



Annex E to SLA 1064_001: Shared Virtual Private Network (VPN) Service

Document No:	1064_E
Version:	3.0
Author:	Primrose Ramuageli
Effective Date:	01 April 2023
Electronic File:	1064_E ver 3.0

me

AS

Annex E : Wide Area Network Service Category

E1. Service Classification

The **Shared Virtual Private Network (VPN) Service** is classified as Managed Infrastructure in terms of the SITA Services Catalogue and is a mandatory service in terms of the SITA Amendment Act (Act number 38 of 2002).

E2. Reference(s)

1064_E 2.0

E3. Benefit Statement

No.	Aspect of business challenge	Value statement	
1	Economies of scale over shared capability (infrastructure, technology, resources, facilities, scalability)	Price and Economies of Scale	1. Shared capability for multiple customers results in lower unit cost based on shared infrastructure and bulk discounts. 2. Access connectivity can be provided from a selection of Service Providers, allowing for the most cost effective solution.
2	Reduction in Duplication	Elimination of duplication	Shared infrastructure for several customers eliminates duplication of infrastructure.
3	Security	Security	Secured policy based access, controlled from a central point, thus limiting possibility of violations.
4	Interoperability (e-Government)	Interoperability	Creates the platform for E-Government due to the integrated design principles of the NGN.
5	Quality Services	Quality	Provides an end to end Wide Area Network service with single point of contact supporting end to end tracking, monitoring and feedback.

mc



E4. Service Category: WAN

E4.1 Service Metric: Shared VPN service- Configured Service

Managed Infrastructure							Service Management			
Service Offering	Service Description	Configured Service			Workload		Service Components	Measurement		
		Basic features	Additional features required	Contracted	Cap	Metric		Unit of measure		
Shared VPN Service	Access connectivity to Shared Core infrastructure in the shared VPN (GOV VPN).	1. Shared VPN for Data services configured on the SITA NGN (GOV VPN) with authorized access to Transversal systems, DR services and other unique applications.				1. Shared VPN Services	1. 95% Carrier Provider Availability	1. % Availability 2. % Reachability 3. Hours		
		2. Provisioning of access links from client sites to the nearest SITA node for access into the shared VPN (GOV VPN). SITA has a total of 25 nodes across the country.					2. 95% Carrier Provider Reachability			
		3. Configuration and management of all client-owned Site Router infrastructure to ensure reliability, reachability and availability.					3. 95% of calls will be responded to and resolved as follows: a. Mean time to Respond MTTr): 4 hours b. Mean time to Resolve (MTTR): 16 hours			
		4. The NMS reports are available electronically via a Network Portal that is available 24/7 and are discussed on the Monthly Service Level meetings.	None Available			2. Access link infrastructure	1. 95% Access Link Availability 2. 95% Access Link Reachability 3. 95% of calls will be responded to and resolved as follows: a. Mean time to Respond	1. % Availability 2. % Reachability 3. Hours		

me



CONFIDENTIAL

[illegible]

