

## Hybrid WAN - MSS Web Module

### Addendum 1- Hybrid WAN Option Operational Details

This Addendum is part of the Service Schedule for the Hybrid WAN - MSS and describes additional terms which apply to the Hybrid WAN Service Option of the Solution.

1. **Service Description.** Supplier shall provide connectivity between Customer and the Solution on the Supplier Network through global virtual private network connectivity which provides users at distributed locations with secure, reliable remote access via broadband and wireless and subject to the Service Terms.
2. **Supplier Responsibilities.** Supplier shall use reasonable endeavors to:
  - 2.1 Give at least three (3) Business Days' notice of the installation date of the CPE (which shall not be earlier than the date agreed between the parties) including the hours during which Supplier requires access to the Customer Premises (which shall be during Business Hours unless the Customer otherwise agrees) and any special site-access requirements.
  - 2.2 Deliver the CPE to the Customer Site, and if delivered prior to the installation date the Customer shall store the CPE in a secure location.
  - 2.3 Unpack and inventory the CPE; Install the CPE in accordance with the Site Plan; Connect electrical power to the CPE; Validate the expected equipment boot sequence; Install the operating system software ordered with the equipment.
  - 2.4 Test the CPE against the ready for function criteria provided by the Customer as relevant to the ordered service, such criteria to be reasonably acceptable to Supplier.
  - 2.5 Establish connectivity between the CPE and the Associated Service.
3. Supplier is not responsible for:
  - 3.1 Any inability to meet ready for function criteria provided by the Customer, where the Internet access requirement information provided by the Customer is inaccurate or incomplete.
  - 3.2 Any customization of software or any installation of software other than the operating system software ordered.
  - 3.3 Resolving operating system software or CPE hardware problems caused by third-party products, or by factors beyond Supplier's reasonable control.
  - 3.4 Providing any hardware, unless separately ordered by Customer, required to run new or updated operating system software.
  - 3.5 The condition and maintenance of the Customer site and, the installation and maintenance of all in-premises cabling, including cabling from the Customer's NTU to the Customer Equipment or CPE, which are the Customer's sole responsibility.
  - 3.6 Any configuration of CPE unless ordered under appropriate service option.



## Addendum 2- (A) Hybrid WAN Service Tier & SLA Definition Charts and (B) SDWAN Select Service Tier

### 1. Service Coverage

#### 1.1 Global Service Locations:

Global Tier-1	Australia	Austria	Belgium	Canada	Denmark	Finland	France
	Germany	Hong Kong	Ireland	Italy	Japan	Netherlands	Norway
	Singapore	South Korea	Spain	Sweden	Switzerland	United Kingdom	United States
Global Tier-2	Albania	Antigua & Barbuda	Barbados	Bermuda	Bosnia Herzegovina	British Virgin Islands	Bulgaria
	Cayman Islands	China	Croatia	Curacao	Czech Republic	Dominica	Dominican Republic
	Egypt	Faroe Island	French Guiana	Greece	Grenada	Guadeloupe	Haiti
	Hungary	Iceland	Indonesia	Israel	Jamaica	Kuwait	Lithuania
	Luxembourg	Macedonia	Malaysia	Martinique	Morocco	New Zealand	Pakistan
	Peru	Poland	Portugal	Qatar	Romania	Russia	Serbia
	Slovakia	St Lucia	St Vincent	Suriname	Taiwan	Trinidad & Tobago	Turkey
	Turks & Caicos Islands	United Arab Emirates	US Virgin Islands				
Global Tier-3	Argentina	Bahrain	Bangladesh	Bermuda	Bolivia	Brazil	Chile
	Colombia	Costa Rica	Ecuador	El Salvador	Estonia	Ghana	Guatemala
	Honduras	Kenya	Latvia	Mexico	Montenegro	Nicaragua	Nigeria
	Panama	Paraguay	Philippines	Puerto Rico	Saudi Arabia	Slovenia	South Africa
	Sri Lanka	Thailand	Tanzania	Ukraine	Uruguay	Venezuela	Vietnam
Global Tier-4	Algeria	Angola	Aruba	Botswana	DRC	Jordan	Kenya
	Mozambique	Namibia	Rwanda	Tanzania	Tunisia	Uganda	Zambia
	Zimbabwe						

### 2. EAS SLA Locations

<b>EAS SLA Tier 1</b>	Australia, Austria, Belgium, Canada, Cyprus, Denmark, Finland, France, Germany, Hong Kong, Ireland, Japan, Luxembourg, Malta, Monaco, Netherlands, Norway, Poland, Portugal, Singapore, South Korea, Spain, Sweden, Switzerland, Taiwan, United Kingdom and the United States.
<b>EAS SLA Tier 2</b>	Bahrain, Bolivia, Brazil, Chile, Croatia, Czech Republic, Ecuador, Egypt, Estonia, Greece, Hungary, Israel, Italy, Latvia, Lithuania, Malaysia, Mexico, New Zealand, Peru, Russia (Moscow, St Petersburg), Slovakia, Slovenia, Saudi Arabia, South Africa, Turkey and United Arab Emirates
<b>EAS SLA Tier 3</b>	All other countries where available

