OUR CUSTOMER TERMS
CLOUD SERVICES – SECURITY

CONTENTS

OUR CUSTOMER TERMS
CLOUD SERVICES – SECURITY

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

1 APPLICABLE TERMS

1.1 In addition to this Cloud Infrastructure Section of Our Customer Terms, unless we agree otherwise, the following terms also apply:

(a) General Terms of Our Customer Terms (see http://www.telstra.com.au/customer-terms/business-government/index.htm); and

(b) General Terms of the Cloud Services section (see https://www.telstra.com.au/customer-terms/business-government#cloud-services); and

(c) other parts of the Cloud Services section, depending on the nature of the products and services that you receive from us.

1.2 For an explanation of the interrelationship between the various sections of Our Customer Terms see clause 1 of the General Terms of the Cloud Services section at the link above.

2 GENERAL

2.1 We do not monitor or manage any of your other services, including any of your other products or services provided under the Cloud Services section as part of your Security product.

2.2 Your options for configuring your Security products are set out on the Cloud Services portal at https://cloud.telstra.com/, or in your application form or other agreement with us.

2.3 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 Security products.

2.4 You may be given a high degree of control over your Security configuration and management. If you configure and manage your Security product 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 fix any problems.

3 SECURITY

3.1 The following table sets out the availability of the Security products you can apply for in connection with your Cloud Services products.

Service	Public Network	Private Network
Cloud Infrastructure Gen1 compute Services		
Internet Protection Services	✓	N/A
Denial of Service Protection	✓	N/A
Firewall (Virtual)	✓	✓
IPSEC VPN	✓	N/A
Vulnerability Discovery	✓	✓
SSL VPN	N/A*	N/A
Cloud Infrastructure Gen2 compute Services		
Denial of Service Protection	✓	N/A
Firewall (virtual)	✓	✓
IPSEC VPN	✓	N/A
Vulnerability Discovery	✓	✓
SSL VPN	N/A	✓
Gateway Protection Advanced	✓	✓

** SSL VPN is available but only for managing Cloud Infrastructure servers*

4 INTERNET PROTECTION SERVICES

4.1 The Internet Protection Services provides security features for email and/or web traffic across your network.

4.2 The terms and conditions for the Internet Protection Services are set out in Part D (Internet Protection Services) of the Internet Solutions section at http://www.telstra.com.au/customer-terms/business-government/internet-services/internet-solutions/.

5 DENIAL OF SERVICE PROTECTION

5.1 The Denial of Service Protection service is designed to filter certain network traffic in our network to assist you in managing the potential impact of distributed denial of service and other agreed attacks which may impact your Internet data service. The Denial of Service Protection service does this by comparing network traffic flows to your Data service based on agreed profiles of normal traffic patterns, behaviour and protocol compliance.

5.2 We do not guarantee that the Denial of Service Protection service will prevent all attacks against your Internet data service. In particular, the service may not provide any protection or assistance to you arising out of an attack to your Internet data service if:

(a) the distributed attack is an application level attack that is not detectable from traffic flows and not threatening the capacity of your Data service; or

(b) the attack occurs during the four week period immediately following the activation of the Service as the Service is adapting to the appropriate network traffic profiles during this period.

5.3 The Denial of Service Protection service is designed to limit network traffic to the Internet data service. If the service detects an attack, then you acknowledge and agree that:

(a) certain network traffic may be blocked from reaching the Internet data service or discarded in our network; and

(b) your use of the Internet data service may be degraded due to network congestion or other related effects.

5.4 You acknowledge that if data traffic volumes from attacks being mitigated by the Denial of Service Protection service exceed or are expected to exceed the capacity of the Denial of Service Protection service then, in order to maintain availability for the majority of your users, further filtering of attack traffic may be implemented at peering points and by network providers carrying traffic before it reaches our networks and this filtering may increase the level of legitimate traffic blocked.

5.5 We are not responsible for any loss that you suffer as a result of the Denial of Service Protection service blocking or limiting Data traffic due to an attack unless such loss arises as a direct result of our negligence.

