DEPARTMENT

Corporate Services

DIRECTORATE

Information Technology Directorate

DIVISION

Information Security Management

PROCUREMENT DOCUMENT

GOODS / SERVICES

Documents are to be obtained, free of charge, in electronic format, from the National Treasury's eTenders website or the eThekwini Municipality's website.

Tender No: 36703-1i

Title: Appointment of a service provider for the provision of a managed Cyber Security Operations Centre service, for a period of 36 months

CLARIFICATION MEETING AND QUERIES

Clarification Meeting: A Compulsory Clarification Meeting will be held 2nd Floor Boardroom, Rennies House, 41 Margaret Mncadi Avenue; Durban on 7th September 2026 at 10h00.

Queries can be addressed to: Questions and answers from the clarification meeting will be consolidated and posted on e-tenders/municipal website on 25th September 2026

General / Contractual: Lethokuhle Ngcobo; Tel: 031-322- 5214; eMail: Letho.Ngcobo@durban.gov.za

Technical: Mark Goad; Tel: 031-311-1810; eMail: mark.goad@durban.gov.za

DELIVERY OF TENDERS

Sealed Tenders, addressed to the City Manager and marked with the Tender Number, are to be placed in the Tender Box **located in the ground floor foyer of the Municipal Buildings, 166 KE Masinga Road (Old Fort Rd), Durban** (and not any other municipal department):Tenderers are to also make an electronic submission via the eThekwini Municipality JDE System (SSS Module)

SSS Queries: Contact: Lindo Dlamini: Tel: 031-322-7133 / 031-322 7153
Email:supplier.selfservice@durban.gov.za

Closing Date: Friday, 02 October 2026

Time: 11:00am

FACSIMILE, eMAIL or POSTED TENDERS WILL NOT BE ACCEPTED

Issued by:

NAME OF TENDERER: .....

Tender Price: R .....

VAT Registered: YES / NO
(circle applicable)

NAME OF TENDERER: ……

Tender Price: R …… **VAT Registered: YES / NO**
(circle applicable)

PROCUREMENT DOCUMENT (Goods / Services)

INDEX

SECTION 1: GENERAL INFORMATION

YOU ARE HEREBY INVITED TO TENDER FOR REQUIREMENTS OF THE ETHEKWINI MUNICIPALITY

TENDER No.: 36703-1i

DESCRIPTION: **Appointment of a service provider for the provision of a managed Cyber Security Operations Centre service, for a period of 36 months**

CLOSING DATE / TIME: Friday, 02 October 2026 at 11:00am

All tenders must be submitted on official tender documentation issued (in electronic format) by the eThekwini Municipality from:

- the National Treasury's eTenders website (https://www.etenders.gov.za/), or
- the eThekwini Municipality's website (https://www.durban.gov.za/pages/business/procurement).

Electronically downloaded documentation should be printed by the tenderer.

- Bidders must submit a "hard copy" submission to the Tender Box located in the ground floor foyer of the Municipal Buildings, 166 KE Masinga Road (Old Fort Rd), Durban and an electronic submission via Supplier Self Service (SSS). Notwithstanding the electronic submission, a tender offer will only be deemed valid if the "hard copy" submission has been made. The "hard copy" submission will be deemed to be the ruling version. Bidders are responsible for resolving all access rights and submission queries before the tender closing date. Tender closing date and time remain unchanged

Tenderers are required to be registered on the **National Treasury Central Supplier Database** (CSD) as a service provider. In the case of a Joint Venture, this requirement will apply individually to each party in the Joint Venture.

Registration on the **eThekwini Municipality's Database** can be done via website:
https://ethekwinivendor.durban.gov.za/ and on **SSS:**supplier.selfservice@durban.gov.za

Tenderers should ensure that tenders are delivered timeously to the correct address as stated in the Conditions of Tender. If a tender is late, it will not be accepted for consideration.

The Municipality will consider a tender submitted in response to this request for tender to be an offer from your company to perform the supply on the basis of that tender. Accordingly, please review the attached General and Special Terms and Conditions which will form the basis for any supply arrangement entered into between the Municipality and your company.

The Municipality is seeking tenders from potential suppliers only and makes no representation or promise in relation to procuring work from a supplier or supplier. The Municipality will not be responsible for any costs associated with preparing and submitting a tender.

The Municipality does not bind itself to accept the lowest or any tender. It reserves the right to accept the whole or any part of a tender to place orders. Bidders shall not bind the Municipality to any minimum quantity per order. The successful Tenderer (s) shall be bound to provide any quantities stipulated in the specification.

The successful tenderer will be required to fill in and sign a written Contract Form (MBD 7).

NB: NO TENDER WILL BE CONSIDERED FROM PERSONS IN THE SERVICE OF THE STATE
(as defined in Regulation 44 of the Local Government: Municipal Supply Chain Management Regulations).

THE FOLLOWING PARTICULARS MUST BE FURNISHED
(Failure to do so may result in your tender being disqualified)

Name of Tenderer: .....

Postal Address: .....

Street Address: .....

E-Mail Address: .....

Telephone Number:				-				-					
Cell phone Number:				-				-					
Facsimile Number:				-				-					

	Circle Applicable
Is your entity registered on the **eThekwini Municipality's supplier database**?	YES / NO
• **If YES insert** your PR Number:	**PR** .....
Is your entity registered on the **National Treasury Central Supplier Database** (CSD)?	YES / NO
• **If YES, insert** your MAAA Number:	**MAAA** .....
Insert a SARS Tax Compliance Status PIN	.....
Is your entity VAT registered?	YES / NO
• **If YES insert** Vat Registration Number:	.....
Has a **Declaration of Municipal Fees** been submitted?	YES / NO
Has a **Declaration of Interest** (MBD 4) been submitted?	YES / NO
Has a **Declaration for Procurement Above R10 Million** (MBD 5) been submitted?	YES / NO
Has a **Preference Points Claim** (MBD 6.1) been submitted?	YES / NO
Has a **Declaration of Bidder's Past SCM Practices** (MBD 8) been submitted?	YES / NO
Has a **Certificate of Independent Bid Determination** (MBD 9) been submitted?	YES / NO
Are you the accredited representative in South Africa for the goods / services / works offered? **If YES, enclose proof** at the back of the tender submission.	YES / NO

Signature of Tenderer: ..... Date: .....

Name / Surname: ..... (in block capitals)

Capacity under which this tender is signed: .....

SECTION 2 : CONDITIONS OF TENDER – (Goods / Services : June 2019)

INDEX

STANDARD CONDITIONS OF TENDER (Goods / Services)

1. DEFINITIONS

General:

(1) Defined words / phrases are printed in Italic font.
(2) Definitions apply to the singular as well as the plural.
(3) Any reference to the masculine gender shall be taken to include the feminine and any reference to the feminine gender shall be taken to include the masculine.
(4) The words "bid" and "tender", and "bidder" and "tenderer" can be used interchangeably.
(5) All definitions as defined in the ***General Conditions of Contract*** are applicable to these ***Standard Conditions of Tender***. These definitions include:

- "Closing time"
- "Contract"
- "Contract Price"
- "Corrupt practice"
- "Countervailing duties"
- "Country of origin"
- "Day"
- "Delivery"
- "Delivery ex stock"
- "Delivery into consignees store or to his site"
- "Dumping"
- "Force majeure"
- "Fraudulent practice"
- "GCC"
- "Goods"
- "Imported content"
- "Local content"
- "Manufacture"
- "Order"
- "Project site"
- "Purchaser"
- "Republic"
- "SCC"
- "Services"
- "Supplier"
- "Tort"
- "Turnkey"
- "Written" or "in writing"

(6) **Bid or Tender**: The offer submitted in respect of an invitation to submit such an offer.
(7) **Bidder or Tenderer**: An entity (company, close corporation, partnership, joint venture, sole proprietor) which submits a *bid/tender*.
(8) **Municipality**: The eThekwini Municipality, as represented by the duly authorised delegate, official or committee.
(9) **SCT:** Special Conditions of Tender (found in Section 3).
(10) **Week**: A period of seven (7) consecutive *days*.
(11) **Material Deviation**: A material deviation or qualification is one which, in the *Municipality's* opinion, would:
  (a) Detrimentally affect the scope, quality, or performance of the services or supply identified in the Scope;
  (b) Significantly change the *Municipality's* or the *Tenderer's* risks and responsibilities under the contract; or
  (c) Affect the competitive position of other *Tenderers* presenting responsive *tenders*, if it were to be rectified.

2. CONDITIONS OF TENDER & CONTRACT

The specification will be governed by the ***Standard Conditions of Tender*** (Goods and Services), ***Special Conditions of Tender (SCT)***, ***General Conditions of Contract (GCC)*** (Government Procurement General Conditions (July 2010), as amended by National Treasury Circular 52 dated 30 July 2010), the ***Special Conditions of Contract (SCC)***, the ***Occupational Health and Safety Act*** (Act No. 85 of 1993), and the ***eThekwini Code of Conduct***.

Complete Acceptance of Conditions

Unless otherwise expressly stipulated in a letter covering the *tender*, every *Tenderer* shall be deemed to have waived, renounced, and abandoned any conditions printed or written upon any stationery used for the purpose of, or in connection with, the submission of their *tender*, which are in conflict with the ***General Conditions of Contract*** and ***Special Conditions of Contract***. *Tenderers* are advised that any *material divergences / qualifications* from the official Conditions or Specification will render their *tenders* liable to disqualification.

3. TENDER INFORMATION

(1) **General**
  (a) *Tenders* will be liable for rejection unless made out on the official tendering documentation.
  (b) Any alterations effected upon any of the tendering documents must be clearly shown by means of a hand written (black, non-erasable ink), or typed, entry and must be signed in full by the *Tenderer*. **The use of correction fluid is not permitted**.
  (c) *Tenderers* may submit alternative solutions that, in the *Tenderer's* opinion, are to the *Municipality's* advantage economically and technically. Full technical details of the alternative *tender(s)* shall be submitted with the tender documents. Alternative *tender(s)* shall be submitted separately.

(2) **Obtaining Tender Documentation**

All tenders must be submitted on official tender documentation issued, in electronic format, by the eThekwini Municipality. Electronically downloaded documentation (obtainable free of charge) should be printed and suitably bound by tenderer.

(3) **Queries Relating to this Tender**

Queries can be directed to the person / Department as stated in the ***SCT***.

(4) **Briefing Session (Clarification Meeting)**

Details of the briefing session are stated in the ***SCT***.
Failure to attend a compulsory briefing session will invalidate the *tender*. *Tenderers* must sign the attendance list in the name of the tendering entity. Tenders will only be evaluated from those tendering entities appearing on the attendance list.

(5) **Closing Date and Delivery of Tender Submissions**

Sealed *tenders* made out on the enclosed Official Tender Form, which shall be signed by or on behalf of the *Tenderer* , and addressed to the City Manager, marked with the appropriate Tender number, must be placed in the **Tender Box** as stated in the ***SCT*** not later than the **date and time** as stated in the ***SCT***, where after they will be opened publicly.

All tender documents **must** be placed directly into the Tender Box and should not be delivered to any other Municipal Department. *Bidders* are advised that *tenders* submitted by post, fax or email **will not** be considered. All couriered documents must be placed directly into the Tender Box and should not be delivered to any other Municipal Department.

Any *tender* received after the closing date and time stated for the receipt thereof **shall not** be accepted for consideration and shall be returned to the *Tenderer*.

(6) **Tender Validity and Withdrawal of Tenders**

Tenders must hold good until 16:00 of the 5th week following the date on which *tenders* are opened, or during such other period as may be specified in the ***SCT***. The *Municipality* may, during the period for which *tenders* are to remain open for acceptance, authorize a *Tenderer* to withdraw their *tender* in whole or in part on condition that the *Tenderer* pays to the *Municipality* on demand, a sum of one thousand Rand (R1,000.00). The *Municipality* may, if it thinks fit, waive payment of such sum in whole or in part.

4. **RETURNABLE SCHEDULES, FORMS, CERTIFICATES**

Each *Tenderer* shall complete fully and accurately the following documents and submit these documents with the *tender*:

(1) **Authority of Signatory:** In terms of Clause 4(5)(c) of the Conditions of Tender.

(2) **Tax Compliance Status PIN / Tax Clearance Certificate:** SARS has introduced a new Tax Compliance Status System. Tenderers can submit a Tax Compliance Status PIN (TCS PIN) instead of an original Tax Clearance Certificate. This TCS PIN can be used by third parties to certify the taxpayer's real-time compliance status.

(3) **Declaration of Municipal Fees:** Only those *Bidders* whose municipal fees are fully paid, or those that have concluded acknowledgement of debt agreements with the *Municipality*, are eligible to *tender*.

All Bidders must sign the Declaration of Municipal Fees returnable form, declaring that their municipal fees are in order or that acknowledgement of debt agreements have been concluded, and include the relevant account numbers in the declaration. Failure to include account numbers or sign will invalidate the *tender*. The completion of the declaration is also applicable to *Bidders* outside of the eThekwini Municipal Area.

(4) **Declaration with respect to the Occupational Health and Safety Act:** Acceptance of undertaking in terms of the Occupational Health and Safety Act (Act 85 of 1993) and the relevant Regulations.

(5) **Municipal Biding Documents** (which includes):

(a) **MBD 4:** Declaration of Interest: All Bidders are to sign the Declaration of Interest wherein they declare any relationship that may exist with an official of the Municipality involved in the evaluation process.

Regulation 44 of the Supply Chain Management Regulations states that a Municipality or Municipal Entity may not make any award to a person:

(i) Who is in the service of the state;
(ii) If that person is not a natural person, of which any Director, Manager, Principal, Shareholder or Stakeholder is a person in the service of the state; or
(iii) Who is an advisor or consultant contracted with the Municipality or municipal entity.

Should a contract be awarded, and it is subsequently established that Regulation 44 has been breached, the Municipality shall have the right to terminate the contract with immediate effect.

(b) **MBD 5:** Declaration for Procurement Above R10 Million (if applicable): For all procurement expected to exceed R10 million (all applicable taxes included), tenderers must complete this questionnaire.

(c) **MBD 6.1**: Preference Points Claim Form: For the awarding of Preference Points, Bidders are required to complete the attached MBD 6.1 form and return it with their tender submission. Failure on the part of a tenderer to complete and submit this form will be interpreted to mean that preference points for **Specific Goals** are not claimed.

The Municipality reserves the right to require of a tenderer, 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 Municipality.

(d) **MBD 8**: Declaration of Bidders Past Supply Chain Management Practices Form: This form serves as a declaration to be used by municipalities and municipal entities in ensuring that when goods and services are being procured, all reasonable steps are taken to combat the abuse of the supply chain management system.

(e) **MBD 9**: Certificate of Independent Bid Determination: Section 4(1)(b)(iii) of the Competition Act No. 89 of 1998, as amended, prohibits an agreement between, or concerted practice by, firms if it involves collusive tendering or tender rigging. In order to give effect to this, the Certificate of Bid Determination must be completed and submitted with the tender.

(5) **Official Tender Form** (see Section 9)

(a) Legal Status of Tenderer
It is essential for the purpose of entering into a legal contract that *Bidders* state on the Official Tender Form, under "Name and Address of Tenderer ", their full legal status:
(i) the full registered name of the company making a *tender*; or
(ii) if the *Tenderer* is a person conducting business under a recognised trading name then:
- State the name of the person(s);
- State recognised trading name; and
- State whether an owner, co-owner, proprietor, etc.

(b) **Signing of Official Tender Form**
Failure of a *Tenderer* to complete, in its entirety, and sign the Official Tender Form will invalidate the *tender*.

(c) **Authority of Signatory**
Bidders are to complete and sign the Authority of Signatory returnable document, and attach the required additional documents.

(d) **Differences or Discrepancies**
Should there be any difference or discrepancy between the prices or price contained in the Official Tender Form and those contained in any covering letter from the Tenderer, the prices or price contained in the Official Tender Form shall prevail.