we



E4.2 Services Detail: Shared VPN services

Service Category	Service Sub-Category	Service Component	Service Component Description	Service Measures	Definition of service measures	Service Level Metrics	Service dependencies
WAN	Shared VPN	1. Shared VPN services	Access connectivity to Shared Core infrastructure in the shared VPN (GOV VPN).	1. Availability 2. Reachability 3. MTTRespond 4. MTTResolve	1. Availability guarantee measurement will be based on NMS measurements 2. Mean time to Respond (MTTr) will be based on hours per incident priority and will be logged on the ITSM7 system.	1. 95% Carrier Provider Availability 2. 95% Carrier Provider Reachability 3. 95% of calls will be responded to and resolved as follows: a. Mean time to Respond (MTTr): 4 hours b. Mean time to Resolve (MTTR): 16 hours	1. Signed User Requirement Specification. 2. Signed Shared VPN Proposal. 3. Signed Shared VPN SLA. 4. Back-to-Back agreements with Service Providers.
WAN	Shared VPN	2. Access link infrastructure	Provision of access links from client sites to the nearest SITA node for access to client services in the shared VPN (GOV VPN).	1. Availability 2. Reachability 3. MTTRespond 4. MTTResolve	1. Reachability guarantee measurement will be based on Access Link Reachability target. 2. Mean time to Respond (MTTr) will be based on hours per incident priority. Access Link Infrastructure.	1. 95% Access Link Availability 2. 95% Access Link Reachability 3. 95% of calls will be responded to and resolved as follows: a. Mean time to Respond (MTTr): 4 hours. b. Mean time to Resolve (MTTR): 16 hours	1. Signed Shared VPN Proposal. Signed Shared VPN SLA. 2. Network Service Application Form to be completed and signed by client. 3. Back-to-Back Agreement with Access Link Service Providers.
WAN	Shared VPN	3. Customer Edge Router Management	Configuration and Management of all client-owned Router infrastructure to ensure reliability, reachability and availability.	1. Availability 2. Reachability 3. MTTRespond 4. MTTResolve	Availability guarantee measurement will be based on Site Router Reachability target. Mean time to Respond (MTTr) will be based on hours per incident priority.	1. 95% Site Router Availability 2. 95% Site Router Reachability 3. 95% of calls will be responded to and resolved as follows: a. Mean time to Respond (MTTr): 4 hours.	1. Signed Shared VPN Proposal. 2. Signed Shared VPN SLA. 3. Maintenance Contract by client on client-owned Customer Edge Router equipment.

CONFIDENTIAL

						b. Mean time to Resolve (MTTR): 16 hours	
WAN	Shared VPN	4. Network Management Services	Provision of Network Management Services & Client Portal reflecting operational performance statistics per client environment and availability of all SLA related reports.	Availability	% Availability of Network Management Services & Client Portal.	1. 99.5% Availability of Network Management Services. 2. Availability of all SLA related reports within the first week of every following month.	1. Configured for Shared VPN. Back-to-Back agreements with Service Providers. 2. Availability of infrastructure and software to provide Network Management Services.
WAN	Shared VPN	5. Service Desk : Call Answering	The handling of agreed inbound communication channels within acceptable response times and quality levels.	Responsiveness and quality of Service Desk	Number of calls handled that have breached 20 seconds before being answered) / Total number of calls received for the calendar month (within stipulated service hours.)	1. 80% of calls handled in 20 seconds over a period of one calendar month. 2. 80% Satisfaction Levels, i.e. (Inbound calls)	Users participating in the survey to obtain a reasonable sample.
WAN	Shared VPN	6. Incident and Request Management : Monitoring and escalation	Implementation of the Incident/ Request Management process supporting effective monitoring and escalation as defined by the escalation procedure with the Customer.	Incident / Request Escalations	% of automated escalations carried out as per agreed escalation procedure.	90% Escalations as per agreed escalation procedure.	As per agreed scope of the escalation procedure enabled by the Customer and/or 3rd Parties.
WAN	Shared VPN	7. Incident Management : Reporting on performance against all	Provision of Incident/ Request Management reports on the performance of all	Availability of Incident/ Request Management	Provision of access to automated reports on :	90% Availability of Service Management Reporting Platform.	Customer and/or 3rd Parties must have internet access.

