data. Apply the default correlation and classification configurations.	Correlate and classify your Security Events. Store your Security Events in a secure environment. Provide access to your Security Events via the Telstra Security Portal.	N/A
Incident notification	N/A	Expert assessment of your Incidents. Provide a ticket on your Incident within the Telstra Security Portal.	Automatically alert your nominated contact point when we detect an Incident.
Vulnerability Management ("Premium" service tier only as set out in clause 3.5 below)	On-board to scanning platform and scanning of IP addresses (up to the number specified in your Application Form). Conduct asset discovery (map) scans. Classify assets. Set up scans for initial reports.	Access to the Telstra Security Portal. Access to scanning reports.	Notify of newly discovered vulnerabilities. Alert if scanners don't respond to configured "heartbeats".

What service tiers are available?

3.5 The features of your CDR service are set out in the table below based on the applicable service tier.

Features	Premium	Premium – ISM Certified
Certified to operate at the "ISM PROTECTED" level	No	Yes
Online log and event retention	Up to 12 months*	Up to 12 months*
Offline log and event retention	Up to 7 years*	Up to 7 years*
Allowed number of notification contacts	Up to 5	Up to 5
Incident notification (includes both event monitoring, correlation and classification and logging services	Included	Included
Vulnerability Management scanning	Included	Not included
Retention of vulnerability scan reports	7 days	7 days
Retention of raw vulnerability scan data	12 months*	12 months*

* This is a rolling period, after which we may not be able to recover the log event.

3.6 We will allocate up to a total of 10 terabytes of storage for your logs, events and reports (based on the package you chose) as part of the CDR service. You can request additional storage. If we accept your request, we will confirm the applicable charge for that additional storage.

3.7 Once you reach your allocated storage, your oldest log and events we stored will be over-written to store your new incoming log and events from your device. When this happens, the "first in and first out" principle will be applied to your allocated storage.

How do we rate and notify you of Incidents?

3.8 As part of your CDR service, we will rate your Incidents using the following table as guidance:

Incident rating				
Impact **Urgency**	**Extensive** (Direct / indirect impact on more than 1 critical asset)	**Significant** (Direct / indirect impact on at least 1 critical asset)	**Moderate** (Direct / indirect impact on more than 1 non-critical asset)	**Minor** (Any other identified Incident)
Category 1 (less than 2 hours)	Priority 1	Priority 2	Priority 2	Priority 3
Category 2 (between 2 hours and up to 12 hours)	Priority 2	Priority 2	Priority 3	Priority 4
Category 3 (more than 12 hours and up to 24 hours)	Priority 2	Priority 3	Priority 3	Priority 4
Category 4 (more than 24 hours)	Priority 3	Priority 3	Priority 4	Priority 4

Impact = How severe we think the Incident is on an **asset**.

Urgency = How soon we think the Incident needs to be addressed.

Asset = A device you own on the network that if compromised, could significantly and detrimentally impact your business. Examples of assets are web servers, databases or workstations. With our agreement, you will nominate to us which of your assets are critical or non-critical (and you must act reasonably in doing so). Although we may give you guidance on the categorising of your assets, you're solely responsible for that categorisation.

3.9 We are solely responsible for rating your Incidents. This means that any security issue or attack blocked by another vendor's product or signature, or by your own policy, is not automatically deemed to be an Incident. A ticket will not be created for that issue or event unless we have rated it in a way that requires a ticket to be created.

3.10 You can choose not to receive email or SMS alerts by changing your preferences on the Telstra Security Portal.

What is Vulnerability Management?

3.11 The Vulnerability Management service:

(a) is only available with the "Premium" service tier and is not available with the "Premium - ISM Certified" service tier of the CDR service;

(b) remotely scans IT assets and IP addresses that we've agreed with you, against a list of known security vulnerabilities; and

(c) is self-service so you can schedule scans, view configurations, and run and download reports via the Telstra Security Portal.

3.12 To obtain the Vulnerability Management service, if we ask you to, you must promptly and at your own cost:

(a) install internal scanners for vulnerability scanning;

(b) configure your systems to allow your assets to be scanned (such as implementation of firewall rule changes); and

(c) comply with our other reasonable requests.

3.13 You are responsible for backing up your data before we provide the Vulnerability Management service to you. You acknowledge and accept the risk that the supply of the Vulnerability Management service may result in or cause interruptions, loss or damage to you and your computer systems, networks, websites, internet connections and data, and that we do not separately back-up any of your data to avoid potential data loss. You agree that to the full extent the law allows and subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we have no liability to you or any party as a result of this.

3.14 You agree that for your Vulnerability Management service:

(a) scan reports show a point in time of your assets at the time of the scan;

(b) your scan uses a list of known vulnerabilities, which is continually updated, and this may impact the currency of your scan reports;

(c) scans don’t detect all vulnerabilities or vulnerabilities that are known at the time of the scan;

(d) you’re responsible for scheduling scans at appropriate intervals based on your security needs; and

(e) the service doesn’t test, exploit, manage, rectify or fix any vulnerabilities or issues - these are your responsibility.

3.15 Given the nature of the service, the service levels and service credits in this section of Our Customer Terms don’t apply to your Vulnerability Management service.

3.16 You must:

(a) only use the Vulnerability Management service (and any reports generated) solely for your internal use and to scan assets that you have the legal right to scan;

(b) not scan the assets of a third party; and

(c) not modify, interfere with, transfer, or affect the operation of the Vulnerability Management service in any way.

What optional components are available?

3.17 You may request:

(a) additional log and event storage capacity and retention periods;

(b) services to extract your logs from storage; and

(c) Where Vulnerability Management is included, scanning of additional IP addresses above the number specified in the Application Form as included in your service tier.

If we agree to your request, we will confirm the applicable charges.

How do you access your service?

3.18 You can access your CDR service via the Telstra Security Portal.

3.19 The Telstra Security Portal aims to let you do the following:

Event monitoring, correlation and rating	Incident notification	Vulnerability Management ("Premium" Service Tier only)
View and track your rated Incidents. Raise a service request to view your archived Incidents. Generate reports on your Incidents.	View expert assessment of your Incidents.	Configure scans. Run reports. View vulnerabilities against assets. View and download reports.

What are the service limitations?

3.20 Subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we don't promise that the CDR service will correctly detect and identify all:

(a) Security Events or Incidents;

(b) unauthorised access to your network;

(c) viruses;

(d) spam; or

(e) other types of attacks or issues.

3.21 You must promptly tell us if you find limitations or issues with your CDR service.

3.22 You must give us at least 10 business days' notice before any vulnerability or penetration testing occurs to your network (except for scans as part of your Vulnerability Management service).

Term and termination

3.23 When you cancel your CDR service;

(a) we will store your logs for up to 90 days from the date of cancellation (at your expense), unless you tell us in writing that you do not want us to do this;

(b) you may request an extract of your logs during this 90 day period;

(c) you must pay a fee for this extraction and we can confirm this fee on request;

(d) you will not be able to request an extract after this 90 day period; and

(e) your Vulnerability Management service will also be cancelled and we won't retain any scan data or reports.

4 WHAT ARE THE CDR SERVICE LEVELS?

What are the provisioning and change service levels?

4.1 The provisioning and change service level targets are:

Item	Description	Service level target
Provisioning time	Time from when we receive your order until the time the service is provisioned	20 business days
Activation time for adds, moves or changes	Time from when we receive and approve a written request from you until the time when we complete the change	10 business days

4.2 Our provisioning and change service level target assume the following:

(a) timing begins when we receive your written order or request with all fields fully and accurately completed;

(b) we have already accredited and approved all of your data sources that we need to provide the CDR service to you;

(c) timing excludes any time waiting for you to provide information we need to progress your order or request; and

(d) excludes any time needed to alter or prepare your network, devices or other resources in connection with the order or request.

