AIRPORTS COMPANY
SOUTH AFRICA

Annexure A - Scope of Work

For

LAN / Wireless / IP Telephony and Network Security Services

Description:

The Supply, Installation, Commissioning, Support and Maintenance of IT Network, IP Telephony and IT Security Infrastructure Services for a period of 60 Months to Airports Company South Africa

Tel: +27 (0)11 723 1400 Fax: +27 (0)11 453 9353
The Maples, Riverwoods, 24 Johnson Road, Bedfordview, Gauteng, South Africa, 2007
PO Box 75480, Gardenview, Gauteng South Africa, 2047

www.airports.co.za

Airports Company South Africa SOC Ltd Reg No. 1993/004149/30 VAT no. 4930138393

Contents

List of Tables:

1.0 LAN/WAN/WLAN/IPT AND SECURITY SCOPE OF WORK OVERVIEW AND OBJECTIVES

1.1 Background

Airports Company South Africa (ACSA) invites qualified and experienced service providers to submit proposals for the comprehensive support, maintenance, and enhancement of its IT network and security infrastructure. As a critical enabler of our operations, ACSA IT seeks a strategic partner to deliver robust, reliable, and innovative solutions that align with our commitment to operational excellence and technological advancement.

This RFP outlines the requirements for a service provider capable of maintaining and building a resilient IT network and security ecosystem, underpinned by a stringent Service Level Requirement (SLR). We aim to leverage technologies to optimise performance, enhance security, and futureproof our investments to support ACSA's long-term growth and operational objectives. Bidders must demonstrate technical expertise, proven experience, and a forward-thinking approach to delivering scalable and sustainable solutions.

We look forward to receiving detailed proposals that showcase your capability to meet ACSA's high standards and contribute to our vision of secure, efficient, and future-ready airports that elevate the global aviation experience.

1.2 High-Level Scope of Work Required

The list below covers the high-level scope included in this RFP.

1.2.1 Campus and Data Centre Wired and Wireless Networks

1.2.1.1 **MPLS VPN Core -** The provider may, from time to time and as and when requested by ACSA in writing, supply and install, maintain and support the hardware, software and configuration of the MPLS VPN core network currently prevalent at JNB, CPT and DUR airports and including any other deployments during the contract period. Refer to Table 1.

1.2.1.2 **Access Switches -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain and support the hardware, software and configuration of the access layer network. This includes fixed and modular, 8, 12, 24, 48 port power over Ethernet and industrial switches**.**

1.2.1.3 **Data Centre Networking -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain and support the hardware, software and configuration of the data centre switches, Unified Computing (UCS) hardware and virtualisation hardware.

1.2.1.4 **Network Management -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain and support the software and appliances. The providers shall ensure accurate and full management of all wired and wireless devices as well as the Catalyst Centre clusters themselves.

1.2.1.5 **Wireless Network -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain, and support the hardware, software and

configuration of the wireless infrastructure, including indoor and outdoor access points, wireless controllers and Public WIFI Captive Portal.

1.2.1.6 **WAN Optimisation and Traffic Analysis -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain and support the hardware, software and configuration of the WAN optimisation infrastructure.

1.2.2 **IP Telephony and Collaboration**

1.2.2.1 **Unified Communication Manager Services -** call control and session management – The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain and support the hardware, software and configuration of the call control and session management services currently installed and including any new deployments during the contract period.

1.2.2.2 **Voice Gateways -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain, and support the hardware, software, and configuration of the Voice Gateways currently installed and any new deployments during the contract period.

1.2.2.3 **Voice Recorders -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain and support the hardware, software and configuration of the Voice recorder appliances currently installed at all ACSA airports, during the contract period**.**

1.2.2.4 **Telephone Billing System -** The provider may, from time to time and as and when requested by ACSA in writing, update and maintain the telephone user billing database, during the contract period**.**

1.2.2.5 **Unified Contact Centre for Automated Call Distribution (ACD) -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain and support the hardware, software and configuration of the CUCX appliances currently installed and including any new deployments during the contract period**.**

1.2.2.6 **Unity Connection for enterprise-grade voicemail and unified messaging platform -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain and support the hardware, software and configuration of the Server appliances currently installed and including any new deployments during the contract period**.**

1.2.2.7 **Integrated Management Controller to allow for a separate, independent management interface to the servers hosting the call control platform -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain and support the hardware, software and configuration of the call control management server controllers installed and including any new deployments during the contract period.

1.2.2.8 **Network Virtual Servers -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain and support the hardware, software and configuration of the standalone Network Virtual Infrastructure and systems installed and including any new deployments during the contract period from a networking operations perspective.

1.2.3 **Network Firewalling and Security**

1.2.3.1 **Site Firewalls -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain, support and monitor the software, hardware and

configuration of the Firewall infrastructure currently installed and including any new deployments at other sites during the contract period.

1.2.3.2 **Perimeter Firewalls -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain, support and monitor the software, hardware and configuration of the Perimeter Firewall infrastructure, currently only prevalent at ORTIA and including any new deployments during the contract period.

1.2.3.3 **Distributed Denial of Service Appliance -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain, support and monitor the software, hardware and configuration of the Distributed Denial of Service (DDOS) protection appliance, currently only prevalent at ORTIA and including any new deployments during the contract period.

1.2.3.4 **Identity Services Engine -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain, support and monitor the software, hardware and configuration of the Network Access Control (NAC) or Identity and Access Management (IAM) Infrastructure and including any new deployments during the contract period**.**

1.2.3.5 **Web Security Appliances -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain, support and monitor the software, hardware and configuration of the Web Security Appliances currently installed and including any new deployments during the contract period**.**

1.2.4 **Public Wi-Fi**

1.2.4.1 **Captive Portal -** The provider may, from time to time and as and when requested by ACSA in writing, supply, install, maintain, support, monitor and administration of the Captive Portal as well as onsite connectors and associated On-premises servers currently installed at all ORTIA. CTIA, KSIA, PLZ. and including any new deployments at other sites during the contract period.

1.2.5 **Service objectives**

These objectives aim to establish a high-performing, cost-effective, and scalable IT infrastructure that supports ACSA’s operational efficiency and strategic growth.

1.2.5.1 **Robust Infrastructure -** Deliver a uniform, reliable, scalable, and resilient network and security infrastructure adhering to industry best practices and validated designs, ensuring consistent performance and adaptability to future needs.

1.2.5.2 **Guaranteed Service Quality -** Provide services with defined quality standards, backed by Service-Level Requirements (SLRs) and supported by Cisco Partner Support Services (or equivalent OEM), ensuring accountability and reliability.

1.2.5.3 **Streamlined Management -** Reduce ACSA's administrative burden by assigning network device management responsibilities to the provider, enabling efficient operations and resource allocation.

1.2.5.4 **SLR Adherence -** Achieve the Service Level Requirements outlined in the Statement of Work (SOW), ensuring all performance metrics and operational standards are consistently met.

1.2.5.5 **Business Agility -** Support ACSA's business initiatives as they arise, providing flexible and responsive services to align with strategic and operational objectives.

1.2.5.6 **Comprehensive Network Solution -** Deliver a high-quality, stable, flexible, managed, monitored, and sustainable LAN/WAN/WLAN, IP telephony, and security infrastructure that meets SLR standards, ensuring seamless connectivity and robust security.

1.2.5.7 **Scalable Service Delivery -** Enable ACSA to expand its service delivery and support capabilities to its business units, subsidiaries, and stakeholders, fostering growth and collaboration.

1.2.5.8 **Cost Efficiency -** Continuously lower service delivery and ownership costs by reusing or transitioning existing infrastructure and optimising current licensing agreements, maximising value and efficiency.

1.2.5.9 **Break/Fix Oversight -** Coordinate and monitor Break/Fix repairs, including those executed by third-party suppliers, to ensure timely resolution and minimal disruption to operations.

1.2.5.10 **IMACD Execution -** Perform approved Install, Move, Add, Change, Dispose and Delete (IMACD) services for hardware and software, ensuring smooth lifecycle management of IT assets.

1.2.5.11 **Asset Tracking -** Maintain accurate inventory records of in-scope software and hardware as required by ACSA, supporting compliance and efficient resource management.

1.2.5.12 **Employee Onboarding -** Provide technical orientation and training for new ACSA employees on existing systems and software, ensuring quick integration and productivity.

1.2.5.13 **End-to-End Service -** Include installation, deployment, ongoing support, and Break/Fix services for all in-scope service tiers, delivering a comprehensive and reliable service experience.

2.0 SERVICE ENVIRONMENT

2.1 Scope of the Infrastructure to be Supported

2.1.1 The following subsections and related Service Environment Appendices further describe the Scope of Services for the network environment to be supported. These Service Environment Appendices are to be maintained by the Service provider, reviewed with ACSA, updated by the provider, and made available to ACSA quarterly.

2.1.2 A high-level listing and description of hardware and software to be supported is provided.

Category	Service	Description
Hardware	Core and LAN	Cisco Catalyst 2960X Series Switches
		Cisco Catalyst 3650 Series Switches – Replacing 2026
		Cisco Catalyst 3850 Series fibre Switches – Replacing 2026
		Cisco Catalyst 9200 Series Switches
		Cisco Catalyst 9300 Series Switches
		Cisco Catalyst 3560CX Series Switches
		Cisco IE3100 and IE3200 Series Industrial Switches
		Cisco Catalyst 6807 -Series Switches - Used as MPLS P and PE nodes.
		Cisco Catalyst 9500 Series switches - Used as MPLS P and PE nodes.
		Cisco Catalyst 9600 Series switches - Used as MPLS PE nodes.
		HUAWEI S6730 Routing Switch
		HUAWEI S5731 Routing Switch
	Data Centre	Cisco Nexus 9300 Series
	WAN Optimisation and Traffic Analysis	Riverbed Steelhead CX770, CX3070, CX5055 and CX5070 Series
		Riverbed Steelhead Controller
		Riverbed Steel Central NetExpress
	Wireless	Cisco C9800-40-K9 and C9800-L-F-K9 wireless controllers
		Cisco CW9164, C9124, C9115, C9120 Series Access Points
		Cisco 1852, 2802, 3802, Series Access Points
	Unified Comms	Cisco UCS-C210M2-VCD2, UCS 240m3, UCSC-C240-M4S server appliance;
		Cisco UCS-C220M3S server appliance; Cisco Business Edition 7000H (M7) Appliance
		Cisco C8200-1N-4T Edge Gateways
		Cisco VG224 and VG-248
		Cisco 3900, 6900, 7800, 7900, 8800, 8900, 9900 series IP Phones
		Cisco ATA 186 Analogue Telephone Adapters;
		Cisco ATA 187 Analogue Telephone Adapters; Cisco VGC Phones;
		Cisco Unified SIP Phone 3900 Series
Software	Access Control	Security/Single Sign-On
		Cisco ISE
	Captive Portal	Cisco Spaces

Category	Service	Description
	Management	3x Cluster of Cisco Catalyst Centre Appliance (Gen 3) - 32 Core
		Unity Connection 11.5;
		Unified Communications Manager 11.5;
		Cisco Contact Centre 11.5;
		CIMC 4.3(5.240021)
		AdaptIT Telephone Management System
		PhonexOne TMS 3.00.009 (revision 00008);
		VMWARE ESXI Host client v7
		Libra Datavoice 11;
Network Firewalls and Security Appliances and Software		
Category	**Service**	**Description**
Hardware	**Firewalls**	Checkpoint 7000 - Security Gateway Appliance
		Checkpoint 6600 - Security Gateway Appliance
		Checkpoint 9100 - Security Gateway Appliance
	FW Management	Checkpoint Smart -1 600-M Security management Sender
	Web Security Appliances	Cisco WSA S396 Web Security Appliance
		Cisco WSA S196 Web Security Appliance
		Cisco WSA S300V Web Security Appliance
		Cisco WSA S100V Web Security Appliance
	ORTIA Perimeter	Cisco ASA5545
		Checkpoint Defence Pro 6-1
		Cisco Identity Services Engine
Software	**FW Software and Functionality**	Security Management - Monitoring Blade (MNTR)
		Mobile access Blade
		User Directory Blade
		Endpoint Security Secure Access Package 1 - 99 Seats
		IPv6 capability
		Anti bot
		Identity Awareness
		IPS
		URL Filtering
		Application Control
		Site to Site VPN
Public WIFI Appliances and Software		
Software	Portal Software	Cisco Spaces
		CMX 10
Hardware		CMX Connector Virtual Machine

Category	Service	Description
	Portal Hardware	CMX On Premises

Table 1 - High-Level List of Existing Infrastructure and Software

2.2 Service locations

2.2.1 A description and location of all ACSA facilities and office locations requiring in-scope network services.

Cluster	Airports in the regions	Site Code
Cluster 1	• OR Tambo International Airport	JNB
	• Aviation Park	AVP
	• Bram Fischer International Airport	BFN
Cluster 2	• Cape Town International Airport	CPT
	• George Airport	GRJ
	• Kimberley Airport	KIM
	• Upington International Airport	UTN
Cluster 3	• King Shaka International Airport	DUR
	• King Phalo Airport	ELS
	• Chief Dawid Stuurman International Airport	PLZ

Table 2 - Distribution of ACSA locations

SITE CODE	ADDRESS
JNB	O.R. Tambo International Airport, Airport Rd, Johannesburg, 1627
AVP	Aviation Park, Western Precinct, OR Tambo International Airport, Kempton Park, 1632
CPT	Cape Town International Airport, Matroosfontein, Cape Town, 7490
DUR	King Shaka International Airport, La Mercy, 4407
PLZ	Chief Dawid Stuurman International Airport, Allister Miller Drive, Walmer, 6070
GRJ	George Airport, Old Mosselbay Road, George, 6529
ELS	King Phalo Airport, Settlers Way, East London, 5200
KIM	Kimberly Airport, Compound Patterson Road, Kimberly, 8300
BFN	Bram Fischer International Airport, Bloemfontein, 9300
UTN	Upington International Airport, Diedericks Street, Upington, 8801

Table 3 - Detailed site schedule

2.2.2 This Site Schedule will be revised by agreement between the ACSA and the provider account manager/Service Manager from time to time to meet the ACSA's requirements at additional locations.

3.0 PRICING NOTES

The following notes should be considered when pricing services for this tender.

3.1 USD-influenced items can be adjusted with the Rate of exchange during the contract term, according to the process and terms in 4.0 **RATE OF EXCHANGE, QUOTATIONS, AND INVOICES**.

3.2 Bidder quotations can be added as additional information, but the pricing file must be filled in, in the format provided.

3.3 Only fill in columns in green in the pricing file.

3.4 **NOTE that ACSA reserves the right to reduce the scope depending on business needs. There is no guarantee that the full bill of materials will be executed.**

4.0 RATE OF EXCHANGE, QUOTATIONS, AND INVOICES

The following terms will be used to deal with the Rate of exchange during the term of the awarded contract for items affected by the rate of exchange as per the pricing files. It also details the requirements for quotations.

4.1 Quotations and Rate of Exchange

4.1.1 All initial Quotations for engagements will use a Fixed Rate of exchange. This rate will be communicated by ACSA to the provider on a 3-monthly basis. This rate will not be used for placing an order.

4.1.2 Once scoping for an engagement is completed and funds are secured. The provider will provide a final quote for the scope. This quotation must be fixed for a period of 14 days.

4.1.3 The final Quotation will be reviewed by the ACSA internal treasury department to approve the quoted rate of exchange.

4.1.4 ACSA will proceed with the order issuing process after treasury approval.

4.1.5 Should a Purchase order not be provided during the quote validity period (as per 4.1.2). The provider must supply ACSA with a Variance order quote once the Purchase order is received.

4.1.6 This Quote must clearly show the original Rate of Exchange and the actual rate of exchange (the spot rate for the day that the order is placed with the provider's supplier).

4.1.7 ACSA will proceed with obtaining approval of the Variance order quotation RoE.

4.1.8 Once approved, a Variance order will be processed.

4.1.9 Pricing is based on a fixed mark-up % per item type. ACSA may, at its own discretion, ask for the supplier quote to be provided for every engagement. This will be used to verify the landed cost and to audit if the % mark-up as quoted for the type of device is upheld as per the pricing schedule.

4.1.10 If products were previously procured by the provider for stock, then the original invoice for that stock should be provided as proof against the quotation.

4.1.11 All quotations to be provided in PDF and Excel format (editable). And must have all relevant fields as per the Pricing schedule.

4.2 Invoices

4.2.1 All invoices are to be accompanied by

I. Copy of Purchase Order
II. Proof of delivery, signed by both the provider and an ACSA representative, that also includes the relevant serial numbers.
III. Asset list in Excel format according to the template provided by ACSA.
IV. Proof of automated asset tracing activation.
V. Invoice to have the ACSA purchase order number coded on it.

4.2.2 All invoices not in dispute will be paid according to payment terms.

5.0 ASSET MANAGEMENT, TRACKING and LOSSES

Due to the nature of the equipment related to the services covered by this RFP, the following should be noted for special attention.

5.1 Asset management

5.1.1 ALL devices (new and returned) remain in the control of the provider until handed over to an ACSA user/representative. This handover needs to be recorded officially with a signed handover form signed by a duly authorised **ACSA employee**. The record must be attached to the ASSET record for future reference.

5.1.2 For approved disposals, the provider must wipe the device; certified proof must be provided and included in the service cost.

5.1.3 The history of every device must be kept in the asset register or system provided for at least 10 years.

5.1.4 An ACSA resource or representative and a provider representative must sign for all deliveries. Planning should consider this when deliveries to the onsite are arranged, as this will affect the Service levels.

5.1.5 On-site stock should be kept to the required levels to ensure service delivery according to SLRs.

5.1.6 The Service Provider must issue their on-site resources with asset scanners to reduce manual data capture and increase data quality.

5.1.7 Scanners provided should be wireless-capable.

5.1.8 Asset scanners must form part of the monthly fixed maintenance cost.

5.1.9 The monthly storeroom stock count is to be completed, with updated stock sheets to be submitted to ACSA and reported on in the monthly SLA meeting. Movements in the month to be accounted for in the summary schedule (listing device info, detail of asset move (i.e. end user it was moved to / new store or location it was moved to) and service request number supporting the move)

5.2 Asset Tags and tracking

5.2.1 ACSA will provide financial asset tags to the provider for affixing to the devices. Devices must be asset-tagged before being installed.

5.3 Asset movement

5.3.1 Any asset that must be transferred to another ACSA site by the provider for whatever reason must follow the ACSA asset transfer process before the movement.

5.3.2 NO device covered under the **onsite repair SLA** can be removed from an ACSA site. The device must be repaired onsite as per the SLA.

5.4 Losses

5.4.1 Any loss needs to be formally reported to ACSA within 2 days of the loss being detected.

5.4.2 Any device, whether new, decommissioned, operational or damaged, that is lost, for whatever reason, that is in the control of the Service Provider must be replaced at the Service Provider's cost.

5.4.3 The process of replacement must be actioned within 5 days after the loss is detected by either party.

5.4.4 Any loss where the Service Provider does not have enough proof that the device was NOT in their control (Issue forms, transfer forms) will be deemed in their control.

5.4.5 The following table lists the value and terms of the replacements:

Device Age	Replacement Terms
<=12 months	Replacement of device with a new device at the current prevailing ACSA standard
12 to < 18 months	Monetary Replacement of 90% of the original device's cost
18 to < 24 months	Monetary Replacement of 70% of the original device's cost
24 to < 30 months	Monetary Replacement of 60% of the original device's cost
30 to < 36 months	Monetary Replacement of 50% of the original device's cost
36 to < 42 months	Monetary Replacement of 30% of the original device's cost
42 to < 54 months	Monetary Replacement of 15% of the original device's cost
54+ months	Monetary Replacement of 10% of the original device's cost

Table 4 – Loss replacement terms and values

5.4.5.1 Monetary values must be credited to ACSA's account and will be used to procure new devices.

5.4.5.2 Monetary values cannot be allocated to outstanding monies for other invoices.

5.5 Replacement due to damage/malfunctions (in warranty)

5.5.1 The Service Provider must endeavour to fix a device rather than to replace it.

5.5.2 If a device needs to be replaced during its life due to damage or malfunction, the service provider must inform the ACSA representative and follow the provided asset disposal process for damaged/malfunctioning devices.

5.6 Equipment Ownership Transfer

5.6.1 Any equipment procured under the agreement only transfers ownership when delivered to an ACSA site, with the approved ACSA resource signature confirming receipt.

5.6.2 The provider must ensure off-site storage is available for the bulk of the equipment until site preparation is concluded.

5.6.3 All warranties and licenses of equipment only "start" when the equipment transfers ownership and must be activated with the OEM.

5.6.4 Although equipment ownership transfers, it is still the responsibility and accountability of the provider to manage the on-site equipment. Until such time, a transfer form is

obtained from an ACSA resource or representative, and the equipment is in the provider's control.

5.6.5 Any losses before obtaining the issue forms are for the provider's account.

5.7 Equipment Storage

5.7.1 All equipment is to be warehoused by the provider at no cost to ACSA until it is delivered.

5.7.2 Equipment delivered to the site will be installed in its final location where possible.

6.0 PERSONNEL

6.1 **Qualified Staffing** - The provider must supply professionally trained and appropriately certified personnel to fulfil the roles, responsibilities, and Service Level Requirements outlined in this service specification, ensuring high-quality service delivery.

6.2 **Certification Compliance** - The provider must maintain compliance with all ACSA-IT certification requirements throughout the contract term. Additional certifications, as communicated by ACSA, must be obtained within four months of the request. Key certification areas include Cisco DNA, Cisco ISE, Cisco APIC, data centre, unified communications, unified computing, hyper-convergence, Cisco WLAN administration, IP telephony, LAN administration, network management, Checkpoint and Cisco firewall administration, Cisco WSA, and OEM certifications for in-scope products and technologies. On-site personnel certification requirements, if applicable, are detailed in Table 5 - Minimum Resource Requirements.

6.3 **Onsite Resource Availability** - Suitably certified personnel must be available onsite at designated locations for preventative and corrective maintenance. While normal working hours apply, after-hours availability may be required to accommodate maintenance windows or resolve disruptive incidents, ensuring minimal service disruption.

6.4 **Flexible Resourcing Model** - The provider must adapt its resourcing model to meet the Service Level Requirements (SLRs) outlined in 15.0 SERVICE MANAGEMENT, utilising permanent onsite resources for preventative maintenance and variable offsite resources for corrective maintenance to ensure efficient and compliant service delivery.

6.5 **Restricted Resource Use** - Onsite resources may not be reassigned to projects without prior written approval from the ACSA Network Operations Manager or Infrastructure Manager, ensuring dedicated support for operational needs.

6.6 **Security Vetting** - All resources must undergo security vetting by the state security agency at a secret level. Required forms and documentation must be submitted within the first month of the contract. Any resource failing the vetting process must be replaced immediately to maintain security compliance.

6.7 **NDA Compliance** - All resources must sign the ACSA Non-Disclosure Agreement (NDA) provided in this tender, ensuring confidentiality and protection of sensitive information.

6.8 The table below indicates the minimum expectation for resources, whether on-site or variable. Please increase, as necessary.

Role	Location	High-Level Function	Minimum Resources Required and coverage window
Network Engineer (CCNA and HCIA, or better)	JNB – Onsite and remote	1st and 2nd Line Network Infrastructure support. Dealing mostly with IMACD's and specific reported incidents and service requests, and dispatching in-scope network, network security, voice, WIFI and managing WAN and 3rd Party connectivity related incidents. This function is performed from the service desk and includes 24x7x365 monitoring of the national infrastructure.	1 Resource must always be onsite.24x7x365 1 Resources available remotely daily 06h00-22h00.

Role	Location	High-Level Function	Minimum Resources Required and coverage window
Network Engineer (CCNA and HCIA, or better)	PLZ, ELS, GRJ, BFN, KIM and UTN – Variable	1st and 2nd Line Network Infrastructure support. Dealing mostly with IMACD's and specific reported incidents.	1 resource for each site. 6 in total- as required according to SLA
Senior Network Engineer (CCNP and HCIP, or better)	JNB – On-site	2nd and 3rd line daily operations support for national WAN, LAN, Core, MPLS, and Riverbed.	1 Person- Office hours
Senior Network Engineer (CCNP and HCIP, or better)	CPT - Onsite	2nd and 3rd line daily operations support for all CTN in-scope network Infrastructure	1 Person - Office hours
Senior Network Engineer (CCNP and HCIP, or better)	DUR - Onsite	2nd and 3rd line daily network operations support for all DUR and Regional Airports in-scope network Infrastructure	1 Person - Office hours
IP Telephony and Collaboration Administrator (CCNP Collaboration or better)	JNB, On-Site	2nd line daily administration and support of Cisco unified communications collaboration infrastructure nationally, excluding projects	1 Person - Office hours
Wireless Network Administrator (CCNP Wireless and HCIA-WLAN or better)	JNB, On-Site	2nd line daily administration and support of the National wireless infrastructure Administration and support of Public WIFI infrastructure	1 Person - Office hours
Network Security and Firewall Administrator (CCSE or better)	JNB – On-site	2nd line daily administration, support and configuration of the National network security infrastructure	1 Person- Office Hours
Enterprise network engineer (CCIE and HCIE)	JNB – Variable	Responsible for end-to-end design, implementation, and escalation-level support of complex network infrastructures. Advanced troubleshooting, performance optimization, and major incident resolution across enterprise routing, switching, wireless and IPT environments	1 Person – as required to meet SLA

Table 5 - Minimum resource requirements

6.9 The provider will be liable to pay office rental space for any resources that are deemed necessary to be located on-site at any ACSA premises. The applicable rates must be agreed upon between the provider and the ACSA Property Department.

6.10 The provider will be liable to pay parking fees for any resources that are deemed necessary to be located onsite or perform work under this contract at any ACSA premises.

6.11 The provider will be liable for any fees and training necessary to obtain ACSA Security Permits for any resources that are deemed necessary to be located onsite or perform work under this contract at any ACSA premises.

6.12 Certified resources will be required onsite for support, preventative, and corrective maintenance of the services during the coverage windows.

<table>
<tr><th>Service Class</th><th>Service Coverage Window</th></tr>
<tr><td>Airport Operating Hours</td><td>
<table>
<tr><th>Airport</th><th>Earliest opening hour</th><th>Latest closing Hour</th></tr>
<tr><td>JNB and AVP</td><td>24-hour operation</td><td>24-hour operation</td></tr>
<tr><td>CPT</td><td>05:00</td><td>23:00</td></tr>
<tr><td>DUR</td><td>04:00</td><td>22:00</td></tr>
<tr><td>PLZ</td><td>05:00</td><td>22:00</td></tr>
<tr><td>ELS</td><td>05:00</td><td>21:30</td></tr>
<tr><td>GRJ</td><td>06:00</td><td>20:00</td></tr>
<tr><td>BFN</td><td>05:30</td><td>20:00</td></tr>
<tr><td>KIM</td><td>06:00</td><td>20:00</td></tr>
<tr><td>UTN</td><td>06:00</td><td>18:00</td></tr>
</table>
</td></tr>
<tr><td>Standard Office Hours</td><td>Normal Office Hours - 08:30 - 17:00 on Mon - Fri, excluding public holidays</td></tr>
<tr><td>Extended Office Hours</td><td>Normal Office Hours - 06:00 - 18:00 on Mon - Fri, excluding public holidays</td></tr>
<tr><td>Weekday After Hours</td><td>After Hours – 18:00 – 06:00 on Mon – Fri, excluding public holidays</td></tr>
<tr><td>Weekends</td><td>Weekend and Public Holidays – 24 Hours Saturday and Sunday, including public holidays</td></tr>
<tr><td>Project & IMACD</td><td>All project and IMACD tasks that impact the live environment will take place after the last flight has departed and before the first flight departs/arrives in the morning. These hours vary from airport to airport, but generally the provider can plan to run project tasks between 23h30 and 05h00; times are subject to change and will be communicated timeously</td></tr>
</table>

Table 6 - Service Coverage Windows definitions

6.13 **Robust Resourcing Model** - The provider must implement a resourcing model that ensures compliance with Service Level Agreements (SLAs) and supports service delivery during defined Service Coverage Windows, always maintaining a full complement of resources to avoid service disruptions.

6.14 **Resource Replacement** - In the event of an assigned resource's absence, the provider must promptly replace them with an equally qualified and competent resource who possesses the necessary access permits, training, and site-specific knowledge to maintain service continuity.

6.15 **Restricted Resource Allocation** - The provider must not deploy support resources to projects or Install, Move, Add, Change, Dispose and Delete (IMACD) activities, ensuring focus on core operational support.

6.16 **Safety Compliance** - The provider must compile and maintain a safety file following ACSA standards within the first month of service commencement. This file must be kept current, unless ACSA communicates that it is not required, ensuring adherence to safety protocols.

6.17 **WLAN Engineer Certification** - WLAN engineers must be certified to work at heights and collaborate with the cabling infrastructure team to safely access equipment at elevated locations, ensuring compliance with safety and operational standards.

7.0 EQUIPMENT AND SPARES HOLDING REQUIREMENTS

7.1 **Technician Equipment** - The provider must equip all service technicians with appropriate tool kits and testing equipment to perform their duties efficiently, ensuring no delays in service delivery.

7.2 **ACSA-Provided Devices** - ACSA will supply laptops or desktops for permanent onsite resources, with the device type determined during the enablement request stage, ensuring compatibility with operational needs.

7.3 **Critical Spares Availability** - The provider must maintain sufficient critical spare parts at all locations to support maintenance activities and meet Service Level Agreements (SLAs), minimising downtime.

7.4 **Backup Stock for SLA Compliance** - If the provider's back-to-back agreement with the OEM cannot meet SLA requirements, the provider must maintain its own backup or loan stock to restore services within the specified maintenance SLA, ensuring uninterrupted operations**.**

7.5 **Quality Replacement Parts** - The provider must replace or repair faulty components using original, manufacturer-guaranteed new parts of the same or higher grade as the original. If an exact match is unavailable, a higher-grade component must be used. Replaced parts must be certified by the device manufacturer to ensure reliability and compatibility.

7.6 **Parts Storage and Obsolescence Management** - Within 60 days of contract award notification, the provider must establish a warehouse or secure storage facility to stock all necessary parts and components, including those for in-scope devices declared obsolete or no longer supported by manufacturers (e.g., post End of SW Maintenance Releases, End of Routine Failure Analysis, End of New Service Attachment, End of Service Contract Renewal, or Last Date of Support). This ensures full SLA compliance and uninterrupted service for all equipment.

8.0 PREVENTATIVE AND CORRECTIVE MAINTENANCE

8.1 **Preventive Maintenance Scope** - Preventive maintenance encompasses planned overhauls, replacements, inspections, tests, software and firmware upgrades, patch management, and other proactive activities to maintain infrastructure condition and prevent failures, including assessments to inform corrective maintenance.

8.2 **Corrective Maintenance Scope** - Corrective maintenance includes all activities initiated following a preventative maintenance inspection to address identified issues, ensuring continued system reliability and performance.

8.3 **Break/Fix Maintenance** - Break/fix maintenance addresses unforeseen issues requiring urgent repairs to restore infrastructure serviceability and system functionality. This may include after-hours, weekend, or public holiday requests, and the provider must respond promptly to all faults.

8.4 **After-Hours Support** - The provider must provide callout-based support for incidents impacting systems during after-hours, weekends, and public holidays. Applicable hourly rates and callout fees must be detailed in the pricing schedule to ensure transparency.

8.5 **Emergency Callouts** - The provider must accommodate short-notice callouts for emergencies caused by system interruptions or airport change processes, providing site-specific callout rates and hourly fees to ensure rapid response and minimal disruption.

8.6 **Planned Activity Coordination** - For planned maintenance activities, ACSA will provide advance notice, and the provider must ensure resource availability as required to execute tasks efficiently.

8.7 **Accessible Support Contacts** - The provider must supply after-hours telephone numbers for reachable support personnel, ensuring constant availability. Any changes to these contact numbers must be promptly communicated to ACSA to maintain seamless support access.

8.8 **Maintenance Schedule Overview** - The Preventative Maintenance Schedules table outlines high-level maintenance tasks and checks to guide the provider’s planning and execution of maintenance activities.

8.9 **Detailed Maintenance Plan** - The provider must submit a comprehensive preventative and corrective maintenance plan/schedule as part of the RFP response, incorporating the minimum requirements from the Preventative Maintenance Schedules table. The plan must detail remedial actions for issues identified during maintenance, including communication protocols (specifying the provider resource responsible, the ACSA recipient, communication format, timelines post-incident detection, and follow-up mechanisms), ensuring effective issue resolution and accountability.

