# OUR CUSTOMER TERMS
# CLOUD SERVICES - NETWORK SERVICES

## CONTENTS

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

## 1 ABOUT THIS PART

1.1 This is the Network Services part of the Cloud Services section of Our Customer Terms. Depending on the nature of the products and services you are receiving under this Cloud Services section, provisions in other parts of the Cloud Services section, as well as in the General Terms of Our Customer Terms at http://www.telstra.com.au/customer-terms/business-government/index.htm, may apply.

1.2 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.

1.3 See section one of the General Terms part of the Cloud Services section for more detail on how the various parts of the Cloud Services section are to be read together.

1.4 As part of your product selection under this Network Services part of the Cloud Services section, we do not monitor or manage any of your other services, including any of your other services provided under the Cloud Services section.

1.5 We capacity-manage the shared core network infrastructure to ensure available bandwidth for all customers to connect to their Cloud Services either via a Public Network or Private Network, but we do not make any representations or guarantees of throughput. The throughput and performance of your Cloud Services will be impacted by a variety of factors including but not limited to load balancers, SSL offloading, proxy servers, firewalls, and other security or networking elements.

## 2 PUBLIC NETWORK

2.1 The Public Network product provides network services required for interoperation with the products set out in the Enterprise Applications, Infrastructure and Data Centres parts, and includes the data services outlined in this "Public Network" section.

### Internet

2.2 If you apply for a Data Centre service, you may acquire a Telstra Internet Direct service for connection to the Internet. The Internet Direct (TID) service provides you with internet access over the public network. The terms and conditions applicable to TID are set out in Part A (Telstra Internet Direct) of the Internet Solutions section of Our Customer Terms.

2.3 If you are applying for an Application (excluding T-Suite applications) or Infrastructure product, internet connectivity is included as a feature of your Application or Infrastructure product. The service level for your internet connectivity is the same as Application or Infrastructure product. Usage charges for internet connectivity are set out in Your Agreement.

### Load Balancing

2.4 You can apply for the following load balancing services:

| **Service** | **Public Network** | | **Private Network** | |
|---|---|---|---|---|
| | Tailored Infrastructure | Cloud Infrastructure | Tailored Infrastructure | Cloud Infrastructure |
| Server Load Balancing | ✓ | ✓* | ✓ | ✓* |
| SSL Offloading | ✓ | x | ✓ | x |
| Geographic Server Load Balancing | ✓^ | ✓^ | x | x |

* *Australian data centres only*
^ *between Sydney and Melbourne data centres only*

### Server Load Balancing

2.5 Server Load Balancing provides a full proxy between users and application servers that creates a layer of abstraction to help secure, optimise, and load-balance traffic.

### SSL Offloading

2.6 This service provides secure sockets layer (SSL) offloading for your Public Network product.

2.7 SSL Offloading is only available with Server Load Balancing.

### Geographic Server Load Balancing

2.8 Geographic Server Load Balancing provides users an enhanced implementation of DNS to spread workload across multiple sites.

## Domain Name Registration

2.9 We offer a domain name registration service. If you ask us to register or renew a domain name on your behalf as part of your service (and we agree to do this for you), these terms apply to you.

2.10 The Domain Name Registration service includes us registering a domain name on your behalf and assisting you with communicating with the relevant registrar of the domain name, where necessary. You acknowledge that we can only register a domain name on your behalf if that domain name is available for use.

2.11 If you request us to register a .com, .net, .org, .biz, or .info domain name ("**TLDs**" or "**Top Level Domains**") on your behalf, the General Registrar Policy located at http://www.tppinternet.com.au/terms-conditions/australian_domains.php is incorporated into this agreement as amended from time to time.

2.12 If you request that we register a .au domain name on your behalf, the policies applicable to .au Domain Name Licences located at http://www.tppinternet.com.au/terms-conditions/gtld-domain-names.php, as amended from time to time and the .au 2LD Domain Name Eligibility and Allocation Policy Rules issued located at http://www.auda.org.au/policies/auda-2005-01/, as amended from time to time are incorporated into this agreement.

