OUR CUSTOMER TERMS
SECUREEDGE SERVICES

CONTENTS

OUR CUSTOMER TERMS SECUREEDGE SERVICES

1 APPLICABLE TERMS

1.1 This is the SecureEdge section of Our Customer Terms.

1.2 Unless you have a separate agreement with us which excludes them, the General Terms of Our Customer Terms apply to the provision of SecureEdge services.

1.3 Certain words are used with the specific meanings set out in this section or in the General Terms of Our Customer Terms.

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

1.5 If a provision of this SecureEdge 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 SECUREEDGE

What is SecureEdge?

2.1 SecureEdge is a collection of security services designed to restrict malicious or unwanted data traffic in or out of your network.

2.2 Each SecureEdge service provides you with a virtualised next generation firewall solution.

2.3 The available SecureEdge services are:

(a) SecureEdge Network; and

(b) SecureEdge Managed Services (SEMS).

2.4 The SecureEdge services aren't available to Telstra Wholesale customers or for resale.

3 GENERAL

3.1 Other than as expressly stated in this section, we do not monitor or manage any of your other services, including any of your other products or services as part of your SecureEdge service.

3.2 We will use due care and skill to provide the SecureEdge services but we do not promise or guarantee that your SecureEdge service will prevent or detect all unauthorised access or breaches to/from your network.

3.3 You are responsible for ensuring that you comply with the licence terms of any software (such as application software or operating system) which you install or use in connection with your SecureEdge service.

3.4 Your use of any Palo Alto Networks software as part of a SecureEdge service, your use is subject to your acceptance of and compliance with the Palo Alto Networks EULA, a copy of which can be found at: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/palo-alto-networks-end-user-license-agreement-eula.pdf

3.5 You may be given a high degree of control over your firewall and security configuration and policies. If you configure and manage your SecureEdge service in such a manner that causes disruption to your service and/or deletion of any of your data, you will be responsible for any loss that you suffer as a result and you may need to pay us an additional charge to rectify any problems.

3.6 You acknowledge and agree that we, and the third party vendors, will need to have management access to your SecureEdge service to perform any installation, configuration, monitoring or other tasks that are necessary to supply the service to you.

3.7 We will carry out your firewall policy configuration requests as instructed but we will not advise on the merits of the request or the potential consequences of implementing the request. You agree and acknowledge that any and all firewall policy configurations, remain your sole responsibility. You further acknowledge and agree that we accept no liability whatsoever, either consequential or direct that may arise from those policy configurations.

User Interface

3.8 We will provide you with access to an online user interface at https://telstra.com.au/secureedge to configure, manage or request reports on your SecureEdge service ("**User Interface**"). If required, we will provide you with means of authentication to enable you to access the User Interface. We recommend that you use multi factor authentication to access the User Interface.

3.9 All standard tier self-managed firewall policy configurations will be applied to the firewall via the User Interface. You will not have access to the underlying firewall management console or web interface.

Term

3.10 We provide your SecureEdge service for the period you nominate in your application form, unless terminated earlier in accordance with this clause.

3.11 The minimum term for each component of your SecureEdge service is 12 months (or the longer period set out in your application form).

3.12 The minimum term is separate for each SecureEdge service.

3.13 After the minimum term:

(a) your SecureEdge service continues until terminated; and

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

3.14 You need to agree to a new minimum term if you want to modify your SecureEdge service. We will waive the once-off connection fee but you may be charged an early termination charge if you reduce the size or otherwise downgrade your existing SecureEdge service.

Termination

3.15 If you or we terminate or downgrade your SecureEdge service during the minimum term for any reason other than our material breach you have to pay us the early termination charges for that SecureEdge service.

3.16 The early termination charges for the SecureEdge service are calculated as follows:

ETC = (A x B) x 55%

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)

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

3.18 We can terminate any or all of your SecureEdge 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 allow us access to your SecureEdge service so we can maintain the currency of the firmware or software. You have to pay early termination charges if we terminate your SecureEdge service under this clause.

3.19 We can terminate your SecureEdge service in respect of a particular feature if we no longer support that feature, by giving you at least 30 days written notice. You do not have to pay early termination charges if we terminate under this clause.

4 SECUREEDGE NETWORK

What is SecureEdge Network?

4.1 SecureEdge Network is a cloud based next generation firewall that provides you with a security gateway for your Telstra IP WAN, IP MAN, or Connect IP service ("Next IP Service").

4.2 The SecureEdge Network product provides a range of security features based on the package selected by you in accordance with your application form or other agreement with us. Details of the features included in each package can be found in your application form.

Eligibility

4.3 You will need to have a Next IP Service for your SecureEdge Network service.

Connection type

4.4 You must select one of these Connection types for your SecureEdge Network service:

(a) Internet connection; or

(b) Extranet connection

Internet connection

4.5 The SecureEdge Network Internet connection provides connectivity from your Next IP Service to the internet.

4.6 You must not use the SecureEdge Network Internet connection in a way that is excessive or unreasonable.

4.7 We consider excessive use to be usage which exceeds 300GB per month. If you exceed this amount, we reserve the right to charge you and will notify you of any applicable charges.

4.8 We consider it unreasonable use if you use the SecureEdge Network Internet connection fraudulently or in a manner that causes significant network congestion. Fraudulent use of the SecureEdge Network Internet connection includes resupplying it without our consent so a third party can take advantage of the SecureEdge Network Internet connection.

Extranet connection

4.9 The SecureEdge Network Extranet connection provides connectivity of your Next IP Service to other organisations that also have a Next IP NetworkService with us via that other customer's SecureEdge Network Extranet connection. You must have the consent of the other organisation before requesting an Extranet connection.