(6) **Any additional Schedules, Forms, or Certificates as stated in the *SCT*.**

5. INFORMATION TO BE SUPPLIED REGARDING SUB-CONTRACTORS

Bidders are to state in their *tenders*, or covering letters, whether, if the contract were to be awarded to them, the whole of the work would be executed by them in their own workshop / factory. If the answer is in the negative, they are required to state which part(s) would be handed to sub-contractors and the name and address of such sub-contractors.

6. SAMPLES

Bidders may be required to state where samples of the full range of products can be inspected or be required to submit samples for inspection prior to the closing date of the *tender*.

7. MANUFACTURERS

The names of the manufacturers of the goods or equipment offered must be stated in the *tender*.

Bidders who are not manufacturers, accredited distributors, or agents must provide a valid agreement / Joint Venture Agreement, entered into with the manufacturer, accredited distributors, or agents, with their submission. This agreement must meet all the requirements as laid down in the *tender* document, and must cover the contract period.

8. CLARIFICATION

The Head: Supply Chain Management Unit, or an authorized representative, may request clarification or further information on any aspect of the *tender*. The *Tenderer* **must** supply the requested information within the time specified. Failure to comply will render the *tender* non-responsive.

9. PRICING

Bidders would be precluded from this *tender* if their pricing structure deviates from the Official Tender Form.

(1) **Nett Prices**
All prices shall be quoted in South African currency (Rand) after deduction of any brokerage or discount allowed to the Municipality.

(2) **Unit Prices**
Bidders shall quote only one price in respect of each item. Such price is to hold good for the full duration of the contract period, being subject to variation only in accordance with specified criteria, as stated in the ***Conditions of Contract***.

(3) **Firm Tenders**
Bidders may submit firm prices for each 12 month period. These prices shall be free from all fluctuations, including any statutory increases.

(4) **Value Added Tax (V.A.T)**
Prices exclusive and inclusive of VAT must be stated separately on the Official Tender Form.

10. ESTIMATED QUANTITIES

The estimated quantities are set out in Section 8 : Bill of Quantities / Schedule of Rates/Activities which forms part of the official tender documents. The quantities are stated purely for the information of the *Bidders* and are in order to ascertain an estimated total contract price. The *Supplier* will, however, be bound to supply whatever quantity or quantities the *Municipality* may actually require, and may exceed, or be less than, the estimated quantities stated.

11. DELIVERY, RISK, PACKAGES, ETC

(1) Unless otherwise provided, all goods are to be supplied only against the form of order issued by the *Municipality*.
(2) *Bidders* shall quote a unit price which shall include delivery to the specified delivery point, as stated in the ***SCT.***
(3) The risk in all goods purchased by the *Municipality* under the contract shall remain with the *Supplier* until such goods shall have been duly delivered.
(4) *Bidders* shall clearly state the period within which delivery will be made after receipt of the official order, as this may be material in the adjudication of the *tender*.

12. **RATES OF EXCHANGE**

(1) Where the goods are imported the *Supplier* shall, within seven days of date of official Purchase Order, arrange through their bankers for the foreign commitment to be covered forward down to the Rand in order to fix the rate of exchange. The *Supplier* shall notify the *Municipality* as soon as possible thereafter regarding the rate which has been fixed on such forward exchange.

Any increase or decrease between the basic rate of exchange as at a date seven days prior to the date of closing of *tenders* and that existing at the date of establishment of the forward exchange cover within the period stipulated above shall be paid or deducted by the Municipality. Upon the failure of the *Supplier* to arrange forward exchange cover, the *Supplier* shall be liable should there be any increase in the basic rate of exchange occurring after the last mentioned date.

The bank charges incurred in obtaining the forward exchange cover shall be for the *Municipality's* account.

(2) The *Supplier* shall on request:
(a) Submit documentary proof of the rate of exchange; and
(b) When an adjustment is claimed in terms of this sub-clause, whether by the *Supplier* or the *Municipality*, submit documentary proof to the satisfaction of the Deputy City Manager: Treasury in respect of such claim.

13. **IMPORT PERMITS**

(1) In order to minimise special importation, *Bidders* should, where possible, have recourse to local suppliers and / or manufacturers.
(2) *Bidders* must state whether their *tender* is dependent upon the issue of a special import permit or whether they are able to supply the goods by making use of the import facilities available to them.
(3) In the event of a tender being dependent upon the issue of a special import permit, application for such special import permit shall be made by the Tenderer , unless otherwise provided for in the ***SCT***.

14. **EVALUATION PROCESS**

The procedure for evaluation of responsive Tender Offers will be in accordance with the eThekwini Municipality's current SCM Policy and the Preferential Procurement Policy Framework Act (5 of 2000), and the Preferential Procurement Policy Framework Act Regulations (November 2022).

Details of additional evaluation criteria, if applicable, are stated in the *SCT*.

Evaluation points for price and preference will only be calculated for *Bidders* who comply with the contractual and technical specification, and if applicable, have attained the minimum Functionality Score as stated in the ***SCT***.

The evaluation process of responsive *tenders* will be as follows:

- Score each *tender* in respect of the financial offer made and preferences claimed (if any);
- Calculate the total number of evaluation points (T_{EV}) in accordance with the following formula:
  $T_{EV} = N_{FO} + N_P$ where: N_{FO} : is the number of evaluation points awarded for the financial offer; and N_P : is the number of evaluation points awarded for preferences claimed.
- Rank *tenders* from the highest number of evaluation points to the lowest.
- Recommend the *Tenderer* with the highest number of evaluation points for the award of the contract, unless there are compelling and justifiable reasons not to do so.
- Rescore and re-rank all *Bidders* should there be compelling and justifiable reasons not to recommend the *Tenderer* with the highest number of evaluation points, and recommend the *Tenderer* with the highest number of evaluation points, unless there are compelling and justifiable reasons not to do so, and the process set out in this sub-clause is repeated.

(1) **Evaluation points awarded for the financial offer:**

Reference is to be made to the Special Conditions of Tender (***SCT)***, and returnable form 5(c) in Section 4.

INCOME-GENERATING CONTRACTS

The financial offer will be scored using the formula:

$$N_{FO} = W\left(1 + \frac{Pt - Pmax}{Pmax}\right)$$

GOODS and SERVICES

The financial offer will be scored using the formula:

$$N_{FO} = W\left(1 - \frac{Pt - Pmin}{Pmin}\right)$$

Where the value of W is:

(a) **90** where the financial value inclusive of VAT of all responsive *tenders* received have a value in excess of R 50,000,000; OR
80 where the financial value inclusive of VAT of one or more responsive *tenders* offers have a value that equals or is less than R 50,000,000.
It is unclear (at the time of advertising) which of the two preference point systems applies. Either the 80/20 or 90/10 preference point system will apply, determined by the price offered by the lowest acceptable tender.

(b) **Pmax** is the comparative offer of the most favourable comparative offer (highest acceptable tender).

(c) **Pmin** is the comparative offer of the most favourable comparative offer (lowest acceptable tender).

(d) **Pt** is the comparative offer of the *tender* offer under consideration.

(2) **Evaluation points awarded for preference:**

The **Specific Goals** for Preference Points are specified in the ***SCT***.

15. **BRIBERY AND COMMUNICATION WITH COUNCILLORS / OFFICIALS**

(1) **Bribery**

No *Tenderer* shall offer, promise or give to any person or person connected with a *tender* or the awarding of a contract, any gratuity, bonus or discount etc, in connection with the obtaining of a contract.

(2) **Communication, Councillors and Officials**

A *Tenderer* shall not in any way communicate with a member of the *Municipality* or with any official of the *Municipality* on a question affecting any contract for the supply of goods or for any work, undertaking or services which is the subject of a *tender* during the period between the closing date for receipt of *tenders* and the dispatch of the written notification of the *Municipality's* decision on the award of the contract; provided that a *Tenderer* shall not hereby be precluded:

(a) At the request of the Head: SCM Unit, or an authorized representative, from furnishing him with additional information or with a sample or specimen for testing purposes or otherwise from giving a demonstration so as to enable the recommendation to the Bid Committee on the award of the contract to be formulated;

(b) From obtaining from the Head : SCM Unit, or an authorised representative, information as to the date upon which the award of the contract is likely to be made, or, after the decision upon the award has been made by the *Municipality* or any Committee to which the *Municipality* has delegated its powers, information as to the nature of the decision or such information as was publicly disclosed at the opening of *tenders* or from submitting to the Accounting Officer in writing any communication relating to their *tender* or the award of the contract or a request for leave to withdraw their *tender*; and

(c) Provided further that nothing contained herein shall be construed so as to prevent information being sought and obtained from an Official in regard to any decision taken at an open Municipal meeting, or any Committee to which the *Municipality* has delegated its powers.

A contravention of subsection (1) and / or (2), or an attempt to contravene such subsection, shall be reported to the Accounting Officer, who may on receipt of such report disqualify the *tender* of the *Tenderer* concerned.

16. **NEGOTIATIONS WITH PREFERRED BIDDERS**

The *Municipality* reserves the right to invoke Regulation 24 of Municipal Finance Management Act if required.

(1) The Accounting Officer may negotiate the final terms of a contract with *Bidders* identified through a competitive tendering process as preferred *Bidders*, provided that such negotiation:

- Does not allow any preferred *Tenderer* a second or unfair opportunity;
- Is not to the detriment of any other *Tenderer* ; and
- Does not lead to a higher price than the *tender* as submitted.

(2) Minutes of such negotiations must be kept for record purposes.

(3) Such negotiation may be delegated by the Accounting Officer.

17. **CANCELLATION OF TENDER PROCESS**

The municipality is entitled to cancel the tender at any time before the award of a tender and the decision to cancel the tender shall be published in the same manner in which the original tender invitation was advertised. The Municipality shall, in no way, be liable for any damages whatsoever, including, without limitation, damages for loss of profit, in any way connected with the cancellation of this bid.

18. **ACCEPTANCE OF BID**

(1) The *Municipality* does not bind itself to accept the lowest or any *tender*, and reserves the right to accept the whole or any part of a *tender* to place orders.

(2) The *Municipality* reserves the right to accept more than one technically and contractually compliant *tender* for part or the whole of the contract and to place orders on the price and availability.

(3) *Bidders* shall not bind the *Municipality* to any minimum quantity per order.

(4) The successful *Tenderer (s)* shall be bound to provide any quantities stipulated in the specification.

(5) Tenders will only be accepted on condition that:

(a) The *tender* is signed by a person authorised to sign on behalf of the *Tenderer* .

(b) A valid (at time of close of tenders), original, Tax Clearance Certificate OR Tax Compliance Status PIN is included with the *tender* submission. Both should have sufficient validity to ensure the process is adequately covered;

(c) A *Tenderer* who submitted their *tender* as a Joint Venture has included an acceptable Joint Venture Agreement and a B-BBEE Certificate pertaining to the Joint Venture with their *tender*.

(6) Financial Standing: The Head: Supply Chain Management reserves the right to require *Bidders* to submit evidence that their financial standing is adequate to meet their obligations under the contract should they be successful.

(7) Change of Ownership or Major Policy: Where it is known to a *Tenderer* that a change in ownership or major policy (of the tendering entity) will occur, or is likely to occur, during a specified contract period, the scope and effect thereof must be fully defined in a covering letter to be submitted with the *tender*.

(8) Purchase of Goods From Other Sources: Nothing contained in this contract shall be held to restrain the *Municipality* from purchasing from persons other than the *Supplier*, any of the goods described or referred to in this contract, if it shall in its discretion think fit to do so.

(9) Capability and Breach of Contract: Tenderers that do not have the capability of undertaking this enquiry in terms of the requirements of the contract or have been in breach of contract previously will not be considered.

19. **PAYMENT and FACTORING**

Payment conditions will be as per the ***Conditions of Contract***.

Payment will be made only to the *Supplier(s).* Factoring arrangements will not be accepted.

20 **APPEALS**

In terms of Regulation 49 of the Municipal Supply Chain Management Regulations persons aggrieved by decisions or actions taken by the *Municipality*, may lodge an appeal within 14 days of the decision or action, in writing to the *Municipality*. The appeal (clearly setting out the reasons for the appeal) and queries with regard to decision of award are to be directed to the office of the City Manager, attention:

Ms. S. Pillay, P.O. Box 1394, Durban, 4000;
eMail: Simone.Pillay@durban.gov.za.

SECTION 3: SPECIAL / ADDITIONAL CONDITIONS OF TENDER

3.1 SPECIAL CONDITIONS OF TENDER (SCT)

The ***Standard Conditions of Tender*** (Goods / Services) make several references to the ***Special Conditions of Tender*** *(SCT)* for details that apply specifically to this tender. The ***Special Conditions of Tender*** shall have precedence in the interpretation of any ambiguity or inconsistency between it and the ***Standard Conditions of Tender***.

Each item below is cross-referenced to the clause in the ***Standard Conditions of Tender*** to which it mainly applies.

SCT 3(1) TENDER INFORMATION: General

The tender document comprises of a cover page and 56 pages.

SCT 3(2) TENDER INFORMATION: Obtaining Tender Documentation

Documents are issued by the eThekwini Municipality electronic format.

Electronically downloaded documentation is obtainable from:

- the National Treasury's eTenders website
  - (https://www.etenders.gov.za/), or
- the eThekwini Municipality's website
  - (https://www.durban.gov.za/pages/business/procurement).

The entire document should be printed on A4 paper (one sided), and suitably bound by the tenderer.

SCT 3(3) TENDER INFORMATION: Queries Relating to this Tender

General and Contractual Queries are to be directed to:

Lethokuhle Ngcobo; Tel: 031-322- 5214; eMail: Letho.Ngcobo@durban.gov.za

Technical Queries are to be directed to:

Mark Goad; Tel: 031-311-1810; eMail: mark.goad@durban.gov.za

SCT 3(4) TENDER INFORMATION: Briefing Session

A Compulsory Clarification Meeting will be held 2nd Floor Boardroom, Rennies House, 41 Margaret Mncadi Avenue; Durban on 7th September 2026 at 10h00.

SCT 3(5) TENDER INFORMATION: Closing Date and Delivery of Tender Submissions

1. Tenderers are hereby advised to submit the following, no later than **Friday, *dd mm yyyy* at 11:00 am**:

   a) A signed **hard copy** of the Tender Document that is sealed, addressed to the City Manager and clearly marked with the Tender Number. This **hard copy** shall be deposited into the Tender Box **located in the ground floor foyer of the Municipal Buildings at 166 KE Masinga Road (Old Fort Rd), Durban**; and

b) An **electronic copy** of the Tender Document, identical to that of the signed **hard copy**, via the eThekwini Municipality JDE System (SSS Module).

2. Notwithstanding the submission of the **electronic copy** of the Tender Document via the JDE System (SSS Module):

   a) The Tender Offer shall only be deemed valid if the **hard copy** submission has been made; and

   b) The **hard copy** submission shall take precedence and be utilised for the evaluation of Tenders.

3. In the event of any ambiguity or inconsistency within the **hard copy** submissions, eThekwini Municipality reserves the right to verify the information by comparing the **hard copy** with the corresponding **electronic copy**. Subsequently, if the **electronic copy** is found not to be identical to the **hard copy**, the Tender Offer shall be deemed invalid.

4. Tenderers shall ensure all access rights and submission queries related to the JDE system are resolved prior to the closing date.:

BID VIEWING, TENDER DOCUMENT DOWNLOAD AND BID SUBMISSION PROCESS

5. The following link must be followed for login, to view advertised bids, and to submit a bid advertised by eThekwini Municipality.

   https://rfq.durban.gov.za/jde/E1Menu.maf

   All queries related to the JDE system shall be directed to:

SSS Queries: Lindo Dlamini Tel: 031-3227133 / 031-3227153 Email: supplier.selfservice@durban.gov.za	**SSS Technical Queries**: Jabulane Chauke: Tel: 031 322 9535 Email: Jabulani.chauke@durban.gov.za

SCT 3(6) **TENDER INFORMATION: Tender Validity and Withdrawal of Tenders**

1. Tenders must remain valid for a period of 120 days following the date on which the Tenders are opened. This period is referred to as the **original validity period**.

