CITY OF TSHWANE METROPOLITAN MUNICIPALITY

TENDER NUMBER:

GICT 03 2025/26

TENDER DESCRIPTION:	TENDER TO PROVIDE, OPERATE AND MAINTAIN THE ICT CORPORATE NETWORK EQUIPMENT, EXISTING HOSTED VOICE AND DATA SOLUTION DEPLOYED, AND THE EXPANSION OF THE EXISTING CORPORATE NETWORK AS AND WHEN FOR A PERIOD OF THREE (3) YEARS

NAME OF BIDDER: ……..

CSD NUMBER: ……..

VENDOR NUMBER (WHERE APPLICABLE) ……..

Prepared by:
City of Tshwane Metropolitan Municipality
Tshwane House
320 Madiba Street
Pretoria CBD
0002
Tel: 012 358 9999

BID CLOSING DATE	**25 SEPTEMBER 2025**

Only bidders registered on the central supplier database (CSD) and with a CSD number will be considered for this tender, as this is a requirement from the National Treasury.

“Note: Bidders are required to submit electronic copies of the bid either by memory stick/USB flash drive/CD/DVD together with the hard copy of the Bid/Proposals”

CITY OF TSHWANE METROPOLITAN MUNICIPALITY

DEPARTMENT: SHARED SERVICES: ICT DIVISION

Bids are hereby invited from suppliers for the following bid:

Bid number	Description	Department	Contact person	Compulsory briefing session	Closing date
GICT 03 2025/26	TENDER TO PROVIDE, OPERATE AND MAINTAIN THE ICT CORPORATE NETWORK EQUIPMENT, EXISTING HOSTED VOICE AND DATA SOLUTION DEPLOYED, AND THE EXPANSION OF THE EXISTING CORPORATE NETWORK AS AND WHEN FOR A PERIOD OF THREE (3) YEARS	Information Communication Technology	Technical enquiries: LeRoy Olivier (leroyo@tshwane.gov.za or 012 358 4994)	Not applicable	25 September 2025 at 10:00

THE DOCUMENT IS DOWNLOADABLE ON THE TSHWANE WEBSITE (www.tshwane.gov.za) and on the E-tender portal.

Each tender shall be enclosed in a sealed envelope that bears the correct identification details and shall be placed in the tender box located at:

"Note: Bidders are required to submit electronic copies of the bid either by memory stick/USB flash drive/CD/DVD together with the hard copy of the Bid/Proposals"

Tshwane House
320 Madiba Street
Pretoria CBD
0002

Documents must be deposited in the bid box not later than **10:00 on 25 September 2025**

Bidders must contact the following officials for any enquiries:

- Technical enquiries: LeRoy Olivier (leroyo@tshwane.gov.za or 012 358 4994)
- Supply chain enquiries: Relebogile Malatswane (RelebogileM@tshwane.gov.za or 012 358 2735)

Bids will remain valid for a period of 90 days after the closing date.

The validity period for the tender after closure is 90 days. The city shall have right and power to extent any tender validity period beyond any initial validity period set and subsequent extensions. SCM shall ensure that an extension of validity is requested in writing from all bidders before the validity expiry date. Extension of validity shall be finalised while the quotations/bids are still valid.

INDEX

VERY IMPORTANT NOTICE ON DISQUALIFICATIONS

A bid that does not comply with the peremptory requirements stated hereunder will be regarded as not being an "acceptable bid", and such a bid will be rejected. An "acceptable bid" means any bid which, in all respects, complies with the conditions of the bid and the specifications as set out in the bid documents, including the conditions as specified in the Preferential Procurement Policy Framework Act, 2000 (Act 5 of 2000) and related legislation as published in *Government Gazette 22549*, dated 10 August 2001, in terms of which provision is made for this policy.

1. If any pages have been removed from the bid document and have therefore not been submitted or if a copy of the original bid document has been submitted.

2. If the bid document is completed using a pencil or Tippex corrections were made, or any other colour ink pen. Only black ink pen must be used to complete the bid document.

3. The bidder attempts to influence or has in fact influenced the evaluation and/or awarding of the contract.

4. The bid has been submitted after the relevant closing date and time.

5. If any bidder who, during the last five years, has failed to perform satisfactorily on a previous contract with the municipality, municipal entity or any other organ of state after written notice was given to that bidder that performance was unsatisfactory.

6. The accounting officer must ensure that, irrespective of the procurement process followed, no award may be given to a person –

   (a) who is in the service of the state;

      i. if that person is not a natural person, of which any director, manager, principal shareholder or stakeholder is a person in the service of the state; or
      ii. who is an advisor or consultant contracted to the municipality in respect of a contract that would cause a conflict of interest.

7. Bid offers will be rejected if the bidder or any of his/her directors are listed on the Register of Bid Defaulters in terms of the Prevention and Combating of Corrupt Activities Act, 2004 (Act 12 of 2004) as a person prohibited from doing business with the public sector.

8. Bid offers will be rejected if the bidder has abused the City of Tshwane supply chain management system.

9. Failure to complete and sign the certificate of independent determination or disclosure of wrong information.

10. Duly Signed and completed MBD forms (MBD 1, 4, 5, 8 and 9) The person signing the bid documentation must be authorised to sign on behalf of the bidder. Where the signatory is not a Director / Member / Owner / Shareholder of the company, an official letter of authorization or delegation of authority should be submitted with the bid document.

11. All MBD documents fully completed and fully signed? By the authorized personnel.

12. False or incorrect declarations on any of the MBD documents will result in the rejection of the bidder.

13 It is the responsibility of the bidder to disclose in MBD4 any interest in any other related companies or business whether they are bidding for this contract. Failure to disclose this interest will result in the rejection of the bid.

14 Joint Ventures (JV) – (Only applicable when the bidder tender as a joint venture)

i. Where the bidder bid as a Joint Ventures (JV), the required or relevant documents under administrative requirements must be provided/submitted for all JV parties. (These include MBD4, MBD5, MBD8, MBD 9, CSD and/ or SARS pin, Confirmation that the bidder's municipal rates and taxes are up to date.)
ii. In addition to the above the bidder must submit a Joint Venture (JV) agreement signed by the relevant parties.
iii. It is a condition of this bid that the successful bidder will continue with same Joint Venture (JV) for the duration of the contract, unless prior approval is obtained from City of Johannesburg.
iv. JV agreement must be complete, relevant and signed by all parties.

Failure to comply with the above will lead to immediate disqualification.

Bidder

CERTIFICATE OF AUTHORITY FOR SIGNATORY

Status of concern submitting tender (delete whichever is not applicable):

COMPANY/PARTNERSHIP/ONE-PERSON BUSINESS/CLOSE CORPORATION/JOINT VENTURE

A. COMPANY

If the bidder is a company, a certified copy of the resolution of the board of directors that is personally signed by the chairperson of the board, authorising the person who signs this bid to do so and to sign any contract resulting from this bid, and any other documents and correspondence in connection with this bid or contract on behalf of the company, must be submitted with this bid.

An example is shown below:

By resolution of the board of directors on ……..…… 20….., Mr/Ms ……..……..... has been duly authorised to sign all documents in connection with Bid Number ……..……

SIGNED ON BEHALF OF THE COMPANY: ……...

IN HIS/HER CAPACITY AS ……....

DATE: …….

SIGNATURE OF SIGNATORY: …….

WITNESSES: 1. ……..…….

2. ……..

B. PARTNERSHIP

The following particulars in respect of every partner must be furnished and signed by every partner:

Full name of partner	**Residential address**	**Signature**
…….....	……	….....
…….....	……	….....
…….....	……	….....

We, the undersigned partners in the business trading as ……....., hereby authorise ……..…… to sign this bid as well as any contract resulting from the bid and any other documents and correspondence in connection with this bid or contract on our behalf.

……	……	……
Signature	**Signature**	**Signature**
……	……	……
Date	**Date**	**Date**

C. ONE-PERSON BUSINESS

I, the undersigned, ……..... , hereby confirm that I am the sole owner of the business trading as …….

……	……
Signature	**Date**

D. CLOSE CORPORATION

In the case of a close corporation submitting a bid, a certified copy of the founding statement of such corporation shall be included with the bid with a resolution by its members, authorising a member or other official of the corporation to sign the documents and correspondence in connection with this bid or contract on behalf of the company.

An example is shown below:

By resolution of the members at the meeting on ……..……..... 20…….... at ……..……, Mr/Ms ……, whose signature appears below, has been duly authorised to sign all documents in connection with Bid Number ……..……..……

SIGNED ON BEHALF OF THE CLOSE CORPORATION: ……..

IN HIS/HER CAPACITY AS: ……..

DATE: …….

SIGNATURE OF SIGNATORY: …….

WITNESSES: **1. ……..**

2. ……..

E. CERTIFICATE OF AUTHORITY FOR JOINT VENTURES

This returnable schedule is to be completed by joint ventures.

We, the undersigned, are submitting this bid offer in joint venture and hereby authorise Mr/Ms ..... , authorised signatory of the company..... , acting in the capacity of the lead partner, to sign all documents in connection with the bid offer and any contract resulting from it on our behalf.

NAME OF FIRM	**ADDRESS**	**DULY AUTHORISED SIGNATORY**
Lead partner		Signature: ..... Name: ..... Designation: .....
		Signature: ..... Name: ..... Designation: .....
		Signature: ..... Name: ..... Designation: .....
		Signature: ..... Name: ..... Designation: .....

CITY OF TSHWANE
IGNITING EXCELLENCE

SHARED SERVICES: ICT DIVISION

TENDER TO PROVIDE, OPERATE AND MAINTAIN THE ICT CORPORATE NETWORK EQUIPMENT, EXISTING HOSTED VOICE AND DATA SOLUTION DEPLOYED, AND THE EXPANSION OF THE EXISTING CORPORATE NETWORK AS AND WHEN FOR A PERIOD OF THREE (3) YEARS

BID NUMBER

(GICT 03 2025/26)

1. INTRODUCTION AND PURPOSE

The purpose of the tender is to provide the City of Tshwane with necessary network and telecoms equipment needed to extend the current network, maintain and improve the current network, monitor, protect and secure the network

2. BACKGROUND

Tender Sections:

- The tender consists of 8 interrelated parts that together will provide a full Voice and Data Networking solutions and related hardware, software to thus be deployed. These sections are:
  - Part 1: Introduction and General Background information
  - Part 2: General Specifications applicable to all parts of the tender
  - Part 3: Expansion of the current network: Supply, Delivery, Deployment, Configuration and Maintenance of New Equipment in the Network as and when required
  - Part 4: Operate and Maintain the existing Alcatel/Huawei network.
  - Part 5: Compliancy of any new Equipment & Solutions with regards the current deployed Network Solutions
  - Part 6: Service Level Agreement (SLA) applicable to Part 3 and 4 of this tender submission
  - Part 7: Price Schedules
- **Duration of the contract**

  The successful bidder will be appointed for a period of 3 years (36 months). The scope includes the training of technical users, maintenance and support, software and hardware.

  The successful bidder should note that the migration and implementation of the service must be completed and operational within a maximum of 3 (three) months from the award date which forms part of the 3 year (36 Month) agreement.

  Successful bidder shall be subjected to SCM annual review to ensure that the tendered prices are still in line with the market related prices and all savings generated by unit price decreases be passed along to Council.

3. PROJECT PURPOSE AND SCOPE

Purpose

The City of Tshwane (CoT) is dependent on Information and Communication Technology (ICT) in almost every segment of its operations.

Bidders are invited to submit a proposal to the City of Tshwane (CoT) to provide such hardware and support services to ensure reliable functioning and sufficient capacity exist for all the CoT communication infrastructure and related services. The sevices entail the supply and maintenance of the ICT Corporate Alcatel network equipment(that is open standards compliance) as well as the expansion of the existing network. The purpose of this document is to:

- Provide the prospective Bidder/s with sufficient information to understand and respond to the requirements.

- Ensure that comparable information is obtained from Bidders.
- Provide a structured framework for the subsequent quantitative and qualitative evaluation of proposed solutions.

Scope

To provide and maintain the CoT with the necessary network and telecoms equipment needed to extend the current network, to maintain and improve the current network, to monitor, protect and secure the network. The document will have the following parts:

- Part 1: Introduction and General Background information
- Part 2: General Specifications applicable to all parts of the tender
- Part 3: Expansion of the current network: Supply, Delivery, Deployment, Configuration and Maintenance of New Equipment in the Network as and when required
- Part 4: Operate and maintain the existing Alcatel/Huawei network.
- Part 5: Compliancy of any new Equipment & Solutions with regards the current deployed Network Solutions
- Part 6: Service Level Agreement (SLA) applicable to Part 3 and 4 of this tender submission
- Part 7: Price Schedules

The bidders must include CVs of certified personnel to deploy new equipment and maintain the current network equipment for the duration of the contract. The pricing schedule is mostly based on the existing Alcatel/Lucent and Huawei Product range deployed and used within the City.

ACRONYMS LIST

Acronym	Meaning
AAA	Authentication, Authorization And Accounting
AC	Alternating Current
ACL	Access Control List
ACLMAN	Access Control List Manager
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
ASA	Authenticated Switch Access
ASCII	American Standard Code for Information Interchange
ASIC	Application-Specific Integrated Circuit

Acronym	Meaning
BC	Business Case
BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Unit
CAC	Call Admission Control
CAT5e	Category 5 Cable
CAT6	Category 6 Cable
CBC	Cipher Block Chaining
CBD	Central Business District
CCMP	Counter Mode Cipher Block Chaining Message Authentication Code Protocol
CE	Customer Edge
CLI	Command Line Interface
CPIX	Consumer Price Index
CPU	Central Processing Unit
CV	Curriculum Vitae
DC	Direct Current
DCBX	Data Center Bridging Capabilities Exchange Protocol
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	De-Militarized Zones
DNS	Domain Name System
DoS	Denial Of Service
DPNSS	Digital Private Netrowk Signaling System
DSS1	Digital Subscriber Signalling System No 1
DTE/DCE	Data Terminal Equipment/Data Circuit-Terminating Equipment
DWDM	Dense Wavelength Division Multiplexing
ECMP	Equal Cost Multipath Protocol

Acronym	Meaning
ERP	Ethernet Ring Protection
ETS	Enhanced Transmission Selection
FCAPS	Fault, Configuration, Administration, Performance and Security
FCC	Federal Communications Commission
FCoE	Fibre Channel over Ethernet
FIP	Fibre Channel over Ethernet Itialization Protocol
FTP	File Transfer Protocol
Gig	Gigabit
GM	Group Mobility
GRE	Generic Routing Encapsulation
HIC	Host Integrity Check
HOL	Head Of Line
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection Systems
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IP PBX	Internet Protoco Private Branch Exchange
IPSEC	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
kbps	kilo bits per second

Acronym	Meaning
L2	Layer 2
L2TP	Layer 2 Tunneling Protocol
L3	Layer 3
L4	Layer 4
LACP	Link Aggregation Control Protocol
LAN	Local Area Networks
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol
LPS	Learned Port Security
MAC	Media Access Control
Mb	Mega Bits
Mbps	Mega Bits Per Second
MC-LAG	Multi-Chassis Link Aggregation Group
MD5	Message Digest 5
MDI/MDIX	Medium Dependent Interface/MDI Crossover
MFMA	Municipal Finance Management Act
MFR	Multilink frame relay
MIB	Management Information Base
MISTP	Multiple Instance Spanning Tree Protocol
MLPPP	Multilink PPP
MPLS	Multiprotocol Label Switching
MPPE	Microsoft Point-to-Point Encryption
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAP	Network Access Policy
NAT	Network Address Translation

Acronym	Meaning
NETBEUI	NETBIOS Extended User Interface
NIC	Network Interface Card
NMS	Network Management System
NOC	Network Operations Center
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
OHSA	Occupational Health And Safety Act
OS	Operating System
OSPF	Open Shortest Path First
OTDR	Optical Time Domain Reflectometer
P/S	Power Supply
PBX	Private Branch Exchange
PC	Personal Computer
PFC	Priority-based Flow Control
PKI	Public Key Infrastructure
PoE	Power Over Ethernet
PSU	Power Suply Unit
QoS	Quality of Service
Qsig BC	ISDN Based Signalling Protocol Basic Calling
Qsig GF	ISDN Based Signalling Protocol Generic Function
RADIUS	Remote Authentication Dial-In User Service/Server
RFP	Request For Proposal
RIP	Routing Information Protocol
RMON	Remote Monitoring
RoHS	Restriction on Hazardous Substances
RTSP	Real Time Streaming Protocol

Acronym	Meaning
RU	Rack Units
SCM	Supply Chain Management
SFN	Software Defined Networking
SFTP	Secured File Transfer Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLB	Server Load Balancing
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SP	Service Provider
SPI	Smart Plug In
SSH	Secure Shell
SSID	Service Set Identifider
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TACACS	Terminal Access Controller Access-Control System
TAPI	Telephony Application Program Interface
TCO	Total Cost Of Ownership
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
UTM	Unified Threat Management

Acronym	Meaning
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Networks
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRF	Virtual Routing And Forwarding
VRPP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
WRR	Weighted Round Robin
WSDL	Web Service Description Language

4. DELIVERABLES

To provide and maintain the CoT with the necessary network and telecoms equipment needed to extend the current network, to maintain and improve the current network, to monitor, protect and secure the network. The document will have 8 parts:

- **Part 1: Introduction and General Background Information**
- **Part 2: General Specifications applicable to all parts of the tender:** Provides for general service related specs that applies to all aspects of this tender.
- **Part 3: Expansion of the current network and services provided in lieu of the V & D network deployed:** This includes the Supply, Delivery, Deployment, Configuration and Maintenance of New Equipment and Services in the Network as and when required. All equipment offered must comply with the technical specifications as provided for in this document.
- Bidders can submit equivalent and or similar products as long as it is 100% conforming to the technical specification of that particular item and 100% compatible with existing equipment that is open standards. Model numbers and technical pamphlets to be supplied. Any bidders submitting a bid, must have the highest possible partnership with the OEM of the proposed equipment.

- Deployment of a hosted voice and data network in line with the latest international trends whereby more services are provided on cloud hosted solutions to bring the deployed networking solutions in Council in line with international trends and developments. The currently deployed cloud hosting solutions must be supported and any Service Provider submitting a tender in this regard. The current cloud hosting platform/service must be continued in its current format and services provided by it.

- **Part 4: Operate and Maintain the Current Voice and Data Network:** In the main, the tender is about support and maintenance of the existing data and voice network and peripheral and other related services thus to be provided. The City has invested heavily in the Alcatel/Lucent and Huawei range of products and to protect this investment, the successful bidder must be able to maintain the current Alcatel/Lucent and Huawei products on the corporate network. This will also include the Voice (Fixed Line & Cellular Services) and Data Communications Audit service.

- Continued use of the current deployed hosted voice and data network as deployed must be continued in Council in its current format and by the current OEM, to ensure that the services currently deployed in regions 5 and 7 not be interrupted again. Should this be done it will continue to comply with the current latest international trends whereby more services are provided on cloud hosted solutions to bring the deployed networking solutions in Council in line with international trends and developments. The currently deployed cloud hosting solutions must be supported and any Service Provider submitting a tender in this regard.

- **Part 5: Compliancy of any new Equipment & Solutions with regards the current deployed Network Solutions:** This part of the tender is about the expansion of/to the existing data and voice network and peripheral and other related services thus to be provided, and the maintenance and support of any suchlike newly deployed equipment. The City has invested heavily in the Alcatel/Lucent and Huawei range of products and to protect this investment, and to ensure data integrity and continued QOS, the successful bidder must be able to maintain the current Alcatel/Lucent and Huawei products on the corporate network as well as add the same range of products on this tender as requested. This will also include the Voice (Fixed Line & Cellular Services).

- **Part 6: Service Level Agreement (SLA) applicable to this tender submission.**

- **Part 7: Price List for all equipment and services requested**

5. STAGES OF EVALUATION

The following tender will be evaluated according to the following stages:

Stage 1: Administrative Compliance
Stage 2: Mandatory Compliance
Stage 3: Functionality Criteria
Stage 4: Preference Point System

STAGE 1: ADMINISTRATIVE COMPLIANCE
All the bids will be evaluated against the administrative responsiveness requirements as set out in the list of returnable documents.

Compulsory Returnable Documentation (Submission of these are compulsory)	**Submitted (YES or NO)**	**Checklist (Guide for Bidder and the Bid Evaluation Committee)**
a) To enable The City to verify the bidder's tax compliance status, the bidder must provide; • Tax compliance status PIN. or • Central Supplier Database (CSD)		Tax status must be compliant before the award.
b) A copy of their Central Supplier Database (CSD) registration; or indicate their Master Registration Number / CSD Number;		CSD must be valid.
c) Confirmation that the bidding company's rates and taxes are up to date: Original or copy of Municipal Account Statement of the Bidder (bidding company) not older than 3 months and account must not be in arrears for more than ninety (90) days; or ,signed lease agreement or In case of bidders located in informal settlement, rural areas or areas where they are not required to pay Rates and Taxes a letter from the local councillor confirming they are operating in that area		Was a Municipal Account Statement or landlord letter provided for the bidding company? The name and / or addresses of the bidder's statement correspond with CIPC document, Address on CSD or Company profile? Are all payment(s) up to date (i.e. not in arrears for more than 90 days?

Compulsory Returnable Documentation (Submission of these are compulsory)	**Submitted (YES or NO)**	**Checklist (Guide for Bidder and the Bid Evaluation Committee)**
d) In addition to the above, confirmation that all the bidding company's owners / members / directors / major shareholders rates and taxes are up to date: • Original or copy of Municipal Account Statement of all the South African based owners / members / directors / major shareholders not older than 3 months and the account/s may not be in arrears for more than ninety (90) days; or a signed lease agreement of owners / members / directors / major shareholders or In case of bidders located in informal settlement, rural areas or areas where they are not required to pay Rates and Taxes a letter from the local councillor confirming they are residing in that area		Was a Municipal Account Statement or landlord letter provided for the bidding company? The name and / or addresses of the bidder's statement correspond with CIPC document, Address on CSD or Company profile? Are all payment(s) up to date (i.e. not in arrears for more than 90 days?
e) Duly Signed and completed MBD forms (MBD 1, 4, 5, 8 and 9) The person signing the bid documentation must be authorized to sign on behalf of the bidder. Where the signatory is not a Director / Member / Owner / Shareholder of the company, an official letter of authorization or delegation of authority should be submitted with the bid document. **NB: Bidders must ensure that the directors, trustees, managers, principal shareholders, or stakeholders of this company, declare any interest in any other related companies or business, whether or not they are bidding for this contract. *See Question 3.14 of MBD 4. Failure to declare interest will result in a disqualification***		All documents fully completed (i.e. no blank spaces)? All documents fully signed by (any director / member / trustee as indicated on the CIPC document, alternatively a delegation of authority would be required? Documents completed in black ink (i.e. no "Tippex" corrections, no pencil, no other colour ink, or **non-submission of the MBD forms**, will be considered)?
f) Audited Financial Statements for the most recent three (3) years or Audited Financial Statements from date of existence for companies less than three years old.		Applicable for tenders above R10m in conjunction with MBD 5)

Compulsory Returnable Documentation (Submission of these are compulsory)	**Submitted (YES or NO)**	**Checklist (Guide for Bidder and the Bid Evaluation Committee)**
NB: The bidder must submit signed audited annual financial statements for the most recent three years, or if established for a shorter period, submit audited annual financial statements from date of establishment. If the bidder is not required by law to prepare signed annual financial statements for auditing purposes, then the bidder must submit proof that the bidder is not required by law to prepare audited financial statements.		Are Audited financial statements provided (Audited financials must be signed by auditor) Or proof that the bidder is not required by law to prepare audited financial statements.
g) Joint Ventures (JV) – (Only applicable when the bidder tenders as a joint venture) Where the bidder bids as a joint venture (JV), the required or relevant documents as per (a) to (f) above must be provided for all JV parties. In addition to the above the bidder must submit a Joint Venture (JV) agreement signed by the relevant parties. **NB**: It is a condition of this bid that the successful bidder will continue with the same Joint Venture (JV) for the duration of the contract unless prior approval is obtained from the City.		If applicable. JV agreement provided? JV agreement complete and relevant? Agreement signed by all parties? All required documents as per (i.e. a to f) must be provided for all partners of the JV.
h) Bidder attended a compulsory briefing session where applicable		A compulsory briefing register must be signed by the bidder. **Bidders will be disqualified should they fail to attend compulsory briefing session**
i) Pricing schedule (All items must be quoted for in pricing schedule and if not, all items are quoted the bidder will be disqualified). Unless the tender is awarded per item or per section		Incomplete pricing schedule results in totals being incomparable.

Compulsory Returnable Documentation (Submission of these are compulsory)	Submitted (YES or NO)	Checklist (Guide for Bidder and the Bid Evaluation Committee)
where the bidder only quoted the items or sections, they are interested in.		Bidder must be disqualified. **Bidder will be disqualified should they make corrections on the price schedule without attaching a signature or initialising thereto.** **Bidder will be disqualified should they use tippex/ correction ink, on the price schedule.**

STAGE 2: MANDATORY REQUIREMENTS

Bidders must comply with the following requirements as failure will result in the disqualification of the bid from further evaluation:

- Provide a valid, *Individual Electronic Communications Service Licence (IECS) and Individual Electronic Communications Network Service Licence (IECNS)* ICASA License*, issued by the Independent Communications Authority of South Africa (ICASA),* in terms of the service to be provided to the City.
- Supply a letter of accreditation by original equipment manufacturer(s) (OEM). The personnel must be certified by the OEM to work on their network & telecoms equipment.

- Proof of Public Liability to the value of R3 million or a letter of intent between the bidders and an accredited financial service provider.
- **Key Personel requirements**
  The minimum years of experience that is expected of all technical personnel is two (2) years. The bidders must submit as part of the tender document the technical personel's Curriculum Viteas that clearly indicate the relevent experience.

  Only certified professionals, on the highest possible certification from the particular OEM, are allowed to configure data and voice equipment, in this case Alcatel/Lucent and Huawei.

The required qualifications/ certifications must be valid and certified and submitted with the tender document.

The following is required as a minimum:

- **Project Manager**:
- Certificate in Project Management,
- ITIL Foundation,
- Intermediate Excel Skills,

Excellent understanding of ICT networking principples, ie, Data & Voice and WiFi networking.

- **Radio Technician:** A National Diploma or B-Tech in Electronic Engineering, Telecommunications, or related field or equivalent.
- **Network Technician:**
- Network +
  Relevant OEM certifications.

- **Network/Voice Engineer:**
- A bachelor's degree in computer science, information technology, or a related qualification.
- Additionally, professional certifications like Network+ and relevant OEM certifications
- **Security Engineer**:
- A bachelor's degree in computer science, information technology, or a related field is required.
- Security Certifications: Relevant certifications like CompTIA Security+, Certified Ethical Hacker (CEH), or vendor-specific certifications (e.g., Check Point certifications) are required.

Note: The City of Tshwane reserve a right to confirm validity of the documents submitted, any invalid documents will result in the disqualification of the bid from further evaluation.

STAGE 3: FUNCTIONALITY CRITERIA

Bidders complying with ALL the requirements on the 2st stages will be evaluated against the Functional Evaluation Criteria as set below. Bidders must score a minimum of 70 points or 70% more out of a total 70 points allocated for Functional Criteria. Bidders that score less than 70 points or 70% will be disqualified and will not be evaluated further.

CRITERIA	SUB-CRITERIA	SCALE	WEIGHT	HIGHEST POSSIBLE SCORE
Company key personnel experience. The Service Provider must provide proof of its personnel's experience level on similar networks as Council has deployed. Personnel certification for proposed OEM support. The	Project Manager or coordinator: 2 to less than 3 years 3 to 4 to less than years 4 to 5 to less than years 6 and above	1 2 3 4	5	20

personnel must be certified by the OEM to work on their network & telecoms equipment. The OEM uses their own firmware/operating systems and the technicians must be trained to work on it. This will apply to the existing equipment base deployed as well as all new equipment thus deployed. *Attach curricula vitae of professional team members.*	Admin Support Officer 2 to less than 3 years 3 to 4 to less than years 4 to 5 to less than years 5 and above	1 2 3 4	5	20
	Service Related Technicians 2 per tender/service section 2 to less than 3 years 3 to 4 to less than years 4 to 5 and more years 5 and above years	2 3 4 5	2	10
Bidder's previous performance and experience in similar sized networks. *Bidders to provide references on work successfully completed. These references must specifically state the periods of experience and whether the person supplying the reference were satisfied with the work completed.*	Services of similar projects (at least 15 000 users and more, fully networked work premises/offices of at least 450 satellite offices or more) for a period of 5 years or more 2000 to 5000 Users 5001 to 7500 Users 7501 to 15 000 Users	1 3 5	4	20
All references must be on the letterhead of the company supplying the reference with contactable reference	References letters for of similar projects 2 reference letters 3 reference letters 4 or more reference letters	1 3 5	3	15

	Providing a Hosted Voice and Data network service to parallel to a legacy Voice and Data network (Hybrid System) for 1000 – 2000 user 2001 – 3999 users 4000 – 5000 users	 1 3 5	3	15
HIGHEST POSSIBLE SCORE				100

STAGE 4: PREFERENCE POINT SYSTEM

The preferential point system used will be the 80/20 points system in terms of the Preferential Procurement Policy Framework Act, 2000 (Act 5 of 2000) Regulations 2022.

- 80 points for price
- 20 points for Specific goals

SPECIFIC GOALS

- **Bidders are required to submit supporting documents for their bids to claim the specific goal points.**
- **Non-compliance with specific goals will not lead to disqualification but bidders will not be allocated specific goal points. Bidders will score points out of 80 for price only and zero (0) points out of 20 for specific goals.**
- **Cot shall act against any bidder or person when it detects that the specific goals were claimed or obtained on a fraudulent basis.**

Specific goals	**80/20 preference point system**	**Proof of specific goals to be submitted**
BB-BEE score of companies • Level 1 • Level 2 • Level 3 • Level 4 • Level 5 • Level 6 • Level 7 • Level 8 • Non-compliant	• 8 Points • 7 Points • 6 Points • 5 Points • 4 Points • 3 Points • 2 Points • 1 Point • 0 Points	Valid Certified copy of BBBEE certificate. Sworn Affidavit for B-BBEE qualifying small enterprise or Exempt Micro Enterprises or CIPC BBBEE certificate.
EME and/ or QSE	2 Points	Valid Sworn affidavit for B-BBEE qualifying small enterprise or Exempt Micro Enterprises or CIPC BBBEE certificate
At least 51% of Women-owned companies	2 Points	Certified copy of Identity Document/s **and** proof of ownership (Sworn affidavit for B-BBEE qualifying small enterprise or Exempt Micro Enterprises, CIPC registration or any other proof of ownership)
At least 51% owned companies by People with disability	2 Points	Medical Certificate with doctor's details (Practice Number, Physical Address, and contact numbers) and proof of ownership

Specific goals	80/20 preference point system	Proof of specific goals to be submitted
		(Sworn affidavit for B-BBEE qualifying small enterprise or Exempt Micro Enterprises, CIPC registration or any other proof of ownership
At least 51% owned companies by Youth	2 Point	Certified copy of Identity Document/s **and** proof of ownership (Sworn affidavit for B-BBEE qualifying small enterprise or Exempt Micro Enterprises, CIPC registration or any other proof of ownership
Local Economic Participation • City of Tshwane • Gauteng • National	 4 Points 2 Points 1 Point	Municipal Account statement/Lease agreement.

6. SUBCONTRACTING/ALLOCATION SPLITTING OF DIFFERENT PARTS OF THE TENDER

6.1 Subcontracting

According to section 47 of The City of Tshwane Supply Chain Management policy 2024/25.
When subcontracting:
The City shall obligate main contractors or service providers to engage targeted enterprises in the performance of their contracts incorporating resource specifications. These will be made a condition of the tender for the city to implement at project management level.
In cases that the city decides to unbundle the tender to appoint different service providers to an extend that the contract value per service provider does not exceed 30million then the provision of sub-contracting will not be applicable.

(1) Sub-contracting must be subjected to approval by the city manager. The appointed service provider must source competent and capable service providers and where applicable be registered with the relevant body and submit a list of sub-contractors for approval to the City of Tshwane.
(2) Sub-contracting entity should have an equal B-BBEE level status or higher than the main contractor.
(3) Minimum of 30% can be sub-contracted for tenders above 30 million.

(5) Local economic participation should be given priority when making a list of potential subcontractors available.

City of Tshwane Participants with specific attention for the region in which the contract is to be executed should be given first priority and the below

competent and capable designated groups should be prioritized

An EME or QSE

o An EME or QSE which is at least 51% Black Owned

o An EME or QSE which is at least 51% Owned by Black youth

o An EME or QSE which is at least 51% Black Women Owned

o An EME or QSE which is at least 51% owned by black people with

disabilities.

o An EME or QSE which is 51% owned by black people living in rural or

underdeveloped areas or townships

o A cooperative which is at least 51% owned by black people

o An EME or QSE which is at least 51% owned by black people who are

military veterans; or

o More than one of the categories referred to in paragraphs (a) to (h).

Should subcontractors within Tshwane not be identified, the appointed service

provider can extend the list of subcontractors to:

• Gauteng Participants

• National participants

Documentation required

Bidders must submit proof of subcontracting agreement, between the main tenderer and the subcontractor. Proof of subcontracting arrangement may include a subcontracting agreement between main bidders and the subcontractor.

Main contractors/ suppliers are discouraged from subcontracting with their subsidiary companies as this may be interpreted as subcontracting with themselves and / or using their subsidiaries for fronting. Where primary contractor subcontracts with a subsidiary this must be declared in tender documents.

The main contractor is also responsible therefore that the proposed subcontractor is fully able to do the work said subcontractor is appointed for.

Tenders that do not meet subcontracting requirements are considered as being not acceptable tenders and must be disqualified and may not be considered for further evaluation or award.

Expanded services provided to Council

- This tender has been expanded to provide services not catered for in the previous tender, currently in use. Thus provision has been made to allow for Hosted Voice and Data services.
- The initial deployment hereof is in Regions 5 and 7. Provision for this will have to be made in the submission to Council.

7. TYPE OF AGREEMENT REQUIRED

ICT tenders, as with this tender has a SLA provided for in the tender. This is provided for in Part ? of the tender wherein a service relevant SLA per section of the tender is required. As this tender consists of ? different aspects of services to be provided to Council, each section (Service) has its own unique relevant SLA applicable to it provided for in the detailed Bid Specifications.

8. VALIDITY PERIOD

The validity period for the tender after closure is 90 days. The city shall have right and power to extent any tender validity period beyond any initial validity period set and subsequent extensions. SCM shall ensure that an extension of validity is requested in writing from all bidders before the validity expiry date. Extension of validity shall be finalised while the quotations/bids are still valid.

9. MATERIAL NUMBER

The material and equipment to be acquired on this tender will be as per the attached pricing schedules Part 2 to 2.8 of **the attached tender Price List (Part 10)**

10. PRICING SCHEDULE

The pricing schedules is in the form of a locked spreadsheet, wherein the bidder must provide their per item cost.

The sub-total summary from the spreadsheet price schedule must be brought forward by the bidder and the totals contained therein must be completed in the below summary schedule.

This must be done for the current equipment deployed as well as the alternative equipment solution as provided for on the price list.

Depending on which solution was used by the individual bidder and in which column the pricing was provided.

Bidders are to printout the completed excel spreadsheet and attach the completed pricing as the pricing schedule. The pricing schedule must be submitted along with the completed tender document. The below summary must be completed in black ink pen.

AWARD

It is the intention of the City to appoint one service provider.

SUMMARY PRICE SCHEDULE

THE FOLLOWING SUBTOTALS MUST BE CARRIED FROM THE ANNEXTURE PRICING SCHEDULE

BIDDERS ARE TO NOTE THAT FOR EVALUATION PURPOSES THE CITY WILL USE CURRENT EQUIPMENT SOLUTION OR THE ALTERNATIVE SOLUTION EQUIPMENT. BIDDERS ARE TO BID ON EITHER THE CURRENT EQUIPMENT SOLUTION OR ALTERNATIVE SOLUTION EQUIPMENT.

Item	Description	Current Equipment: Unit Price: Subtotal (Ex Vat)	Alternative Solution Equipment: Unit Price: Subtotal (Ex Vat)
1	Switches and Voice		
2	Maintenance		
3	Equipment		
4	Firewalls		
5	Electrical		
6	Testers		
7	Training		
8	Resources		
9	Hosting		
10	NAC		
	Subtotal Excl. VAT		
	VAT 15 %		
	TOTAL INC VAT		

11 MARKET ANALYSIS

The city of Tshwane reserves the right to conduct market analysis. Should the city exercise this option, where a tenderer offers a price that is deemed not to be viable to supply goods or services as required, written confirmation will be made with the tenderer if they will be able to deliver on the price, if a tenderer confirm that they cannot, The tenderer will be disqualified on the basis of being non-responsive.

On confirmation by the bidder, a tight contract to mitigate the risk of non-performance will be entered into with the service provider. Further action on failures by the supplier to deliver will be handled in terms of the contract including performance warnings and listing on the database of restricted suppliers.

The city further reserves the right to negotiate a market related price with a tenderer scoring the highest points. If the tenderer does not agree to a market-related price, the city reserves the right to negotiate a market-related price with the tenderer scoring the second highest points, if the tenderer scoring the second highest points does not agree to a market-related price, negotiate a market-related price with the tenderer scoring the third highest points. If a market-related price is not agreed, the city reserves the right to cancel the tender.

12. DRAFT SERVICE LEVEL AGREEMENTS

The draft SLA per section of this tender is provided for in Part E of the Tender Specifications. Specification to be accompanied by draft service level agreements, as is provided for in the tender documents and eventual service providers submissions to Council

Part 2: General Specifications applicable to all parts of the tender

Part 2: GENERAL SPECIFICATIONS

2.1 Applicability

General specifications are applicable to all the parts of the Tender.

2.2 Compatibility

Switches and equipment must be hundred percent (100%) compatible with the existing system based network (open standards). The tenderer should include the installation material wherever required. All essential items including cables (inclusive of power & stacking cables), connectors, cage nuts, etc. needed for the smooth operation of the equipment shall be assumed to have been included in the quoted price/items if these have not been quoted separately.

2.3. Programs, Projects, Maintenance and Audit Services

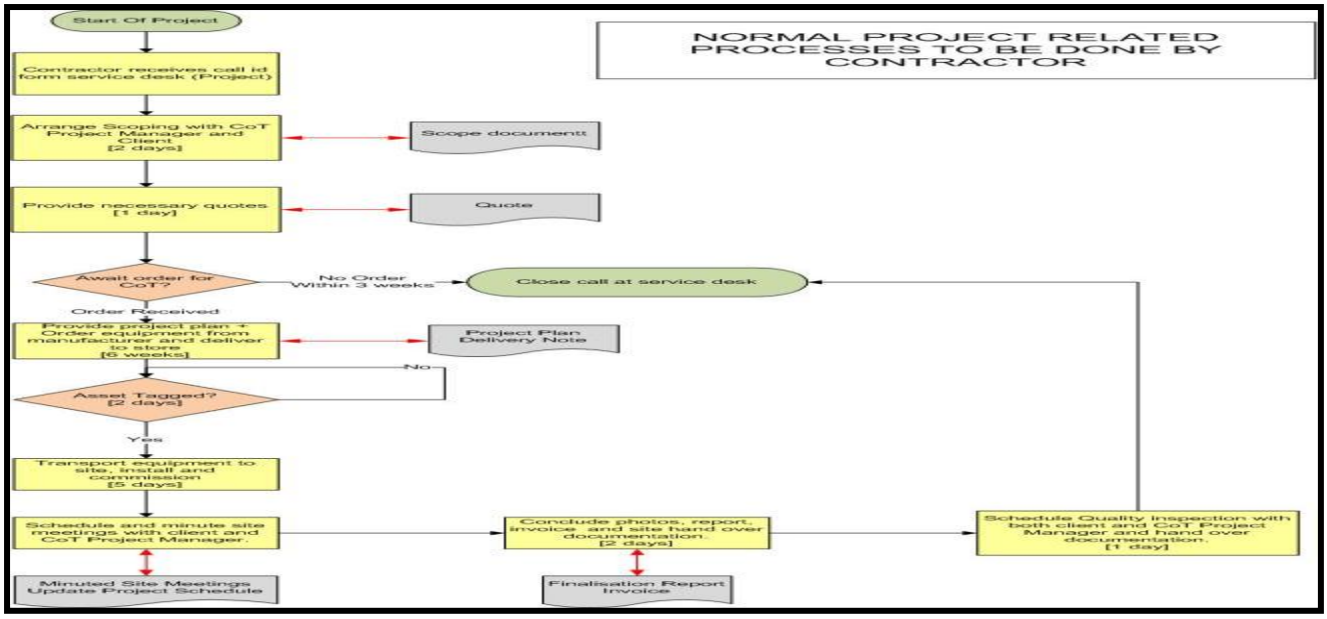
2.3.1 Projects (Extending The Network)

In the main, the tender is about supporting the current data and voice networks. The switches and associated transceivers like Gigabit Interface Converters, shall be delivered, installed, configured and commissioned at the various sites as per the price list (bill of quantities) as and when required. Although cabling and associated cabinets are not part of this contract, the connecting fiber leads shall be supplied and installed by the successful contractor along with the switch or switches.

The contractor shall also patch the users on the switch (patch cables will be supplied by others) and also ensure that every user is connected to the network before signing off on the site. Patching shall be done neatly and a quality inspection will be done by CoT personnel before payment will be made for a specific site. Detailed project role out plans must be supplied as to manage the process from start to finish, when new equipment roll-out is required.

As soon as the project is completed, a final Project Close-Off Report must be submitted to Council by the approved Service Provider Project Manager, within 2 weeks from the go-live to officially hand the site over to relevant Director responsible for ICT infrastructure in Council to allow for the official hand-over to the maintenance teams.

The process is described in the flow chart below, mainly to give an indication of the process but also to list the required documents and to indicate the time frames associated with this. The process can be changed by CoT at any time during the contractual period to incorporate additional requirements or changes.



2.3.2 Programs

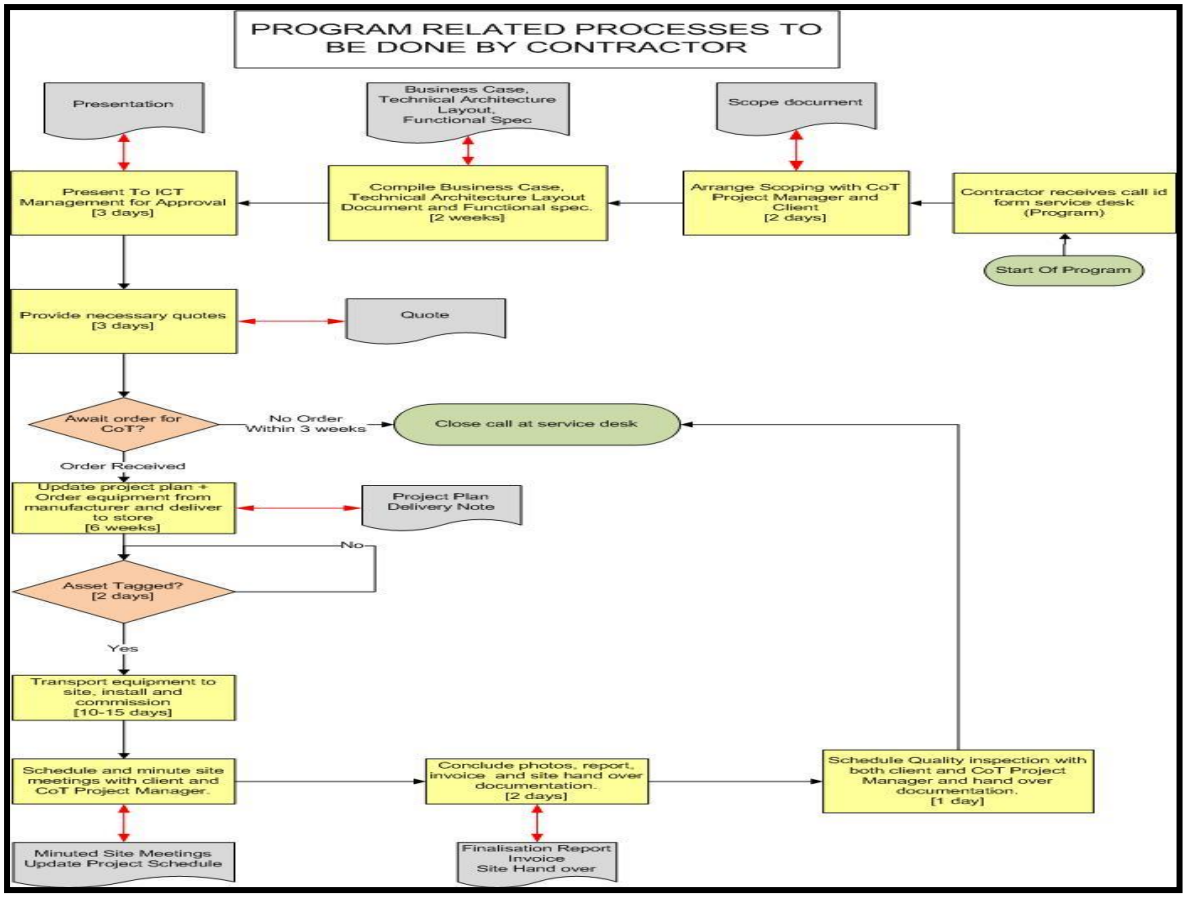
For the purpose of this document, Programs will be defined as special projects that might be required from time to time. CoT will define these special projects. Business cases (BC) are applicable where the BC are required by CoT for strategic decision making and to determine infrastructure technology deployment. Project proposals by the contractor applies once the CoT has determined the scope of a project to meet the specific requirement CoT might have at that stage, with limited scope based on a strategic decision.