Preventative Maintenance Schedules

Network Component	Focus Area	High-Level Maintenance Task/Checks Description	Frequency
Campus Network	MPLS Core PE and P Routers	Conduct redundancy tests to verify BGP routing stability, convergence, multipath, and fast failover between HSRP nodes, including cold reboots to ensure system reliability.	3 Monthly
	Ad Hoc IOS Upgrades	Immediately upgrade IOS on affected devices to address vulnerabilities or operational issues, ensuring system security and stability.	As Needed
	Scheduled Firmware/Software Upgrades	Upgrade IOS/IOS XE/NX-OS and RiOS to the latest OEM-recommended stable release for all systems, maintaining performance and security.	Annually (Minimum), Continuously

	LAN	Test spanning-tree stability and loop protection by simulating layer 2 loops across network domains to ensure network integrity.	6 Monthly
	Syslog Analysis of Network Devices	Monitor syslog for critical, warning, and error alerts (system, network, or environmental). Address alarms/faults reported by Prime Infrastructure and NNMi within the maintenance SLA, as per pricing schedule.	Daily
	Prime Infrastructure and NNMi Maintenance	Verify device credentials, perform configuration backups, and monitor CPU, memory, and environmental status to ensure optimal device performance.	Daily
	Link Performance	Inspect devices for interface errors, high fibre attenuation, packet drops, and flapping links. Report issues to cabling contractor after verifying device port or fibre module and manage incidents until resolution.	Daily
	Change requests	Implement changes as per business needs	As and when needed
	Troubleshooting	Assist in resolving related issues	As and when needed
Wireless Network	Wireless Controllers	Upgrade IOS to the latest Cisco-recommended stable release. Perform High Availability testing and report outcomes. Review licensing to ensure compliance.	As Needed (Upgrades), Quarterly (Testing), Monthly (Licensing)
	Public Wi-Fi Infrastructure	Back up configurations to ensure rapid recovery in case of failures.	Monthly
	Access Point Maintenance	Conduct visual inspections of all Access Points to verify proper condition and functionality, addressing any identified issues promptly.	Quarterly
	Prime Infrastructure Maintenance	Ensure accurate device credentials, proper naming, mapping, and location data. Monitor for coverage holes, high client counts, and failed logins. Perform configuration backups and check device performance and environmental status.	Weekly (Detailed Checks), Daily (Backups/Performance)
	Link Performance	Monitor Access Points for interface errors and flapping links. Report cable faults to the service provider, manage incidents until resolution, and ensure no free ports in WLAN VLAN.	Daily
	Syslog Analysis of Network Devices	Monitor syslog for deviations and address alarms/faults reported by LMS and Prime Infrastructure to maintain system stability.	Daily
	Assets and Inventory	Maintain an up-to-date asset register with tagged devices. Ensure Cisco Smart Collector uploads complete inventory to Cisco Services Connection/Partner Support Service at least one week before monthly SLA meetings.	Ongoing

	Cleaning	Clean visible Access Points in public areas and offices to maintain appearance and functionality.	Once Annually per Device
	Backups	Ensure configuration backups are completed to support rapid recovery.	Weekly
	Change requests	Implement changes as per business needs	As and when needed
	Troubleshooting	Assist in resolving related issues	As and when needed
IP Telephony and Collaboration	Cisco Unified Communication Manager (CUCM) – Call Control	Perform redundancy and failover testing, reporting outcomes to ensure system reliability.	Quarterly
	Voice Gateways	Conduct redundancy and failover testing, reporting outcomes to verify system resilience.	Quarterly
	Voice Recorders	Add, remove users as requested.	As and when needed
	Communications Manager, UCCX	Review licensing to ensure compliance and operational readiness.	Monthly
	Assets and Inventory	Maintain an up-to-date asset register with tagged devices and current architecture drawings to support asset management.	Ongoing
	Telephone Billing System	Add, remove users as requested.	As and when needed
	Ad Hoc IOS Upgrades	Immediately upgrade IOS on affected devices to address vulnerabilities or operational issues, ensuring system security.	As Needed
	Scheduled Firmware/Software Upgrades	Upgrade IOS to the latest OEM-recommended stable release for all systems, maintaining performance and compatibility.	Ongoing, Annually (Minimum),
	Syslog Analysis of Collaboration Devices	Monitor syslog for critical, warning, and error alerts. Address alarms/faults reported by Prime Infrastructure and NNMi within maintenance SLA. Monitor availability, health, environmental status, performance, and capacity.	Daily
	Cisco Unified Contact Centre Express (CUCX)	Perform redundancy and failover testing, reporting outcomes to ensure system reliability.	Quarterly
	Backups	Ensure backups are completed to enable rapid recovery.	Weekly
	User and Phone Provisioning	Resolve issues with Unified CM, including lines without phones, phone locale installers, mismatched loads, phones without lines, users sharing primary extensions, and unregistered phones to maintain system efficiency.	Weekly
	Change requests	Implement changes as per business needs	As and when needed
	Troubleshooting	Assist in resolving related issues	As and when needed
Firewalls and Security Software	Performance and Health Checks	Monitor availability, health, environmental status, performance, capacity, and errors. Provide reports and address identified issues to	Daily

		ensure security and performance.	
	Syslog Analysis of Network Devices	Monitor syslog for deviations and address alarms/faults reported by security monitoring software to maintain system integrity.	Daily
	Backups	Perform configuration backups before and after changes to ensure recoverability.	Weekly
	Security Alerts	Respond to threat or security violation alerts, informing the IT Information Security division of breaches or threats to ensure rapid mitigation.	Daily
	Security	Run IPS updates, check for failed login attempts, and validate user access to maintain security integrity.	Weekly
	Compliance	Run compliance reports, implement recommendations under change control, and optimise rule bases to ensure adherence to security standards.	Monthly
	Redundancy	Conduct redundancy tests to confirm High Availability and load-handling capacity during peak operations, reporting outcomes.	Quarterly
	Ad Hoc IOS/System Software Upgrades	Upgrade IOS/system software on affected devices to address vulnerabilities or operational issues, ensuring security and performance.	As Needed
	IOS Upgrades and System Software	Upgrade IOS and software to the latest OEM-recommended stable release, following change processes. Verify licensing and check device end-of-life status.	Quarterly
	Change requests	Implement changes as per business needs	As and when needed
	Troubleshooting	Assist in resolving related issues	As and when needed
Assets	Assets	Maintain an up-to-date asset register with tagged devices to support accurate tracking and management.	Ongoing

Table 7 - Preventative Maintenance Schedule

9.0 BASELINE INFORMATION

9.1 Service Requirements Baseline: This section summarises key information relevant to determining service requirements, reflecting ACSA's projected needs from the contract's start date. The provider must maintain and update this baseline, reviewing it quarterly with ACSA IT Infrastructure to ensure alignment with evolving requirements.

9.2 Data Accuracy: The information provided in the associated tables was accurate at the time of tender creation. However, additions or subtractions may have occurred since then, and the provider is responsible for validating and updating this data as needed.

SITE CODE	Core Switches 9600, 9500 and 6800 Series	Data Centre Switches Nexus 9300	LAN Access and Distribution Switch Stacks	Wireless Access Points	Wireless LAN Controllers
JNB	25	8	401	557	2
KIM	2		7	17	
BFN	2		14	30	
CPT	10		192	247	2
GRJ	2		16	30	
UTN	2		7	19	
DUR	14		108	174	2
ELS	2		22	28	
PLZ	2		41	81	2

Table 8 - LAN / WAN / WLAN and IP Telephony Baseline

SITE CODE	CUCM Communications Server	CUCM Voice Gateway	Analogue IP Phones	Cisco IP Phones	UCCX Contact Centre	Voice Recorders
JNB	2	43	150	924	1	2
KIM	1	1	0	33	0	0
BFN	1	1	0	53	0	0
CPT	2	2	0	769	1	1
GRJ	1	1	0	32	0	0
UTN	1	1	0	26	0	0
DUR	2	2	0	646	1	1
ELS	1	1	0	20	0	0
PLZ	1	1	0	53	0	0

Table 8 - LAN / WAN / WLAN and IP Telephony Baseline

SITE CODE	Check Point FW	Check Point Management station and reporter	Cisco ASA	Check Point DDOS	Cisco ISE	Cisco Web Security Appliance	Cisco Web Security Appliance Virtual Servers
JNB	2	1		1		2	2
KIM	2					1	1
BFN	2					1	1
CPT	2					2	1
GRJ	2					1	1
UTN	2					1	1
DUR	2					2	1
ELS	2					1	1
PLZ						1	1

Table 9 - Network Firewalling and Web Security Infrastructure Baseline

10.0 ASSET OWNERSHIP STATUS

The following table provides a summary of the asset ownership.

Asset Category	Ownership	Comments
Physical Buildings	ACSA	
Network core and access switches	ACSA	
Campus Network Routers	ACSA	
IPT and Collaboration Devices	ACSA	
Wireless Infrastructure	ACSA	
WAN Optimisation	ACSA	
Security	ACSA	
WAN Services	External vendor	Redundant Metro Ethernet MPLS VPNS per site and LAN-Connect direct fibre between JNB-COR-CTN
Voice SIP Services	External vendor	Redundant Metro Ethernet per site
Enterprise Internet	External vendor	Redundant Enterprise Internet per site
Cabling Infrastructure	ACSA	
Cabinets	ACSA	
Testing tools etc.	SP	SP to provide their own tools and testing equipment

Table 9 - Asset Ownership

11.0 CURRENT OEM DEPLOYMENT

Device Type	Manufacturers
MPLS Core routers	Cisco Systems and Huawei
Data Centre Switches	Cisco Systems
LAN Access Switches	Cisco Systems and Huawei
Industrial Ethernet Switches	Cisco Systems and Rockwell Stratix
Data Centre Facilities	Rittal
LAN Management Systems	Cisco Systems
Wireless Access Points	Cisco Systems and Huawei
Wireless LAN controllers	Cisco Systems and Huawei
Wi-Fi Management system	Cisco Systems and Huawei
Public WIFI Infrastructure	Cisco Systems
Telephones – IP and Analogue	Cisco Systems
Voice Recorders	Datavoice Libra
Voice Gateways	Cisco Systems
Voice Billing System	Adapt IT
IP Telephony Management system	Cisco Systems
UCCX Dashboard	2Ring display dashboard
In-Path Steelhead Appliances	Riverbed
Internal Firewall	Check Point
Perimeter Firewall	Cisco Systems and Fortigate
DDOS Protector	Check Point
ISE Appliance	Cisco Systems
Web Security Appliances	Cisco Systems
Security Management Appliance	Check Point

Table 10 - Current Hardware Device Standards

12.0 SUPPLY GURANTEES AND NOTES

Please take special note of the following items that apply to all Work packages.

12.1 OEM Warranty

- All hardware must be supplied with a 5-year OEM warranty and software with at least next business day replacement, this includes any software for the device to function. Some Work packages have other requirements and should be catered for accordingly.

12.2 Interoperability

- Any OEM can be used to fulfil any work package as long as **FULL** interoperability is guaranteed within the existing environment.
- Efforts are made to describe the current environment for all work packages. Please read this information carefully.
- The bidder can also include the replacement of the up and downstream devices should they wish/need to provide the guarantee.
- Note that some switches are in a “stack” and are required to remain in the stack configuration due to limitations on uplink fibre capacity.

12.3 Management

- All supplied devices must be fully managed.
- Please refer to the currently deployed management software components as per **Error! Reference source not found. Error! Reference source not found.** to determine if the proposed hardware will be able to be managed by the in-place management system
- Should it be needed, the additional management platform must be costed as part of the work package or added to the “Other cost” tab in Annexture C (pricing file)

12.4 Monitoring

- All supplied devices must be fully monitored.
- Please refer to the currently deployed monitoring software components as per **Error! Reference source not found. Error! Reference source not found.** to determine if the proposed hardware will be able to be monitored by the in-place monitoring system
- Should it be needed, the additional monitoring platform must be costed as part of the work package or added to the “Other cost” tab in Annexure C (pricing file)

12.5 Support

- Any proposed OEMs must be fully supported by the bidder using OEM-certified staff at the equivalent requested certification levels.

12.6 Enterprise Campus and Branch Network Modernisation

12.6.1 Intent-Based Fabric Architecture with SD-LAN Capabilities

The current Core network consists primarily of Cisco Catalyst 9000 series switches and routers at core, distribution, and access layers, managed via Cisco Catalyst Centre (formerly DNA Centre) for intent-based networking and Cisco Identity Services Engine (ISE) for security policy enforcement.

We aim to transition to a scalable, automated SD-LAN fabric architecture that supports intent-based provisioning, zero-trust security, and seamless integration with existing investments. This RFP is intentionally vendor-agnostic to promote competition and innovation.

This must be considered when doing costing

12.6.1.1 Requirements

- Implement a unified fabric overlay for wired and wireless networks, enabling L2/L3 mobility, micro-segmentation, and automated provisioning.
- Enhance network assurance through AI-driven analytics and closed-loop automation.
- Maintain compatibility with existing Cisco Catalyst Centre and ISE deployments for policy and management continuity.
- Support hybrid/multi-vendor environments where feasible, with proven interoperability.

12.6.1.2 **Scope**

- Hardware: Core, distribution, access switches/routers; wireless controllers/APs.
- Software: Intent-based management platform; identity/policy enforcement engine.
- Services: Design, supply, deployment, migration, training, and 5-year support.
- Exclusions: Wide-area connectivity (beyond SD-LAN branches).

12.6.1.3 Technical Requirements

12.6.1.3.1 **Architectural Requirements**

The proposed solution to deliver a controller-orchestrated, overlay-based fabric architecture using VXLAN-EVPN encapsulation for campus/branch SD-LAN. Key mandates:

- Fabric Overlay and Mobility: Single-fabric design supporting L2/L3 host mobility across sites without re-IP/re-authentication. Preserve macro/micro-segmentation during roaming. Underlay automation via IS-IS/OSPF; overlay provisioning without manual VXLAN/VRF/LISP configuration on edge nodes.
- Policy Enforcement: Hardware-enforced micro-segmentation using scalable group tags (SGTs) or equivalent, propagated natively in VXLAN headers (not Ethernet-only). Support dynamic policy distribution via RADIUS CoA.
- Control Plane: Use LISP or IETF-equivalent with pub/sub map-register/reply semantics for endpoint registration and forwarding. Demonstrate full interoperability in mixed environments.
- Wireless Integration: Seamless wired/wireless fabric with AP onboarding, RF optimisation, and client policy inheritance.

12.6.1.3.2 **Management Platform Requirements**

The solution to include a unified intent-based network management system (NMS) compatible with existing Cisco Catalyst Centre (version 2.3.x+). It MUST:

- Natively discover, provision, assure, and automate underlay/overlay/policy/wireless via single pane of glass (no third-party tools).
- Support RESTCONF/NETCONF and model-driven telemetry for day-0/1 automation; proven templates for 5+ years in production.
- Provide AI/ML-driven assurance: Path-trace visualization, baseline deviation alerts, and predictive analytics (e.g., telemetry from 10,000+ endpoints).
- Integrate with existing Catalyst Centre via APIs for hybrid management (e.g., Meraki/Catalyst co-visibility).

12.6.1.3.3 **Identity and Security Requirements**

Centralised policy administration point (e.g., PXGrid-equivalent) SHALL integrate with the fabric control plane for:

- Dynamic VLAN/SGT assignment and downloadable ACLs to edge nodes/wireless controllers.
- Host tracking via LISP integration; SGT-to-VTEP mapping without external DBs.
- Zero-trust enforcement: Endpoint profiling, posture assessment, and scalable group-based access.

Compatibility with Cisco ISE 3.1+ ; alternatives must prove seamless policy import/export.

12.6.1.3.4 **Interoperability and Multi-Vendor Support**

- Proposed non-proprietary components MUST interoperate with existing Cisco Catalyst 9000 (IOS-XE 17.9+) in a shared fabric, proven in production references (10,000+ endpoints, 18+ months deployment).

12.6.1.3.5 **Performance and Scalability**

- Support 10,000+ endpoints/site; <50ms convergence on mobility events.
- Redundancy: N+1 for controllers; hitless upgrades.
- SD-LAN Branch: Automated site provisioning.

13.0 OUT OF SCOPE SERVICES

The following items are specifically excluded from the scope of work:

13.1 Cooling and Power Infrastructure within the IT Facilities

13.2 IT Physical Infrastructure, such as cabling, cabinets, etc.

14.0 ROLES AND RESPONSIBILITIES

In this SOW, we use the RASCI ("responsible, accountable, supporting, consulted and informed") chart approach for all roles and responsibilities matrices.
The RACI terminology is as follows:

Code	Role	Role Detail Description	
R	Responsible	An individual operationally responsible for performing a sourcing activity. Responsible individuals report to the Accountable individual.	Only one individual is accountable for any given activity. Responsible is a proactive role.
A	Accountable	An individual with final accountability for the results of a sourcing activity. Accountability includes a mandate to dismiss or accept the results by the activity as realised by the Responsible individual. This individual also holds the budget to back the mandate.	Only one individual is accountable for any given activity. Accountable is a reactive role.
S	Supporting	Individuals who support the Responsible individual in realising the sourcing activity. They actively participate in realising/executing/performing the activity. Supportive individuals report to the Responsible individual.	Multiple individuals can participate in support of the Responsible individual for any given activity. Supporting is a proactive role.
C	Consulted	Individuals who should be consulted in realising/executing/performing the activity, on the scope, budget, time and value of the activity.	Multiple individuals can be required to be heard for any given activity. Consulting is a reactive role.
I	Informed	Individuals who need to be informed but have no role in the realisation/execution/performance of an activity, other than being informed of the result of the activity.	Multiple individuals can be informed of the results of any given activity. Informed is a passive role.

Table 11 - Definition of RASCI Model

The following table identifies the roles and responsibilities associated with this SOW.

14.1 Roles and Responsibilities- General

Sub area	Number	Task/Activity	provider	ACSA
General	1.	Provide Services and the supporting processes that support ACSA business needs, technical requirements and End-User requirements	R, A	C
	2.	Comply with ACSA policies, guiding principles, standards and regulatory requirements applicable to the ACSA for information, information systems, personnel, physical and technical security	R, A	C
	3.	Develop and maintain an approved comprehensive Standards and Procedures Manual that contains the standards, processes and procedures that will be used in the delivery of all Services. The manual will include clearly delineated roles and responsibilities, touch points and measurements between ACSA and the vendor.	R, A	C
	4.	Approve the comprehensive Standards and Procedures Manual that contains the standards, processes and procedures that will be used in the delivery of all Services. The manual will include delineated roles and responsibilities, touch points and measurements between ACSA and the vendor.	I	R, A
	5.	Report performance against Service-Level Requirements (SLRs)	R, A	I
	6.	Coordinate all Changes to the IT systems that may affect the SLRs of any other Service	R, A	C, I
	7.	Provide timely creation, updating, maintenance and provision of all appropriate project plans, project time and cost estimates, technical specifications, management documentation and management reporting in a form/format that is acceptable to the ACSA for all Service projects and major Service activities	R, A	C
	8.	Adhere to IT service management (ITSM) best practices and Key Performance Indicators (KPIs)	R, A	I
	9.	Approve the use of the ITSM best practices and KPIs	C, I	R, A
Site Access	10.	Coordinate with site IT staff to schedule an On-Site Technical Support visit when using non-regular or 3rd party resources	R, A	C, I
	11.	Ensure that all support staff have valid airside permits for the airports that they support.	R, A	C, I
	12.	Ensure that support staff strictly adheres to the terms and conditions of their permit allowances	R, A	C, I
	13.	Ensure that support staff have access to reliable transport and valid driver's licences. This includes access services provider vehicles that are permitted on airside, should there be a requirement to support any device on airside. The operator must have a valid Airport Vehicle Operators Permit (AVOP). The vehicle requires a regulatory permit and must be insured as per ACSA requirements.	R, A	C, I
	14.	Ensure that the provider always has a valid health and safety file	R, A	C, I
	15.	On request from the provider ACSA will provide access to ACSA premises (which will not be unreasonably withheld) to the provider or their 3rd party personnel to effect maintenance and repairs	I	R, A
	16.	Parking fees at ACSA premises	R, A	I
	17.	Rental of office space at ACSA premises	R, A	I
	18.	Any security related training and payments for access to ACSA premises	R, A	I

Table 12 - Roles and Responsibilities – General

14.2 Roles and Responsibilities - Management, Planning and Design

Architecture Planning and Analysis Services are the activities required to assess the requirements for architectural, functional, performance, IT Service Continuity, and security requirements.

Activities associated with documenting the requirements for architectural, functional, performance, IT Service Continuity, and security requirements.

Include identifying the opportunities to improve the efficiency and effectiveness of the Service.

Can also help support competitive business advantage and mitigate risks by reducing defects and improving the quality of IT Services. Look at current and how to bring in efficiencies and improvements.

Sub area	Number	Task/Activity	provider	ACSA
Architecture Planning and Analysis	1.	Adhere to, implement and ensure alignment to the defined standards, timeframes and reporting requirements for planning, project management and analysis activities.	R, A	C,S,I
	2.	Attend and actively participate in the ACSA scheduled focus groups, stakeholder meetings, project and technical workshops to provide the required expertise (addressing all tasks pre and post the meeting as required, such as requirements gathering activities; solution design options)	R,A	C,S,I
	3.	Provide input into the review of the existing Services, architectural standards and project management practices for Planning and Analysis activities to ensure continuous alignment to best practice.	R, A	C,S,I
	4.	Ensure all documentation remains updated in the required ACSA format. Where no existing documentation is available, the standards are to be followed, and documentation is to be drafted.	R, A	C,I
	5.	Define Services, standards, timeframes and reporting requirements for planning, project management, and analysis activities	C,S,I	R,A
	6.	Schedule the required focus groups and technical workshops for architecture planning and analysis requirements – such as to review the existing infrastructure topologies at an enterprise (e.g., technology strategy, technology architecture, functional, availability, capacity, performance, backup and IT Service Continuity)	S,I	R,A
	7.	Provide ACSA documentation format standards. Review and approve the updated documentation presented by the Service provider	I	R,A
	8.	Review and update the existing Services, standards and project management practices for Planning and Analysis activities	I	R,A
Technical Architecture	9.	Attend, actively participate in and provide technical assistance and subject matter expertise in technical and business planning sessions to review standards, architecture and project initiatives to align with best practice	R,A	C,S,I
	10.	Document current and future Technical Architecture in the agreed formats and update these throughout the service lifecycle	R,A	C,S,I
	11.	Evaluate new equipment considered for implementation in compliance with the ACSA's security and IT architecture policies, regulations and procedures.	C,S,I	R,A
	12.	Define and approve any new architecture standards	C,S,I	R,A
	13.	Conduct technical and business planning sessions to review standards, architecture and project initiatives to align with best practices	R,A	C,S,I
Continuous Improvement	14.	Conduct technical reviews and provide recommendations for improvements that increase efficiency, effectiveness and reduce costs	R,A	C,I

Sub area	Number	Task/Activity	provider	ACSA
	15.	Perform ad hoc investigations as requested by ACSA and submit recommendations for ACSA's consideration.	R,A	C,I
	16.	Conduct ongoing, regular planning and recommendations for technology refresh and upgrades	R,A	C,I
	17.	Showcase new technology enhancements to ACSA therefore allowing ACSA the option to upgrade to any new productised technology.	R,A	C,I
	18.	Review and approve any technical improvement recommendations	C,I	R,A
	19.	Review and approve any requested ad hoc investigations	C,I	R,A
	20.	Review and approve recommendations for technology refresh and upgrades	C,I	R,A
	21.	Review any new technology enhancements presented	C,I	R,A
Management and Testing Tools	22.	Use existing System management tools to monitor, measure, manage and document the environment.	R,A	C,I
	23.	Provide access to existing System management tools to monitor, measure, manage and document the environment	C,I	R,A
Research	24.	Provide expert advice and research the latest technologies constantly, and formally submit these presentations to ACSA IT Infrastructure on a 3-monthly basis.	R,A	C,I
	25.	Participate in in-scope IT-Commercial initiatives as requested ACSA-IT – this includes understanding the required solution and outcome, providing solution design and architecture documentation relating to this service towner	C,I	R,A
	26.	Together with ACSA-IT, perform feasibility studies for the implementation of new and existing technologies that best meet ACSA business needs and meet cost, performance and quality objectives.	R,A	C,I
	27.	Review the latest technologies presented by the Service provider.	C,I	R,A
	28.	Request provider to participate in in-scope IT-Commercial initiatives.	C,I	R,A
Design and panning	29.	Develop, document and maintain detailed technical design/engineering plans and environment configuration based on ACSA's business requirements	R,A	C,I
	30.	Provide design documentation for quarterly audits as requested by ACSA	R,A	C,I
	31.	Provide input into design plans through coordination with the appropriate ACSA technology standards groups and design architects	C,I,S	R,A
	32.	Quarterly audit of design documentation	C,I,S	R,A
	33.	Adhere to production acceptance test criteria	R,A	C,I
	34.	Conduct and document test plans and results	R,A	C,I
	35.	Define and document production acceptance test criteria	C,I	R,A
	36.	Review and approve test plans and results	C,I	R,A

Table 13 - Roles and Responsibilities - Management, Planning and design.

14.3 Roles and Responsibilities - Project Management Services

ACSA may, from time to time, request that the provider perform a discrete set of activities in addition to the ongoing services obligations. (a "Project").

Sub area	Number	Task/Activity	provider	ACSA
Project Management Approach	1.	Utilise project management methodologies, knowledge, skills, tools, and techniques consistent with leading internationally recognised and accepted project management practices such as those contained in the Guide to the Project Management Body of Knowledge (PMBOK) or Prince2	R,A	C,I
	2.	Perform project management review and oversight, attend scheduled project meetings, ensure key milestones are achieved by the Service provider, ensure all ACSA project governance processes are in place and are being achieved throughout the project	C,I	R,A
Define Project Plan	3.	Provide project definition and plan, identify major critical milestones, ensure delivery within budget and project deliverables aligned and approved by the ACSA Project Manager	R,A	C,I
	4.	Provide, maintain and update detailed project planning, identify critical path dependencies.	R,A	C,I
	5.	Approve project plan, critical milestones, budget forecast, and project deliverables	C,I	R,A
	6.	Attend scheduled weekly project meetings to review the detailed project plan and critical path dependencies	C,I	R,A
Manage Execution of the Project	7.	Manage, follow up and track the execution of the project plan.	R,A	C,I
	8.	Ensure project plan management activities are carried out, and ensure updated communication to project stakeholders is done.	C,I	R,A
Monitor Project Progress	9.	Report on project progress, budget, risk, and issues	R,A	C,I
	10.	Review and escalate any issues, risks, etc., for action to higher governance authorities as required	C,I	R,A

Table 14 - Roles and Responsibilities - Project Management Services

14.4 Roles and Responsibilities - Acquisition and Management

The acquisition and management process includes the purchase of all service equipment, including new equipment, upgrades to existing equipment, or purchases resulting from a service or repair request. Also, maintains a buying catalogue, executes purchase orders, provides quotations, and deals with goods handling.

Sub area	Number	Task/Activity	provider	ACSA
Policies, Processes, Standards and Procedures	1.	When procurement is requested by ACSA-IT, the provider is to adhere to the acquisition/procurement policies	R,A	C,I
	2.	Guide ACSA acquisition/procurement polices	C,I	R,A
	3.	Develop, document and maintain in the Standards and Procedures Manual Acquisition and Management procedures that meet requirements and adhere to defined policies	R,A	C,I
	4.	Review and approve Acquisition and Management procedures	C,I	R,A
	5.	Perform periodic audits of procurement procedures	R,A	C,I
Demand Management	6.	Escalate any acquisition and management issues to ACSA-IT, notify ACSA immediately upon learning of item shortages, and notify ACSA-IT of out-of-line (e.g. out-of-stock occurrences) deliveries.	R,A	C,I

Sub area	Number	Task/Activity	provider	ACSA
	7.	Attend monthly review sessions to understand the estimated consumption forecast, where available, to ensure achievement of timelines	R,A	C,I
	8.	Address any acquisition and management escalations from the Service provider	C,I	R,A
	9.	Quarterly, ACSA shall provide the Service provider with its estimated consumption forecast of all in-scope infrastructure equipment. The forecast process will be a joint effort between ACSA and the provider using historical data.	C,I	R,A
Equipment Delivery	10.	Ensure all equipment is delivered as scheduled. No uncommunicated delays in delivery will be accepted by ACSA-IT. Any delays are to be communicated in writing and in the relevant meeting (project meeting) to allow for review and any possible business impacts	R,A	C,I
	11.	Request updates on equipment delivery timelines in the relevant meetings (project meetings, etc.)	C,I	R,A
Standards Compliance	12.	Ensure that new equipment/ hardware complies with established ACSA standards and architectures	R,A	C,I
	13.	Ensure all procured hardware and software are listed as part of the ACSA architecture technology standards	C,I	R,A
Goods Handling and Warehousing	14.	Provide facilities for spares holding nationally at the provider's Locations.	R,A	C,I
	15.	Securely store and ensure equipment at designated Service Locations (as agreed with ACSA)	R,A	C,I
	16.	Control and manage the equipment in a secure and auditable manner.	R,A	C,I
	17.	Manage the physical movement (appropriate packing and transportation) of service in scope equipment as required and agreed with ACSA	R,A	C,I
	18.	Allow ACSA audits when requested by ACSA	R,A	C,I
	19.	Inspect the provider's location nationally to confirm required security is in place	C,I	R,A
	20.	Provide proof of valid insurance coverage for equipment held by the provider on ACSA's behalf	R,A	C,I
	21.	Ad hoc inspections of equipment being moved to ensure appropriate packaging and transportation	C,I	R,A
Equipment Inventory Holding	22.	Maintain adequate equipment inventory levels following SLA obligations.	R,A	C,I
	23.	Report on stock levels Monthly	R,A	C,I

Table 15 - Roles and Responsibilities - Acquisition and Management

14.5 Roles and Responsibilities - Documentation

Documentation Services are the activities associated with developing, revising, archiving, maintaining, managing, reproducing, and distributing information (e.g., project planning materials, System design specifications, Procedures Manuals, operations guides) in hard copy and electronic form.

Sub area	Number	Task/Activity	provider	ACSA
Documentation	1.	Ensure that the entire in-scope infrastructure is well documented and constantly updated	R,A	C,I
	2.	Compile a checklist and all documentation for carrying out maintenance tasks related to in-scope infrastructure (detailed maintenance plan). Provide exception reports where risks and issues cannot be addressed via the maintenance plan	R,A	C,I
	3.	A detailed checklist template will be presented to the ACSA for approval.	R,A	C,I
	4.	Specify the content, purpose, format and production schedule of all documents	R,A	C,I
	5.	Store all copies of documents on the ACSA Microsoft Teams sites provided.	R,A	C,I
	6.	Review and approve in-scope documentation to ensure infrastructure is well documented and constantly updated	I	R,A
	7.	Review the checklist and implement action plans based on any exception reports and recommendations	I	R,A
	8.	Work with the provider to specify the content, purpose, format and production schedule of all documents within the scope	C,I	R,A
	9.	Provide space to store physical copies of all documents and a shared folder for digital copies of the documents	I	R,A
	10.	Provide timely creation, updating, maintenance and provision of all documentation, (design documents; architectural diagrams; as built documents; test plans; all ACSA required project documentation; technical specifications, preventative and corrective maintenance plans and checklist; escalation reports; daily service request report; floor layout diagrams; OEM and third party documentation and management reporting in a form/format that is acceptable to ACSA for Service Projects and major Service activities	R,A	C,I
	11.	Manage all documentation following Configuration Management standards and guidelines	R,A	C,I
	12.	Document standard operating procedures (e.g., boot, failover/disaster recovery/COOP, spool management, batch processing, backup)	R, A	I
	13.	Review and approve standard operation procedures Documentation	I	R,A

Table 16 - Roles and Responsibilities – Documentation

14.6 Roles and Responsibilities - Technology Refresh and Replenishment

Technology Refreshment and Replenishment (TR&R) Services are the activities associated with modernising the IT environment continually, to ensure that the system components stay current with evolving industry-standard technology platforms.

Sub area	Number	Task/Activity	provider	ACSA
Technology Refresh and Replenishment	1.	Recommend TR&R life cycle management policies, procedures and plans appropriate for support of ACSA business requirements.	R, A	C, I
	2.	Develop, document, and maintain in the Standards and Procedures Manual TR&R procedures, and develop TR&R plans that meet requirements as well as adhere to defined policies and Change and Release Management processes.	R, A	C, I
	3.	Review and approve TR&R policies, procedures, and plans	I	R, A
	4.	Perform the necessary tasks required to fulfil the TR&R plans	R, A	I
	5.	Provide management reports on the progress of the TR&R plans	R, A	I
	6.	Periodically review the approved TR&R implementation plans to ensure they properly support ACSA business requirements	I	R, A

Table 17 - Roles and Responsibilities - Technology Refresh and Replenishment

14.7 Roles and Responsibilities - Infrastructure Build and Change

Managing all infrastructure changes [standard, low, medium, high risk] within all operations and projects of the airports. This includes initiating change requests and closing out change requests.
IMACDs will be treated as projects when the following is met:

- Ad hoc IT-related installation requests from IT Commercial
- Upgrades to any existing or live facility
- Hardware decommissioning
- Hardware installation

Sub area	Number	Task/Activity	provider	ACSA
Installations and Additions	1.	Complete IMACD plan per installation and addition	R,A	C,I
	2.	Present IMACD plan to ACSA for approval	R,A	C,I
	3.	Complete IMACD (including but not limited to appliances, switches, fibre link, etc. Installations and additions per approved IMACD plan (timelines/tasks / pre-installation checks / UAT, etc.)	R,A	C,I
	4.	Receive and review the IMACD plan per installation and addition presented by the Service provider	I	R,A
	5.	Approve IMACD plans received from the Service provider	I	R,A
	6.	Approve and sign off IMACD installations and additions in alignment with approved plans	I	R,A
Moves	7.	Complete IMACD plan per installation and addition	R,A	C,I
	8.	Present IMACD plan to ACSA for approval	R,A	C,I
	9.	Complete IMACD (including but not limited to appliances, switches, fibre link, etc. Installations and additions per approved IMACD plan (timelines/tasks / pre-installation checks / UAT, etc.)	R,A	C,I
	10.	Receive and review IMACD plan per installation and addition presented by the Service provider	I	R,A
	11.	Approve IMACD plans received from the Service provider	I	R,A
	12.	Approve and sign off IMACD installations and additions in alignment with approved plans	I	R,A
Change	13.	Recommend changes to meet service requirements	R,A	C,I

Sub area	Number	Task/Activity	provider	ACSA
	14.	Perform changes to meet business requirements (including but not limited to e.g., switch replacement, Ethernet and fibre modules, etc.)	R,A	C,I
	15.	Review and approve recommended changes presented by the provider where required	I	R,A
	16.	Sign off on implemented changes	I	R,A
Decommission	17.	Complete IMACD plan per decommission requirement	R,A	C,I
	18.	Present IMACD plan to ACSA for approval	R,A	C,I
	19.	Complete IMACD decommission per approved IMACD plan (timelines/tasks / pre-decommission checks / UAT, etc.)	R,A	C,I
	20.	Disposal of equipment and materials following ACSA policies upon request.	R,A	C,I
	21.	Receive and review IMACD plan per decommission by the Service provider	I	R,A
	22.	Approve IMACD plans received from the Service provider	I	R,A
	23.	Approve and sign off IMACD decommission in alignment with approved plans	I	R,A
	24.	Sign off on the disposal of equipment and materials following ACSA policies with the Service provider, and ensure financial asset disposal tasks are completed	I	R,A
IMACD Completion Sign-Off	25.	Conduct and document production acceptance tests and provide results to obtain a signed completion form (production acceptance) from ACSA	R,A	C,I
	26.	All works must have before, during and after photos taken, which will be submitted with the handover pack. This applies to every task, including removal of old electrical cabling and piping, new installations, upgrades to existing facilities, etc. Photographs may be combined with video recordings. This form of documentation will be required during audits, meetings, etc.	R,A	C,I
	27.	Maintain and update records to ensure the baseline CMDB is always up to date	R,A	C,I
	28.	Review acceptance test and results for sign off	I	R,A
	29.	Review before, during, and after photos taken during changes	I	R,A
	30.	Review CMDB baseline reports quarterly as defined in the report schedule	I	R,A

Table 18 - Roles and Responsibilities - Infrastructure Build and Change

14.8 **Roles and Responsibilities – Maintenance**

Maintenance Services are the activities associated with the maintenance and repair of hardware, software to include "break/fix" Services. Installed platform and product version levels are not to be more than one version behind the current commercial release, unless coordinated with the ACSA architectural standards committee.