What are the service quality service levels?

4.3 The service quality service level targets are:

Item	Description	Incident priority	Service Level Target
Incident rating time	Time from when the CDR platform receives a Security Event to the time an Incident is rated in the Telstra Security Portal	1	15 mins
		2	30 mins
		3	60 mins
		4	180 mins
Incident notification time	Time from when an Incident is reported by the agreed method below	1	15 mins
		2	30 mins
		3	NA
		4	NA
Incident notification method	The method we use to notify your nominated contact person of Incidents	1	Portal + email + phone call
		2	Portal + email+Phone call
		3	Portal
		4	Portal
Service management	How often we contact you about your CDR service	NA	Monthly

What is the service availability service level?

4.4 The monthly service availability service level targets are:

Item	Description	Service level target
Availability of the Telstra Security Portal for the CDR service	Calculated per calendar month	99%
Availability of the CDR platform (excluding the Telstra Security Portal)	Calculated per calendar month	99%
The service level is calculated as follows: Availability = {[(A – B) – C / (A – B)] x 100} A = Total number of hours in the month. B = Number of hours in a planned outage period in the month. C = Number of outage hours for the CDR platform in the month.		

What is the fault reporting service level?

4.5 The fault reporting service level targets are:

Item	Description	Service level target
Initial response time for faults reported via the service desk	Measured from when you report a fault to when we respond	Severity 1: 30 mins Severity 2: 60 mins Severity 3: 120 mins Severity 4: 240 mins
Initial response time for system generated faults	Measured from when you report a fault to when we respond	Severity 1: 15 mins Severity 2: 30 mins Severity 3: 60 mins Severity 4: 120 mins
Service restoration	Measured from when a fault is reported to when the fault is resolved	Severity 1: 95% restored (or work around) in 6 hours Severity 2: 95% restored (or work around) in 12 hours Severity 3: 95% restored (or work around) in 24 hours Severity 4: 95% restored (or work around) in 72 hours

Progress updates	Measured from when we last updated you on the issue	Severity 1: every 1 hour Severity 2: every 4 hours Severity 3: every 12 hours Severity 4: every 24 hours

What service credits may be available?

4.6 If we do not meet the service level targets in this clause 4, you can request a service credit. You must do this by telling us in writing within 30 days from the date that we did not meet the applicable service level.

4.7 After we receive your request under clause 4.6, we will confirm with you if a service credit is due (and we will act reasonably in doing so). The following applies to your service credits:

(a) if a service credit is due, we will rebate you an amount equal to 10% of your monthly charge for the impacted CDR service;

(b) in any given calendar month, your entitlement to service credits is capped to an amount equal to 20% of your monthly charge for the impacted CDR service;

(c) you cannot receive more than one service credit in any 24 hour period, regardless of the number of service legal target failures in that period; and

(d) we endeavour to meet the service level targets in this clause 4 and your request for the applicable service credit is your only remedy for our failure to do so.

4.8 Service credits don’t apply where the failure to meet the service level target is affected by:

(a) a fault with your product, service or resource that is caused by you or a third party;

(b) any third party act or omission;

(c) the cutting of cable or fibre which is needed to provide your product or service;

(d) interference or damage to our equipment or network by you or by a third party;

(e) a fault beyond our network boundary point or with your equipment or resources (unless we have specifically agreed in writing to support these things); or

(f) any other cause beyond our reasonable control (including acts of God, industrial disputes of any kind, lightening, fire, earthquake, storm, flood, government restriction, determination of any government or regulatory body, determination of any court of law or any such similar event).

5 WHAT IS MANAGED NEXT GENERATION FIREWALL BUNDLE?

5.1 The Managed Next Generation Firewall bundle service provides management of a bundle of security services. It includes:

(a) all of the Security Intelligence features;

(b) hardware you have selected that are installed on your premises, and maintenance services;

(c) intrusion protection service (IPS) module;

(d) IPSEC site to site VPN tunnels;

(e) IPSEC / SSL client to site VPN tunnels; and

(f) other services set out below.

5.2 You must rent from us a Managed Next Generation Firewall device that the Managed Next Generation Firewall bundle service will apply to.

5.3 We'll provide the Managed Next Generation Firewall bundle service at the service tier you select in your application form.

5.4 Managed Next Generation Firewall bundle is available:

(a) as a single service, which uses a single device, or as a high availability service, which uses two separate devices, in an active/passive configuration; and

(b) with or without a content security service, further described below.

5.5 You can choose:

(a) our content security service, Internet Protection Services; or

(b) the on-board content security feature available on the device.

5.6 If you choose our Internet Protection Services for content security, the relevant terms of the Internet Protection Services section of Our Customer Terms apply to those services other than:

(a) charges – charges for Internet Protection Services are available on application. If your Managed Next Generation Firewall bundle service is cancelled or terminated earlier and you continue to obtain Internet Protection Services, then the charges set out in the Internet Protection Services section of Our Customer terms will apply to your Internet Protection Services;

(b) minimum term – the minimum term of your Internet Protection Services must be the same as the minimum term of your Managed Next Generation Firewall bundle service; and

(c) early termination charges – these are set out in clause 22.7.

Core elements of Managed Next Generation Firewall bundle

5.7 Managed Next Generation Firewall bundle comprises three stages, with the features set out in the table below:

(a) the first stage is provided on a once-off basis at the commencement of your service;

(b) the second stage is provided on an ongoing basis during the term, once the first stage is completed; and

(c) the third stage is provided periodically during the term as we consider necessary.

First stage	Second stage	Third stage
Design and installation services. Design your policy based on information you provide us. Setup Security Intelligence services. Configure the Telstra shared SOC infrastructure and create the required VPN tunnel to your infrastructure. Configure and implement your policy. If applicable, setup Internet Protection Services.	Provide ongoing Security Intelligence services. Provide health monitoring notifications. Provide break and fix maintenance and restoration. Perform backup and restore of configurations. Provide updates for your firewall device. Provide signature updates for IPS module. If applicable, provide ongoing Internet Protection services. If on-board content security is purchased, provide signature updates for anti-spam, URL filtering and virus scanning.	Providing periodic third stage Security Intelligence services as required from time to time. If applicable, providing periodic Internet Protection Services as required from time to time.

5.8 Managed Next Generation Firewall bundle has two service tiers and features as set out in the table below:

Features	Enhanced	Enhanced Plus
Security Intelligence		
Log and event retention	1 year	7 years
Log and event storage	40 GB per year	60 GB per
Allowed number of assets	Up to 20 assets	Up to 20 assets
Allowed number of Security Events per second	Up to 5 Security Events per second	Up to 5 Security Events per second
Event monitoring, correlation and classification with automatic email notification (includes logging service)	Included	Included
Allowed number of notification contacts	Up to three	Up to three

Features	Enhanced	Enhanced Plus
Security Intelligence		
Security Event notification (includes both event monitoring, correlation and classification and logging services)	Not included	Included
Managed Next Generation Firewall bundle		
Support and helpdesk hours	24x7	24x7
IPSEC site to site VPN tunnels	Up to 2 tunnels	Up to 10 tunnels
IPSEC / SSL client to site VPN tunnels	Up to the device capacity	Up to the device capacity
IPSEC / SSL client to site VPN profiles	One only	Up to three

5.9 You can activate up to the allowed number of VPN tunnels and profiles as part of the initial activation of your Managed Next Generation Firewall bundle service. If you activate fewer at initial activation, and wish to activate new tunnels or profiles at a later time (up to the allowed number), extra charges are applicable.