The Programs will have similar steps than the projects, but in addition need the following documentation that must be completed by the contractor and must be submitted to ICT Management for approval:

- Business Case
  - Cover page
  - Table of contents
  - Authority Signatures
  - Executive Summary
  - Business Needs and Desired Outcomes
    - Strategic environment
    - Strategic Fit
    - Detailed description of business need
    - Scope
  - Analysis and Recommendations
    - Evaluation Criteria
    - Possible Options
    - Viable options
  - Viable Options

        - Strategic Alignment
        - Costs
        - Cost Benefit Analysis and return on investment
        - Implementation and capacity considerations
        - Impact
        - Risks
        - Policy considerations
        - Advantages and disadvantages
    - Recommendation
    - Managing the Investment
    - Project Management Strategy
    - Appendices (if applicable)
    - Glossary
- Technical Architecture Layout
    - Containing all technical detail of the project
    - Hardware details
        - Switch specifications
        - Servers, Storage, Backup and Archiving requirements
        - Necessary SQL design templates (where applicable)
        - Infrastructure requirements i.e. cabling, electrical, air-conditioning, etc.
    - Layout diagrams/drawings of the various components
    - Detailed quotes
    - Risk Matrix
    - Project Plan
- Functional Specification for example the functional requirements of a Call Centre – client to sign off. Said FS refers to the solution functionality as determined by the Client, and excludes technical requirements.

The process is described in the flow chart below, mainly to give an indication of the process but also to list the required documents and to indicate the time frames associated with this. The process can be changed by CoT at any time during the contractual period to incorporate additional requirements or changes.



2.3.3 Maintenance

The successful Tenderer must have sufficient maintenance stock to enable immediate replacement of equipment (whether the equipment is covered by an SLA or not).

Planned down time for equipment replacements and for any network changes must be done in accordance with/in collaboration with CoT's Change Control Policy's (basic ITIL principles).

Faulty equipment under warranty/SLA:

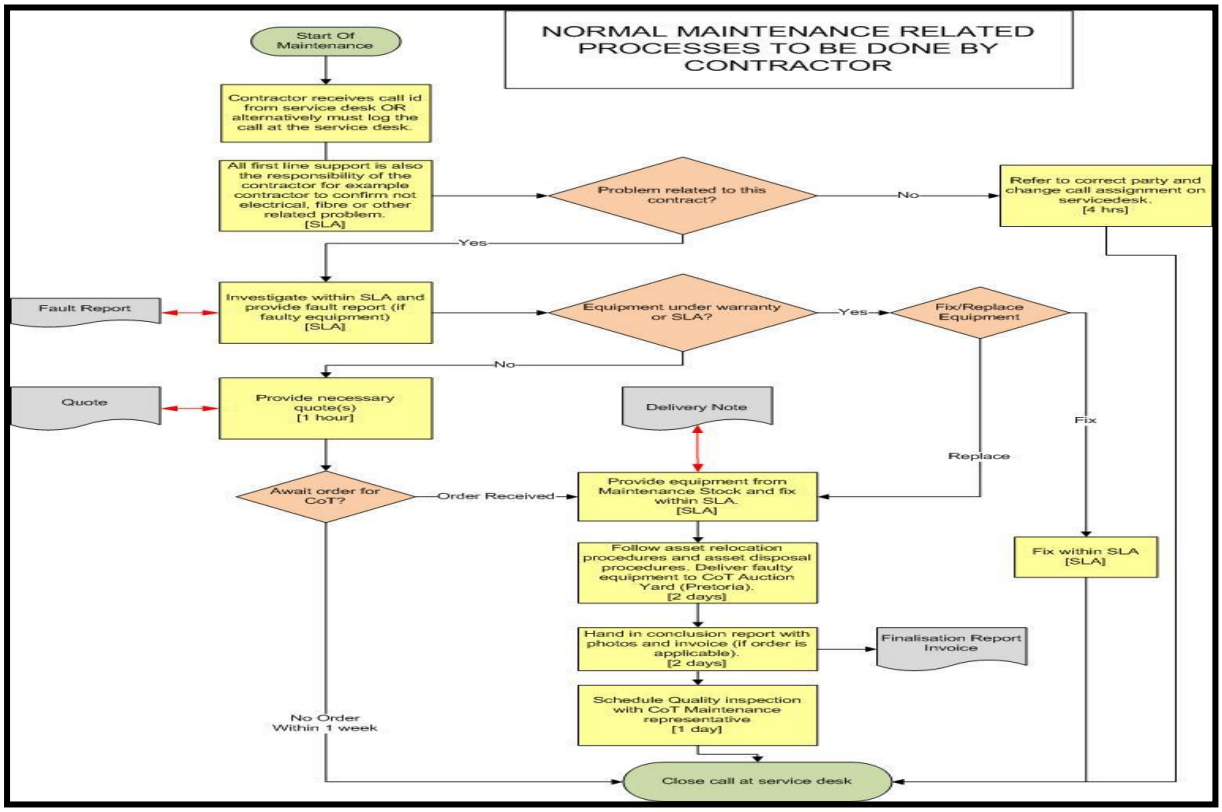
Faulty equipment under warranty and SLA must be replaced immediately under said SLA without any additional cost to CoT. Faulty equipment under warranty and SLA will then be repaired off-site by the Service Provider and returned to site within a period of 6 weeks. A fault report must accompany the equipment. Should the equipment not be repairable, then replacement equipment must be provided without any charges to the CoT.

Faulty older equipment not covered by warranty/SLA:

Faulty equipment must be disposed by the official CoT asset disposal procedures and such equipment must be delivered to the Auction Yard in the CBD by the appointed tenderer.

Faulty equipment that is not covered by warrantee/SLA will be ordered via the official Procurement procedures. However, such equipment must also be replaced immediately with loan stock to ensure continuity of service. It will be expected from the Service Provider to bi-annually provide to Council an equipment replacement plan, with regards to equipment in this tender scope.

New/replacement equipment must first be delivered to Dam Stores in Centurion (or alternative storage facility nominated by the CoT) where it will be asset tagged and must meet CoT's MFMA requirements with regards to delivery and payment issues, including all relevant insurances. Said equipment must then be delivered to site where equipment must be installed, configured and commissioned. All cost related to delivery to the store and final site must be included in the costing.



2.4. Overview Of Current CoT Data Backbone Infrastructure

Solution proposed must be able to fully integrate to the current system and support the same level of functionality and seamless integration of all functions and features. This will be the sole responsibility of the Service Provider to ensure functionality.

2.4.1 Data Platforms

The CoT have developed a carrier grade, high availability, secure and easy to manage infrastructure to carry IP data, voice and video. All applications are thus supported across the existing 1 and 10 Gigabit Ethernet Backbone. Edge or user accesses are all based on Ethernet standards ranging in speeds depending on the need. All networking equipment delivers Layer 2/3/4 switching functionality. The submitter will need to augment the existing high availability IP infrastructure to deliver Value Added Services to CoT existing and future users.

The physical infrastructure is mainly based on fiber optic connectivity (multimode, single mode and long haul single mode) with copper cabling, Cat5e, Copper 10 and 6 (Cat = Category) and wireless links used as required.

The network enables extensive quality of service to support existing response-time critical applications and multimedia services like voice over IP with provision for video on demand and conferencing systems.

Radio links exist ranging from 11 Mbps to 300 Mbps. Wi-Fi (Aruba) equipment is deployed at several sites including public Wi-Fi access.

Any solution provided by the service provider must adhere to a certified carrier grade solution as part of this submission. The solution offered must preferably be scalable to eliver network connectivity on the back-bone from 10Gbps to 100Gbps on a single ASIC. Please provide detail as to how this is to realised.

2.4.2 Voice Platforms

CoT currently utilizes a range of products to fulfil in its voice needs which is seamlessly integrated as a converged voice and data network. It has a wide range of voice products to full-fill these needs including the PCX Enterprise, remote shelves, management software and a wide range of phones ranging through products like digital phones, to a lesser degree, IP phones and soft phones. The same qualtiy/standard of equipment must be provided. Any solutions submitted as part of this tender must expand on this model. The same features and functionality must be maintained by any solution proposed by the bidders.

2.4.3 Management Platform

The CoT has implemented a single Management platform to manage and maintain all the core voice and data equipment, using management applications and SAM (Service Aware Manager).

The centralized management platform covers all the aspects of the management from network hardware configuration, security, Virtual Local Area Networks (VLANs), Quality of Service (QoS), Intrusion Detection System (IDS) integration, and telephony services. These configuration settings are propagated across the entire network in a single operation.

Additionally the Quarantine Manager Application interfaces with the installed IDS devices to automatically isolate any user detected as propagating viruses, using the dynamic, mobile VLAN capabilities.

It will be required of the successful tenderer to provide monthly reports, using their own network management tools with the same functionality as mentioned earlier in this section. In addition the sucessful tenderer will be required to use industry approved Sniffers (1 GB and 10 GB ETHERNET PORTS – Copper and Fiber interfaces). These management tools must be updated regularly to support new features and must also be available to display on overhead monitors and to CoT network personnel.

All reporting is relevant to utilisation, performance, virus activity, service attacks, traffic analysis, etc. All reporting must be made available at set times during the month, and must also be available for any ad hoc requests. All information on the systems is confidential and must at all times be routed through the correct channels and protocols. The successful vendor will be responsible for any licensing fees applicable to sniffers or any other diagnostic software needed to properly support and maintain the environment. The voice/data network must be properly documented (drawings) containing all relevant information such as IP addressing, physical interfaces etc.

2.4.4 Additional Information

The appointed supplier will have to implement and maintain new equipment and integrate it seamlessly with the current based infrastructure, working with the existing support Service Provider who has a maintenance contract for some of the existing equipment.

2.4.5 Network General Information

Key facts:

Number of Users	12 000 (Data) + 14 000 (Voice Users)
Total Switches	±896
Nr of ports	±21 000
Nr of buildings connected	±520 buildings
LAN Ranges:	10/100Mb, 1000 Mb, 10Gig
LAN types:	Multi-Mode & Single-Mode fiber, UTP Cat 5, Copper 10, Cat 6
WAN ranges:	64 kbps, 128 kbps, 512 kbps, 2 Mb, 4 Mb, 11/300Mb, 1000 Mb, 10 000 Mb
WAN types:	Diginet, ISDN, Wireless Radio, Gigabit Ethernet, 10 Gig Ethernet, MPLS
Wi-Fi:	Deployed mostly at conference rooms and libraries.

Network diagrams will only be given to the appointed service provider due to their confidential nature.

2.5. Technical Support Staff And Skills

2.5.1 General

2.5.1.1 Skill Requirements

A complete organogram of the resource base to be deployed at the CoT must be provided. Only certified professionals, on the highest possible certification from the particular OEM, are allowed to configure data and voice equipment, in this case Alcatel/Lucent and Huawei.

Proof of certifications must be submitted along with the bid, failure to adhere to this will lead to disqualification. All identified/nominated resources as listed below, must be deployed on Councils premises and be available to the Council Contract Manager, being the relevant Deputy Directors responsible for the deployment and management of this infrastructure. If such proof cannot be supplied, the bid shall be disqualified. The following summarized technical profile must be attached along with certification:

Name And Surname	
Date of Appointment	
Certifications	
Qualifications	

Experience (On similar systems/networks deployed withing Council at the time of this tender)	
Duration Working For Company	
Designation	
Nature Of Work	

If CoT deems it necessary, it will request a replacement resource if any resource is not performing according to expectations.

2.5.1.2 Working Hours and Availability

Office bound officials working hours for Tshwane is from 7:30 to 16:00, the networks are, however, functional 24/7/365. Resources must always be available to service any problems on the network during any crisis as and when it occurs. The project manager must be onsite during office hours. In this regard also refer to the SLA. Suitable office space will be provided by Tshwane. As some projects/programs can influence the availability of major core switches, such projects/programs can only be done after hours. Prices must therefore include for the overtime requirements, not only for the implementation of the project but also should maintenance issues arise.

Where personnel need to take annual leave or training courses, suitable back-up arrangements must be made to ensure continuity of services. The replacement resource must still be available on site.

2.5.1.3 Standby/Overtime

To ensure service coordination, a roster will be set up for three (3) months in advance for resource planning. At least one team must be on standby after hours, on public holidays and over weekends. Information must be available at all times with the name and contact detail of the persons on standby.

After hours, weekend and public holiday support will be determined by need to resolve issues and problems and to execute planned activities. This support needs to be catered for and, as with standby, provided for by the contractor as per contracting company's HR policy.

In an event of a failure or maintenance issue, the standby person will be notified and must respond in terms of the SLA (Service Level Agreement) contained within this document.

2.5.1.4 Reporting Levels And Communication Protocol

The following applies:

- All resources and project managers to report directly to the CoT Deputy Director responsible for the Networks/Telecommunications services and/or their appointed representative.
- All resources and project managers will adhere to all requests and ad hoc tasks issued to them.

- Project managers\installation and maintenance teams\all other onsite resources of the contractor to interact with project managers of the CoT.
- All reports on SLA issues to be reported directly to the Deputy Director or approved representative.
- All Departmental requests for equipment and services to be referred to the applicable CoT Deputy Director (or approved representative), as body responsible for all related projects.
- All personnel to adhere to the communication protocol. The communication protocol is via the appointed CoT Director responsible for the Networks/Telecommunications services. All requests for hardware or services will be via this office.
- Under no circumstances shall a contractor give feedback to any director but the CoT Director responsible for Networks (or appointed representative). Contractors shall not set up / attend meetings with other directors, or represent ICT in any form or meeting unless express permission was granted, and shall adhere to CoT procedures at all times.

2.5.1.5 ITIL And Change Control

All activities need to be planned and executed as per ITIL practices. The existing CoT forms can be utilized, or modified if the need dictates.

No work will be carried out on the network unless a Change Control was submitted by the successful contractor to ICT. Request for changes must be accompanied by an impact study and the necessary change control as to not to result in unnecessary Maintenance calls. Due notification/communication to users will in some cases be necessary.

In a project setup, communications must be via the project managers. If however, the project managers and team cannot agree, both parties can escalate the matter to ICT Management for final decision.

2.5.1.6 Meetings And Presentations

The contractor will be required to schedule and minute a bi-weekly (forth nightly) meeting with the CoT. The following must be standing discussion points:

- Reporting on complaints i.e. complaints received and scheduling information etc.
- Reporting on status of projects

The contractor may also be required to attend AdHoc meetings as and when required (for example project meeting with the client CoT). From time-to-time, the contractor will be required to either present or prepare a presentation for Top Management.

2.5.1.7 Reporting And Documentation

The following documentation is a requirement:

- Monthly network reports reporting on programs, projects and maintenance.
- Weekly maintenance feedback reports
    - Inclusive of all historical complaints

- Statistics on calls completed within SLA, out of SLA, not completed (and reasons for not completing)

- Need to supply Business Case(s) on request – normally two weeks will be given to compile Business Cases.
- Weekly progress schedules.
- Update all network related architecture for example network drawings
- Technical Architectural Specifications
- Functional Specifications
- Presentations
- Quotes
- Project Plan (+associated project manager) for every project
- Minutes of meetings
- All related documentation that might be listed in this Tender
- Sniff report to be handed in after every sniff request
- Any ad hoc documentation as required from time-to-time.

The CoT does have a service desk, but it remains the responsibility of the contractor to collect the necessary data with regards to maintenance calls and projects. Also note that all calls and projects must be logged at the CoT service desk.

2.5.2 Required Skill Set

2.5.2.1 Certified Switch (Data) Experts

Part 1: Deployment of new equipment

The successfull bidder will be required to have available and if needs be to deploy permanently on site, for the duration of the contract and guarantee period, at least two OEM Certified Data Switch Experts. The certified professionals must have the highest possible certification from the particular OEM and must ensure seamless integration into the current system based network.

Part 2: Maintenance of the current network

The successfull bidder will be required to have available and if needs be to deploy permanently on site, for the duration of the contract and guarantee period, at least two OEM Certified Data Switch for maintenance of the current network.

2.5.2.2 Certified Voice Experts

Part 1: Deployment of new equipment

The successfull bidder will be required to have available and if needs be to deploy permanently on site, for the duration of the contract and guarantee period, at least two Certified Voice Experts. The certified professionals must have the highest possible

certification from the particular OEM and must ensure seamless integration into the current environment.

Part 2: Maintenance of the current network

The successfull bidders will be required to have available and if needs be to deploy permanently on site, for the duration of the contract and guarantee period, at least two Certified Voice Experts for maintenance of the current network.

2.5.2.3 Operations Manager

Part 2: Maintenance of the current network

The successfull bidders will be required to have and deploy permanently on site, for the duration of the contract and guarantee period, an Operations Manager. The duties of the Operations Manager are listed below:

- Day to day management of all maintenance related issues.
- Responsible for monthly reports that provide SLA statistics, projects and other related business information and statistics applicable to all areas of the Service Provider's services to Tshwane.
- Monthly minuted meetings with Deputy Directors and Directors to discuss Operational Reports.
- Service Desk Calls (Maintenance): Handling of daily complaints. Complaints are issued via the Service Desk. The Operations Manager must ensure that the call is logged with the correct category. Completion reaction times will be used as a metric to determine performance. This is a daily activity.
- Procurement tracking and reporting on a weekly and monthly basis. This includes correct invoicing.
- Single point of contact to discuss problems on maintenance issues
- Related ad-hoc tasks.

2.5.2.4 Project Manager (As and when required)

Part 1: Deployment of new equipment

The successfull bidders will be required to have and deploy a project manager on an as and when basis. The duties of the project manager are listed below:

- Minute site (project) meetings with attendance register with all involved parties (including voice, data, UTP, fiber, the customer etc.).
- Weekly summarized project feedback to the Deputy Directors on progress and important dates/events as well as possible delays.
- Single point of contact to discuss problems on projects
- Provide reports with regards to projects and programs
- Scheduling of teams

- Attend site scoping's
- To manage projects according to sound project management principles
- Signing-off of the site and checking correctness of invoice.
- Quality control inspections of sites after completion
- Ensuring completeness of documentation i.e. test results, drawings etc.
- Order tracking

It consists of seven stages:

1. Site scoping stage or site visit to determine extent of project. This consists of all involved parties including fibre, UTP, data-voice contractors, the client etc.
    - Held at location where equipment/linkage is required.
    - Investigate the Link-up Premises as well for example to check availability of spare fiber, Gig ports/blades, ATM ports/blades etc.
2. Quotation Stage
    - Contractor to arrange for quotes.
3. Planning Stage
    - Complete project templates and all planning required for the project including possible change control procedures.
4. Ordering
    - Client/CoT will obtain the necessary order
    - Contractor to ordering equipment after official order has been issued by CoT.
5. Installation
    - Establish and Mobilize teams.
    - Arrange delivery of equipment on site.
    - Site inspections
    - Minute site meetings on site with all involved parties. Minutes should include responsibilities of role players (**Involved Parties**) and due dates on tasks. Sound project management principles must be used.
    - Solving and communicating possible installation problems
    - Summarized reporting to Supervisor and feedback as required.
    - Conformance to specifications unless reasons exist for non-conformance.
    - Inform parties of completion of sub-stages i.e. UTP Cabling completed, Fiber installation completed, Fiber termination and splicing completed, Voice and Data completed.

6. Certification

- Certification for UTP/Fiber Installation
- Neatness of data and voice equipment
- Site as per original condition
- Quality Control

7. Invoicing and completion

- Ensure that invoices are requested and handed in with Payment voucher.
- Ensure that invoice data is received by Supervisor and thereafter handed to the Tshwane Financial Representative.
- Tag keys and arrange for storage in key box.
- Invoices must be handed in after completion (sign-off) within 3 working days.

2.5.2.5 Network Sniffing Expert

Please note: If CoT deems it fit to do so, the services of an external sniffer expert will be obtained where necessary or to double check results. However, the contractor will be required to make the following services available for a reputable sniffing expert.

2.5.2.5.1 Quarterly Sniffs

Quarterly sniffs will be scheduled to ensure that the network is stable. The Sniffing Expert shall sniff the core network for a period of five working days and then submit a detailed report with the finds and corrective measures.

Prices quoted will be per quarterly sniff of five days including for the time needed to examine the sniff and to prepare the report. Prices to include all software and hardware required (it remains the property of the Networking Sniffing Expert or the bidder). Change control procedures must be followed before the sniff is undertaken.

The successful tenderer must ensure that corrective actions are taken as pointed out via the sniff report.

2.5.2.5.2 Sniff On Requirement

Sniffs on requirements will be scheduled when users complain about slow access on the network. The Sniffing Expert shall sniff a particular user(s) and/or system and the building for a period of three working days and then submit a detailed report with the finds and corrective measures.

Prices quoted will be per sniff of three days including for the time needed to examine the sniff and to prepare the report. Prices to include all software and hardware required (it remains the property of the Networking Sniffing Expert or the bidder). Change control procedures must be followed before the sniff is undertaken.

The successful tenderer must ensure that corrective actions are taken as pointed out via the sniff report.

2.5.2.5 Engineer Professional Services

An Engineer from OEM Professional Services will be required for a minimum period of one week per annum for the duration of the contract to health check and audit of the complete environment. A report with findings and recommendations must be provided to CoT within 3 weeks from departure of the engineer. The maintenance incumbent will be required to implement any CoT approved recommendations. The cost for this engineer must be included in the maintenance fees.

2.5.2.6 Additional Resources

Below is a list of additional resources that may be contracted from time to time as the need arise. The bidders must price the resources but CoT is under no obligation to make use said resources:

- Wi-Fi technicians
- Network Monitoring specialist
- Security and Firewall expert
- Quality Controller
- Radio Technicians

2.5.3 Additional Requirements

2.5.3.1 First Line And Expert Support

Not only will the contractor be responsible for expert and all network related support, but for first line support as well. This imply that it is the contractor's responsibility to rule out any electrical, fibre or other related issues that causes the network to be down. The issue must be escalated to ensure faster response times. The contractor must therefore also have the necessary test equipment to determine whether the network is down due to a fibre related problem.

2.5.3.2 Network Drawings and Project Templates

Network drawings must be updated regularly and must also show the fibre connection and type of fibre between the switches. After every project or change, the network drawing must be updated to reflect the necessary updates/changes.

2.5.3.3 Transport Service

New equipment must be delivered to the ICT store for asset tagging. The contractor must therefore provide a transport service inclusive of the necessary insurance, to transport the equipment to the ICT store and then to site after it was asset tagged.

The same transport service must be used to deliver faulty, end-of-life, old and redundant equipment to the Auction Yard, inclusive of the necessary insurance. Official disposal of asset procedures must be adhered to.

2.5.3.4 Radio Support

Radios are mostly located on water towers, reservoirs and other high sites. Support here must be certified for working on heights and any other OHSA requirements.

2.5.3.5 Support Teams

2.5.3.5.1 Project Teams

Project teams will only be assigned to projects and will include a certified Data and Voice expert as well as a project manager. They will be responsible for all projects and programmes.

2.5.3.5.2 Maintenance Teams

Maintenance teams will only be assigned to maintenance and will include certified Data and Voice experts. They will be responsible for the daily maintenance activities. Maintenance teams will be responsible for the support on the whole network therefore inclusive of:

- Newly deployed equipment once guarantee\SLA has expired
- Older Equipment

2.5.3.6 Workload

Should CoT determine that the work load is strenuous, it will inform the contractor to deploy additional teams with immediate effect. This cost must be included in the labour charges quoted in the schedules.

2.5.3.7 Test Equipment

It is the responsibility of the contractor to issue test equipment to the required resources. The following equipment must be on site 24/7:

- VOIP testers
- Network analysis\assistant tools
- OTDR
- Cable testers to test UTP cabling
- Wireless fault tracing tools
- Voice Technical Repair Tool Sets

It is the successful tender's responsibility to provide all tools and test equipment and to ensure that the equipment is maintained and calibrated according to manufacturer's standards. The contractor shall employ or contract suitably qualified and trained personnel to provide the Services to Tshwane in terms of this agreement.

The personnel must be certified and under no circumstances will Tshwane be used as a training facility. Costing related to test equipment must be included in the support costs. After conclusion of the contract, the test equipment will remain the property of the contractor.

2.5.3.8 Leave Arrangements Etc.

The contractor must provide a list with additional ACSE's to act as replacements for example for leave arrangements, courses etc.

2.6 Pricing And Pricing Schedules

2.6.1 Invitation

Please note that this is a mere invitation to do business and under no circumstances whatsoever shall it be construed as an “offer” giving rise to any contractual obligations on the part of the CoT. The City of Tshwane shall not be bound to accept the proposal submitted by the contractor and reserves the right to accept the whole or part of the said proposal.

The CoT further reserves the right to negotiate and/or renegotiate, whichever is applicable, the terms and conditions and quantities of the proposal. The pricing schedules does not constitute the total value of the orders to be placed as it is a shopping list of possible items that can be requested/ordered during the course of the contract period to either expand or maintain the network.

2.6.2 Total Cost Of Ownership [TCO]

A Price proposal is required to be prepared as part of the response. The CoT procurement initiatives are centered on the TCO approach and want bidders to take cognizance of this and assist the CoT in driving down the total cost by considering all the cost drivers making up the component cost.

2.6.3 Pricing Schedules

The cost proposal must be submitted in writing on the schedule within this document. A digital copy of the price list will be provided in spreadsheet format, of which all the formulas will be blocked. It is incumbent on you to ensure that your pricing in both the hard and soft copies are the same that it can expedite the evaluation process. The hard copy will be seen as the official pricing document. If the price on the electronic schedule differ from the hand written/typed schedule, then the price of the hand/typed written schedule will take precedence and the electronic schedule will be changed accordingly. The electronic schedule is required to assist the Tender Evaluation Team.

2.6.4 Inclusion Of All Costs

The Contractor shall be deemed to have satisfied himself before submitting his tender as to the correctness and sufficiency of the tender and to have taken account of all that is required for the full and proper execution of the contract and to have included in his rates and prices all costs related to the supplies.

The prices quoted/tendered must include for handling, packing, loading, transport, delivery, off-loading, transit, shipping, checking, travel, accommodation, subsistence, installation, configuration, commissioning, insurance, administrative costs (such as documents and manuals required), execution, supervision, furnishing of tools required for assembly, extraordinary and/or any other cost.

In other words, the CoT will not entertain any claims for additional costs. Price must include for all requirements as stipulated in this document.

2.6.5 Submission Of Quote

All costs incurred in the submission of the quote shall be for the account of the bidder, whether such quote is successful or not.

2.6.6 Quantities

CoT reserves the right to reduce or increase the quantities (again note that the quantities provided is only for evaluation purposes and NOT for ordering purposes) of items without any

change in unit cost. The eventual quantities of items ordered will be determined by CoT at the time of the order being placed and will be at CoT's sole discretion.

2.6.7 Delivery Penalty Clause

If supplier fails to deliver any or all of the goods within the period specified in the contract, CoT shall, without prejudice to its other remedies under the contract, deduct from the contract price, as liquidated damages, a sum equivalent to 1% of the value of the delayed goods per week of delay until actual delivery up to a maximum deduction of 10 % of the contract sum. Once the maximum is reached, CoT may consider the termination of the contract. Notwithstanding the above, CoT may, without prejudice to any other remedy for breach of contract, by written notice of default sent to the supplier, terminate this contract in whole or in part:

- if the supplier fails to deliver any or all the goods within the period specified in the contract or within any extension thereof granted by CoT;
- or if the supplier fails to perform any other obligation(s) under the contract.

2.6.8 Quote All Items

The bidder must quote/tender on all the items as listed in the attached Item Price List. No omissions will be accepted as it will seriously compromise the evaluation process as the total quoted price per Service Provider will then not be equitable to one another. Incomplete quotations not providing all item prices are grounds for summary dismissal with no recourse from the SP to contest or later provide outstanding item prices.

2.6.9 License Fees

All License Fees for all software deployed on this contract must be included in the contract price. This implies free full version upgrades for the contractual- and warranty period. All software bought as part of this contract, remains the property of the CoT. Should CoT decide not to renew license fees, CoT will be Authorised to continue using the fully functional version at no additional cost. No annual license fees will be entertained as part of this tender.

2.6.10 Power/Stacking/Fibre Cords

To be included in the price of the main switch/equipment.

2.6.11 Firmware or Software Updates

All Firmware/OS software updates for all switches/routers/firewalls/other network equipment deployed on this contract must be included in the contract price. This implies free full version upgrades for the contractual- and warranty period. All firmware/software OS procured or installed as part of this contract, remains the property of the CoT. No annual license fees will be entertained as part of this tender.

2.7 Training

2.7.1 **Training ICT personnel:** Within the tender the successful contractor should provide on-site training for ICT personnel in order that they can operate the equipment supplied. A suitable venue will be provided by CoT, and the contractor will be responsible for the training facilitator, equipment needed and the necessary manuals.

2.7.2 **Training CoT personnel:** This item shall include equipment usage training. For example, if new phones are deployed, then the contractor must train the personnel to use the new phones.

2.7.3 **Training Learners:** Skills transfer shall also be done to accommodate at least 5 learners per year during the contractual period.

2.8 General Conditions

2.8.1 **Authorised Representative:** The bidder must be a reputed manufacturer or his authorized representative of the product offered. In case of representative, the authority from the manufacturer (OEM)/distributor must be submitted. The bids received without authority are liable to be rejected.

2.8.2 **Language:** The offers, all correspondence and documents related to the tender exchanged by the tenderer and the Contracting Authority must be written in the language of the procedure which is English.

2.8.3 **Ethics:** Any attempt of negotiation direct or indirect on the part of the tender with the authority to whom he has submitted the tender or authority who is competent finally to accept it after he has submitted his tender or any endeavor to secure any interest for an actual or prospective tenderer or to influence by any means the acceptance of a particular tender will render the tender liable to be excluded from consideration.

Any attempt by a candidate or tenderer to obtain confidential information, enter into unlawful agreements with competitors or influence the committee or the Contracting Authority during the process of examining, clarifying, evaluating and comparing tenders will lead to the rejection of his candidacy or tender and may result in administrative penalties.

When putting forward a candidacy or tender, the candidate or tenderer shall declare that he is affected by no potential conflict of interest and has no equivalent relation in that respect with other tenderers or parties involved in the project. Should such a situation arise during execution of the contract, the Contractor must immediately inform the Contracting Authority.

The Contractor must at all times act impartially and as a faithful adviser in accordance with the code of conduct of his profession. The Contractor shall refrain from making public statements about the project or services without the Contracting Authority's prior approval. The Contractor may not commit the Contracting Authority in any way without its prior written consent.

For the duration of the contract the Contractor and his staff shall respect human rights and undertake not to offend the political, cultural and religious mores of the beneficiary state.

2.8.4 **Confidentiality:** The information contained in this RFP document, or provided by management or staff of The City of Tshwane, is solely for the purpose of providing Bidders with information on which to submit their proposals. It is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged information and material. Any review, retransmission, dissemination, or other use of, or taking of any action, in reliance upon this information by persons or entities other than the intended recipient, is prohibited. Recipients of this document shall respect the confidentiality of the information contained herein together with any other information obtained during the course of the RFP process.

The Contractor and his staff shall be obliged to maintain professional secrecy for the entire duration of the contract and after its completion. All information, reports and documents drawn up or received by the Contractor shall be confidential. The contractor

shall not, save in so far as may be necessary for the purposes of the contract's execution, publish or disclose any particulars of the contract without the prior consent in writing from CoT. If any disagreement arises as to the necessity for any publication or disclosure for the purpose of the contract, the decision of CoT shall be final.

2.8.5 **Laws and Regulations:** The Contractor shall respect and abide by all laws and regulations in force in South Africa and the by-laws and regulations of CoT and shall ensure that his/her personnel, their dependent's, and his/her local employees also respect and abide by all such laws and regulations. The Contractor shall indemnify CoT against any claims and proceedings arising from any infringement by the Contractor, his/her employees and their dependents of such laws and regulations.

The successful tenderer will be required to comply with the requirements of the Occupational Health and Safety Act, Act 85 of 1993 and regulations as amended. Further information in this regard may be obtained from the Occupational Health and Safety, @ telephone number (012) 358-0069.

2.8.6 **Extension of Period of Implementation**: The Contractor may request an extension to the period of implementation if his implementation of the contract is delayed, or expected to be delayed, for any of the following reasons:

a) Extra or additional supplies ordered by CoT

b) Exceptional weather conditions which may affect installation of the supplies;

c) Physical obstructions or conditions which may affect delivery of the supplies, which could not reasonably have been foreseen by a competent contractor;

d) Failure of the CoT to fulfil its obligations under the contract;

e) Any suspension of the delivery and/or installation of the supplies which is not due to the Contractor's default;

f) Force majeure;

g) Any other causes referred to in these General Conditions which are not due to the Contractor's default.

Within 15 days of realizing that a delay might occur, the Contractor shall notify the Project Manager of his intention to make a request for extension of the period of implementation to which he considers himself entitled and, save where otherwise agreed between the Contractor and the Project Manager, within 30 days provide the Project Manager with comprehensive details so that the request can be examined.

The Project Manager will submit the written request for approval and within 30 days CoT shall, by written notice to the Contractor after due consultation with the necessary authority and, where appropriate, the Contractor, grant such extension of the period of implementation as may be justified, either prospectively or retrospectively, or inform the Contractor that such extension was not granted.

2.8.7 **Projects and Variation Orders:** Variations may include additions, omissions, substitutions, changes in quality, quantity, form, character, kind, as well as drawings, designs or specifications where the supplies are to be specifically manufactured for the Contracting Authority, method of shipment or packing, place of delivery, and in timing of implementation of the supplies.

Variation Orders will be given in writing on an official letterhead of the CIO (Chief Information Officer). No variation shall be made orally. Prior to issuing an administrative order for a variation, the Project Manager shall notify the Contractor of the nature and form of that variation. As soon as possible, after receiving such notice, the Contractor shall submit to the Project Manager a proposal containing:

- a description of the tasks, if any, to be performed or the measures to be taken and an implementation Programme;
- any necessary modifications to the implementation Programme or to any of the Contractor's obligations under the contract;
- any adjustment to the contract price

Following the receipt of the Contractor's submission, the Project Manager shall, after due consultation with the Contracting Authority and, where appropriate, the Contractor, decide as soon as possible whether or not the variation should be carried out. If the Project Manager decides that the variation is to be carried out, he shall issue an administrative order stating that the variation is to be made at the prices and under the conditions given in the Contractor's submission.

2.8.8 **Trademark:** In certain instances, where a reference has been made to a specific make or source, process, trademark, patent or product type, the reference is made only to describe a type of product classification (and all of its equivalents) for which no universally approved industry standard, benchmark or other sufficiently detailed or intelligible description is available at the time of the issuance of the procurement notice. In any and all such instances, the tendering party and the Contracting Authority shall interpret such a description as inclusive of any equivalent (or better) and the Contracting Authority shall accept for evaluation and procurement purposes as "compatible" any specification which is equivalent or better, irrespective of the actual nomenclature used by the tendering party.

2.9 Passwords

Network technicians will be required to use unique usernames and passwords on the switches to effectively track any changes implemented on the network. Any outgoing Service Provider must make provision that this be provided to Council to allow for service continuity.

The admin password will remain the property of the City and unauthorized changing of the admin password will not be allowed. In the event of the City requesting the changing of the admin password, it will be done with the necessary Change Control and only once approved by the Director Infrastructure. The new admin password will then be stored in a safe location by the Director Infrastructure.

2.10 Non-Disclosure Agreement

The contractor will be required to sign the CoT Non-Disclosure Agreement when appointed.

PART 3: EXPANSION OF CURRENT ALCATEL/LUCENT & HUAWEI NETWORK

Part 3: Expansion of the current Alcatel/Lucent & Huawei Network

Supply, Delivery, Deployment, Configuration And Maintenance Of New Network Equipment For The Expansion of The Current Corporate Network

3. NEW EQUIPMENT

3.1 Scope

This section, **Supply, Delivery, Deployment, Configuration and Maintenance of New Network Equipment**, describes the technical and other specifications to which the new data or voice equipment must adhere to. All equipment procured under this section, will also need to be maintained by the service provider from which it was procured, for the duration of the contract and warranty/guarantee period.

The following resources must be provided (refer Part 2):

- 2 x Data switch experts
- 2 x Voice switch experts
- 1 x Project Manager

If CoT deem further resources to be necessary, they will be contracted from the price list.

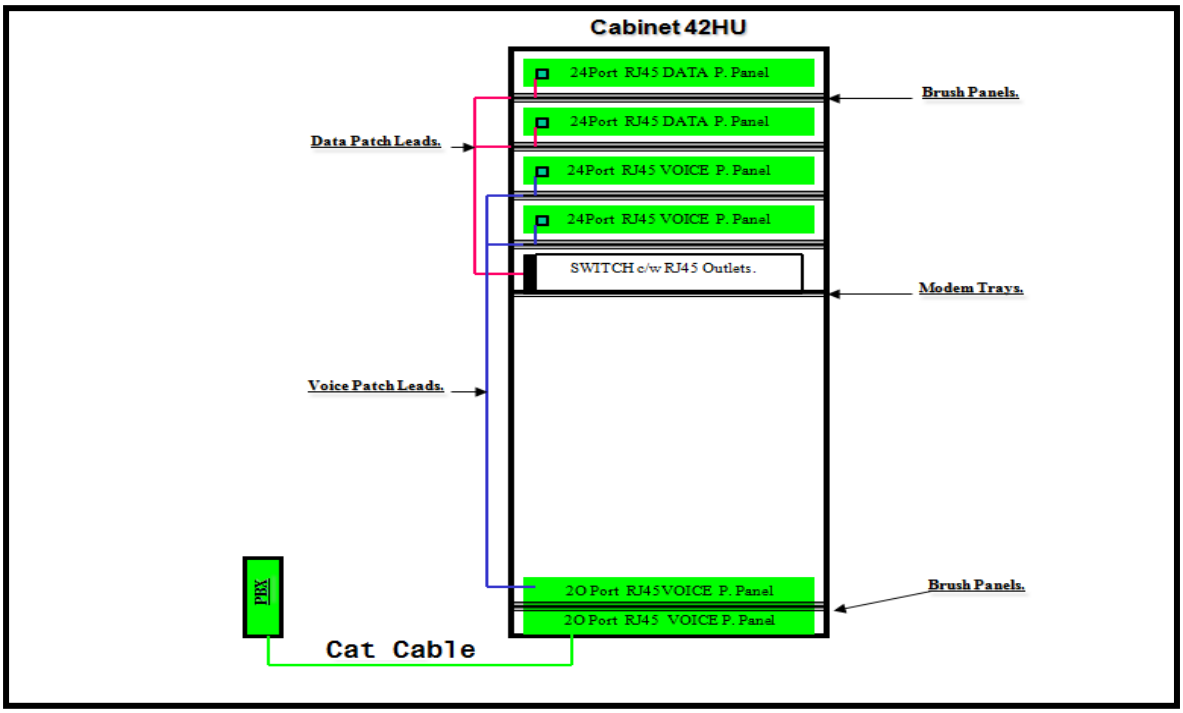
3.2 Cabling And Cabinets

Cabling will be done by others with exception of the following:

- Supply, deliver and install fibre patch leads required to connect the switch with the existing backbone fibre.
- Supply, deliver and install stacking cables and or fibre patch leads required to stack or connect switches or other network equipment.
- Supply, deliver and install electrical power cords as per South African power standards.

- Patch existing users – patch cables will be supplied by others.

Electrical outlets will be supplied by others. A standard layout drawing for a 42U 600x800mm cabinet is shown below but position of the switch may vary and therefore final position must be confirmed by the relevant CoT Project Manager.



3.3 Equipment Requirements

The successful contractor shall be responsible for setting up a working solution and therefore equipment must be 100% compatible and interactable with existing equipment. It will be the responsibility of the supplier to make the whole system operational. This includes configurations of all existing and new equipment and installation of any necessary software as may be required, and to install the equipment on site at the appointed tenderer's cost.

All proposed networking equipment (routers, L3 switch, etc.) must support SNMP protocol (version 2 & 3). Any other Hardware/software required for the proper functioning of the system must be quoted for.

3.3.1 Data Equipment (This applies to both the Alcatel/Lucent and Hauwei products)

3.3.1.1 Switches

Switches shall be suitable to mount securely along the width of the 19" cabinet. The switches must be fastened in accordance with manufacture specifications and all screws, bolts and other fastening accessories must be supplied and fastened by the successful contractor.

Switches shall have a minimum of (8 and 12) 24 ports. Ports shall be 100/1000 Mbps autosensing ports with the ability to force the port speed if required. Core switches shall be linked to Access Level Switches via 1000Mbps fibre optic ports. All switches shall have a

minimum of two fibre uplink ports supporting different Gigabit Interface Converters. Backbone cabling will be supplied by others (with the exception of the fibre patch leads).

Through the use of Virtual LAN technology, it will be possible to virtually isolate the networks of individual CoT Departments/Divisions and restrict/control access to these networks. There is, thus, a need to have strict security measures to segregate these different users although they will be on the same communication backbone. Each Department/Division should be able to function as a Virtual Local Area Network (VLAN). Suppliers should configure VLAN over the Layer 3 switches to ensure security of the various LANs.

To make effective use of bandwidth switches must support features like Quality of Service (QoS)/Traffic Shaping, Policy Based Routing or any other suitable traffic engineering mechanism should also be configured.

Switches must be standards based.

All switches provided as part of this tender must adhere to the below technical specifications to ensure the seamless integration aspect to work as flawlessly as is necessary. Failure to comply with these specifications will result in disqualification of the SP's submission to Council.

3.3.1.1.1 Core Switch

- Large Gigabit and 10 and 40 Gigabit Ethernet port density and performance; offering up to 768 Gigabit Ethernet ports and up to 96 10-Gigabit Ethernet ports on the same chassis-based system.
- Smart Continuous Switching: Hot Swap, Management Module Fail-over, Power Monitoring, and Redundancy.
- No single point of failure and a sub-second fail-over in its redundant configuration.
- Redundant Management and Redundant Switch Fabric.
- Hot swappable components and hot insertable support: switch modules, SFPs/XFPs.
- Redundant Power Supplies (Redundant 1:1 power) and Redundant 1:1 PoE power provided by the PoE P/S.
- Spanning Tree robustness (Single or Multiple STP options): IEEE 802.1D (STP) (802.1D spanning tree for loop free topology and link redundancy) and IEEE 802.1w-Rapid Reconfiguration of Spanning Tree
- Ring Rapid Spanning Tree optimized for ring topology to provide less than 100ms convergence time.
- IEEE 802.1s multiple spanning tree and per-VLAN spanning tree (1x1).
- Fast forwarding mode on user ports to bypass 30-second delay for spanning tree.
- Preventing unauthorized spanning-tree enabled attached bridges from operating.
- BPDU blocking – automatically shuts down switch ports being used as user ports if a spanning tree BPDU packet is seen. Preventing unauthorized spanning-tree enabled attached bridges from operating.
- Priority queues: eight hardware-based queues per port.

