

PART A INVITATION TO BID

| | | | | | |
|--|---|---------------|------------|---------------|----------|
| | | | | | |
| BID NUMBER: | WCNCB 12/09/2025 | CLOSING DATE: | 27/10/2025 | CLOSING TIME: | 11H00 AM |
| DESCRIPTION | CapeNature is seeking to appoint a reputable service provider to provide a Managed Wide Area Network and Internet Services for a period of 3 Years (extendable to 5 Years). | | | | |
| THE SUCCESSFUL BIDDER WILL BE REQUIRED TO FILL IN AND SIGN A WRITTEN CONTRACT FORM (WBD7). | | | | | |

BID RESPONSE DOCUMENTS MAY BE DEPOSITED IN THE BID BOX SITUATED AT CAPENATURE CAPE TOWN OFFICE

| | |
|---|--|
| CapeNature Cape Town Office PGWC Shared Services Centre 3rd Floor Cnr Bosduif & Volstruis Streets Bridgetown 7764 | Please note that a compulsory virtual briefing session will be held on Monday 6 October 2025 at 10:00 AM. RSVP for virtual briefing session by 12:00PM on 3 October 2025, please contact: Ms. Nwabisa Gqoboda: ngqoboda@capenature.co.za Confirmed attendees will be provided with a link to join the virtual briefing session on the day of the briefing session. |
| Tender's Email Address (For submission of bid documents only): tenders@capenature.co.za | |

| 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 | | | | |

| | | | | | |
|--|---|---|---|---------|---|
| | WCSD REGISTRATION No. | | AND | CSD No: | |
| B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE [TICK APPLICABLE BOX] | <input type="checkbox"/> Yes <input type="checkbox"/> No | | B-BBEE STATUS LEVEL SWORN AFFIDAVIT | | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| IF YES, WHO WAS THE CERTIFICATE ISSUED BY? | <input type="checkbox"/> | A VERIFICATION AGENCY ACCREDITED BY THE SOUTH AFRICAN ACCREDITATION SYSTEM (SANAS) | | | |
| | <input type="checkbox"/> | A REGISTERED AUDITOR | | | |

[A B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE/SWORN AFFIDAVIT (FOR EMEs & QSEs) MUST BE SUBMITTED TOGETHER WITH A COMPLETED 6.1 IN ORDER TO QUALIFY FOR PREFERENCE POINTS FOR B-BBEE]

| | | | |
|---|--|--|---|
| ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES WORKS OFFERED? | <input type="checkbox"/> Yes <input type="checkbox"/> No [IF YES ENCLOSE PROOF] | ARE YOU A FOREIGN BASED SUPPLIER FOR THE GOODS /SERVICES WORKS OFFERED? | <input type="checkbox"/> Yes <input type="checkbox"/> No [IF YES ANSWER PART B:3 BELOW] |
| SIGNATURE OF BIDDER | | DATE | |
| CAPACITY UNDER WHICH THIS BID IS SIGNED (Attach proof of authority to sign this bid; e.g. resolution of directors, etc.) | | | |
| TOTAL NUMBER OF ITEMS OFFERED | | TOTAL BID PRICE (ALL INCLUSIVE) | |
| BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO: | | TECHNICAL INFORMATION MAY BE DIRECTED TO: | |
| DEPARTMENT/ PUBLIC ENTITY | CapeNature | CONTACT PERSON | Lucinda Witten |
| CONTACT PERSON | Imran Brey | TELEPHONE NUMBER | 087 087 3176 |
| TELEPHONE NUMBER | 087 087 4103 | FACSIMILE NUMBER | N/A |
| FACSIMILE NUMBER | NA | E-MAIL ADDRESS | luwitten@capenature.co.za |
| E-MAIL ADDRESS | ibrey@capenature.co.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)
- 1.3. BIDDERS MUST REGISTER ON THE CENTRAL SUPPLIER DATABASE (CSD) TO UPLOAD MANDATORY INFORMATION NAMELY: (BUSINESS REGISTRATION/ DIRECTORSHIP/ MEMBERSHIP/IDENTITY NUMBERS; TAX COMPLIANCE STATUS; AND BANKING INFORMATION FOR VERIFICATION PURPOSES). B-BBEE CERTIFICATE OR SWORN AFFIDAVIT FOR B-BBEE MUST BE SUBMITTED TO BIDDING INSTITUTION.
- 1.4. THIS BID IS SUBJECT TO THE PREFERENTIAL PROCUREMENT POLICY FRAMEWORK ACT 2000 AND THE PREFERENTIAL PROCUREMENT REGULATIONS, 2017, THE GENERAL CONDITIONS OF CONTRACT (GCC) AND, IF APPLICABLE, ANY OTHER LEGISLATION OR SPECIAL CONDITIONS OF CONTRACT.

2. TAX COMPLIANCE REQUIREMENTS

- 2.1 BIDDERS MUST ENSURE COMPLIANCE WITH THEIR TAX OBLIGATIONS.
- 2.2 APPLICATION FOR TAX COMPLIANCE STATUS (TCS) MAY ALSO BE MADE VIA E-FILING. IN ORDER TO USE THIS PROVISION, TAXPAYERS WILL NEED TO REGISTER WITH SARS AS E-FILE USER THROUGH THE WEBSITE WWW.SARS.GOV.ZA.
- 2.3 BIDDERS MAY ALSO SUBMIT A PRINTED TCS WITH A RESULT SUMMARY PAGE (DOWNLOADED FROM EFILING) TOGETHER WITH THE BID.
- 2.4 IN BIDS WHERE CONSORTIA / JOINT VENTURES / SUB-CONTRACTORS ARE INVOLVED, EACH PARTY MUST SUBMIT A SEPARATE PROOF OF TCS AS MENTIONED IN 2.3 ABOVE.

3. QUESTIONNAIRE TO BIDDING FOREIGN SUPPLIERS

- 3.1. IS THE BIDDER A RESIDENT OF THE REPUBLIC OF SOUTH AFRICA (RSA)? ☐ YES ☐ NO
- 3.2. DOES THE BIDDER HAVE A BRANCH IN THE RSA? ☐ YES ☐ NO
- 3.3. DOES THE BIDDER HAVE A PERMANENT ESTABLISHMENT IN THE RSA? ☐ YES ☐ NO
- 3.4. DOES THE BIDDER HAVE ANY SOURCE OF INCOME IN THE RSA? ☐ YES ☐ NO

IF THE ANSWER IS “NO” TO ALL OF THE ABOVE, THEN, IT IS NOT A REQUIREMENT TO PROVIDE PROOF OF TAX COMPLIANCE STATUS; NOR OBTAIN A TAX COMPLIANCE STATUS FROM THE SOUTH AFRICAN REVENUE SERVICE (SARS) IF NOT REGISTER AS PER 2.2 ABOVE.

***FAILURE TO PROVIDE ANY OF THE ABOVE PARTICULARS MAY RENDER THE BID INVALID .**

SIGNATURE OF BIDDER:

.....

CAPACITY UNDER WHICH THIS BID IS SIGNED:

.....

(Proof of authority must submitted e.g. company resolution)

DATE:

.....

TAX CLEARANCE REQUIREMENTS

IT IS A CONDITION OF THE TENDER THAT -

1. The taxes of the successful service provider **must** be in order, or that satisfactory arrangements have been made with the Receiver of Revenue to meet his / her tax obligations.
2. Application for tax clearance must be done through the Receiver of Revenue office where the service provider is registered for tax purposes. The Receiver of Revenue will then furnish the Supplier with a Tax Clearance Certificate that will be valid for a period of one year from date of issue.
3. This Tax Clearance Certificate must be submitted in the original together with the tender. Failure to submit the **original** and valid Tax Clearance Certificate **will** invalidate the tender. If a tax clearance certificate was submitted previously to CapeNature please indicate as such.
4. In quotations where Consortia / Joint Ventures / Sub-contractors are involved each party must submit a separate Tax Clearance Certificate. Copies of the Application for Tax Clearance Certificates are available at any Receiver's Office.

| | | |
|---|-----|----|
| HAS A TAX CLEARANCE CERTIFICATE BEEN SUBMITTED | YES | NO |
| ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS/SERVICES OFFERED BY YOU? (IF YES ENCLOSE PROOF) | YES | NO |

PART C
PRICING SCHEDULE

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

| Managed Wide Area Network and Internet Services | Amount (VAT Inclusive) |
|--|-------------------------------|
| Wide Area Network Infrastructure | R |
| Managed and Hosted (dedicated) Firewall | R |
| Internet Services | R |
| Corporate APN Services | R |
| Telephony Services (MS Teams Voice) | R |
| Azure ExpressRoute | R |
| TOTAL TENDER AMOUNT (ALL-INCLUSIVE) | R |

PREFERENCE POINTS CLAIM FORM IN TERMS OF THE PREFERENTIAL PROCUREMENT REGULATIONS 2022 AND IN TERMS OF THE WESTERN CAPE GOVERNMENTS INTERIM STRATEGY AS IT RELATES TO PREFERENCE POINTS

This preference form must form part of all bids invited. It contains general information and serves as a claim form for preference points for Broad-Based Black Economic Empowerment (B-BBEE) Status Level of Contribution.

NB: BEFORE COMPLETING THIS FORM, BIDDERS (TENDERERS) MUST STUDY THE GENERAL CONDITIONS, DEFINITIONS AND DIRECTIVES APPLICABLE IN RESPECT OF THE TENDER, PREFERENTIAL PROCUREMENT REGULATIONS, 2022 AND THE BROAD BASED BLACK ECONOMIC EMPOWERMENT ACT AND THE CODES OF GOOD PRACTICE

1. DEFINITIONS

- 1.1 **“acceptable tender”** means any tender which, in all respects, complies with the specifications and conditions of tender as set out in the tender document.
- 1.2 **“affidavit”** is a type of verified statement or showing, or in other words, it contains a verification, meaning it is under oath or penalty of perjury, and this serves as evidence to its veracity and is required for court proceedings.
- 1.3 **“all applicable taxes”** includes value-added tax, pay as you earn, income tax, unemployment insurance fund contributions and skills development levies;
- 1.4 **“B-BBEE”** means broad-based black economic empowerment as defined in section 1 of the Broad-Based Black Economic Empowerment Act;
- 1.5 **“B-BBEE status level of contributor”** means the B-BBEE status of an entity in terms of a code of good practice on black economic empowerment issued in terms of section 9(1) of the Broad-Based Black Economic Empowerment Act;
- 1.6 **“bid”** means a written offer on the official bid documents or invitation of price quotations and **“tender”** is the act of bidding/tendering;
- 1.7 **“Code of Good Practice”** means the generic codes or the sector codes as the case may be;
- 1.8 **“consortium or joint venture”** 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;
- 1.9 **“contract”** means the agreement that results from the acceptance of a bid by an organ of state;
- 1.10 **“EME”** is an Exempted Micro Enterprise with an annual total revenue of R10 million or less.
- 1.11 **“Firm price”** means the price that is only subject to adjustments in accordance with the actual increase or decrease resulting from the change, imposition, or abolition of customs or excise duty and any other duty, levy, or tax, which, in terms of the law or regulation, is binding on the contractor and demonstrably has an influence on the price of any supplies, or the rendering costs of any service, for the execution of the contract;
- 1.12 **“Large Enterprise”** is any enterprise with an annual total revenue above R50 million;
- 1.13 **“non-firm prices”** means all prices other than “firm” prices;
- 1.14 **“person”** includes a juristic person;
- 1.15 **“price”** means an amount of money tendered for goods or services, and includes all applicable taxes less all unconditional discounts;

- 1.16 **“proof of B-BBEE status level contributor”** means-
- (a) The B-BBEE status level certificate issued by an authorized body or person;
 - (b) A sworn affidavit as prescribed in terms of the B-BBEE Codes of Good Practice; or
 - (c) Any other requirement prescribed in terms of the Broad-Based Black Economic Empowerment Act.
- 1.17 **QSE** is a Qualifying Small Enterprise with an annual total revenue between R10 million and R50 million;
- 1.18 **“rand value”** means the total estimated value of a contract in Rand, calculated at the time of the tender invitation; and includes all applicable taxes;
- 1.19 **“sub-contract”** means the primary contractor’s assigning, leasing, making out work to, or employing, another person to support such primary contractor in the execution of part of a project in terms of the contract.
- 1.20 **“tender”** means a written offer in the form determined by an organ of state in response to an invitation to provide or services through price quotations, competitive tendering process or any other method envisaged in legislation;
- 1.21 **“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;
- 1.22 **“the Act”** means the Preferential Procurement Policy Framework Act, 2000 (Act No. 5 of 2000);
- 1.23 **“the Regulations”** means the Preferential Procurement Regulations, 2022;
- 1.24 **“total revenue”** bears the same meaning assigned to this expression in the Codes of Good Practice on Black Economic Empowerment, issued in terms of section 9(1) of the Broad-Based Black Economic Empowerment Act and promulgated in the Government Gazette on 11 October 2013;
- 1.25 **“trust”** means the arrangement through which the property of one person is made over or bequeathed to a trustee to administer such property for the benefit of another person; and
- 1.26 **“trustee”** means any person, including the founder of a trust, to whom property is bequeathed in order for such property to be administered for the benefit of another person.

2. GENERAL CONDITIONS

- 2.1 The following preference point systems are applicable to all bids:
- 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).
- 2.2 Preference point system for this bid:
- a) The value of this bid is estimated to not exceed R50 000 000 (all applicable taxes included) and therefore the 80/20 preference point system shall be applicable; or
 - b) The 80/20 preference point system will be applicable to this tender.
- 2.3 Preference points for this bid shall be awarded for:
- a) Price; and
 - b) B-BBEE Status Level of Contribution

- 2.4 The maximum points for this bid are allocated as follows:

| | POINTS |
|---|--------|
| PRICE | |
| B-BBEE STATUS LEVEL OF CONTRIBUTOR | |
| Total points Price and B-BBEE must not exceed | 100 |

- 2.5 Failure on the part of a bidder to fill in, sign this form and submit in the circumstances prescribed in the Codes of Good Practice either a B-BBEE Verification Certificate issued by a Verification Agency accredited by the South African Accreditation System (SANAS) or an affidavit confirming annual total revenue and level of black ownership together with the bid or an affidavit issued by Companies Intellectual Property Commission, will be interpreted to mean that preference points for B-BBEE status level of contribution are not claimed.
- 2.6 The organ of state reserves the right to require of a bidder, either before a bid is adjudicated or at any time subsequently, to substantiate any claim in regard to preferences, in any manner required by the organ of state.

3. ADJUDICATION USING A POINT SYSTEM

- 3.1 Subject to Section 2(1)(f) of the Preferential Procurement Policy Framework Act, 2000, the bidder obtaining **the highest number of total points** will be awarded the contract.
- 3.2 A tenderer must submit proof of its B-BBEE status level of contributor in order to claim points for B-BBEE.
- 3.3 A tenderer failing to submit proof of B-BBEE status level of contributor or is a non-compliant contributor to B-BBEE will not be disqualified but will only score:
- (a) points out of 80 for price; and
 - (b) 0 points out of 20 for B-BBEE
- 3.4 Points scored must be rounded off to the nearest 2 decimal places.
- 3.5 In the event that two or more bids have scored equal total points, the successful bid must be the one scoring the highest number of preference points for B-BBEE.
- 3.6 As per section 2(1)(f) of the Preferential Procurement Policy Framework Act, 2000, the contract may be awarded to a bidder other than the one scoring the highest number of total points based on objective criteria in addition to those contemplated in paragraphs (d) and (e) of the Preferential Procurement Policy Framework Act, 2000 that justifies the award to another tenderer provided that it has been stipulated upfront in the tendering conditions.
- 3.7 Should two or more bids be equal in all respects; the award shall be decided by the drawing of lots.