CONFIDENTIAL

	Incidents and Request	Technical Support environments.	Performance Reports.	a. Mean Time to Resolve (MTTR) per service category and priority		
				b. Mean Time to Respond (MTTr) per service category and priority		

me



E5. Roles and responsibilities

Service Sub-Category	Service Component	Responsibilities	
		SITA	Client
Shared VPN	Shared VPN services	1. Establish, operate, monitor and manage Shared VPN services. 2. Operate, monitor and maintain Core Infrastructure. 3. Ensure sufficient core bandwidth capacity to cater for Shared VPN clients. 4. Inform the Client of any change requests on the WAN infrastructure (downtime or disruptive changes) at least 5 working days in advance of such change. No penalties will apply during this downtime period. 5. Establish and maintain processes for Shared VPN fault, incident and change management. 6. Service reporting reflecting Core operational performance statistics.	1. Report all identified shared VPN related calls via the SITA Toll free number (0800 11 55 75). 2. Compliance with SITA's recommended technical standards and specifications to realise this SLA. 3. Advising SITA of significant changes in usage forecasts, planned implementation of future changes or new service requirements where SITA will be impacted. 4. Inform SITA in writing of any Client initiated change controls that will affect the Shared VPN service. 5. Awareness and acceptance of the limitations of the Shared VPN services.
Shared VPN	Access link infrastructure	1. Provisioning of different types of access technologies for connectivity from client sites to SITA NGN. 2. Execute and resolve Service Request Applications. 3. Present Access Link quotations to client on receipt of an official URS. 4. Process orders for procurement and installation of access link infrastructure on receipt of an official government order. 5. Manage application process for data lines to TelCo. 6. Monitor and managed Access link availability. 7. Establish and maintain processes for fault, incident and change management. 8. Service reporting reflecting Access link performance statistics.	1. Report all identified Access link related calls via the SITA Toll free number (0800 11 55 75). 2. Submit completed and signed Service Request Applications to SITA. 3. Issue SITA with an official government order on acceptance of a SITA proposal or quotation for Ad Hoc access link services. 4. Advising SITA of significant changes in usage forecasts, planned implementation of future changes or new service requirements where SITA will be impacted.
Shared VPN	Customer Edge Router Management	1. Configuration and management of all client-owned Site Router infrastructure. 2. Provide configuration support for new installations in respect of Client's site routers. 3. Provide re-active configuration support on Client's site routers. 4. Monitor and manage site router availability. 5. Establish and maintain processes for fault, incident and change management.	1. Report identified incidents and log calls for configuration of new router installations to the SITA Service Desk via the Toll free number (0800 11 55 75). 2. Hardware maintenance and support on site routers remains the responsibility of the Client. 3. Physical transport of Client's site routers for configuration purposes (for new installations), to and from the nearest SITA Office. 4. Safeguarding of Client's LANs from security-related threats and virus.

CONFIDENTIAL

	6. Service reporting reflecting site router performance statistics.	
		5. Acquisition and supply of hardware and software requirements in compliance with SITA's recommended.
		6. Compliance with SITA's recommended technical standards and specifications to realise this SLA.
		7. Advising SITA of significant changes in usage forecasts, planned implementation of future changes or new service requirements where SITA will be impacted.

E6. Pricing

E6.1 Data Line and Port Costs

Building	Town	Province	Circuit No	Band-width	Port Costs	Data line Cost	Total Year 1
MOWANENG	POLOKWANE	Limpopo	ENI12-0001035	16Meg	R37 920.00	R3 762.00	R41 682.00
GOVERNMENT COMPLEX	LEBOWAKGOMO	Limpopo	730643422	40Meg	R82 436.00	R7 607.26	R90 043.26
					SUBTOTAL PER MONTH		R131 725.26
					PLUS: 15% VAT		R19 758.79
					TOTAL PER MONTH		R151 484.05
					TOTAL FOR 12 MONTHS		R1 817 808.60
					Estimate pricing year 2 (2024/2025)		R1 899 428.21
					Estimate pricing year 3 (2025/2026)		R1 984 712.53
					Estimate pricing year 4 (2027/2027)		R2 073 826.13
					Estimate pricing year 5 (2027/2028)		R2 166 940.92

Notes:

1. Pricing will change once a service is commissioned, decommissioned, upgraded or downgraded, and will be reflected on the monthly invoices.
2. Year one is actual and the other years CPI added for budgetary purposes and the new MTEFs will be applied in that specific year or when there are new guidelines from National Treasury.
3. The Client shall be responsible to pay SITA a fixed cost per port per month. In addition, the Client shall pay SITA the once-off installation cost and the monthly TelCo access data line costs from the date of installation of the access data line. The access data line cost is based on current TelCo rates that are normally adjusted annually.

