SERVICE SCHEDULE – DENIAL OF SERVICE PROTECTION

This Schedule sets out the service description that applies to Global Denial of Service Protection.

1 ABOUT THIS SERVICE SCHEDULE

1.1 This Service Schedule sets out the specific terms and conditions under which we will supply you with the Global Denial of Service Protection service ("**Service**").

1.2 If there is any inconsistency between the terms of:

(a) this Service Schedule; and

(b) the terms of your Primary Internet Service,

then the document listed earlier in this clause 1.2 prevails to the extent of the inconsistency.

2 SERVICE DESCRIPTION

2.1 The Service is designed to filter certain network traffic in our network to assist you in managing the potential impact of denial of service (including distributed) attacks ("**Attacks**") against your Primary Internet Service.

2.2 The Service monitors and reports incoming traffic and analyses it for anomalies or misbehaviours, and where necessary, traffic is re-routed to our Cleaning Centre where we filter out the Attack traffic and send the legitimate traffic to your Primary Internet Service ("**Mitigation**").

2.3 The Service analyses traffic by a number of methods, including comparing network traffic flows to your Primary Internet Service based on agreed profiles of normal traffic patterns, behaviour, and protocol compliance.

2.4 You must select one of the following "**Service Tiers**" (as further described in clauses 2.4 to 2.5 below) in your SOF in connection with your Service:

(a) Standard – we will perform the traffic monitoring and reporting functions described in clause 2.2, but if you suspect an Attack against your Primary Internet Service, you must notify us that you wish us to perform Mitigation; or

(b) Premium - we will perform the traffic monitoring and reporting functions described in clause 2.2 on your link and internet facing CPE, and we will also contact you if we suspect an Attack against your Primary Internet Service to ask if you want us to perform Mitigation.

2.5 The features of the Standard and Premium Service Tiers are set out in the table below:

FEATURE	DESCRIPTION	STANDARD	PREMIUM
CPE Monitoring	Netflow data sent from your CPE to us for monitoring.	×	✓
Traffic Baseline	All Internet traffic is used to construct traffic "baseline" to assist Attack detection.	✓	✓
Traffic Re-Injection	You will terminate cleaned traffic on a device at your Site(s) via Generic Routing Encapsulation (GRE) tunnelling (managed or unmanaged).	✓	✓
Hotline	You can contact our Help Desk if you feel that you are under Attack. We will investigate and work with you to Mitigate the Attack if the Attack is confirmed.	✓	✓
Portal Access	You can access alert information and download reports (requires username & password). You can also monitor your network status online.	✓	✓
Service Levels	Service Levels covering Service Availability, time to Mitigate and Mitigation consistency.	✓	✓

FEATURE	DESCRIPTION	STANDARD	PREMIUM
Service Level Rebates	Rebates for non-performance.	×	✓
Mitigation	We will work with you to facilitate the redirection of incoming traffic on your Primary Internet Service through our Cleaning Centre.	✓	✓
Alarming	We will monitor the status of your Primary Internet Service and notify you if agreed profiles of normal traffic patterns, behaviour, and protocol compliance are exceeded.	✓	✓
Additional Service Levels	We offer an Attack monitoring & notification service level on the time taken by us to notify you of an Attack.	×	✓
CPE Management (optional)	Management of your CPE that connects to the Primary Internet Service.	✓	✓

2.6 The Service does not include the Primary Internet Service, which you must acquire separately from us.

LIMITATIONS OF THE SERVICE

2.7 You may only obtain the Service if you have a Primary Internet Service with us unless otherwise agreed in writing by us, upon the terms and conditions (including pricing) contained in your applicable Service Schedule to this Agreement or your separate agreement with us, for provision of such internet service.

2.8 We do not guarantee that the Service will prevent all Attacks against the Primary Internet Service. In particular, the Service may not provide any protection or assistance to you arising out of an Attack on the Primary Internet 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 Primary Internet Service; or

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

2.9 We will not perform deep packet inspection of network traffic on your behalf except where mitigation of an Attack is required. In the event that mitigation of an Attack is required, you may request (and subject to technical feasibility, we may agree to perform) deep packet inspection of your network traffic.