Optional components of Managed Next Generation Firewall Bundle

5.10 As well as the core components of the Managed Next Generation Firewall bundle service, you may also ask us to provide additional set up options, including policy audit, policy optimisation and policy translation, by using our security consulting services, which are available separately at extra cost.

5.11 You may also ask us to update software that is part of the Managed Next Generation Firewall bundle from one major version to another major version. This is available separately at extra cost.

Scope of use of Managed Next Generation Firewall Bundle

5.12 Your particular equipment may require additional software in order to work with the Managed Next Generation Firewall bundle service, or in order to take advantage of particular features of the equipment. If this is the case, we'll let you know, and you can either buy the software yourself, or ask us to buy it for you (at your cost). If required, you authorise us to do all things necessary on your behalf to buy and install the software and use it in conjunction with your service, and you will get any third party consents to allow us to do those things on your behalf.

5.13 If you want to use advanced features of your particular equipment that are beyond the scope of our Managed Next Generation Firewall bundle service, we'll try to include the advanced features into your service. There may be extra charges involved, depending on the nature of the feature, and we'll tell you about the extra charges when you ask for the advanced features.

How do I access Next Generation Firewall Bundle?

5.14 You can access your Next Generation Firewall bundle service via the Telstra Security Portal. The Telstra Security Portal lets you:

(a) access the Security Intelligence features as set out in clause **Error! Reference source not found.**;

(b) access firewall and IPS reports for your device;

(c) submit and track policy change and service requests; and

(d) update your asset information.

5.15 You can use our telephone service desk to:

(a) submit and track policy change and service requests; and

(b) report network or firewall related service faults.

Limitations

5.16 Subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we don't promise that the Next Generation Firewall bundle service will:

(a) protect against all unauthorised access to your network;

(b) remove all viruses or correctly identify all viruses;

(c) screen or block all spam or correctly identify all spam;

(d) detect and remove all types of attacks or correctly identify all attacks;

(e) block all websites you ask us to block or correctly identify websites that you've asked to be blocked; or

(f) block all network activity you ask us to block or correctly detect and protect against network activity that you deem suspicious.

5.17 If you identify limitations in the Next Generation Firewall Bundle service, you should notify us immediately and to the extent possible, we'll try to rectify the limitations at no additional charge.

5.18 You have to:

(a) provide us with 10 business days' notice before you undertake vulnerability or penetration testing of your network;

(b) load and configure any VPN software on your equipment if you use a virtual private network solution; and

(c) nominate a system administrator to manage your master account on your portal. your system administrator is responsible for activating, managing and supporting user accounts for the online portal and to what data your users may access.

Exclusions

5.19 The development of customised IPS signatures for the IPS module is excluded from and not available as an option to the Managed Next Generation Firewall bundle service.

6 WHAT IS MANAGED FIREWALL?

6.1 The Managed Firewall service provides management of a firewall that is installed on your premises. It comprises all of the Security Intelligence features, plus the extra features set out below.

6.2 You must have, or buy or rent from us, dedicated hardware that the Managed Firewall service will apply to. In order for us to provide the Managed Firewall service, your firewall software and hardware must be accredited by us. We'll tell you what software and hardware are accredited if you ask us.

6.3 We'll provide the Managed Firewall service at the service tier you select in your application form.

6.4 Managed Firewall is available as a single service, which uses a single firewall, or as a high availability service, which uses two separate firewalls, in an active/passive configuration.

6.5 The following limits on the Security Intelligence features set out in clause **Error! Reference source not found.** do not apply to the Managed Firewall service:

(a) log and event storage;

(b) number of Security Events per second; and

(c) number of assets.

Core elements of Managed Firewall

6.6 Managed Firewall comprises three stages, with the features set out in the table below:

(a) the first stage is provided on a once-off basis at the commencement of your service;

(b) the second stage is provided on an ongoing basis during the term, once the first stage is completed; and

(c) the third stage is provided periodically during the term as we consider necessary.

First stage	Second stage	Third stage
If you already have a firewall, assessing whether it's accredited for us to provide the service. If you don't have an accredited firewall, buying or renting one from us. Once-off design and	Provide ongoing Security Intelligence services. Providing health monitoring notifications. Providing break and fix maintenance and restoration. Performing back-up and	Providing periodic third stage Security Intelligence services as required from time to time.

installation services. Setting up Security Intelligence monitoring and management interfaces.	restore of configurations. Providing updates for your firewall. Providing end to end service levels for management and carriage if you also acquire an appropriate service assurance package (which will be subject to separate terms and conditions).	

Optional components of Managed Firewall

6.7 As well as the core components of the Managed Firewall service, you may also ask us to provide additional set up options, including policy audit, policy optimisation and policy translation, by using our security consulting services, which are available separately at extra cost.

Scope of use of Managed Firewall

6.8 Your particular equipment may require additional software in order to work with the Managed Firewall service, or in order to take advantage of particular features of the equipment.

6.9 If this is the case, we'll let you know, and you can either buy the software yourself, or ask us to buy it for you (at your cost). If required, you authorise us to do all things necessary on your behalf to buy and install the software and use it in conjunction with your service, and you will get any third party consents to allow us to do those things on your behalf.

6.10 If you want to use advanced features of your particular equipment that are beyond the scope of our Managed Firewall service, we'll try to include the advanced features into your service. There may be extra charges involved, depending on the nature of the feature, and we'll tell you about the extra charges when you ask for the advanced features.

How do I access Managed Firewall?

6.11 You can access your Managed Firewall service via the Telstra Security Portal. The Telstra Security Portal lets you:

(a) access the Security Intelligence features as set out in clause **Error! Reference source not found.**;

(b) access firewall reports for your device;

(c) submit and track policy change and service requests; and

(d) update your asset information.

6.12 You can use our telephone service desk to:

(a) submit and track policy change and service requests; and

(b) report network or firewall related service faults.

Limitations

6.13 We don’t promise that the Managed Firewall service will:

(a) protect against all unauthorised access to your network;

(b) remove all viruses or correctly identify all viruses;

(c) screen or block all spam or correctly identify all spam;

(d) block all websites you ask us to block or correctly identify websites that you’ve asked to be blocked; or

(e) block all network activity you ask us to block or correctly detect network activity that you deem suspicious.

6.14 If you identify limitations in the Managed Firewall service, you should notify us immediately and to the extent possible, we’ll try to rectify the limitations at no additional charge.

6.15 You have to:

(a) provide us with 10 business days’ notice before you undertake vulnerability or penetration testing of your network;

(b) load and configure any VPN software on your equipment if you use a Virtual Private Network solution; and

(c) nominate a system administrator to manage your master account on your portal. Your system administrator is responsible for activating, managing and supporting user accounts for the online portal and to what data your users may access.

7 WHAT IS MANAGED IPS?

7.1 The Managed IPS service provides management of network intrusion protection services that are installed on your premises. It comprises all of the Security Intelligence features plus the extra features set out below.

7.2 You must have, or buy or rent from us, dedicated hardware that the Managed IPS service will apply to. In order for us to provide the Managed IPS service, your hardware and software must be accredited by us. We’ll tell you what hardware and software have been accredited if you ask us.

7.3 We’ll provide the Managed IPS service at the service tier you select in your application form.

7.4 Managed IPS is available as a single service, which uses a single device, or as a high availability service, which uses two separate devices, in an active/passive configuration.

7.5 We provide the Managed IPS service in a range of throughput ratings. The throughput rating you’ve chosen is set out in your application form.

7.6 The following limits on the Security Intelligence features set out in clause **Error! Reference source not found.** do not apply to the Managed IPS service:

(a) log and event storage;

(b) number of Security Events per second; and

(c) number of assets.

