SERVICE SCHEDULE – SECUREEDGE CLOUD AND REMOTE SERVICE

This Service Schedule sets out the service description and service specific terms that apply to the SecureEdge Cloud and Remote Service.

1 SERVICE DESCRIPTION

1.1 The SecureEdge Cloud and Remote Service is a cloud hosted security service including a next-generation firewall (**Cloud Security**) available in the Territories.

1.2 You agree to use the Cloud Security in accordance with the terms of the service guide which contains technical and operational descriptions provided by us to you (**Service Guide**).

2 SERVICE INCLUSION AND PLANS

SECURITY

2.1 Your Service includes the Cloud Security which is a security infrastructure designed to help protect network traffic by applying security features to the traffic as it runs through the Cloud Security.

2.2 The Cloud Security may include the following features and capabilities as your network traffic runs through it, which are subject to change from our third party supplier. Nothing in this Service Schedule limits our or our third party suppliers' ability to change the Cloud Security product from time to time without having any obligation or liability to you. We will provide you with the details of changes if the details are made available to us by our third party supplier. You acknowledge and agree that we may not automatically include the changes available in all instances.

Security Feature	Description
Network antivirus and antispyware protection	Blocks virus or spyware software or applications running on the customer next generation firewall
Sandboxing	Advanced malware and APT prevention
Safe web browsing	Block bad websites, phishing, executables from unknown URLs with parental controls
Vulnerability protection and intrusion prevention	Protects against unauthorized access
Block high-risk file types	Block multi-level encoded files and only allows well behaved applications
Data loss prevention	Sensitive data such as credit card information is not lost
Sinkhole command and control traffic	Stops outbound command and control traffic so malware is not able communicate back to the command server
Port-based firewall with application visibility	Block bad, misbehaving or high-risk applications
DoS and DDoS protection	Block Denial of Service Attacks on specific applications or that have low to mid traffic volumes
Port-based firewall with application visibility	Block bad, misbehaving or high-risk applications
Reputation based IP filtering	Filters out high risk and malicious IP addresses
Threat intelligence with Customisable protection feeds and Blacklist	Ability to blacklist specific items such as Domain Name Servers, IP Addresses, or specific URL's
Policy customization per customer	Each customer can select how they want their policies configured, what specific items they want to block (URL's, IP's etc)
Remote Access	Allows remote/mobile access to customer network
IPSec VPN (site-to-site)	Secure IPsec tunnel between customer sites

SSL / TLS decryption	Ability to decrypt traffic in order to search for threats

2.3 We will allocate an amount of bandwidth for the Cloud Security connectivity based upon site options during the solution design phase. We will provide you with a minimum of 1000Mbps and 1000 remote users. The minimum number of Mbps and remote users may change from time to time and we will notify you accordingly.

3 CHARGES AND EARLY TERMINATION CHARGES

CHARGES

3.1 Your Service includes Cloud Security. We will allocate an amount of bandwidth per site option for Cloud Security connectivity with a minimum of 1000Mbps and/or 1000 Remote users.

EARLY TERMINATION CHARGES

3.2 If you cancel, terminate or downgrade the Cloud Security for any reason other than our material breach of this Agreement:

(a) prior to the Service Start Date for the Cloud Security, you must pay us an Early Termination Charge equal to the costs reasonably incurred by us as a result of the termination (including any amounts payable by us to our Service Provider as a result of the cancellation of the relevant Service); or

(b) during the term for the Cloud Security, you must pay us an Early Termination Charge for the unexpired remaining months in the contract term.

4 SERVICE CONDITIONS AND RESPONSIBILITIES

EXCLUSIONS

4.1 We do not promise or guarantee that the Cloud Security will prevent or detect unauthorised access or breaches to your network.

4.2 We will use, access and configure the Cloud Security on your behalf as part of our supply of the Service to you.

4.3 We may carry out your Cloud Security policy configuration requests as instructed by you but we will not advise on the merits of the request or the potential consequences of implementing the request (unless you request additional advisory service as an Additional Service). It is recommended to have the advisory service however, not mandatory. If you request this advisory service, the scope of these services and any additional fees will be agreed under a SOW.