CONFIDENTIAL

4. The WAN port cost for connectivity to the network will be levied in arrears, with effect from the first day of the month, following the month in which the TelCo data line was installed.
5. Telco prices will change once a service is upgraded or downgraded.
6. Annual price escalations will be based on Consumer Price Index (CPI) and/or annual Vendor pricing adjustments.
7. Pricing excludes shared internet service cost.



E7. Penalties

E7.1 Port Costs

If SITA fails to achieve the service levels on the **Carrier Provider (SITA Core related to the Port Cost) services** that are stipulated in paragraph E4.1 above, and provided that such a failure is not caused by a failure of the client to comply with its obligations and duties in terms of this SLA, SITA shall compensate the client by raising a credit note with an amount calculated as set out in paragraph (a) below.

- (a) If the achieved service level falls below the % availability and reachability as per identified class of service for **Carrier Provider Services**, averaged over any given month during business hours only, the compensation amount shall be calculated at **2.5%** of the monthly Port cost for the affected sites.

E7.2 Access links

If SITA fails to achieve the service levels on the **Access links (Last mile link related to the Vendor Cost)** that are stipulated in paragraph E4.1 above, and provided that such a failure is not caused by a failure of the client to comply with its obligations and duties in terms of this SLA, SITA shall compensate the Client by raising a credit note with an amount calculated as set out in paragraph (a) below.

- (a) If the achieved service level falls below the % reachability as per identified class of service on **Access Links**, averaged over any given month during business hours only, the compensation amount shall be calculated at **2.5%** of the monthly Access Link costs for the affected sites.

E8 Dependencies and constraints

E8.1 Dependencies

- (a) Shared VPN services
 - (i) Service Level Agreement with Carrier Service Provider.
- (b) Access link infrastructure
 - (i) Correctness of completed Service Request Applications as submitted by the Client.
 - (ii) Service Level Agreement with Access Service Provider.
- (c) Customer Edge Router Management
 - (i) Availability and effective functioning of TelCo link to enable re-active remote configuration support.
 - (ii) Compliance with SITA's recommended technical standards and specifications with respect to acquisition of site routers and related hardware and software.
 - (iii) Maintenance Contract by client on client-owned Customer Edge Router equipment to ensure performance and availability of hardware and software.
 - (iv) Performance and availability of hardware and software that is supplied by the Client.
 - (v) Performance and availability of data lines that are supplied by TelCo.
 - (vi) Reasonable access to the Client's sites.
 - (vii) Two working days for router configuration is depended on the quantities of routers to be configured per Client.

E8.2 Constraints

- (a) Shared VPN services
 - (i) Client's own Network Security Policy that will govern the Dedicated VPN.
 - (ii) Minimum Information Security Standard (MISS) Instructions.
- (b) Access link infrastructure
 - (i) Service Level Agreement with TelCo.

E9. Certification:

We hereby certify that this Annex covers the full extent of the Shared VPN as required. We further accept the service and the price accordingly.

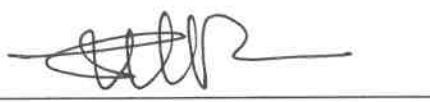
This Annex shall be effective from 1 April 2023 until 31 March 2028.

Thus done and signed at Polokwane on this 16th day of March 2023

Signature: 

Full names: Nape Nchabalele
On behalf of **Limpopo: Office of the Premier**
And duly authorised thereto

Thus done and signed at Polokwane on this 24th day of March 2023

Signature: 

Full names: Mmamodi Molele
On behalf of **State Information Technology Agency SOC Ltd**
And duly authorised thereto