Core elements of Managed IPS

7.7 Managed IPS comprises three stages, with the features set out in the table below:

(a) the first stage is provided on a once-off basis at the commencement of your service;

(b) the second stage is provided on an ongoing basis during the term, once the first stage is completed; and

(c) the third stage is provided periodically during the term as we consider necessary.

First stage	Second stage	Third stage
If you already have an IPS device, assessing whether it's accredited for us to provide the service. If you don't have an accredited IPS device, buying or renting one from us. Once-off design and installation services. Setting up security intelligence monitoring and management interfaces.	Provide ongoing Security Intelligence services. Providing health monitoring notifications. Providing break and fix maintenance and restoration. Performing back-up and restore of configurations. Providing signature updates for IPS. Providing end to end service levels for management and carriage if you also acquire an appropriate service assurance package (which will be subject to separate terms and conditions). Providing ongoing security intelligence monitoring and management services.	Providing periodic third stage Security Intelligence services as required from time to time.

Optional components of Managed IPS

7.8 As well as the core components of the Managed IPS service, you may ask us to develop customised IPS signatures.

How do I access Managed IPS?

7.9 You can access your Managed IPS service via the Telstra Security Portal. The Telstra

Security Portal lets you:

(a) access the Security Intelligence features as set out in clause **Error! Reference source not found.**;

(b) access IPS reports for your device;

(c) submit and track policy change and service requests; and

(d) update your asset information.

7.10 You can also use our telephone service desk to:

(a) submit and track policy change and service requests; and

(b) report network or IPS related service faults.

Limitations

7.11 We don't promise that the Managed IPS service will protect against all attacks.

7.12 You have to:

(a) give us 10 business days warning before you undertake vulnerability or penetration testing of your network; and

(b) nominate a system administrator to manage your master account on your portal (your system administrator is responsible for activating, managing and supporting user accounts for the online portal and to what data your users may access).

8 WHAT IS CYBER DETECTION AND RESPONSE – ENDPOINT (CDR - ENDPOINT)?

8.1 CDR - Endpoint is a managed monitoring service that aims to protect your endpoints against malware and ransomware. An endpoint is a compatible physical or virtual device (such as a computer, server, laptop, mobile phone, tablet, or virtual machine image).

8.2 The CDR - Endpoint service uses a compatible endpoint agent to help monitor, manage and respond to detected Incidents on your endpoints.

8.3 To obtain the CDR - Endpoint service, you must supply a compatible endpoint agent, or buy one from us. We can confirm which endpoint agents are compatible on request.

What service tiers are available with CDR - Endpoint?

8.4 The CDR - Endpoint service has two service tiers ("Essentials" and "Advanced") with the features set out in the table below. We'll provide the CDR – Endpoint service at the service tier you chose and we approved:

Feature	Essentials	Advanced
Managed detection and response	✓	✓
Service activation	✓	✓

Investigation & notification	✓	✓
Indicator enrichment	✓	✓
Endpoint response	✓	✓
Threat detection	✓	✓
Aims to prevent malware	✓	✓
Health monitoring	✓	✓
Certain software upgrades	✓	✓
Access to CDR - Endpoint portal	✓	✓
Advanced threat detection	X	✓
Threat hunting	X	✓
Remote intrusion response	X	✓
KEY: ✓ = included in the service tier. X = not available with the service tier.		

What are the CDR – Endpoint service's key elements?

8.5 **Investigation & notification:** If a suspicious event is detected, an alert is generated. We will triage, investigate, and let you know if we think the event is a true positive, benign, or false positive.

8.6 **Indicator enrichment:** Indicators of compromise associated with detections are automatically extracted, scored, and enriched. Enriched indicators are visible in the CDR – Endpoint portal and are assigned a reputation (e.g. good, suspicious, bad) and classification (e.g. botnet, Zeus, crypto-miner, etc).

8.7 **Endpoint response:** After an investigation is done, we will respond as follows (subject to the pre-approved actions profile set up during service activation):

(a) **Quarantine:** Isolate the endpoint to stop it communicating with the Internet or other devices in your environment.

(b) **Delete File:** Delete specific files on an endpoint if we think it is malicious. File deletion can also occur as per your request as part of policy enforcement (for example, where you give pre-approval to delete potentially unwanted programs).

(c) **Whitelist:** Typically performed in response to an application that is incorrectly being blocked or terminated as malicious by the endpoint agent. We will update policies to whitelist the application for proper execution or set the correct privileges and actions it is allowed to perform. Whitelisting applications is also performed as part of service activation to help reduce the likelihood of unintended business disruption.

(d) **Monitor only:** As part of diagnosing misbehaving endpoint software, we can move an endpoint into monitor only mode. This is usually done in collaboration with you. Monitor only mode will direct the endpoint agent not to interfere with any end user activities on the endpoint.

(e) **Blacklist:** We will blacklist specific files on an endpoint if it we think it is malicious. Blacklisting a specific application either by computed hash or process name will inform the endpoint agent not to allow the application to run on the endpoint (that has the endpoint agent deployed on it).

(f) **Remote intrusion response:** As part of an advanced threat detection, we will use live/real-time response capabilities to perform intrusion response activities (such as searching and modifying the registry, analysing volatile memory, remote file deployment, and remote file retrieval). These activities are usually set up as part of service activation.

8.8 **Threat detection:** We will leverage the endpoint agent to help perform detections and provide visibility of activity on endpoints. These may include:

(a) **Signature Detection:** We use traditional anti-virus techniques to help identify malicious software by the reputation of their computed hash.

(b) **Our signatures:** We may detect new malware before it has been included into the signature database of endpoint platforms. When this happens, we may deploy proprietary new signatures to the endpoint agent.

(c) **Behavioural Detection:** We classify activity on endpoints and analyse them as part of known tactics, techniques, and procedures (TTPs) to help detect patterns of adversarial behaviour. Behavioural detection helps identify malware, not by whether it has been seen previously by detection software, but instead by how it behaves. We may expand on the list of known TTPs provided by the endpoint agent with our developed set of TTPs.

(d) **Reputational detection:** We help detect threats based on reputation, by correlating inbound and outbound network traffic to monitor suspicious and malicious domains and IP addresses.

(e) **Threat fusion:** We focus on identifying and prioritising information about threats using proprietary and open source intelligence. We undertake threat hunt missions (based on the chosen service tier), new detection signatures, new indicators, and reputation scoring.

8.9 **Advanced threat detection:** This includes all the elements of the Essentials service tier, and the following additional components:

(a) **Anomaly detection:** We statistically analyse several types of endpoint metadata to help identify anomalous user, process, and endpoint activity that could indicate malicious use.

(b) **Threat hunting:** Some advanced adversaries can evade standard detection mechanisms of cyber security detection tools. We proactively search through events to help detect and isolate advanced threats that might evade existing security solutions. We also conduct remote hunt missions to search for signs of advanced adversaries.

(c) **Forensic artifact analysis:** We perform advanced forensic artifact collection and analysis to triage anomalous events and determine adversary activity beyond actions captured by real-time telemetry.

(d) **Attacker abuse insights:** We analyse endpoint data to help identify tools, configurations, and security hygiene concerns that might benefit an adversary. We share these insights with our customers via our regular threat intelligence reporting, along with mitigation recommendations.

(e) **Ad-hoc IOC discovery:** As we discover new indicators of compromise or new attacker methodologies, we search your environment for these IOCs and provide response actions and recommendations.

(f) **Malware prevention:** We use the endpoint agent to help prevent the execution of suspicious or known malicious software. We will also help administer malware prevention by blacklist policy management, delivery of unique signatures, and threat intelligence indicator matching.

(g) **Deny or terminate process:** Some applications will not exhibit suspicious or malicious behaviours until after the process has been running. If this happens, we can terminate the application via the malware prevention blacklist. We can extend or manage the conditions which will cause an application to be terminated or denied.