Sub area	Number	Task/Activity	provider	ACSA
Maintenance	1.	Define Maintenance requirements	I	R, A
	2.	Develop, document and maintain in the Standards and Procedures Manual Maintenance procedures that meet requirements.	R, A	I
	3.	Develop Maintenance schedules (OEM-recommended preventative maintenance to be considered)	R, A	
	4.	Review and approve Maintenance procedures and schedules	I	R, A
	5.	Ensure appropriate Maintenance coverage for all Service components	R, A	C, I
	6.	Provide Maintenance and break/fix support in ACSA's defined locations, including dispatching repair technicians to the point-of-service location if necessary	R, A	C, I
	7.	Perform (and/or coordinate with Third-Party Maintenance Vendor if applicable) diagnostics and maintenance on Service components, including hardware, software, peripherals and special-purpose devices as appropriate	R, A	C, I
	8.	Perform an analysis of the impact and/or applicability of Vendor-provided (e.g., Omni) patches and/or service packs, following ACSA policies and requirements	R, A	C, I
	9.	Approve Vendor-provided patches and/or service packs	C, I	R, A
	10.	Review all patches relevant to the IT environment and classify the need and speed at which the Security patches should be installed, as defined by policies and Change Management	R, A	C, I
	11.	Install patches per ACSA's Change Management process and procedures, including acquiring required ACSA approval.	R, A	C, I
	12.	Install (and/or coordinate with Third-Party Maintenance Vendor if applicable) manufacturer field change orders, service packs, firmware and software maintenance releases, etc.	R, A	C, I
	13.	Perform (and/or coordinate with Third-Party Maintenance Vendor if applicable) product patch, "bug fix," service pack installation or upgrades to the current installed version	R, A	C, I
	14.	Perform Maintenance-related software distribution and version control, both electronic and manual	R, A	C, I
	15.	Replace (and/or coordinate with Third-Party Maintenance Vendor if applicable) defective parts, including preventive Maintenance, according to the manufacturer's published mean-time-between-failure rates	R, A	I
	16.	Conduct (and/or coordinate with Third-Party Maintenance Vendor if applicable) Maintenance and parts management, and monitoring during warranty and off-warranty periods	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	17.	Execute preventative maintenance per the high-level schedule, which needs further development by the provider responding to this RFP. The following activities will constitute the minimum requirements. o Inspections and alerts investigations o Syslog analysis – Continuous monitoring and responding with corrective actions to warnings and alerts. o Health Checks o Configuration Backups o Log Analysis o Device performance monitoring for high memory and CPU utilisation o Software upgrades on management systems o Capacity Management o Redundancy Testing o Firmware Upgrades o Advise/recommend improvement for the infrastructure and identify potential risks within the environment, including detailed additional preventative maintenance recommendations which, as experts in the field, are deemed necessary to prevent system failures	R,A	C,I
	18.	Initiate projects to execute on approved preventative maintenance recommendations	I,C	R,A
	19.	Provide detailed monthly reports on capacity, assets, changes, faults, potential risks, etc., as defined in the report schedule	R,A	C,I

Table 19 - Roles and Responsibilities – Maintenance

14.9 Roles and Responsibilities - Infrastructure Monitoring, Operations and Administration

Monitoring, Operations and Administration Services of all in-scope infrastructure are the activities associated with providing a stable environment, thus ensuring a proactive approach to risk mitigation and will aid the provider to meet their SLA targets.

Management of the Infrastructure will always be done in consultation with ACSA-IT Infrastructure and Operations, and no decisions can be made without approvals and the written consent of ACSA.

Sub area	Number	Task/Activity	provider	ACSA
Management and Administration	1.	Utilise ACSA Monitoring tools to monitor the infrastructure that will meet the monitoring and service level reporting requirements	R,A	C,I
	2.	Implement measures for proactive monitoring to limit infrastructure outages.	R,A	C,I
	3.	Manage all in-scope infrastructure elements following ACSA's policies (including security oversight and change management policies)	R,A	C,I
	4.	Manage and coordinate provider-appointed subcontractors and Third Parties to meet Service and SLA requirements	R,A	C,I
	5.	Suggest any additions or changes to the ACSA monitoring tools landscape	R,A	C,I
	6.	Install, customise and maintain the infrastructure management system for event monitoring and availability reporting.	I	R,A
	7.	Implement measures for proactive monitoring to limit infrastructure outages	I	R,A

Table 20 - Roles and Responsibilities - Infrastructure Monitoring, Operations and Administration

14.10 Roles and Responsibilities - Availability Management

The goal of Availability Management is to understand the overall availability requirements of ACSA's business needs and to plan, measure, monitor and continuously strive to improve the availability of the IT Infrastructure, services and supporting IT organisation to ensure these requirements are met consistently, with a focus on providing cost-effective availability improvements that deliver measurable ACSA business benefits.

Availability Management covers the evaluation, design, implementation, measurement and management of the IT Infrastructure Availability from a component and an end-to-end perspective (i.e., Services), including new or modified IT Service Management methodologies and tools, as well as technology modifications or upgrades of IT Infrastructure systems and components. The goal of the Availability Management process is to optimise the capability of the IT Infrastructure, services and supporting organisation to deliver a cost-effective and sustained level of Availability that enables the business to satisfy its business objectives.

Key activities of the Availability Management process are as follows:

- Determining business unit availability requirements for a new or enhanced IT Service and formulating the availability and recovery design criteria for the IT Infrastructure to ensure IT Services are designed to deliver the appropriate levels.
- Determining the critical business functions and impact arising from IT component failure. Where appropriate, reviewing the availability design criteria to provide additional resilience to prevent or minimise impact to the business.
- Identifying opportunities to optimise the availability of the IT Infrastructure to deliver cost-effective improvements that deliver tangible business benefits.
- Supporting the targets for availability, reliability and maintainability for the IT Infrastructure components that underpin the IT Service, to enable these to be documented and agreed within SLAs and contracts.
- Establishing measures and reporting of availability, reliability and maintainability that reflect the business, End-User, and IT support organisation perspectives.
- Monitoring and trend analysis of the availability, reliability and maintainability of IT systems and components
- Reviewing IT Service, system and component availability, identifying unacceptable levels and ensuring appropriate corrective actions are taken to address IT availability shortfalls.
- Investigating the underlying reasons for unacceptable availability and providing recommendations for resolution
- Producing and maintaining a forward-looking Availability Plan, which prioritises and plans overall IT availability improvements aimed at improving the overall availability of IT Services and Infrastructure components to ensure that existing and future business availability requirements can be met.
- Providing IT availability reports to ensure that agreed levels of availability, reliability and maintainability are measured and monitored on an ongoing basis.

Sub area	Number	Task/Activity	provider	ACSA
Availability Management	1.	Establish criteria and SLRs for Availability Management support requirements, including IT systems and services to be covered	C, I	R, A
	2.	Develop Availability Management policies, processes and procedures, and determine appropriate Availability Management tools and methods that support ACSA's Availability Management support requirements	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	3.	Participate in the development of Availability Management policies, processes and procedures, and identify the tools and availability methods to be used	I	R, A
	4.	Review and approve Availability Management policies, processes and procedures	I	R, A
	5.	Implement agreed-upon Availability Management policies, processes and procedures	R, A	I
	6.	Provide unrestricted read access by ACSA-authorised staff and designated personnel to all current and historical availability knowledge base data and records	R, A	I
	7.	Ensure that availability requirements are included when requirements are identified, when upgrading and/or designing new IT systems and services to support business users	I	R, A
	8.	Participate in user requirements gathering and analysis when upgrading and/or designing new IT systems and services, to ensure that they are designed to deliver the required levels of availability (mapped to the SLRs) required by the business	R, A	I
	9.	Create availability and recovery design criteria to be applied to upgrades and/or new or enhanced infrastructure design	R, A	I
	10.	Participate in creating availability and recovery design criteria to be applied to upgrades and/or new IT Infrastructure systems and services design	I	R, A
	11.	Coordinate with the IT service support and IT service delivery process owners and managers from ACSA to research, review and assess Availability issues and optimisation opportunities	R, A	C, I
	12.	Define the availability measures and reporting required for the IT Infrastructure and its components that underpin an upgraded and/or new IT Service, as the basis for an SLA that reflects business, End-User, and IT support organisation requirements	I	R, A
	13.	Participate with ACSA in defining the availability measures and reporting requirements	R, A	I
	14.	Recommend appropriate tools and practices to measure and report on agreed-upon availability measures for upgraded and/or enhanced IT Infrastructure	R, A	I
	15.	Review and approve availability measurement tools and practices	I	R, A
	16.	Ensure that approved availability measurement tools and practices are implemented	R, A	I
	17.	Monitor and maintain an awareness of technology advancements and IT best practices related to availability optimisation, and periodically provide updates to ACSA IT management	R, A	I
	18.	Ensure that all Availability Management improvement initiatives conform to the defined Change Management procedures outlined in the Process and Procedures Manual	R, A	I
	19.	Coordinate and take ownership of Availability Management across all IT service areas within ACSA and Third-Party Service Vendors (e.g., public carriers, Internet service providers, Third-Party providers, etc.)	R, A	I
	20.	Participate in Problem Management review sessions as appropriate, specifically those problems related to outages of critical systems	R, A	C, I
	21.	Monitor actual IT availability achieved versus targets and ensure shortfalls are addressed promptly and effectively	R, A	I
	22.	Conduct Availability Assessment review sessions and provide cost-justified improvement recommendations	R, A	I
	23.	Participate in availability improvement review sessions	I	R, A
	24.	Review and approve cost-justifiable improvement recommendations that ACSA deems appropriate to enhance ACSA's IT and business performance needs	I	R, A

Sub area	Number	Task/Activity	provider	ACSA
	25.	Coordinate with ACSA and Third-Party Service Vendors to gather information on IT systems and service availability issues and trends, to be used for trend analysis.	R, A	I
	26.	Reduce and maintain an Availability Plan that prioritises and plans approved IT availability improvements.	R, A	I
	27.	Review and approve the Availability Plan	I	R, A
	28.	Provide IT availability reporting to ensure that agreed levels of availability, reliability and maintainability are measured, reported and monitored on an ongoing basis.	R, A	I
	29.	Promote Availability Management awareness and understanding within all IT support organisations, including Third-Party Service Vendors.	R, A	I
	30.	Perform regular (e.g., quarterly) reviews of the Availability Management process and its associated techniques and methods to ensure that all are subjected to continuous improvement and remain fit for purpose.	R, A	I
	31.	Periodically audit the Availability Management process to ensure that it continues to deliver desired results in compliance with agreed-upon policies, processes and procedures.	I	R, A

Table 21 - Roles and Responsibilities - Project Management Services

14.11 Roles and Responsibilities - Capacity Management

Capacity Management Services are the activities associated with ensuring that the capacity of the Service matches the evolving demands of ACSA business in the most cost-effective and timely manner. The process encompasses the following:

- Monitoring of performance and throughput of IT Services and supporting IT components
- Understanding current demands and forecasting for future requirements
- Developing capacity plans which will meet demand and SLRs.
- Developing modelling and conducting simulations to manage capacity
- Conducting risk assessment of capacity recommendations
- Developing and implementing a capacity plan, including the financial impact of the Service
- Undertaking tuning activities

Sub area	Number	Task/Activity	provider	ACSA
Capacity Management	1.	Define Capacity Management requirements	I	R, A
	2.	Develop, document and maintain in the Standards, Process and Procedures Manual Capacity Management procedures that meet requirements	R, A	I
	3.	Review and approve the Capacity Management process and procedures	I	R, A
	4.	Establish a comprehensive Capacity Management planning process	R, A	I
	5.	Review and approve the Capacity Management planning process	I	R, A
	6.	Define, develop and implement tools that allow for the effective capacity monitoring/trending of IT Infrastructure, applications and IT components.	R, A	I
	7.	Identify future business requirements that will alter capacity requirements.	I	R, A
	8.	Develop a periodic (usually yearly) capacity plan, including quarterly updates.	R, A	I
	9.	Develop and implement capacity models and run simulations to validate the capacity plan.	R, A	I
	10.	Participate in all capacity planning activities	I	R, A

Sub area	Number	Task/Activity	provider	ACSA
	11.	Assess capacity impacts when adding, removing or modifying applications and infrastructure components.	R, A	I
	12.	Continually monitor IT resource usage to enable proactive identification of capacity and performance issues.	R, A	I
	13.	Capture trending information and forecast future ACSA capacity requirements based on ACSA-defined thresholds.	R, A	I
	14.	Assess incidents/problems related to capacity and provide recommendations for resolution.	R, A	I
	15.	Recommend changes to capacity to improve service performance	R, A	I
	16.	Assess impact/risk and cost of capacity changes	R, A	I
	17.	Approve capacity-related recommendations	I	R, A
	18.	Maintain capacity levels to optimise use of existing IT resources and minimise ACSA costs to deliver Services at agreed-to SLRs	R, A	I
	19.	Ensure adequate capacity exists within the IT environment to meet SLRs and requirements, considering daily, weekly and seasonal variations in capacity demands.	R, A	I
	20.	Validate asset utilisation and capital efficiency	I	R, A

Table 22 - Roles and Responsibilities - Capacity Management

14.12 Roles and Responsibilities - Performance Management

Performance Management Services are the activities associated with managing and tuning Service components for optimal performance. The process encompasses the following:

- Monitoring of performance and throughput of IT Services and supporting IT components
- Assessing the results of the reports
- Conducting trending analysis
- Providing recommendations to tune
- Performing tuning activities
- Updating periodically (at least annually)

Sub area	Number	Task/Activity	provider	ACSA
Performance Management	1.	Define Performance Management requirements	I	R, A
	2.	Develop, document and maintain in the Standards, Process and Procedures Manual Performance Management procedures that meet requirements	R, A	I
	3.	Review and approve Performance Management procedures	I	R, A
	4.	Perform Service component tuning to maintain optimum performance following Change Management procedures.	R, A	I
	5.	Manage Service component resources (e.g., devices and traffic) to meet defined Availability and performance SLRs	R, A	I
	6.	Provide monitoring and reporting of Tower component performance, utilisation and efficiency based on a specified time frame and sequence (e.g., monthly)	R, A	I
	7.	Proactively evaluate, identify and recommend configurations or changes to configurations that will enhance performance	R, A	I
	8.	Conduct trending analysis to recommend changes to improve the performance based on a specified time frame and sequence (e.g., monthly)	R, A	I
	9.	Develop and deliver improvement plans as required to meet SLRs based on a specified time frame and sequence (e.g., monthly)	R, A	I
	10.	Review and approve improvement plans		R, A
	11.	Implement improvement plans and coordinate with Third Parties as required	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	12.	Provide technical advice and support to the application maintenance and development staff as required	R, A	I

Table 23 - Roles and Responsibilities - Performance Management

14.13 Roles and Responsibilities - Configuration Management

Configuration Management Services are the activities associated with providing a logical model of the devices or assets (including software licenses) and their relationships by identifying, controlling, maintaining and verifying installed hardware, software and documentation (i.e., maintenance contracts, SLA documents, etc.).

The goals are to account for all IT assets and configurations, provide accurate information on configurations, provide a sound basis for Incident, Problem, Change and Release Management, and to verify configuration records against the infrastructure and correct any exceptions. The following table identifies the Configuration Management roles and responsibilities that the provider and ACSA will perform.

Sub area	Number	Task/Activity	provider	ACSA
Configuration Management	1.	Define Configuration Management requirements	I	R, A
	2.	Develop, document and maintain in the Standards Process and Procedures Manual Configuration Management procedures that meet requirements	R, A	I
	3.	Review and approve Configuration Management procedures and processes	I	R, A
	4.	Identify and document the configuration item structure	R, A	I
	5.	Approve the configuration item structure	I	R, A
	6.	Establish a Configuration Management database, following ACSA requirements	R, A	I
	7.	Review and approve the Configuration Management database	I	R, A
	8.	Select and provide Configuration Management tools	I	R, A
	9.	Install and maintain Configuration Management tools	R, A	I
	10.	Enter/upload configuration data into the configuration database	R, A	I
	11.	Establish process interfaces to Incident and Problem Management, Change Management, technical support, maintenance and Asset Management processes	R, A	I
	12.	Establish appropriate authorisation controls for modifying configuration items and verify compliance with software licensing	R, A	I
	13.	Establish guidelines for physical and logical separation between development, test and production and the process for deploying and back-out of configuration items	I	R, A
	14.	Develop procedures for establishing configuration baselines as reference points for rebuilds, and provide the ability to revert to stable configuration states	R, A	I
	15.	Develop procedures for establishing security baselines as reference points for rebuilds, and provide the ability to revert to stable configuration states	I	R, A
	16.	Establish procedures for verifying the accuracy of configuration items, adherence to the Configuration Management process and identifying process deficiencies	R, A	I
	17.	Provide a deficiency report and steps taken to address the issues identified	R, A	I
	18.	Provide ACSA Configuration Management reports as required and defined by ACSA	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	19.	Audit Configuration Management process and accuracy of configuration data	I	R, A

Table 24 - Roles and Responsibilities - Configuration Management

14.14 Roles and Responsibilities - Asset Management

Asset Management Services are the activities associated with the process of the ongoing management and tracking of the life cycle of existing Service components (e.g., hardware, software and software licenses, maintenance, circuits) and their attributes (i.e., location, costs, depreciation, contracts, vendor, serial numbers, etc.).

Sub area	Number	Task/Activity	provider	ACSA
Asset Management	1.	Define Asset Management requirements	C, I	R, A
	2.	Recommend improvements to Asset Management requirements	R, A	C, I
	3.	Develop, document and maintain in the Standards and Procedures Manual Asset Management process and procedures that meet requirements and adhere to defined policies	R, A	C, I
	4.	Review and approve the Asset Management process and procedures	C, I	R, A
	5.	Deploy an Asset Management system that meets ACSA requirements and adheres to defined policies	R, A	C, I
	6.	Maintain and manage an Asset Management system	R, A	C, I
	7.	Manage the life cycle of all assets from identification, requisition ordering, inventory, installation and maintenance to disposal	R, A	I
	8.	Develop an asset type list and attributes that would be included in the Asset Management system	I	R, A
	9.	Review asset type list and attributes, and maintain asset types and attributes in the Asset Management system	R, A	I
	10.	Provide ACSA inquiry and reporting access into the Asset Management system for all assets	R, A	I
	11.	Maintain the accuracy of the data of in-scope assets in the Asset Management system, according to SLRs	R, A	I
	12.	Provide an electronic feed of asset data	R, A	I
	13.	Establish, update and maintain the asset database to include, at a minimum, the following asset attributes: • Manufacturer • Model • Serial number • Identification number • Location • Ownership information • Cost information • Maintenance information and history, including the age of the asset • Warranty information • Other billing information (e.g., lease information, ACSA-specific information) • Transaction edit history (e.g., locations, billing and user)	R, A	I
	14.	Update in-scope asset records related to all approved change activities (e.g., install/move/add/change activities, break/fix activities, company reorganisation and Change Management)	R, A	I
	15.	Perform ongoing physical asset audit, following Asset Management SLRs, to validate that data in the database is accurate and current	R, A	I
	16.	Provide reports of Asset Management audit results	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	17.	Provide and, upon ACSA approval, implement the Asset Management remediation plan for Asset Management deficiencies	R, A	I
	18.	Review and approve audit reports and remediation plans for asset inventory management information	C, I	R, A
	19.	Provide reports of ACSA asset financial information, including depreciation, maintenance contracts and value of assets	R, A	I
	20.	Affix Asset Tags supplied by ACSA according to the relevant procedures.	R, A	I
	21.	Conduct periodic/ad hoc quality assurance audit of the Asset Management system	I	R, A

Table 25 - Roles and Responsibilities - Asset Management

14.15 Roles and Responsibilities - Software License Management

Software License Management Services are the activities associated with the identification, acquisition and disposal as well as ongoing management and tracking of software and their corresponding licenses.

Sub area	Number	Task/Activity	provider	ACSA
Software License Management	1.	Define Software License Management requirements	C, I	R, A
	2.	Recommend improvements to Software License Management requirements and policies	R, A	I
	3.	Develop, document and maintain in the Standards and Procedures Manual Software License Management procedures that meet requirements and adhere to defined policies as mapped to Asset Management	R, A	I
	4.	Review and approve Software License Management processes and procedures	I	R, A
	5.	Manage and maintain (e.g., monitor, track status, verify, audit, perform contract compliance, reassign) software licenses and media through the software license life cycle	R, A	C, I
	6.	For ACSA-retained contracts, be responsible for procurement, renewal and upgrade costs, and vendor agreements	I	R, A
	7.	For non-ACSA-retained contracts, be responsible for procurement, renewal and upgrade costs, and vendor agreements	R, A	C, I
	8.	Develop and maintain an inventory of all Software licenses within the Asset Management system	R, A	I
	9.	Report to ACSA on any exceptions to Vendor terms and conditions, including license non-compliance	R, A	I
	10.	Periodically (at least yearly), conduct a software license and maintenance agreements review, allowing for sufficient time prior to expiration for negotiations	R, A	I
	11.	Participate in software license and maintenance agreements review	I	R, A
	12.	Provide ACSA with reports and recommendations to use in making software acquisition and discontinuance decisions	R, A	I
	13.	Provide recommendations to purchase additional license allocation, recommending alternatives or curtailing usage where necessary and appropriate, to restore or continue to maintain license compliance	R, A	I
	14.	Identify and report license compliance issues to ACSA and provide recommendations to resolve the compliance issue	R, A	I
	15.	Review license compliance issues and document completed resolution	I	R, A
	16.	Manage and perform audits and reconcile the number of licenses to the number of installs, as requested by ACSA	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	17.	Provide recommendations to ACSA to resolve any software reconciliation issues	R, A	I
	18.	Report on the resolution of software reconciliation issues	I	R, A
	19.	Obtain approval from ACSA for any license change or replacement	R, A	I

Table 26 - Roles and Responsibilities - Software License Management

14.16 Roles and Responsibilities - Change Management

Change Management Services are activities to ensure that standardised methods and procedures are used for efficient and prompt handling of all changes, to minimise the impact of change upon Service quality and consequently to improve the day-to-day operations of ACSA.

Change Management covers all aspects of managing the introduction and implementation of all changes affecting all Towers and in any of the management processes, tools and methodologies designed and utilised to support the Service components.

The Change Management processes and activities are interrelated and complementary with Release Management and Configuration Management, as well as Incident Management and Problem Management.

The Change Management process includes the following steps:

- Determining metrics for measuring the effectiveness of a change
- Request for change (RFC) process
- Recording/tracking process
- Prioritisation process
- Responsibility assignment process
- Impact/risk assessment process
- Participation in IT service continuity and DR planning
- Coordination of the Change Advisory Board (CAB)
- Review/approval process.
- Establishing and managing the schedule of approved changes
- Implementation process
- Verification (test) process
- Closure process

Sub area	Number	Task/Activity	provider	ACSA
Change Management	1.	Define Change Management policies and requirements, including change priority schema and classifications, per the Change Management process components outlined above	I	R, A
	2.	Develop Change Management procedures and processes per the Change Management process components outlined above	R, A	I
	3.	Review and approve the Change Management process, procedures and policies	I	R, A
	4.	Receive and document all RFCs and classify proposed changes to the Services, which shall include change cost, risk impact assessment and system(s) security considerations	R, A	I
	5.	Review and validate that RFCs comply with Change Management policies, procedures and processes	I	R, A
	6.	Ensure that appropriate back-out plans are documented and in place in the event of a system failure because of the change	R, A	I
	7.	Provide a Change Management plan to ACSA for review	R, A	I
	8.	Approve the Change Management plan	I	R, A
	9.	Develop and maintain a schedule of planned approved changes (Forward Schedule of Changes [FSC]) for ACSA to review	R, A	I
	10.	Coordinate, schedule and conduct CAB meetings to include review of planned changes and results of changes made, ensuring that all appropriate parties are invited and represented in accordance with approved CAB policies	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	11.	Participate in CAB meetings as ACSA deems appropriate or necessary	I	R, A
	12.	Provide change documentation as required, including proposed metrics as to how the effectiveness of the change will be measured	R, A	I
	13.	Review and approve change documentation and change effectiveness metrics	I	R, A
	14.	Review and approve any RFC determined to have a cost, security or significant risk impact to ACSA's IT systems or business	I	R, A
	15.	Authorise and approve scheduled changes or alter the schedule change requests as defined in the Change Management procedures	I	R, A
	16.	Publish and communicate the approved FSC to all appropriate IT and business unit stakeholders within ACSA of the change timing and impact	I	R, A
	17.	Oversee the approved change build, test and implementation processes to ensure these activities are appropriately resourced and completed according to the change schedule	R, A	I
	18.	Ensure that thorough testing is performed before release and assess ACSA business risk related to any change that is not fully tested before implementation	I	R, A
	19.	Participate in business risk assessment for change to be introduced without being fully tested	R, A	I
	20.	Monitor changes, perform change reviews and report results of changes, impacts and change effectiveness metrics	R, A	I
	21.	Verify that the change met objectives based upon predetermined effectiveness metrics, and determine follow-up actions to resolve situations where the change failed to meet objectives	R, A	I
	22.	Review and approve Change Management results	I	R, A
	23.	Close out RFCs that met the change objectives or changes that were abandoned	R, A	I
	24.	Perform Change Management quality control reviews and audits of Change Management processes and records	c, I	R, A
	25.	Provide ACSA Change Management reports as required and defined by ACSA	R, A	c, I

Table 27 - Roles and Responsibilities - Change Management

14.17 Roles and Responsibilities - Training and Knowledge Transfer

Training and Knowledge Transfer Services consist of the following three types of training provider will provide:

- Training for the improvement of skills through education and instruction for the provider's staff. The provider will participate in any initial and ongoing training delivered by ACSA as required, which would provide a learning opportunity about ACSA's business and technical environment.
- Training for ACSA-retained technical staff for the express purpose of exploiting the functions and features of the ACSA computing environment. Delivery methods may include classroom-style, computer-based, individual or other appropriate means of instruction.
- Selected classroom-style and computer-based training (case-by-case basis) for standard COTS and Software as a Service (SaaS) applications, including new employee training, upgrade classes and specific skills.

Sub area	Number	Task/Activity	provider	ACSA
Training and Knowledge Transfer	1.	Define Training and Knowledge Transfer requirements	I	R, A
	2.	Develop, document and maintain in the Standards and Procedures Manual Training and Knowledge Transfer procedures that meet requirements	R, A	C, I
	3.	Review and approve Training and Knowledge Transfer procedures	I	R, A
	4.	Develop and deliver a training program to instruct ACSA personnel on the provision of provider Services (e.g., "rules of engagement," requesting Services)	R, A	C, I
	5.	review and approve provider-developed training program	I	R, A
	6.	Develop, implement and maintain an ACSA-accessible knowledge database/portal	R, A	C, I
	7.	Develop and implement Knowledge Transfer procedures to ensure that more than one individual understands key components of the business and technical environment	R, A	C, I
	8.	anticipate in ACSA-delivered instruction on the business and technical environment	R, A	C, I
	9.	Develop, document and deliver training requirements that support the ongoing provision of ACSA Services, including refresher courses as needed and instruction on new functionality	R, A	C, I
	10.	Take training classes as needed to remain current with systems, software, features and functions for which help desk support is provided, to improve Service performance (e.g., First-Contact Resolution)	R, A	C, I
	11.	Provide training when substantive (as defined between ACSA and provider) technological changes (e.g., new systems or functionality) are introduced into the ACSA environment, to facilitate full exploitation of all relevant functional features	R, A	C, I
	12.	Provide training materials for ACSA technical staff for Level 1-supported applications	R, A	C, I
	13.	Provide ongoing training materials for help desk personnel on ACSA business and technical environments, as defined by ACSA	R, A	C, I
	14.	Provide ACSA-selected classroom-style and computer-based training (case-by-case basis) for standard COTS applications, as requested by ACSA	R, A	C, I

Table 28 - Roles and Responsibilities - Training and Knowledge Transfer

14.18 Roles and Responsibilities - Account Management

Account Management Services are the activities associated with the ongoing management of the Service environment.

Sub area	Number	Task/Activity	provider	ACSA
Management	1.	Define Account Management requirements	I	R, A
	2.	Develop, document and maintain in the Standards Process and Procedures Manual Account Management procedures that meet requirements	R, A	I
	3.	Review and approve the Account Management process and procedures	I	R, A
	4.	Develop a detailed "IT" catalogue that details Services offered, including all Service options, pricing, installation time frames, order process (new, change and remove service) and prerequisites	R, A	I
	5.	Approve the Service catalogue	I	R, A
	6.	Develop a Service ordering process that clearly defines how to order, change or delete Services	R, A	C, I
	7.	Recommend criteria and formats for administrative, Service activity and Service-Level Reporting	R, A	C, I
	8.	Review and approve criteria and formats for administrative, Service activity and Service-Level Reporting	I	R, A
	9.	Develop and implement a customer satisfaction program for tracking the Quality of Service (QoS) delivery to End Users	R, A	I
	10.	Review and approve the customer satisfaction program for tracking the QoS delivery to End Users	I	R, A
	11.	Provide reporting (e.g., statistics, trends, audits, customer satisfaction results)	R, A	I
	12.	Provider to ensure the appropriate resource model is assigned to the account, including relationship manager, project managers, delivery manager, technical managers, etc. The relationship manager will be the single point of contact between the provider and ACSA-IT	R,A	I
Meetings	13.	Actively participate in meetings as defined in the report and meeting schedule.	R,A	I
	14.	Ensure any planning is done before the meetings	R,A	I
	15.	Ensure reports and any required documents are circulated before the meeting	R,A	I
	16.	Ensure all actions documented from the meetings are addressed	R,A	I
	17.	Produce minutes of the meetings	R,A	I
Risk Management	18.	Participate in regular reviews of the risk exposure of the relationship and overall transaction between ACSA and the Service provider.	R,A	I
	19.	Inform ACSA of any immediate risks requiring urgent attention	R,A	I
	20.	Co-develop risk mitigation strategies	R,A	I

Table 29 - Roles and Responsibilities - Account Management

14.19 Roles and Responsibilities - Incident Resolution and Problem Management

The activities associated with restoring normal service operation as quickly as possible and to minimise the adverse impact on ACSA business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

Problem Management also includes minimising the adverse impact of Incidents and Problems on the business that are caused by errors in the in-scope Infrastructure, and to prevent the recurrence of Incidents related to those errors. To achieve this goal, Problem Management seeks to get to the root cause of incidents and then initiate actions to improve or correct the situation.

Sub area	Number	Task/Activity	provider	ACSA
Incident Resolution and Problem Management	1.	Adhere to the ACSA Problem Management process and procedures	R, A	I
	2.	Provide ACSA Problem Management process and procedures	I	R, A
	3.	If the provider requires calls to be logged to their service desk, an integration between ACSA and the provider's service desk must be provided by the Service provider. All accountability and associated costs are for the Service provider. No manual call logging to the provider's Service Desk will be in scope for ACSA. Any failure in communication between ACSA and the provider's service desk does not constitute grounds to miss SLA, as the ACSA service desk is the tool to measure SLA	R, A	I
	4.	Accept, update and close calls as per service level agreements using the ACSA_IT call logging system.	R, A	I
	5.	Provide, configure and operate an Incident and Problem Management system that tracks Incidents	I	R, A
	6.	Perform incident and problem management per ACSA process and procedures, which includes, but is not limited to : o Perform event management monitoring of the Services to detect abnormal conditions or alarms, log abnormal conditions, analyse the condition and take corrective action o Manage the entire Incident/Problem life cycle, including detection, diagnosis, status reporting, repair and recovery o Coordinate and take ownership of problem resolution by managing an efficient workflow of incidents, including the involvement of third-party providers (e.g., vendors). o Assign problems to L2 & L3 technical maintenance and repair staff as required o Review the state of open Problems and the progress being made in addressing these problems. o Interact regularly with the IT service desk to ensure an optimised and efficient level of service delivery [scheduled meetings, reports, etc.]. o Updates must be provided to the service desk in a professional, timely manner in both verbal and in written formats [using the call logging application] o Manage and coordinate subcontractors and third parties in order to resolve Incidents/Problems	R, A	I,C

Sub area	Number	Task/Activity	provider	ACSA
		o Upon rectification of the Incident/Problem, the provider will immediately notify ACSA helpdesk that the Incident/Problem has been resolved o Update all change configuration databases prior to closing any call.		
	7.	ASCA-IT Engineer to review Incident and Problem management tasks by the provider in Monthly Care Review Meetings to ensure the provider is completing tasks following ACSA process and procedures	I	R, A
	8.	Provide a status report detailing the Incident and Problem Management logs as defined in the reporting schedule	R, A	I,

Table 30 - Roles and Responsibilities - Incident Resolution and Problem Management

14.20 Roles and Responsibilities - IT Service Continuity and Disaster Recovery

IT Service Continuity and Disaster Recovery (DR) Services are the activities associated with providing such Services for ACSA applications, and their associated infrastructure (e.g., CPU, servers, network, data and output devices, End-User devices). ACSA applications' associated infrastructure will receive DR Services according to ACSA's Business Continuity Plan. The provider must demonstrate that it will consistently meet or exceed ACSA's IT Service Continuity and DR Services requirements.

Sub area	Number	Task/Activity	provider	ACSA
IT Service Continuity and Disaster Recovery	1.	As needed, assist ACSA in other IT continuity and emergency management activities	R, A	I
	2.	Develop and maintain a detailed DR plan to meet IT Service Continuity and DR requirements. Include plans for data, replication, backups, storage management and contingency operations that provide for recovering ACSA's systems within established recovery requirement time frames after a disaster affects ACSA's use of the Services.	R, A	I
	3.	Participate in DR tests	R, A	I,C,S
	4.	Track and report DR test results to ACSA	R, A	I
	5.	Review and approve DR testing results	I	R, A

Table 31 - Roles and Responsibilities - IT Service Continuity and Disaster Recovery

14.21 Roles and Responsibilities - Service-Level Monitoring and Reporting

Service-Level Monitoring and Reporting Services are the activities associated with the monitoring and reporting of Service Levels with respect to Service-Level Requirements (SLRs). In addition, provider shall report system management information (e.g., performance metrics and system accounting information) to the designated ACSA representatives in a format agreed to by ACSA.