### 3. India SLA Tier Locations

SLA Tier	PoP and SLA Tier
<b>Tier 1</b>	Ahmedabad, Bangalore, Chennai, New Delhi, Emakalim Hyderabad, Kolkata, Mumbai (other than those listed in Tier 2), and Pune
<b>Tier 2</b>	Bhopal, Bhubaneshwar, Coimbatore, Gurgaon, Guwahati, Indore, Jaipur, Jalandhar, Jamshedpur, Karnal, Lucknow, Mohali, Mumbai-BKC, Mumbai – Nelco, Mumbai-Vashi, Mumbai-VSB, Nagpur, Noida, Panaji, Park Road (U.P), Patna, Surat, Trivanthapuram, Vadodara Shivasakti, Vijayawada, and Visakhapatnam (Vizag)
<b>Tier 3</b>	Adoni, Agra, Ahmed Nagar, Ajmer, Allahabad, Alleppy/ Alpuza, Alwar, Ambala, Ambattur, Amritsar, Anand (Nadiad), Asansol, Aurangabad, Bareilly, Belgaum, Bharuch, Bhilai, Bhilwara, Chandigarh, Calicut / Kozhikode, Cannore, Cuttack, Dehradun, Durgapur, Erode, Gandhinagar, Ghaziabad, GIFT (Gujarat), Guntur, Gwalior, Hassan, Himatnagar, Hissar, Hossur, Hubli, Jabalpur, Jalgaon, Jammu, Jamnagar, Jodhpur, Kakinada, Kannur, Kanpur, Kolhapur, Kollam, Kota, Kottayam, Ludhiana, Madurai, Mangalore, Meerut, Mehsana, Mysore, Nasik, Nellore, New Delhi—GK-1,Patiala, Pondicherry, Pune Shivajinagar, Raipur, Rajahmundry, Rajkot, Ranchi, Rohtak, Roorkee, Rourkela, Salem, Sambalpur, Sangli, Satara, Shimla, Siliguri, Solapur, Sonapat, Surat (Udhana),Thirussur, Tiruchirappalli, Tirupati, Tiruppur, Tumkur, Udaipur, Vadodara Jambuva, Valsad, Varanasi, Vellore Warangal

### 4. Hybrid WAN Service Options Locations

Type	Activity	Fully Managed /	IZO Private Connect	EAS Service (Managed)
<b>Fault</b>	Network Monitoring	Yes	Yes	Yes
	End to End Monitoring	Yes	No	Yes
	Fault Isolation	Yes	Yes	Yes
	Proactive Notifications	Yes	No	Yes

	Local maintenance	Loop	Yes	No	Yes
	CPE maintenance		Yes	No	Yes
<b>Configuration</b>	CPE Configuration Management		Yes	No	Yes
	CPE Backup Configuration		Yes	No	Yes
	CPE Change Management		Yes	No	Yes
	CPE & Circuit Information Log		Yes	No	Yes
<b>Asset</b>					
<b>Service Reporting</b>	<b>Level</b> Availability		SAP to SAP	Network only	SAP to SAP
	Performance Functions		SAP to SAP	Network only	Not Applicable

\* The Customer should enable relevant configuration on CPE and access for Supplier, like SNMP Access etc, and/or limited only to up/down status.

## 5. Outage classification; Severity Level

Priority	Incident Type	Definition
Severity 1	Hard	<ul style="list-style-type: none"> <li>Total loss of Service such that Packet Delivery is prevented between the affected SAP and all other SAPs in the VPN</li> <li>Degraded Service such that Packet Delivery is impeded between the affected SAP and other SAPs in the VPN (Customer is unable to use the service due to the serious degradation and ready to release it for immediate testing),</li> </ul>
Severity 2	Soft	<ul style="list-style-type: none"> <li>Degraded Service, but does not stop it from functioning however not able to work at expected levels of performance and productivity. (Customer still want to use the services and not ready to release it for immediate testing)</li> </ul>
Severity 3		<ul style="list-style-type: none"> <li>A Service problem, not seriously affecting service or network availability or functionality used in Customer's business</li> <li>A single non service specific quality or Service enquiry</li> </ul>
Severity 4		<ul style="list-style-type: none"> <li>Customer requests technical support in testing its equipment and verifying service</li> </ul>
Severity 5		<ul style="list-style-type: none"> <li>Non Service affecting. E.g.: incident report or any other queries not covered by Severity 1-4</li> </ul>

5.1 **Redundant and Resilient Site Definition Table.** The Table below further defines the Access Topologies Types. Supplier categorizes Redundant Topologies into different Types based on the network configurations selected by Customer. The table below defines these different Types. These types are identified in the Order Form.