4. FORMULAE FOR PROCUREMENT OF GOODS AND SERVICES

4.1 POINTS AWARDED FOR PRICE

4.1.1 THE 80/20 OR 90/10 PREFERENCE POINT SYSTEM

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

80/20

or

90/10

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

Where

Ps = Points scored for price of bid under consideration

Pt = Price of tender under consideration

Pmin = Price of lowest acceptable tender

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

5.1 POINTS AWARDED FOR PRICE

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

80/20

or

90/10

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

Where

Ps = Points scored for price of bid under consideration

Pt = Price of tender under consideration

Pmax = Price of highest acceptable tender

6. POINTS AWARDED FOR B-BBEE STATUS LEVEL OF CONTRIBUTION

- 6.1 In terms of WCG interim strategy, preference points must be awarded to a bidder for attaining the B-BBEE status level of contribution in accordance with the table below:

| B-BBEE Status Level of Contributor | Number of points (90/10 system) | Number of points (80/20 system) |
|------------------------------------|---------------------------------|---------------------------------|
| 1 | 10 | 20 |
| 2 | 9 | 18 |
| 3 | 6 | 14 |
| 4 | 5 | 12 |
| 5 | 4 | 8 |
| 6 | 3 | 6 |
| 7 | 2 | 4 |
| 8 | 1 | 2 |
| Non-compliant contributor | 0 | 0 |

- 6.2 An **EME** must submit a valid, originally certified affidavit confirming annual turnover and level of black ownership or an affidavit issued by Companies Intellectual Property Commission.
- 6.3 A **QSE that is less than 51 per cent (50% or less) black owned** must be verified in terms of the QSE scorecard issued via Government Gazette and submit a valid, original or a legible certified copy of a B-BBEE Verification Certificate issued by SANAS.
- 6.4 A **QSE that is at least 51 per cent black owned (51% or higher)** must submit a valid, originally certified affidavit confirming turnover and level of black ownership as well as declare its empowering status or an affidavit issued by Companies Intellectual Property Commission.
- 6.5 A **large enterprise** must submit a valid, original or originally certified copy of a B-BBEE Verification Certificate issued by a verification agency accredited by SANAS.
- 6.6 A trust, consortium or joint venture, will qualify for points for their B-BBEE status level as a legal entity, provided that the entity submits their B-BBEE status level certificate.
- 6.7 A trust, consortium or joint venture (including unincorporated consortia and joint ventures) must submit a consolidated B-BBEE status level verification certificate for every separate tender.
- 6.8 Tertiary institutions and public entities will be required to submit their B-BBEE status level certificates in terms of the specialized scorecard contained in the B-BBEE Codes of Good Practice.

7. BID DECLARATION

- 7.1 Bidders who claim points in respect of B-BBEE Status Level of Contribution must complete the following:

8. B-BBEE STATUS LEVEL OF CONTRIBUTION CLAIMED IN TERMS OF PARAGRAPH 6

- 8.1 B-BBEE Status Level of Contribution = (maximum of 20 points)

(Points claimed in respect of paragraph 7.1 must be in accordance with the table reflected in paragraph 6.1 and must be substantiated by means of a B-BBEE certificate issued by a Verification Agency accredited by SANAS or an affidavit confirming annual total revenue and level of black ownership in terms of the relevant sector code applicable to the tender.

9. SUB-CONTRACTING

9.1 Will any portion of the contract be sub-contracted? **YES / NO**

9.1.1 If yes, indicate:

(i) what percentage of the contract will be subcontracted?%

(ii) the name of the sub-contractor?

(iii) the B-BBEE status level of the sub-contractor?

(iv) whether the sub-contractor is an EME or QSE? **YES / NO**

9.1.2 Sub-contracting relates to a **particular** contract and if sub-contracting is applicable, the bidder to state in their response to a particular RFQ that a portion of that contract will be sub-contracted.

10. DECLARATION WITH REGARD TO COMPANY/FIRM

10.1 Name of company/entity :

10.2 VAT registration number :

10.3 Company Registration number :

10.4 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

[SELECT APPLICABLE ONE]

10.5 I/we, the undersigned, who is / are duly authorised to do so on behalf of the company/firm, certify that the points claimed, based on the B-BBEE status level of contribution indicated in paragraph 7 above, qualifies the company/ firm for the preference(s) shown and I / we acknowledge that:

(a) The Western Cape Government reserves the right to audit the B-BBEE status claim submitted by the bidder.

(b) As set out in Section 13O of the B-BBEE Act as amended, any misrepresentation constitutes a criminal offence. A person commits an offence if that person knowingly:

(i) misrepresents or attempts to misrepresent the B-BBEE status of an enterprise;

(ii) provides false information or misrepresents information to a B-BBEE Verification Professional in order to secure a particular B-BBEE status or any benefit associated with compliance to the B-BBEE Act;

- (iii) provides false information or misrepresents information relevant to assessing the B-BBEE status of an enterprise to any organ of state or public entity; or
 - (iv) engages in a fronting practice.
- (c) If a B-BBEE verification professional or any procurement officer or other official of an organ of state or public entity becomes aware of the commission of, or any attempt to commit any offence referred to in paragraph 10.5 (a) above will be reported to an appropriate law enforcement agency for investigation.
- (d) Any person convicted of an offence by a court is liable in the case of contravention of 10.5 (b) to a fine or to imprisonment for a period not exceeding 10 years or to both a fine and such imprisonment or, if the convicted person is not a natural person to a fine not exceeding 10 per cent of its annual turnover.
- (e) The purchaser may, if it becomes aware that a bidder may have obtained its B-BBEE status level of contribution on a fraudulent basis, investigate the matter. Should the investigation warrant a restriction be imposed, this will be referred to the National Treasury for investigation, processing and imposing the restriction on the National Treasury's List of Restricted Suppliers. The bidder or contractor, its shareholders and directors, or only the shareholders and directors who acted on a fraudulent basis, may 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.
- (f) The purchaser may, in addition to any other remedy it may have –
- (i) disqualify the person from the bidding process;
 - (ii) recover costs, losses or damages it has incurred or suffered as a result of that person's conduct;
 - (iii) 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; and
 - (iv) forward the matter for criminal prosecution.
- (g) The information furnished is true and correct.
- (h) The preference points claimed are in accordance with the General Conditions as indicated in paragraph 2 of this form.

SIGNATURE(S) OF THE BIDDER(S):

DATE:

ADDRESS:

.....

WITNESSES:

1.

2.

PROVINCIAL GOVERNMENT OF WESTERN CAPE

DECLARATION OF INTERESTS, BIDDERS PAST SCM PRACTICES AND INDEPENDENT BID DETERMINATION

1. To give effect to the requirements of the Western Cape Provincial Treasury Instructions, 2019: Supply Chain Management (Goods and Services), Public Finance Management Act (PFMA) Supply Chain Management (SCM) Instruction No. 3 of 2021/2022 - SBD 4 Declaration of Interest, Section 4 (1)(b)(iii) of the Competition Act No. 89 of 1998 as amended together with its associated regulations, the Prevention and Combating of Corrupt Activities Act No 12 of 2004 and regulations pertaining to the tender defaulters register, Paragraph 16A9 of the National Treasury Regulations and/or any other applicable legislation.
2. Any person (natural or juristic) may make an offer or offers in terms of this invitation to bid. In line with the principles of transparency, accountability, impartiality, and ethics as enshrined in the Constitution of the Republic of South Africa and further expressed in various pieces of legislation, it is required for the bidder to make this declaration in respect of the details required hereunder.
3. All prospective bidders intending to do business with the Institution must be registered on the Central Supplier Database (CSD) and the Western Cape Supplier Evidence Bank (WCSEB) if they wish to do business with the Western Cape Government (WCG) via the electronic Procurement Solution (ePS).
4. The status of enterprises and persons listed on the National Treasury's Register for Tender Defaulters will be housed on the ePS. Institutions may not under any circumstances procure from enterprises and persons listed on the Database of Tender Defaulters.
5. The status of suppliers listed on the National Treasury's Database of Restricted Suppliers will be housed on the ePS; however, it remains incumbent on institutions to check the National Treasury Database of Restricted Suppliers before the conclusion of any procurement process. For suppliers listed as restricted, institutions must apply due diligence and risk assessment before deciding to proceed with procurement from any such supplier.

6. **Definitions**

"bid" means a bidder's response to an institution's invitation to participate in a procurement process which may include a bid, price quotation or proposal;

"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;

"business interest" means -

- (a) a right or entitlement to share in profits, revenue or assets of an entity;
- (b) a real or personal right in property;
- (c) a right to remuneration or any other private gain or benefit, or
- (d) includes any interest contemplated in paragraphs (a), (b) or (c) acquired through an intermediary and any potential interest in terms of any of those paragraphs;

"Consortium or Joint Venture" 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;

"Controlling interest" means, the power, by one person or a group of persons holding the majority of the equity of an enterprise, alternatively, the person/s having the deciding vote or power to influence or to direct the course and decisions of the enterprise;

“Corruption”- General offences of corruption are defined in the Combating of Corrupt Activities Act, 2004 (Act No 12 of 2004) as:

Any person who directly or indirectly-

- (a) accepts or agrees or offers to accept any gratification from any other person, whether for the benefit of himself or herself or for the benefit of another person; or
- (b) gives or agrees or offers to give to any other person any gratification, whether for the benefit of that other person or for the benefit of another person., in order to act personally or by influencing another person so to act, in a manner—
 - (i) that amounts to the-
 - (aa) illegal, dishonest, unauthorised, incomplete, or biased; or
 - (bb) misuse or selling of information or material acquired in the course of the exercise, carrying out or performance of any powers, duties or functions arising out of a constitutional, statutory, contractual or any other legal obligation;
 - (ii) that amounts to-
 - (aa) the abuse of a position of authority;
 - (bb) a breach of trust; or
 - (cc) the violation of a legal duty or a set of rules;
 - (iii) designed to achieve an unjustified result; or
 - (iv) that amounts to any other unauthorised or improper inducement to do or not to do anything, of the, is guilty of the offence of corruption

“CSD” means the Central Supplier Database maintained by National Treasury;

“employee”, in relation to –

- (a) a department, means a person contemplated in section 8 of the Public Service Act, 1994 but excludes a person appointed in terms of section 12A of that Act; and
- (b) a public entity, means a person employed by the public entity;

“entity” means any -

- (a) association of persons, whether or not incorporated or registered in terms of any law, including a company, corporation, trust, partnership, close corporation, joint venture or consortium; or
- (b) sole proprietorship;

“entity conducting business with the Institution” means an entity that contracts or applies or tenders for the sale, lease or supply of goods or services to the Province;

“Family member” means a person’s -

- (a) spouse; or
- (b) child, parent, brother, sister, whether such a relationship results from birth, marriage or adoption or some other legal arrangement (as the case may be);

“intermediary” means a person through whom an interest is acquired, and includes a representative or agent or any other person who has been granted authority to act on behalf of another person;

“Institution” means –

a provincial department or provincial public entity listed in Schedule 3C of the Act; **“Provincial Government Western Cape (PGWC)”** means

- (a) the Institution of the Western Cape, and
- (b) a provincial public entity;

“RWOEE” means -

Remunerative Work Outside of the Employee’s Employment

“spouse” means a person’s -

- (a) partner in marriage or civil union according to legislation;
- (b) partner in a customary union according to indigenous law; or
- (c) partner with whom he or she cohabits and who is publicly acknowledged by the person as his or her life partner or permanent companion.

7. Regulation 13(c) of the Public Service Regulations (PSR) 2016, effective 1 February 2017, prohibits any employee from conducting business with an organ of state, or holding a directorship in a public or private company doing business with an organ of state unless the employee is a director (in an official capacity) of a company listed in schedules 2 and 3 of the Public Finance Management Act.
 - a) Therefore, by 31 January 2017 all employees who are conducting business with an organ of state should either have:
 - (i) resigned as an employee of the government institution or;
 - (ii) cease conducting business with an organ of state or;
 - (iii) resign as a director/shareholder/owner/member of an entity that conducts business with an organ of state.
8. Any legal person, or their family members, may make an offer or offers in terms of this invitation to bid. In view of potential conflict of interest, in the event that the resulting bid, or part thereof, be awarded to family members of persons employed by an organ of state, it is required that the bidder or his/her authorised representative declare his/her position in relation to the evaluating/adjudicating authority where the bidder is employed by the Institution
9. The bid of any bidder may be disregarded if that bidder or any of its directors abused the institution's supply chain management system; committed fraud or any other improper conduct in relation to such system; or failed to perform on any previous contract.
10. 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). Collusive bidding is a per se prohibition meaning that it cannot be justified under any grounds.
11. Treasury Regulation 16A9 prescribes that accounting officers and accounting authorities must take all reasonable steps to prevent abuse of the supply chain management system and authorises accounting officers and accounting authorities to:
 - (a) disregard the bid of any bidder if that bidder, or any of its directors have abused the institution's

supply chain management system and or committed fraud or any other improper conduct in relation to such system.

- (b) cancel a contract awarded to a supplier of goods and services if the supplier committed any corrupt or fraudulent act during the bidding process or the execution of that contract.
12. Communication between partners in a joint venture or consortium will not be construed as collusive bidding.
13. 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.

SECTION A: DETAILS OF THE ENTITY

| | |
|---|------|
| CSD Registration Number | MAAA |
| Name of the Entity | |
| Entity registration Number (where applicable) | |
| Entity Type | |
| Tax Reference Number | |
| Full details of directors, shareholder, member, partner, trustee, sole proprietor or any persons with a right or entitlement to share in profits, revenue or assets of the entity should be disclosed in the Table A below. | |

TABLE A

[illegible]

SECTION B: DECLARATION OF THE BIDDER'S INTEREST

The supply chain management system of an institution must, irrespective of the procurement process followed, prohibit any award to an employee of the state, who either individually or as a director of a public or private company or a member of a close corporation, seek to conduct business with the WCG, unless such employee is in an official capacity a director of a company listed in Schedule 2 or 3 of the PFMA as prescribed by the Public Service Regulation 13 (c).

Furthermore, an employee employed by an organ of state conducting remunerative work outside of the employee's employment should first obtain the necessary approval by the delegated authority (RWOOE), failure to submit proof of such authority, where applicable, may result in disciplinary action.

| | | | |
|-----|--|----|-----|
| B1. | Are any persons listed in Table A identified on the CSD as employees of an organ of state? (If yes, refer to Public Service Circular EIM 1/2016 to exercise the listed actions) | NO | YES |
| B2. | Are any employees of the entity also employees of an organ of state? (If yes complete Table B and attach their approved "RWOEE") | NO | YES |
| B3. | Are any family members of the persons listed in Table A employees of an organ of state? (If yes complete Table B) | NO | YES |

TABLE B

Details of persons (family members) connected to or employees of an organ of state should be disclosed in Table B below.