(h) **Block operation:** The actions that an application can take can be controlled, including by block network connections, execution of a file-less script, invocation of a command interpreter, etc. We will work with you on what activities are allowed by specific applications to help reduce the possibility of malware.

8.10 **Health monitoring:** We will monitor communication between the CDR – Endpoint portal and the endpoint agent infrastructure. Should communication with that infrastructure become uncommunicative or unreachable, we will try to fix it. We will notify you if the issue leads to an outage.

8.11 **Software upgrades:** As certain third party endpoint software patches and upgrades are released, we may assess them for security, stability, and functionality before certifying it as a supported version. We will work with you to schedule any necessary remote upgrades. We may proactively reach out to you to request an upgrade (for example, if the current version has a major failure or severe vulnerability). You must maintain the current or one previously supported version at all times.

8.12 **CDR - Endpoint portal:** A web-based portal that provides real-time visibility of detected alerts, confirmed Incidents, enables your approved personnel to interact with us, view detected assets, and if applicable, view vulnerabilities. The following is also available through the CDR – Endpoint portal:

(a) **Dashboards:** Dashboards represent a variety of content, including event volume, alert volume, detected assets, and analyst response actions.

(b) **Reports:** Reports include your environment content related to alerts, Incidents, indicators, assets and vulnerabilities.

(c) **Customised reports:** You can request specific reporting on events to be automatically delivered. Extensive customisation of report templates or creation of custom reports are not included and can be performed for an additional fee, which we can confirm on request.

(d) **Threat intelligence reports:** These are threat landscape, sectorial, and intelligence summary reports.

How to contact us about your CDR – Endpoint service

8.13 **CDR – Endpoint portal:** The portal is the main way for you to stay informed of security activity in your environment. You can access the portal and review security alerts, dashboards, or reports.

8.14 **Email:** We may email you as part of the CDR - Endpoint service. Email topics can span a wide variety of matters, but most often will relate to security investigations, notification of risk, or questions on appropriate environment use or behaviours. When we receive emails from you via the CDR - Endpoint portal, a service request case is created and can be viewed within the CDR - Endpoint portal.

8.15 **Telephone:** Your approved personnel can call us on a 24/7 basis on 1800 577 332 or such other number we notify to you from time to time.

8.16 **Approved personnel:** You must give us a list of approved personnel and their email addresses for them to access the CDR - Endpoint portal. We will send these personnel an onboarding email to access the CDR – Endpoint portal and you must ensure they activate multi-factor authentication on their device.

What are the service level targets for the CDR – Endpoint service?

8.17 We aim to notify you of detected Incidents as per the following table:

Severity	Definition	Notification target time	We may notify you by:
Critical	Detected Incidents that are an imminent threat to your assets. This includes data destruction, encryption, exfiltration, or malicious interactive attacker.	Within 30 minutes of Incident classification completion.	Email, phone call, or CDR – Endpoint portal.
High	Detected Incidents that are a significant threat to your assets. This includes rootkits, keyloggers, or trojans, but not defined as "critical", ransomware, confirmed suspicious privilege escalation, confirmed social engineering-based attack.	Within 1 hour of Incident classification completion.	Email, phone call, or CDR - Endpoint portal.
Medium	Detected Incidents that are a potential threat to your assets. This includes malware types that include bots or spyware, but not defined as "critical" or "high".	No notification.	CDR – Endpoint portal.
Low	Detected Incidents that are a minimal threat to your assets. This includes, adware or other	No notification.	CDR – Endpoint portal.

	potentially unwanted programs.		

8.18 We will reasonably assign the relevant severity level to detected Incidents.

8.19 The notification target times are the time difference between when Incident classification is completed and when you are notified by the applicable method in the above table. We notify you after Incident classification to prevent notification of benign or false positive alerts.

8.20 Service level targets don't apply if they are affected by any events outlined in clause 4.8. For clarity, there are no service credits for the CDR – Endpoint service.

8.21 **Service Requests:** We aim to acknowledge standard service requests (applies to all non-change and non-Incident tickets) submitted via the CDR – Endpoint portal, email, or via telephone within one business day from the time stamp on the service ticket that we create.

8.22 **Maintenance and outages**

8.23 **Maintenance windows:** We aim to tell you of schedule maintenance outages at least 24 hours in advance. Service level targets do not apply during maintenance outages.

8.24 **Emergency maintenance:** We may not be able to tell you in advance of emergency maintenance, but we will try to notify you when we can.

What are your responsibilities?

8.25 **Software deployment:** During the CDR - Endpoint service activation process, you must promptly deploy the advanced endpoint agent on identified endpoints as per our instructions.

8.26 **Cooperation:** You must at all times reasonably cooperate with us and promptly follow our instructions during service activation and in relation to the CDR -Endpoint service.

8.27 **Notification of environment changes:** You must tell us in advance of any environment changes that may affect the CDR – Endpoint service.

8.28 **Notification of personnel changes:** You must tell us in advance of any changes to your approved personnel under clause 8.16.

8.29 **Internet access:** You must at all times maintain a reliable Internet connection to endpoints that are monitored by the CDR - Endpoint service.

8.30 **Additional remediation:** During investigation of security alerts, we may give you guidance on your environment to improve your security posture or to remediate an Incident. Performance of this guidance is your responsibility and at your own risk.

8.31 **Software updates:** You must promptly perform upgrades on the deployed endpoint agent as soon as they are available.

8.32 **Renewal of your CDR – Endpoint service:** You must renew your CDR - Endpoint service before its expiry date. If you don't do this, you understand and agree that your CDR – Endpoint service may stop working.

What are the charges for your CDR – Endpoint service?

8.33 Your applicable CDR – Endpoint service charges are set out below. All charges are GST exclusive:

Endpoint license type	Essentials		Advanced	
	Once off	Monthly (per endpoint)	Once off	Monthly (per endpoint)
We supply CrowdStrike Falcon	$2,000	$15.50	$2,000	$17.50
You supply CrowdStrike Falcon	$2,000	$12.50	$2,000	$14.50
You supply Microsoft Defender ATP	$2,000	$12.50	$2,000	$14.50

9 OPTIONAL SERVICES

9.1 Some of the Managed Security Services include options that you can ask us to provide to you.

9.2 If you do ask us to provide any optional services, we use reasonable efforts to comply with your request. We record the detail of your optional services in your application form.

9.3 If additional charges apply for these optional services, we'll tell you what they are when you apply for the optional services, and you have to pay the additional charges on top of the charges for the core components of the logging service.

10 EQUIPMENT

10.1 We can only provide the Managed Security Services if you have equipment that we support. If you don't have that equipment, you can buy or rent it from us.

10.2 We deliver the equipment that you rent or purchase from us to the address you nominate. You're responsible for the security of the equipment once it is delivered to your site. If the equipment is delivered to you before installation, you're responsible for making the equipment available for installation. If equipment isn't available for installation and as a result we need to reschedule installation, there may be a delay and extra cost to you.

Equipment you buy from us

10.3 If you buy equipment from us, you own it once we receive the purchase price. If you cancel your order for the purchase of equipment and we have already ordered the equipment, you may have to pay for the equipment that has been ordered for you. If this happens, you can keep the equipment that you've paid for.

10.4 We procure the right for you to use any software that forms part of the equipment on the same terms that the relevant third party vendor grants such licences. You agree to comply with the licence terms.

10.5 You must ensure that you comply with any reasonable directions that we give you to prepare your site for equipment installation (at your expense). If your site isn't ready for installation and as a result we need to reschedule installation, there may be a delay and extra cost to cover our extra expenses in rescheduling.