Access Topologies							
Topology Type	Type #	Dual Local Loops	Dual PoP	Dual PE/CPE	Connectivity Service		
					GVPN	I Z O	BYO N
Redundant with: Dual Local Loop with Dual CPE	1	X	X	X	2		
Resilient with: Dual Local Loop, Dual POP with CPE(s)	11	X	X		2		
	12	X	X			2	
	13	X	X		1	1	
	14	X	X		1		>=1
	15	X	X			1	>=1
	16	X	X		1	1	>=1
Resilient with: Dual Local Loop, Single PoP with Dual PE with CPE(s)	21	X		X	2		
	22	X		X		2	
	23	X		X	1	1	
	24	X		X	1		>=1
	25	X		X		1	>=1
	26	X		X	1	1	>=1

## 6. SDWAN Select Service Tier

IZO SDWAN Select Service CPE TTR SLA are based on the city tiers. For cities not listed in the table below, SLA offered will be on an individual case by case basis in accordance with the price quotation provided by Supplier.

Country	T1/Metro City				
Algeria	Algiers				
Argentina	Buenos Aires				
Australia	Sydney	Melbourne	Perth	Brisbane	Adelaide
Austria	Vienna	Linz			
Belgium	Brussels	Aachen-Liège			
Brazil	Sao Paulo	Rio de Janeiro	Brasília		
Bulgaria	Sofia				
Canada	Toronto	Montreal	Vancouver	Calgary	Edmonton
	Ottawa	Quebec City	Winnipeg		
Chile	Santiago				
China	Shanghai	Beijing	Guangzhou	Tianjin	Shenzhen
	Suzhou	Chengdu	Hangzhou	Wuxi	Qingdao
	Nanjing	Dalian	Shenyang	Foshan	Dongguan
	Nantong	Hong Kong			
Croatia	Zagreb				
Czech Republic	Prague				
Denmark	Copenhagen				
Egypt	Cairo	Alexandria			
Estonia	Talinn				
Finland	Helsinki				
France	Paris	Lille	Lyon	Marseille	Toulouse
	Nice	Bordeaux	Strasbourg	Nantes	
Germany	Cologne	Frankfurt	Munich	Hamburg	Stuttgart
	Berlin	Karlsruhe	Nürnberg-Fürth	Hannover	Bremen
	Leipzig-Halle				
Greece	Athens				
Hungary	Budapest				
India	Ahmedabad	Bangalore	Baroda	Bhopal	Bhubaneshwar (Puri)
	Chandigarh	Chennai	Cochin	Delhi	Ernakulum
	Ghaziabad	Greater Kailash	Gurgaon	Guwahati	Hyderabad
	Jaipur	Kolkata	Mumbai	Noida	Patna
	Trivandrum	Pune	Secunderabad		
Indonesia	Jakarta				
Ireland	Dublin				
Israel	Tel Aviv				
Italy	Milan	Rome	Naples	Turin	Venice-Padova
	Florence	Bologna			
Japan	Tokyo	Osaka-Kobe			
Kuwait	Kuwait City				
Latvia	Riga				
Lithuania	Vilnius				
Luxembourg	Luxembourg-Trier				
Malaysia	Kuala Lumpur				
Mexico	Mexico City				
Morocco	Casablanca				
Netherlands	Rotterdam	Amsterdam			
New Zealand	Auckland				
Norway	Oslo				
Peru	Lima				
Philippines	Manila				
Poland	Warsaw				
Portugal	Lisbon	Porto			
Qatar	Doha				
Romania	Bucharest				
Russia	Moscow	Saint Petersburg			
Serbia	Belgrade				
Singapore	Singapore				
Slovakia	Bratislava				
Slovenia	Ljubljana				
South Africa	Johannesburg	Cape Town	East Rand	Pretoria	
South Korea	Seoul				
Spain	Madrid	Barcelona	Valencia	Bilbao	Seville

<b>Sweden</b>	Stockholm				
<b>Taiwan</b>	Taipei				
<b>Thailand</b>	Bangkok				
<b>Turkey</b>	Istanbul	Ankara			
<b>United Arab Emirates</b>	Abu Dhabi	Dubai			
<b>United Kingdom</b>	London	Birmingham	Manchester	Leeds	Liverpool
	Glasgow	Portsmouth	Southampton	Bristol	Newcastle
	Sheffield	Edinburgh	Cambridge	Leicester	Coventry
	Belfast	Aberdeen			
<b>United States</b>	New York City	Los Angeles	Chicago	Houston	Washington, DC
	Dallas/Fort Worth	Boston	Philadelphia	San Francisco	Atlanta
	Seattle	Miami	Minneapolis/St. Paul	Detroit	Phoenix
	San Diego	Baltimore	Denver	San Jose	St. Louis
	Pittsburgh	Tampa	Sacramento	Orlando	Cleveland
	Indianapolis	Cincinnati	Columbus	Austin	Kansas City
	San Antonio	Hartford	Nashville	Las Vegas	
<b>Uruguay</b>	Montevideo				
<b>Venezuela</b>	Caracas				
<b>Vietnam</b>	Ho Chi Minh City	Hanoi			

[End of Addendum]



## Addendum 3 – All Service Options Operational Details

This Addendum is attached to and made part of the Service Schedule for the Hybrid WAN - MSS and describes additional terms which apply to all Service Options available with the Solution.