Sub area	Number	Task/Activity	provider	ACSA
Service-Level Monitoring and Reporting	1.	Define Service-Level requirements	I	R, A
	2.	Define Service-Level Monitoring and Reporting requirements	I	R, A
	3.	Develop, document and maintain in the Standards Process and Procedures Manual Service-Level Monitoring and Reporting procedures that meet requirements	R, A	I
	4.	Review and approve Service-Level Monitoring and Reporting procedures	C	R, A
	5.	Report on SLR performance and improvement results	R, A	I
	6.	Coordinate SLR monitoring and reporting with designated ACSA representative and Third Parties	R, A	I

Sub area	Number	Task/Activity	provider	ACSA
	7.	Measure, analyse and provide management reports on performance relative to SLRs	R, A	I
	8.	Conduct SLR Improvement Meetings to review SLRs and recommendations for improvements	R, A	I
	9.	Review and approve SLR improvement plans	I	R, A
	10.	Implement SLR improvement plans	R, A	I
	11.	Review and approve SLR metrics and performance reports	C, I	R, A
	12.	Provide ACSA access to the performance and SLR reporting and monitoring system and data	R, A	I

Table 32 - Roles and Responsibilities - Service-Level Monitoring and Reporting

14.22 Roles and Responsibilities - Financial Management

Manage the financial aspects of the contract. This involves reconciling of billing and internal chargeback. This also includes Processes for maintaining financial management of the contract through unnecessary cost elimination.

Sub area	Number	Task/Activity	provider	ACSA
Financial Management	1.	Adhere to ACSA Standards and Procedures Manual, Financial/Chargeback Management and Invoicing procedures.	R, A	I
	2.	Implement corrective actions for billing disparities	R, A	I
	3.	Provide timely and correct invoices to ACSA and/or respective ACSA Operating Divisions	R, A	I
	4.	Provide ACSA Standards and Procedures Manual, Financial/Chargeback Management, and Invoicing procedures.	I	R, A
	5.	Provide such information as it may reasonably request for it to perform Penalty processes	I	R, A
	6.	Identify billing disparities and work with the provider to identify corrective actions	I	R, A
	7.	Provide information to be used for budgeting in line with the operating plan	R, A	I
	8.	Assist in monitoring and managing charging/invoicing	R, A	I
	9.	Set budgets in line with the operating plan		R, A
	10.	Monitor and manage payments against budgets		R, A
	11.	Maintain an audit trail and records of all costs incurred under the Agreement	R, A	I
	12.	Proactively ensure that all unnecessary costs are eliminated and that costs are managed in an efficient manner	R, A	I
	13.	Participate in financial review meetings	R, A	I
	14.	Identify areas for potential cost savings and provide input for the innovation process where appropriate	R, A	I
	15.	Implement ACSA's invoicing and recharge requirements	R, A	I
	16.	Sign off all delivery notes / Proof of delivery	I	R, A
	17.	Review and approve records of all costs incurred by the provider under the Agreement	I	R, A
	18.	Proactively ensure that all unnecessary costs are eliminated and that costs are managed in an efficient manner	I	R, A
	19.	Participate in financial review meetings	I	R, A
	20.	Identify areas for potential cost savings and provide input for the innovation process where appropriate	I	R, A
	21.	Implement ACSA's invoicing and recharge requirements	I	R, A

Table 33 - Roles and Responsibilities - Financial Management

14.23 Roles and Responsibilities - Human Resources

Human Resource Management Services include the activities associated with the provision and adjustment of appropriate human resources, per workloads, to perform the required Services at the required Service Levels

Sub area	Number	Task/Activity	provider	ACSA
Skills and Staffing	1.	Ensure that staffing and skill levels are adequate to achieve the SLA	R, A	I
	2.	Train and upskill staff as required	R, A	I
	3.	Provide ACSA with staff training plans (especially onsite staff)	R, A	I
	4.	Monitor the staff development	I	R, A
Capacity Management	5.	Proactively keep the provider informed of any requirements that would potentially impact the Service provider's HR resource requirements	I	R, A
	6.	Define any constraints for the use of Subcontractors	I	R, A
	7.	Approve or reject the recommended Subcontractors	I	R, A
	8.	Analyse the impact of any new requests made by ACSA to be implemented by the provider and propose an HR resource (skills and staffing) solution	R, A	I
	9.	Analyse the impact of enhanced SLAs (if required by ACSA) on the allocated human resources and propose a solution	R, A	I
	10.	Recruit and provide the human resources necessary for the performance of required Services in compliance with SLAs	R, A	I
	11.	Manage Employees' time off and replacement	R, A	I
	12.	Recommend Subcontractors for delivery of Services, if applicable	R, A	I
Performance Monitoring	13.	Continuously monitor the performance of all the human resources made available to ACSA to ensure that the Services comply with the SLAs	R, A	I
	14.	Perform Annual Employee performance reviews	R, A	I
	15.	Consider ACSA satisfaction a key component of the assigned Employee performance reviews	R, A	I
Change Management	16.	On request by ACSA, designate certain members of staff as Key Employees	R, A	I
	17.	Inform ACSA with a minimum of two weeks' notice of any potential Key Employee staffing changes and of any new Employee assignments planned for new projects and Services	R, A	I
	18.	Assign a new provider Relationship Manager as necessary to discharge the Service provider's responsibilities	R, A	I
	19.	Provide staff turnover data relevant to the Agreement when requested by ACSA	R, A	I
	20.	ACSA to nominate key employees where required	I	R, A
	21.	Request provider staff turnover data when required	I	R, A
	22.	Communicate changes to internal ACSA Stakeholders	I	R, A

Table 34 - Roles and Responsibilities - Human Resources

14.24 Roles and Responsibilities - Security

Security Services are the activities associated with maintaining physical and logical security of all Service components (hardware and software) and data, virus protection, access protection and other Security Services in compliance with ACSA's Security requirements.

Physical Security focuses on the physical access controls implemented to ensure the security of ACSA's and providers' data processing equipment, facilities and their associated management systems.

Data Security consists of the activities associated with the classification, management, security and encryption of sensitive/confidential data, and the storage of media containing that data.

Identity and Access Management Services consist of the activities to authorise, authenticate and provide access control to the IT Infrastructure

Sub area	Number	Task/Activity	provider	ACSA
General	1.	Install Security patches per ACSA's Change Management process and procedures, including getting required ACSA approval	R, A	I
Physical Security	2.	Provide physical security in conformance with policies, procedures and practices	R, A	I
	3.	Physically secure data processing equipment, facilities and storage media from unauthorised access	R, A	I
	4.	Physically protect and store fixed and portable media (e.g., tape, optical, portable hard drives, flash drives) holding sensitive data	R, A	I
	5.	Ensure only authorised personnel have access to data processing equipment, facilities and storage media	R, A	I
	6.	Track and check all physical access and activities performed on data processing equipment and facilities	R, A	I
	7.	Review logs to show that the access to data processing equipment was business-justified	R, A	I
	8.	Provide the capability to revoke access to data processing equipment, facilities and storage media	R, A	I
	9.	Maintain physical access audit logs	R, A	I
	10.	Physically secure management systems from unauthorised access	R, A	I
	11.	Ensure only authorised personnel have access to management systems	R, A	I
	12.	Track and check all changes performed on management systems	R, A	I
	13.	Provide the capability to revoke access from management systems at once	R, A	I
	14.	Maintain change audit logs on management systems	R, A	I
Data Security	15.	Assume custodial responsibility for all storage media related to services provided	R, A	I
	16.	Protect portable media while in transit and keep transmittal records	R, A	I
	17.	Eradicate all data from storage media (server memory, disk, tape, optical, other) before redeployment or disposal, following ACSA's procedures	R, A	I
	18.	Perform periodic (e.g., monthly) reconciliation reporting of all data media and perform an annual audit to reconcile all storage media	R, A	I
	19.	Report reconciliation discrepancies to ACSA and take corrective action to address the issue	R, A	I
Identity and Access Management	20.	Provide Identity and Access Management in conformance with ACSA practices, policies and procedures	R, A	I
	21.	Establish roles, authorised activities and minimum rights granted to Service provider personnel (including non-user accounts)	R, A	I
	22.	Approve roles and authorisation activities performed by the provider	I	R, A
	23.	Establish and manage a process to support temporary access	R, A	I
	24.	Review and approve the user and system user account management process	I	R, A
	25.	Approve the Service provider personnel who may manage user accounts	I	R, A

Sub area	Number	Task/Activity	provider	ACSA
	26.	Monthly audit production system access logs and activities to identify malicious or abnormal behaviour following established ACSA policies and standards	R, A	I
	27.	Conduct a monthly review of all privileged user accounts to ensure the accounts are valid/required, removing inactive and unneeded accounts following established ACSA policies and standards	R, A	I
	28.	Conduct a monthly review of End-User accounts to ensure each user has appropriate minimal permissions required to perform their job function, following established ACSA policies and standards	R, A	I
	29.	Conduct monthly review of privileged user accounts to ensure each user has appropriate minimal permissions required to perform their job function, following established ACSA policies and standards	R, A	I
Security Configuration Management	30.	Certify that engineering and Configuration Management are secure	R, A	I
	31.	Review and approve engineering designs and Configuration Management security	I	R, A
	32.	Certify equipment meets ACSA's security requirements and provide evidence of compliance	R, A	I
	33.	Periodically review equipment configurations and address any deficiencies or inconsistencies, and provide ACSA with results with detailed recommendations for remediating issues that are found	R, A	I
	34.	Review and approve the remediation approach	I	R, A
	35.	Provide ACSA with secure baselines for standard components (e.g., routers, servers, DBMS, etc.)	R, A	I
	36.	Establish a baseline for the secure configuration of Equipment based on ACSA's technical control specifications (e.g., CIS benchmark)	I	R, A
	37.	Recommend changes to baseline to meet ACSA requirements	I	R, A
	38.	Configure equipment to approved security requirements	R, A	I
	39.	The provider collaborates with ACSA on a plan to implement security patches. This is something	R, A	I
	40.	Install security patches per the Change, Configuration and Release Management processes and procedures	R, A	I
	41.	Establish logging and archiving specifications	R, A	I
	42.	Identify logging and archiving specifications to support business requirements	I	R, A
	43.	Log and archive user and system activity.	R, A	I
	44.	Provide ACSA with reports on any server logs/intrusion detection activities, anomalies or deficiencies that could result in a compromise of the ecommerce system's data confidentiality, integrity or system performance	R, A	I
	45.	Provide ongoing support (patches, upgrades, signatures), tuning and management	R, A	I

Table 35 - Roles and Responsibilities – Security

15.0 SERVICE MANAGEMENT

15.1 Objectives

15.1.1 **SLR Achievement:** A primary goal of this Managed Service agreement is to consistently meet Service Level Requirements (SLRs) to ensure high-quality service delivery.

15.1.2 **SLR Specification:** Applicable SLRs are outlined in this Service Management Statement of Work (SOW), detailing performance expectations.

15.1.3 **Fee Reductions for Non-Compliance:** Specific SLRs linked to Fee Reductions are identified in Section 16.0**SERVICE CREDITS** applicable when business operations are impacted by failure to meet SLRs.

15.1.4 **Compliance Reporting:** The provider must submit written reports to the Technical Operations Manager: Networks, detailing compliance with specified SLRs to ensure transparency and accountability.

15.2 Reports

15.2.1 **Monthly SLA Performance Reporting**: Starting from the Effective Date, the provider must report monthly on service performance against each Service Level Agreement (SLA), including detailed supporting data. Reports must highlight (i) Service Level Failures and (ii) applicable penalties, notifying ACSA of any entitlements.

15.2.2 **Timely Submission:** Reports and supporting data must be provided to ACSA within ten (10) business days after the end of each Measurement Interval. All raw data and detailed information are considered ACSA's Confidential Information.

15.3 Root cause analysis

15.3.1 **Investigation and Correction:** The provider must promptly investigate Service Level Failures, performing Root Cause Analysis as per defined procedures to identify issues and implement corrective actions, preventing recurrence.

15.4 Support services

15.4.1 **Incident Resolution:** Support services involve daily activities to resolve incidents logged by users, monitoring tools, or system-generated alarms and error logs, ensuring operational continuity.

15.4.2 **Incident Management Compliance:** The provider must address and resolve all incidents following ACSA's incident management processes, ensuring alignment with organisational standards.

15.4.3 **SLA Adherence:** The provider must meet specified response and resolution times, which will form part of the agreed SLAs between the provider and ACSA.

15.4.4 **Penalties for Non-Compliance:** Failure to meet agreed SLA times will incur penalties, holding the provider accountable for performance.

15.4.5 **Independent SLA Performance:** Strong performance on one SLA does not offset poor performance on another, ensuring consistent accountability across all metrics.

15.4.6 **SLA Importance:** All SLAs, whether tied to specific services or not, are critical to ACSA, emphasising their importance to overall service quality.

15.5 SERVICE-LEVEL REQUIREMENTS (SLRs)

The following Service-Level Requirements (SLRs) establish the minimum performance standards that the provider must consistently meet or exceed to ensure high-quality service delivery.

15.5.1 Review of Service Levels and KPIS

15.5.1.1 **Annual SLR Review:** After the initial 90-day startup period, ACSA may request changes to any service level annually by notifying the provider, allowing for adjustments to align with evolving business needs.

15.5.1.2 **Change Implementation Process:** The provider has up to three weeks to review the requested change and assess its impact on support and maintenance service delivery. If modifications are needed, ACSA must grant the provider a reasonable time to implement these changes before the new service level takes effect, ensuring a smooth transition.

15.5.2 Measurement of Service Levels

Service levels are measured per site as well as per target. For instance, if there is a P1 incident at JNB and a P2 incident at JNB, they will be measured as 2 different SLRs and will attract service credits individually. In the same example, the response and resolutions are also individual SLRs. The service credit calculations use the at-risk amount for each SLR. This means for incident management, a P1 incident, for example, will have a total of 5 measures.

15.5.3 Priority levels

The following priority levels define the severity of incidents and service requests, guiding response and resolution times to minimise business impact. Providers must adhere to these classifications to meet Service Level Requirements (SLRs).

Priority Level	Business Impact	Description	Examples
Priority Level 1 - Emergency/Urgent	Critical	Incident causes complete work stoppage of a critical function, infrastructure component, or primary business process, affecting a broad group (e.g., entire department, floor, branch, line of business, or external customer). No workaround available.	- Network broadcast storm - MPLS Core routing failure - Layer 3 Core/distribution redundancy failover failure - WAN redundancy failover failure - Internet services are unavailable at one or more sites - One or more SSIDs are non-functional/unusable at one or more sites - Firewall configuration/operational issue impacting critical systems - Cisco Unified Communications Server unreachable - Cisco Voice Gateway is unable to route calls
Priority Level 2 - High	Major	Incident severely degrades business functions, impacts multiple users, a key customer, or a critical function operating at significantly reduced capacity. A workaround may exist, but is not sustainable.	- MPLS Core routing/switching inconsistency - Spanning-tree inconsistency - Switch stack failure (non-critical area) - Core fibre link packet drops/flapping - Slow/degraded internet - Campus-wide slow/degraded WLAN - Slow firewall traffic processing - VPN down - One-way telephone traffic - Telephone calls can only be made or received
Priority Level 3 - Medium	Moderate	Incident affects business processes, rendering certain functions unavailable or degrading system/service performance. A workaround may be available.	- Switch stack member failure (non-critical area) - Network device CPU above threshold - Access switch stack fibre uplink inconsistency - Switch stack member PoE blown ports/ASICs - Non-critical internet site unavailable (few users affected) - WLAN degraded in a small area - Firewall issue affecting a few users - Single voice gateway high CPU impact on call operations
Priority Level 4 - Low	Minimal	Incident has a negligible impact on business processes, can be scheduled, and has minimal effect on user productivity. A workaround is available, or the impact is minor.	- Redundant power supply failure - Fibre redundancy break - Single wireless access point down - Non-critical internet site unavailable (single non-critical user) - Firewall blocking single user resource access

Priority Level	Business Impact	Description	Examples
			- Faulty telephone handset (no power or partial functionality, single user)
Priority Level 5 - Service Requests	None	End-user service requests are logged via the Service Desk for non-incident-related tasks.	- Voice service provisioning - VLAN migration - Request to allow blocked website access - Request to permit firewall-blocked traffic

These priority levels ensure incidents and requests are addressed proportionately to their impact, aligning with ACSA's operational needs.

Table 36 – Priority Levels

15.5.4 **Incident management**

15.5.4.1 Time to resolve incidents/problems following responses to different incident priority level classifications.

15.5.4.2 Each IT Service categorises incidents/problems according to the incident/problem resolution priorities listed below for operational and after-hours.

Incident management response and resolution times for International Airports (Operational Hours)			
Incident/Problem Resolution	**Service Measure**	**Performance Target**	**SLR Performance %**
Time to Notify ACSA of or to accept/acknowledge a Priority 1	Time to Respond	<10 minutes	99.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 2 Incident	Time to Respond	<20 minutes	99.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 3 or 4 Incident	Time to Respond	<120 minutes	98.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 5 Incident	Time to Respond	<3 hours	98.0%
Priority Level 1	Time to Restore (Not linked to hardware failure)	<2 hours	99.0%
Priority Level 2	Time to Restore (Not linked to hardware failure)	<4 hours	98.0%
Priority Level 3	Time to Restore (Not linked to hardware failure)	<8 hours	98.0%
Priority Level 4	Time to Restore (Not linked to hardware failure)	Next business day or as prioritised by provider	98.0%
Priority Level 5	Time to Restore (Not linked to hardware failure)	To be agreed	98.0%
Priority Level 1	Resolution (permanent fix)	To be agreed	99.0%
Priority Level 2	Resolution (permanent fix)	To be agreed	99.0%
Priority Level 3	Resolution (permanent fix)	To be agreed	98.0%
Priority Level 4	Resolution (permanent fix)	To be agreed	98.0%
Priority Level 5	Resolution (permanent fix)	To be agreed	98.0%

Incident management response and resolution times for International Airports (Operational Hours)			
Priority Level1-5 Hardware Failure	Fix/replacement	In line with the hardware support procured by ASCA	99.0%
Root-Cause Analysis	Time to Report	Within 48 hours of incident resolution	98.0%
	Formula	Number of requests completed within Performance Target ÷ Total of all requests occurring during Measurement Interval	
	Measurement Interval	Weekly	
	Reporting Period	Monthly	
	Measurement Tool	Data from ACSA Service Management Tool (Service NOW) complemented with other provider tools if applicable	
	SLR Element Weighting Factor Allocation	50%	

Table 37 - Incident Response and Resolution time (Operational Hours)

Incident management response and resolution times for International Airports (Outside Operational Hours) and regional airports' operational hours.			
Incident/Problem Resolution	**Service Measure**	**Performance Target**	**SLR Performance %**
Time to Notify ACSA of or to accept/acknowledge a Priority 1	Time to Respond	<15 minutes	99.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 2 Incident	Time to Respond	<20 minutes	99.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 3 or 4 Incident	Time to Respond	<160 minutes	98.0%
Time to Notify ACSA of or to accept/acknowledge a Priority 5 Incident	Time to Respond	<3 hours	98.0%
Priority Level 1	Time to Restore (Not linked to hardware failure)	<3 hours	99.0%
Priority Level 2	Time to Restore (Not linked to hardware failure)	<5 hours	98.0%
Priority Level 3	Time to Restore (Not linked to hardware failure)	<10 hours	98.0%
Priority Level 4	Time to Restore (Not linked to hardware failure)	Next business day or as prioritised by the provider	98.0%
Priority Level 5	Time to Restore (Not linked to hardware failure)	To be agreed	98.0%
Priority Level 1	Resolution (permanent fix)	To be agreed	99.0%
Priority Level 2	Resolution (permanent fix)	To be agreed	99.0%
Priority Level 3	Resolution (permanent fix)	To be agreed	98.0%
Priority Level 4	Resolution (permanent fix)	To be agreed	98.0%
Priority Level 5	Resolution (permanent fix)	To be agreed	98.0%

Incident management response and resolution times for International Airports (Outside Operational Hours) and regional airports' operational hours.			
Priority Level1-5 Hardware Failure	Fix/replacement	In line with the hardware support procured by ASCA	99.0%
Root-Cause Analysis	Time to Report	Within 48 hours of incident resolution	98.0%
	Formula	Number of requests completed within Performance Target ÷ Total of all requests occurring during Measurement Interval	
	Measurement Interval	Weekly	
	Reporting Period	Monthly	
	Measurement Tool	Data from ACSA Service Management Tool (Service NOW) complemented with other provider tools if applicable	
	SLR Element Weighting Factor Allocation	50%	

Table 38 - Incident Response and Resolution time at International Airports (outside of operational hours) and regional airports.

15.5.5 Resource Availability

Resource Availability SLR	
Component	**Explanation of Component**
Definition	Measures the availability of the minimum specified resources as outlined in the resource table, ensuring adequate staffing for service delivery.
Coverage	Aligns with the resource table, specifying required resource types and locations.
Measurement Range	Target availability of 98%, ensuring consistent resource presence.
Frequency	Assessed monthly to track compliance with resource availability requirements.
Measurement Tool	Utilises the provider's automated time and attendance tool for accurate tracking of resource availability.
Calculation Formula	Performance is calculated as follows: - Dl = Total downtime hours (when resources are unavailable) - Al = Adjusted downtime hours (accounting for approved exceptions) - H = Total hours in the month (adjusted per resource type and availability requirements) - Ol = Total number of resources per type - El = Expected availability (H × Ol) - Report Only: Availability % = ((El − Dl) / El) × 100 - SLA: Adjusted Availability % = ((El − Al) / El) × 100
SLR Element Weighting Factor Allocation	20% of the overall SLR evaluation, reflecting the critical role of resource availability in service delivery.

Table 39 Resource availability SLR

15.5.6 Requests

System Administration Service-Level Requirements			
System Administration Task	**Service Measure**	**Performance Target**	**SLR Performance %**
Configure an Access port to a specific VLAN	Elapsed Time	1 Hour	99.0%
Configure a new SSID	Elapsed Time	24 Hour (excluding change process)	98.0%
Configure a new Access Point	Elapsed Time	24 Hour (excluding change process)	98.0%
Add a new FW rule	Elapsed Time	24 Hour (excluding change process)	98.0%
Add a new IPSec tunnel	Elapsed Time	24 Hour (excluding change process)	98.0%
Configure a new IPT user profile	Elapsed Time	4 Hour (excluding change process)	98.0%
Configure a new phone	Elapsed Time	4 Hour (excluding change process)	98.0%
Provide access to voice recordings	Elapsed Time	4 Hour (excluding change process)	98.0%
	Formula	Number of instances within Performance Target ÷ Total number of instances during Measurement Interval = "Percent (%) Attained"	
	Measurement Interval	Measure Monthly	
	Reporting Period	Report Monthly	
	Measurement Tool	ACSA Service Desk Stats/ Provider request schedule	
	SLR Element Weighting Factor Allocation	50%	

Table 40 Requests SLR

15.5.7 **Install, Move, Add, Change, Delete (IMACDs)**

15.5.7.1 IMACD Scope: IMACDs encompass the physical installation, dismantlement, or relocation of hardware, as well as hardware or software installations, upgrades, or updates, all performed following ACSA's Change Management policies. These activities are typically planned and scheduled in advance to ensure minimal disruption.

15.5.7.2 IMACD Non-Compliance: If the provider cannot complete an IMACD within the required timeline, they must submit a proposal to ACSA specifying a committed completion time. ACSA reserves the right, at its sole discretion, to accept the proposal or engage an alternative provider (internal or external) to perform the service, ensuring timely execution.

The following outlines the performance targets and weighting for Install, Move, Add, Change, Delete (IMACD) activities to ensure timely and compliant execution.

Service Measure:	Performance Target:	SLR Performance %
Receipt of IMACD Plan	The provider must submit the IMACD plan (covering installation,	98%

	decommissioning, move, or change) per ACSA standards within 5 business days of the request. Failure to provide the plan or written confirmation of inability to meet timelines will be considered a missed SLA.	
Completion of IMACD	Upon approval of the IMACD plan, the provider must complete all milestones on time as outlined in the approved plan. Each milestone not delivered as scheduled will be deemed a missed SLA.	98%
SLR Element Weighting Factor Allocation	50% of the overall SLR evaluation, reflecting the critical importance of timely IMACD execution to ACSA's operations.	50%

Table 41 IMACD SLR

15.5.8 **Asset management**

15.5.8.1 Asset Tracking Accuracy: Within five business days after the start of each calendar quarter, the provider must select a statistically valid sample, following the agreed process, to assess compliance with Service Level Requirements (SLRs) for the accuracy of individual data elements in the asset tracking database. The data accuracy must meet the specified SLR standards to ensure reliable asset management.

15.5.8.2 Data Exclusion Flexibility: Historical information may not always be available, and ACSA may, at its discretion, grant exclusions for certain data elements, allowing flexibility in compliance assessments where applicable.

Asset Tracking SLR			
	Service Measure	**Performance Target**	**SLR Performance %**
Accuracy of Data in Asset Tracking Database	Accuracy	Accuracy percentage of each of the following data elements as determined by audit:	
		Data Element	**Accuracy Percentage**
		ACSA asset tag number, Serial Number, Model number, PO number, Invoice number	99%
		Location (Wire centre, position in Cabinet, Room tag number, Site)	99%
	Formula	Number of tracked assets where data element is determined to be correct ÷ Total number of tracked assets audited	
	Measurement Interval	quarterly as of Effective Date	
	Measurement Tool	Physical Audit.	
	SLR Element Weighting Factor Allocation	30%	

Table 42 Asset Tracking SLR

15.5.9 Configuration management

15.5.9.1 Configuration Management Services: These services involve maintaining a logical model of the infrastructure by identifying, controlling, maintaining, and verifying the versions of installed hardware, software, and utilities. This ensures accurate documentation and operational integrity of the infrastructure.

15.5.9.2 Quarterly Compliance Assessment: Within five business days after the start of each calendar quarter, the provider must select a statistically valid sample to assess and review compliance with Service Level Agreements (SLAs) for configuration management, ensuring consistent accuracy and adherence to standards.

Configuration Management SLR	
Service Measure:	**Performance Target:**
Configuration Record Accuracy: Data accuracy – chosen sample of all configurations (hardware and software) tracked by the ACSA NMS tools	98%
Timelines of updates: Time to update configuration records	1 day after the change to the configuration
Measurement Interval:	Electronic audit, conducted quarterly from the date of contract commencement
Measurement Tool:	ACSA NMS Tools
SLR Element Weighting Factor Allocation	30%

Table 43 Configuration Management SLR

15.5.10 Resource Certifications and Experience

Resource Availability SLR	
Component	**Explanation of Component**
Definition	Measures compliance based on the minimum certified resources and years of experience outlined in the tender evaluation, ensuring qualified personnel for service delivery.
Coverage	Aligns with the resource requirements specified in the tender evaluation, detailing certification and experience expectations.
Measurement Range	Targets a 98% compliance rate, ensuring consistent adherence to certification and experience standards.
Frequency	Assessed monthly to verify ongoing compliance with resource qualification requirements.
Measurement Tool	Utilises the provider's response sheet from the tender, accompanied by a summarised report, to validate certifications and experience.
Calculation Formula	Calculated as per the tender evaluation sheet, providing a standardised method to assess compliance.
SLR Element Weighting Factor Allocation	30% of the overall SLR evaluation, reflecting the critical importance of qualified resources to service quality.

Table 44 Resource Certifications and experience SLR

15.5.11 Overall service satisfaction

15.5.11.1 Satisfaction Measurement: The provider's service performance will be evaluated through client surveys and end-user feedback, using a satisfaction scale of 1 (lowest) to 5 (highest). This metric assesses user experience and service quality to ensure alignment with ACSA's expectations. This requirement ensures continuous improvement and user-focused service delivery through structured feedback mechanisms.

End-User Satisfaction SLR			
End-User Satisfaction	**Service Measure**	**Performance Target**	**SLR Performance %**
Scheduled Survey (conducted semi-annually by ACSA or its designated Third-Party agent)	End-User Satisfaction rate	clients surveyed should be very satisfied or satisfied	90%
	Formula	1. Sum of survey results from each participant ÷ Total number of participants responding to the scheduled survey	
	Measurement Interval	Quarterly	
	Reporting Period	Quarterly	
	Measurement Method/Source Data	ACSA Service Management Tool, or results from a special survey	
	SLR Element Weighting Factor Allocation	10%	

Table 45 Overall satisfaction SLR

15.5.12 Software/Firmware Refresh

Software refresh for all upgrades and new releases.

Software /firmware Refresh Service-Level Requirements			
	Service Measure	**Performance Target**	**SLR Performance %**
Notification of vendor Software upgrades and new releases	Response Time	Within 30 days after the Software vendor announcement	95.0%
Implementation of service packs and updates to "dot" releases	Response Time	Within 60 days after approval by Client	95.0%
Implementation of version or major release updates	Response Time	Within 120 days after approval or be agreed time by ACSA	95.0%
	Formula	Number of requests completed on time ÷ Total of all requests occurring during the Measurement period	
	Measure Interval	Measure Monthly	
	Reporting Period	Report Monthly	
	Measurement Tool	TBD	
	SLR Element Weighting Factor Allocation	30%	

Table 46 Software/Firmware Refresh SLR

15.5.13 **Service level agreement measurement exclusions.**

These exclusions clarify the boundaries of the provider's accountability, ensuring fair assessment of Service Level compliance.

Number	Service Level Measurement Exclusions
1.	Non-Approved Ancillary Equipment: Connection of ancillary equipment not supplied by the provider or approved by the equipment/software manufacturer, which may impact performance or compatibility.
2.	Negligent Use by ACSA: Negligent use, abuse, or misuse of equipment or software by ACSA personnel, leading to operational issues or damage.
3.	Damage During ACSA Transport: Damage to equipment or software occurring during transportation handled by ACSA, outside the provider's scope.
4.	Non-Provider Electrical Work: Electrical work performed by entities other than the provider, which may affect equipment functionality.
5.	External Power Issues: Failures or performance issues caused by external factors, such as verified electrical power fluctuations or outages, beyond the provider's control.
6.	Uncommunicated Changes: Authorised or unauthorised changes to equipment or systems not communicated to the provider, which may disrupt service delivery.
7.	Non-Provider Equipment/Services: Failures of equipment or services not directly managed or maintained by the provider, as they fall outside the provider's responsibility.

Table 47 SLA Measurement Exclusions

16.0 SERVICE CREDITS

The Service Credit Methodology aims to be an appropriate and adequate remedy for non-performance by the Service provider. The philosophy of the Service Credit Methodology is such that it should drive positive behaviour by encouraging compliance with the Service Level Requirements (SLRs) and be consistent with the outcomes required by ACSA. The Service Credit Methodology has been designed recognising this philosophy and incorporates:

- the need to match Service Credit payments to the severity of the failure/defect.
- the need to provide appropriate incentives based on regimes to cure any defect or failure as quickly as possible.
- the need to avoid an inappropriate impact on Service provider funding.
- the need to be easily understood and unambiguous.
- the need to be administratively manageable; and
- the need to avoid consistent non-performance.

16.1 **Principles**

The principles for the calculation of the credits are described below:

16.1.1 Service Credits only occur because of Service Level Failures.

16.1.2 The Service Levels are calculated for each SLR according to the measurement interval specified in each SLR table (monthly by default),

16.1.3 The Service Credits are calculated according to the formula associated with the SLR as specified in each SLR table.

16.1.4 The Service Credits are totalled for each SLR and valued using the contractual value of a Service Credit.

16.1.5 A good performance on an SLR cannot compensate for a bad performance on another one.

16.1.6 The SLRs that are considered critical by ACSA will always be associated with Service Credits assigned. The other set of SLRs can be subject to Service Credits mechanisms, if they are included in a quality improvement plan, or if the Service Levels attained are periodically below requirements.

16.1.7 The fact that an SLR is not associated with a Service Credit does not mean that this SLR is not important to ACSA.

16.1.8 ACSA reserves the right to associate the Services Credit mechanism to SLRs where the Service provider would have been in failure over several consecutive months.

16.1.9 ACSA reserves the right to not apply some or any Service Credits that may occur at its sole discretion.

16.1.10 The provider will be allowed a grace period of ninety (90) days (to familiarise itself with the operations at all airports) before the implementation of service credits will commence. SLA's will be measured and reported on during the grace period; however, no credits will apply.

16.2 **Definitions**

16.2.1 **Total Per Site Monthly Fee -** means the monthly service fixed fee per ACSA Site payable by ACSA to the Service provider for the Services.

16.2.2 **At Risk Amount -** means, for any month during the Term, fifty percent (50%) of the monthly fixed Service Fees per ACSA Site.

16.2.3 **Weighting Factor** - means, for a particular Service Level Requirement (SLR), the portion of the At-Risk Amount used to calculate the Service Credit payable to ACSA in the event of a Service Level Failure with respect to that SLR.

16.2.4 **Monthly Service Credit Pool** - means two hundred percent (200%).

16.2.5 **Service Level Failure(s)** - means whenever the Service provider's actual level of performance for a particular Service Level metric (as calculated by that particular metric's service level calculation) is worse than the Target Performance adjusted by the Minimum Performance Percentage (%) for that Service Level.

16.2.6 **Service Credit** - means a calculated value based on the percentages in Weighting of Monthly Service Credit Pool in Section 3 of this document.

16.2.7 **Service Level Requirement Categories** – SLRs are allocated against the following categories:

16.2.7.1 Primary Category: Has a direct impact on ACSA business. Service Credits will be applied.

16.2.7.2 Secondary Category: Has some direct impact on ACSA business***;*** no service credits are applicable to these SLRs***,*** which have a Weighting Factor of zero percent (0%).

16.3 **Methodology**

16.3.1 **Monitoring; reports; root cause analysis.**

16.3.1.1 Monitoring

The Service provider shall utilise ACSA measurement and monitoring tools and produce the metrics and reports necessary to measure its performance against the Service Levels.