10.6 You must obtain our prior written consent before repairing or servicing the equipment.

10.7 You mustn't alter the labels or other identifying marks on any equipment that we provide to you.

10.8 If we provide the Managed Security Service for equipment that you haven't rented or bought from us, you're responsible for any faults with that equipment. We may not be able to meet our obligations if there's a fault with your equipment.

10.9 If we're providing the Managed Security Service for your servers, you may need to install certain software on your servers before we can provide you with the service.

Equipment you rent from us

10.10 If you choose to rent equipment from us, then clauses 10.10 to 8.19 apply to you.

10.11 You don't have any title to any equipment that you rent from us.

10.12 You have to:

(a) keep the rental equipment in good order and repair;

(b) not sell, dispose of or encumber the rental equipment; and

(c) allow us (or our supplier) to inspect the rental equipment at any reasonable time.

10.13 We can charge you additional amounts if you modify the rental equipment without our written consent, and the modifications reduce the equipment's use or value. We only charge you a genuine pre-estimate of our loss.

10.14 If you remove a part of the rental equipment, then you have to replace the removed part at your own cost with a part that's of equal or better quality (**Replacement Part**). The Replacement Part forms part of the rental equipment.

10.15 You can remove any part of the rental equipment that you've added provided that:

(a) it's not a Replacement Part (unless the Replacement Part is being replaced); and

(b) the removal of the Replacement Part doesn't reduce the equipment's use or value.

10.16 We can increase your rental charges if we supply extra parts or upgrades to the rental equipment. We'll tell you if this happens.

10.17 If any item of the rental equipment is lost, stolen or damaged beyond economic repair (except if caused by our breach or negligence), then you have to notify us promptly and pay us the present value of the rental equipment. If this happens before the end of the rental term for the rental equipment, you may also have to pay us early termination charges.

10.18 If you service or maintain the rental equipment, then you have to comply with the vendor's specifications and any other reasonable requirements.

10.19 You have to hold adequate insurance for the full value of the rental equipment and for your ability to pay all rental charges. You have to show us the insurance policy if we ask.

11 EQUIPMENT INSTALLATION

11.1 We install your rental equipment if you ask us to. We charge you an extra amount for this service, and we'll tell you what it is before we commence the installation.

11.2 Our standard hours for installation of equipment are during our standard business hours. If you ask us to install equipment outside our standard business hours we may charge you an additional charge.

11.3 If you don't provide us with access to your site, we can't install the equipment (and we won't be responsible for any installation delays).

11.4 If the installation of your equipment is more complex than we reasonably expect, we may charge an additional amount to cover any additional expense to us. We'll let you know if this is the case.

12 YOUR MANAGED SECURITY SERVICES

12.1 Your application form sets out the details of the Managed Security Services you've chosen.

12.2 We aim to meet the estimated timeframes and delivery dates set out in your application form but can't guarantee to do so. The time estimates in your application form are based on our previous experience, assumptions as to the nature of your internal environment, the availability of our consultants at the time of contract and the timeliness of your inputs and materials. As a result, any indications we give about delivery dates are only estimates and may change.

Changing your Managed Security Services

12.3 You can change any Managed Security Service to a higher-priced version of the same Managed Security Service at any time. The change, including higher charges, will take effect as soon as we process the request. These changes do not affect the term of your Managed Security Service.

12.4 If you try to change you Managed Security Service to a lower-priced version of the same Managed Security Service, this is treated as an early termination under clause 22.6.

Your responsibilities

12.5 You have to make sure we have your most current details at all times. You can change your details through the Telstra Security Portal.

12.6 We need you to provide various inputs and do various things in order for us to perform the Managed Security Services. These are different for each service, and are set out in our Responsibilities Guide. We make the Responsibilities Guide available at http://www.telstra.com.au/customer-terms/business-government/data-services/managed-security-services/.

12.7 The Responsibilities Guide may change over time and it's up to you to make sure you have the latest version.

12.8 If your particular environment involves special requirements or extra inputs from you, then these are set out in your application form. These are on top of your responsibilities set out in the Responsibilities Guide or Our Customer Terms.

12.9 You have to provide all materials and inputs by the dates specified in your application form or, where no dates are specified, when we tell you.

12.10 You have to maintain the firmware and software on your equipment (whether you own it or buy or rent it from us) to a currency of no less than 2 versions behind the latest production release of the relevant firmware or software (i.e. n-2).

12.11 We aren't responsible for any delay or increase in cost as a result of you not doing anything you have to do. It may also mean that we can't provide your chosen Services at all.

13 WARRANTIES AND LIABILITY

13.1 We don't offer a voluntary warranty against defects for equipment, but we use reasonable endeavours to pass on the benefit of any manufacturer's warranties applicable to the equipment. The Australian Consumer Law may also provide rights in relation to equipment you buy from us.

13.2 If the equipment is faulty during the term, you must call our telephone service desk to let us know.

13.3 Except where otherwise provided by law, you're responsible for the costs associated with claiming under this clause.

13.4 Subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we aim to, but can't guarantee, that the Managed Security Services will produce particular results or outcomes for you (such as achieving external certification, accreditation or industry standards). In particular, internet policies and security can't detect every possible limitation or fraudulent activity, and subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, we can't guarantee that your systems will operate in an error-free way, or that they'll be safe from malicious attack.

13.5 You have to assess whether any of our recommendations are appropriate for you before you implement them or ask us to implement them for you.

Risks and permissions

13.6 You acknowledge that:

(a) subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, the Managed Security Services may result in interruptions, loss and damage to you, including to your computer systems, networks, websites, software, hardware, internet connections and data;

(b) subject to the Australian Consumer Law provisions in the General Terms of Our Customer Terms, security testing is inherently risky and carried out over public networks, which may result in unexpected outcomes like system crashes or the inadvertent disclosure of information;

(c) as part of some of the Managed Security Services, we actively attempt to breach security controls and gain access to your systems, which may be criminal activity if we did it without your permission, so you are giving us that permission throughout the term of the Managed Security Services;

(d) if any of our activities are reported to an external body or authority, you'll do everything necessary to make sure that body is aware you authorised the activities involved in the Managed Security Services; and

(e) our services are based on information you give us and the infrastructure you have in place at the time we perform the Managed Security Services.

14 INTELLECTUAL PROPERTY RIGHTS

14.1 We own all intellectual property rights in any material we develop for you in carrying out the Managed Security Services (including in any reports or materials generated or provided to you as part of your Vulnerability Management service).

14.2 Where we have designed your service we own all intellectual property rights connected with the design, including in the network diagrams, management IP addresses and equipment configurations (**Items**).

14.3 We grant you a licence to use the Items solely for the purpose of your service. The licence ends on expiry or termination of your relevant service.

14.4 The network diagrams and other information that we supply you with your service is confidential information to us. You must ensure that you keep the network diagrams and other information confidential. You may only disclose the network diagrams and other information in your business for the purposes of using your service (unless you have our prior written consent to do otherwise).

15 CHARGES

15.1 The charges for the Security Intelligence and Managed Next Generation Firewall bundle services are available on application, and the charges for the Managed Firewall service and Managed IPS service are set out in your application form. All charges are exclusive of GST.

15.2 We'll tell you the pricing for optional services when you request them.

15.3 You have to pay us the charges at the times set out in your application form, or if no time is set out, then before we start providing the service.

Annual CPI Adjustment

15.4 This clause applies if you sign up to or recontract your Managed Security Service on or after 21 February 2024 and the service has a minimum term of 12 months or longer:

(a) The prices for the service will remain fixed during the first 12 months from the commencement of the minimum term (**Start Date**).

(b) At any time after the first 12 months, we may, by giving you reasonable advance notice, increase the prices for the 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.

16 MANAGED NEXT GENERATION FIREWALL BUNDLE SERVICE REQUESTS

16.1 As part of the Managed Next Generation Firewall bundle Service, we allow you to make certain service requests, as set out in the table below.