[illegible]

SECTION C: PERFORMANCE MANAGEMENT AND BIDDER'S PAST SUPPLY CHAIN MANAGEMENT PRACTICES

To enable the prospective bidder to provide evidence of past and current performance.

| | | | |
|------------|--|----|-----|
| C1. | Did the entity conduct business with an organ of state in the last twelve months? (If yes complete Table C) | NO | YES |
|------------|--|----|-----|

C2. TABLE C

Complete the below table to the maximum of the last 5 contracts.

| NAME OF CONTRACTOR | PROVINCIAL DEPARTMENT OR PROVINCIAL ENTITY | TYPE OF SERVICES OR COMMODITY | CONTRACT/ ORDER NUMBER | PERIOD OF CONTRACT | VALUE OF CONTRACT |
|--------------------|--|-------------------------------|------------------------|--------------------|-------------------|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| C3. | Is the entity or its principals listed on the National Database as companies or persons prohibited from doing business with the public sector? | | | | NO YES |
| C4. | Is the entity or its principals listed on the National Treasury Register for Tender Defaulters in terms of section 29 of the Prevention and Combating of Corrupt Activities Act (No. 12 of 2004)? (To access this Register enter the National Treasury's website, www.treasury.gov.za , click on the icon "Register for Tender Defaulters" or submit your written request for a hard copy of the Register to facsimile number (012) 326 5445.) | | | | NO YES |
| C5. | If yes to C3 or C4, were you informed in writing about the listing on the database of restricted suppliers or Register for Tender Defaulters by National Treasury? | | | NO | YES N/A |
| C6. | Was the entity or persons listed in Table A convicted for fraud or corruption during the past five years in a court of law (including a court outside the Republic of South Africa)? | | | | NO YES |
| C7. | Was any contract between the bidder and any organ of state terminated during the past five years on account of failure to perform on or comply with the contract? | | | | NO YES |

SECTION D: DULY AUTHORISED REPRESENTATIVE TO DEPOSE TO AFFIDAVIT

This form must be signed by a duly authorised representative of the entity in the presence of a commissioner of oaths.

I, hereby swear/affirm;

- i. that the information disclosed above is true and accurate;
- ii. that I have read understand the content of the document;
- iii. that I have arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with any competitor.
- iv. that the entity undertakes to independently arrive at any offer at any time to the Institution without any consultation, communication, agreement or arrangement with any competitor. In addition, that there will be no consultations, communications, agreements or arrangements with any competitor regarding the quality, quantity, specification, prices, including methods, factors or formulas used to calculate prices, market allocation, the intention or decision to submit or not to submit the bid, bidding with the intention not to win the bid and conditions or delivery particulars of the products or services to which this bid invitation relates;
- v. that the entity or its representative are aware of and undertakes not to disclose the terms of any bid, formal or informal, directly or indirectly, to any competitor, prior to the date and time of the official bid opening or of the awarding of the contract; and
- vi. that there have been no consultations, communications, agreements or arrangements made with any official of the procuring institution in relation to this procurement process prior to and during the bidding process except to provide clarification on the bid submitted where so required by the institution; and that my entity was not involved in the drafting of the specifications or terms of reference for this bid.

.....

DULY AUTHORISED REPRESENTATIVE'S

SIGNATURE

I certify that before administering the oath/affirmation I asked the deponent the following questions and wrote down his/her answers in his/her presence:

- 1.1 Do you know and understand the contents of the declaration? ANSWER:
- 1.2 Do you have any objection to taking the prescribed oath? ANSWER:
- 1.3 Do you consider the prescribed oath to be binding on your conscience? ANSWER:.....
- 1.4 Do you want to make an affirmation? ANSWER:

2. I certify that the deponent has acknowledged that he/she knows and understands the contents of this declaration, which was sworn to/affirmed and the deponent's signature/thumbprint/mark was place thereon in my presence.

.....

SIGNATURE FULL NAMES: Commissioner of Oaths

Designation (rank): **ex officio:** Republic of South Africa

Date: **Place:**

Business Address:

.....

GENERAL CONDITIONS OF CONTRACT

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.

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 with 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.

2. 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 analysed 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

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 fulfilment 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 cancelling 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 wilful misconduct, and in the case of infringement pursuant to

(a) 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

(b) 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.



REQUEST FOR PROPOSALS

MANAGED WIDE AREA NETWORK SERVICE and INTERNET SERVICES

Proposals are hereby invited for a reputable service provider to provide a proposal for the following services for a period of 36 months (extendable to 5 years):

1. Wide Area Network Infrastructure
2. Managed and Hosted (dedicated) Firewall
3. Internet Services
4. Corporate APN services
5. Telephony Services (MS Teams Voice)
6. Azure ExpressRoute

1. INTRODUCTION

CapeNature is seeking a qualified and experienced Internet Service Provider (ISP) to deliver reliable, scalable, and secure network connectivity and infrastructure services. The successful provider will be responsible for provisioning, maintaining, and supporting CapeNature's existing SD-WAN environment, as well as meeting future networking requirements. The solution must ensure high performance, robust security, and cost-effectiveness, while providing ongoing support to enable the Entity's operational and strategic objectives.

Existing services that will be in scope for this project include:

1.1. SD-WAN Infrastructure and Connectivity

Provision and support of SD-WAN infrastructure across 43 worksites, each with dedicated internet services providing a minimum bandwidth of 30 Mbps per site (refer to Annexure 1: Site List).

1.2. Dedicated Managed Firewall

Provision a dedicated, fully managed firewall solution to provide secure, resilient, and centrally administered protection for its network environment, in the CapeNature environment (Annexure 5_Firewall Specs).

1.3. Centralised Internet Breakout

Establish a centralised internet breakout (DIA) for all CapeNature internet traffic as per existing configurations.

1.4. Corporate APN

Provision of a secure Corporate Access Point Name (APN) service to enable managed mobile connectivity for CapeNature staff and devices, with appropriate security, monitoring, and usage controls.

1.5. Telephony Services

Provision of enterprise-grade telephony services through Microsoft Teams, including call routing, number management, and integration with existing collaboration tools.

1.6. Azure ExpressRoute

Provision and support of a dedicated Microsoft Azure ExpressRoute connection to ensure secure, reliable, and high-performance connectivity between CapeNature's on-premises network and Azure cloud services.

2. BACKGROUND

CapeNature currently makes use of a 200 Mbps internet service to deliver connectivity across its sites and reserves in the Western Cape. The existing ISP contract will expire at the end of March 2026. The network environment further includes:

- a) A managed, hosted FortiGate FGT100F firewall (with failover), providing advanced security, VPN capability, and unified threat management.
- b) A distributed SD-WAN infrastructure based on Cisco Meraki MX appliances across branch sites and the Cape Town head office, with secure VPN tunnels, local breakout, and LTE failover where feasible.
- c) A corporate APN with approximately 400 active SIMs, enabling mobile staff connectivity through CapeNature's firewall.
- d) An existing Azure ExpressRoute connection providing secure and high-performance integration with Microsoft Azure cloud services.

CapeNature intends to retain its current connectivity and associated services under a Service Level Agreement (SLA) that guarantees quality of service, while also accommodating future growth requirements. A highly available environment with robust failover capabilities is critical to ensuring business continuity.

The preferred bidder must ensure a seamless transition from the existing services with no disruption to CapeNature's operations and must demonstrate capability to manage and

optimise the existing firewalls, SD-WAN, APN, and Azure ExpressRoute as part of their proposal.

The successful bidder will be required to provide the following as part of their proposal:

2.1. Transition Planning

Bidders must develop and execute a **comprehensive takeover and transition plan** that ensures minimal disruption to CapeNature's operations, including day-to-day staff activities and critical business processes. The plan must incorporate:

- **Comprehensive project management practices**, including a dedicated project manager, clear governance structures, and regular status reporting to CapeNature stakeholders.
- **Phased approach with defined milestones**, including maximum allowable transition periods for cutover from the previous solution vendor, to ensure accountability and transparency.
- **Detailed risk management and mitigation measures** to identify, track, and address potential issues that may arise during the transition.
- **Rollback and contingency procedures** to restore services in the event of unforeseen failures, ensuring business continuity at all times.
- **Change management and communication strategies**, including training and user awareness activities, to minimise staff impact and support a smooth adoption of the new services.

2.2. Monitoring Access

Enable CapeNature ICT staff with access to monitoring tools and dashboards covering utilisation, status, quality, uptime, and performance.

2.3. Reporting

Provide detailed monthly service reports, including performance metrics and incidents, for each contracted service.

2.4. Service Level Commitments

Bidders must provide explicit SLA commitments, including a minimum uptime guarantee of 99.8% per site across all contracted services (internet, voice, APN, firewall, and cloud interconnects). The SLA must define response and resolution times by severity level (Critical, High, Medium, Low) with enforced escalation procedures.

A penalty mechanism must be included, with penalties applied as service credits against monthly invoices. The service provider must also commit to continuous

improvement, with SLA thresholds reviewed annually to align with industry best practice and CapeNature's evolving needs.

2.5. Service Management

The service provider must assign a **dedicated Service Delivery Manager (SDM)** as the single point of contact for CapeNature, ensuring effective governance, communication, and incident resolution. Full ITSM integration with CapeNature's service desk is required, aligned with ITIL-based processes, providing end-to-end visibility of incidents, changes, and service requests.

Bidders must commit to **monthly SLA review meetings with detailed reporting**, supported by real-time dashboards and formal governance reports, and to quarterly strategic reviews covering capacity, optimisation, and risk reduction. Comprehensive documentation and change management must be provided, with all service changes subject to CapeNature approval and full-service inventories maintained.

A formal escalation framework must be defined, with clear responsibilities, timelines, and escalation paths up to senior management, ensuring accountability and timely resolution of service issues.

- **Escalation Framework**

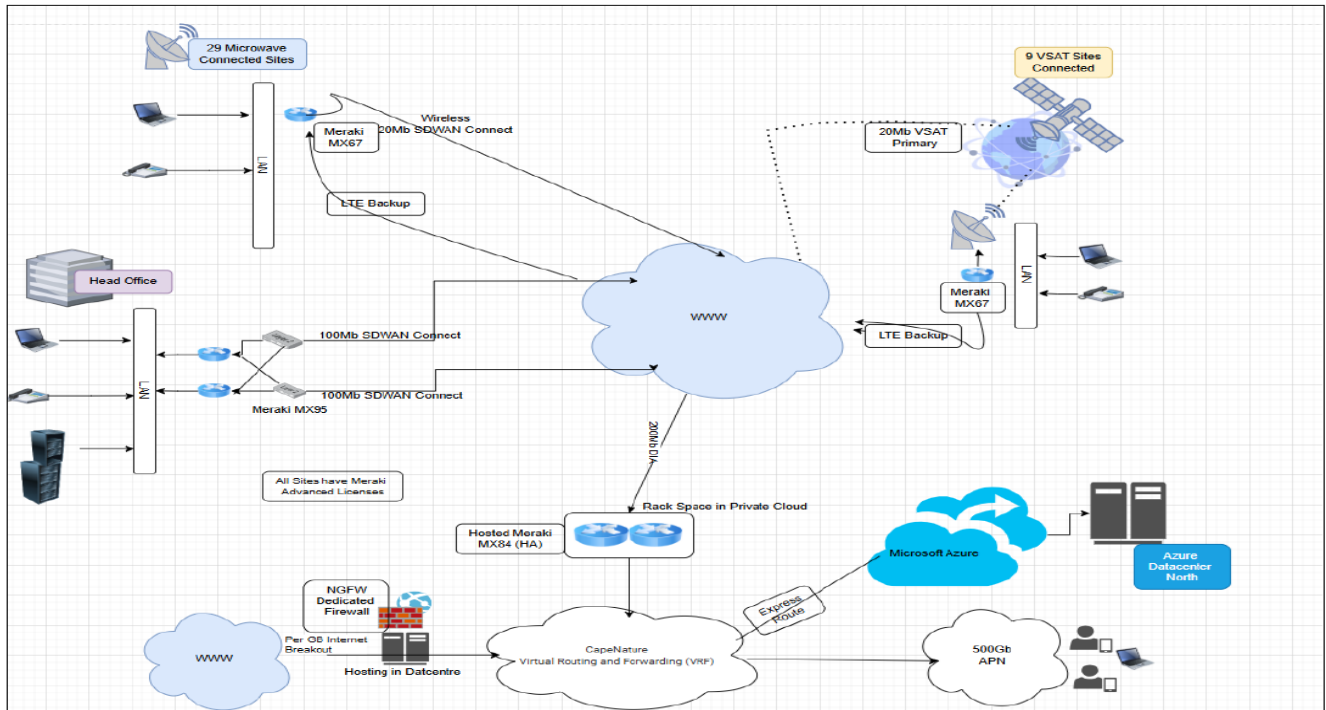
Require documented escalation paths that clearly define roles, responsibilities, and timelines for issue resolution. The framework must ensure accountability at each stage, with pre-defined contact points and escalation to senior management if service levels are not restored within agreed timeframes.

- **24/7 Monitoring**

Ensure all services are monitored continuously (24/7/365), with timely alerts and reporting on outages and service disruptions.

2.6. CapeNature Network Architecture Components (Current) Sites

The network architecture diagram illustrates CapeNature's current hybrid network design, highlighting a secure, scalable, and resilient infrastructure that interconnects multiple remote sites with centralised cloud services. The design emphasises SD-WAN capabilities, seamless cloud integration, and multi-layered connectivity redundancy.



2.6.1. WORK SITES

Each site is equipped with a Cisco Meraki MX64 appliance, licensed with the Advanced Security package, which functions as both a firewall and a unified threat management (UTM) device. The MX64 is connected to a single primary internet link, with LTE / other failover available at sites where feasible.

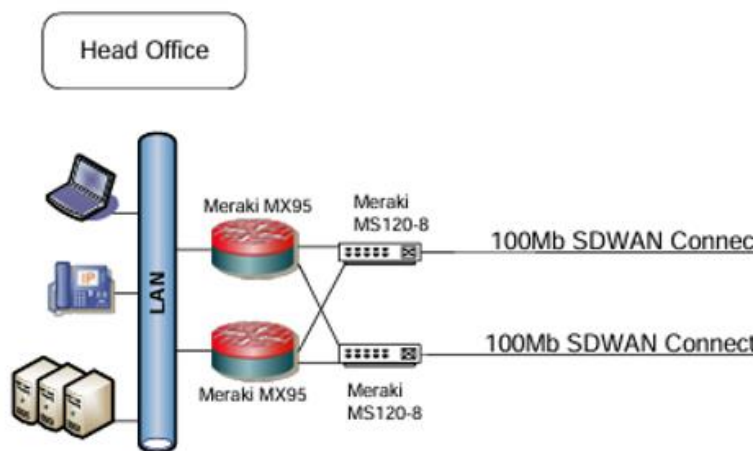
2.6.2. CAPE TOWN OFFICE

At CapeNature's Cape Town Head Office, two independent internet links (each 100 Mbps) are provisioned as part of the SD-WAN design. These links are configured for active load balancing, optimising inbound and outbound traffic.

Each link terminates on a dedicated Meraki MX95 appliance, which is connected to its own Meraki switch to ensure redundancy and separation of traffic flows. Two CapeNature access switches are then connected via LAN interfaces to the Meraki switches, providing resilient connectivity and supporting failover between the MX95 appliances.

This design ensures:

- a) **Resilience and Redundancy** – Dual links, dual CPE appliances, and dual switch interconnections protect against single points of failure.
- b) **Load Balancing** – Traffic is intelligently distributed across both links to maximise performance.
- c) **Scalability** – The architecture supports future bandwidth growth and additional services.
- d) **Security** – The MX95 appliances provide integrated firewalling and SD-WAN security features, extending CapeNature’s security posture to the Head Office.



2.6.3. DATACENTRE

The current service provider supplies rack space within their datacentre to host the following:

- a) A **hosted contact centre**.
- b) **200 Mbps Direct Internet Access (DIA) breakout**. This is utilised across the CapeNature network.
- c) A corporate APN to provide remote users with a secure connection to CapeNature network and services.
- d) A secure breakout to the Microsoft Azure Cloud where CapeNature hosts a number of critical services i.e., Microsoft 365 collaboration tools, virtual machines supporting line-of-business applications, cloud-based storage and backup, and other workloads essential to daily operations.
- e) The current FortiGate firewall(s), which provide secure internet access, and the routing required for connectivity into CapeNature’s private cloud and the **Azure ExpressRoute** link.