2.10 If you request us to perform deep packet inspection of any network traffic directed to the Primary Internet Service on your behalf, you must:

(a) ensure that such network traffic is encrypted; and

(b) indemnify us from and against any and all loss, damages, liability, claims, costs and expenses (including reasonable attorney's fees)(**Loss**) which arise naturally (that is, according to the usual course of things) in connection with your failure to do so (which for the avoidance of doubt includes any liability to implement measures to comply with applicable data protection laws, take steps to inform data subjects or relevant authorities of any personal data processing performed by us on your behalf and for any fines, penalties or costs of any kind (including remediation and audit costs) arising out of, or in connection with the processing of personal data on your behalf) except to the extent the Loss is caused or contributed by us. We will take reasonable steps to mitigate our Loss suffered in connection with your failure to comply with the provisions of this clause 2.10.

2.11 The Service is designed to limit network traffic to the Primary Internet Service. If the Service detects an Attack, then you acknowledge and agree that:

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

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

(c) if data traffic volumes from Attacks being mitigated by the Cleaning Centre exceed or are expected to exceed the capacity of the Cleaning Centre 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.

We are not responsible for any loss that you suffer as a result of the Service blocking or limiting network traffic due to an Attack.

ELIGIBILITY

2.12 The Service is not available to all customers, and we will determine your eligibility for the Service in our absolute discretion.

2.13 The Services is only available in the Available Countries. If we notify you that a particular country is no longer an Available Country, then you must cease to use the Services in that particular country from the date specified in the notice. Failure to do so may require us to suspend or terminate your Service.

2.14 All internet addresses within your protected range must be public IP addresses assigned to you.

2.15 The bandwidth for your Service must align with the Aggregate Bandwidth.

CONFIGURING THE SERVICE

2.16 We will work with you to design and configure the Service. When we have both agreed the design and configuration of the Service, then we will:

(a) implement the agreed configuration and activate the Service;

(b) test the Service with you; and

(c) baseline the Service with you.

3 PRICING

3.1 You must pay us the applicable charges set out in the SOF ("**Service Charges**") in addition to any charges for your Primary Internet Service.

3.2 We will commence billing you on the Service Start Date.

VARIATION TO SERVICE CHARGES

3.3 The Service Charges are fixed for 12 months from the Service Start Date. We will notify you of any changes to the Service Charges after this date as soon as practicably possible.

3.4 If the Aggregate Bandwidth changes at any time during the Service Term, then we will:

(a) automatically adjust the bandwidth for the Service in accordance with clause 2.12 above; and

(b) if relevant, adjust your Service Charge according to the corresponding new Aggregate Bandwidth. Any adjusted Service Charge will be included on your next bill.

4 TERM AND TERMINATION

4.1 This Service Schedule will automatically terminate on the date of termination or expiry of your Primary Internet Service. An early termination charge may apply if your Primary Internet Service is terminated or expires before the end of the Service Term for your Service.

EARLY TERMINATION CHARGE

4.2 If during the Service Term a Service is cancelled for any reason other than for our material breach, we may charge you any waived Service Charges and an amount calculated as follows:

A x B x 25%

"A" = the average Service charges paid or payable each month by you for the Service up to the date of cancellation.

"B" = the number of months (or part of a month) remaining in the Service Term.

You acknowledge that this amount is a genuine pre-estimate of the loss we are likely to suffer.

5 SUPPORT SERVICES

5.1 We will:

(a) provide reports to you;

(b) monitor the operation of the Service; and

(c) provide you with access to the Help Desk.

5.2 You may contact the Help Desk 24 hours a day, seven days a week (including public holidays) in relation to:

(a) any queries you may have with the Service;

(b) notifying us that you wish to mitigate an Attack; and

(c) requesting us to investigate a possible Attack.

5.3 If you ask us to perform major configuration changes, then we will work with you to design and configure the necessary changes to the Service. We will charge you an additional charge for each major configuration change calculated at our then current time and materials rate. We will tell you the charges at the time of your request.

6 SERVICE LEVELS

6.1 You acknowledge and agree that any service levels or service tiers for your Primary Internet Services (including any rebates) will not apply during any period where we are Mitigating your traffic, this includes during any period to identify you traffic baseline and during an Attack.

6.2 We will use reasonable endeavours to meet the service levels set out in this clause 6 ("**Service Levels**"). If you believe there is a fault with your Service, you must contact us via the Help Desk.

6.3 Save for availability targets and restoration targets for the Premium Service Tier, the Service Levels are only indicative targets. We will not be liable to you (whether in contract, tort, including negligence, or otherwise) for any failure to meet a Service Level.

