TATA COMMUNICATIONS

IZO SDWAN-Hybrid WAN
Web Module

Addendum 1

Hybrid WAN Option Operational Details

This Addendum is part of the Service Schedule for the IZO SDWAN- Hybrid WAN 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, subject to the Service Terms.

2. Supplier Responsibilities. Supplier shall use reasonable endeavors to:

2.1 Give at least 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 Site (which shall be during Business Hours unless Customer otherwise agrees) and any special site-access requirements;

2.2 Deliver the CPE to the Site, and if delivered prior to the installation date 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, and install the operating system software ordered with the equipment;

2.4 Test the CPE against the ready for function criteria provided by Customer, as relevant to the ordered service, such criteria to be reasonably acceptable to Supplier; and

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 Customer, where the Internet access requirement information provided by 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 Customer's site, and the installation and maintenance of all in-premises cabling, including cabling from Customer's NTU to the Customer Equipment or CPE, which are Customer's sole responsibility; and

3.6 Any configuration of CPE unless ordered under appropriate service option.

[END OF TEXT]

Addendum 2

(A) Hybrid WAN Service Tier & SLA Definition Charts and (B) SDWAN Select Service Tier

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. **India SLA Tier Locations**.

SLA Tier	PoP and SLA Tier
Tier 1	Ahmedabad, Bangalore. Chennai, New Delhi, Emakalim Hyderabad, Kolkata, Mumbai (other than those listed in Tier 2), and Pune
Tier 2	Bhopal, Bhubaneshwar, Coimbatore, Gurgao, 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)
Tier 3	Adoni, Agra, Ahmed Nagar, Ajmer, Allahabad, Alleppy/ Alpuzha, 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, Sonepat, Surat (Udhana),Thirussur, Tiruchirappallli, Tirupati, Tiruppur, Tumkur, Udaipur, Vododara Jambuva, Valsad, Varanasi, Vellore Warangal

3. **Outage Classification; Severity Level**.

Priority	Incident Type	Definition
Severity 1	Hard	• Total loss of Service such that Packet Delivery is prevented between the affected SAP and all other SAPs in the VPN due to unavailability of the SDWAN CPE or the SDWAN software failure; or serious degradation makes service unusable. (Customer is unable to use the service due to the serious degradation and ready to release it for immediate testing).
Severity 2	Soft	• Degraded Service, not prevented from functioning, however not at expected levels of performance and productivity, e.g, Marginal Packet Loss or Intermittent Errors, link or protocol flapping, Application Performance Issue or Slowness or Throughput. (Customer still wants to use the services and is not ready to release it for immediate testing).
Severity 3		• A Service problem that does not seriously affect service or network availability or functionality as used in Customer's business. • A single non-service specific quality or Service enquiry.
Severity 4		• Customer requests technical support in testing its equipment and verifying service.
Severity 5		• Non- Service affecting, e.g.: incident report or any other queries not covered by Severity 1-4.

4. 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	IZO	BYON
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

5. SDWAN Select Service Tier. IZO SDWAN Select Service CPE break/fix 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
Sweden	Stockholm				
Taiwan	Taipei				
Thailand	Bangkok				
Turkey	Istanbul	Ankara			
United Arab Emirates	Abu Dhabi	Dubai			
United Kingdom	London	Birmingham	Manchester	Leeds	Liverpool
	Glasgow	Portsmouth	Southampton	Bristol	Newcastle
	Sheffield	Edinburgh	Cambridge	Leicester	Coventry
	Belfast	Aberdeen			
United States	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	
Uruguay	Montevideo				
Venezuela	Caracas				
Vietnam	Ho Chi Minh City	Hanoi			

6. **Cisco SDWAN Service Tier**. IZO Cisco SDWAN CPE break/fix 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				
India	Bangalore	Chennai	Hyderabad	Pune	Mumbai
	Gurgaon	Noida	Chandigarh	Kolkata	Ahmedabad
	Vadodara	Mangalore	Coimbatore	Bhubaneswar	Guwahati
	Trivandrum	Kochi	Raipur	Nagpur	Indore
	Jaipur	Lucknow	Delhi	Patna	Vishakapatnam

[End of Addendum]

Approved As To Form:
LEGAL DEPARTMENT
Standard
(No Changes)
ANY CHANGES TO THE STANDARD TEMPLATE DOCUMENT SHALL NOT BE EFFECTIVE.