Additional Tools may be implemented by the provider at its own cost should the ACSA tools not be enough.

Upon request and at no additional charge to ACSA, the Service provider shall provide ACSA or its designees with information and access to the tools and procedures used to produce such metrics.

16.3.1.2 Reports

The Service provider shall report to ACSA its performance of the Services against each SLR every month beginning on the Effective Date, along with detailed supporting information. As part of the standard monthly Service Level reports, the Service provider shall notify ACSA of any:

(i) Service Level Failures, and
(ii) Service Credits to which ACSA becomes entitled.

The Service provider shall provide such reports and supporting information to ACSA no later than 5 (five) Business Days following the end of the applicable Measurement Interval. The raw data and detailed supporting information shall be Confidential Information of ACSA.

16.3.1.3 Root cause analysis

The Service provider shall promptly investigate and correct Service Level Failures in accordance with the procedures for Root Cause Analysis outlined in the Agreement.

16.3.2 **Calculating service credits**

For each Primary Service Level Failure, the Service provider shall pay or credit to ACSA a Service Credit that will be computed by multiplying (a) the Weighting Factor Allocation for such Service Level by (b) the At-Risk Amount.

For example, assume for purposes of illustration only, that the Service provider fails to meet a Service Level with a Weighting Factor of 10% (ten percent) and that the monthly Fees equal R100,000 (one hundred thousand rand) and the At-Risk Amount is 20% (twenty percent). The Service Credit due to ACSA for such Service Level Failure would be: 10% * (20% * R100,000.00) = R2,000.

16.3.3 **Service breach**

If a Service Level Failure recurs **in more than four consecutive** Measurement Intervals, then such Service Level Failure shall constitute a material breach entitling ACSA to the rights set out in the Agreement.

16.3.4 **Several service level failures**

Subject to Section 16.3.5If more than one Service Level Failure with respect to Service Levels has occurred in a single month, the sum of the corresponding Service Credits shall be credited or paid to ACSA.

16.3.5 **Successive service level failures**

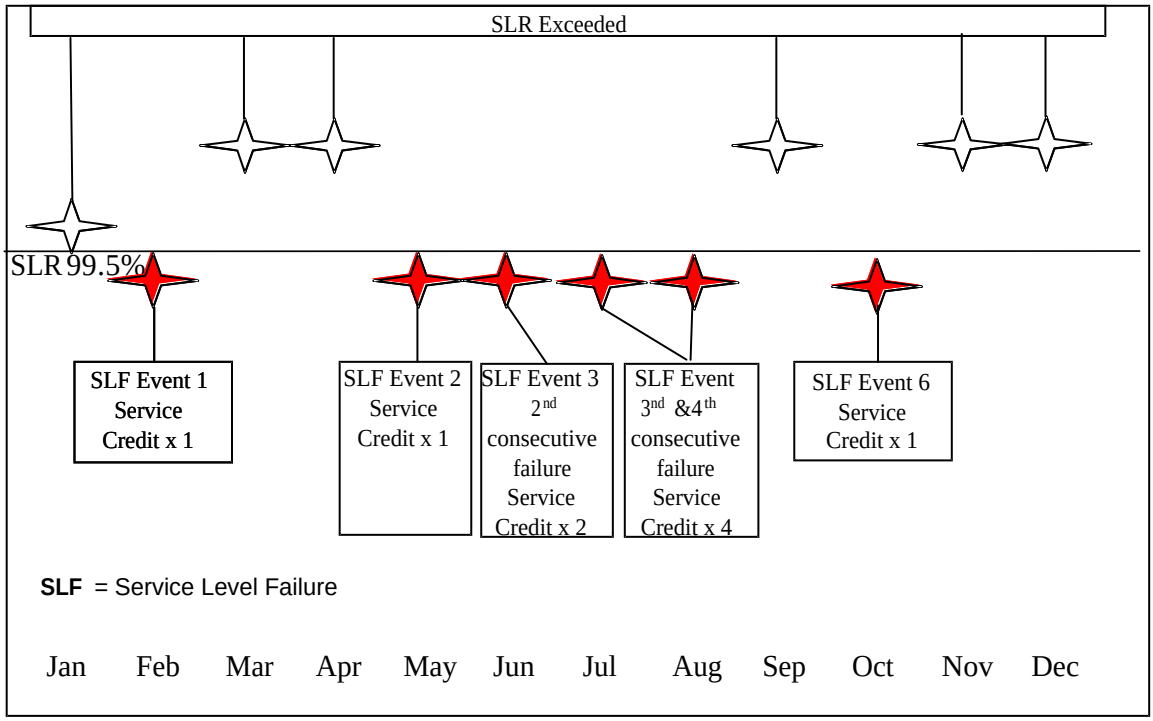
If a Service Level Failure with respect to a given Service Level recurs in consecutive Measurement Intervals, the amount of the applicable Service Credit payable to ACSA shall be multiplied by the following factors for subsequent Measurement Intervals:

(i) Service Level Failure in two consecutive Measurement Intervals, then **twice (x2)** the amount of the Performance Credit as originally calculated; and

(ii) Service Level Failure in three or more consecutive Measurement Intervals, then **four times (x4)** the amount of the Service Credit as originally calculated.

The Service Credit for any given Service Level shall only be increased as described above, and such increase shall be payable for all consecutive Service Level Failures with respect to such Service Level.

Figure 1. Service Credit for Successive Failures Example



16.3.6 **Service credits cap**

In no event shall the aggregate amount of Service Credits credited or paid to ACSA with respect to all Service Level Failures occurring in a single month exceed the At-Risk Amount.

16.3.7 **Payment/credit of service credits**

The Service provider shall itemise the total amount of Service Credits it is obliged to credit to ACSA with respect to Service Level Failures occurring in each month on the invoice that contains charges for such month. The Service provider shall credit the total amount of such Service Credits related to a given month in the subsequent monthly invoice after ACSA signoff of the Service Credits for the applicable Measurement Interval. Upon termination or expiration of the Term, the Service provider shall pay to ACSA the amount of any Service Credits not so paid or credited to ACSA's account or any unused portion of such Service Credits.

16.3.8 **Non-exclusive remedy**

The Service provider acknowledges and agrees that the Service Credits shall not be deemed or construed to be liquidated damages or a sole and exclusive remedy or instead of any other rights and remedies ACSA has under the Agreement, at law or in equity.

16.3.9 **Earn-Back**

Following any service-level failure, ACSA may allow the provider the opportunity to earn back the service credits charged in one or more measurement periods.

If all the service levels for the relevant service and any others agreed to be associated with that service are exceeded, during each of the **three** measurement periods following the service-level failure, ACSA may, at its sole discretion, return half of the service credits paid to the provider.

If all the service levels for the relevant service and any others agreed to be associated with that service are exceeded, during each of the **six** measurement periods following the service-level failure, ACSA may, at its sole discretion, return the remaining half of the service credits paid to the provider.

The provider may, where the requisite levels of performance are exceeded, make representations to the Company in this regard.

16.4 Changes to performance measurements

16.4.1 Changes to weighting factors

ACSA may request changes to the Weighting Factors for any Service Level by sending written notice to the Service provider. These requested changes will be negotiated through the appropriate Relationship Management structures to gain mutual agreement on such changes prior to them taking effect during the next full measurement interval pertaining to such changed metrics.

16.4.2 Additions

No more than once quarterly, ACSA may add Service Levels by sending written notice to the Service provider at least 30 (thirty) days prior to the date that such added Service Levels are to be effective. The target performance levels for such additional Service Levels shall be determined by mutual agreement of the Parties using industry standard measures.

16.4.3 Deletions

ACSA may delete Service Levels by sending written notice to the Service provider at least thirty (30) days before the date that such deletions are to be effective.

17.0 MEETINGS AND REPORT REQUIREMENTS

This section outlines the meeting and reporting obligations for all services to ensure effective communication and performance oversight.

All reports must be submitted according to the timelines specified in the table below. Failure to deliver reports within the stipulated timeframes will result in ACSA withholding invoice payments for the respective month until the reports are provided, ensuring accountability and timely compliance.

17.1 **Project meetings:** Weekly project meetings, or as needed, will be held at ACSA, scheduled by the ACSA Project Manager for the project's duration. Attendees must include the provider's Project Manager and the ACSA Project Manager. The agenda will cover, but is not limited to, project progress, delays, risks, issues, and financials, fostering proactive management and issue resolution.

17.2 **Maintenance and Support Meetings:** Maintenance and support meetings will be held as outlined in the table below, with required attendees from both ACSA and the provider present throughout the contract term. These meetings provide a platform for the provider to report on service performance, ensuring transparency and alignment with Service Level Requirements.

Meeting Name and frequency	Participants and roles	Documents to be produced after the meeting by the Service provider
Weekly Service Review	· ACSA-IT Engineer (chair) · Provider Senior Site Manager · Provider administrator	· Minutes of meeting · Running Action register for any open actions to be addressed
Weekly Project status update	· ACSA-IT PM (chair) · Operations Manager · Provider Senior Site Manager · Provider Project Manager · Provider administrator	· Minutes of meeting · Updated project schedule · Action register for any open actions to be addressed · Risks and Issues register
Monthly Care Review	· Operations Manager (chair) · Provider Senior Site Manager · Provider Relationship Manager · Provider administrator	· Minutes of meeting · Action register for any open actions to be addressed · Risks and Issues register · Service Credit Report
Quarterly review meeting	· Operations Manager (chair) · Provider Senior Site Manager · Provider Relationship Manager · Provider administrator · Senior Manager IT Infrastructure	· Minutes of meeting · Action register for any open actions to be addressed · Risks and Issues register
Annual review meeting	· Operations Manager (chair) · Senior Manager IT Infrastructure · Provider Senior Site Manager	· Minutes of meeting · Action register for any open actions to be addressed · Risks and Issues register

Meeting Name and frequency	Participants and roles	Documents to be produced after the meeting by the Service provider
	· Provider Relationship Manager · Provider administrator · Senior Manager IT Infrastructure	

Table 48 Meetings definitions

Frequency	Report Name	Report Content	Due date	Submit to	Format	Meeting Name and frequency
Daily	Fault Summary	Reported faults summary (resolved and outstanding) Weekly to review previous weeks' reports	Start of business every day	ACSA Technical Lead	Email a written report summary with supporting tables.	Weekly Service Review
	Fault Summary escalation	Outstanding faults and notification Weekly to review previous weeks' reports	Start of business every day	ACSA Technical Lead	Email a written report summary with supporting tables.	Weekly Service Review
	Re-opened fault summary	Re-opened reported faults Weekly to review previous weeks' reports	Start of business every day	ACSA Technical Lead	Email a written report summary with supporting tables.	Weekly Service Review
Weekly	Summary Care Report	Summarised report weekly	COB every Friday	ACSA Technical Lead	Email a written report summary with supporting tables.	Weekly Service Review
	Project and IMACD updates	Installations completed, including relocations and projects. Present detailed job cards.	One day before the project status update meeting	ACSA Technical Lead & ACSA Project Manager	Email a written report summary with supporting tables.	Weekly Project status update
	Data/wire centre areas of concern	Testing done on data/core/wire centres, highlighting areas of concern Weekly to review previous weeks' reports	3 days before the meeting	Operations Manager	Email a written report summary with supporting tables.	Weekly Service Review
Monthly	Consolidated Care Report	Monthly consolidated report · Spares Usage · Calendar month Incidents · Payment	3 days before the meeting	Operations Manager	Email presentation with attached supporting information	Monthly Care Review

Frequency	Report Name	Report Content	Due date	Submit to	Format	Meeting Name and frequency
		· Monthly services deliverables · SLA Report (performance against SLR's) · SLA improvement plan ·Service Credits				
	Preventative maintenance	Schedule of preventative maintenance for the following month for all sites	3 days before the meeting	ACSA Technical Lead	Email Excel schedule document	Monthly Care Review
	Asset Data	Asset Register	3 days before the monthly account meeting	ACSA Technical Lead	Email Excel document	Monthly Care Review
Quarterly	Stock levels	BOM register documenting stock levels on hand	3 days before the quarterly review	ACSA Technical Lead	Email Excel document	Quarterly review meeting
	Contract appendix review	Review updates to the contract appendices are completed	3 days before the Quarterly review meeting	ACSA Technical Lead	Email PDF document	Quarterly review meeting
	Baseline (CMDB) information	Review updates to Baseline CMDB	3 days before the Quarterly review meeting	ACSA Technical Lead	Email Excel document	Quarterly review meeting
	Design documents for audit	Design document audit	3 days before the Quarterly review meeting	ACSA Technical Lead	Email Word document on ACSA template	Quarterly review meeting
	Transformation	Performance, financial and development report of all transformation partners	3 days before the Quarterly review meeting	ACSA Technical Ops manager	Presentation detailing performance and transformation progress, financial report	Quarterly review meeting

Frequency	Report Name	Report Content	Due date	Submit to	Format	Meeting Name and frequency
	Proposed improvements report	Proposed improvements or enhancement report	3 days before the yearly review meeting	ACSA Technical Lead	Email Word document	Annual review meeting
	Annual performance SLA report	Consolidation of the previous 12 months' SLA performance	3 days before yearly review meeting	Operations Manager	Email PDF document	Annual review meeting
	Contract adherence review	Summary of contract requirements and adherence thereof	3 days before the annual review meeting	Operations Manager	Email PDF document	Annual review meeting

Table 49 Reporting definitions

Approvals

Designation	Full Name	Date	Signature
Requested By: Technical Manager: Digital Infrastructure	**Malcolm Perumal**	2025 20 11	
Support By: Senior Manager: Digital Infrastructure and Operations	**Werick Venter**	2025 20 11	
Supported By: Chief Technical Officer	**Vishalan Govender**	2025 21 11	
Approved as per ACSA DLA by: Interim Chief Information Officer	**Sello Makhubela**	2025 24 11	

Annexure B

Proposal Format and Response Form

to

LAN / WAN / Wireless / IP Telephony and Network Security Services

Table of Contents

1. Introduction

Instructions to Bidders for Proposal Submission

- **Use of Proposal Response Template:** This Proposal Response Template serves as the foundation for submitting a formal proposal to ACSA. Bidders are required to adhere to this template to ensure clarity and alignment with ACSA's requirements.
- **Proposal Structure:** Bidders must organise their responses in accordance with the structure provided in this Proposal Response Template. Compliance with the prescribed format is essential for a consistent and thorough evaluation.
- **Appendices:** Bidders are encouraged to limit the inclusion of appendices to only those materials deemed critical for the evaluation and comprehension of the proposal. All appendices must be clearly numbered, referenced within the main response, and kept concise.

2. General Instructions

- **Commitment to Scope of Work:** The Bidder shall perform all services as outlined in the Scope of Work and associated annexures to enable ACSA to achieve the specified service objectives and deliverables throughout the contract duration. This includes performing preventative maintenance tasks and addressing day-to-day service requests in accordance with the service levels defined in the Scope of Work.
- **Completion of Specification Tables:** Bidders are required to complete the provided tables, clearly indicating whether their proposed solution meets the specified requirements. Responses must be comprehensive and precise.
- **Supporting Documentation:** Bidders must submit documentation to substantiate the responses provided in the specification tables. Failure to include supporting documentation or proof will result in the response being deemed non-responsive.
- **Organisation of Supporting Documents:** All supporting documents and proof must be compiled in a clearly indexed Appendix. Each document must include page numbers and be explicitly referenced within the proposal. Non-compliance with indexing and pagination requirements may result in sections being overlooked during evaluation, potentially leading to a non-responsive designation.
- **Proof of Experience:** Bidders may demonstrate experience through either company credentials or the qualifications of individual resources. If resource experience is used, those resources must be employed by the Bidder at the

commencement of the contract. In the event that cited resources are no longer employed, they must be replaced with individuals of equal or superior skills and experience.

- **Service Level Agreement (SLA) Compliance:** Compliance with these requirements will be assessed as part of the monthly SLA reporting process. The selected service provider must consistently meet the defined SLA standards throughout the contract term.
- **POPI Compliance:** All submitted documentation must comply with the Protection of Personal Information Act (POPI) requirements to ensure the confidentiality and lawful handling of personal information.

3. Functional & Technical Criteria

3.1 Resources

3.1.1 Project Management

Certification and Experience: Bidders must provide evidence of at least one Project Manager holding a valid PMBOK or PRINCE2 Practitioner certification and a minimum of five (5) years of relevant project management experience.

Proof of Experience: Experience must be substantiated through reference letters from previous projects. Each reference letter must explicitly name the certified Project Manager whose credentials are provided. Curriculum Vitae (CVs) will not be accepted.

Resource Requirement: A minimum of one qualified Project Manager is required. Bidders may submit details for additional resources if desired, provided all requirements are met for each.

Provide Proof under Appendix P

Resource #	Resource Name	Certification	Year Obtained	Years of Experience	Reference in Document
1					
2					
3					

3.1.2 **Technical Resources**

Certification: Bidders must provide evidence of certified technical resources for the areas specified in the tables below, meeting or exceeding the minimum certification levels indicated. Higher-level certifications are acceptable and will be recognised.

Proof of Experience: Years of experience must be substantiated through reference letters from previous projects. Each reference letter must explicitly name the certified resource whose credentials are provided. Curriculum Vitae (CVs) will not be accepted.

Certificate Submission: A copy of the relevant certificate for each resource must be included, clearly demonstrating the certification held.

Documentation Organisation: All supporting documents (certificates and reference letters) must be organised and submitted under the following appendices, with clear indexing and page numbering referencing the specific section and page where each document is located:

Appendix Q: Technical Resources – Campus Routing and Switching

Appendix R: Technical Resources – IP Telephony and Collaboration, Wireless, and Riverbed RiOS

Appendix S: Technical Resources – Network Firewalling and Security

Minimum Requirements: Only the minimum number of resources specified in the tables is required. Additional resources may be submitted if desired, provided all requirements are met. If a resource does not meet all the minimum certification requirements, then these requirements must be met by multiple individuals. If one resource has more than one Certification the resource can be used multiple times

3.1.2.1 **Technical Resources – Campus routing and switching.**

Certification	Minimum Quantity of Certified Resources Required	Minimum years of networking experience	Qty Available	Certification Name	Expiry Date	Years of Experience	Proof Provided (YES/NO)	Reference in Submission
Principal Network Engineer - (CCIE R&S AND equivalent certification for any proposed new OEMs)	1	3						
Senior Network Engineers - Cisco Certified Network Professional (CCNP R&S OR Enterprise AND equivalent certification for any proposed new OEMs)	3	3						
Network Engineers - Cisco Certified Network Associate (CCNA R&S or CCNA Industrial or enterprise AND equivalent certification for any proposed new OEMs)	4	2						
Network Engineers - Cisco Certified Network Associate Datacentres (CCNA Datacentre AND equivalent certification for any proposed new OEMs)	1	1						

3.1.2.2 Technical Resources – IP Telephony and Collaboration, Wireless and WAN Optimisation

Certification	Minimum Quantity of Certified Resources Required	Minimum years of networking experience	Qty Available	Certification Name	Expiry Date	Years of Experience	Proof Provided (YES/NO)	Reference in Submission
Cisco Certified Internetworking Expert (Voice/Collaboration AND equivalent certification for any proposed new OEMs)	1	3						
IP Telephony and Collaboration Administrators (CCNP Collaboration AND equivalent certification for any proposed new OEMs)	2	2						
Wireless Network Engineer/Administrator (CCNA Wireless AND equivalent certification for any proposed new OEMs)	1	2						
Riverbed WAN Optimisation Administrator (RCSA-W) or minimum to have completed WAN Optimisation Essentials training AND equivalent certification for any proposed new OEMs	1	2						

3.1.2.3 **Technical Resources – Network Firewalling and Security**

Certification	Minimum Quantity of Certified Resources Required	Minimum years of experience	Qty Available	Certification Name	Expiry Date	Years of Experience	Proof Provided (YES/NO)	Reference in Submission
Check Point Certified Security Expert (CCSE AND equivalent certification for any proposed new OEMs)	1	3						
Check Point Certified Security Administrator (CCSA AND equivalent certification for any proposed new OEMs)	1	2						

3.2 Proven Experience

Campus Routing and Switching

Proof of Experience: Bidders must submit original, signed, and/or stamped contactable reference letters on the letterhead of the issuing company to demonstrate experience in maintaining access, distribution, and core hardware and related software for campus routing and switching.

Minimum Requirements: Reference letters must include:

- At least two (2) client references with networks comprising more than 150 access switches.
- At least two (2) client references with networks comprising more than ten (10) campus core and distribution routers and switches.

Content of Reference Letters: All mandatory information specified in the tables below must be clearly addressed in the reference letters to ensure a comprehensive evaluation.

Documentation Submission: All reference letters must be compiled and submitted under Appendix T – Proven Experience: Campus Routing and Switching Maintenance, with clear indexing and page numbering for ease of reference.

Compliance: Failure to provide complete, verifiable, and properly formatted reference letters may result in the response being deemed non-responsive.

3.2.1.1 Campus Network: Access Network References (> 150 access switches)

Information Requirement	Mandatory	Reference Details 1	Reference in Submission	Reference Details 2	Reference in Submission
Company Name	Y				
Industry	N				
Scope of services provided	Y				
% Mean Time to Repair SLR achieved	N				
Environment size	Y				
Start Date	N				
Contract Term	Y				
Contact Person	Y				
Contact Telephone Number	Y				
Contact Position	Y				
Contact e-mail address	Y				

3.2.1.2 Campus Network: Core and distribution References (> 10 Core routers and switches)

Information Requirement	Mandatory	Reference Details 1	Reference in Submission	Reference Details 2	Reference in Submission
Company Name	Y				
Industry	N				
Scope of services provided	Y				
% Mean Time to Repair SLR achieved	N				
Environment size	Y				
Start Date	N				
Contract Term	Y				
Contact Person	Y				
Contact Telephone Number	Y				
Contact Position	Y				
Contact e-mail address	Y				

Unified Communications, Wireless, and Network Security Maintenance

Proof of Experience: Bidders must submit original, signed, and/or stamped contactable reference letters on the letterhead of the issuing company to demonstrate experience in providing national, 365x24x7x4 maintenance services for unified communications, collaboration, wireless, proxy and security hardware and related software.

Minimum Requirements: Reference letters must include:

- At least two (2) client references with networks comprising more than two (2) Unified Communication Manager instances and more than 150 IP Telephones.
- At least two (2) client references with networks comprising more than fifty (50) wireless access points.
- At least two (2) client references with networks comprising more than two (2) Smart Security firewalls.
- At least two (2) client references with networks comprising more than two (2) Proxy appliances.

Content of Reference Letters: All mandatory information specified in the tables below must be clearly addressed in the reference letters to ensure a comprehensive evaluation.

Documentation Submission: All reference letters must be compiled and submitted under Appendix U – Proven Experience: Unified Communications, Wireless, and Network Security Maintenance, with clear indexing and page numbering for ease of reference.

Compliance: Failure to provide complete, verifiable, and properly formatted reference letters may result in the response being deemed non-responsive.

3.2.1.3 Unified Communications and Collaboration References (> 2 UCM and >150 IP Phones)

Information Requirement	Mandatory	Reference Details 1	Reference in Submission	Reference Details 2	Reference in Submission
Company Name	Y				
Industry	N				
Scope of services provided	Y				
% Mean Time to Repair SLR achieved	N				
Environment size	Y				
Start Date	N				
Contract Term	Y				
Contact Person	Y				
Contact Telephone Number	Y				
Contact Position	Y				
Contact e-mail address	Y				

3.2.1.4 Wireless Networking References (> 50 Access Points)

Information Requirement	Mandatory	Reference Details 1	Reference in Submission	Reference Details 2	Reference in Submission
Company Name	Y				
Industry	N				
Scope of services provided	Y				
% Mean Time to Repair SLR achieved	N				
Environment size	Y				
Start Date	N				
Contract Term	Y				
Contact Person	Y				
Contact Telephone Number	Y				
Contact Position	Y				
Contact e-mail address	Y				

3.2.1.5 Network Security References (> 2 Smart Security Firewalls)

Information Requirement	Mandatory	Reference Details 1	Reference in Submission	Reference Details 2	Reference in Submission
Company Name	Y				
Industry	N				
Scope of services provided	Y				
% Mean Time to Repair SLR achieved	N				
Environment size	Y				
Start Date	N				
Contract Term	Y				
Contact Person	Y				
Contact Telephone Number	Y				
Contact Position	Y				
Contact e-mail address	Y				

3.2.1.6 Proxy References (> 2 Web Security Appliance or Proxy Solution)

Information Requirement	Mandatory	Reference Details 1	Reference in Submission	Reference Details 2	Reference in Submission
Company Name	Y				
Industry	N				
Scope of services provided	Y				
% Mean Time to Repair SLR achieved	N				
Environment size	Y				
Start Date	N				
Contract Term	Y				
Contact Person	Y				
Contact Telephone Number	Y				
Contact Position	Y				
Contact e-mail address	Y				

4. Preventive Maintenance Schedule, Corrective Maintenance Procedures, and a Resource Schedule

Preventative Maintenance Plan: Service Providers must submit a comprehensive preventative maintenance plan that adheres to the requirements outlined in Annexure 1A. The plan must address all requirements specified in the Scope of Services, incorporating common and/or generic Original Equipment Manufacturer (OEM) recommended procedures, toolkits, and task lists.

Corrective Maintenance and Resource Scheduling: The submission must include detailed corrective maintenance procedures and a resource schedule, ensuring alignment with the Scope of Services and operational requirements.

Documentation Reference: In the space provided below, Service Providers must include precise references (section and page numbers) to the relevant sections of their proposal where the preventative maintenance plan, corrective maintenance procedures, and resource schedule are detailed.

Documentation Submission: All supporting documentation must be compiled and submitted under Appendix V – Preventive Maintenance Schedule, Corrective Maintenance Procedures and Resource Schedule, with clear indexing and page numbering for ease of reference.

Compliance: Failure to provide a complete, detailed, and properly referenced submission may result in the response being deemed non-responsive.

Reference in Document

5. Transition Plan

Transition Plan Requirements: Service Providers must submit a comprehensive transition plan that aligns with the requirements detailed in Annexure 1A. The plan must provide a clear and structured approach to ensure a seamless transition of services.

Mandatory Topics: The transition plan must address, at a minimum, the following key areas:

- Transition Organisation Structure: Outline the organisational framework for managing the transition.
- Key Roles and Responsibilities: Define the roles and responsibilities of key personnel involved in the transition process.
- Work Breakdown Structure: Provide a detailed breakdown of tasks and deliverables required for the transition.
- Communication Plan: Describe the strategy for effective communication with all stakeholders during the transition.
- Estimated Timetable: Include a realistic timeline for completing the transition, with key milestones.
- Documentation Schedule: Specify the schedule for delivering required documentation.
- Special Costs: Identify any additional or special costs associated with the transition.

Documentation Reference: Service Providers must clearly reference the sections and page numbers in their proposal where the transition plan is detailed, using the space provided below.

Documentation Submission: All supporting documentation for the transition plan must be compiled and submitted under Appendix W – Transition Plan, with clear indexing and page numbering for ease of reference.

Compliance: Failure to provide a complete, detailed, and properly referenced transition plan may result in the response being deemed non-responsive.

Reference in Document

6. Exit Plan

Exit Plan Requirements: Service Providers must submit a comprehensive exit plan that aligns with the requirements detailed in Annexure 1A. The plan must outline a structured and efficient approach to ensure a smooth termination or transition of services at the end of the contract period.

Mandatory Topics: The exit plan must address, at a minimum, the following key areas:

- Activities: Detail the specific activities required to facilitate an orderly exit.
- Key Roles and Responsibilities: Define the roles and responsibilities of key personnel involved in the exit process.
- Work Breakdown Structure: Provide a detailed breakdown of tasks and deliverables necessary for the exit.
- Communication Plan: Describe the strategy for effective communication with all stakeholders during the exit process.
- Estimated Timetable: Include a realistic timeline for completing the exit, with key milestones.
- Documentation Schedule: Specify the schedule for delivering required documentation, including any handover materials.
- Special Costs: Identify any additional or special costs associated with the exit process.

Documentation Reference: Service Providers must clearly reference the sections and page numbers in their proposal where the exit plan is detailed, using the space provided below.

Documentation Submission: All supporting documentation for the exit plan must be compiled and submitted under Appendix X – Exit Plan, with clear indexing and page numbering for ease of reference.

Compliance: Failure to provide a complete, detailed, and properly referenced exit plan may result in the response being deemed non-responsive.

Reference in Document

Annexure C
Pricing Workbo
Instructions

Pricing markup will be fixed for the duration of the contact.
USD influenced items can be adjusted with the Rate of exchange during the contract t
A fixed % mark-up for the duration of the contract will be in place per product type (or
Bidder Quotations can be added as additional information
Only Fill in Columns in Green
Use your own preventative maintenance plan as well as all the requirements in the SO
Use the Baseline Information in Scope of Work to scope the environment that needs t
Pricing will be fixed for the duration of the contact.
Pricing must include at least the minimum Resources as per Scope of Work
Only Fill in Columns in Green

ok

erm, accrding to the process and terms in the SOW
its equvalent replacement)
W (Annexure A) for determining the costs
o be maintained.

Exchange Rate 16.71

Annexure C
Pricing Summary

Area	Total Excluding VAT Y1	Total Excluding VAT Y2	Total Excluding VAT Y3	Total Excluding VAT Y4	Total Excluding VAT Y5	Total Excluding VAT	Total Including VAT
Total Maintenance - Software	R -	R -	R -	R -	R -	R -	R -
Total Maintenance - Hardware	R -	R -	R -	R -	R -	R -	R -
Total Maintenance - Access Switches	R -	R -	R -	R -	R -	R -	R -
Total Maintenance - Core Switches	R -	R -	R -	R -	R -	R -	R -
Total Maintenance - Security	R -	R -	R -	R -	R -	R -	R -
Total Maintenance - RiverBed WAN	R -	R -	R -	R -	R -	R -	R -
Total Maintenance - Telephone	R -	R -	R -	R -	R -	R -	R -
Total Maintenance - WLAN	R -	R -	R -	R -	R -	R -	R -
Monthly Fixed SLA	R -	R -	R -	R -	R -	R -	R -
Total Supply	R -	R -	R -	R -	R -	R -	R -
Tota Resourses - Fixed hours	R -	R -	R -	R -	R -	R -	R -
Total	R -	R -	R -	R -	R -	R -	R -

Annexure C
Summary Supply P

Notes:
This Annexure is for informational Purposes
The pricing below is derived from your detailed pricing submission
Please ensure the pricing totals here match up with your Total Offer for each work Package

Work Package Name	Total Excluding VAT	TOTAL Including VAT
WIFI Work Package Replacement Large Site Wlan controller	R -	R -
WIFI Work Package Replacement of Small site Wlan controller	R -	R -
WIFI Work Package Replacement of Low Spec Access Point	R -	R -
WIFI Work Package Replacement High Spec Access Point	R -	R -
WIFI Work Package Replacement of Outdoor Access Point with external OmiInternal Antennae	R -	R -
WIFI Work Package Replacement of Outdoor Access Point with Internal Antennae	R -	R -
Security Work Package Replacement of Small Site Firewalls	R -	R -
Security Work Package Replacement of Medium Site Firewalls	R -	R -
Security Work Package Replacement of Large Site Firewalls	R -	R -
Security Work Package Replacement of Centralised Firewall Manager	R -	R -
Security Work Package Replacement distributed Denial of Service Protector	R -	R -
Security Work Package Replacement of Existing Perimeter Firewall	R -	R -
Security Work Package Replacement of Existing Public WIFI Firewall	R -	R -
Security Work Package Replacement of Existing Web Proxy Solution	R -	R -
IPT Work Package - Supply and install telephone brackets to secure phones	R -	R -
IPT Work Package - Supply and install IP Telephones	R -	R -
IPT Work Package - Supply and install a high-spec server for the IP Telephony environment	R -	R -
IPT Work Package - Supply and install SIP Voice Gateways for IP Telephony environment	R -	R -
NETWORK Work Package - REPLACE ENTERPRISE ACCESS Switches	R -	R -
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	R -	R -
NETWORK Work Package - REPLACE 1U MPLS PE CORE SWITCHES	R -	R -
NETWORK Work Package - NTP SERVER APPLIANCES	R -	R -
NETWORK Work Package - REPLACE MODULAR MPLS CORE	R -	R -
NETWORK Work Package - REPLACE FIBRE DISTRIBUTION SWITCHES	R -	R -
NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs	R -	R -
NETWORK Work Package - UPGRADE OF SELECTED LINKS TO 25/40/100G	R -	R -
NETWORK Work Package - PHASED REPLACEMENT ENTERPRISE ACCESS SWITCHES	R -	R -
Total	R -	R -