Features	Enhanced	Enhanced Plus
Simple Policy or Configuration Changes	2 per Month	4 per month
Complex Policy or Configuration Changes	Not included	1 per month
Emergency Simple Policy or Configuration Changes	1 per month	1 per month
Dynamic routing	Available as an option at additional cost	Available as an option at additional cost
Out of band management access to the device console port	Available as an option at additional cost	Available as an option at additional cost

16.2 All service requests must be submitted through the Telstra Security Portal.

16.3 If you make:

(a) service requests in excess of the permitted numbers set out above;

(b) an unreasonable number of service requests (in our reasonable opinion); or

(c) a service request that is listed as an option available at additional cost,

we will charge you an additional amount for each such request at our then-current rates.

16.4 If you request:

(a) a Simple Policy Change and we determine the work is out of scope, your request will be treated by us as a Complex Change Request, or otherwise as a project and a quote will be provided to you; or

(b) a Complex Policy Change and we determine the work is out of scope, your request will be treated as a project by us and a quote will be provided to you.

16.5 If you do not implement out of band management, we may not be able to meet our service level targets to resolve incidents.

16.6 All service requests are subject to the technical capability of your equipment. If your equipment doesn't support a particular request, we may not be able to implement it, or may not be able to meet our service target in implementing it.

17 SECURITY INTELLIGENCE SERVICE LEVELS

17.1 The level of service you receive for Security Intelligence service depends on the service tier you select.

17.2 We try to meet the following service level targets when providing the Security Intelligence service. They are estimates only and we're not liable to you if we don't meet them.

Item	Description	Service target

		Enhanced	Enhanced Plus
Automatic email alert of Security Event	How long it takes us to notify you that a security ticket has been created in the Telstra Security Portal.	30 mins	15 mins
Security Event notifications	How long it takes us to notify you by phone of your Security Event after we identify the Security Event	Security Event - Priority One: 60 mins Security Event - Priority Two (if appropriate) - 60 mins	Security Event - Priority One: 60 mins Security Event Priority Two (if appropriate) - 60 mins

18 MANAGED NEXT GENERATION FIREWALL BUNDLE SERVICE LEVELS

18.1 The level of service you receive for the Managed Next Generation Firewall bundle service depends on the service tier you select.

18.2 We try to meet the following service level targets when providing the Managed Next Generation Firewall bundle service. They are estimates only and we're not liable to you if we don't meet them.

Item	Description	Service target	
		Enhanced	Enhanced Plus
Initial response time for faults reported via the service desk	Measured from when you report a fault to when we respond.	Severity 1 - 30 minutes Severity 2 - 30 minutes Severity 3 - 30 minutes Severity 4 - 2 hours	Severity 1 - 30 minutes Severity 2 - 30 minutes Severity 3 - 30 minutes Severity 4 - 60 minutes
Initial response time for system generated faults	Measured from when you report a fault to when we respond.	Severity 1 - 30 minutes Severity 2 - 30 minutes Severity 3 - 30 minutes Severity 4 - 2 hours	Severity 1 - 30 minutes Severity 2 - 30 minutes Severity 3 - 30 minutes Severity 4 - 60 minutes

Item	Description	Service target	
		Enhanced	**Enhanced Plus**
Service restoration	Measured from when a fault is reported to when the fault is resolved.	Severity 1 – 90% restored (or work around) in 18 hours Severity 2 – 90% restored (or work around) in 24 hours Severity 3 – 90% restored (or work around) in 48 hours Severity 4 – 90% restored (or work around) in 72 hours	Severity 1 – 95% restored (or work around) in 6 hours Severity 2 – 95% restored (or work around) in 12 hours Severity 3 – 95% restored (or work around) in 24 hours Severity 4 – 95% restored (or work around) in 72 hours
Progress updates	Measured from when we last updated you on the issue.	Severity 1 – every 4 hours Severity 2 – every 12 hours Severity 3 – every 24 hours Severity 4 – every 72 hours	Severity 1 – every 1 hour Severity 2 – every 3 hours Severity 3 – every 8 hours Severity 4 – every 24 hours
Faulty hardware replacement (for equipment that you bought or rent from us)	Measured from when we determine that the part is faulty.	4 hours on-site	4 hours on-site
Telstra Security Portal availability	Measured as when the portal is available for normal use.	99.9%	99.9%
Simple Policy Change request acknowledgement	Measured from when you request the change through the online portal until we acknowledge the policy change.	2 hours	2 hours
Simple Policy Change request implementation	Measured from when we acknowledge your request for policy change until we tell you we've	24 hours	8 hours

Item	Description	Service target	
		Enhanced	Enhanced Plus
	implemented the change.		
Simple Emergency Policy Change implementation	Measured from when we acknowledge your emergency policy change until we tell you we've implemented the change.	NA	2 hours
Device outage notification	How long it takes us to tell you your firewall service is not available after we determine that is the case.	30 mins	15 mins
Device health alerting (degraded performance)	How long it takes us to tell you your firewall service has degraded performance.	60 mins	60 mins
Security Event Alert Notifications	How long it takes us to respond to your security event after we identify the security incident.	30 mins	15 mins

19 MANAGED FIREWALL AND MANAGED IPS SERVICE REQUESTS

19.1 As part of the Managed Firewall service and the Managed IPS service, we allow you to make certain service requests, as set out in the table below.

Features	Responsive	Proactive
Managed Firewall and Managed IPS		
Simple Policy or Configuration Changes(changes per month)	2	Any reasonable number
Complex Policy or Configuration Changes (changes per month)	Not applicable	2
Emergency Simple Policy or Configuration Changes (changes per month)	Not applicable	1

Features	Responsive	Proactive
Managed Firewall and Managed IPS		
Out of band management access to the device console port	Available as an option at additional cost	Available as an option at additional cost
Managed Firewall only		
Site-to-Site VPN	2 tunnels	Any reasonable number
Client-to-Site VPN (IPSEC/SSL)	N/A	Any reasonable number

19.2 All service requests must be submitted through the Telstra Security Portal.

19.3 If you make:

(a) service requests in excess of the permitted numbers set out above;

(b) an unreasonable number of service requests (in our reasonable opinion); or

(c) a service request that is listed as an option available at additional cost,

we will charge you an additional amount for each such request at our then-current rates.

19.4 If you do not implement out of band management, we may not be able to meet our service level targets to resolve incidents.

19.5 All service requests are subject to the technical capability of your equipment. If your equipment doesn't support a particular request, we may not be able to implement it, or may not be able to meet our service target in implementing it.

20 MANAGED FIREWALL AND MANAGED IPS SERVICE LEVELS

20.1 The level of service you receive for Managed Firewall and Managed IPS services depends on the service tier you select.

20.2 We try to meet the following service level targets when providing the Managed Firewall and Managed IPS services. They are estimates only and we're not liable to you if we don't meet them.