### **1. Billing and Payment Terms.**

- 1.1** In no event shall Supplier be liable for the fraudulent or illegal use of the Services by any customers or end-users of Customer, or for any amounts that Customer is unable to collect from its customers, End Users or others (if applicable). Customer shall pay the fees specified in the mutually agreed upon Order Form and in any signed and approved additional Order Forms, in accordance with the terms thereof.
- 1.2** If Standard Billing option is selected by Customer, Supplier shall submit an invoice ("Invoice") to Customer after the end of the applicable Billing Period, which shall include total charges for the applicable Billing Period and for any prior period for which appropriate charges were not invoiced. Customer shall pay the Invoice amount to Supplier: i) in the Applicable Currency, ii) by wire transfer or such other method as the Parties may agree in writing, and iii) within the applicable Payment Period. In no event shall Supplier be liable for the fraudulent or illegal use of the Services by any customers or end-users of Customer, or for any amounts that Customer is unable to collect from its customers, End Users or others (if applicable). Any Invoice disputes must be submitted by Customer to Supplier within 45 days of date of the relevant Invoice.

**2. Reservation of Rights.** All right, title and interest in and to the Service and all Intellectual Property Rights associated with and in the Service shall at all times remain vested in the Service Provider and its licensors, and Customer shall acquire no rights, express or implied, in the Service, other than the right to use granted in this Service Level Agreement. Customer will not, directly or indirectly, reverse engineer, decompile, disassemble or otherwise attempt to derive source code or other trade secrets from Supplier and/or its third party vendors.

**3. Restrictions.** Service Provider will not access, read or copy content other than by electronic methods and for the purposes of providing the Services. However, Service Provider may utilize the malware, spam, botnets or other information related to the Service for the purpose of: (i) maintaining and improving the Services, (ii) complying with all legal or contractual requirements, (iii) making certain content (e.g. spam, phishing or the like) available to its security partners, and (iv) anonymously aggregating and statistically analyzing the content and (v) other uses related to analysis of the Service.

**4. Local Loops.** For a DSL circuit component of a Service, the feasibility and the acceptance of an Order conducted by Supplier does not fully guarantee the success of delivery of the access circuit and corresponding Service. During the course of delivering the Service, it may be found after Supplier placement of a DSL order to the local carrier, that the Site does not qualify for the DSL access circuit, or that the DSL access circuit will be feasible but with different peak bandwidth (DSL synchronization rate) as specified in the Order Form. In such case the Customer can cancel the Service without charges; and Supplier will endeavor to propose an alternative commercial and technical proposal with a different type of access circuit, that the Customer can choose to accept or not" and "Service Level Target for Service delivered through Local Loops offered using non-wireline technology are subject to the overriding Service Level Target as detailed on the Order Form.

**5.** The following terms shall apply if Customer requires Customer Premises Equipment:

**5.1 General:** When Customer requires CPE for any of the Service options available in this Solution, CPE shall be either sold by Supplier to Customer or provided by Supplier as part of the Service and Supplier shall provide CPE support services as specified in Order Form ("**CPE Support Services**"). CPE shall be used only in conjunction with the Supplier Service for which the CPE was ordered or other Services subsequently authorized by Supplier ("**Associated Service**"). The Customer is entitled to use the CPE and the chosen level of CPE Support Services together with the Associate Service for providing an aggregate service but shall not use them (or components of each) separately. If the Associated Service is terminated by Customer, Supplier shall have the right to terminate provision of the CPE (unless the CPE has been previously sold to Customer) and the CPE Support Services. In such event, the Customer shall be liable to pay the cancellation charge as specified in the Order Form, if the termination occurs within any minimum commitment period. Alternatively, if the Parties agree that the provision of the CPE and/or the CPE Support Service can continue after the termination of the Associated Service, an ancillary charge as decided by Supplier shall be payable by the Customer. CPE Support Services may be provided in whole or part by one or more agents or contractors on behalf of Supplier. The Customer may also be required to deal directly with an agent or contractor on certain aspects of the Service. The following additional conditions shall apply:

- 5.1.1** Where CPE is provided to Customer as part of the Service, Supplier shall retain title to the CPE at all times.
- 5.1.2** Risk in the CPE transfers to the Customer from the time it is delivered to the relevant Customer Site for installation. Customer must immediately inform Supplier if the CPE is damaged in any way on delivery.
- 5.1.3** At termination or expiry of the Service Supplier shall recover the CPE which shall be in good condition and good working order (other than reasonable wear and tear) or Customer shall be required to pay compensation for any damage or cost of replacing the damaged CPE.
- 5.1.4** The Customer shall pay an ancillary charge if the Supplier, at the Customer's request, provides the CPE Support Services, installation, configuration and testing, or undertakes other work at a Customer Premises outside business hours (except where required by the Service levels).