The datacentre is protected by **two Meraki MX75 CPE devices** configured in High Availability (HA) mode. These hosted Meraki appliances perform two key functions:

- Acting as a unified threat management (UTM) firewall for internet and APN security.

- Routing APN and Contact Centre traffic securely back to the Head Office environment.

2.6.4. APN

Access to the Corporate APN is managed through an online administration portal, enabling SIM card provisioning, management, and monitoring. Users connect through a secured firewall, ensuring controlled and protected access to CapeNature's network. All SIM cards are allocated directly to CapeNature, with approximately 400 active APN subscribers currently in use. The number of active subscribers on the APN fluctuates over time depending on operational requirements.

2.6.5. DEDICATED MANAGED (HOSTED) FIREWALL

CapeNature's security infrastructure currently includes a high availability pair of FortiGate FGT100F Next-Generation Firewall(s) (NGFW) for secure internet access. This is configured in active/passive mode.

2.6.6. AZURE EXPRESSROUTE

CapeNature's cloud infrastructure relies on Microsoft Azure for hosting critical workloads. The Azure ExpressRoute provides secure and resilient dedicated connectivity between CapeNature's on-premise network and Azure.

3. HIGH LEVEL SCOPE OF SERVICES REQUIRED

CapeNature intends to enter into a service contract, governed by a Service Level Agreement (SLA), for the supply, installation, configuration, commissioning, and maintenance of scalable WAN and internet services for an initial period of **36 months**. This includes the APN, MS Teams Telephony installation, and managed firewall and Azure ExpressRoute connectivity to the existing Azure environment. Bidders are required to provide **comparative pricing for both three-year and five-year contract options**. The anticipated commencement date is 1 April 2026, subject to the conclusion of all contractual agreements and the successful completion of transition planning. Should the 36-month option be selected by CapeNature, the entity may extend the contract at its sole discretion, for additional terms up to a maximum total duration of five years.

3.1. Technical Specifications (Detailed services required)

Bidders are required to demonstrate their capability to deliver a robust and comprehensive network solution incorporating a redundant and resilient architecture, with high-availability infrastructure designed to minimise downtime and ensure business continuity. The solution must provide secure connectivity that complies with all relevant industry standards and regulations and must be scalable to accommodate CapeNature's future growth requirements. Seamless integration into the Entity's existing IT environment and cloud services is essential. Furthermore, bidders must provide effective remote access and mobility solutions, together with advanced tools for performance optimisation and network traffic management, to ensure consistent, reliable, and efficient service delivery.

3.1.1. SDWAN WIDE AREA NETWORK (WAN) INFRASTRUCTURE

CapeNature currently operates a Cisco Meraki SD-WAN environment across its reserves and offices to provide secure, centralised, and resilient connectivity. The existing Meraki SD-WAN devices deliver cloud-managed networking with integrated security and visibility features. However, CapeNature requires bidders to propose a refreshed, future-proof SD-WAN solution that ensures continuity of service while addressing lifecycle, scalability, and support requirements.

Bidders may:

- **Reuse of existing Meraki devices** where appropriate, provided they comply with CapeNature's lifecycle requirements. Where existing devices do not meet these requirements, bidders must supply and implement replacement units at no additional cost.
- **Propose a full refresh** of the SD-WAN infrastructure using an **alternative or new hardware platform**. In this case, the bidder must ensure the proposed platform provides equal or enhanced SD-WAN functionality, cloud-based centralised management, integrated security, and seamless scalability. In either scenario, the SD-WAN solution must provide high availability, redundant WAN connectivity with diverse last-mile providers, proactive monitoring, secure integration with Azure Cloud (via ExpressRoute or equivalent), and be managed under a comprehensive SLA. The service provider must also maintain an RMA and spares process to minimise downtime at CapeNature's remote reserve sites.
- The **full cost of replacement hardware, implementation, and migration** must be explicitly included in the bid response. All hardware supplied must be quoted at an **amortised cost over 3 years and 5 years** in line with CapeNature's financial requirements. Licensing cost must be transparent, and it should be clearly indicated what the renewal costs are should this be needed during the contract period. All SLA, monitoring, and support costs must be transparently included, with no hidden or undisclosed charges, ensuring CapeNature has

complete visibility of total service and lifecycle costs. **CapeNature must see separate costs for the hardware, licensing and the SLA.**

The successful service provider must ensure:

| Requirement | Description |
|---|---|
| Optimal Connectivity Solutions | Provide the fastest, most stable connectivity available for each site, as listed in Annexure 1: Site List . Must support seamless scalability for future bandwidth upgrades and onboarding of new sites. |
| SD-WAN Devices | The vendor may propose an alternative to Cisco Meraki MX67 that offers equivalent or enhanced SD-WAN functionality, cloud-based management, security features, and integration with the current network. |
| SD-WAN Infrastructure Management | Manage and maintain the enterprise-grade SD-WAN network infrastructure, including proactive monitoring, firmware updates, and adherence to CapeNature's change management processes. |
| QOS | The vendor must configure CapeNature required QOS configurations on the SDWAN to ensure that traffic is prioritised according to CapeNature requirements. |
| Hardware Refresh & Lifecycle | All SD-WAN devices must support future scalability (e.g., licence or module upgrades). Devices must not reach End of Life (EOL) within the first 3 years and must not reach End of Service (EOS) within the extended 5-year support period. Any devices approaching these milestones must be refreshed at no additional cost to CapeNature. |
| RMA & Spares Management | A formal Return Merchandise Authorisation (RMA) process must be established with the vendor. The provider must maintain a pool of critical spares to minimise downtime at remote CapeNature reserves. Replacement timelines must align with SLA requirements, with spares deployed immediately while RMA processes are finalised. |
| Reliable and Redundant Internet Access | <p>Deliver high-speed, reliable internet connectivity with clearly defined redundancy (e.g., dual WAN links, failover, active-passive clustering) to ensure business continuity.</p> <p>All primary and secondary connectivity links must follow physically diverse last-mile routes, using different infrastructure providers where feasible. Evidence of path diversity must be provided.</p> <p>All failover mechanisms must be tested at least annually with documented results provided. Refer to Annexure 1, for details.</p> |
| Comprehensive Network Security | Include robust security measures such as firewalls, VPNs, intrusion detection/prevention systems (IDS/IPS), application control, and URL filtering. |

| Requirement | Description |
|--|---|
| Standards Compliance | Ensure all solutions meet relevant industry standards , and recognised security best practices. |
| 24/7 Support and SLAs | Provide round-the-clock technical support, backed by explicit SLA commitments, defined response and resolution times, penalty structures, and timely escalation procedures (refer draft SLA for specifics). |
| Infrastructure & Other Hidden Costs | Bidders must provide a transparent cost breakdown, including installation, commissioning, Customer Premise Equipment (CPE), licensing, and ongoing support charges. |
| Exit & Transition Planning | Develop and maintain a transition/exit plan to ensure smooth handover of all services, including migration support, rollback scenarios, and full transfer of documentation, configurations, and credentials if services are transitioned to another provider. This documentation should be handed over prior to completion and sign off of the project. |

3.1.2. CONNECTIVITY REQUIREMENTS

The service provider is expected to meet the following minimum requirements regarding internet connectivity and related infrastructure. Failure to meet these requirements may result in disqualification.

| Requirement | Description |
|--|--|
| Primary Fibre Connectivity | Option 1 – Dedicated 200 Mbps Service The service provider must provision a dedicated 200 Mbps fibre connection exclusively for CapeNature’s use. This connection must be uncontended, guaranteed, and supported by a service level agreement (SLA) that ensures high availability and performance. The connection must be uncontended, guaranteed, and supported by the same SLA conditions. |
| Wireless Failover | A wireless backup link of at least 100 Mbps must be provided as failover for the 200 Mbps primary fibre connection in the event of a primary link failure. |
| Failover and Failback Functionality | Failover and failback between the primary and secondary connections must be automatic and seamless, with a maximum failover switch delay of five (5) minutes. The transition should not affect existing routing or IP configurations. All failover mechanisms must be tested at least annually with documented results provided. |
| Coverage Across All Sites | Internet connectivity must be provisioned to all CapeNature sites, including the Cape Town Head Office, as listed in <i>Annexure 1: Site List</i> |

| Requirement | Description |
|---|---|
| Network Uptime Guarantee | The provider must guarantee a minimum of 99.8% uptime. Penalty clauses will be enforced for non-compliance. A full incident report will be required for each outage event. |
| Scalable Bandwidth Provisioning | The provider must offer the ability to scale the contracted speed upward over time, at no additional cost, subject to bandwidth pricing trends and organisational requirements. |
| Provision and Maintenance of Equipment | All required network hardware (e.g., routers, fibre converters, wireless equipment) must be supplied, maintained, and upgraded by the service provider as part of the service. Any exceptions must be clearly identified in the proposal. |
| Public IP Address Allocation | The service must include at least one (1) known public IP address. The configuration must replicate the existing ISP setup to ensure continuity. |
| System Migration and Business Continuity | During migration from the existing ISP, the provider must ensure business continuity with downtime within agreed change windows and SLAs. Proper planning and execution will be critical. |
| Infrastructure & Other Hidden Costs | Bidders must provide a transparent cost breakdown, including installation, commissioning, CPE, licensing, and ongoing support charges. |

3.1.3. DEDICATED MANAGED (HOSTED) FIREWALL

CapeNature requires bidders to provide a managed enterprise firewall solution that includes the **supply of hardware, licensing, and ongoing SLA-based support**. All firewall hardware supply must be quoted at an **amortised cost over 3 years and 5 years** in line with CapeNature's financial requirements. Licensing must be quoted **upfront for the initial 12 months**, and annually thereafter. All SLA, monitoring, and support costs must be transparently included, with no hidden or undisclosed charges, ensuring CapeNature has complete visibility of total service and lifecycle costs. **CapeNature must see separate costs for the hardware, licensing and the SLA which covers the support and monitoring costs**. The proposed firewall solution must meet or exceed the specifications detailed in *Annexure 5_Firewall Specs*.

Although existing firewall rules are available for migration, the incumbent is required to review, validate, and configure all rules to ensure alignment with CapeNature's high security configuration standards and industry best practices. As part of this process, the incumbent must also optimise the rule set by removing redundant, obsolete, or overly permissive rules to maintain a secure and efficient firewall posture

The successful service provider must:

| Requirement | Description |
|---|---|
| Firewall Appliance(s) | Supply enterprise-grade firewall hardware meeting CapeNature's technical and performance requirements. |
| Scalability | The firewall(s) must support future expansion (e.g., licence or module upgrades) and have a minimum vendor-supported lifespan of 3 years , with the option to extend support up to 5 years. The hardware must not reach End of Life (EOL) within the first 3 years , and End of Service (EOS) may not occur within the extended 5-year support term. |
| Hosting and Licensing | The firewall(s) must be hosted in the CapeNature environment. The solution must include valid firewall licensing for a minimum period of 12 months , renewable for the duration of the contract. |
| Redundancy and Business Continuity | The firewall environment is configured in Active-Passive mode or equivalent to ensure service continuity. The solution must support high availability and eliminate single points of failure. The design must support secure failover for both internet and VPN traffic. |
| Management and Monitoring | The firewall must be fully managed and proactively monitored 24/7/365 by the service provider. Continuous monitoring must include performance metrics, availability, attempted breaches, and system health. The service provider is responsible for alerting, and analysis of threats and attempted breaches, not only log retention. |

| Requirement | Description |
|------------------------------------|---|
| | Alerts must be issued timeously in the event of outages or suspicious activity. The cost of this must be separated from the hardware costs. |
| Security Features | The firewall must support and enforce advanced security policies for both voice and data traffic. Capabilities must include IPS/IDS, unified threat management (UTM), malware protection, VPN configuration, web filtering, and DLP features. VPN services must enforce strong encryption, multi-factor authentication, and role-based access control. |
| Logging and Retention | <p>Access and Change Logs All administrative access and configuration changes must be logged in detail, including user identity, timestamp, and nature of the change. These logs must be securely retained for a minimum of 12 months to support governance, audit, and compliance obligations.</p> <p>Rule Processing Logs Logs must capture traffic flows against firewall rules, including permitted, denied, and dropped traffic. These logs must be retained for a minimum of 2 weeks to support operational reviews, troubleshooting, and incident response.</p> <p>Proxy Logs Web browsing and proxy logs must be retained for a minimum of 2 months to provide visibility into user activity, content categories, and potential misuse. These logs must support reporting for compliance, management oversight, and security investigations.</p> <p>Security Event Logging The firewall must generate detailed logs of all security-related events, including intrusion detection/prevention alerts, malware detections, VPN activity, and attempted breaches.</p> |
| Reporting | <p>The service provider must deliver:</p> <p>Weekly reports summarising browsing activity, user behaviour, and security events.</p> <p>Monthly reports providing detailed analysis of performance metrics, attempted breaches, and anomalies.</p> <p>Ad-hoc incident reports in the event of suspected or confirmed security breaches, delivered within agreed SLA timelines.</p> |
| Standards and Best Practice | <p>All firewall configurations must strictly adhere to CapeNature's secure configuration standards, as well as recognised industry best practices. The service provider will be responsible for ensuring that all security configurations are designed, implemented, and maintained in line with the following minimum requirements:</p> <p>Secure Baseline Configuration</p> |

| Requirement | Description |
|---|--|
| | <p>Firewalls must be configured according to CapeNature’s security hardening guidelines and must align with industry benchmarks. The firewall configuration must be assessed against CapeNature’s secure configuration standards annually. Findings must be documented, and remediation recommendations must be provided.</p> <p>Rule Set Review and Optimisation</p> <p>The incumbent must review, validate, and optimise firewall rule sets during onboarding and at least annually thereafter. This includes:</p> <ul style="list-style-type: none"> • Removing redundant or unused rules. • Eliminating overly permissive rules (e.g., “ANY-ANY” policies). • Consolidating rules where appropriate to simplify management. • Ensuring rules are documented with clear business justification and approval. <p>Change Management Compliance</p> <p>All changes to firewall configurations must follow CapeNature’s approved change management process. This includes logging, approval workflows, rollback planning, and post-change verification. Change logs must be made available to CapeNature for audit purposes.</p> <p>Access and Administration must follow the principle of least privilege, and access must only be granted when formally requested by CapeNature. The incumbent must review its own access regularly and remove invalid access soonest i.e., when an employee no longer requires access.</p> <p>Ongoing Alignment with Best Practice</p> <p>The firewall environment must evolve with changing threats and compliance requirements. The incumbent is expected to stay aligned with updates to international best practice standards, emerging security threats, and vendor-recommended hardening guidelines.</p> |
| <p>Patching and Firmware Updates</p> | <p>The service provider must ensure that all firewall appliances are kept up to date with the latest vendor-supported firmware and security patches. Patching must comply with CapeNature policies. The following requirements apply:</p> <p>Patch Management</p> <p>All security patches, hotfixes, and firmware updates must be applied in a timely manner, following vendor recommendations and industry best practice, using the vendor’s stable-path upgrade option. Critical security patches must be deployed within</p> |

| Requirement | Description |
|--|--|
| | <p>the agreed SLA timelines to minimise vulnerability exposure and ensure ongoing system integrity.</p> <p>Testing and Validation</p> <p>All patches and firmware updates must be tested in a controlled environment (where feasible) prior to deployment to ensure stability and compatibility with CapeNature's network.</p> <p>Downtime Management</p> <p>Firmware upgrades and patching must be scheduled to minimise disruption to business operations, with advance notification provided to CapeNature ICT.</p> <p>Documentation and Reporting</p> <p>A full record of applied patches and firmware updates must be maintained, including version history, change logs, and risk justification where updates are deferred.</p> |
| Infrastructure & Other Hidden Costs | Bidders must provide a transparent cost breakdown, including installation, commissioning, licensing, and ongoing support charges. |