2. In addition to the original validity period, Tenders must remain valid for acceptance for a further period of twelve (12) months, unless the Municipality is advised otherwise by the bidder in writing.

3. eThekwini Municipality reserves the right to request confirmation of Tender validity at any time during the twelve (12) month period.

SCT 4(6) **RETURNABLE SCHEDULES, FORMS, CERTIFICATES**

The additional returnable schedules:

- Reference letters (Minimum of two contactable references where the bidder has successfully provisioned a managed Cyber Security Operations Centre service, for more than 12 months (Customers with ICT infrastructure of more than 250 servers) during the last 8 years.
- Accreditations (Provide certificates for the Managed Service Provider/Security Operations Centre (SOC) infrastructure/services, valid ISO 27001 certificate, valid ISO 9001 Certificate, valid ISO 22301 Certificate).
- Data center Tier 4 certificate (awarded by the Uptime institute) or equivalent Independent Attestation report confirming high availability

- Official Letter of Authorization. (Agentic SIEM, EASM and DMW, Autonomous NDR).
- Autonomous NDR leadership report
- Proposal of the Managed Security Operation Centre service (covering all requirements in the scope of supply or services (Section 7 B).
- Comprehensive CVs of the resources (SOC analysts and Senior cybersecurity specialist) with relevant experience, qualifications and certificates (attach).
- Clear photographs of operational Managed Cyber Security Operations Center (SOC)

SCT 14 EVALUATION PROCESS

14.1 Mandatory Requirements

Tender must satisfy ALL the following mandatory requirements. Any response that does not meet ALL the requirements will be deemed non-responsive.
Bidders will be evaluated on the following Mandatory requirements. Those who fulfil all the mandatory requirements will be evaluated on BBBEE and Price. Evaluation will be based on the most responsive tender to the mandatory requirements.

#	Mandatory requirements	Proof	Page reference on bid
1.	**Company experience** The bidder must have successfully provisioned a managed Cyber Security Operations Centre (SOC)/Security Information and Event Management (SIEM)/Threat Detection service for at least two different South African organisations/companies (with ICT server infrastructure of more than 250 servers) during the last 8 years, for at least more than 12 months. The reference letters must include contactable email references (for verification) and include the period of Contract (duration).	Two Reference letters (Official Letter Head)	
2.	**Company Accreditations** The bidder (Managed Security Service Provider/SOC infrastructure/platform/services) must be: a) ISO 27001 (Information Security Management System) certified b) ISO 9001 (Quality Management System), certified c) ISO 22301 (Business Continuity management system) certified Municipality, reserve the right to verify the validity of those certificates	a) Valid ISO 27001 certificate b) Valid ISO 9001 Certificate c) Valid ISO 22301 Certificate	
3.	**High Availability:** a) Data centre hosting the unified agentic SOC/SIEM platform must be Fully Fault-Tolerant, be a Tier 4 data centre, to ensure over 99.995% uptime.	a) Data center Tier 4 certificate (awarded by the Uptime institute) or equivalent Independent Attestation report confirming high availability	
4.	**Accredited partner letters:**		

	The bidder must provide official Letter(s) of Authorization from the Original Equipment/Software Manufacturer for the solutions proposed as part of the Managed SOC. a) Next-gen Agentic SIEM (Security Information and Event Management), with integrated Automation & Orchestration, UEBA (User and Entity Behaviour Analysis), Analytics, Threat intelligence, Continuous Threat Exposure Management (CTEM). External Attack Surface Monitoring (EASM) and Dark Web Monitoring (DWM) b) Fully and semi autonomous Network Detection and Response (NDR)	a) Agentic SIEM, and EASM and DMW Official Letter (s) of Authorization. (OEM/OSM partner letters should not be older than 90 days) b) Autonomous NDR Official Letter of Authorization. (OEM/OSM partner letters should not be older than 90 days)	
5.	**Independent Industry Recognition of the NDR Solution** The proposed Autonomous Network Detection and Response (NDR) solution must be recognized as a Leader by an independent accredited technology/software market research firm in a published industry assessment or report, issued within the last five (5) years.	Autonomous NDR leadership report	
6.	**Proposal** The bidder must provide a detailed proposal for the implementation of the proposed managed Agentic SOC service, including Data sheets for the proposed solutions and covering all requirements in the scope of supply or services (Section 7), showing full understanding of the brief, with clear implementation plan with timelines which should be less than 50 days.	Proposal for the Managed SOC service (covering all the requirements)	
7.	**Resources** The bidder must provide key SOC Analysts and Cybersecurity specialist CV's showing experience or expertise and qualifications and certifications (attach) for those resources that will be allocated for the Municipality Managed SOC. **7.1. SOC analysts L1.5 (24X7, minimum of 6)** a) Certified SOC/Cybersecurity analyst or equivalent entry/mid-level /advanced cybersecurity certificate(s), b) With a minimum of 3 years' relevant experience in cybersecurity monitoring, triage, deep analysis, investigation and incident response/mitigation, threat emulation, threat hunting, executing playbooks, malware & threat analysis. Building attacker timelines, attack chain through log analysis, investigations from	7.1 Comprehensive CVs for the resources (detailing relevant experience) and relevant qualifications (attach qualifications and certificates).	

	different sources such as firewall, endpoint protection, endpoint/server and initiate containment and remediation processes. Understanding of adversary Tactics, Techniques, Procedures, frameworks, kill-chain, malware analysis, and log correlation. Ability to analyze obscure scripts, process logs, and identify malicious activities from SIEM and endpoint protection and network security tools. **7.2** Senior Cybersecurity Specialist (to be based at eThekwini Municipality Durban central office, working 5 days full-time, and on standby 24X7, to act on SOC analyst escalations/incident alerts, respond, and continuously optimise security posture) Certified as an Ethical Hacker or Penetration Tester, or Incident response handler, or computer hacking forensic investigator and advanced information security certificates such as Certified Information Security Mager (CISM)/ Certified Information Systems Security Professional (CISSP) etc, with a minimum of 6 years' relevant experience in security monitoring, data analysis, advanced/deep investigation, proactive threat hunting, red teaming/hands-on, deep technical hacking/testing, prevention, malware & threat analysis, digital forensics, counterintelligence, incident response, ethical hacking, reverse engineering across different IT infrastructure and attack vectors. a) Hold an active certification as an Ethical Hacker or Penetration Tester, or Incident handler, or computer hacking forensic investigator, and b) Hold an active certification in advanced information security such as CISM/CISSP etc, c) With a minimum of 6 years' relevant experience in security monitoring, data analysis, advanced investigation, proactive threat hunting, red teaming/hands-on, deep technical hacking/testing, prevention, malware & threat analysis, digital forensics, counterintelligence, incident response, and reverse engineering across different IT infrastructure and attack vectors. Deep knowledge of operating systems (Windows, Linux servers), networking protocols, and cloud infrastructure. Proficiency in SIEM/SOAR/UEBA/NDR/threat intelligence platforms, ethical penetration testing, forensic investigation. Strong understanding of adversary tactics and Indicators of Compromise (IoCs), and the unified kill-chain, and security posture assessments.	7.2 Comprehensive CV for the resources (detailing relevant experience) and attach relevant qualifications and valid certificates.	
8.	**SOC Operational Proof** Bidders must submit clear photographs of their operational Managed Cyber Security	8 Clear photographs of operational Managed Cyber Security	

	Operations Center (SOC) as part of their proposal, such as showing live Large Screen Displays Central command monitors and Analyst Workstations. **Right to Audit:** All specifications, visual layouts, and live operational capabilities remain subject to verification or remote viewing upon request.	Operations Center (SOC)	

14.2 Price and Preference

The procedure for the evaluation of responsive tenders is **PRICE AND PREFERENCE** in accordance with the Employer's current SCM Policy, the Preferential Procurement Policy Framework Act (5 of 2000), and the Preferential Procurement Policy Framework Act Regulations (2022).

The **80/20** preference points system will be applied. The Formula used to calculate the **Price Points (max. 80)** will be according to that specified Regulation 4.1.

Reference is to be made to **Returnable Form: 5(c) MBD 6.1: Preference Points Claim .**

14.4 Preference Point System and Specific Goals

The definitions as per the SCM Policy are applicable.

Ownership Goal

The tendering entity's **Percentage Ownership**, in terms of the **Ownership Category(s)** listed below, is to be used in the determination of the tenderer's claim for **Preference Points**.

Goal Weighting 50%			
Ownership Categories	**Criteria**	**80/20**	
Race: Black (w1)	0%	0	
	>0% and <51%	4	
	≥51% and <100%	7	
	100%	10	
Proof of claim as declared on MBD 6.1 (1 or more of the following will be used in verifying the tenderer's status) • Companies and Intellectual Property Commission registration document (CIPC) • CSD report. • B-BBEE Certificate of the tendering entity. • Consolidated B-BBEE Certificate if the tendering entity is a Consortium, Joint Venture, or Trust (Issued by verification agency accredited by the South African Accreditation System). • Agreement for a Consortium, Joint Venture, or Trust.			

Preference Points (either 20 or 10) will be derived from points claimed on Returnable Document **MBD 6.1: "Preference Points Claim Form"** (in Section 4 of this procurement document) for the **Specific Goal(s)** as indicated on the table(s) below, and according to the specified **Goal Weightings**.

RDP Goal: The promotion of South African owned enterprises

The tendering entity's **Address** (as stated on the National Treasury Central Supplier Database (CSD) or on the eThekwini Municipality Vendor Portal) is to be used in the determination of the tenderer's claim for **Preference Points** for this Specific Goal.

Goal Weighting 50%		
Location	**80/20**	
Not in South Africa	0	
South Africa	4	
KZN	7	
ETM	10	
Proof of claim as declared on MBD 6.1 (1 or more of the following will be used in verifying the tenderer's status) • CSD report		

SCT 20 **COMPLAINTS AND OBJECTIONS**

In terms of Section 49 of the Ethekwini SCM Policy any person aggrieved by the decisions taken in the implementation of the SCM System may lodge within 14 days of notification, a written objection against the decision of the following:

The City Manager
Attention: Ms S Pillay **(E-Mail: Simone.Pillay@durban.gov.za)**
P O Box 1394
DURBAN
4000

Please be advised that any objection to this decision will only be processed upon receipt of a non-refundable administration fee of R6,131.00 including VAT as stipulated in the municipality's SCM Policy approved on 30/09/2025 as well as the municipal budget for the financial year 2026/27. An objection will only be considered upon receipt of proof of payment of this fee. This amount must be paid into the following bank account as a real-time payment:

EThekwini Municipality
FNB – 631 6574 6331
Reference Number: *Please insert contract number*

3.2 ADDITIONAL CONDITIONS OF TENDER (ACT)

ACT 1 ELIGIBILITY – CSD REGISTRATION

Tenderers are required to be registered on the National Treasury Central Supplier Database (CSD) as a service provider. In the case of a Joint Venture, this requirement will apply individually to each party in the Joint Venture. Tenderers not so registered, at time of closing of tenders, will not be eligible to submit tenders.

The Tenderer's CSD Supplier Number (starting with "MAAA") is to be provided on the information table in Section 1.

Tenderers who wish to register on the CSD may do so via web address https://secure.csd.gov.za.

SECTION 4: RETURNABLE TENDER DOCUMENTS

The required returnable documents are as detailed in Section 2 (Clause 4): "Returnable Schedules, Forms, Certificates" of the Conditions of Tender / Special Conditions of Tender.

1) Authority of Signatory
2) Tax Compliance Status PIN / Tax Clearance Certificate
3) Declaration of Municipal Fees
4) Declaration with respect to The Occupational Health and Safety Act
5(a) MBD 4: Declaration of Interest
5(b) MBD 5: Declaration for Procurement Above R10 Million
5(c) MBD 6.1: Preference Points Claim
5(d) MBD 8: Declaration of Bidder's Past Supply Chain Management Practices
5(e) MBD 9: Certificate of Independent Bid Determination

The Tender Form can be found in Section 9: "Official Tender Form", and any additional schedules, forms, certificates can be found in Section 10: "Annexures".

1) AUTHORITY OF SIGNATORY

Reference is made to the Conditions of Tender: Clause 4(5)(c).

Indicate the status of the tenderer by ticking the appropriate box hereunder.

COMPANY		CLOSE CORPORATION		PARTNERSHIP		JOINT VENTURE		SOLE PROPRIETOR	
Refer to Notes at the bottom of the page									

I / We, the undersigned, being the Chairperson (Company), Member(s) (Close Corporation), Partners (Partnership), Sole Owner (Sole Proprietor), Lead Partner (JV), in the company / business trading as:

……

hereby authorise Mr/Mrs/Ms ……

acting in the capacity of .....

to sign all documents in connection with the tender for Contract No. **36703-1i** and any contract resulting from it on our behalf.

NAME	ADDRESS	SIGNATURE	DATE

Notes

Tenderers are to include, at the back of their tender submission document, a printout of the following documents:

If a Company : a “Resolution of the Board” in this regard.
If a Joint Venture : a “Power of Attorney” signed by the legally authorised signatories of all the partners to the Joint venture.

2) TAX COMPLIANCE STATUS PIN / TAX CLEARANCE CERTIFICATE

SARS has introduced a new Tax Compliance Status System. Tenderers can submit a Tax Compliance Status PIN (TCS PIN) instead of an original Tax Clearance Certificate. This TCS PIN can be used by third parties to certify the taxpayer's real-time compliance status.

Separate Tax Clearance Certificates / TCS PINs are required for each entity in a Joint Venture.

The TCS PIN(s) are to be entered on the information table in **SECTION 1: GENERAL INFORMATION.**

Tenderers are to include, at the back of their tender submission document, a printout of their Tax Compliance Status PIN (TCS PIN) OR an original Tax Clearance Certificate.

Failure to include the required document will make the tender submission non-responsive.

I, the undersigned, who warrants that they are authorised to sign on behalf of the Tenderer, confirms that the information contained in this form is within my personal knowledge and is to the best of my belief both true and correct, ***and that the requested documentation has been included in the tender submission****.*

NAME (Block Capitals): _____ **Date**

SIGNATURE: ---------- ----------

3) DECLARATION OF MUNICIPAL FEES

I, the undersigned, do hereby declare that the Municipal fees of

.....
(full name of Company / Close Corporation / partnership / sole proprietary/Joint Venture)

(hereinafter referred to as the TENDERER) are, as at the date hereunder, fully paid or an Acknowledgement of Debt has been concluded with the Municipality to pay the said charges in instalments.

The following account details relate to property of the said TENDERER:

Account	Account Number: to be completed by tenderer.
Consolidated Account No.	
Electricity	
Water	
Rates	
Other	

I acknowledge that should the aforesaid Municipal charges fall into arrears, the Municipality may take such remedial action as is required, including termination of any contract, and any payments due to the Contractor by the Municipality shall be first set off against such arrears.

- Where the TENDERER'S place of business or business interests are outside the jurisdiction of eThekwini Municipality, a copy of the accounts/agreements from the relevant municipality must be attached (to the back inside cover of this document).

- Where the tenderer's Municipal Accounts are part of their lease agreement, then a copy of the agreement, or official letter to that effect is to be attached (to the back inside cover of this document).

Tenderers are to be include, at the back of their tender submission document, a printout of the above account's and or agreements signed with the municipality.

Failure to include the required document will make the tender submission non-responsive.