**5.2 Installation and Commissioning of CPE:** For the purposes of installation and configuration of the CPE at each Customer Site, the Customer shall provide information about the Customer Site. The Customer shall provide, at its cost, the assistance Supplier reasonably requires to install and commission the CPE, including to:

1. Designate a coordinator who shall be available during the installation and commissioning of the CPE and shall have sufficient authority to make decisions on behalf of the Customer;



2. Give Supplier employees, agents access (including escorted access if required) to the Site to install, maintain, repair, replace and remove the CPE and any associated cabling and other equipment;
3. Clearly label all existing telecommunications and computer cabling at or near the Site or which will be near cabling to be installed for the CPE or the Associated Service;
4. Ensure that, during installation and commissioning and, if required by Supplier, technical personnel are present who are knowledgeable about the systems at the Site.

If the installation date is rescheduled at the request of the Customer on less than seven (7) Business Days' notice; or because the Site space is not ready or Supplier is unable to gain access to the Site premises; or for other reasons attributable to the Customer; then the Customer will incur a rescheduling fee equal to one hundred percent (100%) of Supplier's standard installation charge for a similar Site. Supplier may not be able to reschedule installation to a date requested by the Customer if the Customer gives less than 7 Business Day notice of that requested date.

### **5.3 On-Site support for CPE:**

**5.3.1** Where appropriate for the ordered service option, Supplier shall provide the following on-site support services at Customer Site:

1. Investigation and repair of reported physical faults in accordance with fault service availability and response times set out in the Service Schedule or Customer Order Form;
2. Supply of parts and materials used in undertaking this work; and
3. Installation of all mandatory engineering and factory change notices issued by Supplier.

**5.3.2** The Customer shall pay an ancillary charge if the Customer reports a fault but Supplier determines that there is no problem or that the problem is not a fault covered by the Support Services; or Customer requests other assistance which is not within the support services.

**5.3.3** The Customer must pay to Supplier an ancillary charge to cover the costs of Supplier relocating at Customer's request CPE within a Customer Site; and an installation charge if the Customer requests CPE to be relocated to another Customer Premises.

**5.4 Customer Access Rights to CPE:** Under the Fully Managed Option, Customer shall not be allowed to obtain read / write access to the CPE. On an exceptional basis, when Customer requests write access (with written communications) to the Supplier Managed CPE, Supplier will review such requests before granting permission for a specified duration. Supplier shall track all Customer activities using such exceptional access permissions/rights. Any use/misuse of the write access permissions shall be Customer's responsibility and in no event Supplier shall be liable for any loss, damages, including indirect and consequential in nature by the use of such permissions / rights. In case of unauthorized access or access attempts being found, Supplier shall initiate appropriate actions including criminal prosecution as per the law of the land.

**5.5 Installation and Commissioning of CPE for SDWAN Select:** For the purposes of installation and configuration of the CPE at each Customer Site, the Customer shall provide information about the Customer Site.

**5.5.1** Supplier shall use reasonable endeavors to:

For zero touch provisioning (self-installation by Customer)

- a. Deliver the CPE to the Customer Site.
- b. Supplier will stage, validate boot configure, install the operating system software before delivering CPE to the Customer Site.
- c. Customer will unpack shipment, install equipment (mount equipment to the rack), complete cabling (power cord, cabling as per Supplier instructions and connect the WAN link at CPE port at Customer Site.

For Assisted CPE (Installation by Supplier's field engineer)

- a. provide at least five (5) Business Days' notice of the installation date. In such notice Supplier will inform the time during which Supplier requires access to the Customer Site and any special Site access requirements;
- b. deliver the CPE to the Customer Site, and if delivered prior to the installation date the Customer shall store the CPE in a secure location;
- c. The field engineer will unpack and inventory at the CPE, install the CPE in accordance with the agreed plan, connect electrical power cord to the CPE, validate the expected CPE boot sequence, and if necessary install the operating system software ordered with the CPE. Thereafter the field engineer will connect the CPE to the Underlay Network and test the CPE against agreed ready for service criteria.

**5.5.2** Supplier is not responsible for:

- a. any inability to meet ready for service criteria, where the BYON access requirement information provided by the Customer is inaccurate or incomplete;
- b. any customization of software or any installation of software other than the operating system software ordered;
- c. resolving operating system software or CPE hardware problems caused by third-party products, or by factors beyond Supplier's reasonable control;
- d. providing any hardware, unless separately ordered by Customer, required to run new or updated operating system software;
- e. the condition and maintenance of the Customer Site and, the installation and maintenance of all in-premises cabling, including cabling from the Customer's network termination unit to the CPE, which are the Customer's sole responsibility;
- f. Any configuration of CPE unless provided by Supplier pursuant to Customer's applicable order.