TATA
APPROVED BY LEGAL
LEGAL
TATA COMMUNICATIONS
DEPARTMENT
STANDARD

Addendum 3

All Service Options Operational Details

This Addendum is attached to and made part of the Service Schedule for the IZO SDWAN-Hybrid WAN 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 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 Customer can choose to accept. 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 the 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**"). 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, 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 Customer. CPE Support Services may be provided in whole or part by one or more agents or contractors on behalf of Supplier. 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 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; and

5.1.4 Customer shall pay an ancillary charge if Supplier, at 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, Customer shall provide information about the Customer Site. Customer shall provide, at its cost, the assistance Supplier reasonably requires to install and commission the CPE, including to:

5.2.1 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 Customer;

5.2.2 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;

5.2.3 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;

5.2.4 Ensure that, during installation and commissioning and, if required by Supplier, technical personnel are present who are knowledgeable about the systems at the Site; and

5.2.5 If the installation date is rescheduled at the request of Customer on less than 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 Customer, then Customer will incur a rescheduling fee equal to 100% of Supplier's standard installation charge for a similar Site. Supplier may not be able to reschedule installation to a date requested by Customer if 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 Site:

a. Investigation and repair of reported physical faults in accordance with fault service availability and response times set out in the Service Schedule or Order Form;

b. Supply of parts and materials used in undertaking this work; and

c. Installation of all mandatory engineering and factory change notices issued by Supplier.

5.3.2 Customer shall pay an ancillary charge if 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 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 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, Customer shall provide information about the Site.

5.5.1 Supplier shall use reasonable endeavors to:

a. For zero touch provisioning (self-installation by Customer):

i) Deliver the CPE to the Site;

ii) Stage, validate boot configure, and install the operating system software before delivering CPE to the Site; and

iii) 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 Site.

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

i) Provide at least 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;

ii) Deliver the CPE to the Customer Site, and if delivered prior to the installation date, Customer shall store the CPE in a secure location; and

iii) The field engineer will unpack and inventory 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 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 Site, and the installation and maintenance of all in-premises cabling, including cabling from Customer's network termination unit to the CPE, which are the Customer's sole responsibility; and

f. Any configuration of CPE unless provided by Supplier pursuant to Customer's applicable order.

5.5.3 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 Customer;

b. Give Supplier employees and 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; and

d. Ensure that, during installation and commissioning and, if required by Supplier, technical personnel are present who are knowledgeable about the systems at the Site.

5.5.4 If the installation date acknowledged by Customer in writing is rescheduled at the request of Customer on less than 7 Business Days' notice, or because the Site space is not ready, or Supplier is unable to gain access to the Site, or for other reasons attributable to Customer, then Customer will incur a rescheduling fee equal to 100% of Supplier's standard installation charge for a similar site. Supplier may not be able to reschedule installation to a date requested by Customer if Customer gives less than 7 Business Days' 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

PROACTIVE INCIDENT RESPONSE SERVICE

Part I. GENERAL TERMS

1. SOLUTION DESCRIPTION.

1.1. Services Description: The Proactive Incident Response ("**PIR**") Service is a fully managed Security Event monitoring and Incident Management ("**SIEM**") system for event aggregation, correlation, threat identification, incident management, log management, and compliance reporting offered by Supplier through its Security Operations Centre ("**SOC**"). The PIR Service is available on a 24x7 basis and provides Security Event response of correlated output from the SDWAN Select and SIEM system. Customer may access the PIR Service from its native IT environment, for use across all of its SDWAN Select components. The Solution permits Customer to select from both Service and Cloud deployment options. The PIR Service offers the managed SIEM ("**mSIEM**") Standard Service option. Customer selects this option in the Order Form which is further described in Part II below.

1.2. Features: The PIR Service comes with the following features: (i) long term event storage for analysis (for Cloud mSIEM, storage is provided for 3 months online and 9 months offline), (ii) Security Event correlation, and (iii) integrated threat intelligence.

2. SERVICE LEVEL AGREEMENT. The service level agreement ("**SLA**") applicable to the PIR Service is set-out in Annex A, which forms part of this Exhibit.

PART II. PIR mSIEM SOLUTION –SERVICE AND DEPLOYMENT OPTIONS

This Part II describes the Services that are available to Customer as part of the Solution. If the option described below is not selected by Customer in an Order Form, then the corresponding terms are not applicable to the Solution as described in that Order Form.