3.1.4. CORPORATE APN

The APN will enable secure, reliable, and centrally managed mobile data connectivity across the Entity's fleet of SIM-enabled devices, *see **Annexure 1, APN device list***. The solution must support real-time usage monitoring, device-level controls, secure access to internal resources, and seamless integration with existing firewall and network security infrastructure. The APN service must align with CapeNature's ICT strategy and ensure business continuity, scalability, and compliance with all applicable security standards. All technical specifications and service expectations are detailed in the table below.

| Requirement | Description |
|------------------------------|--|
| APN Management Portal | A secure, web-based portal must be provided for real-time SIM administration, provisioning, usage monitoring, and reporting. The portal must allow CapeNature ICT staff to activate/deactivate SIMs, view usage by device, and generate usage and exception reports. |
| SIM Allocation | Approximately 400 SIM cards must be allocated to CapeNature under the corporate APN. The number of active SIMs will fluctuate over time, therefore pricing must be flexible and based on a per-user (per SIM) cost model. |
| Network Integration | All APN traffic must be routed securely through CapeNature's firewall, with integration into the existing IP schema. This must ensure that mobile devices are subject to the same security controls and monitoring as fixed-site devices. |

| Requirement | Description |
|--|--|
| APN Security and Access Control | <p>The APN service must be designed to enforce strict security controls for all devices connecting via APN dongles or SIM-enabled hardware. The following requirements apply:</p> <p>Controlled Access APN connectivity must not allow automatic connections. All connections must be subject to security-related access control measures, such as authentication prompts, certificate validation, or VPN enforcement, before a device is permitted onto the CapeNature network.</p> <p>Authentication Devices must support secure authentication mechanisms (e.g., multi-factor authentication, digital certificates, or device-level credentials) to prevent unauthorised SIM or dongle use.</p> <p>Device Binding SIM cards must be locked to specific IMEIs or devices, ensuring that lost or stolen SIMs cannot be reused without CapeNature approval.</p> <p>Traffic Enforcement All APN traffic must route through CapeNature's firewall for inspection and enforcement of security policies, including IPS/IDS, content filtering, and logging.</p> <p>Session Control The APN service must support session-level monitoring to detect and terminate suspicious or unauthorised activity in real time.</p> <p>Administration CapeNature ICT staff must have administrative control, via the APN management portal, to enable, disable, or restrict SIMs and dongles as required.</p> |
| Device Compatibility | <p>The APN service must be compatible with Android and iOS devices, as well as routers and mobile hotspots. The incumbent must quote separately on the cost of APN devices/dongles to allow CapeNature to evaluate replacement costs should existing dongles prove incompatible.</p> |
| Coverage | <p>National coverage is required, with guaranteed availability (where feasible) in remote conservation areas and reserves across the Western Cape. Coverage commitments must be supported by coverage maps and service-level assurances. Where guarantees cannot be provided, this must be explicitly stated.</p> |
| Support & SLAs | <p>24/7 support must be provided, backed by a defined SLA with guaranteed response and resolution times. An escalation matrix with clear accountability must be included.</p> |

| Requirement | Description |
|--|--|
| Reporting | Monthly reporting must be provided on data usage per SIM, with proactive alerts for threshold breaches, unusual patterns, and potential misuse. Reports must be available via the APN portal and in downloadable formats. |
| Business Continuity | The service must enable seamless SIM provisioning, activation, and switching with minimal downtime during deployment, fault resolution, or migration to new devices. |
| Data Bundling | The APN must support pooled data bundles across all active SIMs, ensuring efficient use of data and minimising wastage. Providers must specify options for shared corporate data pools, top-ups, and threshold-based notifications. |
| Tiered Bundle Options | Service providers must offer tiered pooled data bundle options (e.g., 500GB, 1 TB, 2 TB, 5 TB) to provide cost-efficiency at scale. Pricing must clearly show the unit cost per GB at each tier, including rollover or top-up options where available. |
| Infrastructure & Other Hidden Costs | Bidders must provide a transparent cost breakdown, including installation, commissioning, CPE, licensing, and ongoing support charges. |

3.1.5. TELEPHONY SERVICES (MS TEAMS VOICE)

CapeNature requires an enterprise-grade telephony solution integrated with Microsoft Teams Voice to provide a unified communication platform for staff across all sites. The service must support internal and external calling, enable secure breakout to the public telephone network (PSTN), and include redundancy measures to ensure uninterrupted operations. Integration with existing Microsoft 365 services is essential, with scalability to support future growth.

Future CRM integration with telephony will be required, and the vendor must ensure that the service provider capability supports this.

| Requirement | Specification |
|-----------------------------|--|
| MS Teams Integration | The service must be integrated natively with Microsoft Teams to provide voice calling, conferencing, and voicemail features across CapeNature's Microsoft 365 environment. |
| PSTN Breakout | Provide secure telephony breakout to the public switched telephone network (PSTN), enabling external inbound and outbound calls via Teams. |
| Direct Routing | The bidder must specify how the solution will be delivered i.e., Direct Routing [using the provider's Session Border Controllers (SBCs) and Session Initiation Protocol (SIP) trunks]. Direct Routing is the expected model, but proposals must clearly define what is being offered, including associated costs and SLAs. |

| Requirement | Specification |
|----------------------------------|--|
| Number Porting | Existing telephone numbers must be ported to the new solution without service interruption. The vendor must provide a cost for this. |
| Redundancy and Continuity | Telephony services must include redundancy (e.g., secondary SBCs, alternative PSTN routing) to ensure continuity in the event of primary link or equipment failure. |
| Call Quality and QoS | The solution must support enterprise-grade call quality, with Quality of Service (QoS) configured to prioritise voice traffic across the WAN/SD-WAN infrastructure. |
| Security | The service must support secure signalling and media encryption (e.g., TLS/SRTP), comply with CapeNature's firewall policies, and ensure telephony traffic is logged and monitored. All SIP signalling must be secured using TLS 1.2 or higher . All voice media streams must be secured using SRTP with AES-128/256 encryption . |
| Administration | Provide CapeNature ICT staff with administrative access to manage users, extensions, call policies, and reporting dashboards. Administrative portals must be accessible only via HTTPS (TLS 1.2+) with MFA for access. Certificates must be managed in line with industry best practices, with no use of self-signed certificates unless specifically approved by CapeNature. |
| Support & SLAs | 24/7 technical support must be provided, backed by SLAs covering call availability, response times, and resolution times. |
| Reporting | Monthly reports on call usage, quality metrics, outages, attempted fraud, and cost patterns must be provided. |
| Call Cost Optimization | The service must include cost control measures, such as preferential routes for local calls, international call rate management, fraud detection and prevention, and the ability to block or restrict high-cost destinations. |
| Scalability | The solution must be able to scale to support additional users, new sites, and integration with future collaboration platforms. |
| Cost Transparency | Bidders must provide a fully itemised cost breakdown for all telephony services, including Direct Routing or Calling Plan licensing, SBC hosting or integration, SIP trunk charges, number porting, call bundles, and support services. |
| No Undisclosed Charges | No additional or undisclosed telephony-related fees may be levied outside of those stated in the bid response. This includes but is not limited to activation fees, DID (Direct Inward Dial) allocation, international call surcharges, emergency services charges, or SLA penalties. |
| Lifecycle Costs | Pricing must account for the full lifecycle of the service, including any future number porting, licence renewals, and upgrades to SBCs or routing equipment. |

| Requirement | Specification |
|-------------------------------|---|
| Call Costs | All per-minute and per-destination call charges (local, national, mobile, and international) must be disclosed upfront, along with options for preferential routing, call bundles, and fraud-prevention mechanisms. |
| Future CRM Integration | It is a requirement that the vendor must have proven experience and capability to integrate the CapeNature selected CRM platform (when required). Note this is a future requirement, but CapeNature wants assurance that the vendor can support this. |
| Change Requests | Any charges relating to user additions, extension changes, call policy adjustments, or other administrative changes must be disclosed upfront with clear rate structures. |

Microsoft Teams Licensing Alignment

CapeNature's Microsoft 365 tenant is licensed primarily under Microsoft 365 E3 (Annexure 3_M365 Licenses) and related service plans. In order to enable Microsoft Teams Voice (Telephony Services), additional licensing is required to bring the current environment in line with Microsoft's telephony requirements.

Licensing Requirements

- a) **Microsoft Teams Phone Standard (Add-on):** Required for each user licensed with Microsoft 365 E3 (or equivalent). This licence enables PBX functionality within Teams, including voicemail, call transfer, auto-attendant, and call queues. The bidder must quote per license.
- b) **Microsoft 365 E5 Alternative:** Where cost-effective, bidders may propose upgrading selected users to Microsoft 365 E5, which includes Teams Phone and advanced security/compliance features. The bidder must quote per license.
- c) **Direct Routing Licenses:** Direct Routing licences using the provider's SIP trunks and Session Border Controllers (SBCs). Direct Routing is the preferred model for CapeNature. If other options are available, the bidder should quote for these as well, if they are cost effective listing the pros and cons of such a choice.

Bidders Must Provide

- a) A detailed review of CapeNature's current Microsoft 365 licensing and the gap to enable full Teams Voice functionality (refer to Annexure 3_M365 Licensing).
- b) A costed proposal for the following:
 - **Licensing uplift for all required users** (Teams Phone Standard add-on, or alternative E5 upgrades) Refer Annexure 3_M365 Licenses.
- c) A clear comparison of options (E3 + Phone System add-on vs. full E5), showing cost and functional differences.

- d) Confirmation that licence renewals will be billed annually, in line with CapeNature's financial planning cycle.

Deliverables

- a) Full alignment of Microsoft 365 licences to support Teams Voice.
- b) Transparent cost breakdown for **initial 12 months** (licences upfront) with annual renewal costs clearly disclosed.
- c) Clear differentiation between **per-user licensing** and **per-meeting room licensing**.

In addition, the bidder is also expected to provide a cost for additional devices to be used with MS Teams telephony. If there is a once-off licensing cost that needs to be purchased, this needs to be stated as a separate cost, together with renewal intervals (if required).

An example of devices that should be quoted on, is listed below. The bidder can use their discretion to identify further options. CapeNature will identify the options that best suits its requirements.

| Device Type | Specification | Cost Model |
|------------------------|--|---|
| Reception Phone | Enterprise-grade Teams-certified phone suitable for reception/front desk, supporting multiple lines, busy lamp field, call transfer and hold, with colour display. | Unit cost per device, itemised separately. |
| Executive Phone | Premium Teams-certified phone for executives, with touch display, video support, and advanced call handling features. | Unit cost per device, itemised separately. |
| Standard Phone | Standard Teams-certified desk phone with HD voice, basic display, and call transfer/hold functions for general staff use. | Unit cost per device, itemised separately. |
| Headsets (wired) | Teams-certified wired USB headset with noise-cancelling microphone and stereo audio, suitable for office staff. | Unit cost per headset, itemised separately. |
| Headsets (wireless/BT) | Teams-certified wireless/Bluetooth headset with noise-cancelling microphone and extended battery life, suitable for mobile or hybrid users. | Unit cost per headset, itemised separately. |

3.1.6. EXPRESSROUTE

CapeNature requires a secure and resilient Microsoft Azure ExpressRoute service to provide dedicated, high-performance connectivity between its on-premises network and Azure cloud environment. The solution must include a zone-redundant ExpressRoute gateway, with dual-circuit or equivalent failover mechanisms to ensure uninterrupted operations. Encryption must

be supported, and routing must follow best practices to restrict advertisements to only required prefixes.

The service must be delivered with bandwidth options of 50 Mbps and 100 Mbps (recommended for scalability), operate on an unmetered billing model, and include features for prioritised workloads. Monitoring must be enabled with proactive alerts and reporting available to CapeNature ICT staff. Transition from the existing ExpressRoute circuit must be carefully planned to minimise disruption to critical business workloads, with rollback procedures in place to ensure business continuity.

| Requirement | Specification |
|--|--|
| Service Type | Provide Microsoft Azure ExpressRoute for dedicated enterprise-grade connectivity between CapeNature's on-premises network and Azure cloud environment. |
| Location | The ExpressRoute circuit must terminate in South Africa. |
| Bandwidth Options | 50 Mbps and 100 Mbps. |
| Billing Model | Unmetered (unlimited data plan). |
| SKU | Standard SKU |
| Gateway | A high availability zone-redundant ExpressRoute Gateway |
| Redundancy & Continuity | Designs must include active/active or equivalent failover mechanisms to minimise downtime and ensure resilience. In addition, the vendor must also provide a cost-effective failover option, that limits downtime to a maximum of 5 minutes. |
| Encryption | The solution must support traffic encryption. The current ExpressRoute is not encrypted but the availability must be provided (and considered during implementation). |
| Routing | Border Gateway Protocol (BGP) must be used with best practice configuration. |
| Performance Features | ExpressRoute FastPath must be enabled to reduce latency and improve throughput. Quality of Service (QoS) must be implemented for prioritised workloads. |
| Alerts & Reporting | Real-time alerts, dashboards, and scheduled reports must be available, covering uptime, latency, and traffic utilisation. |
| Transition & Cutover | Migration from the existing ExpressRoute circuit must be carefully planned and executed with limited disruption. Full rollback procedures must be documented. |
| Support & SLAs | 24/7/365 technical support must be provided, backed by SLAs covering uptime, response, and resolution times. |
| Infrastructure & Other Hidden Costs | Bidders must provide a transparent cost breakdown, including installation, commissioning, ongoing support charges etc. |

4. SERVICE MANAGEMENT

4.1 Reporting and Governance

- A **Dedicated Service Delivery Manager (SDM)** must be assigned to CapeNature as the single point of contact for service management, escalation, and reporting. The SDM must ensure effective governance, communication, and quick resolution of service requests and incidents.
- The service provider must implement **comprehensive project and service governance structures**, including clear escalation paths, defined roles and responsibilities, and documented communication protocols.
- The bidder must ensure **full IT Service Management (ITSM) integration** into CapeNature's service desk environment, including:
 - Alignment with predefined ITIL-based service management processes (incident, problem, change, request, configuration, and escalation management).
 - End-to-end visibility of tickets raised, with CapeNature ICT staff having access to track, monitor, and escalate incidents in real time.
 - Integration of vendor service desk tools with CapeNature's ICT service desk platforms where supported.
 - Predefined SLAs and workflows embedded within the ITSM processes to ensure consistent response and resolution across all services.
- The preferred bidder must hold **monthly SLA review meetings** with CapeNature ICT, supported by detailed reporting on all contracted services. Reports must cover, at a minimum:
 - System availability and uptime per service, benchmarked against SLA thresholds.
 - Utilisation metrics across all services (bandwidth, voice traffic, APN usage, firewall activity, cloud interconnects, etc.).
 - Incident and fault reports, including response times, resolution times, and root cause analysis.
 - Security event reporting (including attempted breaches, anomalies, and suspicious traffic patterns).
 - Change activity logs (installs, moves, adds, changes, cancellations), with clear reference to the CapeNature Change Management process.
 - Monitoring metrics aligned to SLA compliance, allowing CapeNature to independently validate performance.
- Reports should (where feasible) be provided in two formats:

- **Real-time dashboard and portal access** for CapeNature ICT staff, offering drill-down visibility into utilisation, uptime, quality, and performance data.
- **Formal monthly governance reports** suitable for board, audit, and compliance purposes, including trend analysis and SLA compliance scoring.
- The service provider must also conduct **quarterly strategic service reviews**, focused on:
 - Capacity planning and anticipated growth requirements.
 - Service optimisation and technology refresh opportunities.
 - Risk reduction strategies, including security posture reviews and alignment with evolving governance standards.
 - Review of lessons learned from incidents and change activities to drive continuous improvement.
- **Audit trails and historical records** of all incidents, changes, and SLA compliance must be retained and made available for governance, compliance, and external audit purposes.