NAME (Block Capitals): ---------- **Date**

SIGNATURE: _____ ----------

4) DECLARATION WITH RESPECT TO THE OCCUPATIONAL HEALTH AND SAFETY ACT

Definitions

The Act: The Occupational Health and Safety Act No 85 of 1993 (as amended by the Occupational Health and Safety Amendment Act No 181 of 1993), and any associated / applicable Regulations.

Declaration by Tenderer

1. I, the undersigned, hereby declare and confirm that I am fully conversant with the Act.

2. I hereby declare that my company has the competence and the necessary resources to safely carry out the work / supply / services under this contract in compliance with the Act, and the Employer's / Purchaser's / Client's Health and Safety Specifications.

3. I hereby undertake, if my tender is accepted, to provide on request a suitable and sufficiently documented Health and Safety Plan which plan shall be subject to approval by the Employer / Purchaser / Client.

4. I hereby confirm that adequate provision has been made in my tendered rates to cover the cost of all resources, actions, training and all health and safety measures envisaged in the Act, and that I will be liable for any penalties that may be applied by the Employer / Purchaser / Client for failure to comply with the provisions of the Act.

5. I agree that my failure to complete and execute this declaration to the satisfaction of the Employer / Purchaser / Client will mean that I am unable to comply with the requirements of the Act and accept that my tender will be prejudiced and may be rejected at the discretion of the Employer / Purchaser / Client.

NAME (Block Capitals): _____ **Date**

SIGNATURE: _____ _____

5(a) MBD 4: DECLARATION OF INTEREST

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

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

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

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

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

3.1 Name of enterprise	
Name of enterprise's representative	
3.2 ID Number of enterprise's representative	
3.3 Position enterprise's representative occupies in the enterprise	
3.4 Company Registration number	
3.5 Tax Reference number	
3.6 VAT registration number	

3.7 The names of all directors / trustees / shareholders / members / sole proprietors / partners in partnerships, their individual identity numbers and state employee numbers must be indicated in paragraph 4 below. In the case of a joint venture, information in respect of each partnering enterprise must be completed and submitted.

	Circle Applicable	
3.8 Are you presently in the service of the state?	YES	NO

If yes, furnish particulars:
……

……

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

If yes, furnish particulars:
……

……

3.10 Do you have any relationship (family, friend, other) with persons in the service of the state and who may be involved with the evaluation and or adjudication of this bid?	YES	NO
If yes, furnish particulars:		
3.11 Are you, aware of any relationship (family, friend, other) between any other bidder and any persons in the service of the state who may be involved with the evaluation and or adjudication of this bid?	YES	NO
If yes, furnish particulars:		
3.12 Are any of the company's directors, trustees, managers, principle shareholders or stakeholders in service of the state?	YES	NO
If yes, furnish particulars:		
3.13 Are any spouse, child or parent of the company's directors, trustees, managers, principle shareholders or stakeholders in service of the state?	YES	NO
If yes, furnish particulars:		
3.14 Do you or any of the directors, trustees, managers, principle shareholders, or stakeholders of this company have any interest in any other related companies or business whether or not they are bidding for this contract?	YES	NO
If yes, furnish particulars:		

4 The names of all directors / trustees / shareholders / members / sole proprietors / partners in partnerships, their individual identity numbers and state employee numbers must be indicated below. In the case of a joint venture, information in respect of each partnering enterprise must be completed and submitted

Full Name	Identity No.	State Employee No.	Personal income tax No.
Use additional pages if necessary			

I, the undersigned, who warrants that they are authorised to sign on behalf of the Tenderer, confirms that the information contained in this form is within my personal knowledge and is to the best of my belief both true and correct.

NAME (Block Capitals): ..... **Date** .....

SIGNATURE: ....

5(b) MBD 5: DECLARATION FOR PROCUREMENT ABOVE R10 MILLION
(ALL APPLICABLE TAXES INCLUDED)

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

		Circle Applicable	
1.0	Are you by law required to prepare annual financial statements for auditing?	YES	NO
1.1	**If YES, submit audited annual financial statements for the past three years or since the date of establishment if established during the past three years.**		
2.0	Do you have any outstanding undisputed commitments for municipal services towards any municipality for more than three months or any other service provider in respect of which payment is overdue for more than 30 days?	YES	NO
2.1	If NO, this serves to certify that the bidder has no undisputed commitments for municipal services towards any municipality for more than three months or other service provider in respect of which payment is overdue for more than 30 days.		
2.2	If YES, provide particulars.		
	…….		
	…….		
3.0	Has any contract been awarded to you by an organ of state during the past five years, including particulars of any material non-compliance or dispute concerning the execution of such contract?	YES	NO
3.1	If YES, provide particulars.		
	…….		
	…….		
4.0	Will any portion of goods or services be sourced from outside the Republic, and, if so, what portion and whether any portion of payment from the municipality / municipal entity is expected to be transferred out of the Republic?	YES	NO
4.1	If YES, provide particulars.		
	…….		
	…….		

If required by 1.1 above, tenderers are to include, at the back of their tender submission document, a printout of their audited annual financial statements.

I, the undersigned, who warrants that they are authorised to sign on behalf of the Tenderer, confirms that the information contained in this form is within my personal knowledge and is to the best of my belief both true and correct, ***and, if required, that the requested documentation has been included in the tender submission****.*

NAME (Block Capitals): ..... **Date** .....

SIGNATURE: .....

5(c) MBD 6.1: PREFERENCE POINTS CLAIM) (SCMP 52.5: Broad-Based Black Economic Empowerment)

This form serves as a claim form for preference points for **Broad-Based Black Economic Empowerment (B-BBEE) Status Level of Contribution**. **Reference is to be made to the Special Conditions of tender: SCT 14**

1.0 GENERAL CONDITIONS

1.1 The relevant **Preference Points System (80/20 or 90/10)** applicable to this bid is stated in the **Special Conditions of tender: SCT 14**

1.2 Failure on the part of a bidder to fill in and/ or sign this form, and submit a B-BBEE Verification Certificate from a Verification Agency accredited by the South African Accreditation System (SANAS), or a Registered Auditor approved by the Independent Regulatory Board of Auditors (IRBA), or sworn affidavits in the case of Exempted Mico Enterprises or Qualifying Small Enterprises, together with the bid, will be interpreted to mean that preference points for **B-BBEE Status Level Of Contribution** are not claimed.

1.3 The purchaser 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 purchaser.

2.0 ADJUDICATION USING A POINT SYSTEM

2.1 The bidder obtaining the highest number of total points will be recommended for the award of the contract.

2.2 Preference points shall be calculated after prices have been brought to a+ comparative basis taking into account all factors of non-firm prices and all unconditional discounts.

2.3 Points scored will be rounded off to the nearest 2 decimal places.

2.4 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.

2.5 However, when functionality is part of the evaluation process and two or more bids have scored equal points including equal preference points for B-BBEE, the successful bid must be the one scoring the highest score for functionality.

2.6 Should two or more bids be equal in all respects the award shall be decided by the drawing of lots.

3.0 POINTS AWARDED FOR PRICE

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

80/20 Procurement System

$$Ps = 80\left(1 - \frac{Pt - P\min}{P\min}\right)$$

Where: Ps = Points scored for comparative price of bid under consideration
Pt = Comparative price of bid under consideration
Pmin = Comparative price of lowest acceptable bid

4.0 POINTS ALLOCATED FOR B-BBEE STATUS LEVEL OF CONTRIBUTION

4.1 Preference points must be claimed by a bidder for attaining the **B-BBEE Status Level of Contribution** in accordance with the applicable table below:

80/20 Preference Points System	
B-BBEE Level Contributor	**Preference Points**
1	20
2	18
3	14
4	12
5	8
6	6
7	4
8	2
Non-Compliant	0

4.2 All bidders must submit **B-BBEE Status Level of Contribution Certificates**, issued by either verification agencies accredited by the South African Accreditation System (SANAS), or by registered auditors approved by the Independent Regulatory Board for Auditors (IRBA), or sworn affidavits in a case of an Exempted Micro Enterprise (EME) or a Qualifying Small Enterprise (QSE).

4.3 Any enterprise with an annual Total Revenue of R 10 million or less qualifies as an Exempted Micro-Enterprise.

4.4 Exempted Micro-Enterprises are deemed to have B-BBEE Status of "Level Four Contributor" having a B-BBEE procurement recognition of 100% in terms of the Codes of Good Practice.

4.5 An Exempted Micro Enterprise (EME) with at least 51% black ownership qualifies as a Level 2 contributor with BBBEE level of 125% in terms of the Codes of Good Practice.

4.6 An Exempted Micro Enterprise with 100% black ownership qualifies as a Level 1 contributor with BBBEE level of 135% in terms of the Codes of Good Practice.

4.7 An Exempted Micro Enterprise that is regarded as a specialized enterprise with at least 75% black beneficiaries qualifies as a Level 1 contributor with BBBEE level of 135% in terms of the Codes of Good Practice.

4.8 An Exempted Micro Enterprise that is regarded as a specialized enterprise with at least 51% black beneficiaries qualifies as a Level 2 contributor with BBBEE level of 125% in terms of the Codes of Good Practice.

4.9 A Qualifying Small Enterprise (QSE) with at least 51% black ownership qualifies as a Level 2 contributor.

4.10 A QSE with 100% black ownership qualifies as a Level 1 contributor.

4.11 A QSE that is regarded as a specialized enterprise with at least 51% black beneficiaries qualifies as a Level 2 contributor with BBBEE level of 125% in terms of the Codes of Good Practice.

4.12 A QSE with less than 51% black ownership is required to submit a BBBEE level verification certificate issued by a BBBEE verification professional.

4.13 A Trust, consortium or joint venture:

(a) must submit a B-BBEE status level certificate in order to qualify for points;
(b) may qualify for points as an unincorporated entity provided, that they submit their consolidated scorecard is prepared for separate tender; and
(c) where no consolidated scorecard exists, the weighted average (in accordance with participation percentages) must be used and rounded off to the nearest status level.

4.14 Gazetted Sector Codes supersede Generic Codes.

5.0 SUB-CONTRACTING

5.1 B-BBEE points must not be awarded to a tenderer who intends sub-contracting more than 25% of the value of the contract to an enterprise that does not qualify for at least the points that such contractor qualifies for, unless the intended sub-contractor is an EME who has the ability and capability to execute the contract.

5.2 A person awarded a contract may not sub-contract more than 25% of the value of the contract to an enterprise that does not have an equal or higher B-BBEE status level, unless the intended sub-contractor is an EME who has the ability and capability to execute the contract.

5.3 A person awarded a contract in relation to a designated sector may not sub-contract in such a manner that the **Local Production and Content** of the overall value of the contract is reduced to below the prescribed minimum threshold.

6.0 BID DECLARATION

6.1 Bidders who wish to claim points in respect of **B-BBEE Status Level of Contribution** must complete the following:

B-BBEE Status Level of Contribution	Tenderer's Preference Points Claim (maximum of 10 or 20 points)
Points claimed must be in accordance with the relevant table reflected in paragraph 4.1 and must be substantiated by means of a B-BBEE Status Level of Contribution Certificate issued by a verification agency accredited by the South African Accreditation System (SANAS), or by registered auditors approved by the Independent Regulatory Board for Auditors (IRBA), or sworn affidavits in a case of an Exempted Micro Enterprise (EME) or a Qualifying Small Enterprise (QSE).	

Tenderers are to include, at the back of their tender submission, their B-BBEE Status Level of Contribution Certificate.

I, the undersigned, who warrants that they are authorised to sign on behalf of the Tenderer, confirms that the information contained in this form is within my personal knowledge and is to the best of my belief both true and correct, ***and, if required, that the requested documentation has been included in the tender submission****.*

NAME (Block Capitals): ..... **Date**

SIGNATURE: ....

5(c) MBD 6.1: PREFERENCE POINTS CLAIM
In terms of THE PREFERENTIAL PROCUREMENT REGULATIONS (2022)

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

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

1.0 GENERAL CONDITIONS

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

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

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

1.3 Preference Points for this tender shall be awarded for:

- **Price** and **Specific Goals**: Either 80 or 90 (price) and 20 or 10 (specific goals), in terms of 1.2 above.
- The total Preference Points, for Price and Specific Goals, is 100.

1.4 Failure on the part of the tenderer to submit the required proof or documentation, in terms of the requirements in the (Special) Conditions of Tender for claiming **Specific Goal** preference points, will be interpreted that preference points for **Specific Goals** are not claimed.

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

2.0 DEFINITIONS

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

2.2 "**price**" means an amount of money tendered for goods or services, and includes all applicable taxes less all unconditional discounts.

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

2.4 "**tender for income-generating contracts**" means a written offer in the form determined by Municipality 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 Municipality and a third party that produces revenue for the Municipality, 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.

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

3.0 FORMULA FOR CALCULATION OF PREFERENCE PRICE POINTS

3.1 PROCUREMENT OF GOODS AND SERVICES

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

80 / 20 Points System

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

Where:
Ps = Points scored for price of tender under consideration
Pt = Price of tender under consideration
Pmin = Price of lowest acceptable tender

3.2 DISPOSAL OR LEASING OF STATE ASSETS AND INCOME GENERATING PROCUREMENT

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

80 / 20 Points System

$$Ps = 80\left(1 + \frac{Pt - Pmax}{Pmax}\right)$$

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

4.0 POINTS AWARDED FOR SPECIFIC GOALS

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

4.2 In cases where the municipality intends to use Regulation 3(2) of the Regulations, which states that if it is unclear whether the 80/20 or 90/10 preference point system applies, the municipality must, in the tender documents, stipulate in the case of:

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

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

TABLE 1: Specific Goals for the tender and maximum points for each goal are indicated per the table below.

Tenderers are to indicate their points claim for each of the Specific Goals in the shaded blocks.

The Specific Goals to be allocated points in terms of this tender	Number of points ALLOCATED (80/20 system)	Number of points ALLOCATED (90/10 system)	Number of points CLAIMED (80/20 system)	Number of points CLAIMED (90/10 system)
Ownership Goal: Black	10	n/a		n/a
RDP Goal: The promotion of South African owned enterprises.	10	n/a		n/a
Total claimed points (20 Maximum)				
Should the municipality apply a combination of Specific Goals, the **points for the individual goals** will be weighted according to the **Goal Weightings** specified in the Tender Data to arrive at the final points for **Preferential Points for Specific Goals**.				

I, the undersigned, who warrants that they are authorised to sign on behalf of the Tenderer, certify that the points claimed, based on the specific goals as specified in the tender, qualifies the tendering entity for the preference(s) shown.

I acknowledge that:

1) The information furnished is true and correct.

2) The preference points claimed are in accordance with the General Conditions as indicated in paragraph 1 of this form.klkj

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

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

   (a) disqualify the person from the tendering process.
   (b) recover costs, losses or damages it has incurred or suffered as a result of that person's conduct.
   (c) cancel the contract and claim any damages which it has suffered as a result of having to make less favourable arrangements due to such cancellation.
   (d) recommend that the tenderer or contractor, its shareholders and directors, or only the shareholders and directors who acted on a fraudulent basis, be restricted from obtaining business from any organ of state for a period not exceeding 10 years, after the *audi alteram partem* (hear the other side) rule has been applied; and
   (e) forward the matter for criminal prosecution, if deemed necessary.

NAME (Block Capitals): ---------- **Date**

SIGNATURE: _____ ----------

5(d) MBD 8: DECLARATION OF BIDDER'S PAST SUPPLY CHAIN MANAGEMENT PRACTICES

1.0 This Municipal Bidding Document must form part of all bids invited.

2.0 It serves as a declaration to be used by municipalities and municipal entities in ensuring that when goods and services are being procured, all reasonable steps are taken to combat the abuse of the supply chain management system.

3.0 The bid of any bidder may be rejected if that bidder, or any of its directors have:

a) abused the municipal entity's supply chain management system or committed any improper conduct in relation to such system.
b) been convicted for fraud or corruption during the past five years.
c) wilfully neglected, reneged on or failed to comply with any government, municipal or other public sector contract during the past five years.
d) been listed in the Register for Tender Defaulters in terms of section 29 of the Prevention and Combating of Corrupt Activities Act (No 12 of 2004).