Yes
No

Annexure C
Detailed Supply Pricing - OPTION1

WORK PACKAGE NAME	Site	Work Package Description	(A) 2027	(B) 2028	(C) 2029	(D) 2030	(E) 2031	Price influenced by USD Exchange rate (Yes/No)	(H) Base landed Price in USD For US sourced items	(I) ZAR Price (for local sourced items) Excluding VAT	(J) Exchange rate	(K) Total Landed Cost Y1 ((H*J)+I)*A	(L) Total Landed Cost Y2 ((H*J)+I)*B	(M) Total Landed Cost Y3 ((H*J)+I)*C	(N) Total Landed Cost Y4 ((H*J)+I)*D	(O) Total Landed Cost Y5 ((H*J)+I)*E	(R) Markup %	(S) Total Cost Excluding VAT (K+L+M+N+O+P+Q)*(1+R)	Comment
WIFI Work Package Replacement Large Site Wlan controller	JNB	Replacement of existing JNB C9800-40 Wlan controllers	0	0	0	0	2				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement Large Site Wlan controller	CPT	Replacement of existing CPT C9800-40 Wlan controllers	0	0	0	0	2				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement Large Site Wlan controller	DUR	Replacement of existing DUR C9800-40 Wlan controllers	0	0	0	0	2				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Small site Wlan controller	PLZ	Replacement of existing PLZ C9800-L Wlan controllers	0	0	0	0	2				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Low Spec Access Point	JNB	Replacement of existing AIR-AP1852i-E-K9 Access Points	32	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Low Spec Access Point	CPT	Replacement of existing AIR-AP1852i-E-K9 Access Points	65	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Low Spec Access Point	DUR	Replacement of existing AIR-AP1852i-E-K9 Access Points	27	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Low Spec Access Point	PLZ	Replacement of existing AIR-AP1852i-E-K9 Access Points	16	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Low Spec Access Point	ELS	Replacement of existing AIR-AP1852i-E-K9 Access Points	8	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Low Spec Access Point	GRJ	Replacement of existing AIR-AP1852i-E-K9 Access Points	7	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Low Spec Access Point	KIM	Replacement of existing AIR-AP1852i-E-K9 Access Points	5	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Low Spec Access Point	BFN	Replacement of existing AIR-AP1852i-E-K9 Access Points	9	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Low Spec Access Point	UTN	Replacement of existing AIR-AP1852i-E-K9 Access Points	3	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Low Spec Access Point	JNB	Replacement of existing C9115AXI-E Access Points	0	0	0	0	48				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Low Spec Access Point	CPT	Replacement of existing C9115AXI-E Access Points	0	0	0	0	15				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Low Spec Access Point	DUR	Replacement of existing C9115AXI-E Access Points	0	0	0	0	5				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	CPT	Replacement of existing AIR-AP2802E-E-K9 Access Points	0	7	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	JNB	Replacement of existing AIR-AP2802I-E-K9 Access Points	0	106	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	CPT	Replacement of existing AIR-AP2802I-E-K9 Access Points	0	76	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	DUR	Replacement of existing AIR-AP2802I-E-K9 Access Points	0	46	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	PLZ	Replacement of existing AIR-AP2802I-E-K9 Access Points	0	7	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	ELS	Replacement of existing AIR-AP2802I-E-K9 Access Points	0	16	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	GRJ	Replacement of existing AIR-AP2802I-E-K9 Access Points	0	19	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	KIM	Replacement of existing AIR-AP2802I-E-K9 Access Points	0	7	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	BFN	Replacement of existing AIR-AP2802I-E-K9 Access Points	0	16	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	UTN	Replacement of existing AIR-AP2802I-E-K9 Access Points	0	12	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	JNB	Replacement of existing AIR-AP3802E-E-K9 Access Points	0	56	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	JNB	Replacement of existing C9120AXI-E Access Points	0	0	215	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	CPT	Replacement of existing C9120AXI-E Access Points	0	0	48	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	DUR	Replacement of existing C9120AXI-E Access Points	0	0	18	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with external Omilnternal Antennae	CPT	Replacement of existing AIR-AP1572EAC-E-K9 Access Points	0	0	0	10	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with external Omilnternal Antennae	DUR	Replacement of existing AIR-AP1572EAC-E-K9 Access Points	0	0	0	20	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with external Omilnternal Antennae	PLZ	Replacement of existing AIR-AP1572EAC-E-K9 Access Points	0	0	0	5	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with external Omilnternal Antennae	JNB	Replacement of existing AIR-CAP1562E-E-K9 Access Points	0	23	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with external Omilnternal Antennae	CPT	Replacement of existing AIR-CAP1562E-E-K9 Access Points	0	6	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with external Omilnternal Antennae	DUR	Replacement of existing AIR-CAP1562E-E-K9 Access Points	0	22	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with external Omilnternal Antennae	PLZ	Replacement of existing AIR-CAP1562E-E-K9 Access Points	0	3	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with Internal Antennae	CPT	Replacement of existing AIR-CAP1562D-E-K9 Access Points	0	12	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with Internal Antennae	DUR	Replacement of existing AIR-CAP1562D-E-K9 Access Points	0	11	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with Internal Antennae	ELS	Replacement of existing AIR-CAP1562D-E-K9 Access Points	0	2	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with Internal Antennae	GRJ	Replacement of existing AIR-CAP1562D-E-K9 Access Points	0	4	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with Internal Antennae	KIM	Replacement of existing AIR-CAP1562D-E-K9 Access Points	0	1	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with Internal Antennae	BFN	Replacement of existing AIR-CAP1562D-E-K9 Access Points	0	1	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with Internal Antennae	JNB	Replacement of existing C9124AXI-E Access Points	0	0	0	10	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with Internal Antennae	CPT	Replacement of existing C9124AXI-E Access Points	0	0	0	1	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with Internal Antennae	PLZ	Replacement of existing C9124AXI-E Access Points	0	0	0	2	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with Internal Antennae	ELS	Replacement of existing C9124AXI-E Access Points	0	0	0	2	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with Internal Antennae	KIM	Replacement of existing C9124AXI-E Access Points	0	0	0	1	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement of Outdoor Access Point with external Omilnternal Antennae	JNB	Replacement of existing C9124AXE-ROW Access Points	0	0	0	8	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	JNB	Replacement of existing C9136I-ROW Access Points	0	0	0	50	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	JNB	Replacement of existing CW9164I-ROWAccess Points	0	0	0	0	214				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	CPT	Replacement of existing CW9164I-ROWAccess Points	0	0	0	0	100				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	DUR	Replacement of existing CW9164I-ROWAccess Points	0	0	0	0	60				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	PLZ	Replacement of existing CW9164I-ROWAccess Points	0	0	0	0	45				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	JNB	Increase capacity of existing Access Points	0	0	20	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	CPT	Increase capacity of existing Access Points	0	0	20	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	DUR	Increase capacity of existing Access Points	0	0	20	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	PLZ	Increase capacity of existing Access Points	0	0	15	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	ELS	Increase capacity of existing Access Points	0	0	10	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	GRJ	Increase capacity of existing Access Points	0	0	10	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	KIM	Increase capacity of existing Access Points	0	0	10	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	BFN	Increase capacity of existing Access Points	0	0	10	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
WIFI Work Package Replacement High Spec Access Point	UTN	Increase capacity of existing Access Points	0	0	10	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Small Site Firewalls	PLZ	Replacement of the existing CheckPoint Quantum Force 9100 Plus	0	0	0	2	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Small Site Firewalls	ELS	Replacement of the existing CheckPoint Quantum Force 9100 Plus	0	0	0	2	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Small Site Firewalls	GRJ	Replacement of the existing CheckPoint Quantum Force 9100 Plus	0	0	0	2	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Small Site Firewalls	KIM	Replacement of the existing CheckPoint Quantum Force 9100 Plus	0	0	0	2	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Small Site Firewalls	BFN	Replacement of the existing CheckPoint Quantum Force 9100 Plus	0	0	0	2	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Small Site Firewalls	UTN	Replacement of the existing CheckPoint Quantum Force 9100 Plus	0	0	0	2	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Medium Site Firewalls	CPT	Replacement of the existing CheckPoint Quantum 6600 Firewalls	2	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Medium Site Firewalls	DUR	Replacement of the existing CheckPoint Quantum 6600 Firewalls	2	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Large Site Firewalls	JNB	Replacement of the existing CheckPoint Quantum 7000 Firewalls	0	2	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Large Site Firewalls	JNB	Replacement of the existing CheckPoint Quantum 7000 Firewalls	0	0	0	1	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Centralised Firewall Manager	JNB	Replacement of the existing CheckPoint Checkpoint Smart -1 600-M	0	0	1	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement distributed Denial of Service Protector	JNB	Replacement of the existing Checkpoint Defence Pro 6-1	1	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Existing Perimeter Firewall	JNB	Replacement of the existing Cisco ASA 4500X	2	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Existing Public WIFI Firewall	JNB	Replacement of the existing Fortigate 100F	0	0	0	2	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Existing Web Proxy Solution	JNB	Replacement of the existing Cisco Web Secuirty Appliance solution	0	0	0	0	2				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Existing Web Proxy Solution	CPT	Replacement of the existing Cisco Web Security Appliance solution	0	0	0	0	2				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Existing Web Proxy Solution	DUR	Replacement of the existing Cisco Web Security Appliance solution	0	0	0	0	2				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Existing Web Proxy Solution	PLZ	Replacement of the existing Cisco Web Security Appliance solution	0	0	0	0	1				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Existing Web Proxy Solution	ELS	Replacement of the existing Cisco Web Security Appliance solution	0	0	0	0	1				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Existing Web Proxy Solution	GRJ	Replacement of the existing Cisco Web Security Appliance solution	0	0	0	0	1				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Existing Web Proxy Solution	KIM	Replacement of the existing Cisco Web Security Appliance solution	0	0	0	0	1				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Existing Web Proxy Solution	BFN	Replacement of the existing Cisco Web Security Appliance solution	0	0	0	0	1				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Security Work Package Replacement of Existing Web Proxy Solution	UTN	Replacement of the existing Cisco Web Security Appliance solution	0	0	0	0	1				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE ENTERPRISE ACCESS Switches	BFN	Enterprise-Grade 48-Port PoE+ Switch	3	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE ENTERPRISE ACCESS Switches	GRJ	Enterprise-Grade 48-Port PoE+ Switch	4	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE ENTERPRISE ACCESS Switches	UTN	Enterprise-Grade 48-Port PoE+ Switch	2	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE ENTERPRISE ACCESS Switches	JNB	Enterprise-Grade 48-Port PoE+ Switch	14	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE ENTERPRISE ACCESS Switches	DUR	Enterprise-Grade 48-Port PoE+ Switch	28	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE MODULAR MPLS CORE	JNB	4X C9606R Chassis with SUP2/2 and Assorted Line Cards	1	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE FIBRE DISTRIBUTION SWITCHES	JNB	Catalyst 9300X 12x25G Fiber Ports plus Network Module	0	6	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE FIBRE DISTRIBUTION SWITCHES	JNB	Catalyst 9300X 24x25G Fiber Ports	0	4	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE FIBRE DISTRIBUTION SWITCHES	PLZ	Catalyst 9300X 12x25G Fiber Ports plus Network Module	0	2	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE FIBRE DISTRIBUTION SWITCHES	DUR	Catalyst 9300X 12x25G Fiber Ports	0	3	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE FIBRE DISTRIBUTION SWITCHES	CPT	Catalyst 9300X 12x25G Fiber Ports plus Network Module	0	4	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE FIBRE DISTRIBUTION SWITCHES	CPT	Catalyst 9300X 24x25G Fiber Ports	0	2	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	UTN	Stackable 24 Port Enterprise Access Switch	4	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	UTN	Stackable 48 Port Enterprise Access Switch	2	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	KIM	Stackable 24 Port Enterprise Access Switch	2	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	KIM	Stackable 48 Port Enterprise Access Switch	3	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	BFN	Stackable 24 Port Enterprise Access Switch	4	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	BFN	Stackable 48 Port Enterprise Access Switch	3	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	ELS	Stackable 24 Port Enterprise Access Switch	14	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	ELS	Stackable 48 Port Enterprise Access Switch	3	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	GRJ	Stackable 24 Port Enterprise Access Switch	6	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	GRJ	Stackable 48 Port Enterprise Access Switch	4	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	PLZ	Stackable 24 Port Enterprise Access Switch	18	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	PLZ	Stackable 48 Port Enterprise Access Switch	8	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	DUR	Stackable 24 Port Enterprise Access Switch	0	24	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	DUR	Stackable 48 Port Enterprise Access Switch	0	15	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	CPT	Stackable 24 Port Enterprise Access Switch	0	0	146	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	CPT	Stackable 48 Port Enterprise Access Switch	0	0	32	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	JNB	Stackable 24 Port Enterprise Access Switch	0	302	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE BRANCH TYPE ACCESS Switches	JNB	Stackable 48 Port Enterprise Access Switch	0	44	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - REPLACE 1U MPLS PE CORE SWITCHES	JNB	Enterprise Grade 48 Port 1/10/25/40/100Gbps Core Switch	0	0	0	10	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - NTP SERVER APPLIANCES	JNB	Replacement of Network Time Server Appliance - SyncServer	2	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - NTP SERVER APPLIANCES	DUR	Replacement of Network Time Server Appliance - SyncServer	1	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - NTP SERVER APPLIANCES	CPT	Replacement of Network Time Server Appliance - SyncServer	1	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs	JNB	10G LR-S SFP	0	0	0	42	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs	JNB	10G LRM SFP	0	0	0	112	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs	CPT	10G LR-S SFP	0	0	0	36	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs	CPT	10G LRM SFP	0	0	0	64	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs	PLZ	10G LR-S SFP	0	0	0	12	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs	PLZ	10G LRM SFP	0	0	0	18	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs	ELS	10G LR-S SFP	0	0	0	8	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs	ELS	10G LRM SFP	0	0	0	12	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs	GRJ	10G LR-S SFP	0	0	0	8	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs	GRJ	10G LRM SFP	0	0	0	12	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs	BFN	10G LR-S SFP	0	0	0	4	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs	BFN	10G LRM SFP	0	0	0	12	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs	KIM	10G LR-S SFP	0	0	0	4	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs	KIM	10G LRM SFP	0	0	0	12	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED LINKS TO 25/40/100G	JNB	QSFP-100G-LR4-S=	0	0	32	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED LINKS TO 25/40/100G	JNB	SFP-10/25G-LR-S=	0	0	64	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED LINKS TO 25/40/100G	CPT	QSFP-100G-LR4-S=	0	0	0	16	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED LINKS TO 25/40/100G	CPT	SFP-10/25G-LR-S=	0	0	0	32	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED LINKS TO 25/40/100G	PLZ	QSFP-100G-LR4-S=	0	0	0	0	8				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED LINKS TO 25/40/100G	PLZ	SFP-10/25G-LR-S=	0	0	0	0	12				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED LINKS TO 25/40/100G	DUR	QSFP-100G-LR4-S=	0	0	0	0	16				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - UPGRADE OF SELECTED LINKS TO 25/40/100G	DUR	SFP-10/25G-LR-S=	0	0	0	0	32				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - PHASED REPLACEMENT ENTERPRISE ACCESS SWITCHES	JNB	Enterprise-Grade 24-Port PoE+ Switch	0	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - PHASED REPLACEMENT ENTERPRISE ACCESS SWITCHES	JNB	Enterprise-Grade 48-Port PoE+ Switch	0	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - PHASED REPLACEMENT ENTERPRISE ACCESS SWITCHES	CPT	Enterprise-Grade 24-Port PoE+ Switch	0	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - PHASED REPLACEMENT ENTERPRISE ACCESS SWITCHES	CPT	Enterprise-Grade 48-Port PoE+ Switch	0	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - PHASED REPLACEMENT ENTERPRISE ACCESS SWITCHES	DUR	Enterprise-Grade 24-Port PoE+ Switch	0	0	0	0	30				16.71	0.00	0.00	0.00	0.00	0.00		R -	
NETWORK Work Package - PHASED REPLACEMENT ENTERPRISE ACCESS SWITCHES	DUR	Enterprise-Grade 48-Port PoE+ Switch	0	0	0	0	20				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install telephone brackets to secure phones	All	Installation of new stainless steel 2mm IP Phone Brackets Desk / Wall Mount	1	1	1	1	1				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install IP Telephones	All	Installation of general office use IP telephones	0	0	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install a high-spec server for the IP Telephony environment	JNB	Installation of enterprize grade server for use in IP Telephony call control management.	1	0	0	1	4				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install a high-spec server for the IP Telephony environment	CPT	Installation of enterprize grade server for use in IP Telephony call control management.	1	1	0	0	3				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install a high-spec server for the IP Telephony environment	DUR	Installation of enterprize grade server for use in IP Telephony call control management.	1	1	0	0	3				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install a high-spec server for the IP Telephony environment	PLZ	Installation of enterprize grade server for use in IP Telephony call control management.	0	1	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install a high-spec server for the IP Telephony environment	ELS	Installation of enterprize grade server for use in IP Telephony call control management.	0	1	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install a high-spec server for the IP Telephony environment	GRJ	Installation of enterprize grade server for use in IP Telephony call control management.	0	1	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install a high-spec server for the IP Telephony environment	KIM	Installation of enterprize grade server for use in IP Telephony call control management.	0	1	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install a high-spec server for the IP Telephony environment	BFN	Installation of enterprize grade server for use in IP Telephony call control management.	0	1	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install a high-spec server for the IP Telephony environment	UTN	Installation of enterprize grade server for use in IP Telephony call control management.	0	1	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install SIP Voice Gateways for IP Telephony environment	JNB	Installation of enterprize grade voice gateway router for use in IP Telephony SIP call management.	0	2	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install SIP Voice Gateways for IP Telephony environment	CPT	Installation of enterprize grade voice gateway router for use in IP Telephony SIP call management.	0	2	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install SIP Voice Gateways for IP Telephony environment	DUR	Installation of enterprize grade voice gateway router for use in IP Telephony SIP call management.	0	2	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install SIP Voice Gateways for IP Telephony environment	PLZ	Installation of enterprize grade voice gateway router for use in IP Telephony SIP call management.	0	1	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install SIP Voice Gateways for IP Telephony environment	ELS	Installation of enterprize grade voice gateway router for use in IP Telephony SIP call management.	0	1	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install SIP Voice Gateways for IP Telephony environment	GRJ	Installation of enterprize grade voice gateway router for use in IP Telephony SIP call management.	0	1	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install SIP Voice Gateways for IP Telephony environment	KIM	Installation of enterprize grade voice gateway router for use in IP Telephony SIP call management.	0	1	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install SIP Voice Gateways for IP Telephony environment	BFN	Installation of enterprize grade voice gateway router for use in IP Telephony SIP call management.	0	1	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
IPT Work Package - Supply and install SIP Voice Gateways for IP Telephony environment	UTN	Installation of enterprize grade voice gateway router for use in IP Telephony SIP call management.	0	1	0	0	0				16.71	0.00	0.00	0.00	0.00	0.00		R -	
Total												R -	R -	R -	R -	R -		R -	

Annexure C
Monthly Preventative and SLA Maintenance Pricing

Notes:
Use your own preventative maintenance plan as well as all the requirements in the SOW (Annexure 1A) for determining the costs
Use the Baseline Information in Scope of Work to scope the environment that needs to be maintained.
Pricing will be fixed for the duration of the contact. - No further CPI increases
Pricing must include at least the minimum Resources as per Scope of Work
Only Fill in Columns in Green

Locations responsible for	Site	UOM	(A) Monthly Cost excluding Vat - Y1	(B) Monthly Cost excluding Vat - Y2	(C) Monthly Cost excluding Vat - Y3	(D) Monthly Cost excluding Vat - Y4	(E) Monthly Cost excluding Vat - Y5	(H) Qty - Y1	(I) Qty - Y2	(J) Qty - Y3	(K) Qty - Y4	(L) Qty - Y5	(O) Total Cost Excluding Vat - Y1 (A*H)	(P) Total Cost Excluding Vat - Y2 (B*I)	(Q) Total Cost Excluding Vat - Y3 (C*J)	(R) Total Cost Excluding Vat - Y4 (D*K)	(S) Total Cost Excluding Vat - Y5 (E*L)	(V) Total Cost Excluding VAT
Fixed Monthly Pricing to maintain the SLA as required In Scope of work including providing all the Reports and tasks as provided	JNB	Monthly						12	12	12	12	12	R -	R -	R -	R -	R -	R -
Fixed Monthly Pricing to maintain the SLA as required In Scope of work including providing all the Reports and tasks as provided	CPT	Monthly						12	12	12	12	12	R -	R -	R -	R -	R -	R -
Fixed Monthly Pricing to maintain the SLA as required In Scope of work including providing all the Reports and tasks as provided	DUR	Monthly						12	12	12	12	12	R -	R -	R -	R -	R -	R -
Fixed Monthly Pricing to maintain the SLA as required In Scope of work including providing all the Reports and tasks as provided	PLZ	Monthly						12	12	12	12	12	R -	R -	R -	R -	R -	R -
Fixed Monthly Pricing to maintain the SLA as required In Scope of work including providing all the Reports and tasks as provided	ELS	Monthly						12	12	12	12	12	R -	R -	R -	R -	R -	R -
Fixed Monthly Pricing to maintain the SLA as required In Scope of work including providing all the Reports and tasks as provided	GRJ	Monthly						12	12	12	12	12	R -	R -	R -	R -	R -	R -
Fixed Monthly Pricing to maintain the SLA as required In Scope of work including providing all the Reports and tasks as provided	BFN	Monthly						12	12	12	12	12	R -	R -	R -	R -	R -	R -
Fixed Monthly Pricing to maintain the SLA as required In Scope of work including providing all the Reports and tasks as provided	KIM	Monthly						12	12	12	12	12	R -	R -	R -	R -	R -	R -
Fixed Monthly Pricing to maintain the SLA as required In Scope of work including providing all the Reports and tasks as provided	UTN	Monthly						12	12	12	12	12	R -	R -	R -	R -	R -	R -
Total													**R -**	**R -**	**R -**	**R -**	**R -**	**R -**

Annexure C
Software Maintenance

Notes:
Pricing should covers parts, labour and travel
Only Fill in Columns in Green
Please engage the OEM for details if nessesary

OEM	Sites Deployed	Product ID	Description	(A) Qty of licences - Y1	(B) Qty of licences - Y2	(C) Qty of licences - Y3	(D) Qty of licences - Y4	(E) Qty of licences - Y5	(H) License fees Annual in USD (TOTAL) - Y1	(I) License fees Annual in USD (TOTAL) - Y2	(J) License fees Annual in USD (TOTAL) - Y3	(K) License fees Annual in USD (TOTAL) - Y4	(L) License fees Annual in USD (TOTAL) - Y5	(O) Exchange Rate	(P) TOTAL Excluding VAT (A*H*O) - Y1	(Q) TOTAL Excluding VAT (B*I*O) - Y2	(R) TOTAL Excluding VAT (C*J*O) - Y3	(S) TOTAL Excluding VAT (D*K*O) - Y4	(T) TOTAL Excluding VAT (E*L*O) - Y5	(W) TOTAL Excluding VAT	Comments
Cisco	Centralised licensing	SMA-WMGT-LIC	SMA Centralized Web Management Reporting License	2000	2000	2000	2000	2000						16.71	R -	R -	R -	R -	R -	R -	
Cisco	Centralised licensing	WSA-WSP-LIC=	Web Premium SW Bundle (WREP+WUC+AMAL) Licenses	2000	2000	2000	2000	2000						16.71	R -	R -	R -	R -	R -	R -	
Cisco	Centralised licensing	SVS-WEB-SUP-E	Enhanced Support for Web Security	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Cisco	Centralised licensing	Cisco Spaces ACT Cloud (1.0)	Cisco Spaces ACT Licenses	818	818	818	818	818						16.71	R -	R -	R -	R -	R -	R -	
Cisco	Centralised licensing	ISE Advantage	Identity Service Engine Advantage Licensing	3000	3000	3000	3000	3000						16.71	R -	R -	R -	R -	R -	R -	
Cisco	Centralised licensing	ISE Essentials	Identity Service Engine Essential Licensing	386	386	386	386	386						16.71	R -	R -	R -	R -	R -	R -	
Cisco	Centralised licensing	ISE VM	Identity Service VM Engine Licensing	5	5	5	5	5						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	JNB	CPSB-EVS-COMP-25-1Y	Checkpoint Firewall Manager License : SmartEvent, SmartReporter and Compliance bundle for	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	JNB	Co-Prem CPAP-NGSM600M	Checkpoint Firewall Manager Annual Maintenance 600M	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	JNB	CPSB-SNBT-7000-PLUS-1Y	Checkpoint Firewall License : 7000 Plus Next Generation Threat Prevention Appliance - Plus P	2	2	2	2	2						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	JNB	Co-Prem CPAP-SG7000-PLUS-SNBT	CheckPoint Firewall Annual Maintenance 7000 Plus Next Generation Threat Prevention Appli	2	2	2	2	2						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	JNB	Co-Prem MOB (U)	CheckPoint Mobile Access Blade (Unlimited)	2	2	2	2	2						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	JNB	CPSB-NETPRO-G-DPX-1G-1Y	DDoS Protector 6-1 Network Protection Subscription License	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	JNB	Co-Prem CPSB-Ddos 1G-1Y	Annual DDos Maintenance DDoS Protector 6-1 Appliance	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	CPT	CPSB-SNBT-6600-PLUS-1Y	Checkpoint Firewall License : 6600 Plus Next Generation Threat Prevention Appliance - Plus P	2	2	2	2	2						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	CPT	Co-Prem CPAP-SG6600-PLUS-SNBT	CheckPoint Firewall Annual Maintenance 6600 Plus Next Generation Threat Prevention Appli	2	2	2	2	2						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	CPT	Co-Prem MOB (U)	CheckPoint Mobile Access Blade (Unlimited)	2	2	2	2	2						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	DUR	CPSB-SNBT-6600-PLUS-1Y	Checkpoint Firewall License : 6600 Plus Next Generation Threat Prevention Appliance - Plus P	2	2	2	2	2						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	DUR	Co-Prem CPAP-SG6600-PLUS-SNBT	CheckPoint Firewall Annual Maintenance 6600 Plus Next Generation Threat Prevention Appli	2	2	2	2	2						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	DUR	Co-Prem MOB (U)	CheckPoint Mobile Access Blade (Unlimited)	2	2	2	2	2						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	PLZ	CPSB-SNBT-5400-PLUS-1Y	Checkpoint Firewall License : 5400 Plus Next Generation Threat Prevention Appliance - Plus P	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	PLZ	Co-Prem CPAP-SG5400	CheckPoint Firewall Annual Maintenance 5400 Plus Next Generation Threat Prevention Appli	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	PLZ	CPSB-SNBT-5400HA-PLUS-1Y	Checkpoint Firewall License : 5400HA Plus Next Generation Threat Prevention Appliance - Plu	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	PLZ	Co-Prem CPAP-SG5400HA	CheckPoint Firewall Annual Maintenance 5400HA Plus Next Generation Threat Prevention Ap	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	KIM	CPSB-SNBT-5400-PLUS-1Y	Checkpoint Firewall License : 5400 Plus Next Generation Threat Prevention Appliance - Plus P	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	KIM	Co-Prem CPAP-SG5400	CheckPoint Firewall Annual Maintenance 5400 Plus Next Generation Threat Prevention Appli	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	KIM	CPSB-SNBT-5400HA-PLUS-1Y	Checkpoint Firewall License : 5400HA Plus Next Generation Threat Prevention Appliance - Plu	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	KIM	Co-Prem CPAP-SG5400HA	CheckPoint Firewall Annual Maintenance 5400HA Plus Next Generation Threat Prevention Ap	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	ELS	CPSB-SNBT-5400-PLUS-1Y	Checkpoint Firewall License : 5400 Plus Next Generation Threat Prevention Appliance - Plus P	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	ELS	Co-Prem CPAP-SG5400	CheckPoint Firewall Annual Maintenance 5400 Plus Next Generation Threat Prevention Appli	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	ELS	CPSB-SNBT-5400HA-PLUS-1Y	Checkpoint Firewall License : 5400HA Plus Next Generation Threat Prevention Appliance - Plu	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	ELS	Co-Prem CPAP-SG5400HA	CheckPoint Firewall Annual Maintenance 5400HA Plus Next Generation Threat Prevention Ap	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	BFN	CPSB-SNBT-5400-PLUS-1Y	Checkpoint Firewall License : 5400 Plus Next Generation Threat Prevention Appliance - Plus P	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	BFN	Co-Prem CPAP-SG5400	CheckPoint Firewall Annual Maintenance 5400 Plus Next Generation Threat Prevention Appli	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	BFN	CPSB-SNBT-5400HA-PLUS-1Y	Checkpoint Firewall License : 5400HA Plus Next Generation Threat Prevention Appliance - Plu	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	BFN	Co-Prem CPAP-SG5400HA	CheckPoint Firewall Annual Maintenance 5400HA Plus Next Generation Threat Prevention Ap	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	GRJ	CPSB-SNBT-5400-PLUS-1Y	Checkpoint Firewall License : 5400 Plus Next Generation Threat Prevention Appliance - Plus P	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	GRJ	Co-Prem CPAP-SG5400	CheckPoint Firewall Annual Maintenance 5400 Plus Next Generation Threat Prevention Appli	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	GRJ	CPSB-SNBT-5400HA-PLUS-1Y	Checkpoint Firewall License : 5400HA Plus Next Generation Threat Prevention Appliance - Plu	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	GRJ	Co-Prem CPAP-SG5400HA	CheckPoint Firewall Annual Maintenance 5400HA Plus Next Generation Threat Prevention Ap	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	UTN	CPSB-SNBT-5400-PLUS-1Y	Checkpoint Firewall License : 5400 Plus Next Generation Threat Prevention Appliance - Plus P	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	UTN	Co-Prem CPAP-SG5400	CheckPoint Firewall Annual Maintenance 5400 Plus Next Generation Threat Prevention Appli	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	UTN	CPSB-SNBT-5400HA-PLUS-1Y	Checkpoint Firewall License : 5400HA Plus Next Generation Threat Prevention Appliance - Plu	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Checkpoint	UTN	Co-Prem CPAP-SG5400HA	CheckPoint Firewall Annual Maintenance 5400HA Plus Next Generation Threat Prevention Ap	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
3rd Party Voice	ORTIA, CTIA, DUR, COR	Maintenance (1 year) - 8x5x4	Libra Voice Recorder licenses for 3rd Party	3	4	4	4	4						16.71	R -	R -	R -	R -	R -	R -	
3rd Party Voice	ORTIA, CTIA, DUR, COR	2R-SUP-DW-1Y	2Ring Dashboard	3	4	4	4	4						16.71	R -	R -	R -	R -	R -	R -	
Cisco	ORTIA, CTIA, DUR, COR, KIM, UTN, GRJ, B	CCX Flex Premium Seat	Unified CM	14	14	14	14	14						16.71	R -	R -	R -	R -	R -	R -	
Cisco	ORTIA, CTIA, DUR, COR, KIM, UTN, GRJ, B	CCX Flex Standard Seat	Unified CM	126	126	126	126	126						16.71	R -	R -	R -	R -	R -	R -	
Cisco	ORTIA, CTIA, DUR, COR, KIM, UTN, GRJ, B	CCX Inbound Port-Flex	Unified CM	280	280	280	280	280						16.71	R -	R -	R -	R -	R -	R -	
Cisco	ORTIA, CTIA, DUR, COR, KIM, UTN, GRJ, B	CCX Outbound Port-Flex	Unified CM	140	140	140	140	140						16.71	R -	R -	R -	R -	R -	R -	
Cisco	ORTIA, CTIA, DUR, COR, KIM, UTN, GRJ, B	CCX Premium Server License	Unified CM	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Cisco	ORTIA, CTIA, DUR, COR, KIM, UTN, GRJ, B	CCX Premium Warm Standby	Unified CM	1	1	1	1	1						16.71	R -	R -	R -	R -	R -	R -	
Cisco	ORTIA, CTIA, DUR, COR, KIM, UTN, GRJ, B	Cisco Expressway Rich Media Session License	Unified CM	50	50	50	50	50						16.71	R -	R -	R -	R -	R -	R -	
Cisco	ORTIA, CTIA, DUR, COR, KIM, UTN, GRJ, B	CUBE Standard Trunk Session Subscription	Unified CM	240	240	240	240	240						16.71	R -	R -	R -	R -	R -	R -	
Cisco	ORTIA, CTIA, DUR, COR, KIM, UTN, GRJ, B	Emergency Responder User License	Unified CM	1910	1910	1910	1910	1910						16.71	R -	R -	R -	R -	R -	R -	
Cisco	ORTIA, CTIA, DUR, COR, KIM, UTN, GRJ, B	SRST Endpoint License Subscription	Unified CM	4310	4310	4310	4310	4310						16.71	R -	R -	R -	R -	R -	R -	
Cisco	ORTIA, CTIA, DUR, COR, KIM, UTN, GRJ, B	UC Manager Basic License	Unified CM	1210	1210	1210	1210	1210						16.71	R -	R -	R -	R -	R -	R -	
Cisco	ORTIA, CTIA, DUR, COR, KIM, UTN, GRJ, B	UC Manager CUWL License	Unified CM	300	300	300	300	300						16.71	R -	R -	R -	R -	R -	R -	
Cisco	ORTIA, CTIA, DUR, COR, KIM, UTN, GRJ, B	UC Manager Enhanced License	Unified CM	2775	2775	2775	2775	2775						16.71	R -	R -	R -	R -	R -	R -	

Notes:

Service level format is AxBxC, Where , A=Service Coverage hours per day, B= Service coverage days per week, C=Fix/Replace Time
Pricing should covers parts, labour and travel
Please engage the OEM for details if nessesary
A Letter of confirmation can be provided should it be nessesary for you to engage the OEM

Location	Device Name	Chassis Serial Number	Chassis Model Name	(A) Qty - Y1	(B) Qty - Y2	(C) Qty - Y3	(D) Qty - Y4	(E) Qty - Y5	(H) Required Service Level for Preventative mantenance	(I) Required Service Level for OEM Backed Hardware Maintenance	(J) USD PRICE Annual Partner Support Service (1 Year) Chassis Plus Modules - according to HW service level (I) Y1
JNB	JNB-40-CR1-R1C2-01	FDO22282Q6A	N9K-C93108TC-EX	1	1	1	1	0	24x7x4	24x7x4	
JNB	JNB-40-DC-R1C1-01	FDO22281BVZ	N9K-C93108TC-EX	1	1	1	1	0	24x7x4	24x7x4	
JNB	JNB-68-CR1-R2C1A-01	FDO222937T7	N9K-C93180YC-FX	1	1	1	1	0	24x7x4	24x7x4	
JNB	JNB-40-DC-R1C1-03	FDO222937XH	N9K-C93180YC-FX	1	1	1	1	0	24x7x4	24x7x4	
JNB	JNB-68-DC-R1C1-02	FDO222917X4	N9K-C93180YC-FX	1	1	1	1	0	24x7x4	24x7x4	
JNB	JNB-40-CR1-R2C1A-02	FDO2230038D	N9K-C93180YC-FX	1	1	1	1	0	24x7x4	24x7x4	

Notes:

Service level format is AxBxC, Where , A=Service Coverage hours per day, B= Service coverage days per week, C=Fix/Repla
Pricing should covers parts, labour and travel
Please engage the OEM for details if nessesary
A Letter of confirmation can be provided should it be nessesary for you to engage the OEM