4.2 Documentation and Change Management

- All technical documentation, installation records, service configurations, and related materials must be provided to CapeNature before go-live.
- Any subsequent moves, adds, changes, or cancellations must be formally documented and submitted to CapeNature ICT for approval.
- The service provider must align to CapeNature's change management processes and ensure full visibility of all changes, irrespective what they are i.e., firewall, APN, connectivity etc.
- A full service inventory and asset register must be maintained and shared with CapeNature on a bi-annual basis.

4.3 Escalation Framework

The service provider must define and maintain a formal escalation framework, with responsibilities and accountabilities clearly specified at each level of escalation.

The framework must include named contacts, response and resolution timelines, and clear escalation paths up to senior management to ensure service issues are addressed within SLA commitments.

5. BUSINESS CONTINUITY

CapeNature operates multiple worksites (Annexure 2_Site List) across the Western Cape that rely on systems hosted both in the cloud and on-premises at the Cape Town Office. To maintain business continuity, the preferred bidder must provide a comprehensive system migration and continuity plan that ensures uninterrupted access to critical services during implementation, upgrades, or failover events. The plan must:

- Incorporate formal change management processes aligned with CapeNature's governance framework, including advance notification of changes, risk assessments, rollback procedures, and stakeholder communication. No changes may be implemented without prior approval from CapeNature ICT.
- Ensure that business operations are not negatively impacted during maintenance, upgrades, or unplanned outages. All migration or change activities must be scheduled outside of core business hours, unless explicitly approved by CapeNature ICT.

In addition, after go-live, the provider must ensure that:

- Any change in connection status (e.g., failover events, link degradation, outages, or service interruptions) automatically generate both email (to the CapeNature ServiceDesk), and SMS notifications to designated CapeNature ICT staff, ensuring timely awareness and response.
- Annual failover and continuity tests in collaboration with CapeNature ICT is conducted, to validate system resilience and the effectiveness of recovery processes. Test results must be formally documented, and recommendations for improvements must be implemented.

6. SUPPORT AND UPTIME

The Service Level Agreement (SLA) must cover all services provisioned under this bid (Connectivity, Firewall, APN, Telephony, ExpressRoute, and related managed services). The SLA must make provision for the following:

6.1 Minimum Connectivity Requirements

- A minimum of 30 Mbps of dedicated, uncontested internet access at each CapeNature worksite, as specified in the site connectivity list (Annexure 2_Site List). This bandwidth must be guaranteed 100% of the time.

- The service provider must propose the best available connectivity option per site (Annexure2_Site List). If the service provider cannot directly deliver services at certain locations, they must establish flexible alternative agreements with third-party providers, while retaining full accountability for management and performance on behalf of CapeNature.

6.2 Voice Services

Provision of appropriate and unlimited voice services through the Microsoft Teams telephony platform, with PSTN breakout, number porting, and QoS guarantees.

6.3 Support Availability

- 24/7/365 support across all services with direct contact details for fault reporting, incident response, and escalation.
- 24/7/365 proactive monitoring of all services, including internet, firewall, APN, ExpressRoute, and telephony.

6.4 Notifications and Alerts

Automated SMS and email notifications must be sent to CapeNature ICT staff for all errors, warnings, alarms, and service interruptions (planned or unplanned).

6.5 Incident and Fault Management

- Documented fault reporting procedures must be provided, including contact details and reporting channels.
- Documented incident response procedures must outline timelines, accountability, and resolution workflows.
- A formal escalation framework with named contacts, roles, and responsibilities must be included to ensure **accountability at each escalation level**.

6.6 Performance and Uptime Commitments

- The bidder must explicitly state and agree in the SLA the required uptime for all provisioned services, including internet, voice, APN, firewall, and cloud interconnects. The minimum acceptable standard is 99.8% availability per site (Annexure 2_Site List), measured on a monthly basis, but bidders are encouraged to propose higher levels aligned with Tier-1 provider standards.
- Response and resolution times for incidents and service requests must be defined by severity levels (e.g., Critical, Major, Minor) and must be strictly enforced. The bidder must provide clear commitments for each severity level, including escalation procedures where targets are not met.

- The SLA must include a detailed penalty mechanism for non-compliance with uptime and performance commitments. Bidders must propose a penalty framework, including:
 - How penalties will be calculated (e.g., percentage of monthly service fees, service credits, or other measurable mechanisms).
 - Differentiation of penalties by type of breach (e.g., uptime, response times, resolution times, SLA reporting failures).
 - Escalation provisions for repeated or severe breaches, including the possibility of contract termination for cause.
- All proposed commitments and penalty mechanisms must be transparent, auditable, and enforceable, ensuring that CapeNature can independently validate compliance through monitoring tools and governance processes.

6.7 Security and Compliance

- The preferred bidder will be expected to ensure CapeNature is protected against all security risks associated with the provided services.
- The service provider may be required to assist in the resolution of audit findings (e.g., remediation of identified security risks) at CapeNature's request.

6.8 Provider Coverage Transparency

- A list of internet and fibre providers available to the bidder must be submitted for CapeNature's review. This must indicate the range of services and geographical coverage and demonstrate alignment with CapeNature's site connectivity requirements.

7. EXPERIENCE AND QUALIFICATIONS

Interested bidders must demonstrate that they are recognised Tier-1 service providers within South Africa, with the capacity, infrastructure, and resources to deliver enterprise-grade services to CapeNature.

Bidders must provide clear evidence of the following:

7.1 Proven Experience – Network Solutions

Documented experience in designing, delivering, and supporting large-scale WAN, SD-WAN, APN, firewall, and telephony solutions for enterprise or public sector clients in South Africa.

7.2 Proven Experience – Managed Firewall Services

Demonstrable track record in managing hosted, dedicated next-generation firewalls, aligned to industry best practice and incorporating patch management, logging, and reporting capabilities.

7.3 Industry Certifications

Relevant industry and vendor certifications for personnel and solutions, including (but not limited to): Cisco, Fortinet, Microsoft, VMware, ITIL, ISO/IEC 27001, and equivalent Tier-1 certifications.

7.4 Client References and Case Studies

A minimum of four (4) client references and case studies from South African organisations of comparable size and complexity, where similar services have been successfully delivered. References must include scope of services, duration, and client contact details.

7.5 Financial Stability

Evidence of financial stability and sufficient resources to support long-term service commitments (minimum 5 years). This may include audited financial statements or equivalent documentation.

7.6 Local Presence and Capability

- Proof of national footprint and coverage to support CapeNature's distributed worksites (Annexure 2_Site List), including presence in rural areas of the Western Cape.
- Evidence of a 24/7/365 Network Operations Centre (NOC) and dedicated service management teams based in South Africa.

8. PROPOSAL REQUIREMENTS

Bidders should submit a proposal including:

- Company background and experience.
- Detailed approach to fulfilling the scope of work.
- Pricing model, including setup, one off costs, and monthly recurring costs, and any optional services.
- Service-Level agreements (SLAs) and performance guarantees.
- Implementation timeline, which includes plan to migrate from existing service provider

- Support and escalation procedures.
- Compliance with security and regulatory requirements.
- Indicate which services will be outsourced via 3rd party vendors

9. EVALUATION AND FUNCTIONALITY

Proposals will be evaluated based on the following and the functionality adherence

- Bidders will be required to present their proposal to the CapeNature Evaluation Committee (BEC).
- Technical capability and alignment with business needs.
- Registered Telecommunications Service Provider
- Cost-effectiveness and value for money.
- Quality of service and SLAs.
- Vendor experience and track record.
- Innovation and future-proofing capabilities.
- Customer support and responsiveness.

10. TERMS AND CONDITIONS

- CapeNature reserves the right to accept or reject any proposal.
- The selection process will involve interviews, presentations, or proof of c
- All costs related to proposal submission are the responsibility of the bidder.
- The selected partner will be required to sign a contract including confidentiality and data protection clauses.

11. COMPULSORY BRIEFING

Bidders will be required to join a compulsory virtual briefing session held on 6 October 2025 at 10:00 AM. Bidders need to RSVP on or before 12:00 PM on 3 October 2025 of their attendance for a virtual compulsory briefing session.

RSVP for virtual briefing session by 6 October 2025, please contact: Ms. Nwabisa Gqoboda: ngqoboda@capenature.co.za

Confirmed attendees will be provided with a link to join this virtual briefing session on the day of the briefing session.

12. REJECTION OF QUOTES/PROPOSAL

Any effort by a bidder to influence the bid evaluation, comparisons, or award decisions in any manner, may result in rejection of the bid. CapeNature shall reject a bid if the bidder has committed a proven corrupt or fraudulent act in competing for a particular contract.

CapeNature may disregard any bid if the bidder or any of its subcontractors:

- Is not tax compliant
- Have abused the Supply Chain Management (SCM) system of a department or any other government department, agency, or entity.
- Have committed proven fraud or any other improper conduct in relation to such system.
- Have failed to perform on any previous contract.
- Supplied incorrect information in the bid documentation.
- Not fully registered on the Central Supplier Database (CSD).
- Did not submit a valid Declaration of Interest.

13. DISCLAIMER

Details of the award will be published (on the e-tender portal/ other media) by CapeNature under National Treasury Instruction No. 1 of 2015/2016

FUNCTIONALITY CRITERIA - Bidders are required to score a minimum of 85% in order for their bids to be considered.

| No | Evaluation Criteria | Description | Weight (%) |
|------|---|---|------------|
| 1.1 | Network Coverage – National presence | Proof of national ISP footprint across SA. | 5 |
| 1.2 | Network Coverage – Regional/rural site coverage | Coverage of all CapeNature sites, including rural reserves (Annexure 2). | 5 |
| 1.3 | Network Availability – Uptime guarantees | Minimum uptime guarantee of 99.8%, per-site basis. | 5 |
| 2 | Bandwidth – Upgrade flexibility (scalability) | Seamless bandwidth upgrades across sites/cloud. | 5 |
| 3.1 | SLA – Uptime commitment | Uptime SLA commitments (≥99.8%). | 3 |
| 3.2 | SLA – Response/resolution times | Clear response/resolution times by severity. | 3 |
| 3.3 | SLA – Penalties & enforcement | Penalty mechanisms: credits, % of fees, escalation provisions. | 3 |
| 4.1 | Support – 24/7/365 monitoring | 24/7 proactive monitoring, alerts, dashboards. | 5 |
| 4.2 | Support – Service Delivery Manager (SDM) | Dedicated Service Delivery Manager as SPOC. | 5 |
| 4.3 | Support – ITIL/ITSM integration | Full ITIL/ITSM integration with CapeNature desk. | 5 |
| 5 | Latency & Performance | Average latency, jitter, packet loss, QoS prioritisation for critical workloads (voice, ExpressRoute, Azure cloud). | 5 |
| 6.1 | Security – Managed firewall (NGFW, UTM, VPN) | Enterprise NGFW: IPS/IDS, UTM, VPN, DLP, logging. | 5 |
| 6.2 | Security – APN security & SIM controls | Corporate APN: SIM binding, authentication, traffic inspection. | 5 |
| 6.3 | Security – Telephony/Teams Voice security | Teams Voice: TLS/SRTP, secure SBCs, fraud prevention. | 5 |
| 7.1 | Redundancy – WAN/LTE failover | Dual WAN links, LTE/wireless backup ≥100 Mbps. | 3 |
| 7.2 | Redundancy – ExpressRoute dual-circuit | ExpressRoute: zone-redundant gateway, dual-circuit failover. | 3 |
| 8 | References – Comparable case studies | Comparable public-sector/enterprise deployments. | 5 |
| 9 | Transition – Migration/rollback planning | Transition plan with phased migration & rollback. | 5 |
| 10.1 | Value-Added – APN portal & reporting | Secure APN portal with SIM control, usage reports. | 5 |
| 10.2 | Value-Added – Teams Voice/CRM integration | MS Teams Voice integration, CRM-readiness, cost optimisation. | 1 |
| 11.1 | Compliance – ISO/IEC 27001, POPIA, GDPR | Compliance coverage explained and certified | 2 |
| 11.2 | Compliance – Vendor/industry certifications | Vendor staff certs (Cisco, Fortinet, Microsoft, ITIL). | 2 |
| 12.1 | Proposal – Technical completeness | Clear mapping to tender requirements, structured response. | 7 |
| 12.2 | Proposal – Cost transparency | Transparent cost breakdown: hardware, licences, SLA, support. | 2 |
| 13 | Innovation – Future connectivity (5G/fibre) | Future-proof: 5G, fibre expansion, cloud-native readiness. | 1 |