4.4 We are not responsible for, and the Service does not include:

(a) application of security features to data or traffic that has bypassed the Cloud Security; and

(b) defining the Cloud Security configuration to address your business security objectives (however, you can request this as an Additional Service and the scope and any additional fees will be agreed under a SOW).

4.5 Updates to the Cloud Security may be provisioned at the time they are supplied by our third party supplier.

We will notify as soon as reasonably possible (depending on notification provided to us by our third party supplier) if these updates will impact the Cloud Security or your Service.

5 SUPPORT SCOPE

5.1 Depending upon the Partner service arrangement and your requirements, you may have read-only access to a range of default online dashboards and download dynamic and static reports either from the Partner or SD- WAN / Cloud Security portals.

6 SERVICE LEVELS

6.1 We will aim to meet the service level set out in Table 1 below:

Table 1 – Service Level for Cloud Security

SEVERITY LEVEL	TARGET RESPONSE TIME	TARGET RESTORATION TIME	TARGET STATUS REPORTS
Severity 1 Your Service is down at a site or multiple sites causing critical impact to your business operations	15 minutes	Restored (or work around) in 4 hours	Every hour
Severity 2 Your Service is down at a site or your Service is severely degraded impacting significant aspects of your business operations	30 minutes	Restored (or work around) in 8 hours	Every 2 hours
Severity 3 Your Service is degraded, noticeably impaired but most of your business operations continue	60 minutes	Restored (or work around) in 24 hours	Every 8 hours
Severity 4 You require information or assistance regarding the Service	120 minutes	Restored (or work around) in 48 hours	Every 24 hours

6.2 No service credit is payable if the service levels in Table 1 are not fulfilled.

7 COUNTRY SPECIFIC TERMS AND CONDITIONS

INDIA

7.1 For Cloud Security in India, you agree to comply with the following terms and conditions:

(a) the contracting and billing for the Cloud Security will be done outside of India;

(b) you must provide or bring your own network or internet connections;

(c) the Cloud Security must not be provided using Telstra GID service;

(d) the Cloud Security may be provided using Telstra GIE service as advised by us to you from time to time; and

(e) the end user of the Cloud Security must be a legal entity incorporated in India.

8 PERSONAL DATA

8.1 To the extent that you configure your Cloud Security to process personal data covered by UK or EU privacy laws, you agree to the terms of the GDPR Addendum located at https://www.telstra.us.com/en/service-terms, as may be amended from time to time upon notice by us.

9 THIRD PARTY SUPPLIER TERMS AND EXPORT RESTRICTIONS

THIRD PARTY SUPPLIER TERMS

9.1 In operating, downloading, installing, registering or otherwise using the Cloud Security, you acknowledge and agree to be bound to any third party end user license agreement, third party supplier terms and any other related terms (**Third Party Terms**) as advised by us to you or made available to you while using the Cloud Security. If you do not accept the Third Party Terms, you shall not be permitted to use the Cloud Security.

EXPORT RESTRICTIONS

9.2 Our vendor for Cloud Security (**Vendor**) has classified the Cloud Security software to be downloaded by you to use the Service as ECCN 5D002 and eligible for License Exception ENC pursuant to 15 C.F.R. § 740.17(b)(2)(1)(A).