6 FIREWALL (VIRTUAL)

6.1 The Firewall service is a security service which is designed to provide you with functionality to assist you in restricting certain access and traffic into your network.

6.2 The Firewall service provides the following features as selected by you in accordance with your application form or other agreement with us, the availability of which may depend on the firewall tier which you select:

(a) back-up of your configuration data;

(b) reporting of traffic volumes, user activity and device performance;.

(c) an ability to make policy or configuration changes;

The following features are no longer available with new Firewall services purchased from 30 June 2016:

(d) data retention / Storage (Logs Files);

(e) site to site VPN connections (depending on your platform selection);

(f) client to site VPN support;

(g) security event monitoring; and

(h) threat analysis and intelligence service.

6.3 We do not promise that the Firewall (Virtual) service will prevent unauthorised access to your network.

6.4 We can only provide the Firewall (Virtual) service for the devices that are managed by us.

7 SSL VPN/IPSEC VPN

7.1 IPSEC VPN allows you to access your shared or dedicated servers over the Public Network via your Dedicated Gateway service using IPSEC tunnelling technology

7.2 SSL VPN allows you to access your shared or dedicated servers over the Public Network via your Dedicated Gateway service using SSL tunnelling technology.

7.3 We do not promise that the SSL/IPSEC VPN service will prevent or detect all unauthorised access to your network.

8 VULNERABILITY DISCOVERY

8.1 The Vulnerability Discovery service provides vulnerability assessments and includes proactive scanning of your network from within to identify and prioritise potential weak points, risk areas and security exposures. As part of your Vulnerability Discovery service we will provide a Vulnerability Discovery report which will set out:

(a) the date of the Vulnerability Discovery scan;

(b) the scope of the Vulnerability Discovery scan;

(c) an inventory of hosts, operating systems and applications;

(d) a list of vulnerable hosts;

(e) the types of vulnerability detected; and

(f) an explanation of the risk for vulnerabilities detected.

9 GATEWAY PROTECTION ADVANCED

What is Gateway Protection Advanced?

9.1 The Gateway Protection Advanced product is designed to provide you with a managed virtualised next generation firewall appliance on your Cloud Infrastructure Virtual Server (dedicated) Gen2 product.

9.2 The Gateway Protection Advanced product provides the following features based on the package selected by you in accordance with your application form or other agreement with us:

	Essentials	Enhanced	Premium
Size			
Small	✓	✓	✓
Medium	✓	✓	✓
Large	N/A	N/A	N/A
Features			
High Availability	Active / Passive	Active / Passive	Active / Passive
Palo Alto Network (PAN) Features			
Next Generation Firewall	✓	✓	✓
SSL VPN	✓	✓	✓
IP Sec Site to Site Tunnelling	N/A	✓	✓
Threat Prevention (Anti Virus, IDS/IPS)	N/A	✓	✓
Zero day protection	N/A		✓
URL Filtering	N/A	✓	✓
Mobile (Smart Device) Security^	N/A	N/A	✓

^Only available for Gateway Protection Advanced services acquired from 1 March 2017

9.3 We do not promise that the Gateway Protection Advanced product will prevent unauthorised access to your network.

9.4 We can only provide the Gateway Protection Advanced product for the devices that are managed by us.

9.5 You acknowledge and agree that Telstra will have to deploy a virtual appliance software image running as VM instance in your Cloud Infrastructure Virtual Server (dedicated) Gen2 product in order to supply the Gateway Protection Advanced product to you.

9.6 You acknowledge and agree that Telstra will need to have management access to your Cloud Infrastructure Virtual Server (dedicated) Gen2 product to perform any installation, configuration, monitoring or other tasks that are necessary to supply the Product to you.

9.7 You agree you will not use any Telstra-provided or other cloud management access / tools to access, download , copy, store, archive any components that is installed for the purpose of providing the Gateway Protection Advanced product to you.

9.8 If we require access to install devices in connection with your Gateway Protection Advanced product, you agree to provide us, or our subcontractors, with access to your premises and utility sources. We, and our subcontractors, will whilst on your premises comply with any applicable health, safety or security regulations or policies that you notify us of which are applicable to those premises.