Annexure 1 - APN

| APN Subscriber Summary | | |
|------------------------|---------------------|--------------|
| Usage Month: | Aug-25 | |
| capenature | | |
| Subscriber No | Package | Total Usage |
| CN1 | Vodacom APN Connect | 28 695,77 MB |
| CN2 | Vodacom APN Connect | 27 276,23 MB |
| CN3 | Vodacom APN Connect | 19 390,43 MB |
| CN4 | Vodacom APN Connect | 19 089,12 MB |
| CN5 | Vodacom APN Connect | 15 537,85 MB |
| CN6 | Vodacom APN Connect | 12 308,44 MB |
| CN7 | Vodacom APN Connect | 12 243,66 MB |
| CN8 | Vodacom APN Connect | 10 440,75 MB |
| CN9 | Vodacom APN Connect | 9 811,87 MB |
| CN10 | Vodacom APN Connect | 9 067,01 MB |
| CN11 | Vodacom APN Connect | 8 374,24 MB |
| CN12 | Vodacom APN Connect | 6 997,23 MB |
| CN13 | Vodacom APN Connect | 5 860,77 MB |
| CN14 | Vodacom APN Connect | 5 470,84 MB |
| CN15 | Vodacom APN Connect | 5 344,91 MB |
| CN16 | Vodacom APN Connect | 5 199,37 MB |
| CN17 | Vodacom APN Connect | 5 064,44 MB |
| CN18 | Vodacom APN Connect | 4 413,80 MB |
| CN19 | Vodacom APN Connect | 4 316,69 MB |
| CN20 | Vodacom APN Connect | 4 226,48 MB |
| CN21 | Vodacom APN Connect | 4 145,63 MB |
| CN22 | Vodacom APN Connect | 3 897,16 MB |
| CN23 | Vodacom APN Connect | 3 705,36 MB |
| CN24 | Vodacom APN Connect | 3 600,78 MB |
| CN25 | Vodacom APN Connect | 3 329,15 MB |
| CN26 | Vodacom APN Connect | 3 293,52 MB |
| CN27 | Vodacom APN Connect | 3 219,63 MB |
| CN28 | Vodacom APN Connect | 3 099,39 MB |
| CN29 | Vodacom APN Connect | 3 017,61 MB |
| CN30 | Vodacom APN Connect | 2 891,57 MB |
| CN31 | Vodacom APN Connect | 2 823,12 MB |
| CN32 | Vodacom APN Connect | 2 765,58 MB |
| CN33 | Vodacom APN Connect | 2 541,84 MB |
| CN34 | Vodacom APN Connect | 2 513,98 MB |
| CN35 | Vodacom APN Connect | 2 507,82 MB |
| CN36 | Vodacom APN Connect | 2 408,91 MB |
| CN37 | Vodacom APN Connect | 2 308,75 MB |
| CN38 | Vodacom APN Connect | 2 245,32 MB |
| CN39 | Vodacom APN Connect | 2 188,38 MB |
| CN40 | Vodacom APN Connect | 2 152,70 MB |

| | | |
|------|---------------------|-------------|
| CN41 | Vodacom APN Connect | 2 129,78 MB |
| CN42 | Vodacom APN Connect | 2 116,79 MB |
| CN43 | Vodacom APN Connect | 2 114,36 MB |
| CN44 | Vodacom APN Connect | 1 955,02 MB |
| CN45 | Vodacom APN Connect | 1 927,74 MB |
| CN46 | Vodacom APN Connect | 1 758,47 MB |
| CN47 | Vodacom APN Connect | 1 696,04 MB |
| CN48 | Vodacom APN Connect | 1 587,90 MB |
| CN49 | Vodacom APN Connect | 1 519,60 MB |
| CN50 | Vodacom APN Connect | 1 494,63 MB |
| CN51 | Vodacom APN Connect | 1 445,99 MB |
| CN52 | Vodacom APN Connect | 1 440,17 MB |
| CN53 | Vodacom APN Connect | 1 352,54 MB |
| CN54 | Vodacom APN Connect | 1 335,92 MB |
| CN55 | Vodacom APN Connect | 1 326,21 MB |
| CN56 | Vodacom APN Connect | 1 131,39 MB |
| CN57 | Vodacom APN Connect | 1 102,86 MB |
| CN58 | Vodacom APN Connect | 1 040,28 MB |
| CN59 | Vodacom APN Connect | 1 030,89 MB |
| CN60 | Vodacom APN Connect | 1 006,45 MB |
| CN61 | Vodacom APN Connect | 976,10 MB |
| CN62 | Vodacom APN Connect | 940,86 MB |
| CN63 | Vodacom APN Connect | 910,24 MB |
| CN64 | Vodacom APN Connect | 859,57 MB |
| CN65 | Vodacom APN Connect | 836,93 MB |
| CN66 | Vodacom APN Connect | 805,12 MB |
| CN67 | Vodacom APN Connect | 748,39 MB |
| CN68 | Vodacom APN Connect | 744,71 MB |
| CN69 | Vodacom APN Connect | 725,67 MB |
| CN70 | Vodacom APN Connect | 721,94 MB |
| CN71 | Vodacom APN Connect | 669,40 MB |
| CN72 | Vodacom APN Connect | 658,16 MB |
| CN73 | Vodacom APN Connect | 643,05 MB |
| CN74 | Vodacom APN Connect | 637,10 MB |
| CN75 | Vodacom APN Connect | 631,83 MB |
| CN76 | Vodacom APN Connect | 570,82 MB |
| CN77 | Vodacom APN Connect | 568,96 MB |
| CN78 | Vodacom APN Connect | 568,96 MB |
| CN79 | Vodacom APN Connect | 562,30 MB |
| CN80 | Vodacom APN Connect | 538,36 MB |
| CN81 | Vodacom APN Connect | 526,87 MB |
| CN82 | Vodacom APN Connect | 490,15 MB |
| CN83 | Vodacom APN Connect | 474,17 MB |
| CN84 | Vodacom APN Connect | 472,14 MB |

| | | |
|-------|-----------------------------|-----------|
| CN85 | Vodacom APN Connect | 462,30 MB |
| CN86 | Vodacom APN Connect | 461,00 MB |
| CN87 | Vodacom APN Connect | 438,11 MB |
| CN88 | Vodacom APN Connect | 385,45 MB |
| CN89 | Vodacom APN Connect | 367,82 MB |
| CN90 | Vodacom APN Connect | 365,88 MB |
| CN91 | Vodacom APN Connect | 364,44 MB |
| CN92 | Vodacom APN Connect | 353,28 MB |
| CN93 | Vodacom APN Connect | 336,78 MB |
| CN94 | Vodacom APN Connect | 312,11 MB |
| CN95 | Vodacom APN Connect | 299,68 MB |
| CN96 | Vodacom APN Connect | 284,40 MB |
| CN97 | Vodacom APN Connect | 282,58 MB |
| CN98 | Vodacom APN Connect | 281,87 MB |
| CN99 | Vodacom APN Connect | 274,70 MB |
| CN100 | Vodacom APN Connect | 269,61 MB |
| CN101 | Vodacom APN Connect | 245,20 MB |
| CN102 | Vodacom APN Connect | 240,95 MB |
| CN103 | Vodacom APN Connect | 233,74 MB |
| CN104 | Vodacom APN Connect | 213,98 MB |
| CN105 | Vodacom APN Connect | 199,18 MB |
| CN106 | Vodacom APN Connect | 197,32 MB |
| CN107 | Vodacom APN Connect | 186,42 MB |
| CN108 | Vodacom APN Connect | 175,59 MB |
| CN109 | Vodacom APN Connect | 150,14 MB |
| CN110 | Vodacom APN Connect | 130,69 MB |
| CN111 | Vodacom APN Connect | 114,09 MB |
| CN112 | Vodacom APN Connect | 112,23 MB |
| CN113 | Vodacom APN Connect | 108,56 MB |
| CN114 | Vodacom APN Connect | 107,12 MB |
| CN115 | Vodacom APN Connect | 100,88 MB |
| CN116 | Vodacom APN Connect | 97,84 MB |
| CN117 | Vodacom APN Connect | 95,54 MB |
| CN118 | Vodacom APN Connect | 88,62 MB |
| CN119 | Vodacom APN Connect | 79,35 MB |
| CN120 | Vodacom APN Connect | 64,88 MB |
| CN121 | Vodacom APN Connect | 46,73 MB |
| CN122 | RED 1.4GB 100min TopUp Plan | 44,51 MB |
| CN123 | Vodacom APN Connect | 37,84 MB |
| CN124 | Vodacom APN Connect | 33,98 MB |
| CN125 | Vodacom APN Connect | 33,42 MB |
| CN126 | Vodacom APN Connect | 32,23 MB |
| CN127 | Vodacom APN Connect | 17,13 MB |
| CN128 | Vodacom APN Connect | 16,77 MB |

| CN129 | Vodacom APN Connect | 11,55 MB |
|----------------------|-----------------------------|--------------------|
| CN130 | Vodacom APN Connect | 10,67 MB |
| CN131 | Vodacom APN Connect | 10,07 MB |
| CN132 | Vodacom APN Connect | 7,90 MB |
| CN133 | Vodacom APN Connect | 5,59 MB |
| CN134 | Vodacom APN Connect | 2,54 MB |
| CN135 | Vodacom APN Connect | 0,93 MB |
| CN136 | Vodacom APN Connect | 0,91 MB |
| CN137 | Vodacom APN Connect | 0,32 MB |
| CN138 | Vodacom APN Connect | 0,25 MB |
| CN139 | Vodacom APN Connect | 0,16 MB |
| CN140 | Vodacom APN Connect | 0,13 MB |
| CN141 | Vodacom APN Connect | 0,04 MB |
| CN142 | Vodacom APN Connect | 0,02 MB |
| CN143 | Vodacom APN Connect | 0,00 MB |
| CN144 | Vodacom APN Connect | 0,00 MB |
| CN145 | Vodacom APN Connect | 0,00 MB |
| internet | | |
| Subscriber No | Package | Total Usage |
| CN146 | Vodacom APN Connect | 13 749,85 MB |
| CN147 | RED 1.4GB 100min TopUp Plan | 2 755,38 MB |
| CN148 | RED 1.4GB 100min TopUp Plan | 2 210,44 MB |
| CN149 | RED 1.4GB 100min TopUp Plan | 2 000,60 MB |
| CN150 | RED 1.4GB 100min TopUp Plan | 1 930,85 MB |
| CN151 | RED 1.4GB 100min TopUp Plan | 1 817,62 MB |
| CN152 | RED 1.4GB 100min TopUp Plan | 1 676,99 MB |
| CN153 | RED 1.4GB 100min TopUp Plan | 1 670,51 MB |
| CN154 | RED 1.4GB 100min TopUp Plan | 1 540,23 MB |
| CN155 | RED 1.4GB 100min TopUp Plan | 1 477,51 MB |
| CN156 | RED 1.4GB 100min TopUp Plan | 1 465,44 MB |
| CN157 | RED 1.4GB 100min TopUp Plan | 1 442,00 MB |
| CN158 | RED 1.4GB 100min TopUp Plan | 1 441,96 MB |
| CN159 | RED 1.4GB 100min TopUp Plan | 1 438,06 MB |
| CN160 | RED 1.4GB 100min TopUp Plan | 1 437,89 MB |
| CN161 | RED 1.4GB 100min TopUp Plan | 1 393,75 MB |
| CN162 | RED 1.4GB 100min TopUp Plan | 1 388,37 MB |
| CN163 | RED 1.4GB 100min TopUp Plan | 1 304,07 MB |
| CN164 | RED 1.4GB 100min TopUp Plan | 1 070,49 MB |
| CN165 | RED 1.4GB 100min TopUp Plan | 1 019,73 MB |
| CN166 | RED 1.4GB 100min TopUp Plan | 990,04 MB |
| CN167 | RED 1.4GB 100min TopUp Plan | 922,21 MB |
| CN168 | RED 1.4GB 100min TopUp Plan | 914,41 MB |
| CN169 | RED 1.4GB 100min TopUp Plan | 821,14 MB |
| CN170 | RED 1.4GB 100min TopUp Plan | 808,14 MB |

| CN171 | RED 1.4GB 100min TopUp Plan | 691,26 MB |
|----------------|-----------------------------|-------------|
| CN172 | RED 1.4GB 100min TopUp Plan | 645,26 MB |
| CN173 | RED 1.4GB 100min TopUp Plan | 513,03 MB |
| CN174 | RED 1.4GB 100min TopUp Plan | 395,95 MB |
| CN175 | Vodacom APN Connect | 282,40 MB |
| CN176 | RED 1.4GB 100min TopUp Plan | 267,26 MB |
| CN177 | RED 1.4GB 100min TopUp Plan | 258,32 MB |
| CN178 | RED 1.4GB 100min TopUp Plan | 232,81 MB |
| CN179 | RED 1.4GB 100min TopUp Plan | 211,94 MB |
| CN180 | RED 1.4GB 100min TopUp Plan | 180,55 MB |
| lte.vodacom.za | | |
| Subscriber No | Package | Total Usage |
| CN181 | RED 1.4GB 100min TopUp Plan | 5 196,39 MB |
| CN182 | RED 1.4GB 100min TopUp Plan | 2 908,36 MB |
| CN183 | RED 1.4GB 100min TopUp Plan | 2 242,15 MB |
| CN184 | RED 1.4GB 100min TopUp Plan | 1 289,97 MB |
| CN185 | RED 1.4GB 100min TopUp Plan | 74,22 MB |
| CN186 | RED 1.4GB 100min TopUp Plan | 31,05 MB |
| CN187 | PC2022_SRS_Smart S+ | 9,66 MB |
| vlive | | |
| Subscriber No | Package | Total Usage |
| CN188 | RED 1.4GB 100min TopUp Plan | 886,15 MB |