1. SERVICE OPTION.

1.1. mSIEM Standard. Under this option Supplier provides: (i) Log collection, filtering, aggregation, categorization, normalization, and forwarding, (ii) long term Event Storage for analysis (for Cloud mSIEM, storage time-frames are 3 months online and 9 months offline), (iii) Security Event correlation and notification, (iv) Security Event updates, (v) Service request acknowledgment and resolution, (vi) Standard Use Case enablement, and (vii) Integrated threat intelligence.

2. DEPLOYMENT OPTIONS. The deployment option for Customer is as follows:

2.1 Cloud mSIEM: In this option, Supplier provides a multi-tenant mSIEM Service hosted either completely or partially in Supplier's Cloud environment. This multi-tenant-capable deployment provides multi-device correlation, event generation, triage, and escalation to customer security monitoring teams. Security Event monitoring is enriched with Supplier's threat intelligence.

3. OPERATIONAL REQUIREMENTS. Before Supplier deploys the PIR Service, the Parties must complete certain pre-requisite requirements, which depend upon local conditions. Supplier shall inform Customer of the requirements before provisioning Services. Customer shall cooperate with Supplier to comply with the requirements within a reasonable time period. Examples of these requirements include:

a) Returning a Supplier-provided information gathering document at least 5 days prior to a scheduled business requirement mapping session;
b) Review of role and responsibility distribution between Supplier and Customer stakeholders;
c) Returning a redlined draft project plan to Supplier 5 days after receipt of it from Supplier;
d) Making available requisite experts from the network group to finalize the connectivity arrangement between Supplier and Customer; and
e) Making available requisite experts responsible for managing the log sources in Customer's environment who can make available requisite data associated with log sources.

4. CUSTOMER RESPONSIBILITIES. Customer shall inform Supplier's SOC team of any changes to the environment for hardware or software of devices that are subject to mSIEM monitoring. Supplier is not responsible for any unknown threat that may arise due to infrastructure changes for which Customer has not provided Supplier with advance notice. Additional Customer responsibilities are as follows:

a) Provision of documentation on architecture and security processes in Customer environment;
b) Provision of relevant information on any changes that could potentially impact service;
c) Notifying one week in advance of any change in Customer contact information;
d) Security Event response, including forensics, is Customer's responsibility;
e) Making available requisite stakeholders to participate in incident management process;

f) Making sure that designated stakeholders raise Service Requests for any changes to be done for event source integration and report generation; and

g) Hardware management up to the OS layer and backup and license renewal requirements, unless the same is provided by Supplier as part of its Services.

PART III. SOLUTION RESTRICTIONS AND CONDITIONS

This Part III describes restrictions and conditions applicable to the PIR Services, regardless of the constituent Services selected by Customer. Customer agrees to comply with the following terms of use:

1. Before Supplier can turn-up the Solution, the Parties must complete certain provisioning requirements (e.g. Customer's site readiness). These requirements depend upon local conditions and Supplier shall inform Customer of the requirements before provisioning Services. Customer shall cooperate with Supplier to complete such operational requirements within a reasonable time period.

2. Resale of Service by Customer is not allowed except when Customer enters into a contract with Supplier specifically for resale of the Service and provides advance written notice to Supplier prior to selling to each new end customer that will use the subscribed Service.

3. Supplier or its suppliers may, consistent with applicable laws, monitor the Services from time to time for quality assurance and fraud detection.

4. Customer agrees that Supplier has no control over the content of information transmitted through the Services (whether visual, written or audible).

5. Unless otherwise set forth in the applicable Order Form, the Services do not include internet access service or telecommunications transport circuits, which are Customer's responsibility. Customer is responsible for Customer's own network security policy and security violation response procedures. Customer consents to Supplier aggregating anonymized security event log data to look at trends and real or potential threats. This security event log data with similar data of other clients so long as such is aggregated in a manner that will not in any way reveal the data as being attributable to Customer.

6. The provisions of Part III of this Service Schedule shall survive the termination of any Solution Agreement and/or Order Form to which this Service Schedule applies.

PART IV. ADDITIONAL TERMS AND CONDITIONS

1. **DELIVERY OF SOLUTION.** Supplier will endeavor to provide the Solution in accordance with the applicable target dates set out in the Order Form(s). Unless otherwise expressly stated in a SLA, the Customer understands that these are target dates only and that the Supplier does not represent that it can provide the Solution in accordance with these dates and will not be liable to Customer for any damages arising either directly or indirectly from the failure to provide the Solution on or before these dates. Supplier will perform appropriate acceptance testing, as determined by Supplier, to verify that Solution is ready for Customer's use.