**5.5.3** The Customer shall provide, at its cost, the assistance Supplier reasonably requires to install and commission the CPE, including to:

- a. designate a coordinator who shall be available during the installation and commissioning of the CPE and shall have sufficient authority to make decisions on behalf of the Customer;
  - b. give Supplier employees, agents full access (including escorted access if required) to the Site to install, maintain, repair, replace and remove the CPE and any associated cabling and other equipment;
  - c. clearly label all existing telecommunications and computer cabling at or near the Site or which will be near cabling to be installed for the CPE or the associated service;
  - d. ensure that, during installation and commissioning and, if required by Supplier, technical personnel are present who are knowledgeable about the systems at the Customer Site.
- 5.5.4** If the installation date acknowledged by Customer in writing is rescheduled at the request of the Customer on less than seven (7) Business Days' notice; or because the Customer Site space is not ready, or Supplier is unable to gain access to the Customer Site; or for other reasons attributable to the Customer; then the Customer will incur a rescheduling fee equal to one hundred percent (100%) of Supplier's standard installation charge for a similar site. Supplier may not be able to reschedule installation to a date requested by the Customer if the Customer gives less than seven (7) Business Day notice of such requested date.
- 5.6 Customer Access Rights to CPE for SDWAN Select:** For fully managed support services, direct access to CPE is not allowed. Configuration changes to CPE will be allowed only through Supplier's self-service portal. In case of unauthorized access or access attempts being found, Supplier shall reserve the right to stop the applicable Service with immediate effect.

[END OF ADDENDUM]





**Addendum 4 – MSS Components Operational Details**

This Addendum is attached to and made part of the Service Schedule for the Hybrid WAN - MSS and describes additional terms which apply for MSS components of the Solution:

**1. Bundled Managed Security Services.**

- 1.1** CPE may be furnished by Supplier or a Supplier Affiliate or licensor for use at Supplier or Customer's premises as part of Bundled Managed Security Services. The CPE ordered shall be stated in the Order Form, which will also include the pricing and shipping address. Unless otherwise agreed to by the Parties in writing, Customer shall be responsible to pay Supplier for the charges associated with the delivery, installation and configuration of the CPE. With respect to software, Supplier or its Affiliate or licensor retains exclusive ownership of all software which is provided to Customer on a subscription basis as part of the Bundled Managed Security Services and Supplier or its Affiliate or licensor shall be responsible for any and all duties, charges, and applicable import taxes, including VAT and/or withholding taxes, with respect to the software. With respect to hardware, Supplier may provide the hardware as part of the Service, as provided in the applicable Order Form.
- 1.2** If Supplier provides to Customer the hardware as part of the Service, title and ownership will remain with Supplier or a Supplier Affiliate or licensor. As the owner of record, Supplier or Supplier Affiliate or licensor shall (i) be the licensor of record and (ii) obtain all necessary import/export licenses related to the hardware. Supplier or a Supplier Affiliate or licensor shall be responsible for any and all duties, charges and applicable import taxes, including VAT and/or withholding taxes, with respect to the hardware. Risk in the hardware transfers to the Customer from the time it is delivered to the relevant Customer Premises and Customer shall be required to pay compensation for any damage to the hardware or the cost of replacing the damaged hardware. Customer must immediately inform Supplier if the hardware is damaged in any way on or after delivery. Customer shall procure and maintain all risk insurance against loss or damage to the hardware for not less than the full replacement value of the hardware. Upon termination of the Agreement, Customer shall return the hardware within five (5) business days after termination to Supplier or Supplier's Affiliate or licensor, as determined in Supplier's sole discretion.
- 1.3** Upon expiration or other termination of Bundled Managed Security Services, Customer shall permanently delete all Supplier provided software associated with such Bundled Managed Security Services and destroy any related software disks (or other media) and documentation, and certify to Supplier in writing that the foregoing has been completed.

**2. Service Limitations.** The Services are not warranted to operate uninterrupted or error free. New security threats are constantly evolving and a product or Service designed to provide protection from such threats will be able to insulate network resources from all security threats and vulnerabilities, and are no guarantee against unsolicited e-mails and undesirable Internet content. Products and Services are not fault tolerant and are not designed or intended for use in hazardous environments requiring fail-safe operation, including without limitation aircraft navigation, air traffic control systems, weapon systems, life-support systems, nuclear facilities, or any other applications in which product or Service failure could lead to death, personal injury, or property damage. Customer acknowledges products or Services for testing, assessing, scanning or monitoring the security of network resources, including implementation and deployment, may disclose or create problems in the operation of such resources; therefore, Customer and its employees and agents represent and warrant that (i) they are fully authorized by the Customer and the owners of the network resources to enter into this Agreement and each Order Form, and (ii) they and the owners of such network resources understand and accept the risks involved which in some circumstances could include without limitation, down time, loss of connectivity or data, system crashes or performance degradation.

**3. Third-Party Products.** Supplier will pass any Third Party Product warranties through to Customer to the extent Supplier is authorized to do so. Customer agrees to indemnify Supplier against any claims made by third parties with respect to Customer's misuse of Third Party Product(s) supplied hereunder. Customer acknowledges and agrees that the vProxy Service is provided by Zscaler, Inc. ("**Zscaler**"), a third party service provider of Supplier. Customer further acknowledges and agrees that to receive the vProxy Service Customer must enter into a separate end user agreement (which may be the click thru, EUSA or MSA) (the "End User Agreement") directly with Zscaler, Inc. regarding the use of the software made available in the Service. The End User Agreement is available from Zscaler Inc.. Breach of such End User Agreement shall entitle Supplier to immediately terminate the Service. Other than as expressly set forth in this Service Level Agreement, no license or other rights in the Service are granted to the Customer and all such rights are hereby expressly reserved.