- VRRP (Virtual Router Redundancy Protocol), and OSPF ECMP (Equal Cost Multipath Protocol).
- Dynamic link aggregation IEEE 802.3ad (that supports automatic configuration of link aggregates with other switches) with resilient uplink capabilities.
- MC-LAG
- Static link aggregation (that supports automatic configuration of link aggregates with other switches).
- IEEE 802.1s: MISTP (802.1s) is an IEEE standard which allows several VLANs to be mapped to a reduced number of spanning-tree instances. This is possible since most networks do not need more than a few logical topologies. Each instance handles multiple VLANs that have the same Layer-2 topology.
- Software Resiliency: The proposed product must provide fully redundant and resilient system components to insure continuous, non-stop operation. This includes redundant subsystems, hot swappable modules, load-sharing components, “hitless software loading”, downloadable bootstrap, and image rollback which allows the system to automatically re-load previous configurations and software versions.
- Software image rollback and configuration recovery.
- Image and configuration synchronization for Management Modules.
- Hitless loading of optional software (routing/security), without re-booting.
- Broadcast storm control.
- Downloadable bootstrap.
- Chassis thermal protection/shutdown.
- Hardware monitoring, temperature monitoring, and power monitoring and management.
- Short “cold” and “warm” boot times.
- Built-in security and device hardening.
- Network and Link Resiliency: Network and link resiliency are important parts of network availability, and the proposed product must support advanced routing, load sharing, and mechanisms for fast reconfiguration of links between switches, servers, and other network devices:
    - VRRP (Virtual Router Redundancy Protocol), and OSPF Equal Cost Multipath Protocol
- Topological Network Redundancy: In order to provide the highest levels of availability throughout an enterprise, it is important to build redundancy and resiliency into the topology at the network level to ensure that links have backups and traffic is always flowing:
    - Physical redundancy
    - Layer-2 and layer-3 redundancies

- Switch must have modular slots to support following modules -1000Base-T, 1000Base-SX and 1000Base-LX, 10Gig and 40 Gig

- Switch must support standards - IEEE 802.3: 10BASE-T (Ethernet), IEEE 802.3u: 100BASE-TX (Fast Ethernet), IEEE 802. 3z/ab: 1000Base-X (Gigabit Ethernet), IEEE 802.3x (full-duplex flow control)

- Switch must support following features: IEEE 802.1p (Priority Queuing), IEEE 802.1d (Spanning Tree Protocol), IEEE 802.1Q (VLAN), Link Aggregation (IEEE 802.3ad Trunking), IGMP (RFC 1112), Port Mirroring, Jumbo Frame Support and MAC/IP address filtering.

- Switch must have the following SNMP features - SNMP (RFC 1157), Remote Monitoring MIB (RFC 2819), Bridge MIB (RFC 1493), 802.1Q Bridge MIB (RFC 2674).

- Switch must have following Management features - Telnet, RS232 Console Port, Web-Based Management Interface, SNMP, Four RMON groups (1: statistics, 2: history, 3: history, 9: events)

- Switch must be able to filter out data packets based on certain MAC or IP address. This will block these network packets from accessing the network.

- Switch must support ICMP router discovery, Proxy ARP, Routing Information Protocol (RIP v1 and RIP v2), Open Shortest Path First (OSPFv2) for routing path management in a network.

- Switch must support Port-based and Tagged VLAN, which are compliant to IEEE 802.1Q standard and must be able to link these VLANs with wire-speed routing.

- Switch must support min 256 IP subnets / L2 tagged VLANs to segment the IP or MAC-based networks to reduce the network broadcast and improve the performance of the network.

- Must support server load balancing

- Must be a fully distributed architecture with modular software design for scalability
- Must offer Carrier Class Availability (99.999%)
- Must offer high levels of Security capabilities (DOS, A-VLAN's, SSL, Port Binding rules)

Technical Requirements for a Highly Secure System

- Partitioned Management – PM: Protected multiple user access control (i.e., the switch must provide a full suite of commands that allow the user to create and modify User IDs and Passwords (multiple administrative profiles) for access to switch management). The PM feature can utilize an on-board database, or RADIUS, LDAP authentication servers (user profiles are stored within these servers).

- Authenticated Switch Access (ASA): the proposed product must support a user access control or device access control with Secure Access Logging (AAA service) which can utilize an on-board database, RADIUS, LDAP, or ACE authentication servers.

- Automatic Log-out based on a pre-configured timer .

- Port Mapping (Private VLANs).

- Denial of Service Attack Defense (DOS protection).

- TAD traffic anomaly detection
- IEEE 802.1x industry standard port-based authentication challenges users with a password before allowing network access (The proposed product must support IEEE 802.1x used in conjunction with emerging security technologies to provide a method to verify an end user and their device status and either allow admission or quarantine the device to a safe environment where the deficiencies can be remedied).
- IEEE 802.1x multi-client, multi-VLAN support for per-client authentication and VLAN assignment.
- IEEE 802.1x with group mobility.
- IEEE 802.1x with MAC based authentication, group mobility or “guest” VLAN support.
- MAC-based authentication for non-802.1x host.
- Dynamic User Network Profile
- LLDP (LLDP-MED)
- Access Guardian support.
- Port Binding.
- Authenticated VLAN that challenges users with username and password and will support dynamic VLAN access based on user.
- Support for host integrity check and remediation VLAN.
- Security through the implementation of a Quarantine Manager and quarantine VLAN, with Security automation
    - Quarantine VLANs
    - Isolation of intruders through a Quarantine Manager
- PKI authentication for SSH access.
- Learned Port Security (LPS) or MAC address lockdown that will allow only known devices to have network access preventing unauthorized network device access.
- The proposed product must support User authentication.
- Centrally authentication through a RADIUS, TACACS+, LDAP or ACE server.
- The proposed product must support RADIUS and LDAP admin authentication that will prevent unauthorized switch management.
- TACACS+ client allows for authentication-authorization and accounting with a remote TACACS+ server.
- Secure Shell (SSH), Secure Socket Layer (SSL) for HTTPS and SNMPv3 for encrypted remote management communication.
- Access Control Lists (ACLs) to filter out unwanted traffic including denial of service attacks; Access control lists (ACLs) must be per port, MAC SA/DA, IP SA/DA, TCP/ UDP port; Flow based filtering in hardware (L1-L4).

- Support for Access Control List Manager (ACLMAN).
- Support for Microsoft Network Access Policy (NAP) protocol.
- Switch protocol security:
    - MD5 for RIPv2, OSPFv2 and SNMPv3
    - SSHv2 for secure CLI session with PKI support
    - SSLv3 for secure HTTP session
- DHCP Snooping, DHCP IP Spoof protection.
- The proposed product must restrict user ports from sending control traffic (BPDU, RIP, OSPF, BGP).
- The proposed product must prevent IP source address spoofing.

Technical Requirements for a Highly Intelligent system

- Virtual local area networks (VLANs)
    - Up to 4,094 VLANs, and up to 4,094 VLAN tags value support.
    - Per port, 802.1Q and policy based VLAN including authentication VLAN (A-VLAN).
- The proposed product must support wire-speed and feature rich Quality of Service (QoS).
- Industry classification standards including 802.1Q/p, TOS, and DiffServ, which will be enhance with complementary features such as extensive QoS mappings and re-tagging of prioritization:
    - IEEE 802.1p, ToS, DSCP marking.
    - QoS mapping: 802.1p to 802.1p and ToS and DSCP, ToS to ToS and 802.1p and DSCP, DSCP to DSCP and 802.1p and ToS
    - Classification per port, 802.1p (CoS) value, MAC SA/DA, TOS precedence, DSCP value, IP SA/DA, TCP/UDP port range.
    - 8 egress queues per port to support Strict (SP), Weighted Round Robin (WRR), and/or hybrid queuing (Strict + Weighted Round Robin queuing algorithms).
    - Eight hardware-based queues with flow-based classification and processing.
    - Ingress bandwidth rate limiting per port/flow in 64k increments.
    - Egress bandwidth rate limiting per port in 1Mbps increments.
- Wire-speed everything including switching, routing, ACLs, QoS, traffic redirection and Server Load Balancing.
- Featuring full wire rate (including first packet) and 10GigE single flow support.

- Native support for IPv4 and IPv6 for network future proofing
    - Full IPv6 support with hardware-based forwarding, classification and tunnelling.
    - Ability to interconnect the IPv6 “island” through an existing IPv4 network through hardware-based tunnelling.
    - Use of IPv6 across public organizations.
    - Ability to connect to the IPv6 backbone.
    - Ability to control IPv6 flows with extensive QoS/ACL policies.
- The proposed product must support extensive Multicast (L2 non-IP/IPv4/IPv6) IM-DM, PIM-SMv2 and PIM-SSM and DVMRPv3.
- Wire-rate multicast using hardware-based replication in all configurations.
- The proposed product must support high-density traffic aggregation in mission critical business network cores.
- The proposed product must provide fast network response time; including hardware-based source learning, and first packet handling in hardware.
- The proposed product must support Server Load Balancing (SLB).
- Full power-over-Ethernet (PoE) IEEE 802.3af support.
- Residential bridging features: DHCP option-82, DHCP-Snooping and Port Mapping.
- Routing Protocols: IPv4 and IPv6, RIPng, RIPv1/v2 and OSPFv2andv3 and OSPF-ECMP and BGPv4.

Technical Requirements for a Highly Manageable system

- NMS: Data and services network management including OneTouch QoS (PolicyView with OneTouch QoS centralizes and simplifies QoS configuration network wide) and SecureView.
- Carrier-Class Dynamic Group Mobility (GM).
- The proposed product must support dynamic user mobility with authentication that would allow the user to connect securely anywhere and have access to their resources without admin intervention or reconfiguration.
- The proposed product must support converged applications such as the VoIP.
- Diagnosing Switch problems:
    - Port Mirroring: Port based, port mirroring for troubleshooting, supports four sessions with multiple (24) sources-to-one destination configuration.
    - Port monitoring feature that will allow capture of Ethernet packets to a file, or for on-screen display to assist in troubleshooting.
    - SFlow support to monitor and effectively control and manage the network usage.

    - RMON: Support of RFC2819 RMON group (1-Statistics, 2-History, 3-Alarm, and 9-Events).

- Switch Health Monitoring.
- Monitoring Memory Tools and Switch Configuration.
- Switch Logging.
- Local (on the flash) and remote logging (Syslog).
- Logging into the Switch through Telnet, FTP, HTTP, SSH, SSL, and SNMPv1 and v2 and v3.
- Remote telnet management or secure shell access using SSH.
- Secured file upload using SFTP, or SCP.
- SNMPv1/v2/v3.
- Authentication or AAA Servers.
- Policy Servers; Authentication Servers such as RADIUS, LDAP, TACACS+, and ACE.
- Policy-Based Management with LDAP Directory Services.
- System File Management.
- Dual image and dual configuration file storage providing backup.
- The proposed product must support an intuitive CLI.
- The proposed product must support a web-based Element Management with an easy-to-use point and click and with a built-in help for easy configuration of new technology features.
- The proposed product must support remote telnet management or secure shell.
- The proposed product must support secured file upload using SFTP, or SCP.
- Port based, port mirroring for troubleshooting, that will support four sessions with 24 sources to one destination configuration.
- The proposed product must support human readable ASCII based configuration files for offline editing and bulk configuration.
- The proposed product must support managing Switch Users Accounts and Partitioned Management features.
- The proposed product must support the management of Switch Security.
- The proposed product must support IGMPv1/v2/v3 snooping to optimize multicast traffic.
- The proposed product must support BootP/DHCP client that will allow auto-config of switch IP information to simplify deployment.

- The proposed product must support Auto-negotiating 10/100/1000 ports that will automatically configure port speed and duplex setting.
- The proposed product must support Auto MDI/MDIX that will automatically configure transmit and receive signals to support straight thru and crossover cabling.
- DHCP relay to forward client requests to a DHCP server.
- DHCP Option-82 and DHCP Snooping.
- Integration with an SNMP manager for network wide management.
- System event log.
- Network Time Protocol (NTP) for network wide time synchronization.
- Interswitching Protocols.
- Mapping Adjacency Protocol for building topology maps within the SNMP Manager NMS application .
- GMAP and GVRP for 802.1Q-compliant VLAN pruning and dynamic VLAN creation.
- SFN (Software Defined Networking)

3.3.1.1.2 Layer 3 Distribution or Core Switch And Layer 3 Distribution Or Edge Stackable Switch

The following are applicable to a 24 Port Managed Ethernet Switch:

- Ports:
    - 22 auto-sensing 100/1000 ports (IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T)
    - Media Type: Auto-MDIX
    - Duplex: Full Duplex - Auto sensing of communication speed and auto negotiation of duplex mode.
    - 2 dual-personality ports each port can be used as either an RJ-45 10/100/1000 port (IEEE 802.3 Type 10Base-T; IEEE 802.3u Type 100Base-TX; IEEE 802.3ab 1000Base-T Gigabit Ethernet) or an open mini-GBIC slot (for use with mini-GBIC transceivers) for 1000Base-SX, 1000Base-LX, 100Base-FX MM, 100Base-FX SM.

The following are applicable to a 48 Port Managed Ethernet Switch:

- Ports:
    - 44 auto-sensing 100/1000 ports (IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T)
    - Media Type: Auto-MDIX
    - Duplex: Full Duplex - Auto sensing of communication speed and auto negotiation of duplex mode.

- 4 dual-personality ports each port can be used as either an RJ-45 10/100/1000 port (IEEE 802.3 Type 10Base-T; IEEE 802.3u Type 100Base-TX; IEEE 802.3ab 1000Base-T Gigabit Ethernet) or an open mini-GBIC slot (for use with mini-GBIC transceivers) for 1000Base-SX, 1000Base-LX, 100Base-FX MM, 100Base-FX SM.

Layer 3 Capabilities of 24 and 48 Port Managed Ethernet Switches:

- Support Routing Protocols such as RIP v1/2 and OSPF.

The following are applicable to a 24 and 48 Port Managed Ethernet Switches:

- Protocols:
  - TCP/IP
  - NetBEUI
  - Spanning Tree
  - DHCP/BOOTP Interoperation
  - Domain Name System (DNS) support.
  - Trivial File Transfer Protocol (TFTP) and/or FTP support.
  - Network Timing Protocol (NTP) support.

Management Protocols:

- IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
- SSH, SNMP v1, v2c, and v3 and Telnet interface support.
- Has SNMP agent, Supports SMP MIB II, Supports Bridging MIB, Allows out-ofband management via serial port, Allows in-band management via telnet, Allows graphical management via Web interface, Supports RMON, Complete with management S/W.

- Standards:
  - All switches to be standards based
  - IEEE 802.3 (SNAP encapsulated tagged and untagged frames)
  - IEEE 802.3u
  - IEEE 802.3x
  - IEEE 802.1D
  - IEEE 802.1p Priority
  - IEEE 802.1Q VLANs - port based and Tagged VLAN from any port using standards-based 802.1Q tagging.

- IEEE 802.3z/IEEE 802.3 ab
- IEEE 802.3x Flow Control
- IEEE 802.3ad Link Aggregation Control Protocol (LACP)
- RFC 1534 DHCP/BOOTP Interoperation

- Mounting:
  - 19” standard Rack mountable with mounting kit.
  - Maximum use of 2 Rack Units (RU)
- Management Console:
  - Switch should be manageable through Console port, Telnet, SNMP, HTTP, RMON, HTTPS and SSH
  - Must have console port.
  - Provide console cable, power cables and operating manuals.
- Authentication:
  - TACACS+ and RADIUS authentication
- Administration:
  - Allows software upgrade via FTP/TFTP
- Performance:
  - Throughput up to 35.7 million pps (64-byte packets)
  - Switching capacity 48 Gbps
- Security Features:
  - Access Control List
  - Rate Limiting
  - Port Security (by MAC address filtering)
  - IP filtering
  - MAC based port level security, multilevel access security for console
- Indicators and Diagnostic LED’s:
  - Per-port status: Link integrity, activity, speed, full-duplex
  - System status: System, RPS, link status, link duplex, link speed
- Environmental Ranges:

- Operating temperature: 0°C to 45°C
- Storage temperature: -25° to 70°C
- Operating relative humidity: 10 to 85%

- AC Input Voltage:
  - Standard South Africa Power Supply: 220/230 v (±10%), 50 Hz (±5%).
  - Must support power redundancy.
- Expansion through cascading:
  - Switch should be stackable i.e. manageable via single IP address, up to 8 units.
- Quality of Service:
- Other:
  - LAN Base Image installed
  - 16 Gbps switching fabric
  - Capable up to 8000 MAC addresses
  - Capable up to 255 IGMP groups.
  - Configurable maximum transmission unit (MTU) of up to 9000 bytes, with a maximum Ethernet frame size of 9018 bytes for bridging on Gigabit Ethernet ports, and up to 1998 bytes for bridging of Multiprotocol Label Switching (MPLS) tagged frames on both 10/100 and 10/100/1000 ports.
  - Up to 255 VLANs per switch.
  - Four thousand VLAN Ids.
  - Voice VLAN for voice traffic on a separate VLAN.
  - Dynamic VLAN assignment.
  - Dynamic, port-based security.
  - Port security to authenticate the port and manage network access for all MAC addresses
  - Unicast MAC filtering.
  - Unknown unicast and multicast port blocking.
  - SSHv2 and SNMPv3 based network security.
  - Support port monitoring and mirroring.
  - DHCP snooping.

- Multilevel security on console to prevents unauthorized users from altering the switch configuration.
- Rate limiting based on source and destination IP address, source and destination MAC address, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps.
- Web based Setup to configure the switch
- Management capabilities on a per-port and per-switch basis.
- Support spanning tree per VLAN and Rapid Spanning Tree (IEEE 802.1w).
- Bandwidth aggregation through EtherChannel technology enhances fault tolerance and offers higher-speed aggregated bandwidth between switches
- Supports additional frame formats: Ethernet II (tagged and untagged)
- Allows VLAN operation, Supports priority queuing, Supports IGMP snooping, Supports DVMRP
- Support Jumbo Frames
- Must offer Carrier Class Availability (99.999%)
- Must offer support for in-Line Power for IP phones using IEEE 802.3af standard
- Must offer support for 16 ports aggregation using IEEE 802.3ad standard

3.3.1.1.3 Layer 2 Edge Stackable Switch

The following are applicable to a 24 Port Managed Ethernet Switch:

- Ports:
  - 22 auto-sensing 100/1000 ports (IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T)
  - Media Type: Auto-MDIX
  - Duplex: Full Duplex - Auto sensing of communication speed and auto negotiation of duplex mode.
  - 2 dual-personality ports each port can be used as either an RJ-45 10/100/1000 port (IEEE 802.3 Type 10Base-T; IEEE 802.3u Type 100Base-TX; IEEE 802.3ab 1000Base-T Gigabit Ethernet) or an open mini-GBIC slot (for use with mini-GBIC transceivers) for 1000Base-SX, 1000Base-LX, 100Base-FX MM, 100Base-FX SM.

The following are applicable to a 48 Port Managed Ethernet Switch:

- Ports:
  - 44 auto-sensing 100/1000 ports (IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T)

- Media Type: Auto-MDIX
- Duplex: Full Duplex - Auto sensing of communication speed and auto negotiation of duplex mode.
- 4 dual-personality ports each port can be used as either an RJ-45 10/100/1000 port (IEEE 802.3 Type 10Base-T; IEEE 802.3u Type 100Base-TX; IEEE 802.3ab 1000Base-T Gigabit Ethernet) or an open mini-GBIC slot (for use with mini-GBIC transceivers) for 1000Base-SX, 1000Base-LX, 100Base-FX MM, 100Base-FX SM.

The following are applicable to a 24 and 48 Port Managed Ethernet Switches:

- Protocols:
  - TCP/IP
  - NetBEUI
  - Spanning Tree
  - DHCP/BOOTP Interoperation
  - Domain Name System (DNS) support.
  - Trivial File Transfer Protocol (TFTP) and/or FTP support.
  - Network Timing Protocol (NTP) support.
- Management Protocols:
  - IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
  - SSH, SNMP v1, v2c, and v3 and Telnet interface support.
  - Has SNMP agent, Supports SMP MIB II, Supports Bridging MIB, Allows out-ofband management via serial port, Allows in-band management via telnet, Allows graphical management via Web interface, Supports RMON, Complete with management S/W.
- Standards:
  - IEEE 802.3 (SNAP encapsulated tagged and untagged frames)
  - IEEE 802.3u
  - IEEE 802.3x
  - IEEE 802.1D
  - IEEE 802.1p Priority
  - IEEE 802.1Q VLANs - port based and Tagged VLAN from any port using standards-based 802.1Q tagging.
  - IEEE 802.3z/IEEE 802.3 ab

- IEEE 802.3x Flow Control
- IEEE 802.3ad Link Aggregation Control Protocol (LACP)
- RFC 1534 DHCP/BOOTP Interoperation

- Mounting:
  - 19” standard Rack mountable with mounting kit.
  - Maximum use of 2 Rack Units (RU)
- Management Console:
  - Switch should be manageable through Console port, Telnet, SNMP, HTTP, RMON, HTTPS and SSH
  - Must have console port.
  - Provide console cable, power cables and operating manuals.
- Authentication:
  - TACACS+ and RADIUS authentication
- Administration:
  - Allows software upgrade via FTP/TFTP
- Performance:
  - Throughput up to 35.7 million pps (64-byte packets)
  - Switching capacity 48 Gbps
- Security Features:
  - Access Control List
  - Rate Limiting
  - Port Security (by MAC address filtering)
  - IP filtering
  - MAC based port level security, multilevel access security for console
- Indicators and Diagnostic LED’s:
  - Per-port status: Link integrity, activity, speed, full-duplex
  - System status: System, RPS, link status, link duplex, link speed
- Environmental Ranges:
  - Operating temperature: 0°C to 45°C

- Storage temperature: -25° to 70°C
- Operating relative humidity: 10 to 85%

- AC Input Voltage:
  - Standard South Africa Power Supply: 220/230 v (±10%), 50 Hz (±5%).
  - Must support power redundancy.
- Expansion through cascading:
  - Switch should be stackable i.e. manageable via single IP address, up to 8 units.
- Quality of Service

Other:

- LAN Base Image installed
- 16 Gbps switching fabric
- Capable up to 8000 MAC addresses
- Capable up to 255 IGMP groups.
- Configurable maximum transmission unit (MTU) of up to 9000 bytes, with a maximum Ethernet frame size of 9018 bytes for bridging on Gigabit Ethernet ports, and up to 1998 bytes for bridging of Multiprotocol Label Switching (MPLS) tagged frames on both 10/100 and 10/100/1000 ports.
- Up to 255 VLANs per switch.
- Four thousand VLAN Ids.
- Voice VLAN for voice traffic on a separate VLAN.
- Dynamic VLAN assignment.
- Dynamic, port-based security.
- Port security to authenticate the port and manage network access for all MAC addresses
- Unicast MAC filtering.
- Unknown unicast and multicast port blocking.
- SSHv2 and SNMPv3 based network security.
- Support port monitoring and mirroring.
- DHCP snooping.
- Multilevel security on console to prevents unauthorized users from altering the switch configuration.

- Rate limiting based on source and destination IP address, source and destination MAC address, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps.
- Web based Setup to configure the switch
- Management capabilities on a per-port and per-switch basis.
- Support spanning tree per VLAN and Rapid Spanning Tree (IEEE 802.1w).
- Bandwidth aggregation through EtherChannel technology enhances fault tolerance and offers higher-speed aggregated bandwidth between switches
- Supports additional frame formats: Ethernet II (tagged and untagged)
- Allows VLAN operation, Supports priority queuing, Supports IGMP snooping, Supports DVMRP
- Support Jumbo Frames
- Must offer Carrier Class Availability (99.999%)
- Must offer support for in-Line Power for IP phones using IEEE 802.3af standard
- Must offer support for 16 ports aggregation using IEEE 802.3ad standard

3.3.1.2 Routers

Router characteristics:

- Modular chassis routers are preferred
- Hot swappable line cards
- Interface cards/ports:
  - 8 port 10/100/1000 Mbps Ethernet
  - 4 port T1/E1 with RJ48C connectors
  - 4 port serial (V.35/X.21)
- Data rates:
  - Non-channelized T1/E1: Up to 2Mbps
  - Channelized T1/E1: Minimum 24 x 64kbps
- Protocol Support
  - Point-to-Point Protocol (PPP)
  - Frame Relay encapsulation
  - High-Level Data Link Control (HDLC)
  - Multilink PPP (MLPPP)
  - Multilink Frame Relay (MFR)
- Manageable via:
  - CLI
  - HTTP
  - SNMP

- Management Capabilities:
    - System status warnings
    - Reporting
    - Detailed threat descriptions and remediation information queries
    - GUI user interface
- Diagnostics:
    - Digital diagnostic loopback
    - Payload loopback
    - Line loopback
    - Alarm Indication Signal
    - LED’s for: Active, Fault, Local Alarm, Remote Alarm, Carrier detect and loopback
- E1 Interface
    - Transmit/Receive rate: 2.048 Mbps
    - Framing format: CRC4, non-CRC4
    - DTE /DCE interface: ITU-T G.704/G.703
- T1 Interface
    - Transmit/Receive rate: 1.544 Mbps
    - Framing Format: D4 super frame and extended super frame
    - DTE /DCE interface: ITU-T G.704/G.703
- Channel Service Unit/Data Service Unit
    - Selectable cable length
- Routing
    - Static
    - RIP v1/2 dynamic routing
    - VPN routing and forwarding
    - Virtual Router Redundancy Protocol (VRRP)
    - Generic Routing Encapsulation (GRE): IP
    - Border Group Protocol (BGP)/OSPF dynamic routing
- Firewall Features
    - NAT (Network Address Translation)
    - Stateful packet inspection and filtering
    - Network Attack Detection
    - TCP reassembly for packet protection
    - Malformed packet protection
    - Protocol anomaly: IP, TCP, UDP
    - Application Layer Gateway
        - FTP
        - TFTP
        - DNS
        - DHCP
        - SIP
        - Network File System (NFS)

        - Real Time Streaming Protocol (RTSP)
- QoS
    - L3/4 traffic policy definition
    - Ingress policing
    - Egress shaping and priority egress scheduling
    - Differential Services (DiffServ)
    - Call admission control
- VPN (IPSEC)
    - Site-to-site VPN tunnels minimum 2000 tunnel interfaces
    - Encryption: DES, 3DES and AES
    - Authentication (MD-5 and SHA-1)
    - Perfect Forward Secrecy
    - IPSec NAT traversal
    - IKE with pre-shared key or PKI
- Intrusion Detection and Prevention
    - IP Spoofing, Backdoor and DoS Detection
    - Worm, Trojan and Reconnaissance protection
    - Protection against proliferation from infected system
    - Request and response side attack protection
    - Traffic interpretation: Reassembly and Normalization
    - Prevention Mechanisms
        - Drop packets
        - TCP resets client and/or server
    - Notification via log viewer or Syslog
- LAN Features
    - STP
    - Bridging
    - VLAN support
    - Access, trunk and hybrid mode
    - Integrated Routing and bridging
    - Port Mirroring
- Network Services
    - DHCP relay/server
    - DNS client
    - FTP/TFTP client
    - Telnet server/client
    - Radius client
    - TACACS client
- Administration
    - Local administration db
    - Chassis manager (where relevant)
    - System management and logging
    - Support MIB’s for example Standard and custom MIB’s, MIB II

- Ping and traceroute

- Standards
  - IEEE 802.1D 2004 (STP)
  - IEEE 802.1X (Port-based Network Access Control)
  - IEEE802.1x (EAP)
  - IEEE802.1Q (Tagging)
  - IEEE802.2 (Logical Link Control)
  - IEEE802.3 (Ethernet CSMA-CD)
  - IEEE802.3ab (1000BaseT)
  - IEEE802.3z (1000BaseX)
  - ITU-T G.703. G.704

3.3.1.3 Hardware Based Firewalls

Hardware Based Firewall Characteristics:

- State-full Packet Filtering - Must have a TCP State Aware Packet Filter Technology.
- Throughput 200Mbps scalable to 400 Mbps.
- Concurrent connections: 130,000
- Simultaneous VPN tunnels: 2000
- 168-bit 3DES IPSec VPN throughput : Up to 135 Mbps with VAC+ or 63 Mbps with VAC
- 128-bit AES IPSec VPN throughput: Up to 130 Mbps with VAC+
- 256-bit AES IPSec VPN throughput: Up to 130 Mbps with VAC+
- Support for unlimited number of networks.
- Support for unlimited number of users.
- Support Dynamic NAT and Static NAT. Capability to redirect the port requests to user configurable ports (PAT).
- Integrated Security – Must have an inbuilt Anti-spoof engine to drop all such packets.
- Ability to drop all the IP fragment packets.
- Protection against popular attacks such as ping-of-death attack, tear-drop attack, etc.
- Administrator must be able to configure the default timeout for TCP/UDP services.
- Ability to send mail alerts to the administrator.
- Ability to log the number of active TCP/UDP sessions.
- Must have firewall configuration backup and restore facility.
- IP Traffic Control to be based on Source, Destination, Protocols, Ports, etc.

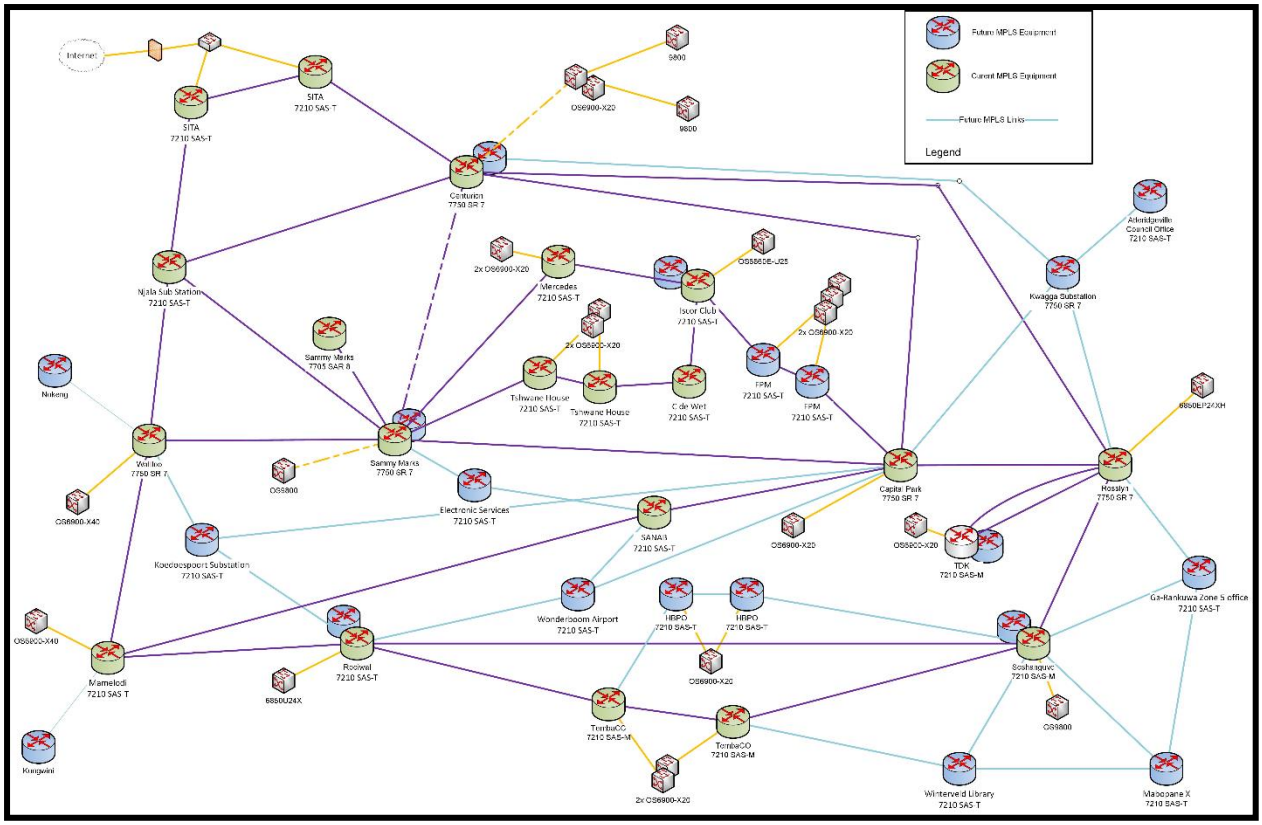
- Provide secure encrypted Web-based Remote Management.
- Provide different privileges for administration and management.
- Display firewall server's current date and time in remote Administrative Console.
- Able to create policies based on Objects
- Must be able to reconfigure the firewall parameters and policies from remote console.
- Provide selective viewing of Logs based on source, destination, source port, destination port, rule number, time etc.
- Auto refresh the most recent logs while viewing.
- VLAN (802.1Q) support.
- Electro Magnetic Compatibility (EMC): FCC Part 15 (CFR 47) Class A, ICES-003 Class A with UTP, EN55022 Class A with UTP, CISPR 22 Class A with UTP, AS/NZ 3548 Class A with UTP, VCCI Class A with UTP, EN55024, EN50082-1 (1997), CE marking, EN55022 Class B with FTP, Cispr 22 Class B with FTP, AS/NZ 3548 Class B with FTP, VCCI Class B with FTP.

3.3.1.4 Transceivers/Convertors

- Depending on the situation, 100/1000Base-SX/LX (fibre) to 100/1000Base-T/TX (copper).
- Must be standards based. One or more of the following standards shall apply depending on the transceiver/convertor.
    - IEEE 802.3ab
    - IEEE 802.3z
    - IEEE 802.3u
- Connectors: SC/LC (fibre), RJ-45 (copper)
- Full Duplex Support
- Must support crossover detection and auto-correction
- Status LED for Power and Link/Activity
- Must function with standard South African supply voltage i.e., 220/230V single phase.

3.3.1.5 MPLS (Multi-Protocol Label Switching)

CoT has invested in a MPLS backbone, and the tenderers must offer equipment that will integrate 100% with the existing solution. The existing backbone is shown below:



3.3.1.6 Optical Service Switch

Characteristics:

- DWDM switch
- GigE and 10GigE multiplexing
- 1/2/4/8 Gigabit fiber channel multiplexing
- E1/DS1, STM-1, STM-4, and STM-16 multiplexing
- Ring and point to point from 10 to 40 Gb/s
- SDH-alike protection possibilities

Typical deployment:

- Data center interconnection
- Private WAN for large enterprises

3.3.2 Wi-Fi Equipment

The CoT has an existing Wi-Fi network, but this network will be extended in future. The network provides for:

- Free public Wi-Fi access to the public at Customer Care and Libraries
- Boardroom and building access via Wi-fi for CoT personnel
- Future inclusion of Wi-Fi blanket to cover the City.

Some futures that the network must be able to support:

- Security related to public and CoT users

- Redundancy solutions i.e., should the controller fail, a backup controller must enable continuous and seamless integration.
- The ability to load more than one SSID on an AP should the need arise ie for VIP Wi-Fi, Public Wi-Fi or normal CoT everyday use.
- Software related to Wi-Fi support, coverage, security, data usage etc.

3.3.3 Security

Network security devices (software/hardware based) to be included in the pricing:

- Firewalls (Internal to network and edge protection) for example Fortinet Unified Threat Management
- InfoExpress Cybergatekeeper
- Wi-Fi security

A firewall is a set of related services, located at a network gateway server that protects the resources of a private network from users from other outside networks. Traditional network firewall services use IP-based access/deny policies, while more recent technologies allow deep packet inspection, being able to enforce policies on acceptable application usage and detection of malicious out-of-band transactions.

The service is made up of various service “layers”, with options according to customer requirements:

- Range of security appliances (firewalls) and associated software / applications, from leading security bidders, provided as SP Equipment
- Fault management; 24x7 customer helpdesks, on-site maintenance and proactive service monitoring
- Configuration management; application patches and changes to customer security policy
- Service reports; service availability, security-related events
- Security consultancy to assist the customer in defining their security requirements (covered by cross-functional services SOW)
- Project managed service installation and service commissioning (covered by cross-functional services SOW)

The optional features provided within the service include (where applicable):

- High availability (resilient) designs
- IPSec VPNs
- De-Militarized Zones (DMZs)
- Threat mitigation

3.3.4 Voice Equipment

Any solution offered to Council must integrate seamlessly without any loss of features. No current feature may be implicated or lost in this process. Should any service provider offer a solution other than the current deployed infrastructure deployed, said service provider must guarantee this integration. Any current and future development cost to enable this requirement will be for the service provider's account. This will extend into the warrantee and guarantee period. However, provision must also be made to allow for a hosted service integration into/parallel to the current deployment.

3.3.4.1 System Architecture

3.3.4.1.1 IP PBX General Specifications and Infrastructure

- The system should provide telephony functions on any underlying data infrastructure – it must be scalable to support and voice/data convergence and traffic increases – as new sites are brought into the network.
- The system call server must be based on SW easily updatable and manageable
- Guaranteed system uptime of 99,999%
- The systems should be able to use SIP end points as extensions for the users and SIP trunks to be interconnected with other IP PBX and to access value added applications like collaboration or Unified Messaging
- The system should offer the choice between distributed or centralized communication servers and media gateways without jeopardizing the WAN VoIP links, features level and applications availability
- The system should integrate with TDM equipment and enable any mix between IP or TDM and Wired or Wireless phones
- The system should be scalable, distributable and modular
- The system should manage CAC (Call Admission Control) mechanisms to optimize the usage of the bandwidth in the WAN for multi-site configurations
- The system must manage a large range of telephonic services, integrated contact center applications, collaboration and Unified Messaging applications
- The system must be able to interoperate with other telephone systems and endpoints using the below standards – Qsig GF, Qsig BC, DPNSS, DSS1, H232, SIP.
- The IP PBX system should provide standard APIs compliant with Internet standards like XML, SOAP & WSDL for CTI, call control and management functions
- The IP PBX system should also provide legacy APIs such as CSTA, TAPI, CSTA
- The IP PBX system should provide call routing points for connecting Contact Center applications

3.3.4.1.2 System Hardware and Software

- The IP PBX hardware must have high flexibility in term of capacity, system upgrade and support IP & TDM without external interfaces.
- The Call Server should able to support minimum 15000 users in a standalone configuration and support up to 100 000 users in a virtual and multi-servers network group.
- The Call Server should able to handle traffic minimum 300K BHCA.
- The system must support the following external telephony interface signalling: E1 CCS PRI (VN3-4-6-7 /ETSI) DASS2, E1 CAS (R2, Q421, MFC Ericsson, Q23, Decadic), T1 CCS generic, T1 CAS, T0 ISDN BRI (VN3-4-6-7 / ETSI), E&M, Analogue Loop Start and Ground Start (with FSK and DTMF CLIP).

- The switching must be able to handle Power over Ethernet devices. PoE devices must be managed for: Economic efficiency according to device needs, Security to avoid overload of the system or the device.

- For bandwidth intensive users, the bidder should be able to supply a switch device to distribute PoE to supplementary Ethernet devices.

- The device must be an economic, plug and play device that offers: auto negotiated 10/100/1000 BT transfer, port-based and 802.1Q VLAN support, 802,3af remote power.

- The proposed system should be based on “open” software architecture, Linux being the preferred one.

- The architecture based on soft-switches should permit the geographical relocation of the communication servers through a standard IP network. Media Gateways should be carrying the interface cards, which should generate their own feeds from a common source.

- The system's software can be hosted in appliance servers or in blade servers architectures

- The system must manage, control and support a range of IP telephone stations for both voice and telephony applications as well as IP application stations for voice, telephony, and Web services support

- The proposed system must support native IP communications in direct or "peer-to-peer" with only the telephone signalling transiting back toward the controlling communications server.

- The voice and signalling frames should be marked [tagged] in order to be recognized. The standards of marking supported will be: Level 2: IEEE 802.1p/Q and Level 3: TOS / DiffServ

- The system should support for voice encoding the following standards: G.711, G.723.1, G.729A.

- The proposed communications system must support H.323, SIP, XML technology

- The proposed system should integrate an H.323 gatekeeper server, without external equipment, that offers the following services: - Automatic registration of the H.323 terminal and assignment of a call number by the RAS protocol; - Resolution of the address, the terminal H.323 can be identified by its call number or by its IP address that can be assigned dynamically by a DHCP server; - establishment of communications in direct mode.

- The proposed system should include the gateways required to allow the buyer to acquire H.323 or SIP devices to interoperate with the traditional telephony devices (digital stations, IP, analogue, private or public lines).

- The proposed system should permit the integration of SIP terminals with other terminals. The SIP modules are: SIP Proxy, Registrar and Gateway

- The hardware of the proposed system must be compliant with the European directive: Restriction of Hazardous Substances in electrical and electronic equipment (RoHS)

- The proposed telecommunication system should allow the use of high level XML APIs based on Web technology standards (XML/SOAP) to ease creation of telephony and call control features for integrating telephony services into web applications.

3.3.4.1.3 Required Profile of the proposed solution

To provide an economic future-proof network, it is important that the current and future working methods should be studied. An audit must be done to qualify and quantify these different types of communications for the client needs and requirements. Based on this type of study the bidder should be able to:

- Determine the types of telephony hardware devices required by the different types company personnel
- Determine the types of telephony services required for the company personnel
- Provide the reasons for the choice of products
- Based on the findings the bidder should be able to provide the devices and services listed in the audit

3.3.4.1.4 System Management

- The IP PBX system should provide a suite of applications and tools to permanently evaluate and report the operational health of the system. It should provide the following functions:
- Software licensing check
- Automatic recognition of plugged sets
- User moving
- Monitoring of all the events on the system
- Capture of performance and level of use of the resources
- Register and log all calls and give accounting information
- Monitor and register all users, attendants, trunks activity to generate traffic and level of use analysis
- The IP PBX system must include the possibility to have remote maintenance access via dial-up having access to the system for configuring, diagnosis and monitoring. This access must be protected with security mechanism to prevent unauthorized intrusions.
- The system must include a dedicated management server/platform that will be based on the latest technologies, such as JAVA/JEE. This server should support a minimum of five (5) clients having different access rights to the applications
- The management platform must provide a single graphical client (Graphical User Interface GUI) as well as a web based interface
- The Management platform must provide web access allowing the administrator to manage the system to use any PC with an internet browser

- The management platform must use a client-server architecture allowing different administration clients to be connected to the system
- The management platform must perform at least the following tasks:
- Configuration and programming of services, users, categories and all system parameters and features. This module must provide centralized management in local or remote environments of a single system or a network. The network manager will be able to quickly and easily edit, create or delete any network object, by the use of import/export functions and multiple operations
- Faults and Alarms management of all the incidents and fail reports generated by the system itself informing date, hour, severity level and action recommended to take. This module must be able to centralize the alarms and events of the system, and
- Notify an alarm depending to the severity level sending an e-mail or activating an script performing an specific action
- Register and generate statistics for the alarms and events in the network in a daily scheme
- Each Alarm must include at least: An identification number, The severity level, The manage object, The notification time, Additional Information, The event type, The probable cause, A Fault diagnosis.
- Generate reports and graphics about the statistics of the alarms and its correspondent resolution time
- Accounting of all calls generated by the users including cost, date, hour. Must provide different options to group the billing of the calls (cost center, extension number, trunk, user, city/area associated to dialled numbers). The accounting module must be able to:
    - Adapt to the financial organization of the company along the cost centers and the organization levels
    - Manage carriers' fees to apply specific costs. Must be able to manage multi-carrier schemes
    - Define thresholds for phone usage and Tracking/monitoring this activity, providing a graphical view of the accounting thresholds per user, cost center or group
- Generate reports and graphics classified by: User, Cost Centre, Organizational Level, Duration, Pin, Project Code, Number Dialled (Destination), Carried used.
- Performance and traffic Analysis of the operation of the system. This must include at least the following information:
    - Measurement of response time
    - Measurement of the VoIP traffic
    - Statistics on the quality of VoIP calls
    - Statistics on the line-occupancy ratio for incoming calls

- Reports and graphics on attendant, trunks and users traffic
- Occupancy rates of the different internal and external links
- Average time spent waiting for an attendant

- The performance module must provide specific tracks on the voice over IP calls to better follow-up of the VoIP traffic and quality, for this, the system must measure:
  - VoIP volume of traffic (volume sent, received and lost)
  - It must generate reports of this activity by periods of time (hourly, daily, monthly)
- Optional must provide:
  - Directory, module to manage the telephone directory. This must be LDAP compatible to be synchronized with other directory applications, must also allow web access and provide information on all desktops allowing click to call features to the users.
  - The management server should provide an application that offers a topological view of the telecommunications system that constitutes the organization's network, as well as the links that exist between sites.
  - The management platform must allow the administrator to generate reports and graphics of the activity per period of time in terms of traffic, accounting and alarms and giving the possibility to generate statistics of all this analysis. Those reports must be predefined but the option to personalize the reports must be also available. These reports should be exportable in HTML, pdf, excel and LDAP(.ldif) formats
- All IP PBX management applications (Fault & alarms, Configuration, Accounting and performance) should belong to a single platform and a single image for data storage, minimizing operation expenses.
- Optionally the management platform should offer a monitoring module which allows the administrator to easily monitor the accounting thresholds of the users of cost centers in graphical interface and must allow to send an e-mail or an alarm in case of threshold crossing.
- The management platform must include an troubleshooting & diagnosis tool accessible by WEB to be used by non-expert administrators
- The management platform should be able to be integrated with enterprise global network management platforms (like CA Unicenter TNG, HP Openview, or IBM Tivoli) using standard protocol SNMP.