2. **ACCEPTANCE OF SOLUTION.** Upon Customer's receipt of an In-Service Notification for Solution, Customer will have 5 days to test the Solution and notify Supplier in writing of its acceptance or non-acceptance of the Solution. Customer may only reject a Solution on the basis that the agreed technical specifications for the Solution have not been met. Such rejection must be in writing and shall reference the specific Solution features not delivered. If the Solution features referenced by the Customer are not referenced in the Order Form, these will not be considered as basis for rejection. If Customer notifies Supplier of its non-acceptance, Supplier shall conduct further tests of the Solution and deliver a new In-Service Notification to Customer, provided that, regardless of anything herein to the contrary, the following will actions will be deemed acceptance of the Solution:

2.1 Customer's failure to notify Supplier of its non-acceptance of the Solution Service within the foregoing time period; or
2.2 Customer's Use of a Service, as incorporated into the Solution, in commercial operations.

[END OF TEXT]

Annex A
mSIEM SERVICE SUPPORT AND CORE SERVICE SLAs

This Annex A is part of the PIR Service ("**Qualifying Services**"). Where Supplier fails to meet a target commitment under a given service level agreement defined below ("**SLA**") (excluding Service Credit Exceptions) and a trouble ticket is opened, Customer will be eligible for Service Credits set forth below. There are two general categories of SLA: i) **Support SLAs**, and ii) **Service SLAs**. Support SLAs apply to the back-office activities in supporting Customer's use of the Solution. Service SLAs relate to the operation of applications contained in the Solution. The following SLAs are available with the Solution:

A) SERVICE SUPPORT SLAS

1. SECURITY EVENT NOTIFICATION SLA.

1.1. Definition: Supplier shall notify Customer of Security Events using an automated email, sent to a pre-determined Customer Security Contact email address, that contains details of the alert generated by the PIR system.

1.2. Measure: Supplier's compliance with Security Event Notification SLA Target is be measured from the time Supplier receives a Security Event to the time it is auto forwarded to the Customer Security Contact email address.

1.3. Applicability: Security Event Notification Target is available only for the mSIEM Standard Service options.

1.4. Target: The Targets are set forth in the table below:

Service Option	Security Event Type	Target	Percentage of Compliance
Standard	Priority 1	60 minutes	90-95
			<90
	Priority 2	120 minutes	90-95
			<90
	Priority 3	240 minutes	90-95
			<90

2. SECURITY EVENT UPDATE SLA

2.1. Definition: Supplier Security Analysts shall provide Customer with updates of all P1, P2, and P3 Security Events based on analysis of a Standard Event Sources within the time periods specified in the table below.

2.2. Measure: Supplier's compliance with Security Event Update SLA is measured using the interval between consecutive updates on an P1, P2, and P3 level Security Event in Supplier's case management system and notified through an email notification to the Customer Security Contact email address. Under this SLA, Supplier shall contact the Customer's Security Contact by telephone for P1 Incidents, and by email for P2 and P3 Incidents. During a P1 event escalation, Supplier shall continue attempting to contact the Security Contact until a contact is reached or all escalation contacts have been exhausted. Operational activities related to events and updates are documented and time-stamped within Supplier's case management system, which shall be used as the sole authoritative information source for purposes of this Target.

2.3. Applicability: Security Event Notification Target is limited only to mSIEM Standard Service options.

2.4. Target: The Targets are set forth in the table below:

Service Option	Incident Type	Target	Percentage of Compliance
Standard	Priority 1	240 minutes	90-95
			<90
	Priority 2	480 minutes	90-95
			<90
	Priority 3	720 minutes	90-95
			<90

3. SERVICE REQUEST ACKNOWLEDGEMENT SLA

3.1. Definition: Supplier shall acknowledge its receipt of Customer's Service Request within Supplier's case management system within the time periods specified in the table below.

3.2. Measure and Calculation: Supplier's compliance with Service Request Acknowledgement SLA Target is be measured from the time Supplier receives a Service Request from a designated Customer Security in Supplier's case management system to the time the Service Request is assigned to Supplier analyst. Operational activities related to Service Request acknowledgments are documented and time-stamped within Supplier's case management system, which shall be used as the sole authoritative information source for purposes of this determining compliance with the Target.

3.3. Target: The Targets are set forth in the table below:

Service Option	Target
Standard	2 hours

4. SERVICE REQUEST IMPLEMENTATION SLA

4.1. Definition: Supplier shall implement Customer Service Requests within the time specified in the table below. This Target is based on actual time of implementation, and not on the time that Customer was notified of the completion of the request. Customer is entitled to make 2 such requests per month.