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

		Circle Applicable	
4.1	Is the bidder or any of its directors listed on the National Treasury's Database of Restricted Suppliers as companies or persons prohibited from doing business with the public sector? (Companies or persons who are listed on this Database were informed in writing of this restriction by the Accounting Officer / Authority of the institution that imposed the restriction after the audi alteram partem rule was applied.) The Database of Restricted Suppliers now resides on the National Treasury's website (www.treasury.gov.za) and can be accessed by clicking on its link at the bottom of the home page.	YES	NO

4.1.1 If YES, provide particulars.

……

……

4.2	Is the bidder or any of its directors listed on the Register for Tender Defaulters in terms of section 29 of the Prevention and Combating of Corrupt Activities Act (No 12 of 2004)? The Register for Tender Defaulters can be accessed on the National Treasury's website (www.treasury.gov.za) by clicking on its link at the bottom of the home page.	YES	NO

4.2.1 If YES, provide particulars.

……

……

4.3	Was the bidder or any of its directors convicted by a court of law (including a court of law outside the Republic of South Africa) for fraud or corruption during the past five years?	YES	NO

4.3.1 If YES, provide particulars.

……

……

4.4	Does the bidder or any of its directors owe any municipal rates and taxes or municipal charges to the municipality / municipal entity, or to any other municipality / municipal entity, that is in arrears for more than three months?	YES	NO

4.4.1 If YES, provide particulars.

……

……

4.5	Was any contract between the bidder and the municipality / municipal entity or any other organ of state terminated during the past five years on account of failure to perform on or comply with the contract?	YES	NO

4.5.1 If YES, provide particulars.

……

……

I, the undersigned, who warrants that they are authorised to sign on behalf of the Tenderer, confirms that the information contained in this form is within my personal knowledge and is to the best of my belief both true and correct.

I accept that, in addition to cancellation of a contract, action may be taken against me should this declaration prove to be false.

NAME (Block Capitals): **Date**

SIGNATURE:

5(e) MBD 9: CERTIFICATE OF INDEPENDENT BID DETERMINATION

NOTES

[1] Includes price quotations, advertised competitive bids, limited bids and proposals.

[2] Bid rigging (or collusive bidding) occurs when businesses, that would otherwise be expected to compete, secretly conspire to raise prices or lower the quality of goods and / or services for purchasers who wish to acquire goods and / or services through a bidding process. Bid rigging is, therefore, an agreement between competitors not to compete.

[3] Joint venture or Consortium means an association of persons for the purpose of combining their expertise, property, capital, efforts, skill and knowledge in an activity for the execution of a contract.

1.0 This Municipal Bidding Document (MBD) must form part of all **bids**[1] invited.

2.0 Section 4 (1) (b) (iii) of the Competition Act No. 89 of 1998, as amended, prohibits an agreement between, or concerted practice by, firms, or a decision by an association of firms, if it is between parties in a horizontal relationship and if it involves collusive bidding (or **bid rigging**).[2] Collusive bidding is a *pe se* prohibition meaning that it cannot be justified under any grounds.

3.0 Municipal Supply Regulation 38 (1) prescribes that a supply chain management policy must provide measures for the combating of abuse of the supply chain management system, and must enable the accounting officer, among others, to:

a. take all reasonable steps to prevent such abuse;
b. reject the bid of any bidder if that bidder or any of its directors has abused the supply chain management system of the municipality or municipal entity or has committed any improper conduct in relation to such system; and
c. cancel a contract awarded to a person if the person committed any corrupt or fraudulent act during the bidding process or the execution of the contract.

4.0 This MBD serves as a certificate of declaration that would be used by institutions to ensure that, when bids are considered, reasonable steps are taken to prevent any form of **bid rigging**.

5.0 In order to give effect to the above, the attached Certificate of Bid Determination (MBD 9) must be completed and submitted with the bid.

CERTIFICATE OF INDEPENDENT BID DETERMINATION

I, the undersigned, in submitting the accompanying bid:

(Bid Number and Description)

in response to the invitation for the bid made by:

(Name of Municipality / Municipal Entity)

do hereby make the following statements that I certify to be true and complete in every respect.

I certify, on behalf of:

(Name of Bidder)

that:

1. I have read and I understand the contents of this Certificate.

2. I understand that the accompanying bid will be disqualified if this Certificate is found not to be true and complete in every respect.

3. I am authorized by the bidder to sign this Certificate, and to submit the accompanying bid, on behalf of the bidder;

4. Each person whose signature appears on the accompanying bid has been authorized by the bidder to determine the terms of, and to sign, the bid, on behalf of the bidder;

5. For the purposes of this Certificate and the accompanying bid, I understand that the word “competitor” shall include any individual or organization, other than the bidder, whether or not affiliated with the bidder, who:
   (a) has been requested to submit a bid in response to this bid invitation.
   (b) could potentially submit a bid in response to this bid invitation, based on their qualifications, abilities or experience.
   (c) provides the same goods and services as the bidder and/or is in the same line of business as the bidder.

6. The bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement, or arrangement with any competitor. However, communication between partners in a joint venture or consortium[3] will not be construed as collusive bidding.

7. In particular, without limiting the generality of paragraphs 6 above, there has been no consultation, communication, agreement or arrangement with any competitor regarding:
   (a) prices.
   (b) geographical area where product or service will be rendered (market allocation).
   (c) methods, factors or formulas used to calculate prices.
   (d) the intention or decision to submit or not to submit, a bid.
   (e) the submission of a bid which does not meet the specifications and conditions of the bid.
   (f) bidding with the intention not to win the bid.

8. In addition, there have been no consultations, communications, agreements, or arrangements with any competitor regarding the quality, quantity, specifications and conditions or delivery particulars of the products or services to which this bid invitation relates.

9. The terms of the accompanying bid have not been, and will not be, disclosed by the bidder, directly or indirectly, to any competitor, prior to the date and time of the official bid opening or of the awarding of the contract.

10. I am aware that, in addition and without prejudice to any other remedy provided to combat any restrictive practices related to bids and contracts, bids that are suspicious will be reported to the Competition Commission for investigation and possible imposition of administrative penalties in terms of section 59 of the Competition Act No 89 of 1998 and or may be reported to the National Prosecuting Authority (NPA) for criminal investigation and or may be restricted from conducting business with the public sector for a period not exceeding ten (10) years in terms of the Prevention and Combating of Corrupt Activities Act No 12 of 2004 or any other applicable legislation.

NAME (Block Capitals): _____ **Date**

SIGNATURE: _____ _____

SECTION 5: CONDITIONS OF CONTRACT

GOVERNMENT PROCUREMENT: CONDITIONS OF CONTRACT (July 2010)

The ***Conditions of Contract*** are the ***General Conditions of Contract*** as published by the National Treasury titled "Government Procurement: General Conditions of Contract (July 2010), as amended by National Treasury Circular 52 dated 30 July 2010, hereinafter referred to as ***GCC***.

THE NATIONAL TREASURY

Republic of South Africa

GOVERNMENT PROCUREMENT:

GENERAL CONDITIONS OF CONTRACT

July 2010

TABLE OF CLAUSES

1. Definitions

The following terms shall be interpreted as indicated:

1.1 "Closing time" means the date and hour specified in the bidding documents for the receipt of bids.

1.2 "Contract" means the written agreement entered into between the purchaser and the supplier, as recorded in the contract form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

1.3 "Contract price" means the price payable to the supplier under the contract for the full and proper performance of his contractual obligations.

1.4 "Corrupt practice" means the offering, giving, receiving, or soliciting of anything of value to influence the action of a public official in the procurement process or in contract execution.

1.5 "Countervailing duties" are imposed in cases where an enterprise abroad is subsidized by its government and encouraged to market its products internationally.

1.6 "Country of origin" means the place where the goods were mined, grown or produced or from which the services are supplied. Goods are produced when, through manufacturing, processing or substantial and major assembly of components, a commercially recognized new product results that is substantially different in basic characteristics or in purpose or utility from its components.

1.7 "Day" means calendar day.

1.8 "Delivery" means delivery in compliance of the conditions of the contract or order.

1.9 "Delivery ex stock" means immediate delivery directly from stock actually on hand.

1.10 "Delivery into consignees store or to his site" means delivered and unloaded in the specified store or depot or on the specified site in compliance with the conditions of the contract or order, the supplier bearing all risks and charges involved until the goods 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 goods 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 "Supplier" means the successful bidder who is awarded the contract to maintain and administer the required and specified service(s) to the State.

1.26 "Tort" means in breach of contract.

1.27 "Turnkey" means a procurement process where one service provider assumes total responsibility for all aspects of the project and delivers the full end product / service required by the contract.

1.28 "Written" or "in writing" means hand-written 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 (excluding professional services related to the building and construction industry), 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 goods, 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 Invitations to bid are usually published in locally distributed news media and on the municipality/municipal entity website.

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.

6.2 When a supplier developed documentation / projects for the municipality / municipal entity, the intellectual, copy and patent rights or ownership of such documents or projects will vest in the municipality / municipal entity.

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.

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 goods to be produced or services to be rendered should at any stage be subject to inspections, tests and analyses, the bidder or contractor's premises shall be open, at all reasonable hours, for inspection by a representative of the purchaser or organization acting on behalf of the purchaser.

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 goods 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 goods or services referred to in clauses 8.2 and 8.3 do not comply with the contract requirements, irrespective of whether such goods or services are accepted or not, the cost in connection with these inspections, tests or analyses shall be defrayed by the supplier.

8.6 Goods 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 goods 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 goods 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 goods, which do comply with the requirements of the contract. Failing such removal the rejected goods shall be returned at the suppliers cost and risk. Should the supplier fail to provide the substitute goods forthwith, the purchaser may, without giving the supplier further opportunity to substitute the rejected goods, purchase such goods 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 22 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 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, and in any subsequent instructions ordered by the purchaser.

10. Delivery and documents

10.1 Delivery of the goods and arrangements for shipping and clearance obligations, shall be made by the supplier in accordance with the terms specified in the contract.

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.

12. Transportation

12.1 Should a price other than an all-inclusive delivered price be required, this shall be specified.

13. Incidental Services

13.1 The supplier may be required to provide any or all of the following services, including additional services, if any:

(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, 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.

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 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, 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.

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.

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 or in the purchaser's request for bid validity extension, as the case may be.

18. Variation orders

18.1 In cases where the estimated value of the envisaged changes in purchase does not vary more than 15% of the total value of the original contract, the contractor may be instructed to deliver the goods or render the services as such. In cases of measurable quantities, the contractor may be approached to reduce the unit price, and such offers may be accepted provided that there is no escalation in price.

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 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 goods are required, or the supplier's services are not readily available.

21.4 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 22.2 without the application of penalties.

21.5 Upon any delay beyond the delivery period in the case of a goods contract, the purchaser shall, without cancelling the contract, be entitled to purchase goods 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 judgement 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 supplier as having no objection and proceed with the restriction.

23.5 Any restriction imposed on any person by the purchaser will, at the discretion of the purchaser, 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 purchaser 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. Antidumping and countervailing duties and rights

24.1 When, after the date of bid, provisional payments are required, or anti-dumping 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 supplier to the purchaser or the purchaser may deduct such amounts from moneys (if any) which may otherwise be due to the supplier in regard to goods 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 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 for goods delivered and / or services rendered according to the prescripts of the contract.

28. Limitation of Liability

28.1 Except in cases of criminal negligence or wilful misconduct, and in the case of infringement pursuant to Clause 6;

(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.

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 SARS must have certified that the tax matters of the preferred bidder are in order.

32.4 No contract shall be concluded with any bidder whose municipal rates and taxes and municipal services charges are in arrears.

33. Transfer of Contracts

33.1 The contractor shall not abandon, transfer, cede assign or sublet a contract or part thereof without the written permission of the purchaser.

34. Amendment of contracts

34.1 No agreement to amend or vary a contract or order or the conditions, stipulations or provisions thereof shall be valid and of any force unless such agreement to amend or vary is entered into in writing and signed by the contracting parties. Any waiver of the requirement that the agreement to amend or vary shall be in writing, shall also be in writing.

35. Prohibition of restrictive practices

35.1 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.

35.2 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 section 59 of the Competition Act No 89 0f 1998.

35.3 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.

SECTION 6: SPECIAL / ADDITIONAL CONDITIONS OF CONTRACT

The ***Conditions of Contract*** make reference to the ***Special Conditions of Contract (SSC)*** for details that apply specifically to this bid. The ***Special Conditions of Contract*** shall have precedence in the interpretation of any ambiguity or inconsistency between it and the ***Conditions of Contract***.

Each item below is cross-referenced to the clause in the ***Conditions of Contract*** to which it mainly applies.

SCC 1.2 **CONTRACT**

This contract is for a period of 36 months.

SCC 7.1 **PERFORMANCE SECURITY**

The liability of the Performance Security shall be Nil.

SCC 16.1 **PAYMENT**

The Contractor shall submit to the Department concerned a detailed account which shall reflect the identifying number of each item / service. Payment will be made on this account when checked and substantiated by the authorised official.

Payment for goods or services received and accepted by the Municipality shall be made no later than 30 days after submission of invoice or claim, provided however that all the terms of the contract are duly complied with.

Payment will be made only to the supplier. Factoring arrangements will not be accepted.

SCC 17 **PRICES**

Prices are fixed for the duration of the contract.

SCC 21.1 **DELAYS IN THE SUPPLIER'S PERFORMANCE**

If the supplier fails to deliver any or all the goods/services or to perform the project implementation services within 50 days of letter of award, the purchaser shall, without prejudice to its other remedies under the contract, deduct from the contract price - A penalty of 0.05% of the order value for each day delivery is delayed will apply for delay in project implementation. The purchaser may also consider termination of the contract pursuant to GCC Clause 23."

Performance in this contract shall be governed by the Service Level Agreement between the Municipality and the Service Provider. The service must be running and available on a 24X7 basis to collect data from in scope device sources, analyse, triage, investigate, respond and notify the Municipality of security incidents. Proposed response times for different levels of priority is shown in the table below, and that will be upon generation of an alert from the unified security monitoring platform or from threat hunting exercises that creates a security incident, and the Security Operations Centre Team must triage, investigate, contain as relevant, respond and escalate with mitigation recommendations to the specialist and Municipality Teams to fully address gaps.

Priority level	Response time (Acknowledge receipt)	Definition	Triage, Investigation, Response and provide mitigation recommendations
1- Critical	15 minutes	Items requiring immediate action, such as indicators of a Distributed Denial of Service, DNS cache poisoning, security breach/intrusion or similar successful attack, exploitation of vulnerable systems, network or account compromise, backdoor installation, evidence of a malware outbreak, lateral movement, obfuscation, privilege escalation, command & control, exfiltration/destruction of data in progress on critical systems.	30 minutes from notification
2- High	30 minutes	Items requiring prompt action, like a major policy violation, reconnaissance, weaponization, intrusion attempts, malware delivery attempts, and other similar risks or threats.	1 hour from Notification
3 - Medium	30 minutes	Items requiring non-urgent attention such as minor policy issues, a single virus occurrence, or a small risk affecting small, limited users.	4 hours from notification
4 - Low	60 minutes	General security related queries	6 hours from notification

SCC 22.1 **PENALTIES**

Subject to GCC clause 22;

If the event the successful tender does not respond to security alerts/incidents detected within the required response time, as indicated in the table below, a penalty as reflected in the table below of the monthly cost X no of hours beyond required response times will be levied (as a penalty):

Priority level	Required Response time	Penalty percentage
1- Critical	30 min	3%
2- High	1 hour	2%
3- Medium	4 hours	1%
4 - low	6 hours	0.5%

The purchaser may also consider termination of the contract pursuant to GCC Clause 23."