6.4 The Service Levels for your chosen Service Tier are set out in the table below and, unless otherwise specified, are measured monthly:

DESCRIPTION	STANDARD	PREMIUM
Service Availability	99.9%	99.9%
Reduction of Attack traffic	80% measured over any 1 hour period*	90% measured over any 1 hour period*
Notification of a significant Attack of the Primary Internet Service	Within 1 hour of agreed capacity threshold being exceeded	Within 15 minutes of agreed capacity threshold being exceeded

DESCRIPTION	STANDARD	PREMIUM
capacity of the filtering platform		
Time frame to begin filtering and commence redirecting traffic from time that instruction is received from you	5 minutes	5 minutes
Number of service requests for Standard Configuration Changes**	2 Standard Configuration Changes 1 emergency configuration change	Unlimited Standard Configuration Changes and emergency configuration changes
Implementation of standard pre-agreed standard changes	Within next Business Day of our acknowledgement of your request	Within next Business Day of our acknowledgment of your request
Implementation of emergency configuration changes	Within 4 hours of the request (you must inform the Help Desk that you require an emergency configuration change)	Within 1 hour of the request (you must inform the Help Desk that you require an emergency configuration change)
Incident resolution targets	As set out in clause 6.5.	As set out in clause 6.5.

* It may not be possible to measure this Service Level accurately. We have provided you with a Service Level to assist you in dimensioning internet links and other infrastructure to expected levels of traffic.
** If configuration changes are in excess of a Standard Configuration Change, we may charge you for the change in accordance with clause 5.3 (Support Services). We will discuss this with you before we make any changes.

6.5 The incident resolution targets are set out in the table below:

INCIDENT SEVERITY	RESPONSE TARGET	STATUS REPORT	RESTORE TARGET
1	15 Minutes	1 hour	1 hour
2	15 Minutes	2 hours	4 hours
3	30 Minutes	1 day	24 hours
4	30 Minutes	N/A	48 hours

We are responsible for determining the incident severity in accordance with the table below and will notify you of the severity we have assigned to an incident that you report to the Help Desk.

INCIDENT SEVERITY	DESCRIPTION
1	Your Service is not available, causing critical impact to business operations.
2	Your Service is not available or severely degraded, impacting significant aspects of business operations.
3	Your Service is degraded. The Service is noticeably impaired, but most business operations continue.
4	All other incidents that are not Severity 1, 2 or 3 incidents.

6.6 We will commence measuring the Service Levels from the time we send an acknowledgement of the incident to you.

7 REBATES FOR PREMIUM SERVICE LEVELS

7.1 If you elect in the SOF to receive the Premium Service Tier, then:

(a) the restoration target will be subject to Service Level rebates being an amount equal to one month's access rental paid at 20% per complete hour beyond the target restoration time and capped at 100% per month per service; and

(b) the availability target will be subject to Service Level rebates where, in any single month, the Availability of the Service does not conform with the Service Level specified, in which case we will pay rebates as outlined in the table below:

Rebates for Service Availability are expressed as a percentage (%) of the monthly Service Charges.

	% AVAILABILITY	REBATE
Target 100% - threshold 99.89 - 99.86%	100 – 99.90	0%
	99.89 – 99.86	5%
	99.85 – 99.83	15%
	99.82 – 99.79	25%
	<99.78	50%

7.2 The rebates above will be your sole remedy for our failure to meet a Premium Service Level.

MAINTENANCE

7.3 Service Levels will not apply during Planned Maintenance or Emergency Maintenance. We will use reasonable endeavours to provide you with at least five days' notice of any planned maintenance.

GENERAL

7.4 To be eligible to claim a rebate, you must:

(a) have successfully completed a service validation test within twelve months of your claim; and

(b) not have any undisputed unpaid amounts in relation to this Service.

(c) confirm that all prior competing mitigation techniques, fixes, and gear have been removed.

7.5 If you have more than one Primary Internet Service protected by this Service, you will not receive credits for unaffected Primary Internet Services.

7.6 To claim a service rebate, you must provide the following details in writing to one of our sales representatives within two months of the original fault report:

(a) your name and address;

(b) the relevant Telstra account number and service number;

(c) the relevant fault reference number; and

(d) the reason for dissatisfaction.

7.7 If you are entitled to a service rebate, we will provide you with a credit on a future bill.

8 YOUR OBLIGATIONS

8.1 You will:

(a) provide reasonable assistance and information to us to enable us to deliver the Service to you;

(b) report all incidents with the Service known to you to the Help Desk;

(c) obtain and maintain (at your own cost) appropriate equipment, software, telecommunications services, internet access and other services or resources needed to use the Service;

(d) not use the Service in a way that may adversely affect the efficiency, security, use or operation of the Primary Internet Service;

(e) not sell, resell or provide the Service (or any part of it) to other people without our prior approval; and

(f) comply with all relevant laws, regulations and regulatory requirements relating to your use of the Service.