4.2. Measure: Supplier's compliance with Service Request Implementation SLA Target is be measured from the time Supplier receives a Service Request from a designated Customer Security in Supplier's case management system, to the time the Service Request is marked as completed in Supplier's case management system by a Supplier analyst.

4.3. Target: The Targets are set forth in the table below:

Service Option	Target
Standard	24 hours

.

5. STANDARD USE CASE ENABLEMENT. Supplier's Standard Use Case Enablement SLA enables Standard Use Cases commensurate with the service package purchased within Supplier's mSIEM. The number of use cases is subject to availability of requisite Event Sources within Customer environment which will be determined post completion of the business requirement mapping ("BRM") session with the Customer. The maximum number of use cases that Supplier Target's to implement is limited to 25, subject to a feasibility analysis by the Supplier analyst's as part of BRM session Supplier will enable additional use cases based on analysis of latest threats and subject to internal validation and sign-off. Supplier will build additional standard cases at an additional charge for specific requirements from Customer for an additional fee.

Service Level Agreement (SLA)	mSIEM – Standard
Standard Use Case Enablement	1. ✔

B) SLA RULESAND EXCEPTIONS

1. SLA RULES: Subject to the Service Credit Exceptions, all SLAs above are subject to the following rules:

1.1 It is further clarified that mSIEM is not a device specific service and is capable of capturing incidents and events from various devices. Therefore, if there are occurrence of certain critical events which may be missed by mSIEM but for whom the service rules are configured and mutually agreed between parties), then only the aforesaid Service Credits shall be applicable. However due to ever changing scope of security threats there may be unknown threats for which service rules cannot be defined and/or device does not have capability to identify and send security events at that point of time. In those case the above SLA and Service Credits shall not be applicable.

1.2 Supplier's Service Level Targets focus on the identification of and response to Security Incidents. These targets assume that traffic has successfully reached the security platform, and therefore the device has the ability to process the traffic against the installed policy and generate a logged event. Traffic that does not logically or electronically pass through a security platform, or that does not generate a logged event is not covered under this SLA.

1.3 Where it is necessary to do so in the Supplier's reasonable opinion, Supplier may take or Supplier may require Customer to take proactive measures to adjust Customer's security agent configuration in the event that there is an excessive amount of Intrusion detection / prevention data

[End of Annex]

Addendum 5

DEFINITIONS

This Addendum is part of the Service Schedule for the IZO SDWAN-Hybrid WAN 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.

"3rd Party VNF" means the Virtual Network Function deployed in Virtual Machine (VM) of IZO SDWAN CPE. i.e., virtual firewall, virtual WAN Optimization service, etc.

"Bring Your Own Network" or **"BYON"** means Customer underlay network not provided by Supplier.

"**Business Day**" means any day other than the weekend (as locally commonly understood) or a day which is a public holiday, in both cases, in the country where the Service is provided.

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

"**CRFS Date**" means committed ready for service date for a customer Site.

"Customer LAN" means a network belonging to Customer, which is connected to Supplier SDWAN Service at one or more SDWAN SAPs.

"Datapath" means a service offering providing transport across an Underlay Network. Examples include IPSEC tunnel, MPLS, etc.

"DoS" means protection resource exhaustion of CPEs from malicious flood traffic.

"DSL" is a standard transmission technology used to provide data communication (e.g. ADSL, SDSL) circuits over copper wires.

"**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.

"Headend" means the set of hardware and software which forms the IZO SDWAN service central nodes, wherein all the policies of communications between the IZO SDWAN service sites are configured. The IZO SDWAN service sites communicate with this headend for all routing and policy decisions.

"**End to End Monitoring**" or **"E2E"** means the monitoring of the Service level targets from one Customer Site CPE to another Customer Site CPE.

"Excused Outage" means those items set forth in Part III of the Service Schedule, "Exclusions".

"**Fault Isolation**" means the process of finding the cause of an identified or reported fault in order to take corrective measures for resolution.

"**Fault Reporting**" means the process of reporting or notifying about an identified fault with reference to the SAP of a Service by Supplier to Customer.

"Features" means the items included in a Service or Option.

"**IPSec**" (Internet Protocol Security) means a secure network protocol suite that authenticates and encrypts the packets of data sent over an internet protocol network.

"**Managed CPE**" means a CPE which is supplied, installed, managed, monitored and maintained by Supplier (or a third-party provider of Supplier). The maintenance covers the replacement of defective hardware parts and the provision of new software versions for patches or upgrades purposes. Management includes configuration management, 24x7 helpdesk, fault isolation, logical fault management (repair), change management and reporting.