Eligibility

9.9 You will need the following products for your Gateway Protection Advanced product.

(a) a Cloud Infrastructure Virtual Server (dedicated) Gen2 product

(b) a Public Network Internet service

(c) a Cloud Direct Connect Gateway (Next IP connectivity) service

Minimum term

9.10 You must acquire the Gateway Protection Advanced product for the minimum term set out in your application.

9.11 If your Gateway Protection Advanced product is terminated for any reason, other than our material breach, we may charge you an early termination fee calculated as:

A x B x 55%

Where:

"A" = the monthly recurring charges for your Gateway Protection Advanced product.

"B" = the number of months (or part of a month) remaining in your minimum term.

User Interface

9.12 We will provide you with access to an online user interface to configure, manage or request reports on your Gateway Protection Advanced product ("**User Interface**"). If required, we will provide you with means of authentication to enable you to access this online tool. We recommend that you use 2-factor authentication to access the User Interface.

9.13 We will endeavour to inform you of an emergency event or any maintenance that may materially affect the Gateway Protection Advanced product by posting an alert message on the User Interface.

Service Levels

9.14 The available service levels for Gateway Protection Advanced are set out in the table below.

Service Level	**Service Level Grade**	
	Bronze	
Service Support Coverage Hours	24 hours x 7 days	
Incidents	**Incident Response Time**	**Incident Restore Time**
Severity 2 An outage of your Gateway Protection Advanced product	60 minutes	4 hours
Severity 3 Partial failure of your Gateway Protection Advanced product leading to increased risk or reduced capacity	120 minutes[1]	8 hours[1]
Severity 4 Notable incident that does not impact your Gateway Protection Advanced product	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

9.15 In addition to the service level exclusions in the General Terms for Cloud Services, 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) the failure relates to your operation of an application on our service platform, as part of a product under the Cloud Services section, which is not version "n-1" or later.

(d) you have accessed the Gateway Protection Advanced product by any other means not agreed with Telstra.

Service Level Rebates

9.16 If we fail to meet the Service Availability service level set out in the table above for your Gateway Protection Advanced product, you may apply for a rebate in accordance with this clause.

9.17 Except where the failure to meet the service level is caused by you, in each monthly period in which the actual Incident Response and Incident Restore times are greater than the target Incident Response and Incident Restore times for your Gateway Protection Advanced product, you may apply for a rebate of five percent (5%) of your monthly fee for each 30 minute block exceeding the target Incident Response and Incident Restore times up to a maximum of 100% of your monthly fee for the impacted Gateway Protection Advanced product.

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

10 POLICY CONFIGURATION AND CHANGE MANAGEMENT (PCCM)

What is Policy Configuration and Change Management (PCCM)?

10.1 The Policy Configuration and Change Management (PCCM) service implements modifications to your eligible security services based on your request.

Availabilty

10.2 The following security services are eligible for PCCM:

(a) Gateway Protection Advanced

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

(a) Gateway Protection Advanced 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

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

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

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

10.7 We allow you to make a PCCM requests, as set out in the table below

PCCM Change Type		**Quota**
Simple Policy Changes	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	4 per month

	existing VPNs; (d) up to three IPS signature changes.	
Simple Configuration Changes	Means Access List changes – changes to the denial or permission of certain IP address range/s or applications on a router or switch device but only if the change doesn't involve a change to a policy.	4 per month
Complex Policy Changes	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.	1 per month
Complex Configuration Changes	Means a change to the configuration that isn't: (a) a policy change of any kind;	1 per month

	(b) a Simple Configuration Change; and in our reasonable opinion, a fundamental change to the nature of the service (which would be an early termination)	
Emergency Simple Policy / Configuration Changes	Means a simple policy or configuration change related to remediating a serious security incident, breach or vulnerability that is impacting or has a high likelihood of signficiantly impacting the customer's enterprise IT environment	1 per month

10.8 All PCCM requests must be submitted via the GPA User Interface.

10.9 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,

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

10.10 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

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
Simple Policy / Configuration Change request implementation	Measured from when we acknowledge your request for policy/configuration change until we tell you	8 hours

	we've implemented the change.	
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