3.3.4.1.5 System Security

- The bidder must only propose an offer that meets with at least the EAL2 requirements of the Common Criteria (ISO-15408) standards
- The system must support centralized firewall management
- The system must support dynamic pin holing to limit access security breaches

- Call Server Security
- The Operating System used by the call server must not use or natively support network resource sharing services (such as NFS, Samba, LPR, etc)
- The Call Server and Media Gateways must provide self-protection mechanisms to counter Denial of Service attacks
- The call Server must avoid the usage of possible virus, worm and Trojan infestation points, such as internal e-mail servers
- The call server must avoid the usage of automatic "download & execute" programs or services from databases or Internet inbound connections
- Internet access from the call server must be restricted to administrator initiated remote maintenance tasks only
- The System must support Network Time Protocol V4.1.2 (RFC 1305) to synchronize the system data/time of network devices
- The System must support Syslog services for both internal and external command and configuration control accounting with a minimum of 5 day history
- The Call Server must not employ the use of a 'default' password that is viable beyond the period of installation.
- The password & access control must include at least:
    - Shadow Passwords to prevent the possibility of an aggressor to easily read or deduce system or account access passwords.
    - Password Aging with configurable time periods
    - Usage of MD5 algorithm (or stronger) for password encryption
    - Internal OS controls for remote point of access restriction and service availability. (i.e. TCP Wrappers & Trusted Hosts)
    - Account access authentication/restriction using external RADIUS resources.
    - Media Gateways should not host services such as proxy, FTP, Telnet or local dynamic routing to prevent exploitation in Distributed Denial of Service attacks.
    - IP Phones should not support direct, external initiated, connections via HTTP, telnet, FTP, TFTP or any other protocol as means to prevent distributed Denial of Service attack exploitation.

Network Security

- The system should offer maximum availability, with the switchover of call control processing functions to an alternate or redundant processor (or soft-switch control point) in the event of significant fault. The redundancy scheme should conform to the model used in most computer systems: the complete "mirroring" of the information (both static and dynamic data.) The switch over between 2 redundant call control processors should not interrupt existing and established communications.

- All critical resource elements (call server, hard disks, data bases, IP interfaces, DSP resources, clocking sources, etc.) must be redundant and in a hot-standby configuration, allowing to install them in two (2) different data centres physically separate

- Media Gateways must have survival mechanisms that allow them to maintain nearly 100% of the telephony services for their users, in case of failure in the WAN links where the signalling with the call server drops.

- IP Phones must support 802.1x (EAP-MD5 or better) for authentication and access control to the network, this mechanism must allow the user to be connected to the call server once he has passed the authentication process; not before.

- The system should have the capability to, based on standard mechanisms (such as 802.1Q and DHCP), assign automatically the corresponding voice VLAN number to the IP station clients during IP station initialization, allowing for the separation of voice and data traffic at the IP station.

- The IP station must have the ability to strip any VLAN tags assigned to traffic entering the network through the 'guest port' of the IP station, and further have the ability to switch that traffic into an identified data VLAN, further enhancing enforced voice and data traffic separation.

- The IP station must have the ability to disable its 'guest port

Management Security

- Administration users connecting directly to the Call Server (console) must be authenticated via a RADIUS server before gaining access to the call server.

- All management traffic between a remote console/session and the call server must be encrypted. (SSH for direct command line sessions, HTTPS (SSL) for web sessions, SFTP for file transfers, etc.)

- Administrators connecting to a management platform must be authenticated via a RADIUS server prior to gaining access to the management platform

- Management flows between the management platform and the call server must be encrypted (SSH, SSL, CMISE, SNMPv3)

- The management platform must provide Role Based Account Management to define different levels of administrator access depending on specific function responsibility.

- The management Platform must provide a backup mechanism for all critical system information in both a manual and an automatic/scheduled archival and a Disaster Recovery mechanism.

Application / Communication Security

- The IP PBX system should provide complete encryption capabilities with the ability to encrypt all traffic (media and call control signaling) between IP phones, softphones, call controllers, media gateways and all other associated endpoints via a strong encryption algorithm (AES, IPsec and SRTP, for example).

- The encryption solution should be hardware-based in order to eliminate system degradation and transmission delay times.

- The system should encrypt the voice content as well as the signaling between the IP station and the call server.
- The encryption solution should be easy to deploy with factory pre-installed certificates and automatic key distribution facilities, requiring no “at-the-phone” intervention
- Wireless IP Phones must support WPA2(AES) for traffic encryption proposes
- For multi-node solutions, IP stations must be capable of communicating via encrypted streams between any and all physical and logical network areas
- Application users should be authenticated using a RADIUS system before being granted access to application servers or associated resources.
- Any web based application must use HTTPS encryption

3.3.4.1.6 Telephony Services

The offered system must support the following services without any external/additional server to support them:

- Text mini-message between advanced sets
- Reception of absence mini-message from the called user
- Calling Line Identification Restriction (CLIR) for local / internal calls
- Communication timeout on outgoing call
- Barring for internal and external calls
- Call Waiting on: Busy set, busy hunting group, busy voice mail
- Intrusion on busy set
- Intrusion on busy set: On no Reply, On busy
- Call back to last caller: Local / Internal, External
- Automatic call back (activate / cancel) on: No reply, busy set, busy trunk group
- Call back request (activate / cancel) on: No reply, Busy Set
- Call back request notification by : LED on the user's set, Icon on wireless phones, Voice guide for analogue sets
- Dial by name with central directory repository
- Last number redial
- Multiple redial
- Abbreviated dialling
- Automatic call set-up on unhook
- Private call / Personal Identification Number (PIN)

- Distinctive ringing for internal and external calls on all types of sets
- Call Overflow: Overflow on either busy or no reply, Overflow on both busy and no reply, Overflow on out of order
- Timed call overflow on no reply
- Call Pick up: Individual or in group
- No Replied Calls Repertory: Local / internal calling numbers with caller name, date and time of calls
- Enquiry call / enquiry call cancel
- Call transfer on: Reply, No reply, Busy
- Call transfer to: Set, Hunting Group, Attendant, Voice Mail, Trunk to call transfer, Trunk to timed transfer
- Three Participants Conference (Multiple)
- Meet-Me Conference
- Announcement / Paging on Loudspeaker
- Announcement / Paging on Loudspeaker
- Calling party name identification (CNID)
- Direct inward dial (DID)
- Direct outward dial (DOD)
- Direct inward system access (DISA)
- User set creation : user validation of his set created by attendant
- User moving : personal plug in / plug out by prefix
- Call recording on voice mail
- Voice guides indicating/helping users independent of type of set
- Outgoing call with business account code (by prefix or suffix)
- DTMF / Pulse Transparency
- Appointment Reminder
- Call Hold
    - Automatic exclusive hold (in case of enquiry call or call waiting consultation)
    - Manual exclusive hold (by Hold or line key or by prefix)
    - Common hold (by Common hold key)
    - Mutual hold (initial hold by Hold key)

- Call Forwarding:
    - Unconditional
    - On no reply
    - On busy
    - On Busy or No Reply
- On ringing (Call Deflection)
- Forwarding destination:
    - Set
    - Voice Mail
    - Hunting Group
    - Attendant of Attendant Group
    - Call Centre Group
    - Automated Attendant
    - External Number
- Substitution
- Monoline or multiline mode for advanced sets
- Multiline key per directory number for advanced sets
- Multi-directory number (DN) for advanced sets
- Multi-directory numbers (DN) with supervision (indication of state) of:
    - Set
    - Trunk
    - Trunk group
- Manager / Secretary features:
    - Call Filtering with manager control
    - Manager/Secretary hot line
    - Private Line for Manager set
    - Absent secretary key
    - Secret listening of the secretary by the manager
    - Multiple Managers / Multiple Secretaries

- Twinset: Two multiline sets with (same) Directory Number (TDN) and common voice mail and accounting
- Personal password for
- set lock override for DOD
- set unlock
- Substitution and DISA
- DND
- General mini messaging consultation
- Programming individual repertory
- key programming
- follow-me
- remote forwarding
- private call
- consultation of no replied calls repertory
- Hunting Groups
- Do not Disturb

3.3.4.1.7 End User Devices and Terminals

- End Users must be able to access all telephony services
- Voice prompts or guides (multi language) the system should guide users during the various steps needed to activate specific features by means of voice guides that indicate the services available at each stage of a call.
- Multi-language display on TDM and IP stations - The language presented on the station displays must be changeable by the user directly. When the user makes this change, the modification of the display language will automatically synchronize the language of the vocal guides and the prompts on the voice-messaging component.
- Call (dial) by name - Users whose station is equipped with a display and alphabetic keyboard should have the capability to call, to transfer, or forward calls to other internal or external parties by entering their NAME.
- Multi-key / Multiple-number stations - This function allows a user with a station that is assigned only one number, to simultaneously establish several outgoing or incoming calls. Each station key can be programmed for a different extension number, to permit easy differentiation of incoming calls.
- Call Screening - Several screening stations can supervise a screened station. A screening station can screen several stations and lastly a station can have the status of screening station and screen station simultaneously

- Work groups - Users should be able to clustered in Supervised workgroup, station group or Intercom group
- Text messaging - Users whose station is equipped with a display and alphabetic keyboard must be able to conveniently access a text messaging service, allowing them to exchange short messages from terminal to terminal
- Automated attendant - the system should be equipped with an automated attendant system that, under designated conditions, welcomes outside callers, and proposes (in an interactive manner) a way to reach a desired service or pre-defined party
- Music on hold - The music source will support X seconds of operation, and should provide a good tonal quality. For reliability, the system proposed should be digital (magnetic devices are excluded) regardless of whether it is integrated into the system or external to the system.
- Direct Inward System Access – DISA - allow a user who is calling from outside of the system to establish an internal or external system connection from his or her DTMF telephone.
- Remote management of the telephone - allow a user who is outside of the system to modify the answering modes of his or her telephone terminal (voice messaging, external call-back, etc.)
- IP Telephone stations should support dial by name features using alphanumeric qwerty integrated keyboard

IP Telephone stations should support:

- 802.1x (MD5) for authentication
- Remote power feed per the 802.3af standard or local 120 / 230 -volt feed
- Auto-sensing 10/100 Ethernet switch interfaces
- PC port 10/100
- IP address Assignment by DHCP or statically configured
- QoS (Internal the station and priority to the voice signal)
- Frame marking voice level 2 802.3 p / Q and level 3 ToS / DiffServ
- Transparent recovery of frames by the associated PC (not by the station)
- Fixed or dynamic assignment of the IP address by customer DHCP
- AES for voice content encryption
- G.711, G.723.1 and G.729a Audio compression

IP and TDM Telephone and application stations should support:

- Large colour or black and white adjustable screen at least for the IP phones

- Context-sensitive keys associated to the display – These contextual keys are linked to the context displayed on the screen to directly activate function
- Navigation keys to navigate inside the graphical interface (change of application or context, return to the home page)
- Numeric keypad to dial a number or enter digits in an entry field
- Integrated alphabetic keyboard for functions such as text messaging and dial by name
- Full duplex hands-free mode with echo cancellation • Audio operation to tune audio levels, mute, loudspeaker,
- Connector for headset or additional speakerphone
- Automatic and transparent switch from one to another communication mode (headset, handset, hands-free, etc.)
- Wireless Bluetooth® capabilities (Based on 1.2 Bluetooth© specification) at least for the IP phone
- Open to applications: Access to corporate or external Web based application via third party SDKs, APIs (XML, SIP)
- The system must support an IP Softphone application that allows the users to manage their calls from a PC. This user must have access to the full set of telephony services without any degradation. The voice should be manage by the multimedia resources of the PC
- The system should support PC based Attendant terminals that have a colour screen, as well as attendant station software that can be used on PCs that are not dedicated to the attendant operation

Attendant operator positions should support the following features:

- Station Supervision
- Manual or Automatic answer
- Call by name to internal or external parties
- Text Messaging
- Multiple Attendant positions
- Call Recording
- The phone sets should support alphanumeric integrated keyboard
- The system must support an Attendant IP softphone application that allows the operators to manage the calls from a PC. This application must support the same features of the Attendant operator. The voice should be managed by the multimedia resources of the PC.

3.3.4.1.8 Wireless Terminals

The system should support a fully integrated and feature rich wireless phones solution for either TDM or IP sets

- Telephone sets must comply with current RoHS requirements
- The mobile phones should be tested and certificated for: Dust, Humidity, Physical Abuse (Drop Test)
- The level of services offered on either TDM and IP wireless sets must be the same of the desktop phones and only restricted by each kind of set ergonomics itself.

Mobility requirements

- The system must provide for: Dect, VoWlan, Cellular Extension, Dual Mode, Softphones, VPN
- Mobile Applications such as: Microsoft Win 5/6, Symbian, Nokia Intellisync Call Connect Client

IP Wireless Phones

- The IP Wireless Phones should support Wi-Fi 802.11b 2,4 GHz radio
- The IP Wireless Phones should support Wi-Fi 802.11b 5,150_5,825 GHz radio
- The IP Wireless Phones should support G.711a, G.711mu and G.729 audio compression codecs
- The type of transmission should support 802.11a, 802.11g: Orthogonal Frequency-Division Multiplexing (OFDM), or 802.11b: Direct Sequence Spread Spectrum (DSSS)
- Transmission data rates should be in the 802.11b network: 11, 5.5, 2, 1 Mb/s, auto rate selection, or for 802.11a and 802.11g: up to 54 Mb/s
- The IP Wireless solution must offer a QoS on the Wi-Fi radio spectrum solution
- If a spectra link Voice priority is used - Spectralink Radio Protocol- Timed Delivery- Spectralink CAC
- Without Spectralink:- Wi-Fi Multimedia (WMM)- U-APSD- Tspec, the IP wireless phones should have at least following functions:
    - 128x64 pixels display
    - 4 dynamic keys having function according communication state
    - 1 Key to access the functions menu of the phone
    - 1 key to navigate on the menu
    - 1 function key to access a customization menu
    - Option to connect a corded headset
- The IP Wireless phones must support IP address assignment by DHCP
- The IP Wireless phones must support the following standards for security features:
    - 128 bit static Wired Equivalent Privacy (WEP)

- Wi-Fi Protected Access (WPA)
- WPA Pre-Shared Key (PSK)
- Temporal Key Integrity Protocol (TKIP)
- IEEE 801.11i, Wi-Fi Protected Access 2 (WPA2)
- Advanced Encryption System (AES) Algorithm
- The telephone must support G.711, G.729a/ab voice encoding

- The IP Wireless phone must provide easy access to the dial by name features of the IP PBX system
- In addition to the standard 256 Latin characters, Greek, Cyrillic and Unicode characters should be handled
- Supported languages should include: French, English, Spanish, German, Dutch, Portuguese, Italian, and Greek
- If required by the client, a push to talk feature should be available

TDM Wireless Phones

- The system must offer a range of TDM Wireless Phones that support the below standards:
  - Digital Enhanced Cordless Telecommunications (DECT): 1880 - 1900 MHz
  - Digital Enhanced Cordless Telecommunications (DECT): 1900 - 1930 MHz
- The TDM Wireless Phones should have at least following functions:
  - Graphic Display with monochrome or colour availability, as required by the client
  - Dynamic keys
  - Menu access key
  - Navigation key
  - Directory key
  - Trackpoint key
  - Volume Key
  - Option to connect a corded headset
  - As required, a loudspeaker should be available
- The TDM Phone should support the following security features:
  - International Portable User Identity (IPU-I) for user identification proposes

- 128 bits encryption key for authentication
- 64 bits key for signalling and content encryption

- The TDM Wireless phone should support (for DECT) the GAP and Advanced GAP (AGAP) mobility level of services
- The TDM wireless phone must provide easy access to the dial by name features of the IP PBX system

3.3.4.1.9 Voice Messaging Systems

- Voice Messaging system must be fully integrated to the call server and should not require external server to be hosted
- Voice Messaging system must be fully integrated to the call server and should not require external server to be hosted
- Voice Messaging system must be manageable from the system management platform
- Answering or answering with date stamp - The system should provide voice mailbox holders the choice of two functions: answering the messages or answering them with a date stamp
- When a call is forwarded to the voice messaging system, the box holder will be able to choose between two personalized announcements. If the personal announcement has not been recorded, the standard system announcement will be substituted automatically.
- Recording of calls conversation - The holder of a voice mailbox must be able to take advantage of this service to record internal or external calls. Recorded calls will receive the same service as messages that have been left by callers.
- Forwarding of voice mail messages - The box holder will be able to send a copy of previously received messages to other boxes (with or without requesting acknowledgement of receipt.
- Call by name - To provide universal access, it must be possible to select a voice mailbox by its name by using the telephone dialling keypad. The caller will be guided in this operation by voice prompts.
- Multiple languages - To ensure consistency with the system voice prompts, the proposed system should be multi-lingual, offering four different languages
- The voice messaging system should be centralized or distributed to serve different sites
- The notification of messages must be on: LED/Icon on Phone, Voice Guide, Outbound call to any telephone number
- The voice messaging systems must provide silence detection to avoid recording of blanks at beginning or end of recording
- The System should allow distribution lists for message broadcast
- The System must allow the caller reaching a mailbox to choice forwarding destination

- The System must provide External Info-Service / Audiotex
- Additionally, the voice message system must provide the following features:
    - Record of standard Greeting
    - Record of alternate greeting
    - Record Name
    - Urgent delivery option
    - Voice mail navigation (rewind, pause, forward, play)
    - Skip Greeting
    - Confirmation to send recorded message
- Visual user interface with sensitive keys on large screen phones
- Autoplay of unheard/new messages
- Delete messages
- Save messages
- Reply Messages

3.3.4.1.10 Convergence

General

- To offer an economic solution, the client must be able to select an efficient IP network that takes into account voice, data and mobility
- The bidder must provide a coherent system that, by its convergent qualities offers superior network security, availability and manageability
- The convergence should provide seamless behaviour provided for the data and voice requirements
- The management should ensure the best possible use of routing to maintain voice and data traffic

Availability

- The bidder must provide a high level terabit capacity switch that can handle a fully converged IP communication network
- Blade centre support
- To reduce power and installation costs, the bidder must be able to offer PoE capabilities to distribute power as required according to the device class
- PoE must be managed in a secure way to provide for real economy and reliability
- Any homogenous network must be able to support up to 15000 IP users in a standalone and 100000 users in a multi network configuration

Security

- Any converged network must include a comprehensive structured security architecture to cover traffic inside and outside the network
- The security management should be centralized to improve cohesion
- To maintain security and availability the converged solution must be resilient and offer: 802,1x authentication for IP phones, Voice/data LAN partitioning, dynamic firewall pin-holing.

Management:

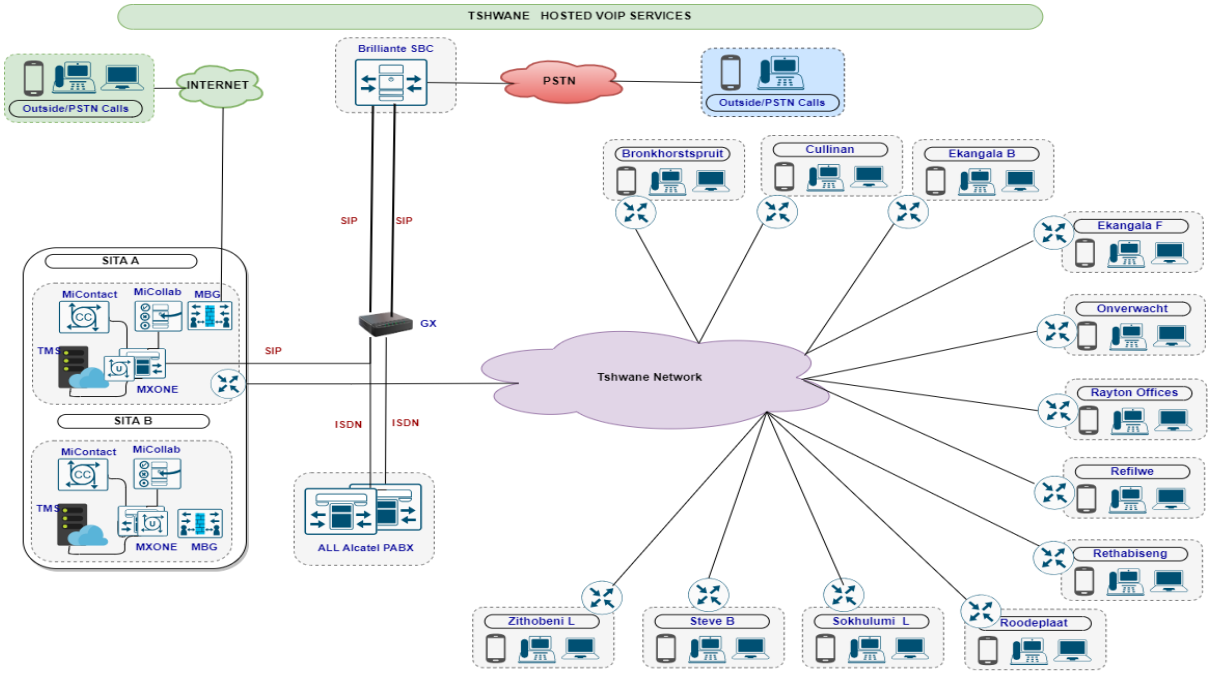
- The converged solution must offer centralised management solutions for the entire system that can offer:
    - QoS management
    - Inventory management for all IP devices and addresses
    - Performance management that can handle nearly all third-party devices switches and IP Phones
    - Central firewall management

3.3.4.1.11 Value Added and Mobility Services

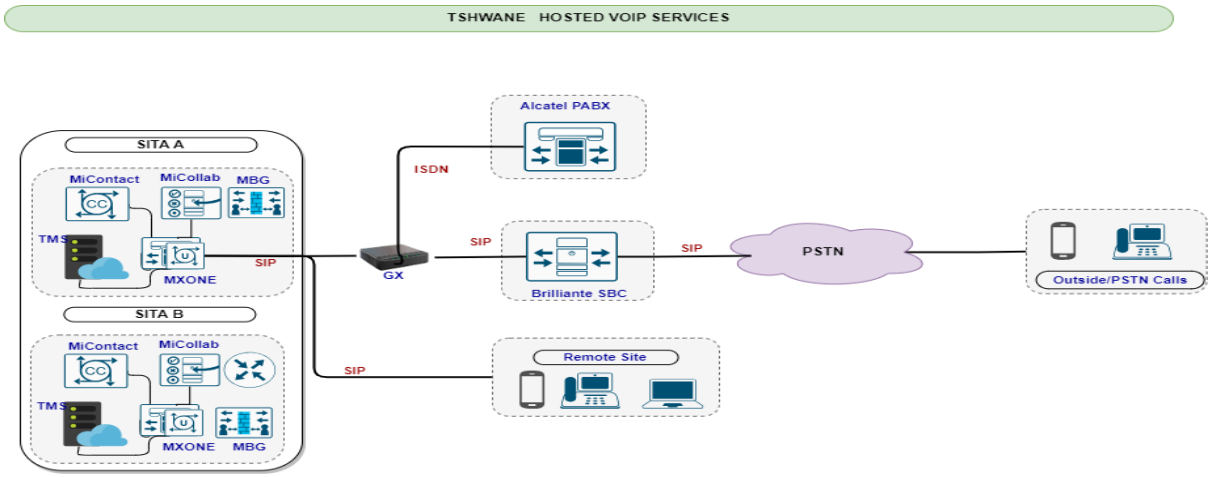
- Automatic Route Selection (ARS) to select the best route available to set up a call in terms of resources availability and cost
- The system should support free desktop / free seating features in stand alone or in multi-site
- The system should support an integrated cellular extension solution providing full IP PBX features from cellular-mobile phones supporting:
- The cellular extension application should not require external server, must be embedded into the IP PBX
- User of Cellular extension must be equipped with contextual menus running on any cellular phone: SIM based, Windows Mobile 5 and 6 based or Symbian based
- The system should support Dual Mode (Wi-Fi/GSM) terminals, Symbian & Windows Mobile 5 or 6 based to run both cellular extension and/or Wi-Fi softphones.
- The system should support Nokia Intellisync Call Connect Client
- The Dual mode cellular extension should be possible for SIP clients
- The system must allow remote users to be connected using softphone applications and having the same level of service as they were at the office desk
- The system should support users' mobile devices to work in tandem mode with the desktop phone

3.4 Hosting Solutions across the Voice and Data services spectrum

3.4.1 Hosting is a relatively new development in the market that has not yet been fully embraced by Council as to date Council has predominantly been focusing on legacy and on-prem solutions. Resulting in resultant high capex input cost and continued annual upgrade cost to stay recent as well the exorbitant licensing cost as is being charged. At present the Hosted Solution is provided to Council by Messrs Mitel and was deployed under the current Voice and Data Network tender. With connectivity being provided in the Sita environment and must also integrate seamlessly with the current deployed Alcatel/Lucent voice deployment as well the Alcatel/Lucent & Huawei deployment. The configuration of the current service/system, as was initially deployed in Regions 5 and 7 is as below. The VoIP network is in schematic 1 below.



Below schematic is of the Voice Network deployment.



3.4.2 Council has started moving moving towards the hosting environment with all of its IT applications, platforms and services, as per the above to schematics of the deployments done in regions 5 and 7 that is not very well equipped with own or rental infrastructure at present. This deployment will be carried forward over time to deploy the same over

the rest of the current network, emphasizing the smaller sites not yet accommodated onto the current network.

3.4.3 <u>It is expected of the Service Provider whom will be providing this service to Council to apply the following principles</u>:

- Any solution thus provided must ensure against data loss and must provide in for the insurance cost that might be brought about by any form of data, hardware or software loss.
- Any newly appointed SP must make sure that the Mitel hosting solution in place is catered for in their submission and also that they have the resources to provide for here.
- The cost for this must be provided for and will be for the account of the Service Provider.
- The service provided to Council must be built in such a way that it exceeds the minimum industry norms and must be flexible and adaptable to meet changes in Council's needs without having to go the tender route again.
- The Disaster Recovery DC must be TIA certified to ensure that it complies to all set norms and standards.
- The prosed solution must ensure that sufficient connectivity be provided into and onto the network that the principle of a single point of failure be negated/prevented.
- The SLA provided must be set at the 99% level.
- Guaranteed power availability beyond 4.4kW per rack, per customer must be guaranteed.
- Strict security controls must be applied to ensure rack isolation is guaranteed.
- Access control and video monitoring, remotely accessible (Remote Hands)
- Advanced fire detection & suppression and in-row precision cooling using the latest free air cooling solutions to reduce cost,
- Prime Location for disaster recovery DC,s must be identified preferably in Tshwane or if not available there, in the larger Gauteng area.
- BMS system (or a comparative system providing the same functions) must be provided to monitor all aspects of the Data Centre (24/7/365).
- Unrestricted Interconnects must be provided for.
- Skilled, technical resources – 6 Certified Uptime Institute Data Centre Design Engineers
- The solution provided must be a Intelligent Data Centre to allow for the use of and deployment of the latest AI technologies to improve security and enhance monitoring.
- Hosted Unified Communication solution must be deployed to ensure that a unified secure voice solution can be done from any location.

3.4.4 <u>The following Security principles must be provided for:</u>

- 24/7/365 on-site automated security
- Proximity & Biometric Access Control
- Digital Security Video Surveillance
- Follow Me AI controlled surveillance
- Automated reception visitor control'
- 512 bit SSL encryption depending on Client Certification
- IP address blocking (White- and Blacklisting)

3.4.5 <u>The following Support principles must be provided for:</u>

- Dark Disaster Recovery Facility
- 24/7 Data Centre Remote Monitoring

- Advanced Resolution System
- Trouble Ticketing System

3.4.6 The following Connectivity principles must be provided for:

- Unlimited Connectivity
- Private VLAN via Public & Private NW
- Geographically redundant DNS
- Dual-Stack IPv4 and IPv6 Capable

3.4.7 The following Power, Fire and Cooling principles must be provided for:

- A & B redundant Electrical Distirbution configured 2(n+n), better than TIA 3 certified.
- Fully redundant in row Cooling System configured 2(n+1), better than TIA 3 certified
- Fire detection and Gas Suppression system (Co2)

3.4.8 **The following Advanced Monitoring principles must be provided for**

- Remote monitoring systems, infrared cameras with unlimited recording preserved to be provided for
- Biometric access control system throughout the facility must be provided for
- 19 inch 42U racks with electronic access control

The current Mitel solution thus deployed has the following component configuration, that can provide services to up to 100 000 users. This configuration is regarded as the minimum requirement that must be provided for and must for part of this submission to council. Failure to do so will result in cancellation of the services providers submission to council. This is regarded as the minimum technical configuration to be provided. Any improvement on this will be regarded as a bonus and can be submitted as such.

- **Solution Components**
- 2 X- Virtual Platform Servers
- 2 X MXOne - Virtual Appliance - is a complete SIP-based communications system scalable from 500 to 100,000+ users, with a fully distributed architecture for deployment flexibility. The integration of voice, video and data with mobile capabilities provide increased efficiency and operation flexibility.
- MiCollab - MiCollab Audio, Web, and Video Conferencing is a Unified Communications Conference Unit within MiCollab that provides the ability to provide internal and external conferences of one-to-many users for voice, video, and presentation
- MBG – the Mitel call recording solution
- Connectivity - SIP trunks are presently established between the Mitel ICP and the SIP trunking service provider to Council, namely Messts Brilliantel,
- SBC – IP connected SIP trunks to Tshwane current network depending on current networkconfuration.
- MiContact Centre
- MXOne GX
- End point Devices – IP handsets and Soft Phone service deployment
- Training

3.4.9 The following hardware and software requirements must be met for the hosted voice and data solution as provided for on this bid to council

3.4.9.1 Entry Level Open Sip IP Phone

- SIP Protocol Support: An entry-level SIP phone should support this protocol for making and receiving calls over the internet.
- Number of Lines: Entry-level SIP phones usually support 1 to 2 lines, allowing users to handle multiple calls simultaneously.isplay: A basic monochrome or colour display is typical on entry-level SIP phones. The display may show caller ID, call logs, and other basic information.
- Keypad: A standard keypad for dialling numbers and navigating menus is included on entry-level SIP phones. Some models may have additional programmable keys for features like speed dial or call transfer.
- Audio Quality: Decent audio quality for voice calls is expected in entry-level SIP phones. Look for features like echo cancellation and HD voice support.
- Speakerphone: Many entry-level SIP phones come with a built-in speakerphone for hands-free communication.
- PoE (Power over Ethernet) Support: Some entry-level SIP phones support PoE, allowing them to receive power over the Ethernet connection. This can simplify installation and reduce cable clutter.
- Ethernet Port: An Ethernet port for connecting the phone to the network is standard on entry-level SIP phones.
- Headset Jack: A headset jack for connecting a headset for private conversations is a common feature on entry-level SIP phones.
- Compatibility: Entry-level SIP phones should be compatible with popular VoIP product and SIP-based PBX systems.
- Basic Call Features: Typical call features include call hold, call transfer, call waiting, caller ID, conference calling, and voicemail support.
- Support for SIP Trunking: Some entry-level SIP phones may support SIP trunking, which allows for making and receiving calls over the internet using a SIP provider.

3.4.9.2 Manager Level Open Sip IP Phone

- Multiple Line Support: Manager-level SIP phones often support a higher number of lines, typically 4 or more, allowing managers to handle a larger volume of calls simultaneously.
- High-Resolution Display: Manager-level SIP phones usually come with a high-resolution colour display that provides better visibility and allows for easier navigation of menus and features.
- Touchscreen Display: Some manager-level SIP phones may feature a touchscreen display for intuitive navigation and control of the phone's functions. Advanced Call Handling Features: These phones offer advanced call handling features such as call forwarding, call recording, call park, call pickup, shared line

appearances, and more to help managers effectively manage calls within their team or department.

- Busy Lamp Field (BLF) Keys: Manager-level SIP phones often come with programmable BLF keys that provide at-a-glance status information of other extensions within the organization, allowing managers to monitor the presence and availability of their team members.
- Expansion Module Support: Manager-level SIP phones may support expansion modules that can be added to the phone to increase the number of programmable keys for quick access to various features and functions.
- Enhanced Audio Quality: These phones may offer enhanced audio quality features such as wideband audio support, noise cancellation, and echo suppression for crystal-clear voice communication.
- Built-in Bluetooth and Wi-Fi Support: Some manager-level SIP phones may include built-in Bluetooth and Wi-Fi connectivity for wireless headset pairing and network connectivity.
- Integrated Gigabit Ethernet Port: Manager-level SIP phones often come with a Gigabit Ethernet port for high-speed network connectivity, ensuring optimal call quality and performance.
- Integration with Productivity Applications: These phones may support integration with productivity applications such as CRM systems, email clients, and other business applications to streamline communication workflows and enhance productivity.
- Customizable and Programmable Keys: Manager-level SIP phones typically offer a higher number of programmable keys that can be customized to access frequently used features and applications with a single touch. Support for SIP-Based Unified.
- Communications Platforms: Manager-level SIP phones are designed to seamlessly integrate with SIP-based unified communications platforms, providing access to advanced collaboration and communication tools.

3.4.9.3 Executive Level Open Sip IP Phone

- High-Quality Audio:
- HD Voice support for crystal-clear voice communication.
- Wideband audio codec support such as Opus, G.722, or similar for enhanced audio quality.
- Noise-cancelling technology to minimize background noise and ensure clear conversations.
- Advanced Display:
- Large, high-resolution colour display for easy navigation and viewing of call information, contacts, and other features.
- Touchscreen interface for intuitive control and operation.
- Customizable display options to personalize the user experience.
- Expandability and Flexibility:
- Support for multiple lines/extensions to handle simultaneous calls or manage different departments/teams.

- Programmable soft keys and function keys for quick access to frequently used features and functions.
- Compatibility with expansion modules for additional line appearances or programmable keys.
- Integration and Connectivity:
- SIP protocol support for seamless integration with VoIP systems and platforms.
- Built-in Ethernet port for network connectivity.
- Optional Wi-Fi support for flexible placement within the office environment.
- Bluetooth connectivity for pairing with mobile devices or wireless headsets.
- Enhanced Calling Features:
- Support for advanced call handling features such as call transfer, call forwarding, call waiting, and conferencing.
- Visual voicemail indication and management.
- Busy Lamp Field (BLF) support for monitoring the status of other extensions or lines.
- Call recording functionality for compliance or training purposes.
- Security and Management:
- Built-in security features such as Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) for secure communication.
- Support for secure provisioning methods such as HTTPS or encrypted configuration files.
- Remote management capabilities for IT administrators to easily configure and monitor devices.
- Ergonomic Design:
- Sleek and professional design suitable for executive environments.
- Adjustable stand and ergonomic handset for comfortable use during long calls.
- Wall-mountable option for flexible placement in various office setups.
- Compatibility and Interoperability:
- Compatibility with a wide range of SIP-based VoIP platforms, PBX systems, and hosted VoIP services.
- Interoperability with third-party applications and services for integration with CRM systems, unified communications platforms, etc.
- Power Options:
- Support for Power over Ethernet (PoE) for convenient power and data connectivity over a single Ethernet cable.
- Optional AC adapter for non-PoE environments or for added flexibility in deployment.
- Scalability and Futureproofing:
- Firmware upgradeability for adding new features, fixing bugs, and ensuring compatibility with future standards and technologies.
- Compatibility with future hardware expansions or accessories to extend functionality as needs evolve.

3.4.9.4 Executive Level Open Sip IP Phone

- Multiple Line Support:

- Ability to handle multiple SIP lines simultaneously for hosting or participating in multiple conference calls or managing various communications.
- High-Quality Audio:
- Advanced audio processing technology for crystal-clear voice transmission.
- Support for HD Voice and wideband audio codecs to ensure excellent sound quality.
- Noise-canceling technology to minimize background noise and ensure clear conversations.
- Large Display:
- A large, high-resolution color display for easy viewing of call information, contact lists, and other essential details.
- Intuitive user interface with menu navigation and function access directly from the display.
- Expansion Options:
- Support for expansion modules to increase the number of available lines or programmable keys for enhanced functionality.
- Daisy-chain capability for connecting multiple conference phones together to expand coverage in large meeting rooms.
- Advanced Call Handling Features:
- Conference call support with the ability to host multi-party calls effortlessly.
- Call management features such as call transfer, call hold, call waiting, and call forwarding.
- Flexible mute options for individual participants or the entire conference.
- Connectivity Options:
- Ethernet port for network connectivity, ensuring a stable connection during conference calls.
- Optional Wi-Fi support for flexibility in deployment and placement within the office environment.
- Bluetooth connectivity for pairing with mobile devices or wireless headsets.
- Integration and Compatibility:
- SIP protocol support for seamless integration with VoIP systems and platforms.
- Compatibility with popular conferencing platforms and applications for easy setup and use.
- Interoperability with third-party applications and services for integration with CRM systems, unified communications platforms, etc.
- Security and Management:
- Built-in security features such as Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) for secure communication.
- Support for secure provisioning methods such as HTTPS or encrypted configuration files.
- Remote management capabilities for IT administrators to configure and monitor devices centrally.
- Ergonomic Design:
- Sleek and modern design suitable for conference room environments.
- Omnidirectional microphones for capturing voices from all directions in large meeting rooms.

- Easy-to-use control buttons for adjusting volume, muting, and other essential functions during conferences.
- Scalability and Flexibility:
- Firmware upgradeability for adding new features, fixing bugs, and ensuring compatibility with future standards and technologies.
- Compatibility with future hardware expansions or accessories to extend functionality as conference needs evolve.

3.4.9.5 Operators Console USB HD Headset

- Audio Quality:
- High-definition audio with wideband support for clear, natural-sounding voice transmission.
- Advanced noise-canceling microphone to eliminate background noise and ensure clear communication.
- Echo cancellation technology to prevent audio feedback during calls.
- Comfort and Ergonomics:
- Lightweight and adjustable headband for a comfortable fit during extended wear.
- Cushioned ear pads made from breathable materials to reduce fatigue.
- Swiveling ear cups for convenient storage and comfortable resting when not in use.
- Durability and Build Quality:
- Durable construction with high-quality materials to withstand daily use in a busy office environment.
- Reinforced, tangle-resistant cables for long-term reliability.
- Replaceable components such as ear pads and microphone foam for easy maintenance and extended lifespan.
- Connectivity:
- USB connectivity for plug-and-play compatibility with computers and VoIP softphones.
- Inline controls for convenient adjustment of volume, mute, and call answer/end functions.
- Compatibility with major operating systems such as Windows, macOS, and Linux.
- Integration with Operator Console Software:
- Compatibility with operator console software for seamless integration with call handling features.
- Programmable buttons or inline controls for quick access to commonly used functions within the operator console software.
- Noise Management:
- Active noise-canceling technology to reduce background noise and distractions in the operator's environment.
- Optional ambient noise monitoring feature to adjust microphone sensitivity based on environmental conditions.
- Compatibility and Interoperability:
- Compliance with industry standards such as USB Audio Device Class Specification for broad compatibility with software applications and platforms.

- Compatibility with Unified Communications (UC) platforms, including popular options such as Teams, Zoom, Cisco Webex, and others.
- Security and Privacy:
- Privacy features such as a red LED indicator to signal when the microphone is muted for confidential conversations.
- Secure communication protocols to prevent eavesdropping or interception of audio data

3.4.9.6 Hearing Aid Compatibility Headset

- Hearing Aid Compatibility (HAC):
- Compliant with FCC requirements for hearing aid compatibility (HAC) to ensure compatibility with hearing aids used by individuals with hearing impairments.
- Support for telecoil (T-coil) technology commonly found in hearing aids, allowing users to switch to the "T" mode for better clarity and reduced interference during calls.
- Audio Quality and Clarity:
- High-definition audio with wideband support for clear, natural-sounding voice transmission.
- Noise-cancelling microphone to minimize background noise and ensure clear communication for both parties.
- Enhanced digital signal processing (DSP) to improve speech clarity and reduce distortion.
- Volume Control and Amplification:
- Adjustable volume control to accommodate varying levels of hearing loss and individual preferences.
- Built-in amplification to boost audio levels without sacrificing clarity or introducing distortion.
- Comfort and Fit:
- Lightweight and adjustable headband for a comfortable fit during extended wear.
- Cushioned ear pads made from breathable materials to reduce fatigue and provide comfort for users wearing hearing aids.
- Swiveling ear cups for convenient storage and comfortable resting when not in use.
- Durability and Build Quality:
- Durable construction with high-quality materials to withstand daily use in a variety of environments.
- Reinforced, tangle-resistant cables for long-term reliability.
- Replaceable components such as ear pads and microphone foam for easy maintenance and extended lifespan.
- Connectivity:
- Wired or wireless connectivity options to accommodate different hearing aid users' preferences.
- Compatibility with hearing aid-compatible telephones and other assistive listening devices for seamless integration into existing communication systems.
- Compatibility and Interoperability:

- Compliance with industry standards for compatibility with a wide range of devices, including telephones, computers, and mobile devices.
- Compatibility with popular Unified Communications (UC) platforms and VoIP softphones for use in professional settings.
- Design for Accessibility:
- Large, tactile controls for easy adjustment of volume and other settings, suitable for users with dexterity challenges.
- Clear visual indicators for power, mute status, and other functions to accommodate users with visual impairments.
- Privacy and Security:
- Privacy features such as a red LED indicator to signal when the microphone is muted for confidential conversations.
- Secure communication protocols to protect the privacy of users' conversation.

3.4.9.7 ATA Devices

- Ports and Interfaces:
- Analog FXS (Foreign Exchange Station) ports for connecting traditional analog telephones, fax machines, or other analog devices.
- Ethernet port(s) for connecting to the local network or broadband internet connection.
- Optional USB port(s) for additional connectivity options or future expansion.
- Protocol Support:
- Support for Session Initiation Protocol (SIP), the most common protocol used for VoIP communication.
- Compatibility with other VoIP protocols such as H.323 for interoperability with different VoIP platforms.
- Voice Codec Support:
- Support for a range of voice codecs including G.711, G.729, G.722, and others for efficient voice compression and transmission.
- Wideband audio codec support for high-definition voice quality (optional).
- Quality of Service (QoS):
- QoS features to prioritize voice traffic over data traffic, ensuring consistent call quality even during periods of network congestion.
- Traffic shaping and packet prioritization mechanisms for optimizing voice performance.
- Security Features:
- Built-in security features such as Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) for secure communication.
- Support for virtual private network (VPN) tunnels for secure remote access and communication.
- Management and Provisioning:
- Web-based configuration interface for easy setup and management of device settings.
- Support for remote provisioning protocols such as TR-069 or HTTP/HTTPS for centralized device management.