**4. Audit.** At Customer's own expense, Customer or its authorized representatives may audit Supplier's Facilities, records and documents pertaining to the Supplier's provisioning of Services to Customer during the term of the Agreement. Customer and its representative shall provide Supplier a thirty (30) days prior written notice of such audit request. Notwithstanding the foregoing, for audit requests from a government regulator or authority supported by a written confirmation from such regulator or authority, Supplier will endeavor to meet such other timeline as may be reasonably requested by said regulator or authority. Customer and its representatives (i.e., third party auditors, consultants, etc.) shall enter into satisfactory confidentiality undertakings. Both Parties shall agree in writing an audit scope and schedule. Supplier shall provide a copy of ISO, ISAE or other relevant reports or certifications to the Customer to assist in formulating and limiting the scope of the audit appropriately. Customer will perform such audit during normal business hours only and in accordance to generally accepted auditing standards. Notwithstanding any other charges set forth herein, Supplier will Charge Customer at Remote Hands Charges rates for all audits except for the first audit conducted in any given year, provided that the first audit shall not be more than four (4) hours. For the purpose of this clause, "Remote Hands Charges" shall mean a minimum rate of [INR 15,000/- (for India locations) and US\$ 250/- (for outside India locations)] per hour or such other rate as agreed in the audit Schedule subject to change depending on the location of the audit, and such Remote Hands Charges will cover Supplier Charges for providing Customer access to Supplier Facilities and personnel during the audit. The audit will be conducted by Customer with the utmost integrity, employing an acceptable level of skill and technical knowledge. Prior to any personnel performing any such audit, Customer represents and warrants that it will perform, or will cause to be performed, appropriate background screening of the personnel (including personnel of its third party representatives) appointed to perform such audit and the personnel is of a good repute. Supplier shall not permit an audit to be performed by any third party auditing firm (including its personnel) or consultant (including its personnel) that has been blacklisted or that has not been properly screened as set forth above. Customer will take all necessary care to avoid loss or damage to Supplier property and to prevent unnecessary and excessive consumption of Supplier personnel time. Customer will indemnify Supplier for any resulting damage to Supplier's property and additional costs incurred by Supplier in pursuant to facilitating the audit. Access to premises or web links provided to Customer as reasonably required to perform the audit shall be subject to Customer's strict adherence to Supplier's Safety, Security and Privacy policies and procedures then in effect. No images of the premises may be taken or made and no documents may be copied (or otherwise duplicated), altered or removed from the premises without Supplier's prior written consent. Supplier shall retain the necessary records as required under law and provide

reasonable assistance during the audit. Customer's representative shall declare all the IT equipment's that it owns, before entering the Supplier's site for audit. Upon completion of the audit, Customer shall share the audit report within (30) thirty days from the date of completion of the audit otherwise the audit shall be deemed to have resulted in no findings.

[END OF ADDENDUM]



## Addendum 5

### DEFINITIONS

This Addendum is part of the Service Schedule for the Hybrid WAN – SDWAN - MSS Solutions Portfolio and describes defined terms used in that document. In the event of a conflict between any terms in this Addendum and a definition in the General Terms governing the Solution Agreement, the definitions in this Addendum shall govern.

**"Bundled Managed Security Services"** means the combination of Supplier-provided hardware and software along with certain Managed Security Services. Bundled Managed Security Services also include Supplier-provided maintenance for the software and hardware provided as part of the Bundled Managed Security Services.

**"Business Day"** means any day other than Saturday, Sunday or a day which is a public holiday in the country where the Service is provided.

**"Business Hour"** means any hour from 9am to 5pm on a Business Day.

**"Caller Line Identification"** or **"CLI"** means a service whereby the caller's number is transmitted and presented to the called party.

**"Class of Service"** or **"COS"** means the priority of the IP packets that can be set and sent to Supplier Network as part of the GVPN Service Class of Service package ordered by Customer as set out in the Customer Order Form. COS values can be a combination of COS 1, 2, 3, 4, 5 or 6.

**"Class of Service Package"** means predetermined packages of Classes of Service as detailed in the Appendix and which is a standard of service ordered by Customer as set out in the Customer Order Form.

**"Customer Portal"** means the website(s) where Customer and Users access the Service(s).

**"Customer Premises Equipment"** or **"CPE"** means, certain hardware and/or software provided by Supplier and installed at Supplier or Customer Premises to facilitate Supplier delivery of Managed Security Services.

**"Enterprise Traffic Profile"** or **"ETP"** means data moving across a network at a given point of time which consists of up to 95% TCP and up to 5% UDP excluding data designated as COS-1.

**"GVPN Port"** means a VPN access point to which Customer is connected to the Supplier Network via a provider edge router, and which is the Service Access Point for the delivery of Unmanaged Service to Customer.