Location	Device Name	Chassis Serial Number	Chassis Model Name	(A) Qty - Y1	(B) Qty - Y2	(C) Qty - Y3	(D) Qty - Y4
BFN	BFN-APR-CAB1-1	JAE26370ZU6	C9200-24P	1	1	1	1
BFN	BFN-MNE-ENV1-1	JAE2637118J	C9200-24P	1	1	1	1
BFN	BFN-PERMIT-CAB1-1	FOC26436A2V	C9200-24P	1	1	1	1
CPT	CIA-BRV-CCTV-H1	JAE26360RSL	C9200-24P	1	1	1	1
CPT	CIA-BRV-CCTV-H2	JAE26360RSR	C9200-24P	1	1	1	1
CPT	CIA-BRV-CCTV-H3	JAE26360RTD	C9200-24P	1	1	1	1
CPT	CIA-BRV-CCTV-H4	FOC28020ZU8	C9200-24P	1	1	1	1
CPT	CIA-BRV-CCTV-H5	FOC280213TK	C9200-24P	1	1	1	1
CPT	CIA-BRV-CCTV-H6	FOC28020ZTF	C9200-24P	1	1	1	1
CPT	CIA-DC-RACK16-CTBX-SW1	JAE26360RGQ	C9200-24P	1	1	1	1
CPT	CIA-DC-RACK16-INTX-SW3	FOC2802140W	C9200-24P	1	1	1	1
CPT	CIA-DC-RACK5-CTBX-SW1	JAE26360RNG	C9200-24P	1	1	1	1
CPT	CIA-DC-RACK5-INTX-SW3	JAE26360RHB	C9200-24P	1	1	1	1
CPT	CIA-F12A-CCTV-SW1	FOC264307J6	C9200-24P	1	1	1	1
CPT	CIA-F12-CCTV-SW1	FOC28020ZSQ	C9200-24P	1	1	1	1
CPT	CIA-F3A-CCTV-SW1	FOC280213YD	C9200-24P	1	1	1	1
CPT	CIA-F3-CCTV-SW1	FOC28020ZTY	C9200-24P	1	1	1	1
CPT	CIA-F5-CCTV-SW1	FOC28020ZSR	C9200-24P	1	1	1	1
CPT	CIA-H10-CCTV-SW1	FOC28020ZRT	C9200-24P	1	1	1	1
CPT	CIA-INT-P4P5-PARK	JAE26360RHJ	C9200-24P	1	1	1	1
CPT	CIA-INT-P4P5PARK-CAB1-1	FOC28020ZB7	C9200-24P	1	1	1	1
CPT	CIA-INT-WC3-CAB3-STACK1	JAE26360R4Z	C9200-24P	1	1	1	1
CPT	CIA-INT-WC3-CAB3-STACK1	JAE26360R4Y	C9200-24P	1	1	1	1
CPT	CIA-INT-WC5-CUTE-CAB5-STACK1	JAE26360RMU	C9200-24P	1	1	1	1
CPT	CIA-MSP1-WC0-ARCHIVE1-CUTE-SW1	FOC28020ZPY	C9200-24P	1	1	1	1
CPT	CIA-MSP1-WC2-CUTE-SW1	FOC280213WU	C9200-24P	1	1	1	1
CPT	CIA-NWC-Entry-CCTV-STACK1	JAE26360RMK	C9200-24P	1	1	1	1
CPT	CIA-NWC-Exit-CCTV-SW1	JAE26360RGR	C9200-24P	1	1	1	1
CPT	CIA-SOB-CR1-CAB5-STACK1	JAE26360RAB	C9200-24P	1	1	1	1
CPT	CIA-SOB-WC14-CAB1-1	FOC28020ZBN	C9200-24P	1	1	1	1
DUR	DUR-BirdRadar	JAE26360QQ2	C9200-24P	1	1	1	1
DUR	DUR-CUTE-MSO-WC02-CAB2-2	FVH28300X8W	C9200-24P	1	1	1	1

Location	Device Name	Chassis Serial Number	Chassis Model Name	(A) Qty - Y1	(B) Qty - Y2	(C) Qty - Y3	(D) Qty - Y4
DUR	DUR-CUTE-MSP-WC02-CAB2-2	FVH28300XD3	C9200-24P	1	1	1	1
DUR	DUR-CUTE-TMB-CC02-CAB1-1	FVH28300X80	C9200-24P	1	1	1	1
DUR	DUR-CUTE-TMB-CC03-CAB1-1	FVH28300XAJ	C9200-24P	1	1	1	1
DUR	DUR-CUTE-TMB-CC04-CAB1-1	FVH28300X8D	C9200-24P	1	1	1	1
DUR	DUR-CUTE-TMB-CC05-CAB1-1	FVH28300XAG	C9200-24P	1	1	1	1
DUR	DUR-CUTE-TMB-WC10-CAB1-1	FVH28300XA4	C9200-24P	1	1	1	1
DUR	DUR-CUTE-TMB-WC10-CAB1-1	FVH28300X9A	C9200-24P	1	1	1	1
DUR	DUR-CUTE-TMB-WC13-CAB1-1	FVH28300X8S	C9200-24P	1	1	1	1
DUR	DUR-CUTE-TMB-WC13-CAB1-1	FVH28300XC5	C9200-24P	1	1	1	1
DUR	DUR-CUTE-TMB-WC16-CAB1-1	FVH28300XC3	C9200-24P	1	1	1	1
DUR	DUR-CUTE-TMB-WC17-CAB1-1	FVH28300XBQ	C9200-24P	1	1	1	1
DUR	DUR-CUTE-TMB-WC18-CAB1-1	FVH28300X7R	C9200-24P	1	1	1	1
DUR	DUR-CUTE-TMB-WC20-CAB1-1	FVH28300XA5	C9200-24P	1	1	1	1
DUR	DUR-CUTE-TMB-WC21-CAB1-1	FVH28300X8G	C9200-24P	1	1	1	1
DUR	DUR-CUTE-TMB-WC22-CAB1-1	FVH28300XC2	C9200-24P	1	1	1	1
DUR	DUR-CUTE-TMB-WC23-CAB1-1	FVH28300X8X	C9200-24P	1	1	1	1
DUR	DUR-DOZ-WC01-CAB1	JAE26360RPY	C9200-24P	1	1	1	1
DUR	DUR-FFD-WC02-CAB1	JAE26360R12	C9200-24P	1	1	1	1
DUR	DUR-MSO-PRK-CC01	JAE26360RB9	C9200-24P	1	1	1	1
DUR	DUR-MSP-CC01-CAB1	JAE26360RCH	C9200-24P	1	1	1	1

Annexure C
Hardware Maintenance Core Switches

Notes:
Service level format is AxBxC, Where , A=Service Coverage hours per day, B= Service coverage days per week, C=Fix/Replace Time
Pricing should covers parts, labour and travel
Please engage the OEM for details if nessesary
A Letter of confirmation can be provided should it be nessesary for you to engage the OEM

Location	Device Name	Chassis Serial Number	Chassis Model Name	(A) Qty - Y1	(B) Qty - Y2	(C) Qty - Y3	(D) Qty - Y4	(E) Qty - Y5	(H) Required Service Level for Preventative mantenance	(I) Required Service Level for OEM Backed Hardware Maintenance	(J) USD PRICE Annual Partner Support Service (1 Year) Chassis Plus Modules - according to HW service level (I) Y1	(K) USD PRICE Annual Partner Support Service (1 Year) Chassis Plus Modules - according to HW service level (I) Y2	(L) USD PRICE Annual Partner Support Service (1 Year) Chassis Plus Modules - according to HW service level (I) Y3	(M) USD PRICE Annual Partner Support Service (1 Year) Chassis Plus Modules - according to HW service level (I) Y4	(N) USD PRICE Annual Partner Support Service (1 Year) Chassis Plus Modules - according to HW service level (I) Y5	(Q) Exchange Rate	(R) Monthly Maintenance according to Service Level (H) - Y1	(S) Monthly Maintenance according to Service Level (H) - Y2	(T) Monthly Maintenance according to Service Level (H) - Y3	(U) Monthly Maintenance according to Service Level (H) - Y4	(V) Monthly Maintenance according to Service Level (H) - Y5	(Y) TOTAL Excluding VAT - Y1 ((A*J)*Q)+((A*R)*12))	(Z) TOTAL Excluding VAT - Y2 ((B*K)*Q)+((B*S)*12))	AA) TOTAL Excluding VAT - Y3 ((C*L)*Q)+((C*T)*12))	(AB) TOTAL Excluding VAT - Y4 ((D*M)*Q)+((D*U)*12))	(AC) TOTAL Excluding VAT - Y5 ((E*N*Q)+((E*V)*12))	(AF) TOTAL Excluding VAT	Comments
CPT	CIA-CTB-CR3-PE2	TBC - NEW	C9606R	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-TA-CR1-R2C6-PE1	TBC - NEW	C9606R	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
CPT	CIA-DC-RACK1-PE1	TBC - NEW	C9606R	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-TA-WC8-R1C1-2-PE4	TBC - NEW	C9606R	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-TA-WC8-R1C1-1-PE2	TBC - NEW	C9606R	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-TB-CR3-R2C8-PE3	TBC - NEW	C9606R	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
CPT	CIA-CTB-CR3-PE12	TBC - NEW	C9606R	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
CPT	CIA-CPU-CR4-PE13	TBC - NEW	C9606R	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-TMB-CR2-R2-CAB3-SFM2	TBC - NEW	C9500-24Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-TMB-CR1-R2-CAB2-PE1	TBC - NEW	C9606R	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-TMB-CR1-R2-CAB3-SFM1	TBC - NEW	C9500-24Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-TMB-CR2-R2-CAB2-PE2	TBC - NEW	C9606R	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-TMB1-CR1-R2-CAB4-SFM3	TBC - NEW	C9300-48T-E	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-TMB1-CR1-R2-CAB4-SFM3	TBC - NEW	C9300-48T-E	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-TMB1-CR1-R2-CAB4-SFM3	TBC - NEW	C9300-48T-E	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-TMB1-CR1-R2-CAB4-SFM3	TBC - NEW	C9300-48T-E	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-TMB1-CR1-R2-CAB4-SFM3	TBC - NEW	C9300-48T-E	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-TMB1-CR1-R2-CAB4-SFM3	TBC - NEW	C9300-48T-E	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-TA-DC1-R2C4-P2	FGE20491C6K	C6807-XL	1	0	0	0	0	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-TA-CR1-PE24	FGE20491C9Y	C6807-XL	1	0	0	0	0	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-TA-CR1-R1C1-P1	SMC1839002Z	C6807-XL	1	0	0	0	0	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-DC-CR2-PE25	FGE20491CDL	C6807-XL	1	0	0	0	0	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
CPT	CIA-DC-RACK19-PE15	FDO281302D9	C9500-24Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
CPT	CIA-CTB-CR3DC-PE14	FDO281302BF	C9500-24Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-TMB-CR1-R2-CAB1-P1	FDO281301XG	C9500-24Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-TMB-CR2-R2-CAB1-P2	FDO281300LV	C9500-24Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-MB2-WC1-R1-CAB1-PE2	FDO281300TG	C9500-24Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-MB1-WC1-R1-CAB1-PE1	FDO281300UB	C9500-24Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
UTN	UTN-CR1-CAB1-PE1	FDO28470HC0	C9500-24Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
KIM	KIM-CR1-CAB6-PE1	FDO28470BU1	C9500-24Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
UTN	UTN-CR1-CAB1-PE2	FDO28470HDP	C9500-24Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
KIM	KIM-CR1-CAB6-PE2	FDO28470HEF	C9500-24Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
BFN	BFN-CR1-CAB1-PE1	FDO28470BV9	C9500-24Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
BFN	BFN-CR1-CAB1-PE2	FDO28470HC7	C9500-24Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-CUTE-CR2-PE14	FDO28470HBQ	C9500-24Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-CUTE-CR1-PE13	FDO28470HEL	C9500-24Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-NP-IPA5-CAB1-PE14	FCW2236A1SW	C9500-40X	1	1	1	1	0	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-A1A2-CR2-CAB3-PE21	FCW2214A10U	C9500-40X	1	1	1	1	0	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-A1A2-CR2-CAB3-PE23	FCW2236A3T1	C9500-40X	1	1	1	1	0	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-WP-ICC-TELCO-B-PE27	FCW2204A4GR	C9500-40X	1	1	1	1	0	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-A1A2-CR1-CAB1-PE20	FCW2228A4D8	C9500-40X	1	1	1	1	0	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-NP-IPA4-CAB1-PE15	FCW2231A56C	C9500-40X	1	1	1	1	0	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-WP-ICC-TELCO-A-PE26	FCW2204A38T	C9500-40X	1	1	1	1	0	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-A1A2-CR1-CAB1-PE22	FCW2237A0BU	C9500-40X	1	1	1	1	0	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-WP-BAS01-TA-PE1	FOC2551Y0ZC	C9500-40X	1	1	1	1	0	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-WP-BAS01-TB-PE2	FOC2550YHSP	C9500-40X	1	1	1	1	0	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-MSP-WC34-R1C5-PE13	FDO281213P6	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-MSP-CR01-CAB1-PE12	FDO28120TF0	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
CPT	CIA-CTB-CR3-P2	FDO281213NG	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
CPT	CIA-SOB-CR1-P1	FDO28120TL7	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
PLZ	PLZ-CR1-CAB1-PE1	FDO281213MD	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
PLZ	PLZ-CR2-CAB1-PE2	FDO28120TLG	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-MSP-WC6-R1-CAB1-PE2	FDO281213T4	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
DUR	DUR-MSP-WC2-R1-CAB1-PE1	FDO281213TV	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-CTB-CR1-CAB4-PE1	FDO28470TP1	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-CTB-CR1-CAB5-PE18	FDO28470Z1N	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-CTB-CR2-CAB4-PE2	FDO28470Z1V	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNB-CTB-CR2-CAB3-PE19	FDO28470Z0B	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
CPT	CIA-CTB-CR3-PE4	FDO28470HWB	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
CPT	CIA-INT-CR2-PE3	FDO28470HYA	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
ELS	ELS-CR1-CAB3-PE1	FDO2845113Z	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
GRJ	GRJ-CR1-CAB2-PE1	FDO28470HY0	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
GRJ	GRJ-CR1-CAB2-PE2	FDO28470HY1	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
ELS	ELS-WC1-CAB3-PE2	FDO28460GWC	C9500-48Y4C	1	1	1	1	1	24x7x4	24x7x4						16.71						R -	R -	R -	R -	R -	R -	
Total																						**R -**	**R -**	**R -**	**R -**	**R -**	**R -**	

Notes:
Service level format is AxBxC, Where , A=Service Coverage hours per day, B= Service coverage days per week, C=Fix/Replace Time
Pricing should covers parts, labour and travel
Please engage the OEM for details if nessesary
A Letter of confirmation can be provided should it be nessesary for you to engage the OEM

Location	Device Name	Chassis Serial Number	Chassis Model Name	(A) Qty - Y1	(B) Qty - Y2	(C) Qty - Y3	(D) Qty - Y4
JNB	JNBVMFWMGMT01	HZ8WTX3	Checkpoint Smart -1 600-M Firewall Manager	1	1	1	1
JNB	JNBCR1FW01	2239BA2619	Checkpoint 7000 Firewall	1	1	1	1
JNB	JNBCR3FW02	2239BA2620	Checkpoint 7000 Firewall	1	1	1	1

Annexure C
Hardware Maintenance Riverbed WAN

Notes:
Service level format is AxBxC, Where , A=Service Coverage hours per day, B= Servic
Pricing should covers parts, labour and travel
Please engage the OEM for details if nessesary
A Letter of confirmation can be provided should it be nessesary for you to engage the OEM

Location	Device Name	Chassis Serial Number	Chassis Model Name	(A) Qty - Y1	(B) Qty - Y2	(C) Qty - Y3	(D) Qty - Y4	(E) Qty - Y5	(H) Required Service Level for Preventative maintenance	(I) Required Service Level for OEM Backed Hardware Maintenance	(J) USD PRICE Annual Partner Support Service (1 Year) Chassis Plus Modules - according to HW service level (I) Y1	(K) USD PRICE Annual Partner Support Service (1 Year) Chassis Plus Modules - according to HW service level (I) Y2	(L) USD PRICE Annual Partner Support Service (1 Year) Chassis Plus Modules - according to HW service level (I) Y3	(M) USD PRICE Annual Partner Support Service (1 Year) Chassis Plus Modules - according to HW service level (I) Y4	(N) USD PRICE Annual Partner Support Service (1 Year) Chassis Plus Modules - according to HW service level (I) Y5	(Q) Exchange Rate	(R) Monthly Maintenance according to Service Level (H) - Y1	(S) Monthly Maintenance according to Service Level (H) - Y2	(T) Monthly Maintenance according to Service Level (H) - Y3	(U) Monthly Maintenance according to Service Level (H) - Y4	(V) Monthly Maintenance according to Service Level (H) - Y5	(Y) TOTAL Excluding VAT - Y1 ((A*J)+(Q+(A*R)*12))	(Z) TOTAL Excluding VAT - Y2 ((B*K)+(Q+(B*S)*12))	(AA) TOTAL Excluding VAT - Y3 ((C*L)+(Q+(C*T)*12))	(AB) TOTAL Excluding VAT - Y4 ((D*M)+(Q+((D*U)*12)))	(AC) TOTAL Excluding VAT - Y5 ((E*N)+(Q+((E*V)*12)))	(AF) TOTAL Excluding VAT	Comments
JNB	jnbsacr2r1c7ucc	ESCT2003F5741	SCC-01005-BASE SteelCentral Controller 1000	1	1	1	0	0	24X7X4	Gold						16.71						R -	R -	R -	R -	R -	R -	
JNB	JNBCR1EVP01	LE18P001C8D37	SCNE-00470-BB9339E SteelCentral NetExpress 4	1	1	1	0	0	24X7X8	Silver						16.71						R -	R -	R -	R -	R -	R -	
DUR	durtmbcr1r2	LDBVN000F9A4B	CXA-03070-B110 SteelHead CX 3070	1	1	1	0	0	8X5XNBD	Silver						16.71						R -	R -	R -	R -	R -	R -	
DUR	durtmbcr2r1	LDBVJ000F9A01	CXA-03070-B110 SteelHead CX 3070	1	1	1	0	0	8X5XNBD	Silver						16.71						R -	R -	R -	R -	R -	R -	
JNB	jnbbcr3r2c4	LDCNY000F9ABE	CXA-03070-B110 SteelHead CX 3070	1	1	1	0	0	8X5XNBD	Silver						16.71						R -	R -	R -	R -	R -	R -	
JNB	jnbsacr2r1c7	LDCKX000F9A91	CXA-03070-B110 SteelHead CX 3070	1	1	1	0	0	8X5XNBD	Silver						16.71						R -	R -	R -	R -	R -	R -	
GRJ	gtjcr1cab2	ECTKQ000F6ED4	CXA-00770-B120 SteelHead CX 770	1	1	1	0	0	8X5XNBD	Silver						16.71						R -	R -	R -	R -	R -	R -	
PLZ	plzcr1cab3	ECTX3000F7A33	CXA-00770-B120 SteelHead CX 770	1	1	1	0	0	8X5XNBD	Silver						16.71						R -	R -	R -	R -	R -	R -	
ELS	elscr1cab3	ECTKQ000F79A7	CXA-00770-B120 SteelHead CX 770	1	1	1	0	0	8X5XNBD	Silver						16.71						R -	R -	R -	R -	R -	R -	
BFN	bfncr1cab1	ECTXW000F7A21	CXA-00770-B120 SteelHead CX 770	1	1	1	0	0	8X5XNBD	Silver						16.71						R -	R -	R -	R -	R -	R -	
KIM	kimtacr1cab6	ECTMG000F7B08	CXA-00770-B120 SteelHead CX 770	1	1	1	0	0	8X5XNBD	Silver						16.71						R -	R -	R -	R -	R -	R -	
ELS	elswcr1cab3	ECTWV000F7666	CXA-00770-B120 SteelHead CX 770	1	1	1	0	0	8X5XNBD	Silver						16.71						R -	R -	R -	R -	R -	R -	
UTN	utncr1cab3	ECTUU000F6D03	CXA-00770-B120 SteelHead CX 770	1	1	1	0	0	8X5XNBD	Silver						16.71						R -	R -	R -	R -	R -	R -	
PLZ	plzcr2cab1	ECTWR000F79E3	CXA-00770-B120 SteelHead CX 770	1	1	1	0	0	8X5XNBD	Silver						16.71						R -	R -	R -	R -	R -	R -	
Total																						R -	R -	R -	R -	R -	R -	

Notes:

Service level format is AxBxC, Where , A=Service Coverage hours per day, B= Service coverage days per week, C=Fix/Replace Time
Pricing should covers parts, labour and travel
Please engage the OEM for details if nessesary
A Letter of confirmation can be provided should it be nessesary for you to engage the OEM

Location	Device Name	Chassis Serial Number	Chassis Model Name	(A) Qty - Y1	(B) Qty - Y2

Notes:

Service level format is AxBxC, Where , A=Service Coverage hours per day, B= Service coverage days per week, C=Fix/Replace Time
Pricing should covers parts, labour and travel
Please engage the OEM for details if nessesary
A Letter of confirmation can be provided should it be nessesary for you to engage the OEM

Location	Device Name	Chassis Serial Number	Chassis Model Name	(A) Qty - FY27	(B) Qty - Y2	(C) Qty - Y3	(D) Qty - Y4

Annexure C
Hardware Maintenance Data

Notes:

Service level format is AxBxC, Where , A=Service Coverage hours per day, B= Service coverage days per
Pricing should covers parts, labour and travel
Please engage the OEM for details if nessesary
A Letter of confirmation can be provided should it be nessesary for you to engage the OEM

Location	Resourse	(A) Qty - Y1	(B) Qty - Y2	(C) Qty - Y3	(D) Qty - Y4	(E) Qty - Y5
All	CCIE - Routing and Switching	50	50	50	50	50
All	CCIE - Wireless	50	50	50	50	50

Annexure C
Resource Hourly Rates

Notes:
Pricing will be fixed for the duration of the contact.

		Year 1			Year 2			Year 3			Year 4			Year 5		
Resouce Certification Level / Purpose	OEM	Business Hours Hourly Rate - Y1	After Hours Hourly Rate - Y1	Weekend and Public Holidays Hourly Rate - Y1	Business Hours Hourly Rate - Y2	After Hours Hourly Rate - Y2	Weekend and Public Holidays Hourly Rate - Y2	Business Hours Hourly Rate - Y3	After Hours Hourly Rate - Y3	Weekend and Public Holidays Hourly Rate - Y3	Business Hours Hourly Rate - Y4	After Hours Hourly Rate - Y4	Weekend and Public Holidays Hourly Rate - Y4	Business Hours Hourly Rate - Y5	After Hours Hourly Rate - Y5	Weekend and Public Holidays Hourly Rate - Y5
CCIE - Routing and Switching	Cisco	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
CCIE - Collaboration	Cisco	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
CCIE - Service Provider	Cisco	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
CCIE - Wireless	Cisco	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
CCIE - Data Centre	Cisco	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
CCNP - Routing and Switching	Cisco	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
CCNP - Wireless	Cisco	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
CCNP - Collaboration	Cisco	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
CCNP - Data Centre	Cisco	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
CCCNP - Routing and Switching	Cisco	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
CCNA - Wireless	Cisco	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
CCNA - Collaboration	Cisco	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
CCNA - Industrial	Cisco	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
Voice Communications Administrator	NA	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
Wireless Communications Administrator	NA	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
Riverbed RIOS 2nd line technician	Riverbed	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
Riverbed RIOS 3rd line technician	Riverbed	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
Checkpoint Certified Security Expert	Checkpoint	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
Checkpoint Certified Security Associate	Checkpoint	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
HCIE - Datacom	Huawei	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
HCIE - WLAN	Huawei	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -
HCIA - Datacom	Huawei	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -	R -

MANDATORY REQUIREMENTS – LAN WAN WLAN IPT

TENDER NUMBER: xxx/2025/RFP

		Compliant?	
	Mandatory Requirements Evaluation	**Yes**	**No**
1.	Bidders must provide an OEM Certification/Accreditation letter for all the OEM equipment being supported and supplied. The certification must be in place for at least 24 consecutive months and be current. **Requirement: The bidder must provide valid and verifiable evidence of their current OEM Certification/Accreditation that covers a 24-month consecutive period. If multiple OEMs are used in the bid, all must be provided.**		
	Compliant?		

Annexure E – Work package specifications

For

LAN / Wireless / IP Telephony and Network Security Services

Description:

Specifications for the Work Packages related to the Supply, Installation, Commissioning, Support and Maintenance of IT Network, IP Telephony and IT Security Infrastructure Services for a period of 60 Months to Airports Company South Africa

Contents

General Notes

Please take special note of the following items that are applicable to all Work packages.

- **OEM Warranty –**
    - All hardware must be supplied with a 5-year OEM warranty and software with at least next business day replacement, this includes any software for the device to function. Some Work packages have other requirements and should be catered for accordingly.

- **Interoperability –**
    - Any OEM can be used to fulfil any work package as long as FULL interoperability is guaranteed within the existing environment.
    - Efforts are made to describe the current environment for all work packages. Please read this information carefully.
    - The bidder can also include the replacement of the up and downstream devices should they wish/need to provide the guarantee.
    - Note that some switches are in a “stack” and are required to remain in the stack configuration due to limitations on uplink fibre capacity.

- **Management –**
    - All supplied devices must be fully managed.
    - Please refer to the currently deployed management software components as per Annexture A – Section 2: Service environment to determine if the proposed hardware will be able to be managed by the in place management system
    - Should it be needed, the additional management platform must be costed as part of the work package or added to the “Other cost” tab in Annexture C (pricing file)

- **Monitoring –**
    - All supplied devices must be fully monitored.
    - Please refer to the currently deployed monitoring software components as per Annexure A – Section 2: Service environment to determine if the proposed hardware will be able to be monitored by the in place monitoring system
    - Should it be needed, the additional monitoring platform must be costed as part of the work package or added to the “Other cost” tab in Annexure C (pricing file)

- **Support –**
    - Any proposed OEMs must be fully supported by the bidder using OEM certified staff at the equivalent requested certification levels.

- **Wi-Fi roaming –**
    - In the case of Wi-Fi devices, the provider must fully guarantee seamless, near-zero loss to clients while roaming between network segments at each site, should a mix of OEM equipment be proposed.

- **IP Telephony**
    - The solution must integrate with existing Cisco Unified Communications Manager (CUCM) version 11.5 or higher, Unity Connection, and Contact Centre platforms.

1.0 WIFI Work Package - Replacement High Spec Access Point

Supply, physically install and configure WIFI Access points that meet enterprise-grade Wi-Fi 6E or latest equivalent standards to replace existing devices that have reached end of life.

The high specification devices for dense areas must have the following features:

- Tri-band Wi-Fi 6E (2.4 GHz, 5 GHz, 6 GHz)
- 4x4 MIMO for high throughput and user density
- Advanced RF management (band steering, interference mitigation)
- Enterprise security (WPA3, secure boot)
- IoT-ready architecture
- Centralised management (cloud/on-prem support)
- Must include all required licenses for full feature activation (connectivity, analytics, location services)
- Include OEM hardware warranty for a period of 5 years, with Next Business Day (NBD) replacement.
- The devices must either be supported by the existing WLAN controllers or separate controllers can be supplied; however, there needs to be seamless roaming between new and existing APs, ensuring no degradation in connectivity or user experience.
- Support for ACSA Wi-Fi portal, or provision of a suitable replacement captive portal with equivalent functionality
- Include decommissioning of existing EOL infrastructure, documentation, asset tagging and validation testing and commissioning of new infrastructure
- Installation should cater for all equipment required for installation at heights, including Skyjacks where required.

2.0 WIFI Work Package - Replacement of Low Spec Access Point

Supply, physically install and configure WIFI Access points that meet enterprise-grade Wi-Fi 6E or latest equivalent standards to replace existing devices that have reached end of life.

The Low specification devices for standard-density environments and general-purpose wireless connectivity must have the following features:

- Tri-band Wi-Fi 6E (2.4 GHz, 5 GHz, 6 GHz)
- 2x2 MIMO antenna configuration, delivering reliable performance for light to moderate client density scenarios.
- Basic RF management features, including automatic channel selection and load balancing to ensure stable operation.
- Enterprise security (WPA3, secure boot)
- IoT-ready architecture
- Centralised management (cloud/on-prem support)
- Must include all required licenses for full feature activation (connectivity, analytics, location services)
- Include OEM hardware warranty for a period of 5 years, with NBD replacement.
- The devices must either be supported by the existing WLAN controllers or separate controllers can be supplied; however, there needs to be seamless roaming between new and existing APs, ensuring no degradation in connectivity or user experience.
- Must be supported by the ACSA WIFI portal, or a suitable replacement portal must be provided.
- Include decommissioning of existing EOL infrastructure, documentation, asset tagging and validation testing and commissioning of new infrastructure
- Installation should cater for all equipment required for installation at heights, including Skyjacks where required.

3.0 WIFI Work Package - Replacement of Outdoor Access Point with external Omnidirectional Antennae

Supply, physically install and configure WIFI Access points that meet enterprise-grade Wi-Fi 6E or latest equivalent standards to replace existing devices that have reached end of life.

- Tri-band Wi-Fi 6E (2.4 GHz, 5 GHz, 6 GHz)
- 2x2 MIMO antenna configuration, delivering reliable performance for light to moderate client density scenarios
- Outdoor-rated enclosure with N-type connectors for external antennas
- Omni-directional dipole antennas with 4 dBi (2.4 GHz), 8 dBi (5 GHz), and 8 dBi (6 GHz) gain
- Basic RF management features, including automatic channel selection and load balancing to ensure stable operation
- Enterprise security (WPA3, secure boot)
- IoT-ready architecture
- Centralised management (cloud/on-prem support via vendor platform)
- Must include all required licenses for full feature activation (connectivity, analytics, location services)
- Include OEM hardware warranty for a period of 5 years, with NBD replacement.
- Include decommissioning of existing EOL infrastructure, documentation, asset tagging and validation testing and commissioning of new infrastructure
- The devices must either be supported by the existing WLAN controllers or separate controllers can be supplied; however, there needs to be seamless roaming between new and existing APs, ensuring no degradation in connectivity or user experience.
- Support for ACSA Wi-Fi portal, or provision of a suitable replacement captive portal with equivalent functionality
- Installation should cater for all equipment required for installation at heights, including Skyjacks where required.

4.0 WIFI Work Package - Replacement of Outdoor Access Point with Internal Antennae

Supply, physically install and configure WIFI Access points that meet enterprise-grade Wi-Fi 6E or latest equivalent standards to replace existing devices that have reached end of life.

The low specification devices with directional antennae for standard-density environments and general-purpose outdoor wireless connectivity must have the following features:

- Outdoor-rated enclosure with N-type connectors for external antennas
- Directional patch antennas with 8 dBi (2.4 GHz), 9 dBi (5 GHz), and 9 dBi (6 GHz) gain
- Basic RF management features, including automatic channel selection and load balancing to ensure stable operation
- Enterprise security (WPA3, secure boot)
- IoT-ready architecture
- Centralised management (cloud/on-prem support via vendor platform)
- Must include all required licenses for full feature activation (connectivity, analytics, location services)
- Include OEM hardware warranty for a period of 5 years, with NBD replacement.
- The devices must either be supported by the existing WLAN controllers or separate controllers can be supplied; however, there needs to be seamless roaming between new and existing APs, ensuring no degradation in connectivity or user experience.
- Include decommissioning of existing EOL infrastructure, documentation, asset tagging and validation testing and commissioning of new infrastructure
- Support for ACSA Wi-Fi portal, or provision of a suitable replacement captive portal with equivalent functionality
- Installation should cater for all equipment required for installation at heights, including Skyjacks where required.

5.0 WIFI Work Package - Replacement of Small site Wlan controller

Supply, physically install, and configure a enterprise grade WLAN controller to replace the existing controller infrastructure supporting enterprise-grade Wi-Fi 6E or the latest equivalent access points. The controller must have the following features:

- Supports up to 250 access points
- Handles up to 5,000 clients
- Throughput: ~5 Gbps
- Support for Wi-Fi 6E or the latest equivalent and backward compatibility with Wi-Fi 5/6 access points that may still be in operation.
- Centralised management of access points, SSIDs, RF profiles, and security policies
- Integrated security features including WPA3, secure boot, and policy-based access control
- Scalable architecture supporting small to medium enterprise deployments with future expansion capability
- Cloud-managed or on-premises deployment options, compatible with existing network and security infrastructure
- Support for ACSA Wi-Fi portal, or provision of a suitable replacement captive portal with equivalent functionality
- Must support high availability
- Licensing model must include all required features (connectivity, analytics, location services, policy enforcement)
- Include OEM hardware warranty for a period of 5 years, with 4-hour replacement
- Include decommissioning of existing controller infrastructure, documentation, asset tagging, and validation testing and commissioning of new controller
- The new controller must be able to support and manage all existing WIFI access points that connect to the existing controller, and retain all existing features.

6.0 WIFI Work Package - Replacement Large Site WLAN controller

Supply, physically install, and configure a enterprise grade WLAN controller to replace the existing controller infrastructure supporting enterprise-grade Wi-Fi 6E or the latest equivalent access points. The controller must have the following features:

- Supports up to 2,000 access points
- Handles up to 32,000 clients
- Throughput: ~40 Gbps
- Support for Wi-Fi 6E or the latest equivalent and backward compatibility with Wi-Fi 5/6 access points that may still be in operation.
- Centralised management of access points, SSIDs, RF profiles, and security policies
- Integrated security features including WPA3, secure boot, and policy-based access control
- Scalable architecture supporting small to medium enterprise deployments with future expansion capability
- Cloud-managed or on-premises deployment options, compatible with existing network infrastructure
- Support for ACSA Wi-Fi portal, or provision of a suitable replacement captive portal with equivalent functionality
- Must support high availability
- Licensing model must include all required features (connectivity, analytics, location services, policy enforcement)
- Include OEM hardware warranty for a period of 5 years, with 4-hour replacement
- Include decommissioning of existing controller infrastructure, documentation, asset tagging, and validation testing and commissioning of new controller.
- The new controller must be able to support and manage all existing WIFI access points that connect to the existing controller, and retain all existing features.

7.0 Security Work Package - Replacement of Small Site Firewalls

Supply, physically install, and configure a enterprise grade next-generation firewall and threat prevention appliance to replace the existing small site firewalls, ensuring advanced threat protection, high availability, and centralised security management.