- Auto-provisioning capabilities for seamless deployment in large-scale VoIP deployments.
- Fax Support:
- Compatibility with T.38 protocol for reliable fax over IP (FoIP) transmission.
- Support for fax pass-through and fax relay modes for seamless integration with analog fax machines.
- Additional Features:
- Caller ID support for displaying incoming caller information on compatible analog phones.
- Call waiting, call forwarding, three-way calling, and other standard telephony features.
- Message waiting indicator (MWI) support for notifying users of new voicemail messages.
- Power Options:
- Power over Ethernet (PoE) support for simplified deployment and reduced cabling requirements.
- Optional external power adapter for situations where PoE is not available or feasible.
- Compatibility:
- Compatibility with a wide range of VoIP service providers, IP PBX systems, and hosted VoIP platforms.
- Interoperability with analog devices from different manufacturers for flexibility in deployment.
- Physical Design:
- Compact and sturdy design suitable for desktop or wall-mount installation.
- LED indicators for power, network activity, and phone status for easy troubleshooting and monitoring

3.4.9.8 Sip DECT Handset

- DECT Standard Compliance:
- Compliance with the Digital Enhanced Cordless Telecommunications (DECT) standard for secure and interference-free wireless communication.
- Support for DECT standards such as DECT 6.0 or CAT-iq (Cordless Advanced Technology – internet and quality).
- SIP Protocol Support:
- Full support for SIP protocol for seamless integration with SIP-based VoIP systems, IP PBXs, and hosted VoIP services.
- Compatibility with popular SIP platforms and services, ensuring interoperability and ease of deployment.
- HD Voice Support:
- Support for high-definition (HD) voice codecs such as G.722 for superior voice clarity and natural sound quality.
- Wideband audio support for enhanced speech intelligibility and a more lifelike conversation experience.
- Multiple Line Support:
- Ability to handle multiple SIP lines or registrations simultaneously for increased flexibility and call management.

- Support for multiple SIP accounts or identities, allowing users to differentiate between personal and business calls.
- Display and User Interface:
- Clear and intuitive color display for easy navigation of menus, contacts, and call logs.
- Backlit keypad for enhanced visibility in low-light environments.
- User-friendly interface with customizable settings and preferences.
- Enhanced Mobility Features:
- Seamless handover between DECT base stations for uninterrupted call coverage across large areas or multiple floors.
- Range optimization features to extend coverage range and ensure reliable connectivity in challenging environments.
- Support for DECT repeaters to expand coverage range and overcome obstacles such as thick walls or interference sources.
- Battery Life and Charging:
- Long battery life for extended talk time and standby time, minimizing the need for frequent recharging.
- Convenient charging options such as desktop charging cradles or USB charging for flexibility in charging the handset.
- Durability and Ergonomics:
- Durable construction with shock-resistant materials for reliability in demanding environments.
- Ergonomic design for comfortable handling during long calls and ease of use.
- Security Features:
- Encryption and authentication mechanisms to ensure the security and privacy of voice communications.
- Support for secure provisioning methods such as HTTPS or encrypted configuration files.
- Integration and Compatibility:
- Compatibility with a wide range of SIP-based VoIP platforms, IP PBX systems, and hosted VoIP services.
- Interoperability with third-party applications and services for integration with unified communications platforms, CRM systems, etc.
- Additional Features:
- Advanced call handling features such as call transfer, call hold, call waiting, and conferencing.
- Support for voicemail, caller ID, call forwarding, and other standard telephony features.
- Headset jack for hands-free communication using compatible wired or wireless headsets.

3.4.9.9 Sip DECT Handset

- Teams Integration:
- Full compatibility with Teams for making and receiving calls, joining meetings, and accessing Teams collaboration features directly from the phone interface.
- SIP Protocol Support:

- Native support for SIP (Session Initiation Protocol) for seamless integration with SIP-based VoIP systems and platforms.
- Compatibility with industry-standard SIP RFCs (Request for Comments) to ensure interoperability with third-party SIP devices and platforms.
- HD Voice and Audio Quality:
- Support for high-definition (HD) voice codecs such as Opus, SILK, or G.722 for superior audio quality and clarity.
- Wideband audio support for enhanced speech intelligibility and a more natural conversation experience.
- Large Color Display:
- Large, high-resolution color display for easy navigation of menus, contacts, and call logs.
- Touchscreen interface for intuitive control and operation, allowing users to access Teams features with ease.
- Presence Indicators:
- Presence indicators to display the availability status of colleagues and contacts within the Teams environment.
- Integration with Teams presence information for real-time visibility into users' availability.
- Teams Button:
- Dedicated Teams button for quick access to Teams features such as joining meetings, initiating calls, or checking voicemail.
- Connectivity Options:
- Ethernet port for network connectivity, ensuring a stable connection to the Teams service.
- Optional Wi-Fi support for flexible placement within the office environment and wireless connectivity.
- Security and Compliance:
- Support for secure provisioning methods such as HTTPS or encrypted configuration files.
- Management and Provisioning:
- Support for centralized device management platform for easy deployment, configuration, and monitoring of SIP phones.
- Remote management capabilities for IT administrators to configure and update devices centrally.
- Interoperability:
- Interoperability with Teams-certified devices and peripherals for a seamless user experience across different endpoints

3.4.9.10 Audio and Video Conference SIP Phone

- Audio Features:
- High-definition (HD) audio support for crystal-clear voice transmission.
- Advanced audio processing technology for noise reduction and echo cancellation.
- Wideband audio codec support for enhanced speech clarity and natural sound reproduction.
- Full-duplex speakerphone for hands-free communication during conference calls.

- Video Features:
- High-definition (HD) video camera with autofocus and zoom capabilities.
- Support for video resolutions up to 1080p for clear and detailed video conferencing.
- Pan-tilt-zoom (PTZ) functionality for flexible camera positioning and framing.
- Wide-angle lens for capturing participants in large conference rooms.
- Display:
- Large, high-resolution colour display for viewing video feeds, presentation content, and call information.
- Touchscreen interface for intuitive control of conference features and settings.
- Multi-touch support for easy navigation and interaction with on-screen elements.
- Connectivity:
- Ethernet port(s) for network connectivity, ensuring a stable connection to SIP-based VoIP systems.
- Optional Wi-Fi support for flexibility in deployment and placement within the office environment.
- Bluetooth connectivity for pairing with mobile devices or wireless headsets.
- SIP Protocol Support:
- Native support for SIP protocol for seamless integration with SIP-based VoIP systems and platforms.
- Compatibility with industry-standard SIP RFCs (Request for Comments) to ensure interoperability with third-party SIP devices and platforms.
- Conference Call Features:
- Support for multi-party audio and video conferences with multiple participants.
- Advanced call handling features such as call transfer, call hold, call waiting, and conferencing.
- Presentation sharing capabilities for sharing documents, presentations, and multimedia content during conferences.
- Security and Management:
- Built-in security features such as Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) for secure communication.
- Support for secure provisioning methods such as HTTPS or encrypted configuration files.
- Remote management capabilities for IT administrators to configure and monitor devices centrally.
- Integration and Compatibility:
- Compatibility with a wide range of SIP-based VoIP platforms, IP PBX systems, and hosted VoIP services.
- Interoperability with third-party video conferencing platforms and applications for flexible collaboration options.
- Scalability and Flexibility:
- Support for expansion microphones and cameras to accommodate larger conference rooms or additional participants.
- Firmware upgradeability for adding new features, fixing bugs, and ensuring compatibility with future standards and technologies.

3.4.9.11 Physical Session Border Controller (SBC)

- Capacity and Performance:
- Throughput capacity measured in concurrent sessions, calls per second, and maximum bandwidth to accommodate the communication needs of the network.
- Scalability options such as the ability to add expansion modules or licenses to increase capacity as the network grows.
- Redundancy and High Availability:
- Redundant power supplies, fans, and other critical components to ensure continuous operation and minimize downtime.
- Support for High Availability (HA) configurations with failover capabilities for uninterrupted service in case of hardware or software failures.
- Security Features:
- Advanced security features such as stateful firewall, intrusion detection and prevention, and access control lists (ACLs) to protect against malicious attacks and unauthorized access.
- Secure signaling and media encryption using protocols such as Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) to safeguard communication sessions.
- Interoperability:
- Support for a wide range of signalling protocols including SIP, H.323, and others to ensure interoperability with different communication networks and devices.
- Interworking capabilities for protocol mediation and transcoding to facilitate communication between disparate networks with different signalling and media formats.
- Quality of Service (QoS):
- Traffic shaping and prioritization mechanisms to prioritize real-time communication traffic over data traffic and ensure consistent quality of service.
- Call admission control (CAC) to prevent network congestion and maintain service quality during peak usage periods.
- Media Handling:
- Support for a variety of audio and video codecs to ensure compatibility with different devices and applications.
- Media manipulation capabilities such as transcoding, packetization, and bandwidth management to optimize media streams and ensure efficient use of network resources.
- Session Routing and Policy Enforcement:
- Flexible routing capabilities based on criteria such as source/destination address, protocol, user identity, and time of day to route sessions according to predefined policies.
- Call routing and manipulation features such as number translation, prefix stripping, and digit manipulation to support complex call routing scenarios.
- Monitoring and Reporting:
- Comprehensive logging and reporting capabilities to track session activity, monitor network performance, and generate usage reports.
- Real-time monitoring tools for monitoring session status, network traffic, and system health.
- Management and Provisioning:

- Centralized management interface for configuring, monitoring, and managing multiple SBCs from a single location.
- Support for industry-standard management protocols such as SNMP, SSH, and RESTful APIs for integration with existing management systems.
- Physical Design:
- Rack-mountable form factor with modular design for easy installation and integration into existing network infrastructure.
- Front-panel status indicators and LED displays for monitoring system status and activity.
- Fanless or low-noise design for quiet operation in office environments.

3.4.9.12 Voice Over LTE router

- LTE Support:
- Full support for LTE networks, including various bands and frequencies, to ensure compatibility with different carriers and regions.
- Advanced LTE features such as carrier aggregation and MIMO (Multiple Input, Multiple Output) for improved data speeds and network performance.
- VoLTE Support:
- Native support for Voice over LTE (VoLTE) technology to enable high-quality voice calls over LTE networks.
- Compliance with 3GPP standards for VoLTE implementation, ensuring interoperability with different network equipment and devices.
- Voice Quality:
- Support for HD Voice codecs such as AMR-WB (Adaptive Multi-Rate Wideband) for superior voice quality and clarity.
- Noise reduction and echo cancellation features to enhance call quality and minimize background noise during voice calls.
- Router Functionality:
- Integrated router functionality to provide wireless connectivity to multiple devices via Wi-Fi or Ethernet.
- Support for Wi-Fi standards such as 802.11ac for high-speed wireless internet access.
- Ethernet ports for wired connections to devices such as computers, IP phones, or VoIP gateways.
- QoS Features:
- Quality of Service (QoS) mechanisms to prioritize voice traffic over data traffic, ensuring optimal voice call performance.
- Traffic shaping and packet prioritization algorithms to minimize latency and packet loss for voice calls.
- Security Features:
- Built-in firewall and intrusion detection/prevention mechanisms to protect against cyber threats and unauthorized access.

- VPN (Virtual Private Network) support for secure remote access and communication over public LTE networks.
- Management and Monitoring:
- Web-based management interface for configuring router settings, managing network connections, and monitoring device status.
- SNMP (Simple Network Management Protocol) support for integration with network management systems and monitoring tools.
- Failover and Redundancy:
- Failover mechanisms to automatically switch to backup LTE networks or alternative connection methods (e.g., Ethernet, Wi-Fi) in case of LTE network outages.
- Redundant power supply options for increased reliability and uptime.
- Voice Service Features:
- Support for traditional telephony features such as call forwarding, call waiting, caller ID, and voicemail.
- Compatibility with analog telephones and devices via FXS (Foreign Exchange Station) ports for VoIP-to-PSTN connectivity.
- Compatibility and Interoperability:
- Compatibility with major VoLTE networks and carriers worldwide.
- Interoperability with SIP-based VoIP platforms, IP PBX systems, and hosted VoIP services for seamless integration into existing voice networks.
- Physical Design:
- Compact and rugged design suitable for deployment in various environments, including homes, offices, and industrial settings.
- External antenna connectors for optional external antenna installation to enhance LTE signal strength and coverage.

3.4.9.13 Physical Voice Gateway

- Analog and Digital Interfaces:
- Analog FXS (Foreign Exchange Station) ports for connecting analog telephones, fax machines, and other devices.
- Analog FXO (Foreign Exchange Office) ports for connecting to the PSTN (Public Switched Telephone Network) or analog trunk lines.
- Digital T1/E1 or PRI (Primary Rate Interface) ports for connecting to digital telephony equipment or ISDN (Integrated Services Digital Network) lines.
- SIP Protocol Support:
- Full support for the SIP (Session Initiation Protocol) for signalling and call control, enabling seamless integration with VoIP networks and platforms.
- Compatibility with industry-standard SIP RFCs (Request for Comments) for interoperability with SIP-based devices and services.
- Voice Codecs:
- Support for a wide range of voice codecs including G.711 (μ-law and A-law), G.722, G.729, and others for efficient voice compression and transmission.
- Optional support for HD (High Definition) voice codecs such as Opus or SILK for enhanced voice quality.
- Call Routing and Transformation:

- Flexible call routing capabilities based on destination, caller ID, time of day, or other criteria to route calls to appropriate destinations.
- Digit manipulation and number translation features for converting between different dialing formats and numbering plans.
- Protocol Conversion:
- Protocol mediation and conversion capabilities for translating between different signalling protocols such as SIP, H.323, and MGCP (Media Gateway Control Protocol).
- Interworking features for converting between different media formats and codecs to ensure compatibility between analog/digital and IP-based networks.
- QoS (Quality of Service):
- Traffic prioritization mechanisms to prioritize voice traffic over data traffic and ensure consistent voice quality.
- Support for traffic shaping and bandwidth management to optimize voice performance and minimize latency and jitter.
- Security Features:
- Built-in security features such as TLS (Transport Layer Security) and SRTP (Secure Real-Time Transport Protocol) for secure communication and encryption of voice traffic.
- Support for authentication and access control mechanisms to prevent unauthorized access to the gateway.
- Management and Monitoring:
- Web-based management interface for configuring gateway settings, monitoring call activity, and managing device status.
- SNMP (Simple Network Management Protocol) support for integration with network management systems and monitoring tools.
- Redundancy and High Availability:
- Redundant power supplies, fans, and other critical components for ensuring continuous operation and minimizing downtime.
- Support for High Availability (HA) configurations with failover capabilities for uninterrupted service in case of hardware or network failures.
- Physical Design:
- Rack-mountable form factor with modular design for easy installation and integration into existing network infrastructure.
- Front-panel status indicators and LED displays for monitoring system status and activity.
- Fanless or low-noise design for quiet operation in office environments

- Open SIP IP Phone licence
- Conference open SIP IP phone licence
- Audio and Video Conference SIP Phone licence
- SIP DECT Software licence
- Mitel SIP trunking licence
- Mitel Operators Console licence
- Call Recording Software licencing for Contact Centre
- Call Recording Software licencing for Contact Centre
- Mitel soft switch licence

- Mitel Telephony Server licence
- Mitel Integrated Media Server licence
- Mitel Contact centre omnichannel solution software licensing
- Mi Collab Solution/Teams Collaboration application with Instant messaging and Presence licences
- VMware vSphere Server Virtualization licences
- Fax-to-Email Software licencing
- VoIP Monitoring Software licencing
- VoIP Monitoring System
- SIP Trunks with redundancy
- Uncapped voice minutes to all networks per user
- Call Recording Solution (50 extensions, the recording to be kept for five years)
- Number porting
- Contact Centre Solution
- End User Training per user
- Off-net SIP trunk as a service
- Issue of new numbers
- Porting of existing numbers
- Microsoft Teams Direct Routing
- Router Installation per site including all required licenses
- Monthly Router rental
- Data line (Site with 1-100 users)- 10Mbps
- Data line (Site with 101-300 users)- 30Mbps
- Data line (Site with 301-500 users)- 50Mbps
- Data line (Site with 501-1000 users)- 100Mbps
- Telephone Management System
- Installation, Configuration, Support and Maintenance

3.5 Other Conditions and Considerations

3.5.1 Quality Assurance

The successful tenderer shall have a quality insurance program to ensure the quality of both product and service.

3.5.2 Environmental

Suppliers shall make recommendations concerning earthing, lighting protection, environmental conditions (ie air conditioning) and other environmental requirements.

3.5.3 Technical Documentation

A detailed network topology/architecture for the above should be proposed and a properly labelled layout (showing, for example, clearly the used and free ports on the switch) of the network design should be handed over to the Client by the successful bidder during commissioning.

Supplier should provide a technical document for each building to the CoT:

- Configuration of the equipment (router, L3 switch)
- A layout of the system with proper labelling
- Troubleshooting procedures

- Complete technical details along with make, model number, complete specification, pamphlets, literature of the systems highlighting the special features must be supplied along with the bid.

All final-handover documentation (at completion of the project) shall be electronically either in word or acrobat format. Drawings to be in Visio format.

3.5.4 Expansion Protocols

Any expansion, ie, where new equipment is deployed or configuration changes, requires that the successful bidder will be responsible to update all diagrams/drawings applicable to the relevant environment. All changes and expansions must be managed in accordance with Council's existing Change Control processes and procedures in line with ITIL best practice. All new projects must be deployed adhering to these principles.

3.5.5 Third Party Network Management Tools

Where applicable, it will be required that certified personnel be deployed on site to manage and maintain all deployed systems and tools. Reporting must be made available either at set times during the month, and also for any ad hoc requests. All information on the systems are confidential and must at all times be routed through the correct channels and protocols.

3.5.6 Product Range

The CoT has a range of products for its Voice and Data switching equipment needs, and proposed solution, must be able to enhance the existing infrastructure with seamless implementation of new equipment and the maintenance of any new equipment installed to the specifications and levels as determined by CoT, to tender.

3.5.7 Current Equipment

The successful bidder would also need to have certified on-site engineers able to maintain and enhance the current infrastructure. The prospective bidders also need to be well versed in installing additional services like video streaming solutions, radio links and other technologies as needed by CoT from time to time.

3.5.8 Materials And Workmanship

Materials and workmanship to be of the highest quality

3.5.8.1 Delivery

New equipment must be delivered within 6 (six) consecutive weeks from date on the official CoT order to the CoT's stores. The Contractor shall bear all risks relating to the goods until provisional acceptance at destination. Once delivery is ready, the CoT appointed Project Liaison must be notifies and the equipment will then be inspected at the delivery premises.

The supplies shall be packaged so as to prevent their damage or deterioration in transit to their destination. Packaging must be as per accepted international standards for air/surface transportation taking into account the climatic conditions prevailing in South Africa at time of delivery. The packaging shall be disposed by the contractor. Each delivery shall include all necessary documents as specified in the technical specifications (operating and maintenance manuals, drawings, material, conformity or test certificates and certificates etc). The CoT order nr and installation site must be clearly marked on the packaging.

The necessary documents shall include an inventory list of items delivered indicating the serial numbers of the goods provided. All operating and maintenance manuals shall be in English.

Each delivery must be accompanied by a statement drawn up by the Contractor. Each package shall be clearly marked in accordance with the order number and equipment it contains. Delivery shall be deemed to have been made when there is written evidence available to both Parties that delivery of the supplies has taken place in accordance with the terms of the contract.

3.5.8.2 Spare Parts

The bidders must have spares and stockholding at their own premises and not in a bonded warehouse or distribution channel warehouse, proof of this must be supplied.

3.5.8.3 Warranty

The Contractor shall warrant that the supplies are new, unused, of the most recent models and incorporate all recent improvements in design and materials, unless otherwise provided in the contract. The Contractor shall further warrant that all supplies shall have no defect arising from design, materials or workmanship, except insofar as the design or materials are required by the specifications, or from any act or omission, that may develop under use of the supplies in the conditions obtaining in the country of the Contracting Authority.

The Contractor shall be responsible for making good any defect in, or damage to, any part of the supplies which may appear or occur during the warranty period and which:

- Results from the use of defective materials, faulty workmanship or design of the Contractor; or
- Results from any act or omission of the Contractor during the warranty period; or
- Appears in the course of an inspection made by CoT.

If any such defect appears or such damage occurs during the warranty period, the Contracting Authority or the Project Manager shall notify the Contractor. If the Contractor fails to remedy a defect or damage within the time limit stipulated in the notification, the Contracting Authority may:

- Remedy the defect or the damage itself, or employ someone else to carry out the work at the Contractor's risk and cost, in which case the costs incurred by the Contracting Authority shall be deducted from monies due to or guarantees held against the Contractor or from both;
- Or, terminate the contract.

The on-site comprehensive warranty shall be for a minimum period of **one year** after commissioning of the equipment. During the warranty period, the call back time of the supplier for any problem will be in accordance to the SLA stipulations. The supplier should provide a replacement equipment to cater for any contingency. Warranty shall include free maintenance of the whole equipment supplied including free replacement of parts. The defects, if any shall be attended to on immediate basis.

3.5.8.4 Loan Equipment

Should damages occur to equipment due to circumstances not covered under warranty for example lightning strikes, the following will apply:

- Contractor will replace equipment as stated under the warranty.

- Contractor will investigate and hand in a report to verify the equipment failure and cause.
- If repairable, a quote must be given for said repairs. CoT will either supply an order for the repairing of the equipment or for new equipment depending on the repair costs.
- If non-repairable, CoT will supply an order for new equipment based on the prices in this document.
- The equipment provided under the warranty will therefore become loan equipment until the repaired or new equipment is installed and commissioned.

3.5.8.5 Pre-Delivery Inspection

CoT's Project Liaison shall have the right to inspect or to test the items to confirm their conformity to the ordered specifications. The supplier shall provide all reasonable facilities and assistance to the inspector at no charge to CoT. In case any inspected or tested goods fail to conform to the specifications, CoT may reject them and supplier shall either replace the rejected goods or make all alterations necessary to meet specification required free of cost to CoT.

3.5.8.6 Verification Process

The CoT Project Liaison shall, during the progress of the delivery of the supplies and before the supplies are taken over, have the power to order or decide:

- the removal from the place of acceptance, within such time or times as may be specified in the order, of any supplies which, in the opinion of the Project Manager, are not in accordance with the contract;
- their replacement with proper and suitable supplies;
- the removal and proper re-installation, notwithstanding any previous test thereof or interim payment therefor, of any installation which in respect of materials, workmanship or design for which the Contractor is responsible, is not, in the opinion of the Project Liaison, in accordance with the contract;
- that any work done or goods supplied or materials used by the Contractor is or are not in accordance with the contract, or that the supplies or any portion thereof do not fulfil the requirements of the contract.

The Contractor shall, with all speed and at his own expense, make good the defects so specified. If the Contractor does not comply with such order, the Contracting Authority shall be entitled to employ other persons to carry out the orders and all expenses consequent thereon or incidental thereto shall be deducted by the Contracting Authority from any monies due or which may become due to the Contractor.

Supplies which are not of the required quality shall be rejected. A special mark may be applied to the rejected supplies. This shall not be such as to alter them or affect their commercial value. Rejected supplies shall be removed by the Contractor from the place of acceptance, if the Project Manager so requires, within a period which the Project Manager shall specify, failing which they shall be removed as of right at the expense and risk of the Contractor. Any works incorporating rejected materials shall be rejected.

3.5.8.7 Final Inspection

Final inspection will take place at the location(s) of delivery. The inspection will test the completed installations and integration and the proper operation confirming the technical validity of the equipment and documents with the design specification documents and quality standards prescribed. This final inspection will be the basis for provisional acceptance. A letter will be sent to the contractor at least one week before the final inspection will take place.

3.5.8.8 Administrative

The Contractor shall comply with administrative orders given by the Contract Manager (Relevant Director in Council). Where the Contractor considers that the requirement of an administrative order goes beyond the scope of the contract, he shall, on pain of breach of contract, notify the Contract Manager (Relevant Director in Council) thereof, giving his reasons, within 30 days of receipt of the order. Execution of the administrative order shall not be suspended because of this notice.

3.5.8.9 Implementation Methodology/Programme

The Contractor shall submit a program of implementation of the contract for the approval of the Project Manager. The program shall contain at least the following:

- The order in which the Contractor proposes to perform the contract including design, manufacture, delivery to place of receipt, installation, testing and commissioning.
- Detailed schedule of all activities and sub activities, allowing weekly and monthly reports to be extracted.
- Job description for every activity or milestone.
- Define delivery contents and time.
- Define final delivery and final operating time.
- The deadlines for submission and approval of the drawings;
- A general description of the methods which the Contractor proposes to adopt for executing the contract; and
- Such further details and information as the Project Manager may reasonably require.

No material alteration to the program shall be made without the approval of the Project Manager. If, however, the progress of the implementation of the contract does not conform to the program, the Project Manager may instruct the Contractor to revise the program and submit the revised program for approval.

Approved drawings, documents, samples and models shall be signed or otherwise identified by the Project Manager and may only be departed from on the Project Manager's instructions. The approval of the drawings, documents, samples or models by the Project Manager shall not relieve the Contractor from any of his obligations under the contract.

3.5.8.10 Model and Serial

All equipment should have a solidly fixed metallic type (or similar) approved label, approx. size 75 X35 mm, model and serial number. The contractor must keep a detailed order book tracking the following:

- Requisition Nr

- Order Nr
- Quote Nr
- The different assets, description and worth
- Serial nr matched to an Asset Nr
- Place deployed
- Any other relevant information.

3.5.8.11 Electricity

Nominal voltage in South-Africa is 220/230V single phase. The quality and stability of the supplied current may undergo fluctuations of more than ±10%. All supplied hardware must operate on a 220 V ± 20 V, 50 Hz ± 0.5 Hz, power supply and be suitable for direct connection to the standard power outlets in South Africa.

3.5.8.12 Final Acceptance

Upon expiry of the warranty period or, where there is more than one such period, upon expiry of the latest period, and when all defects or damage have been rectified, the Project Manager shall issue the Contractor a final acceptance certificate, with a copy to the Contracting Authority, stating the date on which the Contractor completed his obligations under the contract to the Project Manager's satisfaction. The final acceptance certificate shall be issued by the Project Manager within 30 days of the expiry of the warranty period or as soon as any repairs ordered have been completed to the satisfaction of the Project Manager.

The contract shall not be considered to have been performed in full until the final acceptance certificate has been signed or is deemed to have been signed by the Project Manager.

Notwithstanding the issue of the final acceptance certificate, the Contractor and the Contracting Authority shall remain liable for the fulfilment of any obligation incurred under the contract prior to the issue of the final acceptance certificate which remains unperformed at the time that final acceptance certificate is issued. The nature and extent of any such obligation shall be determined by reference to the provisions of the contract.

3.5.8.13 Inspection and Testing

The Contractor shall ensure that the supplies are delivered to the place of acceptance in time to allow the Project Manager to proceed with acceptance of the supplies.

The Project Manager shall be entitled, from time to time, to inspect, examine, measure and test the components, materials and workmanship, and check the progress of preparation, fabrication or manufacture of anything being prepared, fabricated or manufactured for delivery under the contract, in order to establish whether the components, materials and workmanship are of the requisite quality and quantity. This shall take place at the place of manufacture, fabrication, preparation or at the place of acceptance.

For the purposes of such tests and inspections, the Contractor shall:

- provide the Project Manager, temporarily and free of charge, with such assistance, test samples or parts, machines, equipment, tools, labour, materials, drawings and production data as are normally required for inspection and testing;

- agree, with the Project Manager, the time and place for tests;
- give the Project Manager access at all reasonable times to the place where the tests are to be carried out.

If the Project Manager is not present on the date agreed for tests, the Contractor may, unless otherwise instructed by the Project Manager, proceed with the tests, which shall be deemed to have been made in the Project Manager's presence. The Contractor shall immediately send duly certified copies of the test results to the Project Manager, who shall, if he has not attended the test, be bound by the test results.

When components and materials have passed the above-mentioned tests, the Project Manager shall notify the Contractor or endorse the Contractor's certificate to that effect.

If the Project Manager and the Contractor disagree on the test results, each shall state his views to the other within 15 days of such disagreement. The Project Manager or the Contractor may require such tests to be repeated on the same terms and conditions or, if either Party so requests, by an expert selected by common consent. All test reports shall be submitted to the Project Manager, who shall communicate the results of these tests without delay to the Contractor. The results of retesting shall be conclusive. The cost of retesting shall be borne by the Party whose views are proved wrong by the retesting.

In the performance of their duties, the Project Manager and any person authorized by him shall not disclose to unauthorized persons information concerning the undertaking's methods of manufacture and operation obtained through inspection and testing.

3.5.8.14 Suspension

The Project Manager may, by administrative order, at any time, instruct the Contractor to suspend:

- the manufacture of the supplies; or
- the delivery of supplies to the place of acceptance at the time specified for delivery in the implementation programme or, if no time specified, at the time appropriate for it to be delivered; or
- the installation of the supplies which have been delivered to the place of acceptance.

The Contractor shall, during suspension, protect and secure the supplies affected at the Contractor's warehouse or elsewhere, against any deterioration, loss or damage to the extent possible and as instructed by the Project Manager, even if supplies have been delivered to the place of acceptance in accordance with the contract but their installation has been suspended by the Project Manager.

The Contractor shall not be paid any additional expenses if the suspension is:

- necessary by reason of abnormal climatic or other environmental conditions at the place of acceptance
- necessary owing to some default of the Contractor
- necessary for the safety or the proper execution of the contract or any part thereof insofar as such necessity does not arise from any act or default by the Project Manager or the Contracting Authority.

If the period of suspension exceeds 180 days, and the suspension is not due to the Contractor's default, the Contractor may, by notice to the Project Manager, request to proceed with the supplies within 30 days, or terminate the contract.

PART 4: OPERATE AND MAINTAIN THE EXISTING ALCATEL/LUCENT & HUAWEI NETWORK

Part 4: Operate and Maintain the existing Alcatel/Lucent & Huawei network

4.1 Scope

This section, **Maintenance of the Current Corporate Voice and Data Network,** describes maintenance of the current network. This is a service-oriented approach ie personnel will be contracted from the attached price list.

4.2 Resources

The resources will be responsible for maintenance of the current network and it therefore excluded any new equipment that will be bought under this contract. However, the contractor will also be responsible for the monitoring of the whole network and should any new switches be down, this must be reported to the relevant party for action.

The following resources be provided (refer Section 2):

- 2 x Data switch experts
- 2 x Voice switch experts
- 1 x Operational Manager
- 2 x Junior Technicians

If CoT deem further resources to be necessary, they will be contracted from the price list.

Resources are expected to monitor the network and to respond to any network related problems. They will report directly to the Deputy Director of the applicable section and will have to comply to any ad-hoc requests and service responses ie they are seen as an extension of the applicable section.

4.3 Hardware Related Failures

The maintenance contractor will not be responsible for providing hardware under this section. Hardware related failures can be categorized:

- Hardware failure for new equipment procured under this contract: The failure must reported to the responsible party. Responsible party to follow procedures as set out in Section 2.

- Hardware failure for equipment still under warranty/SLA from previous tender: The failure must reported to the responsible party.

- Hardware failure for equipment not covered by SLA/Warranty: The failure must reported to the responsible party whom in turn need to submit a quotation for replacement equipment (under this contract Section 3).

4.4 Network/Voice Monitoring

4.4.1 Types and Description of Monitoring

The following are normal types of monitoring:

Server Performance The items being monitored would include such things as CPU usage, server load, disk utilization, memory usage, and entries in selected log files. This monitoring can provide advance warning of impending system problems if the alert thresholds are set properly.

SNMP Monitoring Almost every piece of equipment in a company network can be monitored via SNMP polling. This methodology uses device specific management information blocks (MIBs) to obtain additional information about a device's health. This information is collected at regular polling intervals. SNMP enabled devices can also be programmed to send SNMP trap information to message handlers in real time

Application Monitoring Monitor the actual health and well-being of applications. An application can be active but performing so slowly that customers or employees can't use it. For example, this type of monitoring might be used to determine how fast server based applications respond to employees.

Bandwidth Monitoring It provides a way to monitor usage and optimize the capacity of circuits, identify bottlenecks etcetera.

Agent Based Monitoring This is a requirement for IT Managers who are serious about operating system and applications monitoring. It is unlikely that 99% uptime can be reached without employing this type of technology. A monitoring software agent would usually operate with a Smart Plug In (SPI) or Knowledge Module (KM) that was designed to monitor specific operating systems and applications such as IIS and SQL.

4.4.2 Network/Voice Monitoring as a Service (QOS)

The tenderers must price network monitoring as a service ie the CoT do not own the software, but are rather charged a monthly amount. This will entail:

- Providing all software and or hardware related to network management. Hardware to include the servers – ie turn-key solution.

- Providing all updates and patches related to network management software
- Displaying the software in the CoT based NOC (Network Operations Cetre)
- Providing detailed reports and actions based on the reporting received from the tools.
- Provide for the auditing of all infrastructure and services obtained and rented from any external service providers as well as any service accounts emanating from the rental of these services. Of which the Service provider can bill a % of the saving as a cost to Council. No upfront retainer will be paid here for this service.

4.4.3 Network/Voice Monitoring Purchasing of Software

The tenderer prices the individual software components based on the newest pricing detail. However, CoT is entitled to free version upgrades and patches during the contractual period. The software must be displayed in the NOC and detailed reports and actions must be provided on the reporting received from the tools. Servers will be provided by the CoT, however requirements for the servers to be provided by the bidder. Software to support virtualized environment. This will be as per the provided pricing schedules to this tender.

4.5 Sniffing

Should the network behave erratic or slow problems are experienced etc, then CoT will request the maintenance contractor to bring in a sniffing expert to determine the cause and to rectify if possible. Sniffing requirements is discussed in Section ?.

4.6 Security

The maintenance contractor must ensure that network security remains intact and must therefore also monitor the network for intrusions and other malicious activity.

4.7 Alcatel Product Range

As mentioned the City has a substantial investment in the current Alcatel/Lucent & Huawei Product Range as used in the Corporate network and the successful bidder needs to operate and maintain these. The list of devices is for the data network is as below: (Charl – bevestig onderstaande – moet ook opsomming van die huidige Huawei toerusting basis hier invoeg)

Device Type	Total Number of Devices
OAW-4324	1
OAW-4450	3
OAW-6000	1
OS10K	4
OS6250-8M	8
OS6400-48	1
OS6400-P24	9
OS6400-U24	2

Device Type	Total Number of Devices
OS6450-P10	10
OS6450-P24	12
OS6450-P48	10
OS6600-P24	50
OS6602-24	35
OS6602-48	20
OS6624	50
OS6648	56
OS6850-24	1
OS6850-24L	3
OS6850-24X	1
OS6850-P24	61
OS6850-P48	16
OS6850-P48L	23
OS6850-U24X	6
OS6850E-P24	49
OS6850E-P24X	8
OS6850E-P48	19
OS6850E-P48X	151
OS6850E-U24X	3
OS6860-P24	3
OS6860-P48	3
OS6860E-P24	47
OS6860E-P48	151
OS6860E-U28	3
OS6865-P16X	10

Device Type	Total Number of Devices
OS6900-X20	21
OS6900-X40	1
OS6900-X72	4
OS7700	4
OS7800	5
OS9700	4
OS9800	6
	875

MPLS switches:

Device Type	Total Number of Devices
7210 SAS-M	5
7210 SAS-T	11
7705 SAR-8	1
7750 SR-7	5

Firewalls:

Device Type	Total Number of Devices
Fortigate 3000D	6
Fortigate 3950B	1
Fortigate 200D	6
Fortigate 200E	6
FortiAnalyzer 1000E	1

Software

- Alcatel Omnivista 2500
- Alcatel Omnivista 3600
- Alcatel Omnivista 8770

- Nokia Service Aware Manager
- Clearpass

The voice network: (Martin – BT – Gaan die hier moet bevestig)

The network consists of 6 x Alcatel Lucent OmniPcx Enterprise nodes driving a hybrid digital, analog, IP and SIP solution consisting of:

31 x act28 user shelves

- 34 x voice hub user shelves
- 8 x common platform user shelves
- With 10 482 users

Alcatel phone models deployed would primarily be:

- 8018 ± 60%
- 8028 ± 10%
- 8038 ± 10%
- Old model analogue and digital phones ± 20%

SECTION 5: COMPLIANCY OF ANY NEW EQUIPMENT & SOLUTION WITH REGARDS TO THE CURRENT DEPLOYED NETWORK SOLUTION

Section 5: Compliancy of any new equipment & solution with regards to the current deployed network solution

Local Area Network and Wireless Local Area Network

Generic Requirements

The Switching port-folio should provide a solution for access through to Core and Data Centre. They must support the same operating system on all switches in the portfolio, providing a consistent look and feel when configuring access functionality. The whole switch Access Point portfolios must be fully manageable; on the switches every single CLI command can be performed through SNMP. Also, the Web interface is fully implemented; with this GUI everything that is configurable through CLI can be configured through the Web GUI.

Management

Description	Compliance	Notes
The Network Management System, shall : • Proactively report lifecycle and obsolescence management of the entire network Infrastructure through an active connection to the main equipment vendor via the cloud. • Be a Single converged solution for wired and wireless networks. • Be a Simple and cost-effective solution for provisioning, monitoring and troubleshooting • Be a Wireless Network Management System	C/PC/NC	
Wired and Wireless device management is a critical requirement of the network. It shall be highly available, secure, provide location services, and allow application integration to the client.	C/PC/NC	
The system architecture shall have simplified configuration, monitoring and reporting of network services/devices. To help enable IT staff to efficiently	C/PC/NC	

design, deploy, maintain, monitor their network infrastructure.		
The management application shall allow multiple staff members to manage, monitor, and troubleshoot the network. Capabilities such as policy and template creation shall be included to simplify operation. Integration with location services for ease of locating clients, rogue Access Points, and wireless location tags is required. A single management application that can help enable deployment and management of wired and wireless devices, Access Points, location services, security settings, client troubleshooting, and client monitoring.	C/PC/NC	
The Network Management System (NMS) shall provide detailed application analytics information based on Layer 7 application fingerprinting and deep packet inspection (DPI) classification capabilities of network devices for both Ethernet LAN switches and WLAN Access Points. Detailed application usage (e.g. Facebook, Youtube, Bittorrent, etc…) shall be reported, and the NMS shall enforce unified (LAN and WLAN) QoS policies.	C/PC/NC	
The Network Management System (NMS) shall be able to read and analyze standards based sFlow information from network devices and display graphical analytics based on top network consumers (users, switches, ports, applications). The properly plan IT operations, the NMS shall further provide predictive analysis where it reports expected future network behavior in light of historic analyzed data.	C/PC/NC	
The Network Management System (NMS) shall integrate with various server virtualization hypervisor platforms to provide virtual machine and appliance visibility, locating virtual machine ports, and support features like VM motion.	C/PC/NC	
Shall provide converged user, access and identity management across wired and wireless networks.	C/PC/NC	
Shall support network troubleshooting by giving IT complete visibility into connectivity, regardless of device, network or location.	C/PC/NC	
Shall allow maintaining and managing of the end-to-end network infrastructure from a unified platform including RF management, user access visibility, reporting, and troubleshooting along with wired lifecycle functions such as discovery, inventory, configuration and image	C/PC/NC	

management, automated deployment, compliance reporting, integrated best practices, and reporting.		
The design feature shall allow assess, planning, and configurations required to roll out new network services and technologies. Shall facilitate monitoring of key network resources, devices, and attributes.	C/PC/NC	
Shall allow scheduling for the rollout and implementation of network changes. Changes may include software image updates, or support for user-initiated ad hoc changes and compliance updates.	C/PC/NC	
To operate, predefined dashboards shall provide status monitoring on the overall health of the network and troubleshooting. The system alarms and alerts shall have the ability to respond automatically by taking further action such as trigger an email exchange.	C/PC/NC	
Shall provide wide variety of predefined reports of the network including detailed inventory, configuration, compliance, audit, capacity, end-of-sale, security vulnerabilities etc.	C/PC/NC	
Network administrators shall have a single solution for wired and wireless management, policy provisioning and auditing, network optimization using inputs from advance tools, troubleshooting, device tracking, security monitoring, and wireless LAN systems management.	C/PC/NC	
Must have "heat maps", coverage hole detection capabilities and Voice Audit and Planning Mode tools, administrators shall be able to quickly determine if coverage in an area is suitable for Voice over Wi-Fi applications and/or provide accurate location.	C/PC/NC	
Must support the industry-standard SNMP protocol	C/PC/NC	
Must support dedicated Infrastructure appliance or on a VMware server.	C/PC/NC	
Must support web browser.	C/PC/NC	
Must support backup and restore.	C/PC/NC	
Management access through authenticated and authorized local database, or through RADIUS or TACACS. User groups shall be defined to allow administrative rights to specific tasks (i.e., monitor only clients, ability to configure controllers, and many other combinations of administrative attributes).	C/PC/NC	

Shall allow virtual domain consists of a set of devices and/or maps and restricts a user's view to information relevant to these devices and maps. In addition, through the use of the virtual domain's filters, users shall be able to configure, view alarms, and generate reports for only their assigned part of the network.	C/PC/NC	
Shall support TACACS and RADIUS authentication along with SSO and Local Authentication.	C/PC/NC	
To ensure continued operation in case of failure, the architecture shall provide a high availability or failover framework.	C/PC/NC	
Shall have the IoT focus dashboard widgets to facilitate the operational management for faster time to decision	C/PC/NC	
Shall support TACACS and RADIUS authentication along with SSO and Local Authentication.	C/PC/NC	

Access Switch 1 Gig Uplinks

Description	Compliance	Notes
The switch shall have 24 or 48 Gigabit Ethernet ports configuration, with or without Power over Ethernet (PoE).	C/PC/NC	
The switch shall have 4 x 1Gbps SFP uplink ports.	C/PC/NC	
The switch shall support Time Domain Reflectometry (TDR).	C/PC/NC	
The switch shall support automated assignment of QoS and Security based on MAC address (range) or IP address (range), preferably using the concept of configurable Network Profiles holding QoS and Security parameters, and which are dynamically assigned.	C/PC/NC	
The switch shall support an auto-configuration process (DHCP, TFTP/FTP) when deployed in a remote location.	C/PC/NC	
Up to four switches, 1RU per node and interconnected with SPF+ interfaces in a loop topology, may be logically merged as a single logical chassis behaving as a single equipment at management, forwarding and control planes.	C/PC/NC	
The switch shall be stackable with up to four switches.	C/PC/NC	

The switch shall support Power over Ethernet standards PoE (802.3af) and PoE+ (802.3at).	C/PC/NC	
The 24-port PoE switch shall have a PoE budget no less than 380W.	C/PC/NC	
The 48-port PoE switch shall have a PoE budget no less than 780W.	C/PC/NC	
The switch shall support advanced layer-2+ features with basic layer-3 routing for both IPv4 and IPv6.	C/PC/NC	
Shall support IEEE 802.az (Energy Efficient Ethernet) for lower TCO.	C/PC/NC	
IEEE 802.1D (STP)	C/PC/NC	
IEEE 802.1p (CoS)	C/PC/NC	
IEEE 802.1Q (VLANs)	C/PC/NC	
IEEE 802.1s (MSTP)	C/PC/NC	
IEEE 802.1w (RSTP)	C/PC/NC	
IEEE 802.1X (Port Based Network Access Protocol)	C/PC/NC	
IEEE 802.3i (10Base-T)	C/PC/NC	
IEEE 802.3u (Fast Ethernet)	C/PC/NC	
IEEE 802.3x (Flow Control)	C/PC/NC	
IEEE 802.3z (Gigabit Ethernet)	C/PC/NC	
IEEE 802.3ab (1000Base-T)	C/PC/NC	
IEEE 802.3ac (VLAN Tagging)	C/PC/NC	
IEEE 802.3ad (Link Aggregation)	C/PC/NC	