"**Minimum Point of Entry**" or "**MPOE**" means the closest practical point to where a telecommunications fiber-optics and/or copper cablings enters a building or multi-unit building (also known as a telecom closet).

"**Mean Time to Restore**" or "**MTTR**" is the averaged time to restore service at a particular SAP from more than one incident each causing Service Unavailability. The duration of all Qualified Downtime is totalled at the end of the billing month and is divided by the total number of associated Trouble Tickets opened by Customer for that month.

"**Monthly Recurring Charge**" or "**MRC**" means the monthly recurring charges for the Service (at a Site), including any Service(s), as set out in the Customer Order Form.

"**Non-Recurring Charge**" or "**NRC**" means the one-time non-recurring charges to be made by Supplier for installing, commissioning and provisioning of the Service (at a Site) as set out in the Order Form.

"Options" means the items that Customer can select.

"**Outage Classifications**" means the priority as it relates to the severity of a particular Service Outage.

"Physical Break/Fix" means rectification of the CPE hardware.

"Planned Maintenance" means any preventative, routine or scheduled maintenance which is performed with regard to the Services, the Supplier Network or any component thereof, which Supplier or its agents reasonably believe is necessary in order to maintain the Service or prevent or

remedy a defect which may affect Customer's use or access to the Services. Supplier shall endeavor to give Customer at least 7 days' notice of any Planned Maintenance event.

"Planned Installation Date' is a mutually agreed date between Customer and Supplier to install the service.

"Policy" means a set of rules that describe the desired handling of Application traffic.

"**Proactive Notification**" means Supplier shall monitor in-band the reachability of the CPE and proactively dispatch an unreachability notification to Customer.

"**Qualified Down Time**" means the duration recorded by Supplier of a Qualifying Incident which is characterized by Supplier as a Severity 1 fault.

"**Qualifying Incident**" shall mean an incident other than for an Excused Outage 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.

"Redundant" means a service option under which the Service is provided via two CPE such that there is no change in available Performance Functions nor generation of a Severity 1 Qualifying incident should one CPE fail.

"Routine" option is Service provided via a single CPE.

"Service" means stand-alone service offered as part of a Solution.

"**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 percentage of time that the Service is available at the Service Access Point.

"**Service Credits**" means credits provided by Supplier to Customer for Service Unavailability or failure to meet other Service Level Targets as set out herein.

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

"**Service Unavailability**" means Qualified Down Time at a SAP.

"**Self-Service Portal**" means the portal Supplier provides to Customer for changing policies by itself.

"**Service Availability**" means the percentage of time the Supplier platform is available for use.

"**Site**" shall mean a site owned or controlled by Customer or end user where the SAP is located.

"Solution" means the combination of Services, Options, and Features that Customer buys.

"**Stateful Firewall**" means a network firewall that tracks the operating state and characteristics of network connections traversing it. Only packets matching a known active connection are allowed to pass the firewall.

"**SDWAN**" means a software-defined WAN.

"SDWAN Edge" means the virtual or physical "machine" that terminates the Supplier side of the SAP connection between Customer and the Service Provider on one side, and one or more WAN connections on the other side.

"**Third Party Network**" means a network service provided to Customer by service providers other than Supplier.

"**Tier 1 City**" means the metro cities where Supplier can provide greater SLA.

"**Time to Restore**" or "**TTR**" means at a particular SAP, the total time taken to restore service from an incident causing a Service Unavailability after a Trouble Ticket is opened by Customer.

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

"Tunnel Virtual Connection" or **"TVC"** means a point-to-point path between SD-WAN Edges across an Underlay Network Service that provides a well-defined set of transport characteristics (e.g., delay, security, bandwidth, etc.).

"Underlay Network" means a physical network that provides all or part of the connectivity associated with SDWAN Service.

"Underlay Network Service Provider" means an organization that provides an Underlay Network Service to Customer.

"**Universal Customer Premise Equipment**" or "**uCPE**" means equipment provided by Supplier and used as a physical SDWAN edge. In no event shall Supplier own or hold tile to CPE in a country where it is not licensed.

"vCPE_Cloud" or "Virtual customer premise equipment Cloud" means a virtual network function (VNF) image which is supplied, installed, managed, monitored and maintained by Supplier (or a third party provider or partner of supplier), which will be deployed in any third party public cloud platform.

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

"**WAN Interface**" means the physical interface of Wide Area Network on the CPE.

[End of Addendum]