2.13 You acknowledge that additional policies relating to your domain name may come into effect from time to time and you agree to comply with such additional policies.

2.14 If there is a dispute regarding the registration or use of your TLD, you agree to:

(a) submit to and be bound by Uniform Domain Name Dispute Resolution Policy located at http://www.icann.org/udrp/udrp.htm as amended from time to time; and

(b) be subject to arbitration, suspension or cancellation by any ICANN procedure, or by any registry administrator procedure approved by ICANN policy, relating to:

(i) the correction of mistakes by us or the registry administrator in registering the domain name; or

(ii) the resolution of disputes concerning the domain name.

2.15 In the event of a dispute in registering a .au Domain, or a dispute about a .au Domain after registration, you will submit to and be bound by the .au Dispute Resolution Policy (auDRP) located at http://www.auda.org.au/policies/auda-2002-22/, as amended from time to time.

2.16 You must pay any registration or delegation charges to us in advance. We cannot register a domain name for you unless you pay for it in advance.

2.17 You authorise and direct us to nominate Telstra Corporation Limited (ABN 33 051 775 556) as the authorised billing contact for your domain name.

2.18 We are not liable for any loss or damage resulting from the non-renewal of your domain name if you fail to provide us with consent to renew the domain name registration or you delay in providing us with such consent.

2.19 You indemnify us against all claims arising out of the registration, use or renewal of your domain name, unless and to the extent that the claim arises out of our breach of this agreement, or our negligent act or omission.

### SMTP Mail Relay

2.20 The SMTP Mail Relay service for the Public Network product provides you with a dedicated mail relay for use with any mail servers that you operate on our service platform.

### DOS & DDOS Protection of Telstra Cloud Services

2.21 In the event of a DOS or DDOS attack directed against a customer service hosted by Telstra we reserve the right take any reasonable steps to protect the hosting compute platform. Unless you are able to activate an effective DOS or DDOS mitigation strategy this may involve *rate limiting* traffic and/or *blacklisting* the source IP addresses or *black-holing* the affected service (removing it from service).

## 3 PRIVATE NETWORK

3.1 The Private Network product provides network services required for interoperation with the products provided under the Enterprise Applications, Infrastructure and Data Centres, and includes the data services outlined in this "Private Network" section.

### Next IP™ services

3.2 If you apply for a Data Centres service, you may apply to use a Telstra connecting carriage service (such as Business IP, Connect IP or IP MAN). The applicable terms and conditions (including price) for your carriage service are set out in the corresponding section of Our Customer Terms.

3.3 If you are applying for an Application (excluding T-Suite applications) or Infrastructure product, Next IP connectivity is included as a feature of your Application or Infrastructure product. The service level for your Next IP connectivity is the same as your Application or Infrastructure product. Usage charges for Next IP connectivity are set out in Your Agreement.

### SMTP Mail Relay

3.4 The SMTP Mail Relay service for the Private Network product provides you with a dedicated mail relay for use with any mail servers that you operate on our service platform.

### VLAN Extension

3.5 VLAN Extension allows you to bridge a private VLAN in Cloud Infrastructure with a private VLAN in another data centre connected to your Next IP network in order to share the same private subnet (also known as a "stretched VLAN").

3.6 VLAN Extension allows you to access your shared or dedicated servers in Cloud Infrastructure over your private Next IP Network using VLAN tunnelling technology.

3.7 You must obtain and use compatible equipment or virtual appliances to utilise VLAN Extension. We do not manage or support these devices.