The appliance must have the following features:

- Firewall throughput of up to 18 Gbps
- Next-generation firewall (NGFW) throughput of 6.2 Gbps
- Threat prevention throughput of 3.7 Gbps, including IPS, antivirus, anti-bot, URL filtering, DNS security, and sandboxing
- VPN throughput of 4.9 Gbps using AES-256 encryption
- Connection rate of 116,000 connections per second, supporting up to 2 to 8 million concurrent connections depending on memory configuration
- Hardware configuration includes, minimum:
    - 16 GB RAM
    - 240 GB SSD storage
    - Lights-Out Management (LOM) module
    - 10x 1GbE copper ports
    - 4x 10GbE SFP+ ports with transceivers
    - Dual AC power supplies
- Supports Layer 2 and Layer 3 routing, NAT, VRRP, OSPF, BGP, RIP, and multicast protocols
- Supports HTTPS inspection, including TLS 1.3 and HTTP/2 traffic
- Modular chassis, rack mountable with high port density and expansion options
- Must be configured in high availability configuration offering seamless failover and continuous service availability
- Includes 5-year license and maintenance, with OEM hardware warranty and 4-hour replacement SLA
- Includes sandboxing subscription Package - for advanced threat prevention, file sanitisation, and zero-phishing
- Include decommissioning of existing security appliance, documentation, asset tagging, and validation testing and commissioning of new appliance with existing firewall rule base.
- The firewall appliance must be integrated with the existing centralised firewall management system to ensure unified policy enforcement, monitoring, and administration across the network.
- SFPs must be supplied, if the existing SFPs are not supported in the proposed OEM models.

8.0 Security Work Package - Replacement of Medium Site Firewalls

Supply, physically install, and configure a enterprise grade next-generation firewall and threat prevention appliance to replace the existing medium site firewalls, ensuring advanced threat protection, high availability, and centralized security management.

The appliance must have the following features:

- Firewall throughput of up to 55 Gbps, with 80 Gbps for large UDP packets (1518B)
- Threat prevention throughput of up to 4.95 Gbps, including IPS, antivirus, anti-bot, and sandboxing
- Next-generation firewall (NGFW) throughput of 18.6 Gbps
- VPN throughput of 22.1 Gbps using AES-256 encryption
- Connection rate of 190,000 connections per second, supporting up to 16.2 million concurrent connections
- Hardware configuration includes:
    - 32 GB RAM
    - 480 GB SSD SATA storage
    - Lights-Out Management (LOM) module
    - 4-port 1GBase-F SFP+ interface card with 4 SFPs
    - Dual AC power supplies
- Supports Layer 2 and Layer 3 routing, NAT, VRRP, OSPF, BGP, RIP, and multicast protocols
- Supports HTTPS inspection, including TLS 1.3 and HTTP/2 traffic
- Modular chassis, rack mountable with high port density and expansion options
- Must be configured in high availability configuration offering seamless failover and continuous service availability
- Includes 5-year license and maintenance, with OEM hardware warranty and 4-hour replacement SLA
- Includes sandboxing subscription Package - for advanced threat prevention, file sanitisation, and zero-phishing
- Include decommissioning of existing security appliance, documentation, asset tagging, and validation testing and commissioning of new appliance with existing firewall rule base.
- The firewall appliance must be integrated with the existing centralised firewall management system to ensure unified policy enforcement, monitoring, and administration across the network.
- SFPs must be supplied, if the existing SFPs are not supported in the proposed OEM models.

9.0 Security Work Package - Replacement of Large Site Firewalls

Supply, physically install, and configure an enterprise grade next-generation firewall and threat prevention appliance to replace the existing large site firewalls, ensuring advanced threat protection, high availability, and centralized security management.

The appliance must have the following features:

- Firewall throughput of up to 70 Gbps, with 80.2 Gbps for large UDP packets (1518B)
- Threat prevention throughput of up to 10.5 Gbps, including IPS, antivirus, anti-bot, DNS security, and sandboxing
- Next-generation firewall (NGFW) throughput of 28.2 Gbps
- VPN throughput of 33 Gbps using AES-256 encryption
- Connection rate of 300,000 connections per second, supporting up to 16.2 million concurrent connections
- Hardware configuration includes:
    - 32 GB RAM
    - 480 GB SSD SATA storage
    - Dual AC power supplies for high availability
    - Lights-Out Management (LOM) for remote monitoring and control
    - 8 x RJ45 ports and 8 x 1/10GbE SFP+ ports for high-density connectivity
- Supports Layer 2 and Layer 3 routing, NAT, VRRP, OSPF, BGP, RIP, and multicast protocols
- Supports HTTPS inspection, including TLS 1.3 and HTTP/2 traffic
- Modular chassis, rack mountable with high port density and expansion options
- Must be configured in high availability configuration offering seamless failover and continuous service availability
- Includes 5-year license and maintenance, with OEM hardware warranty and 4-hour replacement SLA
- Includes sandboxing subscription Package - for advanced threat prevention, file sanitisation, and zero-phishing
- Include decommissioning of existing security appliance, documentation, asset tagging, and validation testing and commissioning of new appliance with existing firewall rule base.
- The firewall appliance must be integrated with the existing centralised firewall management system to ensure unified policy enforcement, monitoring, and administration across the network.
- SFPs must be supplied, if the existing SFPs are not supported in the proposed OEM models.

10.0 Security Work Package - Replacement of Centralised Firewall Manager

Supply, physically install, and configure a next-generation firewall and security management appliance to manage the small, medium and large site firewalls by replacing the existing management server infrastructure. This appliance will provide centralised security policy management, log aggregation, and reporting for existing distributed firewall gateways.

The appliance must have the following features:

- Support management of up to 10 security gateways
- Log ingestion capacity of up to 25,000 logs per second sustained
- Log indexing and storage optimised for high-throughput environments
- Support for log correlation between all firewalls, event analysis, compliance reporting
- 32 GB RAM (or higher)
- Dual 480 GB SSD in RAID 1 configuration (mirrored storage for log redundancy)
- Centralised management of:
    - Policy Package - (Firewall, NAT, VPN, Threat Prevention)
    - Objects database and global policy layers
- Include 5-year maintenance and support, with OEM hardware warranty and Next Business Day (NBD) replacement SLA
- Include 5-year compliance event and reporting all firewalls.
- Include decommissioning of existing security appliance, documentation, asset tagging, and validation testing and commissioning of new appliance with existing firewall rule base.

11.0 Security Work Package - Replacement distributed Denial of Service Protector

Supply, physically install, and configure the enterprise grade Distributed Denial of Service Protector appliance to replace the existing DDOS protector, ensuring protection against denial of service attacks.

The appliance must have the following features:

- Dedicated hardware appliance for DDoS mitigation
- Mitigation throughput of up to 12 Gbps
- Protects against both network-layer and application-layer DDoS attacks
- Supports customised signature creation for evolving threats
- Flexible filter engines to detect and block malicious traffic
- Protection against HTTP floods, bandwidth saturation, and protocol anomalies
- Includes 5-year license and maintenance, with OEM hardware warranty and Next Business Day (NBD) replacement SLA
- Include decommissioning of existing security appliance, documentation, asset tagging, and validation testing and commissioning of new appliance
- The DDOS appliance must be integrated with the centralised firewall management system to ensure unified policy enforcement, monitoring, and administration across the network.

12.0 Security Work Package - Replacement of Existing Perimeter Firewall

Supply, physically install, and configure an enterprise-grade next-generation firewall appliance from a different vendor than the internal firewalls, to replace the current perimeter security infrastructure. The solution must ensure advanced threat protection and high availability, while maintaining vendor diversity to minimise OEM specific vulnerabilities.

The appliance must have the following features:

- Firewall throughput of at least 80 Gbps
- Threat protection throughput of at least 10 Gbps, including IPS, anti-malware, application control, and sandboxing
- SSL/TLS inspection throughput of at least 8 Gbps, with support for TLS 1.3
- VPN throughput of at least 40 Gbps, supporting IPsec and SSL VPN
- Concurrent session capacity of at least 10 million, with a new session rate of 400,000 per second
- Integrated SD-WAN capabilities for link optimisation and application-aware routing
- Advanced routing support including BGP, OSPF, RIP, and multicast
- High port density, including multiple 1G and 10G interfaces for flexible deployment
- Must be configured in high availability configuration offering seamless failover and continuous service availability
- Licensing model must include all required features (NGFW, SD-WAN, threat protection, application control, reporting)
- Include OEM hardware warranty for a period of 5 years, with 4-hour replacement SLA
- Include decommissioning of existing firewall infrastructure, documentation, asset tagging, and validation testing and commissioning of new appliance
- Centralised management via vendor-supported platform for policy, logging, and analytics

13.0 Security Work Package - Replacement of Existing Public WIFI Firewall

Supply, physically install, and configure an enterprise-grade next-generation firewall appliance from approved vendors to replace the existing perimeter security infrastructure, ensuring advanced threat protection and high availability.

The appliance must have the following features:

- Firewall throughput of at least 40 Gbps
- Threat protection throughput of at least 5 Gbps, including IPS, anti-malware, application control, and sandboxing
- Concurrent session capacity of at least 5 million, with a new session rate of 400,000 per second
- High port density, including multiple 1G and 10G interfaces for flexible deployment
- Must be configured in high availability configuration offering seamless failover and continuous service availability
- Licensing model must include all required features (NGFW, SD-WAN, threat protection, application control, reporting)
- Include OEM hardware warranty for a period of 5 years, with 4-hour replacement SLA
- Include decommissioning of existing firewall infrastructure, documentation, asset tagging, and validation testing and commissioning of new appliance
- Centralised management via vendor-supported platform for policy, logging, and analytics

14.0 Security Work Package - Replacement of Existing Small Site Web Proxy Solution

Supply, physically install, and configure an enterprise-grade secure web gateway (SWG) appliance from approved vendors to replace the existing web proxy infrastructure, providing advanced web security, URL filtering, malware protection, and policy enforcement capabilities for outbound web traffic.

The solution must have the following features:

- The solution must fit into ACSA's existing architecture or include the costs of any additional requirements including bandwidth
- Solution throughput must support sustained web traffic inspection for the user base per site
- Solution throughput must support concurrent HTTP/HTTPS connections for the userbase per site.
- Comprehensive URL filtering with support for URL categories and real-time updates
- Advanced malware protection with real-time threat intelligence and file reputation scoring
- HTTPS (SSL/TLS) traffic inspection with full certificate validation, policy control, and support for TLS 1.3
- Integrated Data Loss Prevention (DLP) capabilities for web uploads and posts
- Support for ICAP to integrate with external DLP and AV engines
- Must support user quotas for time and bandwidth.
- Authentication integration with Active Directory, LDAP, and SAML
- Policy-based control over user access, applications, content categories, and file types
- Support for Active Directory user, Active Directory group-based and IP-based reporting and policy enforcement
- Must be configured in high availability configuration offering seamless failover and continuous service availability
- Support for log forwarding to SIEM systems using syslog, CEF, or LEEF formats
- Must be deployment as a transparent proxy to ensure seamless mobility across sites.
- Centralised management and reporting platform for policy administration and traffic analytics
- Include OEM hardware warranty for a period of 5 years, with 4-hour replacement SLA
- Include decommissioning of existing web proxy infrastructure, documentation, asset tagging, and validation testing and commissioning of new appliance

15.0 Security Work Package - Replacement of Existing Large Site Web Proxy Solution

Supply, physically install, and configure an enterprise-grade secure web gateway (SWG) appliance from approved vendors to replace the existing web proxy infrastructure, providing advanced web security, URL filtering, malware protection, and policy enforcement capabilities for outbound web traffic.

The solution must have the following features:

- The solution must fit into ACSA's existing architecture or include the costs of any additional requirements including bandwidth
- Solution throughput must support sustained web traffic inspection for the user base per site
- Solution throughput must support concurrent HTTP/HTTPS connections for the userbase per site.
- Comprehensive URL filtering with support for URL categories and real-time updates
- Advanced malware protection with real-time threat intelligence and file reputation scoring
- HTTPS (SSL/TLS) traffic inspection with full certificate validation, policy control, and support for TLS 1.3
- Integrated Data Loss Prevention (DLP) capabilities for web uploads and posts
- Support for ICAP to integrate with external DLP and AV engines
- Must support user quotas for time and bandwidth.
- Authentication integration with Active Directory, LDAP, and SAML
- Policy-based control over user access, applications, content categories, and file types
- Support for Active Directory user, Active Directory group-based and IP-based reporting and policy enforcement
- Must be configured in high availability configuration offering seamless failover and continuous service availability
- Support for log forwarding to SIEM systems using syslog, CEF, or LEEF formats
- Must be deployment as a transparent proxy to ensure seamless mobility across sites.
- Centralised management and reporting platform for policy administration and traffic analytics
- Include OEM hardware warranty for a period of 5 years, with 4-hour replacement SLA
- Include decommissioning of existing web proxy infrastructure, documentation, asset tagging, and validation testing and commissioning of new appliance

16.0 IPT Work Package - Supply and install a high-spec server for the IP Telephony environment

Supply, install, and configure enterprise-grade server appliances, including applicable call control and telephony application software, to replace end-of-life servers within the IP Telephony infrastructure. The server must support hosting multiple IP Telephony applications such as specified in **Annexure A, table 1.**

Minimum Technical Specifications

- Rack-mountable server appliance (2U)
- Dual high-performance CPUs, minimum 16 cores per CPU (32 cores total), base frequency ≥ 2.8 GHz
- Minimum 192 GB DDR5 RDIMM memory
- 24 × 600 GB SAS 10K RPM SFF HDD, hot-swappable
- RAID controller with minimum 4 GB Flash Backed Write Cache, supporting RAID 0, 1, 5, 6, 10, 50, 60
- Minimum 8 × 10 Gigabit Ethernet ports (SFP+), plus 1 GbE management port
- Dual redundant hot-plug power supplies (minimum 1200W AC Titanium)
- TPM 2.0 module (FIPS 140-2, Common Criteria EAL4+ certified)
- Compatible with VMware ESXi hypervisor
- Enterprise-grade compliance for reliability and security
- Supply, installation, configuration, integration, testing, commissioning, documentation, and removal of old hardware.
- Provide virtualization capability for hosting these applications on a single platform.
- Ensure seamless integration with existing IP Telephony infrastructure.
- Support migration from legacy servers without downtime.
- Minimum 5-year OEM hardware warranty with Next Business Day replacement.

17.0 IPT Work Package - Supply and install SIP Voice Gateways for IP Telephony environment

Supply, install, and configure enterprise-grade edge routers to replace end-of-life voice gateways, as specified as in **Annexure A, table 1.** Must support SIP voice integration and secure, high-performance connectivity for each airport site. The supplied SIP Voice Gateways must be fully compatible with the existing IP Telephony platform (including call control servers, dial plans, and voice features) and support SIP trunking as currently implemented with external service providers. The solution must allow migration of voice services from legacy gateways without redesign or downtime.

Minimum Technical Specifications

- Rack-mountable, 1RU design with 19" rack-mount kit
- Multicore CPU architecture (minimum 8 cores)
- Minimum 8 GB DRAM memory
- Minimum 16 GB internal flash storage
- Minimum 4 × 1 Gigabit Ethernet WAN ports (RJ45 and SFP)
- USB interface for storage/configuration
- NIM slot with 64-channel DSP capability for voice services
- Embedded IPsec VPN hardware acceleration (≥ 1 Gbps)
- Support for SASE architecture and container-based security services
- Zero-touch provisioning (Plug-and-Play)
- Support for modular OS with SD-WAN capability
- Tamper-resistant hardware with TPM module
- Must integrate with existing IP Telephony infrastructure and SIP trunking.
- Support migration of voice services without downtime.
- Supply, installation, configuration, integration, testing, commissioning, documentation, and removal of old hardware.
- Minimum 5-year OEM hardware warranty with Next Business Day replacement.

18.0 IPT Work Package - Supply and install IP Telephones

Supply, install, and configure new IP telephones to replace end-of-life units at all airport check-in counters, departure gates and iHelp areas.

Minimum Technical Specifications

- Colour: Carbon Black or equivalent
- Dual Ethernet ports (RJ-45) with PoE support
- 100/1000BASE-T Ethernet compliance (IEEE 802.3 standards)
- Compatibility with enterprise UC platforms and SIP-based systems
- Multiline operation (minimum 4 lines)
- Caller ID display
- Full-duplex speakerphone
- High-resolution colour display
- Support for secure SIP signalling and media encryption (TLS/SRTP)
- Must integrate with existing IP Telephony infrastructure without service disruption.
- Support centralized provisioning and firmware upgrades.
- Supply, installation, configuration, integration, testing, commissioning, documentation, and removal of old hardware.

19.0 IPT Work Package - Supply and install single telephone brackets to secure phones

Supply and install telephone brackets at all airport check-in counters, boarding gates and iHelp areas, to securely hold IP telephones and prevent tampering.

Minimum Technical Specifications

- Material: Mild steel, powder-coated for corrosion resistance
- Finish: Matte black
- Dual-purpose design for wall and desk mounting
- Lockable enclosure or tamper-resistant fasteners
- Provision for cable management and securing network/power cables
- Bracket dimensions to be finalized based on IP telephone model
- Supply, installation, secure mounting of IP telephones, removal of old hardware, documentation, and handover.

20.0 NETWORK Work Package - REPLACE ENTERPRISE ACCESS SWITCHES

Enterprise-Grade 48-Port PoE+ Access Switches

Supply, configure and implement Enterprise-Grade 48-Port PoE+ Access Switches at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. All installations are to be done after every location-specific operating hours and after last flight. Include decommissioning of existing Cisco 3650 switches and asset management in your pricing.

- "Bidders are invited to propose switches that meet or exceed these specifications.
- Port Configuration: 48 Gigabit Ethernet ports with Power over Ethernet Plus (PoE+) support, delivering up to 30W per port.
- PoE Budget: Minimum 700W total PoE power budget
- Switching Capacity: Minimum 200 Gbps switching capacity (non-stacked) with support for stacking to achieve higher throughput (up to 400 Gbps or greater preferred).
- Uplink Ports: Modular or fixed uplinks supporting at least 4x 10 Gigabit Ethernet (10GE) SFP+ ports for high-speed connectivity.
- Layer Support: Layer 2
- **Stacking: Include modules and cables for each switch stacking with a minimum stacking bandwidth of 100 Gbps**
- Reliability: High availability, including **redundant power supplies** and hot-swappable components.
- Software Features: Support for enterprise-grade software capabilities, including network analytics, automation, and integration with modern network architectures (e.g., SD-Access or equivalent).
- Form Factor: 1RU rack-mountable design.
- Interoperability: Must interoperate with existing Cisco equipment in mixed environments.
- **Warranty and Support: Minimum 5-year warranty with Next Business Day replacement and options for extended support and maintenance services.**
- **Include 2 added 10G Long Range Single Mode SFPs per switch if you NO NOT propose Cisco as your solution.**

21.0 NETWORK Work Package - REPLACE BRANCH TYPE ACCESS SWITCHES

Stackable 24 or 48 Port Enterprise PoE+ Access Switches

Supply, configure and implement stackable 24 and 48-Port PoE+ Access Switches at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. All installations are to be done after every location-specific operating hours and after the last flight. Include decommissioning of existing Cisco 2960X switches and asset management in your pricing.

- Bidders are invited to propose switches that meet or exceed these specifications.
- Type: Stackable, managed Layer 2/3 enterprise access switch.
- Minimum 24 or 48 Gigabit Ethernet (GE) ports (RJ45) for client connectivity.
- Minimum 4x 10 Gigabit Ethernet (1/10GE) SFP+ uplink ports
- Support for PoE/PoE+ (IEEE 802.3af/at) on all GE ports.
- Minimum PoE power budget of 370W (for 24-port models) or 740W (for 48-port models), upgradable to higher budgets.
- Modularity: Support for hot-swappable, redundant power supplies and fans.
- Switching Capacity: Minimum 128 Gbps for 24-port models or 176 Gbps for 48-port models.
- Support for physical or virtual stacking of up to 6 switches.
- **Dual, hot-swappable AC power supplies (redundant).**
- **Stacking: Include modules and cables for each switch**
- Warranty: Minimum 5-year hardware warranty with next-business-day replacement.
- **Include 1x Stack Kit per switch**
- Interoperability: Must interoperate with existing Cisco equipment in mixed environments.
- **Warranty and Support: Minimum 5-year warranty with Next Business Day replacement and options for extended support and maintenance services.**
- **Include 1x 10G Long Range Single Mode SFP per switch if you NO NOT propose Cisco as your solution.**

22.0 NETWORK Work Package - REPLACE 1U MPLS PE CORE SWITCHES

Enterprise Grade 48 Port 1/10/25/40/100Gbps Core Switch

Supply, configure and implement an Enterprise Grade 48 Port 1/10/25/40/100Gbps Core Switch at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. All installations are to be done after operating hours and after the last flight. Include decommissioning of existing 9500X switches and asset management in your pricing.

- Bidders are invited to propose switches that meet or exceed these specifications.
- Enterprise-Grade 48-Port 1/10/25/40/100Gbps Core Switch
- Form Factor: 1RU (Rack Unit) fixed configuration switch.
- Minimum 48 ports supporting 25 Gigabit Ethernet (SFP28 or equivalent).
- Minimum 4 to 6 ports supporting 40/100 Gigabit Ethernet (QSFP28 or equivalent).
- All ports must support auto-negotiation and backward compatibility with lower speeds (e.g., 1/10 Gbps).
- Switching Capacity: Minimum 2 Tbps, with preference for higher capacity up to 6.6 Tbps.
- Layer Support: Full Layer 2 and Layer 3 functionality, including VLANs, QoS, and IPv4/IPv6 routing and MPLS.
- Stacking/Virtualisation: Support for switch stacking or virtual chassis technology to enable unified management of multiple switches.
- Programmability: Support for APIs (e.g., NETCONF, RESTCONF, or equivalent) for integration with SDN environments.
- Monitoring: Support for telemetry, sFlow, or equivalent for real-time network analytics.
- Power Supply**: Dual redundant AC power supplies**, with minimum power consumption efficiency (80 PLUS Platinum or equivalent).
- Must support industry-standard protocols (e.g., IEEE 802.1Q, 802.3ad, OSPF, BGP, MPLS).
- **Compatibility with existing Cisco enterprise network infrastructure, including downstream switches**
- **Minimum 5-year license and OEM warranty with 24/7/4 hardware replacement.**
- **Include 112x 10G Long Range Single Mode SFPs if you NO NOT propose Cisco as your solution.**

"

23.0 NETWORK Work Package - NTP SERVER APPLIANCES

SyncServer S650 GNSS-Referenced NTP/PTP Time Server

Supply, configure and implement SyncServer S650 GNSS-Referenced NTP/PTP Time Server at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. Include decommissioning of existing NTP appliances and asset management in your pricing.

- 090-15200-650 "Microchip model SyncServer S650, includes Kit: 75 ft. total length: 50 ft.
- Cable; Lightning Arrestor; 25 ft. Cable; Antenna Kit"
- 090-15201-002 Dual AC Power Supply
- 090-15201-009 SyncServer 10 GbE Module
- 090-15201-013 SyncServer Timing I/O Module with Fiber Outputs

24.0 NETWORK Work Package - REPLACE MODULAR MPLS CORE SWITCHES

Supply, configure and implement 4x Core Switches at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. All installations are to be done after operating hours and after the last flight. Include decommissioning of existing Cisco 6807 chassis and modules, and asset management in your pricing.

Generic Specification for Modular High-Density Ethernet Switch System. This specification outlines the requirements for a modular, high-performance Ethernet switch system suitable for enterprise core or aggregation network deployments. The system shall provide scalable, non-blocking Layer 2/3 switching with high port density for 10/25 Gigabit Ethernet (GbE) and 40/100 GbE interfaces, dual supervisor redundancy, and N+1 power supply redundancy. The design shall support future scalability to at least 25 Tbps total switching capacity. All components must be hot-swappable for high availability, with support for redundant fans and power inputs. The system shall comply with relevant standards including IEEE 802.3, RoHS, and NEBS Level 3 (if applicable for carrier-grade deployments).1. Chassis Requirements

- Form Factor: Rack-mountable chassis, occupying no more than 8 rack units (RU) height.
- Slot Configuration: Minimum 4 slots for line cards, plus 2 dedicated slots for supervisor modules.
- Switching Capacity: Up to 25 Tbps full-duplex (12.5 Tbps half-duplex) wired switching capacity, with per-slot forwarding bandwidth of at least 6 Tbps.
- Port Density: Capable of supporting up to 96 native 10/25/50 GbE ports or equivalent mix of 40/100 GbE ports across all line cards.
- Backplane/Interconnect: Non-blocking fabric with full-mesh connectivity between all slots, supporting distributed forwarding across line cards.

2. Supervisor Module Requirements

- Quantity: 2 redundant supervisor modules (active/standby or active/active SSO configuration for stateful switchover).
- Performance: Each module shall provide a minimum of 3 Tbps full-duplex switching capacity, based on a programmable ASIC architecture optimized for high-scale routing and security features.
- Processing: Multi-core CPU (at least 2 GHz) with at least 16 GB DRAM and 16 GB flash storage for system software and logging.
- Features:
    - Hardware-based forwarding for IPv4/IPv6 unicast/multicast, MPLS, QoS, and ACLs up to 1 million entries.
    - Integrated security with TrustSec and MACsec encryption.
    - Software-defined networking (SDN) compatibility, including OpenFlow and NETCONF/YANG.
- Redundancy: 1+1 supervisor redundancy with sub-second failover, including redundant clocks and fabric interfaces.

3. Line Card Requirements for 10/25 GbE

- Type: Modular line cards compatible with the chassis slots, supporting 1/10/25 GbE breakout configurations.

- Port Density
    - 2X 24-port line card with SFP28 transceivers, configurable for 1/10/25 GbE per port.
- Performance: Minimum 2.4 Tbps per line card; non-blocking at line rate for all ports simultaneously.
- Interfaces: SFP28 cages supporting multimode/single-mode fiber, DAC, and AOC transceivers; compliant with IEEE 802.3by (25GBASE-SR/CR) and 802.3ae (10GBASE).
- Features:
    - Wire-rate Layer 2/3 forwarding with VXLAN/EVPN support.
    - Per-port QoS with 8 queues, ingress/egress policing up to 100 Gbps.
    - Hardware timestamping for PTP (IEEE 1588v2) and SyncE.
- Power Consumption: Maximum 400W per card under full load.

4. Line Card Requirements for 40/100 GbE

- Type: Modular line cards compatible with the chassis slots, supporting 40/100 GbE with breakout to lower speeds.
- Port Density
    - 2X 24-port line card with QSFP28 transceivers, configurable as 24 x 40 GbE or 12 x 100 GbE (non-blocking).
- Performance: Minimum 2.4 Tbps per line card; non-blocking at line rate, with support for 4:1 oversubscription if hybrid ports are used.
- Interfaces: QSFP28 cages supporting multimode/single-mode fiber, DAC, and AOC; compliant with IEEE 802.3ba (40GBASE) and 802.3bm (100GBASE).
- Features:
    - Flexible port grouping for breakout (e.g., 100 GbE to 4 x 25 GbE).
    - Advanced buffering (minimum 40 MB shared) for bursty traffic.
    - Telemetry and analytics via gRPC and model-driven programmability.
- Power Consumption: Maximum 500W per card under full load.

5. Power System Requirements

- Redundancy Mode: N+1 power supply redundancy, where N is the number of active power supplies required for full system load, and +1 provides hot-standby failover without service interruption.
- Quantity and Type: Minimum 4 hot-swappable power supply units (PSUs) per chassis; support for both AC (100-240V) and DC (-48V) inputs.
- Capacity: Each PSU rated for at least 2500W output; total system power budget supporting full chassis population (up to 10 kW).
- Efficiency: 80 PLUS Platinum certified (minimum 94% efficiency at 50% load).
- Monitoring: Integrated power management with real-time telemetry, fault detection, and automatic load balancing across PSUs.

- Input Safeguards: Independent input circuits per PSU pair, with protection against single-point failures.

6. General System Features

- High Availability: Stateful switchover (SSO), non-stop forwarding (NSF), and graceful restart (GR) for routing protocols (OSPF, BGP, IS-IS).
- Software: Vendor-provided network operating system with unified image across chassis and line cards; support for zero-touch provisioning (ZTP) and automation via Ansible/Python APIs.
- Security: Role-based access control (RBAC), 802.1X authentication, and encrypted management (SSHv2, TLS 1.3).
- Warranty and Support: Minimum 5-year hardware warranty with 4 HOUR advance replacement;
- Compliance and Testing: System shall undergo interoperability testing with standard transceivers (e.g., MSA-compliant) and provide documentation for RFP compliance.

7. Pricing (RFP Guidance)

- Bidders shall provide pricing for a baseline configuration: 1 chassis, 2 supervisor modules, 2 x 10/25 GbE line cards, 2 x 40/100 GbE line cards, 4 x PSUs, and redundant fans.

25.0 NETWORK Work Package - REPLACE FIBRE DISTRIBUTION SWITCHES

Supply, configure and implement Enterprise Grade 12 and 24 Port 1/10/25/Gbps L2/L3 Fibre Distribution Switches at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. All installations are to be done after operating hours and after the last flight. Include decommissioning of existing Cisco 3850-12S and 3850-24S switches and asset management in your pricing. **All devices to have a 5-year SNTP 24X7X4 warranty.**

The switch shall support modular uplink options for scalability, advanced security features, and model-driven programmability. It must be compatible with open standards (e.g., IEEE 802.3), run on a modular OS supporting NETCONF/RESTCONF/YANG, and provide investment protection through backward compatibility with similar series components. Target use cases include SD-WAN edge, aggregation for access switches, and secure fabric underlay.

Hardware Specifications

- The switch shall be 1RU rack-mountable with field-replaceable units (FRUs) for fans and power supplies.
- Downlink Ports - 12 or 24 multi-rate SFP28 ports supporting 1G/10G/25G fiber (e.g., SR/LR transceivers) - Auto-negotiation for speed and duplex
- Uplink Ports - Modular expansion: 8 x 10G/25G SFP28 via removable network module
- Cooling & Redundancy - 3 x redundant, hot-swappable fans (N+1)
- Power Supplies - Dual hot-swappable AC (1+1 redundant); default 715W AC, scalable to 1,100W for 24 port models.
- Stacking Bandwidth - Up to 1 Tbps bidirectional (e.g., via dedicated StackWise cables: 1m lengths)
- Maximum Stack Members: 4 switches (mixable with compatible access models)
- High Availability: Stateful switchover (SSO), non-stop forwarding (NSF), graceful restart; hitless software upgrades; ISSU support
- Redundancy Protocols: VRRP/HSRP/GLBP for first-hop; LACP/MLAG for link aggregation
- Protocols: SNMPv3, NETCONF/RESTCONF/gRPC, Syslog, sFlow/NetFlow (up to 64K flows)
- Programmability: Python scripting, guest shell for containers/apps (e.g., via Docker)
- Orchestration: gNMI telemetry, OpenConfig support; integration with SDN controllers (e.g., Cisco DNA or open equivalents)
- OS: Modular, patchable network OS with zero-touch provisioning (ZTP)
- Licensing: Perpetual base + optional add-ons for advanced routing/security (e.g., DNA Advantage equivalent)
- Warranty: Minimum 5 years with next-business-day support; optional 24x7 TAC
- **Include 10x 10G Long Range Single Mode SFPs for every 12-port switch if you NO NOT propose Cisco as your solution.**
- **Include 20x 10G Long Range Single Mode SFPs for every 24-port switch if you NO NOT propose Cisco as your solution.**

26.0 NETWORK Work Package - UPGRADE OF SELECTED 1G to 10G SFPs

Supply, configure and implement link speed upgrades at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. All installations are to be done after operating hours and after the last flight. Equipment must be OEM certified

Part Number	Description
SFP-10G-LRM=	10GBASE-LRM SFP Module
SFP-10G-LR-S=	10GBASE-LR SFP Module, Enterprise-Class

27.0 NETWORK Work Package - UPGRADE OF SELECTED LINKS TO 25/40/100G

Supply, configure and implement link speed upgrades at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. All installations are to be done after operating hours and after the last flight. Equipment must be OEM certified

Part Number	Description
QSFP-100G-LR4-S=	100GBASE LR4 QSFP Transceiver, LC, 10km over SMF
SFP-10/25G-LR-S=	10/25GBASE-LR SFP28 Module

28.0 NETWORK Work Package - PHASED REPLACEMENT ENTERPRISE ACCESS SWITCHES

Enterprise-Grade 48-Port PoE+ Access Switches

Supply, configure and implement Enterprise-Grade 48-Port PoE+ Access Switches at the quantities and locations as defined in the pricing schedule. Include professional fees and project management costs in the total price. All installations are to be done after every location-specific operating hours and after the last flight. Include decommissioning of existing Cisco 9300 switches and asset management in your pricing.

- "Bidders are invited to propose switches that meet or exceed these specifications.
- Port Configuration: 48 Gigabit Ethernet ports with Power over Ethernet Plus (PoE+) support, delivering up to 30W per port.
- PoE Budget: Minimum 700W total PoE power budget
- Switching Capacity: Minimum 200 Gbps switching capacity (non-stacked) with support for stacking to achieve higher throughput (up to 400 Gbps or greater preferred).
- Uplink Ports: Modular or fixed uplinks supporting at least 4x 10 Gigabit Ethernet (10GE) SFP+ ports for high-speed connectivity.
- Layer Support: Layer 2
- **Stacking: Include modules and cables for each switch stacking with a minimum stacking bandwidth of 100 Gbps**
- Reliability: High availability, including **redundant power supplies** and hot-swappable components.
- Software Features: Support for enterprise-grade software capabilities, including network analytics, automation, and integration with modern network architectures (e.g., SD-Access or equivalent).
- Form Factor: 1RU rack-mountable design.
- Interoperability: Must interoperate with existing Cisco equipment in mixed environments.
- **Warranty and Support: Minimum 5-year OEM warranty with Next Business Day replacement and options for extended support and maintenance services.**
- **Include 1 additional 10G Long Range Single Mode SFPs per switch if you NO NOT propose Cisco as your solution.**

Area	Functional and Technical Criteria
Resources	3.1.1 Project Management
	3.1.2.1 Technical Resources – Campus routing and switching
	3.1.2.2 Technical Resources – IP Telephony and Collaboration, Wireless and WAN Optimisation
	3.1.2.3 Technical Resources – Network Firewalling and Security
Proven Experience	3.2.1.1 Campus Network: Access Network References
	3.2.1.2 Campus Network: Core and distribution References
	3.2.1.3 Unified Communications and Collaboration References
	3.2.1.4 Wireless Networking References
	3.2.1.5 Network Security References
	3.1.2.6 Proxy references
TOTALS	