Access Switch 10 Gig Uplinks

Description	Compliance	Notes

24-port and 48-port, PoE and non-PoE with fixed small form factor pluggable (SFP+) 10G interfaces	C/PC/NC	
Support for 10 GigE stacking or 20 GigE stacking	C/PC/NC	
Support for IEEE 802.1AE MACSec encryption	C/PC/NC	
Internal modular AC redundant power supplies	C/PC/NC	
AOS field-proven software with management through web interface (WebView), command line interface (CLI), and Simple Network Management Protocol (SNMP)	C/PC/NC	
MACSec encryption to secure the network edge: 1G/2.5G user and 10G up-link ports	C/PC/NC	
Flexible device and user authentication with (IEEE 802.1x/MAC/captive portal) with Host Integrity Check (HIC) enforcement	C/PC/NC	
Enables deployment of comprehensive and secure BYoD services in enterprise networks such as guest management, device on-boarding, device posturing, application management and dynamic change of authentication (CoA).	C/PC/NC	
Advanced Quality of Service (QoS) and Access Control Lists (ACLs) for traffic control, including an embedded denial of service (DoS) engine to filter out unwanted traffic attacks	C/PC/NC	
Extensive support of user-oriented features such as learned port security (LPS), port mapping, Dynamic Host Configuration Protocol (DHCP) binding tables and User Network Profile (UNP)	C/PC/NC	
Advanced layer-2+ features with basic layer-3 routing(RIP&OSPF) for both IPv4 and IPv6+	C/PC/NC	
Triple speed (10/100/1G/2.5G) user interfaces and fiber interfaces (SFPs) supporting 1000Base-X or 10GBase-X optical transceivers	C/PC/NC	
10 G uplinks	C/PC/NC	
Wire-rate switching and routing performance	C/PC/NC	
High availability with virtual chassis concept, redundant stacking links, primary/secondary unit failover, hot-swappable power options and configuration rollback	C/PC/NC	

Enhanced Voice over IP (VoIP) and video performance with policy-based QoS	C/PC/NC	
Future-ready support for multimedia applications with wire-rate multicast	C/PC/NC	
Airgroup™ Network Services for Bonjour speaking devices provides consistent experience over wireless and wired networks	C/PC/NC	
IEEE 802.3af, IEEE 802.3at and IEEE802.3bt PoE support for IP phones, wireless LAN (WLAN) access points and video cameras	C/PC/NC	
Switch capacity with all 1G/10G/20G ports (all ports, full duplex) 24 port (132 Gb/s) 48 ports (180 Gb/s)	C/PC/NC	
Should support MultiGigabit interfaces (2.5 or 5 G).	C/PC/NC	
24-port and 48-port, PoE and non-PoE with fixed small form factor pluggable (SFP+) 10G interfaces	C/PC/NC	
Support for 10 GigE stacking or 20 GigE stacking	C/PC/NC	
Support for IEEE 802.1AE MACSec encryption	C/PC/NC	

Aggregation Switch

Description	Compliance	Notes
24-port and 48-port, PoE and non-PoE with fixed small form factor pluggable (SFP+) and QSFP 10G/25Gig/40Gig and 100Gig interfaces	C/PC/NC	
Support for 42 GB/s or 84 GB/s aggregate STACKING	C/PC/NC	
Support for IEEE 802.1AE MACSec encryption	C/PC/NC	
Internal modular AC redundant power supplies	C/PC/NC	
AOS field-proven software with management through web interface (WebView), command line interface (CLI), and Simple Network Management Protocol (SNMP)	C/PC/NC	
MACSec encryption to secure the network edge: On all up-link ports	C/PC/NC	

Flexible device and user authentication with (IEEE 802.1x/MAC/captive portal) with Host Integrity Check (HIC) enforcement	C/PC/NC	
Enables deployment of comprehensive and secure BYoD services in enterprise networks such as guest management, device on-boarding, device posturing, application management and dynamic change of authentication (CoA).	C/PC/NC	
Advanced Quality of Service (QoS) and Access Control Lists (ACLs) for traffic control, including an embedded denial of service (DoS) engine to filter out unwanted traffic attacks	C/PC/NC	
Extensive support of user-oriented features such as learned port security (LPS), port mapping, Dynamic Host Configuration Protocol (DHCP) binding tables and User Network Profile (UNP)	C/PC/NC	
Advanced layer-2+ features with advance layer-3 routing Multiple VRF • Static routing • Routing Information Protocol (RIP)v1 and v2 • Open Shortest Path First (OSPF) v2 with Graceful Restart • Intermediate System to Intermediate System (IS-IS) with Graceful Restart • Border Gateway Protocol (BGP) v4 with Graceful Restart • Generic Routing Encapsulation (GRE) and IP/IP tunneling • Virtual Router Redundancy Protocol (VRRPv2)	C/PC/NC	
Triple speed (10/100/1G/2.5G/5G) user interfaces and fiber interfaces (SFPs) supporting 1000Base-X, 10GBase-X,QSFP+ optical transceivers	C/PC/NC	
10 G,25G,40G and 100G uplinks	C/PC/NC	
Wire-rate switching and routing performance	C/PC/NC	
High availability with virtual chassis concept, redundant stacking links, primary/secondary unit failover, hot-swappable power options and configuration rollback	C/PC/NC	
Enhanced Voice over IP (VoIP) and video performance with policy-based QoS	C/PC/NC	
Future-ready support for multimedia applications with wire-rate multicast	C/PC/NC	

Airgroup™ Network Services for Bonjour speaking devices provides consistent experience over wireless and wired networks	C/PC/NC	
IEEE 802.3af, IEEE 802.3at and IEEE802.3bt PoE support for IP phones, wireless LAN (WLAN) access points and video cameras	C/PC/NC	
Switch capacity up to 1,020 Tb/s	C/PC/NC	
Application monitoring and enforcement	C/PC/NC	
Extensive security features for network access control (NAC), policy enforcement and attack containment	C/PC/NC	
Shortest path bridging (SPB-M) for bridging and routed services	C/PC/NC	
• Advanced guest management capabilities • Device on-boarding and automated IEEE 802.1x provisioning • Device posture/health check and fingerprinting • Application management	C/PC/NC	

Core Switch

Description	Compliance	Notes
From 2.16 Tbps to 6,4 Tbps of bandwidth in a 1 RU form factor	C/PC/NC	
Shall support different models that can integrate into one virtual chassis 48 fixed 1/10-Gbps SFP+ ports,32 fixed 100 Gbps Ports and 24 Port fixed 1/10Gig ports	C/PC/NC	
Shall support 10Gig,25Gig,40Gig and 100Gig Port combinations in one virtual chassis	C/PC/NC	
Shall support up to 72 SFP+ ports by splitting each available QSFP28 ports into 4 x 10G/25 SFP+ ports.	C/PC/NC	
Latency of less than or equal to 650 nanoseconds	C/PC/NC	
Front-to-back or back-to-front airflow configurations	C/PC/NC	
1+1 redundant hot-swappable power supplies	C/PC/NC	
Shall allow upgrade to entire operating system without impacting data forwarding for a lossless fabric environment	C/PC/NC	
Shall have cut-through switching on all the ports	C/PC/NC	

Shall support, with multiple node virtualization, a mix-and-match architecture with various switch models providing a virtual chassis with flexible port models of 1/10/25/40/100G fiber or 1G/10G copper connectivity.	C/PC/NC	
Shall support a virtual chassis architecture of up to 6 switches for future scalability.	C/PC/NC	
Shall support Shortest Path Bridging (SPB) protocol for network service virtualization.	C/PC/NC	
Shall allow Link aggregation w/ loop free active-active topology w/o STP.	C/PC/NC	
Shall support equal-cost multipath packet forwarding	C/PC/NC	
Shall support virtualization	C/PC/NC	
Shall support link aggregation of up to 16 links	C/PC/NC	
Shall support Link Aggregation Control Protocol (LACP): IEEE 802.3ad	C/PC/NC	
Shall allow link aggregation with loop free active-active topology without STP	C/PC/NC	
Shall run Layer-3 routing protocols	C/PC/NC	
The switch operating system source code shall undergo independent verification and validation by a third-party company specializing in software and cyber security to ensure total operating system hardening.	C/PC/NC	
The switch operating system distribution shall support multiple operating system copies each with different diversified software mapping to prevent exploitation.	C/PC/NC	
Shall support the following industry standards: IEEE 802.1D: Spanning Tree Protocol, IEEE 802.1p: CoS prioritization, IEEE 802.1Q: VLAN tagging, IEEE 802.1Qaz: Enhanced transmission selection, IEEE 802.1Qbb: Per-priority Pause, IEEE 802.1s: Multiple VLAN instances of Spanning Tree Protocol, IEEE 802.1w: Rapid reconfiguration of Spanning Tree Protocol, IEEE 802.3: Ethernet, IEEE 802.3ad: LACP with fast timers, IEEE 802.3ae: 10 Gigabit Ethernet, RMON, IEEE 1588-2008: Precision Time Protocol (Boundary Clock)	C/PC/NC	
Shall allow Scalable integrated security service into network fabric.	C/PC/NC	

802.3X Ethernet PAUSE auto-negotiation enhancements	C/PC/NC	
BGP,OSPF,Virtual Router Redundancy Protocol (VRRP)	C/PC/NC	
VLAN-tagged Layer 3 logical interfaces	C/PC/NC	
BPDU protection for spanning-tree protocols	C/PC/NC	
Loop protection for spanning-tree protocols	C/PC/NC	
Root protection for spanning-tree protocols	C/PC/NC	
Spanning-Tree (All variants)	C/PC/NC	
Private VLANs	C/PC/NC	
Q-in-Q Tunneling & VLAN Translation	C/PC/NC	
Layer 2 Tunneling Protocol	C/PC/NC	
Reflective relay (IEEE 802.1bg)	C/PC/NC	
Bidirectional Forwarding Detection (BFD)	C/PC/NC	
Intermediate System-to-Intermediate System (IS-IS)	C/PC/NC	
Routing Information Protocol versions 1 and 2 (RIPv1 and RIPv2)	C/PC/NC	
Virtual router routing instances for multicast protocols	C/PC/NC	
Protocol Independent Multicast sparse mode (PIM SM)	C/PC/NC	
Remote port mirroring	C/PC/NC	
sFlow monitoring technology	C/PC/NC	
Simple Network Management Protocol version 3 (SNMPv3)	C/PC/NC	
Link fault propagation	C/PC/NC	
DHCP snooping	C/PC/NC	
Resilient hardware system architecture.	C/PC/NC	

VXLAN snooping for dynamic real-time multi-tenant visibility and SLA policy enforcement	C/PC/NC	
Integrated overlay (VXLAN) and underlay internetworking automated with OpenStack neutron plug-in	C/PC/NC	
Intelligent policy control through OpenFlow 1.3.1/1.0.	C/PC/NC	
Hardware virtual routing and forwarding (VRF) support for VRF-lite and IP Virtual Private Network (IP VPN) SPB for bridging and routed services, Multiple VLAN Registration Protocol (MVRP) and dynamic Virtual Network Profiles (VNP).	C/PC/NC	
Zero-touch provisioning and network automation with out-of-the-box plug-and-play Auto-Fabric for automatic protocol and topology discovery	C/PC/NC	
Unified virtual chassis with support for up to 6 switches.	C/PC/NC	
Flexible and programmable Layer 2, Layer 3, ACL, QoS network virtualization function abstracted into a single virtual routing and bridging instance	C/PC/NC	
embedded scripting capabilities supporting Python and Bash programming.	C/PC/NC	
Fully programmable RESTful web services interface with XML and JSON support. The API enables access to Command Line Interface (CLI) and individual management information base (MIB) objects.	C/PC/NC	
Powerful WebView Graphical Web Interface through HTTP and HTTPS over IPv4/IPv6	C/PC/NC	
Full configuration and reporting using Simple Network Management Protocol (SNMP) v1/2/3 to facilitate third-party network management over IPv4/IPv6	C/PC/NC	
Multiple microcode image support with fallback recovery	C/PC/NC	
sFlow v5 and Remote Network Monitoring (RMON)	C/PC/NC	
Dynamic Host Configuration Protocol (DHCP) relay	C/PC/NC	
Built-in CPU protection against malicious attacks	C/PC/NC	
Dynamic Virtual Network Profiles (vNP)	C/PC/NC	
Multiple VRF	C/PC/NC	

Static routing with route labeling	C/PC/NC	
Routing Information Protocol (RIP) v1 and v2	C/PC/NC	
Open Shortest Path First (OSPF) v2 with graceful restart	C/PC/NC	
Intermediate System to Intermediate System (IS-IS) with graceful restart	C/PC/NC	
Border Gateway Protocol (BGP) v4 with graceful restart	C/PC/NC	
Generic Routing Encapsulation(GRE) and IP/IP tunneling	C/PC/NC	
Virtual Router Redundancy Protocol (VRRPv2)	C/PC/NC	
DHCP relay (including generic UDP relay)	C/PC/NC	
USB port	C/PC/NC	
Out-of-band Ethernet port	C/PC/NC	
Shall support the technology of multiple switch virtualization which consists of multiple interconnected switches becoming a single node at control, forwarding, and management planes. The resulting virtual chassis shall have a single IP address and MAC address for the management and data planes, and shall support link aggregation (802.3ad) with ports spread across different switches for full redundancy and load balancing.	C/PC/NC	

WLAN

Solution & Architecture Overview

Description	Compliance	Notes
1. The wireless LAN solution shall be based on IEEE 802.11 and shall be WFA certified for Data and Voice.	C/PC/NC	
2. The wireless LAN solution shall propose a distributed control function (no centralized controller) with inherent support for redundancy, elimination of traffic bottlenecks and lowered latency.	C/PC/NC	
3. The wireless LAN solution shall rely on a distributed data plane.	C/PC/NC	

4.The wireless LAN solution shall come in two flavors allowing three deployment types: ▪ "small deployment" for a mono-site deployment with Access Points spread over a single management VLAN and operating in a common RF environment ▪ "large deployment" for a multi-site deployment with Access Points spread over multiple management VLANs, and that may operate in a different RF environment ▪ "Cloud deployment" for any deployment (single or multi-site) with Centralized Management in the cloud. For all deployment types, the solution shall offer advanced features like Intrusion Detection/Prevention or a Captive Portal to manage guests' connections without additional third-party components.	C/PC/NC	
5. The wireless LAN solution shall propose a centralized management function, irrespective of the deployment model ("small" or "large") as described previously [4].	C/PC/NC	
6. The wireless LAN solution shall scale up to 4096 Access Points for the "large deployment" model [4], 255 Access Points for the "small deployment" model [4] and thousands of users while guarantee ease of deployment and expansion (to be described).	C/PC/NC	
7. The "small deployment" option previously described [4] shall not require any license fee.	C/PC/NC	
8. The "large deployment" option previously described [4] shall rely on a licensing model that is as simple as possible, with one license per AP including all functions (basic or advanced) handled by the AP.	C/PC/NC	
9.The "small deployment" (255 APs) option shall allow an easy migration to a "large deployment" (4096 APs) when needed.	C/PC/NC	
10. The wireless LAN solution shall have been designed with scalability in mind in order to allow the 4096 APs limit to be extended in the future (to be described) *without requiring new equipment or deployment design change.*	C/PC/NC	
11. For a "small deployment" scenario as described previously [4], the wireless LAN solution shall propose built-in DHCP, DNS and NAT capabilities.	C/PC/NC	

12. The WLAN solution shall allow to connect two distant sites over a wireless point-to-point link.	C/PC/NC	
13. The WLAN solution shall allow to connect multiple distant sites over wireless. (Mesh Network)	C/PC/NC	
14. The WLAN solution shall allow easier deployment of Mesh Networks.	C/PC/NC	
15. The WLAN solution shall support IPv6 for wireless clients.	C/PC/NC	
16. The WLAN solution shall support L2GRE tunneling with a highly flexible architecture.	C/PC/NC	
17. The WLAN solution shall support RAP functionality, allowing an AP to secure the traffic sent over an untrusted network like the Internet. Should use the latest security standards like WireGuard.	C/PC/NC	

Access Control, Authentication and Encryption

Description	Compliance	Notes
15. The wireless LAN solution shall support MAC based authentication.	C/PC/NC	
16. The wireless LAN solution shall support 802.1x based authentication.	C/PC/NC	
17. At least for a “large deployment” scenario as described previously [4], the WLAN solution shall include a built-in RADIUS server for 802.1x and MAC authentication that shall not be proposed as a separate product.	C/PC/NC	
18. The built-in RADIUS server as described previously ([17]) shall be able to interface with an external authentication server (Radius, LDAP, Active Directory): Free Radius, Microsoft NPS Radius Server, Microsoft AD, OpenLDAP…	C/PC/NC	
19. The built-in RADIUS server as described previously [17] shall support at least following EAP types: EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-PEAP-MSCHAPv2, EAP-GTC.	C/PC/NC	

20. At least for a “large deployment” scenario as described previously [4], the WLAN solution shall include a built-in RADIUS server for 802.1x and MAC authentication that shall not be proposed as a separate product.	C/PC/NC	
21. The built-in RADIUS server as described previously ([20]) shall be able to interface with an external authentication server (Radius, LDAP, Active Directory): FreeRadius, Microsoft NPS Radius Server, Microsoft AD, OpenLDAP…	C/PC/NC	
22. The built-in RADIUS server as described previously [20] shall support following EAP types: EAP-MD5, EAP-TLS, EAP-AKA, EAP-PEAP, EAP-FAST, EAP-SIM, EAP-TTLS, EAP-GTC.	C/PC/NC	
23. At least for a “large deployment” scenario as described previously [4], the wireless LAN solution shall have the ability to utilize RADIUS attributes to assign each authenticated user/device to a specific ROLE. A role defines a VLAN and enforces security and QoS through the use of role-based ACLs and QoS policies that can be directly integrated with the roles defined within existing authentication servers.	C/PC/NC	
24. At least for a “large deployment” scenario as described previously [4], the wireless LAN solution shall include and handle a flexible and adaptive RADIUS attributes dictionary allowing to add an IETF or any vendor specific RADIUS attribute.	C/PC/NC	
25. If the built-in RADIUS server as described previously ([20]) shall interface with an external RADIUS server, then it shall be able to interface with multiple and distinct RADIUS servers depending on specific access conditions (SSID name, Access Point IP address, identity of the connecting user…)	C/PC/NC	
26. The wireless LAN solution shall support following link layer encryption standards: WPA2_AES, WPA2_TKIP, WPA_AES, WPA_TKIP, DYNAMIC_WEP, WPA_PSK_AES, WPA_PSK_TKIP, WPA_PSK_AES_TKIP, WPA2_PSK_AES, WPA2_PSK_TKIP, WPA3_PSK_SAE_AES, WPA3_SAE_AES.	C/PC/NC	
27. The wireless LAN solution shall support the latest WPA3 encryption standard.	C/PC/NC	

28. The wireless LAN solution shall support following 802.1x supplicants: Windows 7, 10, MAC OS, IOS, Android, Chromebook…	C/PC/NC	
29. The wireless LAN solution shall support time-based policy access to a SSID.	C/PC/NC	
30. Irrespective of the deployment model (“small” or “large”) as described previously [4], the wireless LAN solution shall propose a “Guest” management solution based on an embedded and built-in Captive Portal providing web based authentication for guests and visitors.	C/PC/NC	
31. The Guests Captive Portal included in the wireless LAN solution shall allow a customizable look & feel.	C/PC/NC	
32. The Guest management solution shall allow, at least, following authentication methods: • Username & Password • Access Code • Simple Term & Condition acceptance	C/PC/NC	
33. A least for a “large deployment” scenario as described previously [4], the Guest management solution shall allow guests to authenticate using their favorite social network account (supported social networks shall be listed).	C/PC/NC	
34. Irrespective of the deployment model (“small” or “large”) as described previously [4], the wireless LAN solution shall offer the possibility to build a walled garden environment (with configured domain names) for guest users before they authenticate.	C/PC/NC	
35. The Guest management solution shall allow non-IT staff (e.g., a receptionist) to create temporary guest accounts.	C/PC/NC	
36. A least for a “large deployment” scenario as described previously [4], the WLAN solution shall allow guest self-registration and employee sponsored access.	C/PC/NC	
37. The WLAN solution shall allow guests accounts bulk provisioning by importing a file containing guest accounts information and shall propose a template import file.	C/PC/NC	
38. A least for a “large deployment” scenario as described previously [4], the WLAN solution shall allow	C/PC/NC	

to create batch of guests accounts just by specifying a guest prefix and a number of accounts to be created.		
39. A least for a “large deployment” scenario as described previously [4], the WLAN solution shall allow to define networking SLAs (security, QoS…) to be applied to guests network connections.	C/PC/NC	
40. A least for a “large deployment” scenario as described previously [4], the WLAN solution shall allow to define and apply “data quotas” to guests to limit access based on total traffic consumed.	C/PC/NC	
41. A least for a “large deployment” scenario as described previously [4], the WLAN solution shall allow guests SMS notification.	C/PC/NC	
42. Irrespective of the deployment model (“small” or “large”) as described previously [4], the wireless LAN solution shall offer the possibility to interface with a third-party external Captive Portal for guests authentication, without necessarily forcing the traffic to through any server or appliance.	C/PC/NC	
43. A least for a “large deployment” scenario as described previously [4], the WLAN solution shall implement strict guests traffic isolation.	C/PC/NC	
44. For a “small deployment” scenario as described previously [4], the Guest management solution shall not require any license fee.	C/PC/NC	
45. For a “large deployment” scenario as described previously [4], the Guest management solution shall allow setting a validity period for an authenticated device, in order to avoid entering credentials each time a guest access the network.	C/PC/NC	
46. A least for a “large deployment” scenario as described previously [4], the WLAN solution shall implement strict guests traffic isolation.	C/PC/NC	
47. The WLAN solution shall allow data retention on user sessions when providing Guest Wi-Fi.	C/PC/NC	
48. In the framework of a “large deployment” scenario as described previously [4], the WLAN solution shall support BYOD and be able to provide device on-boarding that is as simple as possible and without requiring additional third-party components.	C/PC/NC	

49. The on-boarding process of employee devices shall be based on employee corporate accounts.	C/PC/NC	
50. The BYOD application shall allow setting the validity period for the device, and the maximum number of devices per account.	C/PC/NC	
51. The licensing model of the BYOD application shall be based on the number of on-boarded devices.	C/PC/NC	
52. The WLAN solution shall support DSPSK to allow the use of different Pre-Shared Keys (PSK) in the same SSID at the same time	C/PC/NC	
53. The WLAN solution shall support the WIFI4EU initiative from the EU. That includes support for Hotspot 2.0 (Passpoint Wi-Fi Alliance certification program)	C/PC/NC	
54. The WLAN solution shall support the EDUROAM authentication hierarchy for Universities and Research Centers	C/PC/NC	

RF Management

Description	Compliance	Notes
55. The WLAN solution shall allow automatic and/or manual RF management (channel and power).	C/PC/NC	
56. The WLAN solution shall support Short Guard Interval.	C/PC/NC	
57. The WLAN solution shall be smart enough to guide a new client to the optimal band/channel (2.4GHz/5GHz) considering, at a given time, both the number of associated clients on each band, and the medium utilization.	C/PC/NC	
58. If no band/channel (2.4GHz/5GHz) is overloaded (high medium utilization) or crowded (high client count), an AP shall by default guide a new client to the 5GHz band.	C/PC/NC	
59. Even if the 5GHz band is not overloaded but is crowded (high client count), an AP shall guide a new client to the 2.4GHz band.	C/PC/NC	
60. If a band/channel (2.4GHz/5GHz) is overloaded (high medium utilization) and even if it is not crowded,	C/PC/NC	

an AP shall guide a new client to the less loaded band/channel.		
61. If all bands/channels (2.4GHz/5GHz) are overloaded (high medium utilization) and no band/channel is crowded, an AP shall guide a new client to the 5GHz band.	C/PC/NC	
62. If all bands/channels (2.4GHz/5GHz) are overloaded (high medium utilization) and the 5GHz is crowded, an AP shall guide a new client to the 2.4GHz band.	C/PC/NC	
63. When a new client discovers multiple APs to associate to, the new client shall be guided to the AP that has the fewest associated clients, thus allowing smart/dynamic load balancing.	C/PC/NC	
64. The WLAN solution shall force clients to the 5GHz only when there are dual band capable.	C/PC/NC	
65. The WLAN solution shall deny connection to an AP when the signal of the client becomes too weak and disconnect a client to force it to roam when the signal becomes too weak.	C/PC/NC	
66. The WLAN solution shall support the IEEE 802.11v and 802.11k standards to facilitate network guided roaming.	C/PC/NC	
67. The WLAN solution shall support data rate control to encourage clients to roam at higher rates.	C/PC/NC	
68. The WLAN solution shall propose APs that can scan the air in order to provide interfering/rogue APs and wireless attacks detection and shall not rely on dedicated scanning equipment.	C/PC/NC	
69. The scanning function of the APs shall not impact active voice or video calls (SIP and H.323).	C/PC/NC	
70. At least for the 5GHz band, the WLAN solution shall allow to define the list of channels which can participate in dynamic configuration.	C/PC/NC	
71. The WLAN solution shall allow to define a range of transmit power per band (min & max) even if power settings are configured for automatic and dynamic assignments.	C/PC/NC	
72. The WLAN solution shall propose Access Points which can all be configured and deployed in a dedicated scanning mode.	C/PC/NC	

73. The WLAN solution shall propose Access Points with wireless packet capture capabilities.	C/PC/NC	
74. The WLAN solution shall make it simple to review the roaming history for a given client device.	C/PC/NC	
75. The WLAN solution shall allow long interval background scanning.	C/PC/NC	

Intrusion Detection and Prevention

Description	Compliance	Notes
76. The WLAN solution have wIDS/wIPS capabilities with no additional and dedicated equipment nor additional license.	C/PC/NC	
77. The WLAN solution shall be able to identify Interfering APs.	C/PC/NC	
78. The WLAN solution shall be able to identify and contain Rogue APs.	C/PC/NC	
79. The WLAN solution shall allow the definition of flexible policies to classify an AP as a Rogue AP.	C/PC/NC	
80. A least for a “large deployment” scenario as described previously [4], the WLAN solution shall allow the definition of flexible AP attacks detection policies.	C/PC/NC	
81. A least for a “large deployment” scenario as described previously [4], the WLAN solution shall allow the definition of flexible client attacks detection policies.	C/PC/NC	
82. A least for a “large deployment” scenario as described previously [4], the WLAN solution shall be able to blacklist a WLAN client, either manually or automatically after a client attack has been detected.	C/PC/NC	
83. A least for a “large deployment” scenario as described previously [4], the WLAN solution shall allow to configure a blacklist duration.	C/PC/NC	
84. A least for a “large deployment” scenario as described previously [4], the WLAN solution shall allow to configure an authentication failure times threshold.	C/PC/NC	

Quality of Service

Description	Compliance	Notes
85. At least for a “large deployment” scenario as described previously [4], the WLAN solution shall offer WLAN Access Points that shall support fine-tuned Quality of Service (QoS) allowing following actions based on the identity of the connecting user: - ACL based (source/destination IP address and TCP/UDP ports) permit/deny decision - QoS priority marking and queuing	C/PC/NC	
86. The wireless LAN solution shall comply with the 802.11e WMM standard and shall allow for custom QoS tag (802.1p/DSCP) to WMM queue mapping.	C/PC/NC	
87. A least for a “large deployment” scenario as described previously [4], the WLAN solution shall have traffic Deep Packet Inspection (DPI) capabilities allowing an administrator to take control of applications (even if they all run on top of the HTTP or HTTPs protocols), including not only blocking applications, but also allowing to prioritize and rate-limit applications.	C/PC/NC	
88. The wireless LAN solution shall be able to define and guarantee bandwidth based on the SSID. At least for a “large deployment” scenario as described previously [4], it shall also be to define and guarantee bandwidth based on the user/device role.	C/PC/NC	
89. At least for a “large deployment” scenario as described previously [4], the WLAN solution shall allow to set the maximum number of clients per band/radio and per AP for a specific SSID.	C/PC/NC	
90. The wireless LAN solution shall propose broadcast traffic optimization mechanisms (including Broadcast filtering and Broadcast/Multicast Key rotation).	C/PC/NC	
91. Leveraging its IGMP snooping capabilities, the wireless LAN solution shall be able to optimize multicast traffic by converting multicast traffic to unicast traffic.	C/PC/NC	
92. At least for a “large deployment” scenario as described previously [4], Multicast optimization shall stop on high load.	C/PC/NC	
93. The wireless LAN solution shall propose the WMM Automatic Power Save delivery (APSD) feature to allow clients conserve battery life.	C/PC/NC	

94. The wireless LAN solution shall by default identify Voice and Video (SIP and H323) calls and provide appropriate treatment.	C/PC/NC	

Mobility

Description	Compliance	Notes
95. The WLAN solution shall support Layer 2 roaming capabilities across APs with no special client-side software required.	C/PC/NC	
96. At least for a “large deployment” scenario as described previously [4], the WLAN solution shall support Layer 3 roaming across APs with no special client-side software required.	C/PC/NC	
97. The WLAN solution shall support both *Opportunistic Key Caching (802.11k).*	C/PC/NC	
98. The WLAN solution shall comply with the 802.11k Radio Resource Management standard.	C/PC/NC	
99. The WLAN solution shall comply with the 802.11v BSS Transition Management standard.	C/PC/NC	

Wireless LAN Services

Description	Compliance	Notes
100. The solution shall provide BYOD Zeroconf services for mDNS	C/PC/NC	

Management

Description	Compliance	Notes
101. The wireless LAN solution shall propose a centralized management function based on an embedded and secure WEB GUI, irrespective of the deployment model (“small” or “large”) as described previously [4].		
102. In addition to a centralized management function, all Access Points of the wireless LAN solution shall propose a dedicated web interface to monitor and configure a single AP in the global infrastructure,	C/PC/NC	

irrespective of the deployment model (“small” or “large”) as described previously [4].		
103. If the centralized management function requires the deployment of a dedicated application, this one shall be in the form of a Virtual Appliance that can be installed on top of any of following hypervisors: VMware ESXi, Microsoft HyperV and Oracle VirtualBox.	C/PC/NC	
104. At least for a “large deployment” scenario as described previously [4], the centralized management function shall be able to handle wired equipment (switches) management for a “unified management” approach.	C/PC/NC	
105. The WLAN solution shall be able to automatically discover new APs added to the network.	C/PC/NC	
106. At least for a “large deployment” scenario as described previously [4], the centralized management function shall allow to display the physical topology of the network, including wireless links between APs.	C/PC/NC	
107. The centralized management function shall allow per equipment configuration and software backup and restore, and bulk backup and restore	C/PC/NC	
108. The centralized management function shall allow access to all wIPS/wIDS features.	C/PC/NC	
109.At least for a “large deployment” scenario as described previously [4], the centralized management function shall offer, based on an application signature file, insight at application layer (e.g. facebook.com, youtube.com, salesforce.com…) even if the applications run on top of the HTTP or HTTPs protocols. It shall also allow control of those applications.	C/PC/NC	
110. At least for a “large deployment” scenario as described previously [4], the centralized management function shall allow to display the Wi-Fi coverage quality within a given area (“Heat Map”).	C/PC/NC	
111. At least for a “large deployment” scenario as described previously [4], the centralized management function shall allow, before deployment, to determine optimal placement of Access Points (APs) in a location (RF Planning).	C/PC/NC	

112. At least for a “large deployment” scenario as described previously [4], the centralized management function shall be collocated with the Guest and BYOD management applications.	C/PC/NC	

Indoor Access Point – Basic

Description	Compliance	Notes
The WLAN solution shall propose an 802.11ax MU-MIMO indoor tetra-radio AP Access Point (2,4GHz, 5GHZ, Full Band Scanning dedicated Radio and Bluetooth/Zigbee): “**Error! Reference source not found.**”.	C/PC/NC	
The “Basic” Access Point shall offer native BLE5.1/Zigbee radio support.	C/PC/NC	
The “Basic” Access Point shall support up to 32 SSIDs (16 per radio).	C/PC/NC	
The “Basic” Access Point shall offer up to 1,2Gbps throughput on the 5Ghz band and up to 573Mbps throughput on the 2.4GHz band.	C/PC/NC	
The “Basic” Access Point shall support up to 512 clients.	C/PC/NC	
The “Basic” Access Point shall have two 1Gb Ethernet ports, which may be aggregated as a single logical link (LACP).	C/PC/NC	
The “Basic” Access Point shall have one 1Gb Ethernet port, for LAN connectivity or “downlink”.	C/PC/NC	
The “Basic” Access Point shall propose L7 Application recognition (DPI) capabilities providing a real-time classification of flows at the application level.	C/PC/NC	
The “Basic” Access Point shall support 802.3af/at PoE with 19.1W maximum consumption.	C/PC/NC	
The MTBF for the “Basic” Access Point shall be at least 978,601 h (111.71 years).	C/PC/NC	
The “Basic” Access Point shall propose a Factory reset button.	C/PC/NC	
The “Basic” Access Point shall propose a console port.	C/PC/NC	

The “Basic” Access Point must have a dedicated radio for scanning the whole WLAN spectrum (2,4GHz and 5GHZ) for detecting security and RF anomalies.	C/PC/NC	
The “Basic” Access Point shall support 802.3af/at PoE with 19.1W maximum consumption.		

Indoor Access Point-Mid-Range

Description	Compliance	Notes
The WLAN solution shall propose an 802.11ax MU-MIMO indoor tetra-radio AP Access Point (2,4GHz, 5GHZ, Full Band Scanning dedicated Radio and Bluetooth/Zigbee): “Medium Density”.	C/PC/NC	
The “Medium Density” Access Point shall have integrated omnidirectional antennas or be equipped with external antennas.	C/PC/NC	
The “Medium Density” Access Point shall offer native BLE5.1/Zigbee radio support.	C/PC/NC	
The “Medium Density” Access Point shall support up to 32 SSIDs (16 per radio).	C/PC/NC	
The “Medium Density” Access Point shall offer up to 2,4Gbps throughput on the 5Ghz band (low and high bands) and up to 573Mbps throughput on the 2.4GHz band.	C/PC/NC	
The “Medium Density” Access Point shall support up to 1024 clients.	C/PC/NC	
The “Medium Density” Access Point shall have one 1Gb Ethernet port and one 2.5Gb Ethernet (IEEE 802.3bz Multi-rate Gigabit Ethernet), which may be aggregated as a single logical link (LACP)	C/PC/NC	
The “Medium Density” Access Point shall propose L7 Application recognition (DPI) capabilities providing a real-time classification of flows at the application level.	C/PC/NC	
The “Medium Density” Access Point shall support 802.3af/at PoE with 24.8W maximum consumption.	C/PC/NC	
The MTBF for the “Medium Density” Access Point shall be at least 1,104,490 h (126.08 years).	C/PC/NC	

The “Medium Density” Access Point shall propose a Factory reset button.	C/PC/NC	
The “Medium Density” Access Point shall propose a console port.	C/PC/NC	
The “Medium Density” Access Point must have a dedicated radio for scanning the whole WLAN spectrum (2,4GHz and 5GHZ) for detecting security and RF anomalies.		

Indoor Access Point- High Range

Description	Compliance	Notes
The “High Density ” Access Point shall propose an 802.11ax MU-MIMO indoor AP WITH five built-in radios, three radios 2.4Ghz/5Ghz Low/5Ghz High Density band serving High Density Wi-Fi clients, one full band radio dedicated for scanning, which can inherently improve network security and Wi-Fi quality, and an integrated Bluetooth/Zigbee radio	C/PC/NC	
The “High Density” Access Point shall have integrated omnidirectional antennas or be equipped with external antennas.	C/PC/NC	
The “High Density” Access Point shall offer native BLE5.1/Zigbee radio support.	C/PC/NC	
The “High Density” Access Point shall support up to 48 SSIDs (16 per radio).	C/PC/NC	
The “High Density” Access Point shall offer up to 9.6Gbps throughput on the 5Ghz band (low and High Density bands) and up to 1.2Gbps throughput on the 2.4GHz band.	C/PC/NC	
The “High Density” Access Point shall support up to 1536 clients.	C/PC/NC	
The “High Density” Access Point shall have 2x multi-Gigabit 1/2.5/5/10 Gig autosensing(RJ-45) ports, Eth0-Eth1, Power over Ethernet (PoE) 802.3bt compliant 1x USB 3.0 Type A (5V, 500mA)	C/PC/NC	
The “High Density” Access Point shall propose L7 Application recognition (DPI) capabilities providing a real-time classification of flows at the application level.	C/PC/NC	
The “High Density” Access Point shall support 802.3af/at/bt PoE with 45W maximum consumption.	C/PC/NC	

The MTBF for the “High Density” Access Point shall be at least 572,332h (65.33 years).	C/PC/NC	
The “High Density” Access Point shall propose a Factory reset button.	C/PC/NC	
The “High Density” Access Point shall propose a console port.	C/PC/NC	
The “High Density” Access Point must have a dedicated radio for scanning the whole WLAN spectrum (2,4GHz and 5GHZ) for detecting security and RF anomalies.	C/PC/NC	

Outdoor Access Point

Description	Compliance	Notes
The WLAN solution shall propose a 802.11ax MU-MIMO outdoor ruggedized tetra-radio AP Access Point (2,4GHz, 5GHZ, Full Band Scanning dedicated Radio and Bluetooth/Zigbee). “Outdoor”	C/PC/NC	
The “Outdoor” Access Point shall have integrated omnidirectional antennas, integrated sectorial antennas, or be equipped with external antennas.	C/PC/NC	
The “Outdoor” Access Point shall support up to 32 SSIDs (16 per radio).	C/PC/NC	
The “Outdoor” Access Point shall offer up to 2.4Gbps throughput on the 5Ghz band and up to 573Mbps throughput on the 2.4GHz band.	C/PC/NC	
The “Outdoor” Access Point shall support up to 1024 clients.	C/PC/NC	
The “Outdoor” Access Point shall have one (1) 10/100/1000/2500MBaseT Ethernet port UPLINK port, 802.3at/bt compliant.	C/PC/NC	
The “Outdoor” Access Point shall have one (1) 10/100/1000MBaseT Ethernet port DOWNLINK, 802.3at compliant, with PoE PSE output so that an end device can be directly connected and powered from the AP, for example an Outdoor CCTV camera.	C/PC/NC	
The “Outdoor” Access Point shall have one (1) SFP port for connecting optical fiber transceivers or GPON SFP-ONT.	C/PC/NC	

The “Outdoor” Access Point shall propose L7 Application recognition (DPI) capabilities providing a real-time classification of flows at the application level.	C/PC/NC	
The “Outdoor” Access Point shall be IP66/67 certified.	C/PC/NC	
The “Outdoor” Access Point shall support persistent moisture and precipitation, and high and low temperatures: -40°C to 65°C.	C/PC/NC	
The “Outdoor” Access Point shall support 802.3af/at PoE with 64W maximum consumption, when powering a PSE device with 802.3at	C/PC/NC	
The MTBF for the “Outdoor” Access Point shall be at least 1,003,257h (114.5 Years).	C/PC/NC	
The “Outdoor” Access Point shall propose a Factory reset button.	C/PC/NC	
The “Outdoor” Access Point must have a dedicated radio for scanning the whole WLAN spectrum (2,4GHz and 5GHZ) for detecting security and RF anomalies.	C/PC/NC	

Asset Tracking Chapter

Tool Management

Description	Compliance	Notes
The Asset Tracking solution, must support the following features as minimum	C/PC/NC	
Sign-in/sign-up to asset tracking access	C/PC/NC	
User profile management (Role)	C/PC/NC	
Create and modify a site, buildings and floors	C/PC/NC	
Geo-referencing a site	C/PC/NC	
Asset management and configuration	C/PC/NC	
Asset category management	C/PC/NC	
Web-based Asset provisioning tool	C/PC/NC	
Web-based Asset search tool, based on Asset category and Asset Name	C/PC/NC	

See the assets on a map and filter on all categories defined	C/PC/NC	
Gateway configuration	C/PC/NC	
Tags management and configuration	C/PC/NC	

Asset Provisioning

Description	Compliance	Notes
Configuration and parameterization of the tags to a material or a person	C/PC/NC	
Each device can be associated with an image, a category and personalized parameters	C/PC/NC	
Reassigning tags to new equipment/people	C/PC/NC	
Asset Provisioning via Web Access.	C/PC/NC	
Asset Provisioning via an App tool, running in a smartphone	C/PC/NC	

Asset Search

Description	Compliance	Notes
Search and location of material, people in real time	C/PC/NC	
Search per category of equipment	C/PC/NC	
Search per category of person	C/PC/NC	

Analytics

Description	Compliance	Notes
Analytics Dashboard	C/PC/NC	
History of location coordinates, equipment/people.	C/PC/NC	
Data related to the use of Geo Notification in each area.	C/PC/NC	

Geo-notification

Description	Compliance	Notes
Geo-Fence and Geo-fence Notification	C/PC/NC	
Web-Application and email geo-fence notification	C/PC/NC	

Tags

Description	Compliance	Notes
The Asset Tracking solution, must support the inclusion of the following Tags:	C/PC/NC	
Asset tag with Accelerometer	C/PC/NC	
Equipment tag with Wristband support	C/PC/NC	
Card shaped tag, to attach to a user (ex: doctor/Nurse) badge	C/PC/NC	
Small wristband tag, to attach to a user (ex: patient)	C/PC/NC	
Asset tag with a configurable button	C/PC/NC	

Gateways

Description	Compliance	Notes
Explain what models of Gateways an APs, are supported in the Asset Tracking solution For the Gateways	C/PC/NC	
The Gateways, must have the capacity to receive the signals from the tags, and send the information by wireless or an attached RJ45 port	C/PC/NC	
The gateways must be compatible with any Wi-Fi WLAN in the market, and be a Wi-Fi client of them	C/PC/NC	
The gateways must support PoE	C/PC/NC	
The gateways must support a local power supply in alternative	C/PC/NC	

Telecommunication Systems Chapter

Telephone System:

Description	Comply (Y/N)	Tenderer comment
The PBX solution should be highly available, resilient, and potential for additional facilities		
This system will operate 24/24, 365 days per year. It should be designed to make it easy for maintenance and the upgrades without service interruption		
In case of failure of one of the PBX components, the PBX system should continue to operate via a redundant service		
The IP telephony system should comply to the IETF, IEEE, CEPT and ITU-T recommendations, and with the country rules		
The voice system should be based on the following standards: - IETF: SIP capable - Proprietary		
The offered solution should allow interoperability between H.323 equipment with any legacy devices (digital, analogue, DECT, public and privates lines) and SIP devices		
SIP compliance: The SIP minimum version should be compliant to: - Proxy SIP - SIP Registry - SIP gateway - SIP applications		
The Tenderer will point out the session ports (TCP or UDP) used by the applications and subscribers		
Connection « direct mode » - G711 Fallback orT38 faxes - Direct RTP		
The offered conversation system should allow additional services such as: - Call Center - FMC (fixe-mobile-convergence) and BYOD - Subscribers' mobility (DECT/ IP-DECT or VoWLAN) - Voice messaging - Call recording - Call log - Unified Communications (UC) - Alarms to fix or mobiles subscribers		

General PBX Requirements:

Description	Comply (Y/N)	Tenderer comment
The property PBX solution should be highly available, resilient, and potential for additional facilities.		