**"IAS"** means Internet Access Service formerly known as Internet Leased Line.

**"Internet Emergency"** means an incident has affected a significant portion of Supplier's protected Customer networks, or the public internet. Such emergencies are declared through Supplier's security services operations center (S-SOC).

**"Managed Security Services"** means those managed security services which allow an organization to outsource the management of certain internet security functions as further described in this Service Schedule. Managed Security Services may include, without limitation, managing and monitoring, implementation, deployment, training, security assessment, and security scanning.

**"Mean Time to Restore"** or **"MTTR"** is the average time to restore service for a specific connection during Service Outage(s). The length of all Service Outages related to Customer is totaled at the end of the billing month and is divided by the total number of Trouble Tickets opened by Customer for that month.

**"Monthly Recurring Charge"** or **"MRC"** means the charge payable by Customer to Supplier for each relevant service every month during the duration of the Agreement.

**"Planned Maintenance"** means any preventative, routine or scheduled maintenance which is performed with regard to the Services, any CPE or any component thereof, or any of Supplier's hardware or software necessary for the provision of the Services, which Supplier or its agents reasonably believe is necessary in order to prevent or remedy a defect which may affect Customer's use or access to the Services. Performance of Planned Maintenance will normally be carried out on Saturdays 8AM – 10AM, US Eastern Standard Time (GMT -0500) or performed during monthly maintenance windows on the second Saturday of every month from 8AM-4PM, US Eastern Standard Time (GMT -0500). Supplier shall endeavour to give Customer at least seven (7) day notice of any Planned Maintenance event.

**"Priority 1 Security Incident"** means high-risk events that have the potential to cause severe damage to Customer's environments and require defensive actions within 30 minutes.

**"Priority 2 Security Incident"** means lower-risk events that have potential to impact Customer's environments and require actions within 12-24 hours of notification.

**"Priority 3 Security Incident"** means low-risk events or low confidence events that have low potential to impact Customer's environments and should be further investigated within 1-7 days but may not be directly actionable.

**"Qualifying Incidents"** means the incidents for which Customer raises a Trouble Ticket and which are confirmed by Supplier as a fault or Service degradation or an incident where a Trouble Ticket is raised by Supplier.

**"Qualified Down Time"** means that portion of a Qualifying Incident that is not an Exclusion.

**"Scheduled Maintenance"** means any maintenance of the Supplier Network or to any Supplier Network element which is a part of Customer's service and for which Customer shall be sent a notice of Scheduled Maintenance a minimum of 24 hours in advance. Notice of Scheduled Maintenance will be provided to Customer's designated point of contact by a method elected by Supplier (telephone, email, fax, account manager).

**"Service(s)"** means the Managed Security Services and may include Bundled Managed Security Services, as further described in this Service Schedule.

**"Service Access Point"** or **"SAP"** means the logical or physical element which acts as the demarcation point between Customer's domain and Supplier's domain, representing the point at which Service is available and specific Service level targets are committed and measured.

**"Service Availability"** means the duration that the Firewall platform is available to access, calculated on a monthly basis.

**"Service Commencement Date"** means (i) the date Customer has accepted or is deemed to have accepted the Services in accordance with the provisions of the MSA or applicable Service Schedule; or (ii) the date Customer begins using the Services other than for testing purposes, whichever date is earlier.

**"Security Content update"** means a content update designed to enhance the detection capabilities of a security product. These updates are published from time to time as new security vulnerabilities/threats are identified. Examples include updates to IPS signature, virus definitions, SPAM signatures, etc. Example may not apply to the specific products used in this offering.

**"System Compromise"** means an event which results in unauthorized access, loss, disruption, or destruction of information resources where malicious intent is identified.

**"Service Level Agreement"** means the document so entitled applicable to a Managed Security Service.

**"Service Outage"** or **"Outage"** means an instance when Customer is unable to convey traffic to one (1) or more Sites via the Supplier Network (other than an Exclusions) which results in Service Unavailability.

**"Service Unavailability"** means the duration of any Qualified Down Time experienced at a Service Access Point.

**"Site"** or **"Managed Site"** means the site owned or controlled by Customer which is directly connected to Supplier's PoP and which hosts a physical element(s) which is managed by Supplier as set out in the Customer Order Form.

**"Supplier Network"** means the telecommunications network and network components owned, operated and maintained by Supplier and its Affiliates, including points of presence (**"PoP"**). The Supplier Network does not include Customer Premises Equipment (**"CPE"**) such as modems, routers, etc., local data links between a POP and Customer's location or any networks or network equipment not owned or controlled by Supplier.

**"Third Party Product(s)"** means any software and/or hardware that are supplied to Customer under this Agreement but that are not produced by Supplier. Third Party Products may include hardware, software and other related products.

**"Trouble Ticket"** means the official method used by Customer to advise Supplier of a potential Service Outage.

**"VPN"** means virtual private network.

**"WAN"** means "wide area network."

**"Users"** means the persons authorized by the Customer to use the Service.

[End of Addendum]