8.2 You are solely responsible for any use or attempted use of the Service by you or any third party except to the extent that such third party use is the result of our neglect or wilful misconduct.

9 INTELLECTUAL PROPERTY RIGHTS

9.1 All intellectual property rights connected with the design of the Service, including any intellectual property rights relating to:

(a) network diagrams; and

(b) management IP addresses,

remain with us at all times.

9.2 You acknowledge and agree that all information relating to the design of the Service, including the information identified in clause 9.1, is our confidential information.

10 AUSTRALIAN SERVICE TERMS

10.1 If the Service is provided to you in Australia, then:

(a) we may limit, suspend or cancel the provision of the Service at any time:

(i) without notice to you in the event of an emergency or in order to provide resources to emergency and other essential services;

(ii) after giving you as much notice as we reasonably can, if the Australian Competition and Consumer Commission (ACCC) issues or we reasonably anticipate that the ACCC may issue a competition notice in relation to the Service; or

(iii) after giving you notice if you are or become a carrier or carriage service provider (as defined in the Act);

(b) you agree and will ensure that your Personnel, your Related Companies and their Personnel, and any individuals who receive the Service or whose information is disclosed to us, in connection with our provision of the Service, are aware that we may use and disclose information about you and each of them in accordance with our Australian privacy statement (as amended by us from time to time), which is available at http://www.telstra.com.au/privacy/privacy-statement/index.htm; and

(c) If you are a consumer as defined in the Australian Consumer Law, our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

11 DEFINITIONS

11.1 Words that are capitalised but not defined in this Service Schedule will have the same meaning given to it in the

Agreement Terms except where the context otherwise requires.

11.2 In this Service Schedule, unless otherwise stated:

Act means the *Telecommunications Act 1997* (Cth) unless otherwise stated.

Aggregate Bandwidth means the total bandwidth of all of your Primary Internet Services.

Attacks has the meaning given to it in clause 2.1.

Available Countries means Australia, Hong Kong, India, Japan, Malaysia, New Zealand, Philippines, Singapore, South Korea, United Kingdom, United States of America, and Taiwan.

CPE or **Customer Premise Equipment** means the equipment located at your Site(s) and connects your network to the Primary Internet Service links.

Cleaning Centre means our cleaning centres to which your traffic is re-routed during an Attack.

Emergency Maintenance is any activity that we, in our sole discretion, deem necessary to correct an immediate threat to the ongoing availability and quality of our services.

Help Desk means our Service Desk available by calling 1800 220 849 (within Australia) or +61 2 6129 4688 (international calls) or such other number as we may notify you of from time to time.

Managed Object means a grouping of IP address prefixes to be monitored as part of your Service.

Netflow means the network protocol for monitoring traffic on your router.

Personnel means a person's officers, employees, agents, contractors and sub-contractors and, in our case, includes our Related Bodies Corporate.

Primary Internet Service means your Telstra internet service, being either:

(a) Telstra Internet Direct (TID);

(b) Global Internet Direct (GID); or

(c) IP Transit.

Related Bodies Corporate has

(a) for the purpose of the definition of Related Company, the meaning given under the *Corporations Act 2001* (Cth); and

(b) for all other purposes, the meaning given under the *Corporations Act 2001* (Cth), but as if each reference to a "body corporate" includes a proprietary company, a partnership or a trust.

Service has the meaning given to it in clause 1.1.

Service Availability means the period of time the Service is monitoring, detecting, filtering and reporting Attacks, where applicable, in each case, within the specifications and the configuration parameters of the Service. Service Availability is measured on a monthly basis and excludes the period of any and all planned outages.

Service Charges has the meaning given to it in clause 3.1.

Service Levels has the meaning given to clause 6.1.

Service Start Date means the date we first activate your Service.

Service Term commences from the Service Start Date and continues for the Initial Period set out in the SOF unless terminated or renewed in accordance with the Agreement Terms.

Site means your premises or location as nominated in your SOF.

SOF means the Service Order Form.

Standard Configuration Change means a change to the configuration of the Service that requires no more than a total of 2 hours of work by us. The 2 hours of work does not need to be consecutive and may be undertaken over a number of days.