Item	Description	Service target	
		Service Tier - Responsive	**Service Tier - Proactive**
Initial response time for faults reported via the service desk	Measured from when you report a fault to when we respond.	Severity 1 - 30 minutes Severity 2 - 30 minutes	Severity 1 - 30 minutes Severity 2 - 30 minutes

Item	**Description**	**Service target**	
		Service Tier - Responsive	**Service Tier - Proactive**
		Severity 3 - 30 minutes Severity 4 - 2 hours	Severity 3 - 30 minutes Severity 4 - 60 minutes
Initial response time for system generated faults	Measured from when you report a fault to when we respond.	Severity 1 - 30 minutes Severity 2 - 30 minutes Severity 3 - 30 minutes Severity 4 - 2 hours	Severity 1 - 30 minutes Severity 2 - 30 minutes Severity 3 - 30 minutes Severity 4 - 60 minutes
Service restoration	Measured from when a fault is reported to when the fault is resolved.	Severity 1 – 90% restored (or work around) in 18 hours Severity 2 – 90% restored (or work around) in 24 hours Severity 3 – 90% restored (or work around) in 48 hours Severity 4 – 90% restored (or work around) in 72 hours	Severity 1 – 95% restored (or work around) in 6 hours Severity 2 – 95% restored (or work around) in 12 hours Severity 3 – 95% restored (or work around) in 24 hours Severity 4 – 95% restored (or work around) in 72 hours
Progress Updates	Measured from when we last updated you on the issue.	Severity 1 – every 4 hours Severity 2 – every 12 hours Severity 3 – every 24 hours Severity 4 – every 72 hours	Severity 1 – every 1 hour Severity 2 – every 3 hours Severity 3 – every 8 hours Severity 4 – every 24 hours

Item	Description	Service target	
		Service Tier - Responsive	**Service Tier - Proactive**
Faulty hardware replacement (for equipment that you bought or rent from us)	Measured from when we determine that the part is faulty.	Next business day	4 hours
Telstra Security Portal availability	Measured as when the portal is available for normal use.	99.9%	99.9%
Simple Policy Change Request Acknowledgement	Measured from when you request the change through the online portal until we acknowledge the policy change.	2 hours	2 hours
Simple Policy Change Request Implementation	Measured from when we acknowledge your request for policy change until we tell you we've implemented the change.	24 hours	8 hours
Simple Emergency Policy Change Implementation	Measured from when we acknowledge your emergency policy change until we tell you we've implemented the change.	NA	2 hours
Device Health Alerting	How long it takes us to tell you your firewall service is not available after we determine that is the case.	30 mins	15 mins
Security Event Alert Notifications	How long it takes us to respond to your Security Event after we identify the Security Event.	30 mins	15 mins

20.3 The timeframes are suspended while we're waiting for you to provide us with information or access to your equipment or sites, or for any matter outside our reasonable control.

21 TELSTRA SECURITY PORTAL

21.1 We provide you with access to the Telstra Security Portal so you can use the services.

21.2 Your use of the Telstra Security Portal is subject to any separate terms of use that apply to it from time to time.

22 TERM AND TERMINATION

22.1 We provide your Managed Security Services for the period you nominate in your application form, unless terminated earlier in accordance with this clause.

22.2 The minimum term for each component of your Managed Security Service is 12 months (or the longer period set out in your application form).

22.3 The minimum term:

(a) is separate for each Managed Security Service; and

(b) must be the same as the period you have rented equipment from us (if applicable).

22.4 After the minimum term:

(a) your Managed Security Service continues until terminated; and

(b) either you or we may terminate your Managed Security Service in whole or in part by giving at least 30 days written notice.

22.5 Where you rent equipment from us after the minimum term, you may:

(a) keep renting the equipment from us;

(b) give the equipment back to us; or

(c) if we agree, buy it from us (we'll tell you the price when you ask us).

22.6 If you or we terminate your Managed Security Service during the minimum term for any reason other than our material breach or our inability to support your equipment (except where we can't support your equipment because you haven't maintained the firmware or software to the required currency, in which case this clause does apply), you have to:

(a) pay us the early termination charges for that Managed Security Service; and

(b) pay the full amount of all rental payments that you'd have made during the term of your rental agreement with us for that equipment. In exchange for making those payments, we'll give you title in the equipment.

22.7 The early termination charges for the Managed Security Service and Internet Protection Services are equal to the actual costs and expenses that we have incurred or committed to in anticipation of providing the service to you and that cannot be reasonably avoided by us as a result of the cancellation, which will not exceed an amount calculated as follows:

For Managed Next Generation Firewall bundle, Cyber Detection and Preseason-Endpoint and Internet Protection Services:

ETC = (A x B) x 80%

For other Managed Security Services:

ETC = (A x B) x 50%

where:

A = number of months remaining in minimum term for the terminated service (as set out in your application form)

B = the monthly charge for the terminated service (as set out in your application form)

22.8 You acknowledge the early termination charges are a genuine pre-estimate of the loss we'd suffer if you terminated early.

22.9 We can terminate any or all of your Managed Security Services if you cause a defect or incident by accidental damage, or improper or negligent use of the equipment or the network, or you don't maintain the currency of the firmware or software on your equipment as required by clause 10.10. You have to pay early termination charges if we terminate your Managed Security Service under this clause.

22.10 We can terminate your Managed Security Service in respect of a particular device in accordance with the General Terms of Our Customer Terms.

22.11 If you rent a device from us, we can suspend or cancel your service in accordance with the General Terms of our Customer Terms.

23 SPECIAL MEANINGS

23.1 The following words have the following special meanings:

Complex Configuration Change means a change to the configuration that isn't:

(a) a policy change of any kind;

(b) a Simple Configuration Change; and

(c) in our reasonable opinion, a fundamental change to the nature of the service (which would be an early termination).

Complex Policy Change means one of the following policy change requests:

(a) ten or more access control list and or policy rules, with ten or more objects, with five or more network address translation and or port address translation modifications;

(b) changes over two or more devices for single services;

(c) four or more VPN tunnel changes/configurations for new and existing VPNs;

(d) four or more VPN client/account modifications for new and existing VPNs;

(e) four or more signature changes for IPS modules;

(f) interface configuration changes (changing the IP address on the Interface, as it may impact the policy); or

(g) internet service provider changes, where the IP address has changed.

Emergency Policy Change means a change with ten or fewer Access Control Lists and or Policy Rules, with ten or fewer objects, which you tell us is an emergency change.

Incident means a Security Event that we consider poses a real risk to your systems or environment.

Managed Firewall means the service described in clause 5.

Managed IPS means the service described in clause 7.

Responsibilities Guide means the guide we publish that sets out your responsibilities regarding the Managed Security Services, as updated from time to time.

Security Event means an observable change to the normal behaviour of your system, environment, process, workflow or person occurrence that may pose a security risk to your systems or environment.

Security Event – Priority One has the meaning given to it in clause Error! Reference source not found..

Security Event – Priority Two has the meaning given to it in clause Error! Reference source not found..

Security Event – Priority Three has the meaning given to it in clause Error! Reference source not found..

Severity 1 Incident means an Incident where your service is not available at a site (or multiple sites) causing critical impact to business operations.

Severity 2 Incident means an Incident where your service is not available, or severely degraded, impacting significant aspects of business operations.

Severity 3 Incident means an Incident where your service is degraded. Customer service is noticeably impaired but most business operations continue.

Severity 4 Incident means all other Incidents that are not Severity 1, 2 or 3 Incidents.

Simple Configuration Change means any of the following changes:

(a) **Access List changes** – changes to the denial or permission of certain IP address range/s or applications on a router or switch device;

(b) **Device Interface changes** – changes to the interface on a router (which provides the network connectivity to the router);

(c) **Device Management Access changes** – changes to the network protocol for collecting IP traffic information from specified network devices; or

(d) **Dynamic Host Configuration Protocol (DHCP) changes** – changes to the automation of the assignment of IP addresses, subnet masks, default gateway, and other IP parameters,

but only if the change doesn’t involve a change to a policy.

Simple Policy Change means one of the following policy change requests:

(a) ten or fewer access control lists and or policy rules, with ten or fewer objects, including up to five network address translation and or port address translation modifications;

(b) up to three site to site VPN tunnel configuration changes for new and existing VPNs;

(c) up to three clients to Site VPN tunnel configuration changes for new and existing VPNs;

(d) up to three signature changes for Managed IPS.

SOC or **Security Operations Centre** means Telstra’s security operations centre.