ADDITIONAL CONDITIONS OF CONTRACT

ACC1 PERFORMANCE MONITORING & ASSESSMENT OF SERVICE PROVIDERS

For contract awards that are greater than R10m, the Contractor shall be subjected to "Performance Monitoring" assessments in terms of the applicable Section of the Council's current Supply Chain Management Policy.

ACC2 QUALITY OF PRODUCTS

No inferior products will be accepted under this enquiry.

Should there be any cause for complaint against the standard of service or quality of products offered which is not resolved within a period of 10 working days, the Municipality reserves the right to cancel the contract after serving one month's notice, in writing, to the supplier involved. Should such notice be given, the supplier shall nevertheless be obliged to perform the duties covered by the contract up to the date of expiration of the period of notice.

ACC3 SATISFACTORY PERFORMANCE

The supplier shall employ for the purpose of this contract only such personnel as are careful and competent and the Municipality shall be at liberty to object to and require the supplier to remove from the job forthwith any person, including supervisory staff, employed by the supplier who, in the opinion of the Municipality, misconducts himself/herself or is incompetent or negligent in the proper performance of his/her duties and such person shall not again be employed upon this contract without the permission of the Municipality.

ACC4 OCCUPATIONAL INJURIES AND DISEASES ACT

This act replaces the Workmen's Compensation Act:

The supplier **shall, before commencement of work, produce documentary proof to the Deputy Municipal Manager, Treasury: Finance that he has complied in all respects with the provisions of the Occupational Injuries and Diseases Act**. The supplier undertakes that he/she will perform and comply with all provisions of the Occupational Injuries and Diseases Act and more particularly that he/she will render all returns and pay all assessments for which he/she is liable in terms of such Act.

ACC5 DAMAGE TO PERSONS AND PROPERTY

(1) The supplier **shall** indemnify and keep indemnified the Council against any claim for death, injury, damage or loss to any person or property whatsoever in respect thereof or in relation thereto.

(2) The supplier enters into this contract as an independent contractor and shall be solely liable in respect of any claim for death, injury, damage or loss to any person or property whatsoever in respect thereof or in relation thereto.

ACC6 RATE OF EXCHANGE VARIATION

Where the goods are imported the Contractor shall within seven days of date of Official Purchase Order, arrange through his bankers for the foreign commitment to be covered forward down to

the Rand in order to fix the rate of exchange. The Contractor shall notify the Municipality as soon as possible thereafter regarding the rate which has been fixed on such forward exchange. The forward cover shall be from a reputable South African bank. The Contractor is to confirm with the employer prior to placing forward cover if the service provider is acceptable.

Any increase or decrease between the basic rate of exchange as at 12:00 on the date of close of the bid and that existing at the date of establishment of the forward exchange cover within the period stipulated above shall be paid or deducted by the Municipality. Upon the failure of the Contractor to arrange forward exchange cover, the Contractor shall be liable should there be an increase in the basic rate of exchange occurring after the last-mentioned date.

The bank charges incurred in obtaining the forward exchange cover must be included in the Tenderer's bid.

ACC7 **ESTIMATED QUANITITIES**

The quantities stated in Section 8 are applicable for evaluation purposes only. The final quantity of goods and services required shall vary, depending on the total number of actual instances service/goods will be required over the Contract Period. The rates tendered shall be applicable, irrespective of the total quantity of goods and services procured over the contract duration.

ACC8 **SERVICE PROVIDER OFFICE REQUIREMENTS**

The service provider must have, for the duration of the contract, a local presence (within the geographical area of Kwa-Zulu Natal).

ACC9 **SKILLS TRANSFER**

The Service Provider must provide and execute a skill transfer plan covering the duration of the contract whereby all relevant skills are transferred to nominated municipal employees. The appointed service provider will be expected to conduct skill transfer to nominated municipal employees 20 hours per month.

The Service provider will be required to submit monthly reports on the skills transfer plan and progress made thereof, monthly.

The skills transfer must provide experience and necessary skillset for monitoring, investigating, and responding to Security Incidents logged from the managed Cyber Security Operations Centre.

The Skills Transfer Plan proposed by the Service Provider will be reviewed and coordinated with IT.

The Skills Transfer Plan shall form a part of the Service Level Agreement to be signed by the successful Service Provider.

The Service provider will be required to also provide OEM formal relevant training and certification vouchers to at least 4 IT security employees on the proposed platform security/solutions proposed.

SECTION 7: SCOPE AND SPECIFICATION OF REQUIRED SUPPLY / SERVICES

Background

With Cyber risks and the threat landscape evolving, with Artificial intelligence (AI) accelerating the scale and sophistication of cyber threats (autonomous agents uncover exploits faster), it is essential for the eThekwini Municipality (eM) to ensure that it maintains a good Information and Communication Technology (ICT), Operational Technology (OT) security posture that will enable the achievement of service delivery objectives reliant on digital systems and ensure resiliency and adequate protection of information held and processed.

Currently eThekwini Municipality (Municipality) is utilising an integrated real-time solution to provide insight and single pane visibility into security risks and threats across the different critical ICT infrastructure and systems from a Managed service provider to monitor, detect or identify, investigate threats or security incidents, through relevant system to correlate or aggregate events from the multiple sources to fully understand the extent of incidents and find answers and respond or resolve on a 24X7 basis, from the SOC team, and also enable by AI Network Detection and Response solution at the network level to autonomously respond to novel or stealthy attacks, that pass endpoint detection and response.

Driven by that commitment to improve maintain a security posture across different critical ICT environments and have effective proactive, real-time cyber security services. The Municipality is inviting bids from leading and accredited Managed Security Service Providers (MSSP) to define, roll-out, manage, monitor and support a comprehensive Security Operations Center (SOC) service that is cost-effective for the Municipality, which will provide an integrated security platform (complete visibility) to monitor the security posture and enhance the Municipality's capabilities to effectively defend against security breaches and proactively identify, respond to advanced cyber threats or risks in real-time at machine speed, shortening the dwell time and mean time to detect threats.

As can be noted that cybersecurity specialist skills are scare and difficult to acquire and retain and building and effectively operating a SOC with all capabilities is expensive. The Municipality intends engaging a MSSP that has a sustainable and proven business model, recognized accreditation, established customer-base, distinguishable solution accelerators and enablers, highly qualified and expert's security personnel with suitable complement, continuity measures and relevant capabilities of a modern world-class SOC and presence in South Africa/KwaZulu Natal, while maintaining the ability to support and respond to evolving cybersecurity requirements.

A Scope of Supply / Services

The end goal is for the eThekwini Municipality to be able to have continuous full visibility and insight across the different critical ICT environments (single pane dashboard for all cyber events), to be able to proactively monitor in real-time the security posture, anticipate, address and withstand threats being enabled by appropriate intelligent solutions or platforms that drives actionable intelligence, autonomous response and expert security analyst and specialist to monitor, detect, hunt, investigate, triage, and respond quicker to advanced threats or sophisticated cyber-attacks across the different lifecycle “unified kill chain”. Be able to effectively manage information security incidents, remediate issues and gain insights into improvements necessary to improve cyber resilience, enabled by relevant comprehensive tactics and techniques cyber defense frameworks to identify weaknesses and assist mitigate those risks.

eThekwini Municipality needs to be able to proactively monitor and defend against disruptive cyber events based on a robust self-healing digital immunity, and active cyber defense, real-time cyber visibility on real-time threats, through machine-added detection, automated hunting, and advanced situational awareness, being reliant on automation, machine learning, artificial intelligence adaptive cyber-threat detection, and autonomous response and expert security specialists on a 24X7 basis to address cyber threats to the business effectively and proactively. Also having the ability to rapidly restore digital platforms being assisted by expert responders and digital forensic, adapt, and recover mission-critical systems, and continuously assess and measure the state of cyber performance and continuous improvement to support the business (protect critical data, reduce risk, and enhance information security governance).

B Specifications

	Managed Unified modern Agentic Security Operation Center (SOC) service requirements	
1)	**The service must provide an enterprise unified modern cybersecurity management platform that provides:** a) Real-time asset discovery, with built in CMDB, visibility, threat monitoring and detection, in a form of a modern agentic Security Information and Events Management (SIEM) system or similar solution, with advanced analytics, built in Orchestration, Automation, and Response powered by Artificial Intelligence (AI), and capabilities to continuously manage and correlate security logs or events and continuously identify vulnerabilities; threats, exposure and manage (CTEM); respond to intrusions from multiple sources (core network devices, server Operating Systems and application systems, users, endpoint protection/security platform, Cloud computing as listed table 1 below). b) Agentless collection of information and seamless integration with other deployed security vendor products and different ICT/OT environments, utilising relevant appliances and software to monitor and collect relevant metadata for storage, analysis and to detect systems and network threats covering all in scope devices listed in the table 1 below and monitoring east-west and north-south traffic. Agents can be utilised for a few servers that cannot work agentless, and ensuring	

	compatibility/support to pull logs from systems such as Oracle JD Edwards, Revenue Management System, VMWare ESXi etc. c) Automation of detection and response to threats with machine learning and artificial intelligence (AI), for automated threat detection, alerting, triaging, investigation, and response, with relevant playbooks and use case library out-of-the-box, and custom use cases to enable real time response to threats. d) Have User and Entity Behaviour Analysis (UEBA) analysis to model baseline standard behaviour for all users and entities in the critical ICT/OT environment, such as servers, systems, routers, core switches and data repositories, utilising a variety of analytics techniques, to identify activities that are anomalous compared to the established baselines, discover threats, and detect security incidents across the unified cyber kill chain and unauthorised internal activities. e) A comprehensive integrated advanced and timely Global Threat Detection (Threat Intelligence), and relevant threat research and breach detection to enable detection of advanced threats across the unified kill chain. Analyze internal network traffic, log files, and endpoint behavior for indicators of compromise (IoC) or abnormal activity, combine threat intelligence with security data, to intelligently detect and respond to attacks in the ICT/OT environment, in real-time. f) Continuous External Attack Surface Monitoring and dark web monitoring service for the municipality public facing assets, domains, and monitor breaches related to major third-party vendors/suppliers utilised by the municipality. g) Honeypots (client listening for connections/client request etc, emulating crucial systems) must be implemented in the demilitarized zone and for internal servers, to gain insights and intel on different attempted attacks and behaviour and techniques form malicious actors. h) An integrated dashboard, with all security alerts categorised accordingly, case and incident management platform with workflow capabilities, allowing for escalation of all incidents. i) Capabilities to monitor, threat hunt, analyse, detect, report on all security incidents affecting all devices in scope, and provide alerts, dashboard portal for the Municipality ICT Team, that allows drilling down on details, providing actionable intelligence on all threats and remediation where relevant and escalate relevant recommendations for remediating other threats and security improvements. j) Risks and compliance monitoring and reporting based on industry standards such as ISO 27001/2, GDPR/POPIA etc. k) Rapid post breach incident response, recovery and digital forensic capability to uncover incident chain of events/reconstruction of sessions, detailed view of exactly what happened and to assist with investigations, and post incident root cause analysis.	
	l) Autonomous AI-powered Network Detection and Response- NDR (that's accredited as a leader) that utilises self-learning AI and agentic AI analysts to establish baseline network behaviours and detect anomalous patterns and respond/defend network (full autonomous desktops and semi-autonomous for servers, with human intervention), across 12 000 devices (Servers and Desktops etc). The system must autonomously neutralize threats (e.g., TCP connection resets, device isolation) in real-time by identifying and stopping lateral movements and data exfiltration, beaconing, to algorithmic/C2 domains without requiring prior knowledge of specific attack signatures. Automatic preservation, parsing, and correlating of deep-dive forensic artifacts (including timeline, disk, memory, process data, and system logs).	
	m) SOC service data processing must be in a South African data centre, with retention and archival, backup of historic data accordingly for at least 18 months, with 90 days being available for real-time event searching, and with capabilities to download any required threat information, all logs collected from different devices and environments must be correlated and stored for relevant investigations. n) Experienced and skilled resources (SOC/security analyst, and cybersecurity specialist) for security monitoring, analysis, triage, threat hunting, incident investigation, response, digital forensic, threats tactics and techniques, research, remediation, and response on a 24X7 basis, focused targeted penetration testing or continuous validation every quarter for specific attack surface.	
	Other requirements from the managed SOC service provider: a) In-case of a major cyber event the service provider would be required to provide relevant extra cybersecurity expert resource (s) to do a thorough investigation and assist remedy that incident and where applicable come at the Municipality site to assist with incident investigation, forensics and response or recovery services (cater for at least 300 hours per year, for experts for major incident investigation and response services, which shall be utilised for advanced cybersecurity posture assessments if not utilised at the end of each year).	

b) Provide relevant security tools, appliances, servers and deploy, implement, onboard, integrate, and provide security operations management, support, and Dashboard view and provide skills transfer for key ICT Teams.
c) Provide Information on the hosting location (South Africa), SOC service platform capabilities, architecture, tools, process, data security, collection options, high-availability, failover, redundancy, and continuity measures for the managed SOC service that is proposed, and security specialists staff complement. Include an implementation plan and project management information.
d) Provide senior experienced project manager certified as an advanced project manager, and relevant engineers/cyber expert to ensure efficient implementation and onboarding of all the required services within the set limits of less than 50 days, from receiving the letter of award.
e) Show that having experienced and adequate management team for the upkeep of the managed services (supervision and maintenance for the duration of the contract).

List of devices / servers /users/Data centres

Data sources, to base the log size estimations based on industry benchmark, which should be complete and having relevant buffer to accommodate for any peaks.

Table 1:

No.	Category	Details	Qty
1.	Network	Core and distribution routers/switches (CISCO and Huawei)	60
2.	Firewalls	External and Internal Firewalls (UTM, ID/PS, VPN, WAF, Proxy, Gateways, NAC etc) – (Forti)	5
3.	Total number of servers		**540**
	General Production Servers	Microsoft windows (88% virtual and 12% physical)	481
	General Production Servers	Linux and Unix	59
		(I) Database Servers: Oracle, SQL and DB2	79
		(II) Web servers: Exchange, Applications, and web servers	68
		(III) Domain Controllers: Active Directory servers	15
		(IV) Endpoint security platforms: Utilising Trend Micro SaaS, Apex and Workload security for threat protection and detection for 11460 endpoints and 540 servers)	2
4.	Cloud services	Microsoft Office 365 (14 460 users) and Azure workloads (20), also utilising Defender for some devices.	2
5.	Data centre	Main (FM), Secondary (OF), Electricity and two Disaster Recovery (Local collectors/syslog servers must be provided for each of the sites as part of the manged services, and adequate NDR appliances covering server farm and desktop subnets, and any infrastructure required for the	5

			managed services.)		

C) MINIMAL USE CASES REQUIRED AS PART OF THE SPECIFICATION ABOVE FOR THE MANAGED SOC SERVICE.

1) Security Monitoring, correlation, and threat detection

(a) The Managed Security Service Provider (MSSP) should monitor security logs to detect malicious or abnormal events and raise alerts for any suspicious events that may lead to a security breach.

(b) The unified security platform should have capability to collect logs from most of the standard platforms like Windows, Linux, Unix, Firewall, Network and other security devices or solutions, etc, providing relevant log collection and management for all in scope devices, applications, and different Operating systems from the below and more:
- Syslog, Log File, Netflow; ODBC databases, SNMP, VMware, Windows events, Linux and Unix operating system logs, Flat files etc

(c) The unified security platform should be able to collect logs from most of the standard network security devices, Databases, Web servers and cloud services (Azure), SAAS Solutions: O365, etc.

(d) MSSP should have capability to integrate logs from non-standard application and devices, and the platform provided should be able to process them for generating alerts and reports.

(e) MSSP should detect both internal & external attacks.