9.3 You represent and warrant that you are eligible to receive items (including, but not limited to, Cloud Security) regulated by the EAR and that neither you nor any of your direct or indirect owners, officers, directors, employees, affiliates, agents, representatives, end users or subcontractors are subject to U.S. or other applicable sanctions or export restrictions, including being designated on or pursuant to the U.S. Department of Commerce's Denied Persons List, Unverified List, or Entity List; the U.S. Department of State's Non- Proliferation Sanctions Determinations; the U.S. Department of the Treasury's Specially Designated Nationals List, Foreign Sanctions Evaders List, or Sectoral Sanctions Identifications List; or sanctions-related U.S. Executive Orders. You further represent and warrant that you do not qualify as a more sensitive government end user, as that term is defined in Section 772.1 of the EAR, are not part of the national armed services (army, navy, marine, air force, or coast guard), the national guard, the national police, or a government intelligence or reconnaissance organization; nor do you otherwise qualify as a military end user or military- intelligence end user, as those terms are defined in Sections 744.21 and 744.22 of the EAR and related U.S. government guidance, such as by being designated on the EAR's Military End-User List or by developing, producing, maintaining, or using military items. You must immediately notify us, in writing, of any change that may impact the representations above.

9.4 You understand that the direct or indirect export, re-export, transfer (in-country), sale, lease, or supply, or any other access to or use of the software or Services to or in another country or to, by, or for a different end user or end use may require a license or other authorization, including from the Government of the United States; and agree that it will comply with any such license or authorization requirements. You also specifically agrees that it will not transfer (in-country), re-export, or otherwise divert the software or Services to any sanctioned or prohibited country/region or person or for any prohibited end use, which can include military-intelligence end uses/end users, military end uses/end users, and end uses related to weapons proliferation. It is your sole responsibility to screen for sanctioned and prohibited countries/regions, persons, and end uses and to obtain any necessary licenses or other governmental authorizations. We make no warranty that any such licenses or other authorizations will be granted and shall have no liability for your inability to obtain such licenses or other authorizations or for any violation by you of any applicable export control, import, and/or economic sanctions law or regulation.

9.5 Notwithstanding any other provision in the Service Schedule or the Agreement of which it is a part, we shall have the right to terminate the Agreement in whole or in part or stop performance immediately upon our determination, in our sole discretion, that you have breached, intend to breach, or insist upon breaching any of the provisions in this Clause 9. Under such circumstances, we shall be released from responsibility for fulfilling our obligations under the Agreement, you shall be liable for any Early Termination Charges and we shall not be subject to any liability for lack of performance or breach of the Agreement.

9.6 You shall indemnify and hold harmless us and our affiliates and group members, from and against any and all damages, claims, allegations, losses, liabilities, penalties, fines, costs, and expenses (including attorney's fees which arise out of, relate to, or result from your failure to comply with the provisions of this Clause 9 or any applicable export control, import, or sanctions law or regulation.

10 DEFINITIONS

Additional Service means any other related additional services that have been agreed under a SOW or any other documents.

EAR means the U.S. Export Administration Regulations.

Partner means our third party suppliers, vendors and service providers.

SOW means statement of work as defined in the Agreement Terms.

Territories means the countries listed in Appendix 1 of this Service Schedule.

Appendix 1 – Territories

ASIA

No.	Countries	Remarks (if any)
1	Japan	None
2	Bangladesh	None
3	Pakistan	None
4	Cambodia	None
5	Indonesia	To be bundled with connectivity services as advised by us to you from time to time.
6	Malaysia	None
7	Myanmar	None
8	Philippines	None
9	Singapore	None
10	Thailand	None
11	Vietnam	None
12	Australia	Please refer to Australian Service Schedule or Online Customer Terms for services in Australia.
13	Papua New Guinea	None
14	Hong Kong	None
15	Taiwan	None
16	South Korea	None
17	India	Refer to Clause 7.1 above.
18	New Zealand	None

Note: Some countries (for example: Hong Kong and Singapore) may be subject to export restrictions and we will advise further where necessary.

EMEA AND THE US

No.	Countries	Remarks (if any)
1	Austria	None
2	Belgium	None
3	Canada	None
4	Denmark	None
5	France	None
6	Germany	None
7	Ireland	None
8	Italy	None
9	Netherlands	None
10	Portugal	None
11	South Africa	None

12	Spain	None
13	Sweden	None
14	Switzerland	None
15	USA (including US territories)	None
16	UK	None