Annexure 2 - Site List

| | Priority | Site Name | Endpoints | Device | Fibre | Vsat | MW | LTE Failover | Speed | | SLA/Response | SLA/Resolution | Latitude | Longitude | Comments |
|----|----------|-----------------------------------|-----------|--------|-------|------|----|--------------|---------|----------------|--------------|----------------|---------------|---------------|--|
| | | | | | | | | | Current | New /Suggested | | | | | |
| 1 | | ANYNSBERG NATURE RESERVE | 6 | MX64 | | X | | | 20mbps | 30 | 2hrs | 12hrs | 33°27'49.38"S | 20°35'18.28"E | |
| 2 | | BIRD ISLAND NATURE RESERVE | 4 | MX64 | | | X | X | 20mbps | 30 | 2hrs | 12hrs | 32°5'25.23"S | 18°18'12.32"E | Alternative solution to be recommended |
| 3 | | CEDERBERG WILDERNESS ALGERIA | 9 | MX64 | | | X | X | 20mbps | 50 | 2hrs | 12hrs | 32°22'28.53"S | 19°3'36.57"E | |
| 4 | | DASSEN ISLAND NATURE RESERVE | 2 | MX64 | | | X | X | 20mbps | 30 | 2hrs | 12hrs | 33°25'10.22"S | 18°5'2'22"E | |
| 5 | | DCCP NATURE RESERVE | 8 | MX64 | | | X | X | 20mbps | 30 | 2hrs | 12hrs | 33°30'48.20"S | 18°28'35.15"E | |
| 6 | | DE HOOP NATURE RESERVE | 13 | MX64 | | | X | X | 20mbps | 30 | 2hrs | 12hrs | 34°22'28.87"S | 20°32'0.81"E | |
| 7 | | DE MOND NATURE RESERVE | 6 | | | X | | | 20mbps | 30 | 2hrs | 12hrs | 34°42'38.69"S | 20°6'17.84"E | Alternative solution to be recommended, not cyrrently on SDWAN |
| 8 | | DYER ISLAND NATURE RESERVE | 1 | | | | X | | 20mbps | 30 | 2hrs | 12hrs | 34°40'49.22"S | 19°25'10.04"E | Not on SDWAN - will need to be migrated |
| 9 | | GAMKABERG NATURE RESERVE | 8 | MX64 | | X | | X | 20mbps | 30 | 2hrs | 12hrs | 33°40'15.33"S | 21°53'19.53"E | Alternative solution to be recommended |
| 10 | | GAMKASKLOOF OU PLAAS | 2 | MX64 | | X | | | 20mbps | 30 | 2hrs | 12hrs | 33°21'44.68"S | 21°37'25.18"E | Alternative solution to be recommended |
| 11 | | GEELKRANS NATURE RESERVE | 5 | MX64 | | | X | X | 20mbps | 30 | 2hrs | 12hrs | 34°22'37.30"S | 21°24'40.28"E | |
| 12 | HIGH | GEORGE REGIONAL OFFICE | 17 | MX64 | | | X | X | 50mbps | 50 | 2hrs | 12hrs | 33°57'36.50"S | 22°27'16.19"E | |
| 13 | | GOUKAMMA NATURE RESERVE | 7 | MX64 | | X | | X | 20mbps | 30 | 2hrs | 12hrs | 34°3'51.19"S | 22°56'33.52"E | Alternative solution to be recommended |
| 14 | | GROOTVADERSBOSCH | 10 | MX64 | | X | | X | 20mbps | 30 & 50 mbps | 2hrs | 12hrs | 33°59'7.92"S | 20°49'24.33"E | Alternative solution to be recommended |
| 15 | | GROOTWINTERHOEK NATURE RESERVE | 7 | MX64 | | X | | | 20mbps | 30 | 2hrs | 12hrs | 32°59'54.37"S | 19°3'23.41"E | Alternative solution to be recommended |
| 16 | HIGH | HEAD OFFICE CAPE TOWN - Fibre | 146 | | X | | X | | 200mbps | 200 | 2hrs | 12hrs | 33°57'30.42"S | 19°3'23.36"E | |
| 17 | | HOTTENTOTS HOLLAND NATURE RESERVE | 14 | MX64 | | | X | X | 20mbps | 30 | 2hrs | 12hrs | 34°4'18.34"S | 19°2'55.66"E | |
| 18 | | JONKERSHOEK NATURE RESERVE | 23 | MX64 | | | X | X | 20mbps | 30 | 2hrs | 12hrs | 33°58'0.33"S | 18°55'24.93"E | |
| 19 | | KAMMANASSIE NATURE RESERVE | 6 | MX64 | | | X | X | 20mbps | 30 | 2hrs | 12hrs | 33°39'11.36"S | 23°7'47.64"E | |
| 20 | | KEURBOOMS RIVER NATURE RESERVE | 9 | MX64 | X | | | X | 20mbps | 30 | 2hrs | 12hrs | 34°2'41.50"S | 23°22'6.52"E | |
| 21 | | KNERSVLAKTE NATURE RESERVE | 13 | MX64 | | | X | X | 50mbps | 30 | 2hrs | 12hrs | 31°36'28.44"S | 18°44'24.93"E | |
| 22 | | KOGELBERG NATURE RESERVE | 10 | MX64 | | X | | | 20mbps | 50 | 2hrs | 12hrs | 34°19'23.28"S | 18°58'1.40"E | Alternative solution to be recommended |
| 23 | | KOGELBERG NATURE STONY POINT | 7 | MX64 | | | | X | 20mbps | 30 | 2hrs | 12hrs | 34°22'20.12"S | 18°53'31.96"E | |
| 24 | | LIMIETBERG NATURE RESERVE | 21 | MX64 | | | X | X | 20mbps | 30 | 2hrs | 12hrs | 33°43'42.26"S | 18°57'30.91"E | |
| 25 | | MARLOTH NATURE RESERVE | 11 | MX64 | | | X | X | 20mbps | 30 | 2hrs | 12hrs | 34°0'21.69"S | 20°26'26.28"E | |
| 26 | | MATJIESRIVIER NATURE RESERVE | 4 | MX64 | | X | | | 20mbps | | 2hrs | 12hrs | 32°30'0.68"S | 19°20'9.85"E | Alternative solution to be recommended |
| 27 | | OUTENIQUA NATURE RESERVE | 11 | MX64 | | | X | X | 50mbps | 30 | 2hrs | 12hrs | 33°56'8.00"S | 22°25'38.11"E | |
| 28 | HIGH | PORTERVILLE REGIONAL OFFICE | 14 | MX64 | X | | | X | 50mbps | 50 | 2hrs | 12hrs | 33°0'22.33"S | 18°59'37.14"E | |
| 29 | | RIVERLANDS NATURE RESERVE | 6 | MX64 | | | X | | 20mbps | 30 | 2hrs | 12hrs | 33°29'24.49"S | 18°36'53.97"E | |
| 30 | | RIVERSDALE OFFICE | 2 | MX64 | | | X | X | 20mbps | 30 | 2hrs | 12hrs | 34°5'0.71"S | 21°15'9.56"E | |
| 31 | | ROCHERPAN NATURE RESERVE | 5 | MX64 | | | X | X | 20mbps | 30 | 2hrs | 12hrs | 32°36'53.07"S | 18°18'5.61"E | |
| 32 | | RUITERBOS | 2 | MX64 | | | X | X | 20mbps | 30 | 2hrs | 12hrs | 33°54'52.56"S | 22°1'46.63"E | |
| 33 | | SWARTBERG NATURE RESERVE | 23 | MX64 | | | X | X | 20mbps | 30 | 2hrs | 12hrs | 33°35'29.28"S | 22°12'7.25"E | |
| 34 | | TWEEDETOL NATURE RESERVE | 1 | MX64 | | X | | | 20mbps | 30 | 2hrs | 12hrs | 33°34'12.75"S | 19°8'18.20"E | Alternative solution to be recommended |
| 35 | | VROLIKHEID OFFICE COMPLEX | 16 | MX64 | | | X | X | 20mbps | 30 | 2hrs | 12hrs | 33°55'5.62"S | 19°52'35.03"E | |
| 36 | | WALKER BAY NATURE RESERVE | 28 | MX64 | X | | | X | 50mbps | 30 | 2hrs | 12hrs | 34°24'46.19"S | 19°18'1.62"E | |
| 37 | | WATERVAL NATURE RESERVE | 12 | MX64 | | | X | X | 20mbps | 30 | 2hrs | 12hrs | 33°20'56.45"S | 19°6'39.44"E | |
| 38 | | WOLWEKLOOF | 5 | | | | X | | 20mbps | 30 | 2hrs | 12hrs | 33°25'48.22"S | 19°16'20.12"E | Not on SDWAN - will need to be migrated |
| 39 | | KLIIPHUIS | 2 | | | | | | | 30 | 2hrs | 12hrs | 32°8'7.83"S | 19°0'13.42"E | Alternative solution to be recommended |
| 40 | | DEKELDERS | 2 | | | | | | | 30 | 2hrs | 12hrs | 34°32'47.10"S | 19°22'41.10"E | Alternative solution to be recommended |
| 41 | | GRAND CANYON | 2 | | | | | | | 30 | 2hrs | 12hrs | 33°25'56.94"S | 20°47'45.40"E | Alternative solution to be recommended |
| 42 | | WOLWEKLOOF GATE HOUSE | 2 | | | | | | | 30 | 2hrs | 12hrs | 33°25'34.58"S | 19°16'6.34"E | Alternative solution to be recommended |
| 43 | | GOUKAMMA WELCOME CENTRE - NEW | 2 | | | | | | | 30 | 2hrs | 12hrs | 34°3'55.51"S | 22°56'37.11"E | Alternative solution to be recommended |

Annexure 3 - M365 Licences

| Product Title | Total Licenses | Expired Licenses | Assigned licenses |
|------------------------------------|----------------|------------------|-------------------|
| Microsoft 365 E3 | 550 | 0 | 548 |
| Microsoft 365 E5 | 25 | 0 | 20 |
| Microsoft 365 E5 Security | 550 | 0 | 546 |
| Microsoft Fabric (Free) | 1,000,000 | 0 | 19 |
| Microsoft Power Apps Plan 2 Trial | 10,000 | 0 | 3 |
| Microsoft Power Apps for Developer | 10,000 | 0 | 1 |
| Microsoft Power Automate Free | 10,000 | 0 | 288 |
| Microsoft Stream Trial | 1,000,000 | 0 | 2 |
| Planner and Project Plan 5 | 1 | 0 | 1 |
| Teams Premium (for Departments) | 4 | 0 | 4 |
| Visio Plan 1 | 3 | 0 | 3 |
| Visio Plan 2 | 1 | 0 | 0 |
| | | | |

Annexure 4 - CapeNature Usage

| Model | Name | Network | Clients | Usage | Contacted at | Configuration status |
|---------|-----------------------------------|-----------------------------------|---------|-----------|----------------|-------------------------------|
| MX64 | GAMKABERG NATURE RESERVE | GAMKABERG NATURE RESERVE | 16 | 42.44 GB | 2 minutes ago | Up to date |
| MX64 | SWARTBERG NATURE RESERVE | SWARTBERG NATURE RESERVE | 53 | 132.58 GB | 41 seconds ago | Up to date |
| MX64 | ANYSBURG NATURE RESERVE | ANYSBURG NATURE RESERVE | 12 | 30.95 GB | 2 minutes ago | Up to date |
| MX64 | ASSEGAIBOSCH NATURE RESERVE | ASSEGAIBOSCH NATURE RESERVE | 44 | 79.97 GB | 2 minutes ago | Up to date |
| VMX-S | AZURE - CAPENATUREVmx | AZURE - CAPENATUREVmx | 0 | None | 8.1 months ago | Dormant |
| MX64 | Bird Island Nature Reserve | BIRD ISLAND NATURE RESERVE | 9 | 27.34 GB | 2 minutes ago | Up to date |
| MX64 | CEDERBERG WILDERNESS ALGERIA | CEDERBERG WILDERNESS ALGERIA | 23 | 114.22 GB | 48 seconds ago | Up to date |
| MX84 | CFO - Secondary | CFO HOSTING CENTRE | 0 | None | 36 seconds ago | Up to date |
| MX84 | CFO HOSTING CENTER | CFO HOSTING CENTRE | 1 | 2.96 TB | 35 seconds ago | Up to date |
| MX64 | DASSEN ISLAND NATURE RESERVE | DASSEN ISLAND NATURE RESERVE | 2 | 568.2 MB | 80 seconds ago | Up to date |
| MX64 | DCCP NATURE RESERVE | DCCP NATURE RESERVE | 13 | 32.97 GB | 28 seconds ago | Up to date |
| MX64 | DE HOOP NATURE RESERVE | DE HOOP NATURE RESERVE | 84 | 76.76 GB | 2 minutes ago | Up to date |
| MX64 | GEORGE | GEORGE | 58 | 81.96 GB | 74 seconds ago | Up to date |
| MX64 | GOUKAMMA NATURE RESERVE | GOUKAMMA NATURE RESERVE | 14 | 42.74 GB | 58 seconds ago | Up to date |
| MX64 | GROOTVADERSBOSCH | GROOTVADERSBOSCH | 28 | 46.88 GB | 2 minutes ago | Up to date |
| MX64 | GROOTWINTERHOEK NATURE RESERVE | GROOTWINTERHOEK NATURE RESERVE | 12 | 20.65 GB | 81 seconds ago | Up to date |
| MX64 | Gamkaskloof Nature Reserve | Gamkaskloof Nature Reserve | 0 | None | 52 days ago | Up to date |
| MX64 | Geelkrans Nature Reserve | Geelkrans Nature Reserve | 8 | 29.79 GB | 40 seconds ago | Up to date |
| MX95 | HEAD OFFICE - PRIMARY | HEAD OFFICE | 3 | 927.39 GB | 82 seconds ago | Up to date |
| MS120-8 | HEAD OFFICE - PRIMARY SWITCH | HEAD OFFICE | 4 | 1.45 TB | 2 minutes ago | Up to date |
| MX95 | HEAD OFFICE - SECONDARY | HEAD OFFICE | 0 | None | 2 minutes ago | Up to date |
| MS120-8 | HEAD OFFICE - SECONDARY SWITCH | HEAD OFFICE | 4 | 1.42 TB | 2 minutes ago | Up to date |
| MX64 | HOTTENTOTS HOLLAND NATURE RESERVE | HOTTENTOTS HOLLAND NATURE RESERVE | 25 | 62.68 GB | 34 seconds ago | Up to date |
| MX64 | KAMMANASSIE NATURE RESERVE | KAMMANASSIE NATURE RESERVE | 44 | 57.02 GB | 31 seconds ago | Up to date |
| MX64 | KEURBOOMS RIVER NATURE RESERVE | KEURBOOMS RIVER NATURE RESERVE | 16 | 46.46 GB | 87 seconds ago | Up to date |
| MX64 | KNERSVLAKTE NATURE RESERVE | KNERSVLAKTE NATURE RESERVE | 28 | 59.04 GB | 31 seconds ago | Up to date |
| MX64 | KOGELBERG STONY POINT | KOGELBERG STONY POINT | 13 | 84.42 GB | 2 minutes ago | Up to date |
| MX64 | Koegelberg Nature Reserve | KOEGELBURG NATURE RESERVE | 101 | 69.08 GB | 81 seconds ago | Up to date |
| MX64 | LIMIETBERG NATURE RESERVE | LIMIETBERG NATURE RESERVE | 69 | 122.83 GB | 2 minutes ago | Up to date |
| MX64 | MARLOTH NATURE RESERVE | MARLOTH NATURE RESERVE | 20 | 79.15 GB | 76 seconds ago | Up to date |
| MX64 | MATJIESRIVIER NATURE RESERVE | MATJIESRIVIER NATURE RESERVE | 38 | 91.14 GB | 73 seconds ago | Up to date |
| MX64 | OUTENIQUA NATURE RESERVE | OUTENIQUA NATURE RESERVE | 24 | 67.18 GB | 61 seconds ago | Up to date |
| MX64 | PORTERVILLE REGIONAL OFFICE | PORTERVILLE REGIONAL OFFICE | 35 | 105.87 GB | 72 seconds ago | Up to date |
| MX64 | RIVERLANDS NATURE RESERVE | RIVERLANDS NATURE RESERVE | 29 | 52.90 GB | 38 seconds ago | Up to date |
| MX64 | RIVERSDALE | RIVERSDALE | 6 | 9.87 GB | 33 seconds ago | Up to date |
| MX64 | ROCHERPAN NATURE RESERVE | ROCHERPAN NATURE RESERVE | 15 | 41.07 GB | 28 seconds ago | Up to date |
| MX64 | Ruiterbos Nature Reserve | Ruiterbos Nature Reserve | 6 | 3.55 GB | 73 seconds ago | Up to date |
| MX64 | TWEEDE TOL | TWEEDE TOL | 0 | None | 3.1 months ago | Vandalized, currently offline |

| | | | | | | |
|------|----------------------------|----------------------------|----|-----------|----------------|------------|
| MX64 | VROLIJKHEID OFFICE COMPLEX | VROLIJKHEID OFFICE COMPLEX | 70 | 79.46 GB | 89 seconds ago | Up to date |
| MX64 | WALKER BAY NATURE RESERVE | WALKER BAY NATURE RESERVE | 81 | 174.14 GB | 68 seconds ago | Up to date |
| MX64 | WATERVAL NATURE RESERVE | WATERVAL NATURE RESERVE | 23 | 60.21 GB | 76 seconds ago | Up to date |

| Firewall Specifications | |
|---|--|
| The firewall environment must be: | |
| <ul style="list-style-type: none"> Configured in Active-Passive Mode to ensure redundancy and continuity of service in the event of a device failure. | |
| <ul style="list-style-type: none"> Hosted in Shared Rack Space in the CapeNature private cloud. | |
| <ul style="list-style-type: none"> Fully Redundant, and support for high availability to minimise downtime. | |
| a) Security Features and VPN | |
| <ul style="list-style-type: none"> Firewall rules and security policies must safeguard both voice and data traffic. | |
| <ul style="list-style-type: none"> The firewall must support the configuration of site-to-site VPNs, client VPNs, and secure remote access for telephony and other corporate services. | |
| <ul style="list-style-type: none"> VPN services must enforce strong encryption, multi-factor authentication, and role-based access control. | |
| b) Logging, Retention, and Reporting | |
| <ul style="list-style-type: none"> Logging capabilities must support advanced analysis and forensic investigation. | |
| <ul style="list-style-type: none"> Access and Change Logs must be retained for a minimum of 12 months. | |
| <ul style="list-style-type: none"> Rule Processing Logs must be stored for at least 2 weeks. | |
| <ul style="list-style-type: none"> Proxy Logs must be retained for a minimum of 2 months to support reporting requirements. | |
| The firewall solution must provide: | |
| <ul style="list-style-type: none"> Monthly browsing reports covering usage trends, top sites, categories, and anomalies. | |
| <ul style="list-style-type: none"> Weekly summary reports highlighting user activity, browsing categories, and security events. | |
| <ul style="list-style-type: none"> Alerts and reports on any attempted breaches, intrusion attempts, or other security risks. | |
| c) Security Services | |
| The firewall must include and support: | |
| <ul style="list-style-type: none"> Standard Intrusion Prevention and Detection (IPS/IDS) | |
| <ul style="list-style-type: none"> Antivirus and Anti-Malware Protection | |
| <ul style="list-style-type: none"> Application Control and Web Filtering | |
| <ul style="list-style-type: none"> DLP (Data Loss Prevention) Features | |
| <ul style="list-style-type: none"> Comprehensive Reporting Dashboards for ICT staff visibility. | |