3.8 We do not promise a particular data performance or throughput with VLAN Extension.

## 4 SECURITY SERVICES

4.1 The following table sets out the availability of the Security services you can apply for in connection with your Public Network product or Private Network product in this Network Services part. As set out in the table below, the availability of a service will depend on whether you select a Cloud Infrastructure or Tailored Infrastructure product under Part E Infrastructure part.

| Service | Public Network | | Private Network | |
|---|---|---|---|---|
| | Tailored Infrastructure | Cloud Infrastructure | Tailored Infrastructure | Cloud Infrastructure |
| Internet Protection Services | ✓ | ✓ | x | x |
| Denial of Service Protection | ✓ | ✓ | x | x |
| Firewall (Dedicated) | ✓ | x | ✓ | x |
| Firewall (Shared) | ✓ | x | ✓ | x |
| Firewall (Virtual) | x | ✓ | x | ✓ |
| Intrusion Prevention (Dedicated) | x | x | x | x |
| Intrusion Prevention (Shared) | ✓ | x | ✓ | x |
| IPSEC VPN (Shared) ^ | x | x | x | x |
| IPSEC VPN | ✓ | ✓ | x | x |
| SSL VPN | ✓ | x* | x | x |

| Service | Public Network | | Private Network | |
|---|---|---|---|---|
| | Tailored Infrastructure | Cloud Infrastructure | Tailored Infrastructure | Cloud Infrastructure |
| Vulnerability Discovery | ✓ | ✓ | ✓ | ✓ |

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

*^ Intrusion Prevention (Dedicated) and IPSEC VPN (Shared) is not available to new customers on and from 1 June 2015. We will continue to support adds, moves and changes for Intrusion Prevention (Dedicated) and IPSEC VPN (Shared) services existing prior to 1 June 2015 and which have not been cancelled.*

*✓ Service is available.*

*x Service is not available.*

### Internet Protection Services

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

4.3 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/.

### Denial of Service Protection

4.4 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.

4.5 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.

4.6 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.

4.7 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.

4.8 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.

**Firewall**

4.9 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.

4.10 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;

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

(e) a quarterly vulnerability assessment (only for customers who acquired their service before 31 May 2012);

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

(g) client to site VPN support;

(h) security event monitoring; and

(i) threat analysis and intelligence service.

4.11 Under the shared firewall configuration, the features of your service will depend on the service tier that you select.

4.12 Under the dedicated firewall configuration, the hardware that we use to provide you with the service will be dedicated to you and the services of your service will depend on the service tier that you select.

4.13 The dedicated firewall configuration also includes:

(a) custom analysis, design and configuration of your dedicated firewalls;

(b) management of change requests to your Firewall service; and

(c) access to any additional firewall modules (such as a deep packet inspection module) where these modules are supported by your chosen firewall.

4.14 We do not promise that the Firewall service will prevent unauthorised access to your network.

4.15 We can only provide the Firewall service for the devices that are managed by us.

4.16 If you select a dedicated firewall service, we do not guarantee that the additional modules will remove all viruses or correctly identify all viruses, screen or block all spam or correctly identify all spam, block all websites you ask us to block or correctly identify websites that you have requested to be blocked or block all network activity you ask us to block or correctly detect network activity that you deem suspicious.

**Intrusion Prevention (Network)**

4.17 This service provides intrusion protection for the public and private networks and comprises:

(a) attack recognition and response service;

(b) notification to you if we become aware of a security threat;

(c) automatic escalation process for known threats and vulnerabilities; and

(d) monitoring of traffic and uptime when an unauthorised intrusion has occurred.

4.18 We cannot guarantee that the Intrusion Protection service will protect against all attacks

**SSL VPN/IPSEC VPN**

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

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

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

**Vulnerability Discovery**

4.22 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.

## 5 SPECIAL MEANINGS

The following words have the following special meanings:

**Spam** means unsolicited commercial email.

**URL** means the uniform resource locator.

**User** means a person or mailbox on behalf of which email is being scanned by the relevant Internet Protection service.

**Virus** means a piece of program code, including a self-replicating element, usually (but not necessarily) disguised as something else that causes some unexpected and, for the victim, usually undesirable event and which is designed so that it may infect other computer systems.

**VLAN** means Virtual Local Area Network.

**VPN** means Virtual Private Network.