Limitations

4.10 We may limit from time to time the number of IP addresses you may use with your SecureEdge Network service. We will let you know if we are going to apply a limit to your IP addresses before we do so.

4.11 You acknowledge that you are responsible for providing us with information so that we can configure your SecureEdge Network service. Once we have provided you with your SecureEdge Network service, you will have the ability to change the configuration. You will be responsible for any changes to the configuration that you request or make.

4.12 If we provide you with a report as part of your SecureEdge Network service, then you acknowledge that the report should be used as a guide only. We will not be responsible for loss which you suffer as a result of relying on the report.

Service Levels

4.13 The available service levels for SecureEdge Network are set out in the table below.

Service Level	**Service Level Grade**	
Service Support Coverage Hours	24 hours x 7 days	
Incidents	**Incident Response Time**	**Incident Restore Time**
Severity 1	30 minutes	4 hours
Severity 2	60 minutes	6 hours
Severity 3	120 minutes[1]	8 hours[1]
Severity 4	180 minutes[1]	24 hours[1]

[1] We only accept responsibility for a failure to meet this service level if the Incident relating to the relevant product occurs between 7am and 7pm on a business day.

Service Level Exclusions

4.14 We are not responsible for a failure to meet a service level where:

(a) the failure is caused due to the corruption of data as part of a backup;

(b) you failure to comply with a request from us to maintain sufficient storage capacity for your virtual disks provided under your Storage feature under the Infrastructure part of the Cloud Services section;

(c) you have accessed the SecureEdge service by any other means not agreed with Telstra.

5 SECUREEDGE MANAGED SERVICE (SEMS)

What is SecureEdge Managed Service (SEMS)?

5.1 The SecureEdge Managed Service (SEMS) service implements modifications to your eligible security services based on your request.

Availabilty

5.2 The following security services are eligible for SEMS:

SecureEdge Network

5.3 The different types of security policy and configuration changes than can be requested for:

(a) SecureEdge Network are:

(i) Security Zones

(ii) IP addresses

(iii) NAT/PAT

(iv) Security objects

(v) AppID filter rules

(vi) Data blocking rules

(vii) File filtering rules

(viii) URL filtering rules

(ix) SSL/IPSec VPN

(x) AV/IPS

Limitations

5.4 Any SEMS requests must be applicable to and compatible with your security service and are limited to the technical features of your security service.

5.5 We will carry out your SEMS request as instructed and will not advise on the potential consequences of implementing the request.

5.6 We are not responsible for any impacts to applications that we have not provided to you as part of the SEMS service as a consequence of completing your SEMS request.

5.7 We allow you to make a SEMS requests, as set out in the Responsibilities Guide, a copy of which will be provided to you.

5.8 All SEMS requests must be submitted via the SecureEdge User Interface.

5.9 If you make:

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

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

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

5.10 If you request:

(a) a Simple Policy/Configuration 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/Configuration 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.

Service Levels

5.11 The table below sets out the service level targets for implementing your change requests.

Item	Description	Service Target
Simple Policy / Configuration Change request acknowledgement	Measured from when you request the change through the online portal until we acknowledge the policy / configuration change.	2 hours
Complex Policy / Configuration Change request implementation	Measured from when we acknowledge your request for policy/configuration change until we tell you we've implemented the change.	8 hours
Simple Emergency Policy / Configuration Change implementation	Measured from when we acknowledge your emergency simple policy change until we tell you we've implemented the change.	2 hours

6 SECUREEDGE SERVICE LEVELS

6.1 These service levels apply to all SecureEdge services unless otherwise stated.

Provisioning and Changes service levels

6.2 The provisioning and change service levels 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

6.3 Our provisioning and change service levels 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 validated all of your requirements that we need to provide the SecureEdge 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.

Service availability service level

6.4 The monthly service availability service level is:

Item	Description	Service level target
Availability of the User Interface for the SecureEgde service	Calculated per calendar month	99%
Availability of the SecureEdge service (excluding the Telstra Security Portal)	Calculated per calendar month	97%
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 Security Monitoring platform in the month.

Fault reporting service level

6.5 The fault reporting service level is:

Item	Description	Service level target
Service restoration	Measured from when a fault is reported to when the fault is resolved	Severity 1: 90% restored (or work around) in 12 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
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 48 hours Severity 4: every 72 hours

Scheduled & Emergency Maintenance

6.6 We may perform scheduled maintenance on your SecureEdge service, which may cause your Services to be temporarily unavailable.

6.7 We aim (but do not guarantee) to give you reasonable notice before performing such scheduled maintenance. We can do this by posting information on the SecureEdge portal, or by sending an e-mail to the person you have nominated as your technical contact.

6.8 However, we reserve the right to instigate emergency security or maintenance procedures and updates, to address urgent or critical issues without notice, if required to protect our customers and the SecureEdge services.

Service credits

6.9 If we do not meet the service level targets in this clause 6, 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.

6.10 After we receive your request under clause 6.9, 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 Security Monitoring 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 Security Monitoring 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 6 and your request for the applicable service credit is your only remedy for our failure to do so.

6.11 Any rebate will be applied to your Telstra bill (at the end of the billing cycle).

Service Level exclusions

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

(a) you fail to follow our reasonable directions to avoid or remedy an Incident;

(b) you do not provide us with full and accurate information detailing any requests or relating to any Incidents that you report to us;

(c) scheduled or emergency maintenance;

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

(e) any third party act or omission;

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

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

(h) 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

(i) 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).

7 SPECIAL MEANINGS

7.1 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.

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

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 IPS.