Public network requirements:

Description	Comply (Y/N)	Tenderer comment
SIP Trunking from several providers, with overflow, for outgoing		
ISDN E1 support		
ISDN T0 support		
Analogue Trunk support		
DDI		
CLI, adopted to SIP Trunk Provider, in Multi SIP Trunk provider scenario		

Voice Features:

Description	Comply (Y/N)	Tenderer comment
Account Codes: Allow for the input of either validated (pre-programmed in PBX) or non-validated account codes to place long distance calls. Codes shall be a minimum of 4 and a maximum of 12 Digits. This feature must be enabled by a class of service separate from all other classes of service. CDR must include the account code in addition to the station number from which the call was made (insert description of the -locations in the CDR output where the account code and station number will appear).		
User can also assign a project number to an incoming call: The system manager is also able to configure a phone with a forced project code. In this case, for every external call the user must dial the project code to set up the call. During a consultation		

call the project account code for the new external call maybe change. During an automatic callback on busy trunk group, the project account code is automatically stored. On callback, the user does not have to dial the code again.		
Alarm Condition: major and minor. The system shall provide six severity levels with visual (colors) and numerical display: - Critical - Major - Minor - Warning - Indeterminate Clear (related a former alarm that has been corrected) The total number of alarms/levels is indicated at the bottom of the list, for the item selected in the tree. The maximum number of alarms stored can be configured by the manager. (Default = 1,000 alarms). The oldest alarms are automatically overwritten.		
Alternate Answer Position: In addition to the attendant console, it shall be possible for any station to answer incoming calls.		
Area/Office Code Restriction: The system has the capability for single digit, multiple digits, or area code/country code toll restriction, depending on completion of calls.		
Attendant multiple camp-on: This feature is used when the attendant console routes an external call to an internal phone. During the ringing phase, the attendant can monitor the call using the camp-on soft key. Pressing this soft key will display calls that remain unanswered (internal and external numbers). Then, the attendant can decide to: Cancel the selected station Re-select a new station Switch back and forth between calls Send a message to the station Release the call		
Attendant Trunk Selection with Supervision This function indicates the external line status (free, busy, on hold, or ringing). The supervision key can also be used to intercept an incoming call on the trunk line. When the trunk line is in idle state, pressing the icon supervision key seizes the trunk line.		
Controlled Private calls: With the controlled private call feature, a company can track and charge back for personal outgoing		

employee calls. The user is defined by the following items (if the user has a phone): One directory number (virtual or real) One PIN One call class of service restriction for private calls The user can make a private call according to the following rules: Only from the user' own phone From any authorized phone in the sub network From a few selected phones (linked with 256 connection classes of service) The Communication Server shall control the PIN code and ensure that two employees cannot have the same PIN. Such private calls can be forwarded to internal (including network) or external numbers. Automatic Call back - No Answer: An internal call reaching an unanswered station shall have the ability to activate a Call back code: When the unanswered station is placed off-hook and then on-hook the system shall then attempt to connect the original party		
Automatic Route Selection: see least cost routing below.		
Automatic Station Release: Provides automatic release of stations where handsets are left off-hook for a pre-determined length of time.		
Call pickup group: The PBX must support a minimum of thirty (30) digita1/analog stations in a pick group.		
Rerouting Calls on Ringing: When a phone is called, the called party can forward (transparent to the caller) this call to another phone during the ringing period. Dialing the number or name of the addressee’s phone activates the service on single-line phones. On multi-line phones, a soft key is pressed prior to the number of the addressee. If an attendant call, rerouting call on ringing cannot be activated.		
All incoming calls (DID or Internal) that are extended to a station that is busy will route to that station's voice mail if the forward busy is programmed as voice mail		
When the voice mail is inoperable, external incoming calls should return to the operator consoles after a pre-determined number of rings (in seconds).		

Calling Name ID: The multi-line station display provides a visual display of the called party name when connected to a station.		
Calling Number Display: The multi-line station users shall be presented with the number and name (if available) of the calling party's station before answering.		
Called Party Status: The multi-line station display provides a visual indication of the called party status (i.e., Busy, forwarded)		
Class of Service: Specify number of classes available. The console shall be able to change a station's class of service. These classes of service shall include but not be limited to: Out of service Intercom line Internal extensions only Local calls on Local calls and domestic long distance only Unrestricted In any case all extension shall be able to call the operator without restriction		
Conference calls: Provide the capability for six (6) party conference calls and the ability to drop one (1) or more of the parties during the conference call and add one (1) or more parties during the same conference call. Data privacy:		
Music on Hold: System will be equipped with an audio input port for music to callers who have been put on hold or in a camped-on position either by the operator or station user. This feature shall be configurable by station. For example, callers put on hold to reservations will get music. Callers to other departments will not.		
Power Failure Restart: After a power failure, system automatically restarts. No station database information, including extension numbers, classes of service, system speed call numbers, etc. can be lost		
Power Failure Transfer: If batteries become spent, this feature provides automatic ringing of and direct access to a pre-designated number 0 Central Office lines at a predetermined number of single line phones on a one-to-one basis during the failure. At least twenty-eight lines will be so transferred during a complete failure Private Line Termination: It shall be possible to		

terminate a Central Office line on a specific instrument or instruments. Such line need not be terminated on all instruments.		

Facilities Requirements:

Description	Comply (Y/N)	Tenderer comment
The PBX will be able to support the following ETSI or ANSI facility features: Capable of supporting a variety call route types including incoming, DID, Direct E1, 2-way trunks within E1 circuits, ISDN PRI or BRI connectivity and Analogue Trunks		
Able to support dynamically allocated incoming toll-free calls on both-way E1 circuits, routing the toll-free calls to specific extensions or ACD groups separate from incoming calls to other numbers		
Supports distant end completed call signaling (answer supervision) over E1 or T0 and ISDN services and outputs CDR only when distant end completed call signaling is received over those trunks.		
Supports answer supervision on local switched trunks and output CDR only when such signaling is received over those trunks provided the local central office provides that information to the switch.		
Supports call by call allocation through the Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) connection.		
Progress tones: At a minimum, the following progress tones shall be available: dial tone, busy tone, ring back tone		
Support shall be either by card difference, software changes or both		

Station Set Features:

Description	Comply (Y/N)	Tenderer comment
Add-On Conference: allows a station user to add a third party to an existing two-party conversation.		
Answer Hold: Working in association with an incoming call or camped-on call, the station user, upon hearing the appropriate camp-on or call waiting tone, will flash the switch hook on the		

station instrument. The ongoing call is placed on hold and a connection to the waiting call is Immediate.		
Alphanumeric Display: for all electronic sets with digital display.		
Automatic call distribution: for all phones in the reservations department, as well as key groups.		
Automatic Privacy: Upon answering any line the automatic privacy feature shall be invoked. This feature shall prevent any other telephone instrument from gaining access to that line while a conversation is in progress.		
Call Forwarding - Busy: Calls to a busy station hunt to a second station, a message centre, or an operator. It must be possible for this destination to be different from the call forward no answer destination.		
Call Forwarding - No Answer: Calls automatically reroute to the attendant or programmed secondary station when a given station does not answer within a prescribed time. It must be possible for this destination to be different from the call forward busy destination.		
Call Forwarding - Station Programmable: Station user can program any extension number to which to route all Incoming calls. This feature takes precedence over call forward no answer feature.		
Call Forwarding - All: Forwards calls to a particular extension overriding any busy, no-answer, or station-programmed setting.		
Call Forward destinations may be internal extensions or off-site numbers, with appropriate classes of service.		
Call Park: A called party can place a call in the "park" state on a designated terminal number until it is retrieved. When placed in "park" the caller shall hear music if such is configured. If the "parked" call is not retrieved within 60 seconds, the call should re-ring the attendant. A five-lamp line status indicator shall display the status of each parked number at the attendant console. A park number may be accessed from either an internal station calls or a DID call		
Call Pickup: A station user can answer a call at any other station by use of a code number and the extension number of the ringing station. Pickup - Grouping a station user may answer a call at a station with a pre-defined group by use of a code number.		

Call to a hunt group: A hunt group may be called by dialing a specific directory number, which is different from the individual directory number of the phones belonging to the group. A group member may receive both group and personal calls. The selection of a free phone in the group may be performed in three different ways: • Serial hunt or fixed distribution: starting systematically from the headphone of the group • Circular hunt or cyclical distribution: if the last phone called in the group has the position n, the search for a free phone begins at the phone with the position n +1 • Parallel distribution: all phones ring simultaneously		
A queue can be defined for each group. When all the group's phones are busy, the call is camped on the ringing tone or on a specific waiting message. The queue size is defined by a ratio of the active group's phones; this ratio can reach 100%. After handling a call, a group phone will be called only after a fixed time period. Management defines this as wrap-up time. A phone can exit from its group via a special prefix. In this state, it can still receive personal calls. The user can return to the group at any time by dialing a prefix or pressing the specific soft key. A phone may only belong to one group		
Call Waiting: Assigned on a Class of Service per station basis and working in conjunction with attendant or station camp-on facilities, this shall permit a station to receive a second call.		
Calling Number Name Display: As part of a multi-line telephone, a display will indicate the incoming call status as well as the extension number and/or name of the caller or called party. Allow to display second incoming call on hunt line.		
Conference: three and six party		
Consultation Hold: Allows the station user to put the original call on hold, establish a second call, without using key equipment		
Do Not Disturb: This feature shall be provided either through a do not disturb-button on each instrument or a programmable feature code.		
Executive COS: Assigned to a given station, feature denies any other station or attendant the ability to use various overriding features or apply tones associated with call waiting to that busy line. When the Executive busy on a call there must be no interruptions, like intrusion or tones		
Extension to Extension dialing: Each extension shall have the ability to dial any other extension without the aid of PBX operators.		
Certain extensions must be prevented from making calls to other extensions		

Flexible Station-Controlled Conference: A station-initiated conference facility which allows non-preselected internal stations to be added to a conference situation as well as adding outside trunk circuits. This is accomplished by dialing each desired party individually in sequence.		
Fully Restricted Stations: Through class of service, selected station lines are denied the ability to place or receive any but internal station-to-station calls.		
Howler Alert: When a station instrument is off-hook without dialing after a predetermined time interval, the system will provide a howler tone to indicate that the phone is off-hook. While the phone is in this state and an external user calls the station, the caller will be connected to the operator.		
Hunting: Allows internal or external calls to a busy or no-answer station to be re-directed to a free station within the hunt group. The call searches for the free station in a pre-determined manner.		
Indication of Clear to Station: A short burst of tone is transmitted to the busy station to indicate another call is waiting. The party to whom the busy station is talking does not hear the tone.		
Individual Transfer Intercom service: Multi-line instruments may be connected in pairs or larger groups by private talk paths. Dial or button signaling is provided. Key groups: for various departments with more than three phones		
Last Number Redial		
Loud Ringing Option: Allows for the connection of an external loud signaling device to be connected to an electronic multi-line telephone.		
Message Waiting Indication: must be visual. Must be available on all guest and administrative sets as per station review. All set types must be able to be activated by command from voice mail system.		
Off-Premises Extensions: The PBX is capable of extending system station line circuits to industry standard instruments at off-premise locations.		
Protection against Barge-in: Station users may prevent interruption of their call by any tone or signal, by the attendant or others using a code		
Speed Calling: Users may dial telephone numbers by use of a code that is programmed as either system wide or personal.		

Speed Calling by Name: For sets with a keypad the call can be made by typing a name and select		

Attendant Console Features:

Description	Comply (Y/N)	Tenderer comment
Alarms: catastrophic and major alarms requiring immediate action to maintain service shall appear on the attendant console or an associated display. Alphanumeric Display for Attendant Position: A visual display using numeric and alphabetic characters indicating the trunk or line to which the attendant is connected. Other information such as intercept details, class of service and call type should also be displayed.		
Attendant Conference: Allows the attendant to establish a conference call between a set number of inside or outside parties		
Attendant Numerical Call Waiting Display: A special display located on the console giving an indication of the number of calls waiting for attendant processing.		
Attendant Transfer - All Calls: Ability for the attendant to transfer any call that appears at the console position (internal, incoming to any non-busy extension in the system		
Automatic Recall: Automatically alerts the attendant after a prescribed period to a camped-on or unanswered call completed through the console. This enables the attendant to give a status report to the outside calling party. These calls will queue in order of presentation, as well as being placed first in the overall queue.		
Bad Line Reporting		
Busy Override: Allows attendant entry into an existing busy connection, providing a warning tone to the parties to indicate third-party entry		
Busy Verification of Stations and Trunks: Permits positive verification that a given circuit is busy, idle, or out of order.		
Call Splitting: Allows the attendant to speak privately with the source and destination parties, and to alternate between them without connecting them by use of special control keys		
Camp On: An incoming call that an attendant attempt to complete on a busy line within the system is placed in a special waiting mode until the desired station becomes idle. The called station is then automatically rung and connected to the incoming call upon answer.		

Cancellations: Attendant may cancel at any time on either a system wide or individual basis such station activation features as call forwarding or do not disturb.		
Console Answering Priorities: The priority with which calls are presented to the console can be programmed.		
Attendant can provide a line to an extension that do not have to rights to make a call. This is allowed for a single call only. The user can afterwards request a line again		
Direct Trunk Access, for testing		
Message Waiting: In the event the PMS system interface is down, messages waiting control should be done through the console		
Night Service: The attendant shall be able to transfer selected trunks to a specified telephone or console whenever regular consoles are not in use.		
Supervisory Console: In a multi-console system, one console can be programmed to have control over the others or have access to certain features which are denied to the other consoles.		
System Changes: The attendant, through the console, may restrict local and long-distance calls, change extension numbers, assign direct inward dial service, change station forwarding, and change COS assignments		
Trunk Group Status: The attendant receives a visual indication when all trunks in a given group are busy.		
Type of Call Display: Provides a visual display of the type of call reaching the attendant console.		
Volume Control - Console: Allows variable control of electronic audible signals at the attendant console. An on or off switch is not acceptable		
Realtime notification icons to show the status of users and call the user by selecting, click on		

Automatic Call Distribution ACD:

Description	Comply (Y/N)	Tenderer comment
The ACD must accept trunk and tie line calls from a variety of locations and process them by their originating point. These lines may include but are not restricted to:		

• Toll-free lines, Direct central office trunks, Tie line appearances, Extension lines from both in-house and remote PBX systems and IP routing		
The system will provide outgoing call forwarding or call diversion to other locations during hours when the reservations department is closed.		
ACD Display Feature: Logged-on agents see on their display telephones, the number of calls queued and trunk text. Each time an agent answers a call change in the call queue are reflected on the display. - ACD: Number of ACD calls processed in the processing group - Private: Number of private calls processed in the processing group - On wait: Number of calls waiting in the processing group		
Agent Activation: An agent joins a group through use of Logon key and (optionally) an agent ID code. If ID codes are used performance can be tracked by agent. Agent ID codes are assigned from the ACD Supervisor console. An ID can be used by only one agent. Logoff removes the agent from the group. Indicate the maximum number of agent IDs. Agent Outbound Calling: ability to restrict agent to intra system calls, local calls or limited long distance.		
Automatic Number Identification: Display the Automatic Number Identifier (ANI) on agent and supervisor telephones if the ANI is sent to the PBX		
Call Activity Display: Display real-time and, at a minimum display: • The number of calls waiting, • The number of calls abandoned within the last fifteen (15) minutes, • The total number of incoming calls within the last fifteen (15) minutes, • Non-active agents by agent • Average talk time per call by agent.		
Call Direction: Ability to direct calls to certain agents, and prioritize calls to specific numbers to specific agents, i.e., more experienced agents ret more calls, automatically direct a specific DID call to a specific agent.		
Call overflow: Overflow calls between agent and operator consoles, showing the number of the agent		
Disconnect: When the agent finishes a call, a specified key is pressed to disconnect. Position is then ready to accept another call.		

Forced Answer: Calls are connected automatically. The telephone will not ring, and agent does not have to press any key to answer. A tone will be provided to alert the agent when a call is presented.		
Group Size: Must be able to support a minimum often (10) agents in each ACD group		
Help: By pressing a designated key at any time an agent can reach supervisor for assistance. This places all on hold and automatically dials supervisor.		
Manual Answer: Phone rings and agent presses a specified key to answer		
Record: When pressed this key activates a recording machine. .		
Recorded Announcements: Must be able to direct a different sound source and/or at least three (3) different announcements to each ACD group simultaneously.		
Reports: • Whether placed in a queue or not, show the number of calls directed to group, • The number of calls abandoned by quarter-hour, • Average speed of answer, • Average wait time before answer, • Average talk time per call by group and agent, • Average post call processing (Wrap up) by group and agent, • Average calls handled in quarter-hour segments by individual agents, • Total number of calls processed by group and by individual agents, • Total incoming calls and CCS by trunk/extension by hour • Number of calls answered within x period of time (e.g., Twenty (20) seconds).		
ACD reports can be programmed to print automatically daily. Reports shall also be available on demand and at any time as elected by the Property. Reports from all ACD groups must be able to be configured to print on a single printer. A print report to file application will be reviewed if available		
Transfer - Agent to agent: within queue to an agent in a busy condition		
Transfer - Outside Line: ability to transfer a call to an outside line. If available, this must be restricted on a set-by-set basis.		

Unavailable: Pressing a -designated key will prevent additional ACD calls from being presented to position.		

Announcements:

Description	Comply (Y/N)	Tenderer comment
Greeting: notifies caller that call has been recognized but cannot be answered immediately. The call is placed in a queue.		
Night: callers reach an ACD when all agents logged off. After callers hear the announcement, the call is disconnected.		
Delay: encourages callers to continue holding until call can be serviced. A call is taken from the call queue to hear the delay message and then returned to its original place in queue		
Overflow: in lieu of or in combination with an overflow answering (station or another ACD group) calls are routed to an overflow point when the queue exceeds maximum number of calls. Each group can have its own announcements or groups can share. Announcement lengths can vary for groups, but all announcements within a group must be the same length. Permissible ranges are 0-255 seconds.		
All announcements are broadcast, allowing many callers to get the same announcement simultaneously which requires only a single announcement source per announcement.		
Automatic Answer: The system automatically answers incoming calls with an announcement if all agents are busy.		
Call Queue: When all agents are busy additional incoming calls are answered with the greeting announcement and placed in a queue in order of arrival. While in queue, calls can be provided with Music-on-Hold. Calls are processed using FIFO. When the number of calls in a queue exceeds the maximum, calls can be routed to other answering positions for handling. Call Queue Full: If the queue contains the maximum number of calls allowed, the call will not receive the greeting announcement but is routed directly to the overflow point.		

Supervisor Features:

Description	Comply (Y/N)	Tenderer comment
Break in: Pressing a designated key while listening to a busy tone or while monitoring an agent/customer conversation sounds the break in tone and a three-way conversation is established.		

Observe: key allowing supervisor to listen in on call without notification.		
Barge-in with being heard by the calling party: supervisor can speak with the agent without informing the calling party.		
Permanent monitoring: proceed to a silent listening or a barge-in		

Video Conferencing:

The primary purpose of video conferencing is to improve communications between people. To this end, video conferencing should serve to:

- Increase the quality and effectiveness of long-distance collaboration including the ability explain complex issues, share ideas, resolve problems, and take more immediate action.
- Provide more efficient access to key decision makers and domain experts across the organisation.
- Improve the ability to hold regular management meetings.
- Improve the ability to broadcast senior management briefings (both live and recorded).
- Reduce the amount and cost of unnecessary business travel between the shopping centres and head office.
- Reduce the amount and cost of lost productivity – particularly on the part of senior management.

Description	Comply (Y/N)	Tenderer comment
User can make a video conference call with 120 participants		
Join from Desk phone, PC, Smart phone, or external users can join by Browser (HTTPS)		
Users can connect via Application or Internet browser		
Video, Audio, Instant Messaging, File and Screen sharing		
One-on-one recoding of video call from PC, including Screen sharing recording		
Invitations sent through user application or email		
External parties can join without installing an application or the need of a license, with ‘click-to-join’ in the invite		
Instant meetings or scheduled		
Calendar invites via Outlook or Google		

Video codec (VP8) or similar with 720p at 30 fps, H264 also supported		
Participants can be added during the conference		
During conference list of participants visible		
Organizer can Mute or un-mute participants		
Active speaker indication, minimum four simultaneous speakers		
Promote a participant to Organizer role		
Enable Screen sharing rights to a participant during a conference		

Mobility (Unified Communications)

- Mobility on Private and Public network
- One account for all devices; multi-devices
- The user can decide where to take his audio or video call. Desk phone, PC or Smart phone
- Whether the user is on the WIFI network or outside on 4/5G, without VPN
- This is additional functionality not covered by technologies such as DECT, IP-DECT and VoWLAN

Description	Comply (Y/N)	Tenderer comment
One account with multiple devices - PBX Deskphone - Smartphone - Tablet - PC		
Integration with PBX and PBX features such as: - Search the PBX phonebook - Click to call to extension users - Call log - Manage call routing of desk phone, smartphone, tablet, and PC - Transfer - 3 Party Conference - VoIP calling - Make and receive external incoming and outgoing calls through the PBX from the Private or Public network - Hold and retrieve call - Redial - Divert call to Voicemail - PBX Voicemail		

- Broker call - Send DTMF - Voicemail		
User can make and receive audio calls with the Smart phone while on the 4/5G Network outside the company and transfer the call to another user on the PBX		
User can answer an audio call made to the Desk phone from the Smart phone while on the 4/5G Network outside the company and transfer the call to another user on the PBX		
User can make a video call to another user from Desk phone, PC, Tablet or Smart phone		
User can make a video conference call with 30 participants		

Unified Communication and Collaboration

- Refer to section on Mobility (UC) and Video conferencing, also included
- Instant creation of a group, and addition and deletion of members by the user
- Use case collaboration between Citizens, Government Staff, Guests and Politicians

Description	Comply (Y/N)		Tenderer comment
Video, Audio, Instant Messaging, File and Screen sharing			
Promote another user to group organizer			
Presence status display of team members			
Invites sent by email, SMS, Google contacts			
Share company information/ news to all employees and external people			
Collaboration between employees and external parties			
Instant Messaging Group messaging Copy messages Share geo-locations from Smart phones with GPS capabilities Send messages by email Remove messages Use of emoticons and animated GIFs Spell check Record and send voice messages			

CPaaS (Communication Platform as a Service)

- Digital transformation, integration with Government platforms
- People tracking and Asset's tracking
- Connecting the communication platform with Government processes
- Connecting the staff, external Government services, citizens, guests, and politicians, etc.

Description	Comply (Y/N)		Tenderer comment
API to share via Web interface administrative documents: - Users log onto the Web Portal and has access to documents for download - Uploading of documents			
API to access Web Portal, which offers: - IM, web audio and callback - Chat bot			
Appointment application: - To remind a person of an appointment - Via Web page, Smart phone, or Tablet			
Chatbot application: - Via Web Portal			
SDK for Teleconsultation			
Pathfinding application on BYOD. Self-guided navigation tool. Find equipment and assets			
Self-service application on BYOD, during visits.			
Video call between people via BYOD			
Asset tracking: - Physical location tracking - Alarm when assets leave pre-configured areas			
Remote specialist consultations			
Virtual Waiting room			

Notification Services

- Notification solution with various applications integrating with the PBX and UC platform
- In the case of an emergency, people must be notified by multiple media options

- Connecting the communication platform (PBX) with a Notification Service platform

Description	Comply (Y/N)		Tenderer comment
Loudspeaker broadcast on Desk phones triggered by alarms, such as a fire alarm			
Nurse call to multiple destinations, including smart applications and PBX phones, as well as nurse calendar checking			
ESPA/ TAP, broad spectrum protocols support			
Camera integration and movement detection alarms			
Wander detection with alarm to security with location services (map location) - Map of building and grounds			
Alarm escalation via SMS, if nurse not acknowledging alarm			
Alarms to security team through smart applications on mobile devices			
Video call between people and family or helpers via BYOD			
Input and output from and to: - Email - Social media, such as Twitter and Facebook - ESPA/TAP - Dry contacts - Smartphones/ tablets - Web interface - IP phones - WIFI handsets			
Graphical location services/ display of building map and floorplans To identify the location of the notification trigger			

Management System

- Easy to use comprehensive management solution to manage the PBX system with devices
- System monitoring

Description	Comply (Y/N)	Tenderer comment

PBX management system - Mass deployment			
Graphical display			
Topology view of PBX system and devices			
PBX Alarm notification by email, SNMP			
VoIP auditing of PBX calls and Performance Monitoring			
APIs for integration with Microsoft Active Directory - Users added on company database automatically added on PBX			
LDAP Company Directory integration for 'Dial-by-name'			
System maintenance: scheduled backups of the PBX system			
The web client provides an easy access to the company directory, with the possibility to update the information, a personal address book and "Click to call"			
Users can place a call by clicking on the displayed phone number from the Directory via the web client			
Automatic reports sent via email			
More than 10 concurrent Administration client logins			

Security:

Telephones:

Description	Comply (Y/N)	Tenderer comment	
NAC: - 802.1.x - EAP-MD5 - EAP-TLS			
ARP spoofing protection			
DOS attack protection			
Signalling Encryption: - TLS 1.2 - With Authentication - Certificate based authentication, SHA_2 signed			

Media Encryption: - SRTP			

Communication Server (PBX):

Description	Comply (Y/N)		Tenderer comment
Traffic filtering: - Trusted hosts - TCP Wrapper			
Encryption: - SSHv2 access - TLS1.2 for secure HTTP session (web based management) -			
Authentication - Local authentication database (password policy enforcement) - External authentication protocols supported (RADIUS & LDAP/LDAPs)			
OS Hardening			
Defence against DOS attacks			
TFTP files integrity check			
Anti-MAC spoofing			

Management System:

Description	Comply (Y/N)		Tenderer comment
Access to server: - Hard Client with IPSec - Web Client via HTTPS			
Password policy enforcement: - Minimum length - Aging - Historic not allowed - Blocking			
External Radius authentication			

Client rights: - Different accounts with different right to manage PBX - Client and Administrator profiles			
SMTP			
LDAPS: - Integration with PBX - Integration with External AD			
PKI (Public Key Infrastructure): - Certificate creation			

Redundancy:

Description	Comply (Y/N)		Tenderer comment
PBX Redundancy: - Active Standby servers - IP phones stays in communication with switch-over - Dual LAN ports for network redundancy			
Media Redundancy - Dual LAN ports for network redundancy			
Remote sites: - Full services of phones and lines when network break with Central system			

Telephone devices:

- Common criteria:
- All Desk phone terminals must have the following capabilities:

Description	Comply (Y/N)		Tenderer comment
1GB network interface			
1GB PC port. PC behind phone			
Headset capabilities - Either USB, 3.5mm jack, RJ9 or Bluetooth			
Support Wideband audio			
POE			
Security. See security compliance for terminals in previous section			
Screen			
Programmable function keys			

Executive phones:

- Can also be used as a conference room device

- Or Video Doorcam device with Door opening capabilities

Description	Comply (Y/N)		Tenderer comment
Support Video			
Built-In camera or without camera			
Touch screen 7”			
Color screen			
Bluetooth for handset or headset			
eHD Audio and Loudspeaker			
HDMI port for external screen			
Alphabetic keyboard			
Support Android applications			
Access to ‘YouTube’ videos			
Video Doorcam receive with Door open capability			

Executive phones2:

Description	Comply (Y/N)		Tenderer comment
Touch screen 5”			
Color screen			
Bluetooth for handset or headset			
eHD Audio and Loudspeaker			
Alphabetic keyboard			
Add-on keys, additional keys			
Hot desking			

Executive phones3:

Description	Comply (Y/N)		Tenderer comment
Color screen			
Bluetooth for handset or headset			
eHD Audio and Loudspeaker			
Alphabetic keyboard			
Add-on keys, additional keys			
Hot desking			

Soft Phone:

Description	Comply (Y/N)		Tenderer comment
Windows and MAC PC based			
Smartphone Android and iOS			
Tablet Android and iOS			
Same capabilities as Executive phone3			

VoWLAN phone Entry level:

Description	Comply (Y/N)		Tenderer comment
Unified Communication device			
Backlit			
Handsfree speaker			
Talk time 15 hours			
PBX Directory integration			
PBX features			
Backlit/ Color screen			
Radio			
Programmable keys			
Multi device of Desk phone			
Reliability: Ingress Protection IP44			
802.11a/b/g radio			
802.11e QOS and WMM			

VoWLAN phone advance level:

Description	Comply (Y/N)		Tenderer comment
Unified Communication device			
Backlit			
Handsfree speaker			
Talk time 15 hours			
PBX Directory integration			
PBX features			
Backlit/ Color screen			
Radio			
Programmable keys			
Multi device of Desk phone			
Reliability: Ingress Protection IP44			
802.11a/b/g radio			
802.11e QOS and WMM			
Push-to-talk			
Alarm button			
Color screen			
Vibrate mode			

Hosted Voice and Data Services:

Description	Comply (Y/N)		Tenderer comment
Does your submission provide for a hybrid deployment whereby the legacy system (Alcatel/Lucent & Huawei) can work together seamlessly.			
Are you using Sita as your connectivity provider			
Does your solution have sufficient checks and balances in place to prevent data loss between the different sites and different platform users/deployments (Legacy/Hosted)			

The current Hosted Solution is provided on the Mitel platform/ application, it being the preferred solution provider here, does your solution provide for it.			
Do you have sufficient resources (HR) available to provide all services and support on the Mitel Hosted Solution,			
Does your solution adhere to the minimum industry standards and norms in this sphere of operations but must be flexible enough to be able to meet any changes in Councils requirements here.			
The disaster recovery DC must be TIA certified. If not this will lead to disqualification. (The DC used must be in Tshwane)			
Sufficient connectivity into and out of the system must be provided that the principle of 1 point of failure be prevented.			
SLA level must be at 99%. Nothing less will be accepted.			
Power levels of 4.4kw per rack, per customer must be guaranteed.			
Strict security per rack per customer must be guaranteed (Remote Monitoring and Control – Remote Hands)			
Advanced fire detection & suppression and in-row cooling, using the latest AC principles must be guaranteed			
BMS system (or a comparative system providing the same functions) must be provided to monitor all aspects of the Data Centre (24/7/365).			
Unrestricted interconnects must be provided for			
Skilled, technical resources – 6 Certified Uptime Institute Data Centre Design Engineers must be provided for or must be readily available for support.			
The solution provided must be a Intelligent Data Centre to allow for the use of and deployment of the latest AI technologies to improve security and enhance monitoring			
Hosted Unified Communication solution must be deployed to ensure that a unified secure voice solution can be done from any location			
The following Security Principles must be provided for: • 24/7/365 on-site automated security • Proximity & Biometric Access Control • Digital Security Video Surveillance • Follow Me AI controlled surveillance • Automated reception visitor control' • 512 bit SSL encryption depending on Client Certification • IP address blocking (White- and Blacklisting			
The following Support principles must be provided for: • Dark Disaster Recovery Facility • 24/7 Data Centre Remote Monitoring • Advanced Resolution System • Trouble Ticketing System			
The following Connectivity principles must be provided for: • Unlimited Connectivity • Private VLAN via Public & Private NW • Geographically redundant DNS			

• Dual-Stack IPv4 and IPv6 Capable			
The following Power, Fire and Cooling principles must be provided for: • Unlimited Connectivity • Private VLAN via Public & Private NW • Geographically redundant DNS • Dual-Stack IPv4 and IPv6 Capable			
The following Power, Fire and Cooling principles must be provided for • A & B redundant Electrical Distirbution configured 2(n+n), better than TIA 3 certified. • Fully redundant in row Cooling System configured 2(n+1), better than TIA 3 certified. • Fire detection and Gas Suppression system (Co2)			
The following Advanced Monitoring principles must be provided for • Remote monitoring systems, infrared cameras with unlimited recording preserved to be provided for • Biometric access control system throughout the facility must be provided for • 19 inch 42U racks with electronic access control			

MBD1

PART A
INVITATION TO BID

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE CITY OF TSHWANE MUNICIPALITY					
BID NUMBER:	GICT 03 2025/26	CLOSING DATE:	25 September 2025	CLOSING TIME:	10:00
DESCRIPTION	TENDER TO PROVIDE, OPERATE AND MAINTAIN THE ICT CORPORATE NETWORK EQUIPMENT, EXISTING HOSTED VOICE AND DATA SOLUTION DEPLOYED, AND THE EXPANSION OF THE EXISTING CORPORATE NETWORK AS AND WHEN FOR A PERIOD OF THREE (3) YEARS				
THE SUCCESSFUL BIDDER WILL BE REQUIRED TO FILL IN AND SIGN A WRITTEN CONTRACT FORM (MBD7).					

BID RESPONSE DOCUMENTS MAY BE DEPOSITED IN
THE BID BOX SITUATED AT *(STREET ADDRESS)*

Tshwane House
Supply Chain Management
320 Madiba Street
Pretoria CBD
0002

SUPPLIER INFORMATION						
NAME OF BIDDER						
POSTAL ADDRESS						
STREET ADDRESS						
TELEPHONE NUMBER	CODE		NUMBER			
CELLPHONE NUMBER						
FACSIMILE NUMBER	CODE		NUMBER			
E-MAIL ADDRESS						
VAT REGISTRATION NUMBER						
TAX COMPLIANCE STATUS	TCS PIN:		OR	CSD No:		
B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE [TICK APPLICABLE BOX]	☐ Yes ☐ No		B-BBEE STATUS LEVEL SWORN AFFIDAVIT		☐ Yes ☐ No	
[A B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE/ SWORN AFFIDAVIT (FOR EMES & QSEs) MUST BE SUBMITTED IN ORDER TO QUALIFY FOR PREFERENCE POINTS FOR B-BBEE]						
ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS	☐Yes ☐No [IF YES ENCLOSE PROOF]		ARE YOU A FOREIGN BASED SUPPLIER FOR THE		☐Yes ☐No [IF YES, ANSWER PART B:3]	

/SERVICES /WORKS OFFERED?		GOODS /SERVICES /WORKS OFFERED?	
TOTAL NUMBER OF ITEMS OFFERED		TOTAL BID PRICE CURRENT EQUIPMENT SOLUTION	R
TOTAL NUMBER OF ITEMS OFFERED		TOTAL BID PRICE ALTERNATIVE EQUIPMENT SOLUTION	R
SIGNATURE OF BIDDER	……	DATE	
CAPACITY UNDER WHICH THIS BID IS SIGNED			

BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO:		**TECHNICAL INFORMATION MAY BE DIRECTED TO:**	
DEPARTMENT	Supply Chain Management	DEPARTMENT	SHARED SERVICES: ICT DIVISION
CONTACT PERSON	Relebogile Malatswane	CONTACT PERSON	LeRoy Olivier
TELEPHONE NUMBER	012 358 2735	TELEPHONE NUMBER	012 358 4994
EMAIL ADDRESS	RelebogileM@tshwane.gov.za	EMAIL ADDRESS	siphomadh@tshwane.gov.za

PART B
TERMS AND CONDITIONS FOR BIDDING

1. BID SUBMISSION	
1.1	BIDS MUST BE DELIVERED BY THE STIPULATED TIME TO THE CORRECT ADDRESS. LATE BIDS WILL NOT BE ACCEPTED FOR CONSIDERATION.
1.2	**ALL BIDS MUST BE SUBMITTED ON THE OFFICIAL FORMS PROVIDED–(NOT TO BE RE-TYPED) OR ONLINE**
1.3	THIS BID IS SUBJECT TO THE PREFERENTIAL PROCUREMENT POLICY FRAMEWORK ACT AND THE PREFERENTIAL PROCUREMENT REGULATIONS, 2022, THE GENERAL CONDITIONS OF CONTRACT (GCC) AND, IF APPLICABLE, ANY OTHER SPECIAL CONDITIONS OF CONTRACT.
2. TAX COMPLIANCE REQUIREMENTS	
2.1	BIDDERS MUST ENSURE COMPLIANCE WITH THEIR TAX OBLIGATIONS.
2.2	BIDDERS ARE REQUIRED TO SUBMIT THEIR UNIQUE PERSONAL IDENTIFICATION NUMBER (PIN) ISSUED BY SARS TO ENABLE THE ORGAN OF STATE TO VIEW THE TAXPAYER'S PROFILE AND TAX STATUS.
2.3	APPLICATION FOR THE TAX COMPLIANCE STATUS (TCS) CERTIFICATE OR PIN MAY ALSO BE MADE VIA E-FILING. IN ORDER TO USE THIS PROVISION, TAXPAYERS WILL NEED TO REGISTER WITH SARS AS E-FILERS THROUGH THE WEBSITE WWW.SARS.GOV.ZA.

2.4	FOREIGN SUPPLIERS MUST COMPLETE THE PRE-AWARD QUESTIONNAIRE IN PART B:3.
2.5	BIDDERS MAY ALSO SUBMIT A PRINTED TCS CERTIFICATE TOGETHER WITH THE BID.
2.6	IN BIDS WHERE CONSORTIA / JOINT VENTURES / SUB-CONTRACTORS ARE INVOLVED, EACH PARTY MUST SUBMIT A SEPARATE TCS CERTIFICATE / PIN / CSD NUMBER.
2.7	WHERE NO TCS IS AVAILABLE BUT THE BIDDER IS REGISTERED ON THE CENTRAL SUPPLIER DATABASE (CSD), A CSD NUMBER MUST BE PROVIDED.

3. QUESTIONNAIRE TO BIDDING FOREIGN SUPPLIERS

3.1	IS THE ENTITY A RESIDENT OF THE REPUBLIC OF SOUTH AFRICA (RSA)?	YES ☐ NO ☐
3.2	DOES THE ENTITY HAVE A BRANCH IN THE RSA?	YES ☐ NO ☐
3.3	DOES THE ENTITY HAVE A PERMANENT ESTABLISHMENT IN THE RSA?	YES ☐ NO ☐
3.4	DOES THE ENTITY HAVE ANY SOURCE OF INCOME IN THE RSA?	YES ☐ NO ☐
3.5	IS THE ENTITY LIABLE IN THE RSA FOR ANY FORM OF TAXATION?	YES ☐ NO ☐

IF THE ANSWER IS "NO" TO ALL OF THE ABOVE, THEN IT IS NOT A REQUIREMENT TO REGISTER FOR A TAX COMPLIANCE STATUS SYSTEM PIN CODE FROM THE SOUTH AFRICAN REVENUE SERVICE (SARS) AND IF NOT REGISTER AS PER 2.3 ABOVE.

NB: FAILURE TO PROVIDE ANY OF THE ABOVE PARTICULARS MAY RENDER THE BID INVALID. NO BIDS WILL BE CONSIDERED FROM PERSONS IN THE SERVICE OF THE STATE.

SIGNATURE OF BIDDER: ……

CAPACITY UNDER WHICH THIS BID IS SIGNED: ……

DATE: ……

CITY OF TSHWANE
IGNITING EXCELLENCE

MBD 3.1

PRICING SCHEDULE: FIRM PRICES (PURCHASES)

NOTE: **ONLY FIRM PRICES WILL BE ACCEPTED. NON-FIRM PRICES (INCLUDING PRICES SUBJECT TO RATES OF EXCHANGE VARIATIONS) WILL NOT BE CONSIDERED**

IN CASES WHERE DIFFERENT DELIVERY POINTS INFLUENCE THE PRICING, A SEPARATE PRICING SCHEDULE MUST BE SUBMITTED FOR EACH DELIVERY POINT

Name of Bidder……	Bid Number ……
Closing Time ……	Closing Date ……

OFFER TO BE VALID FOR …… DAYS FROM THE CLOSING DATE OF BID.

ITEM NO.	QUANTITY	DESCRIPTION	BID PRICE IN RSA CURRENCY **(ALL APPLICABLE TAXES INCLUDED)

- Required by: ……..……...
- At: ……..…….……..
  ……..….
- Brand and Model ……..
- Country of Origin ……..
- Does the offer comply with the specification(s)? *YES/NO
- If not to specification, indicate deviation(s) ……..……
- Period required for delivery ……..……....
  *Delivery: Firm/Not firm
- Delivery basis ……..……....

Note: All delivery costs must be included in the bid price, for delivery at the prescribed destination.

** “all applicable taxes” includes value- added tax, pay as you earn, income tax, unemployment insurance fund contributions and skills development levies.

* Delete if not applicable

PRICING SCHEDULE: NON-FIRM PRICES (PURCHASES)

NOTE: PRICE ADJUSTMENTS WILL BE ALLOWED AT THE PERIODS AND TIMES SPECIFIED IN THE BIDDING DOCUMENTS.

IN CASES WHERE DIFFERENT DELIVERY POINTS INFLUENCE THE PRICING, A SEPARATE PRICING SCHEDULE MUST BE SUBMITTED FOR EACH DELIVERY POINT

Name of Bidder ……..	Bid number ……
Closing Time ……...	Closing Date ……

OFFER TO BE VALID FOR 90 DAYS FROM THE CLOSING DATE OF BID.

ITEM NO.	QUANTITY	DESCRIPTION	BID PRICE IN RSA CURRENCY **(ALL APPLICABLE TAXES INCLUDED)

- Required by: ……
- At: ……..…….
- Brand and model ……..……
- Country of origin ……..……
- Does the offer comply with the specification(s)? *YES/NO
- If not to specification, indicate deviation(s) ……..
- Period required for delivery ……..……
- Delivery: *Firm/Not firm

** ”all applicable taxes” includes value- added tax, pay as you earn, income tax, unemployment insurance fund contributions and skills development levies.

* Delete if not applicable

PRICE ADJUSTMENTS

A. NON-FIRM PRICES SUBJECT TO ESCALATION

1. IN CASES OF PERIOD CONTRACTS, NON FIRM PRICES WILL BE ADJUSTED (LOADED) WITH THE ASSESSED CONTRACT PRICE ADJUSTMENTS IMPLICIT IN NON FIRM PRICES WHEN CALCULATING THE COMPARATIVE PRICES

2. IN THIS CATEGORY PRICE ESCALATIONS WILL ONLY BE CONSIDERED IN TERMS OF THE FOLLOWING FORMULA:

$$Pa = (1 - V)Pt\left(D1\frac{R1t}{R1o} + D2\frac{R2t}{R2o} + D3\frac{R3t}{R3o} + D4\frac{R4t}{R4o} \right) + VPt$$

Where:

Pa = The new escalated price to be calculated.

(1-V) Pt = 85% of the original bid price. **Note that Pt must always be the original bid price and not an escalated price.**

D1, D2.. = Each factor of the bid price eg. labour, transport, clothing, footwear, etc. The total of the various factors D1,D2…etc. must add up to 100%.

R1t, R2t…… = Index figure obtained from new index (depends on the number of factors used).

R1o, R2o = Index figure at time of bidding.

VPt = 15% of the original bid price. This portion of the bid price remains firm i.e. it is not subject to any price escalations.

3. The following index/indices must be used to calculate your bid price:

Index……. Dated……. Index……. Dated……. Index……. Dated…….

Index……. Dated……. Index……. Dated……. Index……. Dated…….

4. FURNISH A BREAKDOWN OF YOUR PRICE IN TERMS OF ABOVE-MENTIONED FORMULA. THE TOTAL OF THE VARIOUS FACTORS MUST ADD UP TO 100%.

FACTOR (D1, D2 etc. eg. Labour, transport etc.)	PERCENTAGE OF BID PRICE

B. PRICES SUBJECT TO RATE OF EXCHANGE VARIATIONS

1. Please furnish full particulars of your financial institution, state the currencies used in the conversion of the prices of the items to South African currency, which portion of the price is subject to rate of exchange variations and the amounts remitted abroad.

PARTICULARS OF FINANCIAL INSTITUTION	ITEM NO	PRICE	CURRENCY	RATE	PORTION OF PRICE SUBJECT TO ROE	AMOUNT IN FOREIGN CURRENCY REMITTED ABROAD
				ZAR=		
				ZAR=		
				ZAR=		
				ZAR=		
				ZAR=		
				ZAR=		

2. Adjustments for rate of exchange variations during the contract period will be calculated by using the average monthly exchange rates as issued by your commercial bank for the periods indicated hereunder: (Proof from bank required)

AVERAGE MONTHLY EXCHANGE RATES FOR THE PERIOD:	DATE DOCUMENTATION MUST BE SUBMITTED TO THIS OFFICE	DATE FROM WHICH NEW CALCULATED PRICES WILL BECOME EFFECTIVE	DATE UNTIL WHICH NEW CALCULATED PRICE WILL BE EFFECTIVE

ADJUSTMENT PERIODS	DATE FROM WHICH NEW CALCULATED PRICES WILL BECOME EFFECTIVE
1st Adjustment	After 12 calendar months
2nd Adjustment	After 24 calendar months

NB: Unless prior approval has been obtained from Supply Chain Management, no adjustment in contract prices will be made

MBD 4

DECLARATION OF INTEREST

1. No bid will be accepted from persons in the service of the state[1].

2. Any person, having a kinship with persons in the service of the state, including a blood relationship, may make an offer or offers in terms of this invitation to bid. In view of possible allegations of favouritism, should the resulting bid, or part thereof, be awarded to persons connected with or related to persons in service of the state, it is required that the bidder or their authorised representative declare their position in relation to the evaluating/adjudicating authority.

3. In order to give effect to the above, the following questionnaire must be completed and submitted with the bid.

3.1 Full Name of bidder or his or her representative: ……

3.2 Identity Number: ……

3.3 Position occupied in the Company (director, trustee, hareholder[2]) ……

3.4 Company Registration Number: …….

3.5 Tax Reference Number: ……..

3.6 VAT Registration Number: ……..

3.7 The names of all directors / trustees / shareholders members, their individual identity numbers and state employee numbers must be indicated in paragraph 4 below.

3.8 Are you presently in the service of the state? **YES / NO**

3.8.1 If yes, furnish particulars. ……

……..

[1] MSCM Regulations: "in the service of the state" means to be –
(a) a member of –
(i) any municipal council;
(ii) any provincial legislature; or
(iii) the national Assembly or the national Council of provinces;
(b) a member of the board of directors of any municipal entity;
(c) an official of any municipality or municipal entity;
(d) an employee of any national or provincial department, national or provincial public entity or constitutional institution within the meaning of the Public Finance Management Act, 1999 (Act No.1 of 1999);
(e) a member of the accounting authority of any national or provincial public entity; or
(f) an employee of Parliament or a provincial legislature.