(f) MSSP platform should also be able to monitor the following:
- Monitor Access to Sensitive Data (i.e. Personal Information, or sensitive proprietary data)
- Database access including logins, client IP, server IP and source program information.
- Track and audit administrative commands, and privileged accounts.

(g) MSSP platform should carry out correlations amongst the logs from multiple sources to detect multi-vector attacks.

(h) MSSP should bring workflows and solutions that can automate majority of the incident response activities such as false positive management, managing whitelists, escalation workflow, SLA management etc. Alerts should be notified to relevant Municipality ICT personnel only after proper triage process.

(i) Alerts from the SIEM/log management should be enriched with context data, environmental data, vulnerability data, historical data, threat intelligence etc.

(j) MSSP operations team should send alerts with details of mitigation steps to designated personnel of the Municipality.

(k) Reports should be provided on vulnerability status along with mitigation recommendations, based on the integrated continuous vulnerability assessments for the unified Threat management platform proposed to get a 360-degree view of the assets and exposure risks.

(l) MSSP reports should follow industry best practice and international standards like ISO 27001, PCI, SOC1, SOC2 etc. and regulatory requirement like GDPR/POPIA.

(m) Historical parameters should include and not limited to attack volume, attacker volume, and destination volume for every alert.

(n) MSSP should give long term solution to prevent such threats in future, Define, Develop, and implement Use Cases and relevant processes based on standard methodologies such as the Cyber Kill Chain, and the MITRE ATT&CK framework.

(o) MSSP to assist the Municipality to ensure the log retention is as per local regulatory requirements, and that the log and incident information is kept for as long as possible.

(p) MSSP solution should have capabilities to define rules on event logs captured from various sources to detect suspicious activities such as the follows (provide dashboard view)
- Failed login attempts

- Successful Login attempts from suspicious locations or unusual systems
- Authorization attempts outside of approved list
- Vendor logins from unauthorized subnets
- Vertical & Horizontal port scans
- Traffic from blacklisted Ips
- Login attempts at unusual timings
- Network Intrusion and exploits attempts

(q) MSSP platform should be able to provide charts for top attacks & attackers, OWASP based threat analysis, Trending threats, attack demographics etc.

(r) The proposed platform shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.

(s) The proposed solution should prevent tampering of any type of logs and log any attempts to tamper with logs. It must provide encrypted transmission of log data to the log management system. Any failures of the event collection infrastructure must be detected, and ICT operations personnel must be notified.

(t) The solution should be able to support enrichment of data with contextual information like Geo Data, malicious IPs, Domains, URLs, Threat Intel and custom specified tags and annotations. The enrichment fields should be indexed along with the event in real-time at an individual event level and not done as a separate lookup process.

(u) Using the outbound plugins architecture, the Vendor must provide integrations with services like ticketing systems, messaging platforms, vulnerability management such as SCCM etc. to facilitate automation of workflows.

(v) MSSP should detect both internal and external attacks. In addition to security attacks on ICT infrastructure, should also monitor for security events on critical business applications, databases and identify network behaviour, user behaviour anomalies.

(w) MSSP should monitor, detect, and manage incidents for the following minimum set of ICT infrastructure security events. This is indicative minimum list and is not a comprehensive or complete set of events.

- Buffer Overflow attacks,
- Port and vulnerability Scans
- Brute force, Password cracking
- Kerberos and NTLM relay attacks
- Malware outbreaks and RATs
- File access failures
- Stealthy attacks, and Advanced persistence threats
- Unauthorized service restarts
- Unauthorized service/process creation
- Unauthorized changes to firewall rules
- Unauthorized access to systems
- SQL injection
- Cross site scripting
- All layer 7 web attacks via internet / intranet

(x) MSSP should monitor, detect and manage incidents for the following minimum set of business application security events. This is an indicative list and is not a comprehensive / complete set of events.

- Attempted segregation of duties violations
- Attempted access violations
- Critical user additions, deletions
- Creation, deletion and modification of critical application roles/groups
- Changes to permissions or authorizations for critical application roles/groups
- Changes to account and password policies in the application
- Changes to critical application parameters
- Changes to audit parameters

2) Incident Analysis

(a) The Proposed solution should support centralized incident management to prioritize and manage security incidents.
(b) Solution should support triaging of alerts from several security products including Firewalls, IPS, Endpoint security, EDR etc.
(c) Solution should support machine driven triaging algorithms that considers contextual parameters, historical behavior and external threat intelligence to enrich and arrive at a triage score in real time. Triage score should form the basis for prioritizing the alert and further action on the same.
(d) Environmental parameters should include and not limited to asset criticality, user criticality, and vulnerability status for every alert.
(e) Historical parameters should include and not limited to attack volume, attacker volume, destination volume for every alert, severity of alert and so on.
(f) Central Threat Intelligence feed should also be applied to identify threats through known bad actors.
(g) Solution should support a rule engine for users to define custom triage rule. Rule engine should support asset data fields, event data fields, user data fields, triage score, and triage parameters.
(h) Solution should enable investigation of triaged alert/custom alerts deemed critical.
(i) Investigation module should integrate with different log sources on demand to pull data related to the investigated alert. It should also include charting and graphs to analyse data.
(j) Solution should have features to analyse impact of the attack on the targeted asset including configurations, Indicators of Compromise (IOCs), external network connections.
(k) Solution should support features to identify attacker attributes including threat intelligence score of attackers, who-is lookup information, geo- mapping in a single console.
(l) Solution should support models to build up the entire attack chain from attack inception, progress of the attack and spread to attack in the network.
(m) Solution should provide run books for investigation steps corresponding to different types of attacks, derive attack inception and progress of the attack i.e. Detect Zero day attacks, Bots, Attack origin and Blast Radius.
(n) Solution should support integration with open source or commercial IOC sources, supported sources should provide relevant threat intel.
(o) Solution should support features to analyse and identify the impact of the attack on other assets.
(p) Solution should support models to derive attack inception and progress of the attack, with relevant investigation models.
(q) Solution should provide case management features to store raw and analyzed data for a specific alert or set of alerts, storing different artefacts related to an investigation.
(r) Solution should support quick search across stored datasets in the Solution.
(s) Solution should provide run books for investigation steps corresponding to different types of attacks.
(t) Solution should provide features to do free flow visual analysis of alerts and logs from integrated data sources based on custom criteria. This visual analytics feature should have appropriate graphical representation options to visualize large scale data.

3) Incident Response

(a) Solution should support quick response to an ongoing incident or serious threats with remote configuration of parameters in servers/desktops, Firewalls, AD (Active Directory), IPS, Network Switches & Routers.
(b) Automated Remediation for responding to commodity threats (e.g., recall malicious mails from inboxes, isolate devices, block bad/malicious IPs/URL Firewall, Disable compromised users in Active Directory, etc.). Autonomous AI driven response with minimal human supervision.
(c) Orchestration (connect disparate tools), Automation (execute workflows via playbooks), and Response (auto remediating threats).: Ensure broad, API-driven connectors to integrate third-party tools like SIEM, EDR, firewalls, etc into a unified ecosystem. Playbook & Workflow Automation: No-code/low-code visual editors to build standardized incident response

workflows for common threats. Threat Intel Management & Triage: Automated ingestion, deduplication, and normalization of IOCs from various feeds, mapped to threat frameworks. Centralized Case Management: Unified workspaces with shared task tracking, evidence chains of custody, and automatic audit logs for compliance. AI & Agentic Capabilities: Advanced features like alert enrichment, contextual risk-based scoring, and AI agents for multi-step investigations.

(d) Solution should support multiple configuration parameters to servers/desktops including removal/changes to services, users, registry keys, software, and browser plugins.
(e) Solution should support the full workflow for incident classification, incident coordination such as assigning activities to different teams and tracking for closure, escalation of tasks, and exception approvals.
(f) Solution should support the full workflow for incident coordination, assigning activities to different teams and tracking for closure.
(g) Solution should support the workflow required to approve such auto mitigation action or have option to exempt certain auto mitigation from approval process.
(h) Solution should support escalation workflows. With relevant escalation matrix within solution along with the levels and utilise relevant escalation medium (SMS/email)
(i) Solution should support tracking of security exception approvals for those threats and incidents for which remediation is not possible or compensating controls are available.
(j) Solution should integrate with external service desks such as i.e., Internal ticketing tool (CA Uni-centre) for leveraging existing service desk platform or Service Provider to provide Ticketing tool that is part of the SOC operations management to the Municipality.
(k) Solution should provide alert details and investigation outcomes linked and viewable for relevant remediation tickets.
(l) MSSP should provide Incident Reports with classification, chronology of events, RCA, IOC, and track impacted assets related to an incident, and provide tools for Response based on data and analytics.
(m) Solution should have ability for quick Counter Response by integrating with devices such as firewall or Office 365 for blocking traffic or quarantine system, or disable account
(n) The MSSP platform should track the following at a minimum:
    - Usage of Ticketing and case management workflow, Classification of incidents.
    - Maintain track of first response and subsequent measures taken for the Incident.
    - Maintain chronological order of events related to incident response.
(o) MSSP Incident response should include analysis, investigation of end points logs (such as servers) if required to conclude the investigation, and there should be centralized incident management to prioritize and manage security incidents.
(p) MSSP should bring a platform which facilitates collaboration between SOC team and the Municipality ICT with comments on incidents, maintaining a history of conversation with timeline, ability to add artifacts.

4) Autonomous Network Detection and Response (NDR)

a) The solution must learn "normal" behavior to detect subtle deviations and unknown threats (the "unknown unknowns") that evade conventional signature-based firewalls, Zero-Day & Novel Attack Detection.
b) The solution must continuously monitor East-West and North-South traffic to flag anomalous admin/RDP sessions, unusual SMB enumeration, and suspicious network scans, Lateral Movement & Internal Threats.
c) The solution must identify "low and slow" smash-and-grab data transfers or DNS tunnelling attempts, even when hidden within encrypted traffic. Must monitor total data volumes, destinations, and transfer times to detect abnormal outbound connections and unauthorized bulk data transfers, Data Exfiltration & Tunnelling blocking.
d) The solution must profile and categorize assets with IP and immediately flag them if they communicate with unauthorized or rogue servers, IoT/OT & Unmanaged Devices protection.
e) The vendor proposal should include active neutralization capabilities that quarantine compromised devices or block specific suspicious connections without disrupting legitimate

business operations, utilising Autonomous Response.

f) The system must utilize unsupervised machine learning to autonomously build a dynamic model of every user, device, and network connection, utilising Self-Learning AI.
g) The architecture must not require continuous manual updates of rules, indicators of compromise (IoCs), or pre-configured threat intelligence.
h) The solution must automatically stitch together isolated alerts into a complete incident narrative, reducing human triage and investigation times, Automated Investigation (with AI Analyst):
i) Full-Stack Visibility: It must ingest traffic across physical, virtual, cloud, and hybrid infrastructures, processing both north-south and east-west telemetry.
j) Multi-Domain Correlation: The platform should natively integrate with endpoint, email, and cloud telemetry to map cross-estate attacks.
k) Unified Telemetry: Native capability to combine mixed network traffic and endpoint process telemetry to trace lateral movement and exfiltration back to the root-cause process.
l) Ecosystem API Integration: Seamless integration with identity platforms and email security layers to track credentials used in lateral movement and prevent secondary attacks.
m) Attack Path Modelling: Visual dashboards that map all potential attack paths between vulnerable assets to proactively identify and close gaps before attackers can exploit them

5) Threat Hunting

(a) MSSP to use algorithms and relevant tools to actively hunt of attacks in large volume of data and create alerts that are passed on to IT Team for remediation. Supports use of Big data platform for collection and analysis.
(b) MSSP should define, develop, implement, update and maintain Hunting Framework which contains:
- Create Strategic Hunt Missions which are objective based to identify malicious activity that has not triggered an alert.
- Search for Indicators of Compromise received from Threat Intelligence and Analytics.
- Create knowledge base of IOCs

(c) MSSP solution should provide security analytics to be able to detect unknown attacks. The analytics service should have models that are able to detect attacks in various stages of a cyber kill chain.
(d) MSSP should be able to detect threats from various attacks vectors such as malware, web application attacks, network attacks, watering hole attacks, DNS attacks, targeted attacks, rogues, insider threat, data breaches, and data exfiltration. With more use cases which can detect above attacks and other advanced attacks using pre-built machine learning techniques and analytical models.
(e) The Analytics utilised should use machine learning techniques and use multiple sources to identify malicious activity. A minimum the following sources should be used:
- Netflow
- Firewall
- IPS/IDS
- Proxy
- Windows logs
- Sys logs
- DNS
- Endpoint Security Protection
- Encrypted traffic (provide for deep inspection) etc.

(f) Solution should have pre-built AI models to detect targeted attacks (unknown attacks from unknown threat actors).
(g) Solution should have analytical models to detect different stages of Cyber Kill chain.
(h) Network Threat Hunting should leverage existing network sources for better detection of advanced attacks. Network sources should include Netflow, Proxy, DNS, IPS, VPN, Firewall, WAF, AD/Windows, Email logs, Security gateways etc.
(i) Network threat hunting should use Artificial intelligence and smart rules on network sources and enable hunting for attacks including but not limited to reconnaissance, NTLM relays,

access attempts/attacks, Lateral Movement, Malware Beaconing, Data Exfiltration, Watering Hole, Targeted network attacks, zero-day exploits, Dynamic DNS attacks, execution of malicious PowerShell scripts, privilege escalation, defense evasion, covering all the MITRE ATT&CK tactics and techniques.

(j) The service must be capable of identifying suspicious undiscovered communication patterns. The service must support detection of newly discovered pattern in future.

(k) The service should identify network traffic from potentially risky applications (i.e., file sharing, peer-to-peer, etc.) and support Deep Packet Inspection (DPI) to classify protocols & applications by capturing packet.

6) Endpoint Detection & Response Service

(a) Integrate the Unified Security Management solution that will be utilised for the SOC managed service with the current Trend Micro platform XDR/DDI/Workload Security, and with any relevant appliances in the network such as firewall if that service will provide or enable intelligence, to expose threats concealed in network traffic and for Endpoint threat hunting, so as to hunt for Process anomalies, Service anomalies, Hash values, Connection anomalies and indicators of compromises.

(b) Utilise that intelligence to detect anomalies at the endpoint/servers such as:
- Detect Command and control activities
- Detect Data stealing activities
- Assess weakness by looking at vulnerabilities.
- Searching for IOCs
- Outlier detection of active system process, driver, services, network connections, etc.
- Looking at forensic artifacts (Name, Hash code, Size, Loaded DLLs) of all binaries running in Municipality systems. Matching of forensic artifacts against known indicator of compromise.
- Segregating unknown forensic artifacts from known forensics artifacts.
- Clustering and analysing of unknown forensic artifacts to find outlier binaries, and a full chain of events and related events.

(c) Advise on threat hunting results to enable for quick response actions, working with the eM team such as:
- Killing anomalous processes, deleting malicious binaries.
- Isolating end points.
- Detect threats on endpoints by deploying EDR agents. The service should be able to take containment actions such as isolating infected endpoints.
- Detect user anomalies using a combination of rules and machine learning model. Optionally provide sensors to capture network traffic to detect threats at the network level.

(d) Service should support business application threat hunting for application to detect access and authorization anomalies using application logs, NetFlow.

(e) Services should be able to search proactively and iteratively through a network or logs data to detect and isolate advanced threats that evade Signature based systems (IDS, DLP etc.).

(f) Service should support applying AI models on firewall and web server events to detect targeted web application attacks.

(g) MSSP should submit a daily threat hunting based on the threat hunting models to be deployed at the Municipality.

7) User Behavior Analysis (UBA)

(a) Solution should provide UBA dashboard based on various UBA models outcome, to detect malicious/illegal activities performed by users on critical IT systems in scope.

(b) UBA Dashboard should highlight risky users based on objective scoring of users based on composite risk score comprising all behavior anomalies of the user, to enable defining risk thresholds.

(c) Solution to have capabilities to collect user data from variety of sources like Directory Services, IAM, VPN, Proxy, O365, etc.

(d) Service should be able to track user ‘s activities locally and remote network sites and should be able to report usage behavior across the entire network.
(e) The service should incorporate multiple baseline behavioral models which cover behavioral risk categories like Data Exfiltration, Malicious Users, Illicit Behavior, compromised credentials, etc. Also utilising the intelligence gartered from the Dark web monitoring service that is required as part of the SOC.
(f) Provide information on the behavior of users and other entities in the corporate network. Perform monitoring, detection and alerting of anomalies. Provide for multiple use cases, for employee monitoring, trusted hosts monitoring, fraud, privilege access and so on.
(g) User monitoring, including baselining and advanced analytics to analyze access and authentication data, establish user context and report on suspicious behavior.
(h) The service should apply sophisticated statistical and quantitative models, such as machine learning and deep learning, on security log and event data to detect anomalous activity, and help understand which incidents are particularly abnormal, suspicious or potentially dangerous. Measure malicious intent or discover, detect and analyze bad activities that the attacker carries on via the compromised account.

8) Threat Intelligence

(a) Service should anticipate likely threats to the Municipality based on global threat events and data and provide proactive measures to prevent such happenings in the Municipality.
(b) Service should support integration of machine-readable threat intelligence from different open and commercial sources. It should support providing weightage against sources and support algorithms to reduce noise and false positives in threat intelligence feeds.
(c) Service should provide strategic threat intelligence about incidents and breaches happening across the global and provide actionable intelligence such as can eM be susceptible to such an attack? If yes, which assets in the organization are susceptible?
(d) Provide IoC’s where relevant and provide mitigation steps for each advisory.
(e) Service must provide near real-time monitoring across the dark web, deep web, and open web to identify leaks of employee credentials, executive impersonation, or sensitive data.
(f) Automated Data Integration: Native support for threat sharing protocols like STIX/TAXII, and ingestion of commercial, open-source, and internal threat feeds.
(g) Risk Scoring: Automated correlation to apply context-specific risk scores to alerts, based on known attacker behavior and relevance to your industry.
(h) Typo-squatting & Brand Monitoring: Proactive domain tracking and automated takedowns of impersonating domains or brands.
(i) Actionable Dashboards: Access to real-time, interactive dashboards to track active threats and ongoing incidents.
(j) Proactive, expert-led threat hunting to identify stealthy, anomalous activities that evade standard automated rules.
(k) Continuously maps, validates, and prioritizes real-world attack surface as it affects eM environment. Continuously scan the entire hybrid environment—including on-premises, cloud, SaaS, endpoints, and external attack surfaces—to capture an accurate inventory of exposures.
(l) Service should apply the threat intelligence to eM assets, network traffic, security event and users to provide actionable report on likely impact on each entity and recommend pre-emptive measures.
(m) Solution should track status of assets against IoCs, CVEs and support the workflow for remediation. As an example, CVEs related to shadow broker release should be used to identify affected assets. Workflow should enable tracking the CVEs to closure through patching/other activities. Service provider should track closure and corresponding risk Reduction.
(n) Service should have machine algorithms to auto-evaluate an asset and assign a business value to the asset and provide actionable intelligence.
(o) Service should support 3rd party / external threat intelligence to aid incident response by bringing in organizational context and internal information available in other sources of security

information.

9) Security Incident and Crisis Management services

(a) The Service provide must provide a Security Incident management plan that will guide how incidents will be handled (service provider to manage the complete IR lifecycle based on relevant best practice such as the NIST Incident Response Process) to enable eM to ensure alignment of that with eM Cyber Incident Response Plan (IRP) and Security Policy.
(b) The Incident and Cyber crisis management support shall be (preferred offsite and, in case of emergency or a major security incident, additional onsite cyber experts support is mandatory) provided by the service provider.
(c) The Managed Service provided will provide a detailed process for managing cyber incidents - describing each phases of the process – prepare, identify, contain, eradicate, recover and learn from the incidents, and that needs to guide the response plan/ strategy which will describe the prioritization of incidents based on impact.
(d) Establish a process for identifying, preventing, detecting, analysing & reporting all Information Security incidents as per the best practices, this may revise time to time as per the requirements, that process shall include the roles and responsibilities and scope of action.
(e) Incident and problem Management, resolution, root cause analysis, and reporting within time limit as per the agreed service requirements, for security incidents and recommend implementation of controls to prevent reoccurrence.
(f) Managed Service Provider must provide on demand timely support by performing investigation and forensic analysis on the logs by doing the necessary analysis on the logs and providing required data on a timely fashion.
(g) Faster incident response by replacing purely ad-hoc activities with Advanced playbooks, analytical tools, incident management tools and reporting, which liberates security analysts to spend less time doing research and more time doing analysis. The service provider shall provide backend professional incident management team support in case of severe incident occurs.

10) General Requirements

(a) Service provider team should have the following skills:
- Security analysts, Incident investigator, Threat hunter, Data scientists, Threat intelligence analytics
- Incident responders, Specialized security team for IOC collection, deeper analysis, forensic investigation.

(b) Solution should provision reconstructing common file formats including word document, image, Web page.
(c) The platform should have machine learning capabilities and other advanced analytics of structured as well as unstructured security and network data.
(d) The Log management solution (Centralized) is required for collection of logs from different log sources, that can be hosted on-premises and VMs with relevant Storage for logs collected will be provided by eM. The bidder ‘s response should include the calculations/ logic used to arrive at the sizing, including catering for adequate redundancy for failures. Alternatively, a secure Cloud hosted logging solution will be accepted if the Service provider can provide such and detail the capacity, network bandwidth requirements and capabilities to ensure continuity and scalability of that and how that will securely collect security information (meta-data) utilising different collectors in the form of appliances or software and only transmit relevant metadata for analysis.
(e) Service Provider shall build the capacity of the SIEM solution that can handle the log retention as mentioned below:
- Three months – Online
- Two Years – Offline
- 24x7x365 real time logs monitoring, analysis and correlation using security analytics, Threat hunting, Threat Intelligence consisting of Indicators of Compromise (IOC) and other

threat intel (vulnerabilities report, incident reports etc.).
- store logs in industry standard solution and format.

(f) The proposed solution should provide end-to end visibility in a form of a SIEM, Security Analytics Platform allowing for indexing, searching, analysis, correlation, reporting, visualization, orchestration and automation of different types of structured / semi-structured data generated within the Municipality.
(g) If connectivity between log collection agents and logger is down, then the Log collector agents should store the logs of at least 3 days and send them once connectivity is established.
(h) Alerting events/incidents and recommending remedial actions.
(i) Incident analysis (Triage) to remove false positives, incident notification.
(j) Daily report of events/incidents, correlation, analysis and recommendations. The daily report shall cover the correlation analysis of all the devices included as part of scope.
(k) Monthly report summarizing the list of events/incidents reported, correlation analysis, recommendations, status of actions by Municipality and other security advisories. It should include the trend analysis comparing the present month's data with the previous month data.
(l) Detect known as well as unknown threats by using machine learning and security analytics.
(m) Consolidate data and extract actionable insight from a variety of intelligence sources and existing security technologies.
(n) Proactive threat hunting on daily basis, which otherwise gets undetected via signature-based systems.
(o) Be Cyber-Ready to respond to attacks swiftly. Complete analysis and correlation of logs from all the devices/solutions under scope.
(p) Provide or develop parsing rules for standard/ non-standard logs respectively. Pre-defined / custom parsers should be available for parsing logs for the following applications but not limited to: - Oracle JD Edward Enterprise one, Opentext Documentum platform, Revenue Management systems, asset management systems, Human resources systems, etc.
(q) The proposed solution should have available connectors to support the standard devices / applications, wherever required the vendor should develop customized connectors for all standard/custom devices/applications at no extra Price.
(r) 24x7x365 uninterrupted security monitoring operations. Submit a report in case of service non availability of the devices along with the status.
(s) Automate security processes to reduce resource drain and threat response Times.
(t) Skilled and capable staff with expertise in at least the following domains:
- Event monitoring and analysis
- Incident detection and response
- Threat Intelligence
- Use Case engineering and new integrations to increase visibility
- Threat Hunting
- Security Analytics
- Correlation of low priority alerts with subsequent alerts to detect multi-stage attacks.

(u) Reduction of remediation time, Automated real time prioritization of alerts
(v) Automated data collection for investigation followed by quick analysis on a single window.
(w) Assisted remediation steps (integration with security devices to push policy/configuration remotely) for faster mitigation of threats.
(x) Provide central dashboard to capture risk posture and maturity levels of eM at any given point of time.
(y) Comprehensive security dashboard (web-based dashboard) for viewing real-time incidents/events, alerts, status of actions taken, tracking of key security metrics and provide security threat scorecards. Vendor shall also provide customized dashboard to suit as per eM requirements.
(z) Vendor shall provide different dashboard and screens for different roles as mentioned below for viewing real-time incidents / events, alerts, status of actions taken etc.:
(aa) Top Management (Company View)
(bb) Information Technology Systems, Network, Security Team (complete and detailed dashboard of security posture of the eM setup being monitored through the managed SOC)
(cc) Auditors (Internal auditor, External auditors etc.)

(dd) Vendor needs to ensure that the managed SOC solution can integrate with the IT system using standard methods/ protocols/ message formats without affecting the existing functionality of eM.
(ee) The Managed SOC setup/infrastructure may be subjected to audit from eM and/or third party and/or regulatory body. It shall be responsibility of the Vendor to co-operate and provide necessary information and support to the auditors. The Vendor must ensure that the audit observations are closed on top priority and to the satisfaction of eM and its appointed auditors. Extreme care should be taken by the Vendor to ensure that the observations do not get repeated in subsequent Audits. Such non-compliance by Vendor shall attract penalty, which should be defined in SLA.
(ff) Service Providers should propose monitoring platforms, to best suit the requirements stated in the RFP.
(gg) To Develop and recommend improvement plans for the managed SOC as needed to maintain an effective and secure computing environment.
(hh) For improvement of the SOC Monitoring at eM, service provider should provide a comprehensive security posture analysis or simulate an attack on a yearly basis and advise on any gaps.
(ii) Effective and Efficient Governance reporting fortnightly, monthly, quarterly and annual reviews.
(jj) SLA's and implementation timelines for the various activities would be mutually agreed while signing a contract with the selected SP. However, SP is expected to give an overall implementation and roll out plan as part of this proposal with templates of SLA, Project Plan, Governance requirements etc.
(kk) Standard Operating Procedure (SOP) shall be developed for all the products /solutions /services provided including alert management, incident management, forensics, report management, log storage and archiving, SOC business continuity, operational documents, escalation matrix, change management, use cases, knowledge documents, playbook etc.
(ll) Analytical reports on Daily, weekly, and Monthly basis and Ad-hoc reports as and when to be provided by service provider.
(mm) IT Forensic services for root cause of incident and investigations as and when required.
(nn) During the exit of the contract or services vendor should provide logs as per retention period from their end to eM without any Price.

Drawings (if applicable)

SECTION 8: BILL OF QUANTITIES / SCHEDULE OF RATES / ACTIVITIES

Services related costs for the Managed SOC.

This does not constitute an actual order, this will guide on the costing for the service, costing to be provided in the below format. For the Unified Agentic Security Monitoring and Response platform **the bidder must provide a separate breakdown of how the collective price (No2) was reached, based on the devices in scope, as the Municipality reserves the right to reduce the number of devices as relevant**.

Item	Description / Item Code	Unit of Measure	Estimated Quantity Required	* Price Year 1 (excl)		* Price Year 2 (excl)		* Price Year 3 (excl)	
				R	c	R	c	R	c
1	Managed Security Operation Center (SOC) services, project implementation and transition (once off)	SUM	1			**Not Applicable**		**Not Applicable**	
2	Unified Security Monitoring and Response Platform (Agentic SIEM/Orchestration /Automation/Behavioural Analysis / Analytics/Threat Intelligence/ vulnerability identification/ CTEM//Forensic/ attack surface monitoring/Dark web monitoring/honeypot etc) licensing for all in scope devices (Core and distribution switches, Firewalls, Servers, Databases, web and application servers, Office 365, Active Directory, Endpoint protection through Vision one etc)	SUM	1						
3	Fully and Semi autonomous Network Detection and Response (NDR) for 12 000 devices	SUM	4						
4	SOC Analysts (24X7 SOC)	Number	6						
5	Cybersecurity Specialist (to be fulltime based at eThekwini Municipality)	Number	1						

Item	Description / Item Code	Unit of Measure	Estimated Quantity Required	* Price Year 1 (excl)		* Price Year 2 (excl)		* Price Year 3 (excl)	
				R	c	R	c	R	c
6	Cybersecurity Experts for major Incident response and recovery services/Security posture assessments (300 hours per year - **at eThekwini Municipality**)	Number	1						
				Year 1		Year 2		Year 3	
			Sub-Totals :						

Sub-Total (excl) = Year1 + Year 2 + Year 3:		
VAT:		
Total (incl) carried forward to the Tender Form:		

SECTION 9 : OFFICIAL TENDER FORM

Part A: OFFER BY TENDERER - In response to **Tender Number : 36703-1i** I / we hereby offer to supply the goods / services detailed hereunder in accordance with the Technical Specification, and subject to the Standard and Special Conditions of Tender (Goods/Services), and General and Special Conditions of Contract, which accompanied your Tender (with which I / we acknowledge myself / ourselves to be fully acquainted) at the price stated below, or in the case of individual rates are indicated in Section 8 : Bill Of Quantities / Schedule of Rates / Activities.

QUOTATION PRICE EXCLUSIVE OF VAT	VAT AMOUNT	QUOTATION PRICE INCLUSIVE OF VAT
R	**R**	*** R**
*** AMOUNT IN WORDS (incl. VAT):**		
.....		

I / We hereby agree that this tender will hold good and remain open for acceptance as specified in the Conditions of Tender or during such other period as may be specified in the Special Conditions of Tender.

eThekwini Vendor Portal Registration Number: **PR**

C.S.D Registration Number: **MAAA**

S.A.R.S Pin Number: _____

Completion of the following is compulsory. Failure to declare the following will invalidate your offer.

Declaration of Interest

Are any of the entity's directors, managers, principle shareholder or stakeholders currently in the service of the state or have been in the service of the state in the past twelve (12) months? ☐ Yes ☐ No				
Is any spouse, child or parent of the entity's directors, managers, principle shareholder or stakeholder currently in the service of the state or have been in the service of the state in the past twelve (12) months? ☐ Yes ☐ No				
Name of entity's member	**Position in Entity**	**Name of Relative (if applicable)**	**Name of State Institution**	**Nature of Relationship**
Do you or any other directors, managers, principle shareholder or stakeholder of your entity have any relationship (spouse, family, friend, associate) with persons in the service of the state and/or who may be involved with the evaluation of this quotation? If yes please furnish particulars below ☐ Yes ☐ No				
Name of entity's member	**Position in Entity**	**Name of Relative (if applicable)**	**Name of State Institution**	**Nature of Relationship**

Refer to the Consolidated MBD Documents in Section 4(d) for the definition of "in service of the State"

*** Signature :** _____ *** Name** *(capitals)*: _____

Date: _____ **Capacity:** _____

*** Name of Business:** _____ **Tel:** _____

Address: _____ **Fax:** _____

_____

*** Denotes Mandatory Information**

Failure to complete the Mandatory Information and sign this Tender Form will invalidate the tender

Part B: ACCEPTANCE BY PURCHASER - The Purchaser, as represented by the following Official, hereby accepts the Tenderer's offer in terms of the Conditions of Tender, Specifications, and Conditions of Contract.

Signature: **Name** *(capitals)*:

Date: **Capacity:**

SECTION 10: ANNEXURES (if applicable)

Insert as required