[2] Shareholder" means a person who owns shares in the company and is actively involved in the management of the company or business and exercises control over the company.

3.9 Have you been in the service of the state for the past twelve months? **YES/NO**

3.9.1 If yes, furnish particulars. ……

……..

3.10 Do you have any relationship (family, friend, other) with persons in the service of the state and who may be involved with the evaluation and or adjudication of this bid? **YES / NO**

3.10.1 If yes, furnish particulars. ……...

……..

3.11 Are you, aware of any relationship (family, friend, other) between any other bidder and any persons in the service of the state who may be involved with the evaluation and or adjudication of this bid? **YES / NO**

3.11.1 If yes, furnish particulars. ……

……..

3.12 Are any of the company's directors, trustees, managers, principle shareholders or stakeholders in service of the state? **YES / NO**

3.12.1 If yes, furnish particulars. ……

……..

3.13 Are any spouse, child or parent of the company's directors trustees, managers, principle shareholders or stakeholders in service of the state? **YES / NO**

3.13.1 If yes, furnish particulars. ……

……..

3.14 Do you or any of the directors, trustees, managers, principle shareholders, or stakeholders of this company have any interest in any other related companies or business whether or not they are bidding for this contract. **YES / NO**

3.14.1 If yes, furnish particulars: ……

……

CITY OF TSHWANE
IGNITING EXCELLENCE

4. Full details of directors / trustees / members / shareholders.

Full Name	Identity Number	State Employee Number

…… ……..

Signature **Date**

…… ……..

Capacity **Name of Bidder**

MBD 5

DECLARATION FOR PROCUREMENT ABOVE R10 MILLION (ALL APPLICABLE TAXES INCLUDED)

For all procurement expected to exceed R10 million (all applicable taxes included), bidders must complete the following questionnaire:

1 Are you by law required to prepare annual financial statements for auditing? ***YES / NO**

1.1 If yes, submit audited annual financial statements for the past three years or since the date of establishment if established during the past three years.

……

……

2 Do you have any outstanding undisputed commitments for municipal services towards any municipality for more than three months or any other service provider in respect of which payment is overdue for more than 30 days? ***YES / NO**

2.1 If no, this serves to certify that the bidder has no undisputed commitments for municipal services towards any municipality for more than three months or other service provider in respect of which payment is overdue for more than 30 days. ***YES / NO**

2.2 If yes, provide particulars.

……

……

……

……

3 Has any contract been awarded to you by an organ of state during the past five years, including particulars of any material non-compliance or dispute concerning the execution of such contract? ***YES / NO**

3.1 If yes, furnish particulars

……..

……..

4.1 Will any portion of goods or services be sourced from outside ***YES / NO**

the Republic, and, if so, what portion and whether any portion of payment from the municipality / municipal entity is expected to be transferred out of the Republic?

4.1 If yes, furnish particulars

……..

……..

CERTIFICATION

**I, THE UNDERSIGNED (NAME) ……..
CERTIFY THAT THE INFORMATION FURNISHED ON THIS DECLARATION FORM IS CORRECT. I ACCEPT THAT THE STATE MAY ACT AGAINST ME SHOULD THIS DECLARATION PROVE TO BE FALSE.**

…….. ……..
Signature Date

……..... …….
Position Name of Bidder

PREFERENCE POINTS CLAIM FORM IN TERMS OF THE PREFERENTIAL PROCUREMENT REGULATIONS 2022

This preference form must form part of all tenders invited. It contains general information and serves as a claim form for preference points for specific goals.

NB: BEFORE COMPLETING THIS FORM, TENDERERS MUST STUDY THE GENERAL CONDITIONS, DEFINITIONS AND DIRECTIVES APPLICABLE IN RESPECT OF THE TENDER AND PREFERENTIAL PROCUREMENT REGULATIONS, 2022

---

1. GENERAL CONDITIONS

1.1 The following preference point systems are applicable to invitations to tender:

- **the 80/20 system for requirements with a Rand value of up to R50 000 000 (all applicable taxes included);** and
- the 90/10 system for requirements with a Rand value above R50 000 000 (all applicable taxes included).

1.2 **To be completed by the organ of state**

a) The applicable preference point system for this tender is the 80/20 preference point system.

1.3 Points for this tender (even in the case of a tender for income-generating contracts) shall be awarded for:

(a) Price; and

(b) Specific Goals.

1.4 **To be completed by the organ of state:**

The maximum points for this tender are allocated as follows:

	POINTS
PRICE	80
SPECIFIC GOALS	20
TOTAL POINTS FOR PRICE AND SPECIFIC GOALS	**100**

1.5 Failure on the part of a tenderer to submit proof or documentation required in terms of this tender to claim points for specific goals with the tender, will be interpreted to mean that preference points for specific goals are not claimed.

1.6 The organ of state reserves the right to require of a tenderer, either before a tender is adjudicated or at any time subsequently, to substantiate any claim in regard to preferences, in any manner required by the organ of state.

2. DEFINITIONS

(a) **"tender"** means a written offer in the form determined by an organ of state in response to an invitation to provide goods or services through price quotations, competitive tendering process or any other method envisaged in legislation;

(b) **"price"** means an amount of money tendered for goods or services, and includes all applicable taxes less all unconditional discounts;

(c) **"rand value"** means the total estimated value of a contract in Rand, calculated at the time of bid invitation, and includes all applicable taxes;

(d) **"tender for income-generating contracts"** means a written offer in the form determined by an organ of state in response to an invitation for the origination of income-generating contracts through any method envisaged in legislation that will result in a legal agreement between the organ of state and a third party that produces revenue for the organ of state, and includes, but is not limited to, leasing and disposal of assets and concession contracts, excluding direct sales and disposal of assets through public auctions; and

(e) **"the Act"** means the Preferential Procurement Policy Framework Act, 2000 (Act No. 5 of 2000).

3. FORMULAE FOR PROCUREMENT OF GOODS AND SERVICES

3.1. POINTS AWARDED FOR PRICE

3.1.1 THE 80/20 OR 90/10 PREFERENCE POINT SYSTEMS

A maximum of 80 or 90 points is allocated for price on the following basis:

80/20 **or** **90/10**

$$Ps = 80\left(1 - \frac{Pt - P\,min}{P\,min}\right) \text{ or } \quad Ps = 90\left(1 - \frac{Pt - P\,min}{P\,min}\right)$$

Where

Ps = Points scored for price of tender under consideration

Pt = Price of tender under consideration

Pmin = Price of lowest acceptable tender

3.2. FORMULAE FOR DISPOSAL OR LEASING OF STATE ASSETS AND INCOME GENERATING PROCUREMENT

3.2.1. POINTS AWARDED FOR PRICE

A maximum of 80 or 90 points is allocated for price on the following basis:

80/20 **or** **90/10**

$$Ps = 80\left(1 + \frac{Pt - P\,max}{P\,max}\right) \text{ or } \quad Ps = 90\left(1 + \frac{Pt - P\,max}{Pmax}\right)$$

Where

Ps	=	Points scored for price of tender under consideration
Pt	=	Price of tender under consideration
Pmax	=	Price of highest acceptable tender

4. POINTS AWARDED FOR SPECIFIC GOALS

4.1. In terms of Regulation 4(2); 5(2); 6(2) and 7(2) of the Preferential Procurement Regulations, preference points must be awarded for specific goals stated in the tender. For the purposes of this tender the tenderer will be allocated points based on the goals stated in table 1 below as may be supported by proof/ documentation stated in the conditions of this tender:

4.2. In cases where organs of state intend to use Regulation 3(2) of the Regulations, which states that, if it is unclear whether the 80/20 or 90/10 preference point system applies, an organ of state must, in the tender documents, stipulate in the case of—

(a) an invitation for tender for income-generating contracts, that either the 80/20 or 90/10 preference point system will apply and that the highest acceptable tender will be used to determine the applicable preference point system; or

(b) any other invitation for tender, that either the 80/20 or 90/10 preference point system will apply and that the lowest acceptable tender will be used to determine the applicable preference point system,

then the organ of state must indicate the points allocated for specific goals for both the 90/10 and 80/20 preference point system.

Table 1: Specific goals for the tender and points claimed are indicated per the table below.

(Note to organs of state: Where either the 90/10 or 80/20 preference point system is applicable, corresponding points must also be indicated as such.

***Note to tenderers: The tenderer must indicate how they claim points for each preference point system.*)**

N.B For points to be allocated as per above the tenderers will be required to submit proof of documentation as evidence for claims made. Any tenderer that does not submit evidence as stated in the bid document to claim applicable points will be allocated zero points.

DECLARATION WITH REGARD TO COMPANY/FIRM

Specific goals	80/20 preference point system	Points allocations
BB-BEE score of companies • Level 1 • Level 2 • Level 3 • Level 4 • Level 5 • Level 6 • Level 7 • Level 8 • Non-compliant	• 8 Points • 7 Points • 6 Points • 5 Points • 4 Points • 3 Points • 2 Points • 1 Point • 0 Points	
EME and/ or QSE	2 Points	
At least 51% of Women-owned companies	2 Points	
At least 51% owned companies by People with disability	2 Points	
At least 51% owned companies by Youth	2 Point	
Local Economic Participation • City of Tshwane • Gauteng • National	4 Points 2 Points 1 Point	

4.3. Name of company/firm…….

4.4. Company registration number:

……...

4.5. TYPE OF COMPANY/ FIRM

- Partnership/Joint Venture / Consortium
- One-person business/sole propriety
- Close corporation
- Public Company
- Personal Liability Company
- (Pty) Limited
- Non-Profit Company
- State Owned Company

[TICK APPLICABLE BOX]

4.6. I, the undersigned, who is duly authorised to do so on behalf of the company/firm, certify that the points claimed, based on the specific goals as advised in the tender, qualifies the company/ firm for the preference(s) shown and I acknowledge that:

i) The information furnished is true and correct;

ii) The preference points claimed are in accordance with the General Conditions as indicated in paragraph 1 of this form;

iii) In the event of a contract being awarded as a result of points claimed as shown in paragraphs 1.4 and 4.2, the contractor may be required to furnish documentary proof to the satisfaction of the organ of state that the claims are correct;

iv) If the specific goals have been claimed or obtained on a fraudulent basis or any of the conditions of contract have not been fulfilled, the organ of state may, in addition to any other remedy it may have –

(a) disqualify the person from the tendering process;

(b) recover costs, losses or damages it has incurred or suffered as a result of that person's conduct;

(c) cancel the contract and claim any damages which it has suffered as a result of having to make less favourable arrangements due to such cancellation;

(d) recommend that the tenderer or contractor, its shareholders and directors, or only the shareholders and directors who acted on a fraudulent basis, be restricted from obtaining business from any organ of state for a period not exceeding 10 years, after the *audi alteram partem* (hear the other side) rule has been applied; and

(e) forward the matter for criminal prosecution, if deemed necessary.

.....

SIGNATURE(S) OF TENDERER(S)

SURNAME AND NAME: .....

DATE: .....

ADDRESS: .....

.....

.....

CONTRACT FORM: RENDERING OF SERVICES

THIS FORM MUST BE FILLED IN DUPLICATE BY BOTH THE SERVICE PROVIDER (PART 1) AND THE PURCHASER (PART 2). BOTH FORMS MUST BE SIGNED IN THE ORIGINAL SO THAT THE SERVICE PROVIDER AND THE PURCHASER WOULD BE IN POSSESSION OF ORIGINALLY SIGNED CONTRACTS FOR THEIR RESPECTIVE RECORDS.

PART 1 (TO BE FILLED IN BY THE SERVICE PROVIDER)

1. I hereby undertake to render services described in the attached bidding documents to (name of the institution City of Tshwane in accordance with the requirements and task directives / proposals specifications stipulated in Bid Number **GICT 03 2025/26** at the price/s quoted. My offer/s remain binding upon me and open for acceptance by the Purchaser during the validity period indicated and calculated from the closing date of the bid.

2. The following documents shall be deemed to form and be read and construed as part of this agreement:

    - Invitation to bid;
    - Tax clearance certificate;
    - Pricing schedule(s);
    - Filled in task directive/proposal;
    - Preference claims for specific goals in terms of the Preferential Procurement Regulations 2022;
    - Declaration of interest;
    - Declaration of Bidder's past SCM practices;
    - Certificate of Independent Bid Determination;
    - Special Conditions of Contract;

    (ii) General Conditions of Contract; and

    (iii) Other (specify)

3. I confirm that I have satisfied myself as to the correctness and validity of my bid; that the price(s) and rate(s) quoted cover all the services specified in the bidding documents; that the price(s) and rate(s) cover all my obligations and I accept that any mistakes regarding price(s) and rate(s) and calculations will be at my own risk.

4. I accept full responsibility for the proper execution and fulfilment of all obligations and conditions devolving on me under this agreement as the principal liable for the due fulfillment of this contract.

5. I declare that I have no participation in any collusive practices with any bidder or any other person regarding this or any other bid.

6. I confirm that I am duly authorised to sign this contract.

NAME (PRINT) …….

CAPACITY …….

SIGNATURE …….

NAME OF FIRM …….

DATE …….

WITNESSES

1 ……..……

2 ……..……

DATE: ……..

MBD 7.2

CONTRACT FORM: RENDERING OF SERVICES

PART 2 (TO BE FILLED IN BY THE PURCHASER)

1. I……. in my capacity as ……..……... accept your bid under reference number …… dated…… for the rendering of services indicated hereunder and/or further specified in the annexure(s).

2. An official order indicating service delivery instructions is forthcoming.

3. I undertake to make payment for the services rendered in accordance with the terms and conditions of the contract, within 30 (thirty) days after receipt of an invoice.

DESCRIPTION OF SERVICE	PRICE (ALL APPLICABLE TAXES INCLUDED)	COMPLETION DATE	B-BBEE STATUS LEVEL OF CONTRIBUTION

4. I confirm that I am duly authorised to sign this contract.

SIGNED AT …… ON ……

NAME (PRINT) ……..

SIGNATURE ……..

OFFICIAL STAMP

WITNESSES

1 ……
2 ……

DATE: ……..

MBD 8

DECLARATION OF BIDDER'S PAST SUPPLY CHAIN MANAGEMENT PRACTICES

1 This Municipal Bidding Document must form part of all bids invited.

2 It serves as a declaration to be used by municipalities and municipal entities in ensuring that when goods and services are being procured, all reasonable steps are taken to combat the abuse of the supply chain management system.

3 The bid of any bidder may be rejected if that bidder, or any of its directors have:

a. abused the municipality's / municipal entity's supply chain management system or committed any improper conduct in relation to such system;

b. been convicted for fraud or corruption during the past five years;

c. willfully neglected, reneged on or failed to comply with any government, municipal or other public sector contract during the past five years; or

d. been listed in the Register for Tender Defaulters in terms of section 29 of the Prevention and Combating of Corrupt Activities Act (No 12 of 2004).

4 In order to give effect to the above, the following questionnaire must be completed and submitted with the bid.

Item	Question	Yes	No
4.1	Is the bidder or any of its directors listed on the National Treasury's Database of Restricted Suppliers as companies or persons prohibited from doing business with the public sector? (Companies or persons who are listed on this Database were informed in writing of this restriction by the Accounting Officer/Authority of the institution that imposed the restriction after the *audi alteram partem* rule was applied). **The Database of Restricted Suppliers now resides on the National Treasury's website(www.treasury.gov.za) and can be accessed by clicking on its link at the bottom of the home page.**	Yes ☐	No ☐
4.1.1	If so, furnish particulars:		
4.2	Is the bidder or any of its directors listed on the Register for Tender Defaulters in terms of section 29 of the Prevention and Combating of Corrupt Activities Act (No 12 of 2004)?	Yes ☐	No ☐

	The Register for Tender Defaulters can be accessed on the National Treasury's website (www.treasury.gov.za) by clicking on its link at the bottom of the home page.		
4.2.1	If so, furnish particulars:		
4.3	Was the bidder or any of its directors convicted by a court of law (including a court of law outside the Republic of South Africa) for fraud or corruption during the past five years?	Yes ☐	No ☐
4.3.1	If so, furnish particulars:		
4.4	Does the bidder or any of its directors owe any municipal rates and taxes or municipal charges to the municipality / municipal entity, or to any other municipality / municipal entity, that is in arrears for more than three months?	Yes ☐	No ☐
4.4.1	If so, furnish particulars:		
4.5	Was any contract between the bidder and the municipality / municipal entity or any other organ of state terminated during the past five years on account of failure to perform on or comply with the contract?	Yes ☐	No ☐
4.7.1	If so, furnish particulars:		

CERTIFICATION

I, THE UNDERSIGNED (FULL NAME) ……..……..…… CERTIFY THAT THE INFORMATION FURNISHED ON THIS DECLARATION FORM TRUE AND CORRECT.

I ACCEPT THAT, IN ADDITION TO CANCELLATION OF A CONTRACT, ACTION MAY BE TAKEN AGAINST ME SHOULD THIS DECLARATION PROVE TO BE FALSE.

……... ……..
Signature Date

MBD 9

CERTIFICATE OF INDEPENDENT BID DETERMINATION

1 This Municipal Bidding Document (MBD) must form part of all bids[1] invited.

2 Section 4 (1) (b) (iii) of the Competition Act No. 89 of 1998, as amended, prohibits an agreement between, or concerted practice by, firms, or a decision by an association of firms, if it is between parties in a horizontal relationship and if it involves collusive bidding (or bid rigging).[2] Collusive bidding is a *pe se* prohibition meaning that it cannot be justified under any grounds.

3 Municipal Supply Regulation 38 (1) prescribes that a supply chain management policy must provide measures for the combating of abuse of the supply chain management system, and must enable the accounting officer, among others, to:

a. take all reasonable steps to prevent such abuse;

b. reject the bid of any bidder if that bidder or any of its directors has abused the supply chain management system of the municipality or municipal entity or has committed any improper conduct in relation to such system; and

c. cancel a contract awarded to a person if the person committed any corrupt or fraudulent act during the bidding process or the execution of the contract.

4 This MBD serves as a certificate of declaration that would be used by institutions to ensure that, when bids are considered, reasonable steps are taken to prevent any form of bid-rigging.

5 In order to give effect to the above, the attached Certificate of Bid Determination (MBD 9) must be completed and submitted with the bid:

[1] Includes price quotations, advertised competitive bids, limited bids and proposals.

[2] Bid rigging (or collusive bidding) occurs when businesses, that would otherwise be expected to compete, secretly conspire to raise prices or lower the quality of goods and / or services for purchasers who wish to acquire goods and / or services through a bidding process. Bid rigging is, therefore, an agreement between competitors not to compete.

MBD 9

CERTIFICATE OF INDEPENDENT BID DETERMINATION

I, the undersigned, in submitting the accompanying bid: **GICT 03 2025/26**

TENDER TO PROVIDE, OPERATE AND MAINTAIN THE ICT CORPORATE NETWORK EQUIPMENT, EXISTING HOSTED VOICE AND DATA SOLUTION DEPLOYED, AND THE EXPANSION OF THE EXISTING CORPORATE NETWORK AS AND WHEN FOR A PERIOD OF THREE (3) YEARS

in response to the invitation for the bid made by:

CITY OF TSHWANE MUNICIPALITY

do hereby make the following statements that I certify to be true and complete in every respect:

I certify, on behalf of: _____that:
(Name of Bidder)

1. I have read and I understand the contents of this Certificate;

2. I understand that the accompanying bid will be disqualified if this Certificate is found not to be true and complete in every respect;

3. I am authorized by the bidder to sign this Certificate, and to submit the accompanying bid, on behalf of the bidder;

4. Each person whose signature appears on the accompanying bid has been authorized by the bidder to determine the terms of, and to sign, the bid, on behalf of the bidder;

5. For the purposes of this Certificate and the accompanying bid, I understand that the word “competitor” shall include any individual or organization, other than the bidder, whether or not affiliated with the bidder, who:

   (a) has been requested to submit a bid in response to this bid invitation;

   (b) could potentially submit a bid in response to this bid invitation, based on their qualifications, abilities or experience; and

   (c) provides the same goods and services as the bidder and/or is in the same line of business as the bidder

6. The bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with any competitor. However communication between partners in a joint venture or consortium[3] will not be construed as collusive bidding.

[3] Joint venture or consortium means an association of persons for the purpose of combining their expertise, property, capital, efforts, skill and knowledge in an activity for the execution of a contract.

7. In particular, without limiting the generality of paragraphs 6 above, there has been no consultation, communication, agreement or arrangement with any competitor regarding:

   (a) prices;

   (b) geographical area where product or service will be rendered (market allocation)

   (c) methods, factors or formulas used to calculate prices;

   (d) the intention or decision to submit or not to submit, a bid;

   (e) the submission of a bid which does not meet the specifications and conditions of the bid; or

   (f) bidding with the intention not to win the bid.

8. In addition, there have been no consultations, communications, agreements or arrangements with any competitor regarding the quality, quantity, specifications and conditions or delivery particulars of the products or services to which this bid invitation relates.

9. The terms of the accompanying bid have not been, and will not be, disclosed by the bidder, directly or indirectly, to any competitor, prior to the date and time of the official bid opening or of the awarding of the contract.

10. I am aware that, in addition and without prejudice to any other remedy provided to combat any restrictive practices related to bids and contracts, bids that are suspicious will be reported to the Competition Commission for investigation and possible imposition of administrative penalties in terms of section 59 of the Competition Act No 89 of 1998 and or may be reported to the National Prosecuting Authority (NPA) for criminal investigation and or may be restricted from conducting business with the public sector for a period not exceeding ten (10) years in terms of the Prevention and Combating of Corrupt Activities Act No 12 of 2004 or any other applicable legislation.

……	…….....
Signature	Date
……	…….....
Position	Name of Bidder

THE NATIONAL TREASURY

Republic of South Africa

GOVERNMENT PROCUREMENT

GENERAL CONDITIONS OF CONTRACT

July 2010

GENERAL CONDITIONS OF CONTRACT

July 2010

NOTES

The purpose of this document is to:

(i) Draw special attention to certain general conditions applicable to government bids, contracts and orders; and

(ii) To ensure that clients be familiar with regard to the rights and obligations of all parties involved in doing business with government.

In this document words in the singular also mean in the plural and vice versa and words in the masculine also mean in the feminine and neuter.

- The General Conditions of Contract will form part of all bid documents and may not be amended.
- Special Conditions of Contract (SCC) relevant to a specific bid, should be compiled separately for every bid (if (applicable) and will supplement the General Conditions of Contract. Whenever there is a conflict, the provisions in the SCC shall prevail.

TABLE OF CLAUSES

General Conditions of Contract

1. Definitions

1. The following terms shall be interpreted as indicated:

1.1 “Closing time” means the date and hour specified in the bidding documents for the receipt of bids.

1.2 “Contract” means the written agreement entered into between the purchaser and the supplier, as recorded in the contract form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

1.3 “Contract price” means the price payable to the supplier under the contract for the full and proper performance of his contractual obligations.

1.4 “Corrupt practice” means the offering, giving, receiving, or soliciting of anything of value to influence the action of a public official in the procurement process or in contract execution.

1.5 "Countervailing duties" are imposed in cases where an enterprise abroad is subsidized by its government and encouraged to market its products internationally.

1.6 “Country of origin” means the place where the goods were mined, grown or produced or from which the services are supplied. Goods are produced when, through manufacturing, processing or substantial and major assembly of components, a commercially recognized new product results that is substantially different in basic characteristics or in purpose or utility from its components.

1.7 “Day” means calendar day.

1.8 “Delivery” means delivery in compliance of the conditions of the contract or order.

1.9 “Delivery ex stock” means immediate delivery directly from stock actually on hand.

1.10 “Delivery into consignees store or to his site” means delivered and unloaded in the specified store or depot or on the specified site in compliance with the conditions of the contract or order, the supplier bearing all risks and charges involved until the supplies are so delivered and a valid receipt is obtained.

1.11 "Dumping" occurs when a private enterprise abroad market its goods on own initiative in the RSA at lower prices than that of the country of origin and which have the potential to harm the local industries in the RSA.

1.12 ”Force majeure” means an event beyond the control of the supplier and not involving the supplier’s fault or negligence and not foreseeable. Such events may include, but is not restricted to, acts of the purchaser in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.

1.13 “Fraudulent practice” means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of any bidder, and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the bidder of the benefits of free and open competition.

1.14 "GCC" means the General Conditions of Contract.

1.15 "Goods" means all of the equipment, machinery, and/or other materials that the supplier is required to supply to the purchaser under the contract.

1.16 "Imported content" means that portion of the bidding price represented by the cost of components, parts or materials which have been or are still to be imported (whether by the supplier or his subcontractors) and which costs are inclusive of the costs abroad, plus freight and other direct importation costs such as landing costs, dock dues, import duty, sales duty or other similar tax or duty at the South African place of entry as well as transportation and handling charges to the factory in the Republic where the supplies covered by the bid will be manufactured.

1.17 "Local content" means that portion of the bidding price which is not included in the imported content provided that local manufacture does take place.

1.18 "Manufacture" means the production of products in a factory using labour, materials, components and machinery and includes other related value-adding activities.

1.19 "Order" means an official written order issued for the supply of goods or works or the rendering of a service.

1.20 "Project site," where applicable, means the place indicated in bidding documents.

1.21 "Purchaser" means the organization purchasing the goods.

1.22 "Republic" means the Republic of South Africa.

1.23 "SCC" means the Special Conditions of Contract.

1.24 "Services" means those functional services ancillary to the supply of the goods, such as transportation and any other incidental services, such as installation, commissioning, provision of technical assistance, training, catering, gardening, security, maintenance and other such obligations of the supplier covered under the contract.

1.25 "Written" or "in writing" means handwritten in ink or any form of electronic or mechanical writing.

1. Application

2.1 These general conditions are applicable to all bids, contracts and orders including bids for functional and professional services, sales, hiring, letting and the granting or acquiring of rights, but excluding immovable property, unless otherwise indicated in the bidding documents.

2.2 Where applicable, special conditions of contract are also laid down to cover specific supplies, services or works.

2.3 Where such special conditions of contract are in conflict with these general conditions, the special conditions shall apply.

3. General

3.1 Unless otherwise indicated in the bidding documents, the purchaser shall not be liable for any expense incurred in the preparation and submission of a bid.

Where applicable a non-refundable fee for documents may be charged.

	3.2	With certain exceptions, invitations to bid are only published in the Government Tender Bulletin. The Government Tender Bulletin may be obtained directly from the Government Printer, Private Bag X85, Pretoria 0001, or accessed electronically from www.treasury.gov.za
4. Standards	4.1	The goods supplied shall conform to the standards mentioned in the bidding documents and specifications.
5. Use of contract documents and information inspection.	5.1	The supplier shall not, without the purchaser's prior written consent, disclose the contract, or any provision thereof, or any specification, plan, drawing, pattern, sample, or information furnished by or on behalf of the purchaser in connection therewith, to any person other than a person employed by the supplier in the performance of the contract. Disclosure to any such employed person shall be made in confidence and shall extend only so far as may be necessary for purposes of such performance.
	5.2	The supplier shall not, without the purchaser's prior written consent, make use of any document or information mentioned in GCC clause 5.1 except for purposes of performing the contract.
	5.3	Any document, other than the contract itself mentioned in GCC clause 5.1 shall remain the property of the purchaser and shall be returned (all copies) to the purchaser on completion of the supplier's performance under the contract if so required by the purchaser.
	5.4	The supplier shall permit the purchaser to inspect the supplier's records relating to the performance of the supplier and to have them audited by auditors appointed by the purchaser, if so required by the purchaser.
6. Patent rights	6.1	The supplier shall indemnify the purchaser against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the goods or any part thereof by the purchaser.
7. Performance security	7.1	Within thirty (30) days of receipt of the notification of contract award, the successful bidder shall furnish to the purchaser the performance security of the amount specified in SCC.
	7.2	The proceeds of the performance security shall be payable to the purchaser as compensation for any loss resulting from the supplier's failure to complete his obligations under the contract.
	7.3	The performance security shall be denominated in the currency of the contract, or in a freely convertible currency acceptable to the purchaser and shall be in one of the following forms: (a) a bank guarantee or an irrevocable letter of credit issued by a reputable bank located in the purchaser's country or abroad, acceptable to the purchaser, in the form provided in the bidding documents or another form acceptable to the purchaser; or (b) a cashier's or certified cheque
	7.4	The performance security will be discharged by the purchaser and returned to the supplier not later than thirty (30) days following the date of completion of the supplier's performance obligations under the contract, including any warranty obligations, unless otherwise specified in SCC.
8. Inspections, tests and analyses	8.1	All pre-bidding testing will be for the account of the bidder.

8.2 If it is a bid condition that supplies to be produced or services to be rendered should at any stage during production or execution or on completion be subject to inspection, the premises of the bidder or contractor shall be open, at all reasonable hours, for inspection by a representative of the Department or an organization acting on behalf of the Department.

8.3 If there are no inspection requirements indicated in the bidding documents and no mention is made in the contract, but during the contract period it is decided that inspections shall be carried out, the purchaser shall itself make the necessary arrangements, including payment arrangements with the testing authority concerned.

8.4 If the inspections, tests and analyses referred to in clauses 8.2 and 8.3 show the supplies to be in accordance with the contract requirements, the cost of the inspections, tests and analyses shall be defrayed by the purchaser.

8.5 Where the supplies or services referred to in clauses 8.2 and 8.3 do not comply with the contract requirements, irrespective of whether such supplies or services are accepted or not, the cost in connection with these inspections, tests or analyses shall be defrayed by the supplier.

8.6 Supplies and services which are referred to in clauses 8.2 and 8.3 and which do not comply with the contract requirements may be rejected.

8.7 Any contract supplies may on or after delivery be inspected, tested or analyzed and may be rejected if found not to comply with the requirements of the contract. Such rejected supplies shall be held at the cost and risk of the supplier who shall, when called upon, remove them immediately at his own cost and forthwith substitute them with supplies which do comply with the requirements of the contract. Failing such removal the rejected supplies shall be returned at the suppliers cost and risk. Should the supplier fail to provide the substitute supplies forthwith, the purchaser may, without giving the supplier further opportunity to substitute the rejected supplies, purchase such supplies as may be necessary at the expense of the supplier.

8.8 The provisions of clauses 8.4 to 8.7 shall not prejudice the right of the purchaser to cancel the contract on account of a breach of the conditions thereof, or to act in terms of Clause 23 of GCC.

9. Packing

9.1 The supplier shall provide such packing of the goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in the contract. The packing shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packing, case size and weights shall take into consideration, where appropriate, the remoteness of the goods' final destination and the absence of heavy handling facilities at all points in transit.

9.2 The packing, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the contract, including additional requirements, if any, specified in SCC, and in any subsequent instructions ordered by the purchaser.

10. Delivery and documents

10.1 Delivery of the goods shall be made by the supplier in accordance with the terms specified in the contract. The details of shipping and/or other documents to be furnished by the supplier are specified in SCC.

10.2 Documents to be submitted by the supplier are specified in SCC.

11. Insurance

11.1 The goods supplied under the contract shall be fully insured in a freely convertible currency against loss or damage incidental to manufacture or acquisition, transportation, storage and delivery in the manner specified in the SCC.

12. Transportation

12.1 Should a price other than an all-inclusive delivered price be required, this shall be specified in the SCC.

13. Incidental services, services

13.1 The supplier may be required to provide any or all of the following services, including additional services, if any, specified in SCC:

(a) performance or supervision of on-site assembly and/or commissioning of the supplied goods;

(b) furnishing of tools required for assembly and/or maintenance of the supplied goods;

(c) furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied goods;

(d) performance or supervision or maintenance and/or repair of the supplied goods, for a period of time agreed by the parties, provided that this service shall not relieve the supplier of any warranty obligations under this contract; and

(e) training of the purchaser's personnel, at the supplier's plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the supplied goods.

13.2 Prices charged by the supplier for incidental services, if not included in the contract price for the goods, shall be agreed upon in advance by the parties and shall not exceed the prevailing rates charged to other parties by the supplier for similar services.

14. Spare parts

14.1 As specified in SCC, the supplier may be required to provide any or all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the supplier:

(a) such spare parts as the purchaser may elect to purchase from the supplier, provided that this election shall not relieve the supplier of any warranty obligations under the contract; and

(b) in the event of termination of production of the spare parts:

(i) Advance notification to the purchaser of the pending termination, in sufficient time to permit the purchaser to procure needed requirements; and

(ii) following such termination, furnishing at no cost to the purchaser, the blueprints, drawings, and specifications of the spare parts, if requested.

15. Warranty

15.1 The supplier warrants that the goods supplied under the contract are new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials unless provided otherwise in the contract. The supplier further warrants that all goods supplied under this contract shall have no defect, arising from design, materials, or workmanship (except when the design and/or material is required by the purchaser's specifications) or from any act or omission of the supplier, that may develop under normal use of the supplied goods in the conditions prevailing in the country of final destination.

15.2 This warranty shall remain valid for twelve (12) months after the goods, or any portion thereof as the case may be, have been delivered to and accepted at the

final destination indicated in the contract, or for eighteen (18) months after the date of shipment from the port or place of loading in the source country, whichever period concludes earlier, unless specified otherwise in SCC.

15.3 The purchaser shall promptly notify the supplier in writing of any claims arising under this warranty.

15.4 Upon receipt of such notice, the supplier shall, within the period specified in SCC and with all reasonable speed, repair or replace the defective goods or parts thereof, without costs to the purchaser.

15.5 If the supplier, having been notified, fails to remedy the defect(s) within the period specified in SCC, the purchaser may proceed to take such remedial action as may be necessary, at the supplier's risk and expense and without prejudice to any other rights which the purchaser may have against the supplier under the contract.

16. Payment

16.1 The method and conditions of payment to be made to the supplier under this contract shall be specified in SCC.

16.2 The supplier shall furnish the purchaser with an invoice accompanied by a copy of the delivery note and upon fulfillment of other obligations stipulated in the contract.

16.3 Payments shall be made promptly by the purchaser, but in no case later than thirty (30) days after submission of an invoice or claim by the supplier.

16.4 Payment will be made in Rand unless otherwise stipulated in SCC.

17. Prices

17.1 Prices charged by the supplier for goods delivered and services performed under the contract shall not vary from the prices quoted by the supplier in his bid, with the exception of any price adjustments authorized in SCC or in the purchaser's request for bid validity extension, as the case may be.

18. Contract amendments

18.1 No variation in or modification of the terms of the contract shall be made except by written amendment signed by the parties concerned.

19. Assignment

19.1 The supplier shall not assign, in whole or in part, its obligations to perform under the contract, except with the purchaser's prior written consent.

20. Subcontracts

20.1 The supplier shall notify the purchaser in writing of all subcontracts awarded under this contracts if not already specified in the bid. Such notification, in the original bid or later, shall not relieve the supplier from any liability or obligation under the contract.

21. Delays in the supplier's performance

21.1 Delivery of the goods and performance of services shall be made by the supplier in accordance with the time schedule prescribed by the purchaser in the contract.

21.2 If at any time during performance of the contract, the supplier or its subcontractor(s) should encounter conditions impeding timely delivery of the goods and performance of services, the supplier shall promptly notify the purchaser in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the supplier's notice, the purchaser shall evaluate the situation and may at his discretion extend the supplier's time for performance, with or without the imposition of penalties, in which case the extension shall be ratified by the parties by amendment of contract.

21.3 No provision in a contract shall be deemed to prohibit the obtaining of supplies or services from a national department, provincial department, or a local authority.

21.4 The right is reserved to procure outside of the contract small quantities or to have minor essential services executed if an emergency arises, the supplier's point of supply is not situated at or near the place where the supplies are required, or the supplier's services are not readily available.

21.5 Except as provided under GCC Clause 25, a delay by the supplier in the performance of its delivery obligations shall render the supplier liable to the imposition of penalties, pursuant to GCC Clause 22, unless an extension of time is agreed upon pursuant to GCC Clause 21.2 without the application of penalties.

21.6 Upon any delay beyond the delivery period in the case of a supplies contract, the purchaser shall, without canceling the contract, be entitled to purchase supplies of a similar quality and up to the same quantity in substitution of the goods not supplied in conformity with the contract and to return any goods delivered later at the supplier's expense and risk, or to cancel the contract and buy such goods as may be required to complete the contract and without prejudice to his other rights, be entitled to claim damages from the supplier.

22. Penalties

22.1 Subject to GCC Clause 25, if the supplier fails to deliver any or all of the goods or to perform the services within the period(s) specified in the contract, the purchaser shall, without prejudice to its other remedies under the contract, deduct from the contract price, as a penalty, a sum calculated on the delivered price of the delayed goods or unperformed services using the current prime interest rate calculated for each day of the delay until actual delivery or performance. The purchaser may also consider termination of the contract pursuant to GCC Clause 23.

23. Termination for default

23.1 The purchaser, without prejudice to any other remedy for breach of contract, by written notice of default sent to the supplier, may terminate this contract in whole or in part:

(a) if the supplier fails to deliver any or all of the goods within the period(s) specified in the contract, or within any extension thereof granted by the purchaser pursuant to GCC Clause 21.2;

(b) if the Supplier fails to perform any other obligation(s) under the contract; or

(c) if the supplier, in the judgment of the purchaser, has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

23.2 In the event the purchaser terminates the contract in whole or in part, the purchaser may procure, upon such terms and in such manner as it deems appropriate, goods, works or services similar to those undelivered, and the supplier shall be liable to the purchaser for any excess costs for such similar goods, works or services. However, the supplier shall continue performance of the contract to the extent not terminated.

23.3 Where the purchaser terminates the contract in whole or in part, the purchaser may decide to impose a restriction penalty on the supplier by prohibiting such supplier from doing business with the public sector for a period not exceeding 10 years.

23.4 If a purchaser intends imposing a restriction on a supplier or any person associated with the supplier, the supplier will be allowed a time period of not more than fourteen (14) days to provide reasons why the envisaged restriction should not be imposed. Should the supplier fail to respond within the stipulated

fourteen (14) days the purchaser may regard the intended penalty as not objected against and may impose it on the supplier.

23.5 Any restriction imposed on any person by the Accounting Officer / Authority will, at the discretion of the Accounting Officer / Authority, also be applicable to any other enterprise or any partner, manager, director or other person who wholly or partly exercises or exercised or may exercise control over the enterprise of the first-mentioned person, and with which enterprise or person the first-mentioned person, is or was in the opinion of the Accounting Officer / Authority actively associated.

23.6 If a restriction is imposed, the purchaser must, within five (5) working days of such imposition, furnish the National Treasury, with the following information:

(i) the name and address of the supplier and / or person restricted by the purchaser;

(ii) the date of commencement of the restriction

(iii) the period of restriction; and

(iv) the reasons for the restriction.

These details will be loaded in the National Treasury's central database of suppliers or persons prohibited from doing business with the public sector.

23.7 If a court of law convicts a person of an offence as contemplated in sections 12 or 13 of the Prevention and Combating of Corrupt Activities Act, No. 12 of 2004, the court may also rule that such person's name be endorsed on the Register for Tender Defaulters. When a person's name has been endorsed on the Register, the person will be prohibited from doing business with the public sector for a period not less than five years and not more than 10 years. The National Treasury is empowered to determine the period of restriction and each case will be dealt with on its own merits. According to section 32 of the Act the Register must be open to the public. The Register can be perused on the National Treasury website.

24. Anti-dumping and countervailing duties and rights

24.1 When, after the date of bid, provisional payments are required, or antidumping or countervailing duties are imposed, or the amount of a provisional payment or anti-dumping or countervailing right is increased in respect of any dumped or subsidized import, the State is not liable for any amount so required or imposed, or for the amount of any such increase. When, after the said date, such a provisional payment is no longer required or any such anti-dumping or countervailing right is abolished, or where the amount of such provisional payment or any such right is reduced, any such favourable difference shall on demand be paid forthwith by the contractor to the State or the State may deduct such amounts from moneys (if any) which may otherwise be due to the contractor in regard to supplies or services which he delivered or rendered, or is to deliver or render in terms of the contract or any other contract or any other amount which may be due to him

25. Force Majeure

25.1 Notwithstanding the provisions of GCC Clauses 22 and 23, the supplier shall not be liable for forfeiture of its performance security, damages, or termination for default if and to the extent that his delay in performance or other failure to perform his obligations under the contract is the result of an event of force majeure.

25.2 If a force majeure situation arises, the supplier shall promptly notify the purchaser in writing of such condition and the cause thereof. Unless otherwise directed by the purchaser in writing, the supplier shall continue to perform its obligations under the contract as far as is reasonably practical, and shall seek all

reasonable alternative means for performance not prevented by the force majeure event.

26. Termination for insolvency

26.1 The purchaser may at any time terminate the contract by giving written notice to the supplier if the supplier becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the supplier, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the purchaser.

27. Settlement of Disputes

27.1 If any dispute or difference of any kind whatsoever arises between the purchaser and the supplier in connection with or arising out of the contract, the parties shall make every effort to resolve amicably such dispute or difference by mutual consultation.

27.2 If, after thirty (30) days, the parties have failed to resolve their dispute or difference by such mutual consultation, then either the purchaser or the supplier may give notice to the other party of his intention to commence with mediation. No mediation in respect of this matter may be commenced unless such notice is given to the other party.

27.3 Should it not be possible to settle a dispute by means of mediation, it may be settled in a South African court of law.

27.4 Mediation proceedings shall be conducted in accordance with the rules of procedure specified in the SCC.

27.5 Notwithstanding any reference to mediation and/or court proceedings herein,

(a) the parties shall continue to perform their respective obligations under the contract unless they otherwise agree; and

(b) the purchaser shall pay the supplier any monies due the supplier.

28. Limitation of liability

28.1 Except in cases of criminal negligence or willful misconduct, and in the case of infringement pursuant to Clause 6;

the supplier shall not be liable to the purchaser, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the supplier to pay penalties and/or damages to the purchaser; and

the aggregate liability of the supplier to the purchaser, whether under the contract, in tort or otherwise, shall not exceed the total contract price, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.

29. Governing language

29.1 The contract shall be written in English. All correspondence and other documents pertaining to the contract that is exchanged by the parties shall also be written in English.

30. Applicable law

30.1 The contract shall be interpreted in accordance with South African laws, unless otherwise specified in SCC.

31. Notices

31.1 Every written acceptance of a bid shall be posted to the supplier concerned by registered or certified mail and any other notice to him shall be posted by ordinary mail to the address furnished in his bid or to the address notified later by him in writing and such posting shall be deemed to be proper service of such notice

31.2 The time mentioned in the contract documents for performing any act after such aforesaid notice has been given, shall be reckoned from the date of posting of such notice.

32. Taxes and duties

32.1 A foreign supplier shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed outside the purchaser's country.

32.2 A local supplier shall be entirely responsible for all taxes, duties, license fees, etc., incurred until delivery of the contracted goods to the purchaser.

32.3 No contract shall be concluded with any bidder whose tax matters are not in order. Prior to the award of a bid the Department must be in possession of a tax clearance certificate, submitted by the bidder. This certificate must be an original issued by the South African Revenue Services.

33. National Industrial Participation (NIP) Programme

33.1 The NIP Programme administered by the Department of Trade and Industry shall be applicable to all contracts that are subject to the NIP obligation

34. Prohibition of Restrictive practices

34.1 In terms of section 4 (1) (b) (iii) of the Competition Act No. 89 of 1998, as amended, an agreement between, or concerted practice by, firms, or a decision by an association of firms, is prohibited if it is between parties in a horizontal relationship and if a bidder (s) is / are or a contractor(s) was / were involved in collusive bidding (or bid rigging).

34.2 If a bidder(s) or contractor(s), based on reasonable grounds or evidence obtained by the purchaser, has / have engaged in the restrictive practice referred to above, the purchaser may refer the matter to the Competition Commission for investigation and possible imposition of administrative penalties as contemplated in the Competition Act No. 89 of 1998.

34.3 If a bidder(s) or contractor(s), has / have been found guilty by the Competition Commission of the restrictive practice referred to above, the purchaser may, in addition and without prejudice to any other remedy provided for, invalidate the bid(s) for such item(s) offered, and / or terminate the contract in whole or part, and / or restrict the bidder(s) or contractor(s) from conducting business with the public sector for a period not exceeding ten (10) years and / or claim damages from the bidder(s) or contractor(s) concerned.