


TENDER DOCUMENT GOODS AND SERVICES		 CITY OF CAPE TOWN ISIXEKO SASEKAPA STAD KAAPSTAD
SUPPLY CHAIN MANAGEMENT		
SCM - 542	Approved by Branch Manager: February 2024	Version: 10

TENDER NO: 252S/2025/26

TENDER DESCRIPTION: SUPPLY, INSTALLATION, MAINTENANCE AND SUPPORT OF IDENTITY LIFECYCLE MANAGEMENT SOLUTION FOR THE CITY OF CAPE TOWN

CONTRACT PERIOD: 10 YEARS FROM THE COMMENCEMENT DATE OF THE CONTRACT (SUBJECT TO MFMA SECTION 33)

CLOSING DATE	02 July 2026
CLOSING TIME	10:00 am
TENDER BOX NUMBER	207
TENDER FEE	R200

Non – refundable tender fee payable to the City of Cape Town (CCT) for a hard copy of the tender document. This fee is not applicable to website downloads of the tender document.

TENDERER	
NAME of Company/Close Corporation or Partnership / Joint Venture/ Consortium or Sole Proprietor /Individual (hereinafter the "Tenderer")	
TRADING AS (if different from above)	
Registration number of Tenderer	
Physical address and chosen domicilium citandi et executandi of Tenderer	

NATURE OF TENDER OFFER (please indicate below)	
Main Offer (see clause 2.2.11.1)	
Alternative Offer (see clause 2.2.11.1)	

TENDER SERIAL NO.:
SIGNATURES OF CCT OFFICIALS AT TENDER OPENING
1
2
3

TABLE OF CONTENTS

THE TENDER	4
T.1 GENERAL TENDER INFORMATION	4
T.2 CONDITIONS OF TENDER	5
2.1 General.....	5
2.2 Tenderer’s obligations	8
2.3 The CCT’s undertakings.....	18
THE CONTRACT	25
C.1 DETAILS OF TENDERER/SUPPLIER	27
C.2 FORM OF OFFER AND ACCEPTANCE	28
C.2.1 OFFER (TO BE COMPLETED BY THE TENDERER AS PART OF TENDER SUBMISSION)	28
C.2.2 ACCEPTANCE (TO BE COMPLETED BY THE CCT)	29
C.2.3 SCHEDULE OF DEVIATIONS (TO BE COMPLETED BY THE CCT UPON ACCEPTANCE)	30
C.2.4 CONFIRMATION OF RECEIPT (TO BE COMPLETED BY SUPPLIER UPON ACCEPTANCE).....	31
C.3 OCCUPATIONAL HEALTH AND SAFETY AGREEMENT	32
C.4 PRICE SCHEDULE	33
<i>SCHEDULE A. SUPPLY OF SOLUTION FOR IDENTITY GOVERNANCE AND ADMINISTRATION (IGA) SOLUTION(S)</i>	<i>34</i>
<i>SCHEDULE B. SUPPLY OF SOLUTION AND SERVICES FOR PRIVILEGED ACCESS MANAGEMENT (PAM) SOLUTION... ..</i>	<i>41</i>
<i>SCHEDULE C. SUPPLY OF SOLUTION AND SERVICES FOR IDENTITY PROOFING SOLUTION</i>	<i>48</i>
C.5 SPECIFICATION(S).....	55
1. ABBREVIATIONS	55
2. INTRODUCTION AND BACKGROUND	57
3. OVERVIEW OF CCT ENVIRONMENT	57
4. BUSINESS GOAL.....	57
5. OBJECTIVES	57
6. SCOPE OF WORKS	58
6.1. FUNCTIONAL REQUIREMENTS OF IGA SOLUTION.....	58
6.2. NON-FUNCTIONAL REQUIREMENTS for IGA	64
6.3. FUNCTIONAL REQUIREMENTS OF PAM SOLUTION.....	65
6.4. NON- FUNCTIONAL REQUIREMENTS OF PAM SOLUTION	75
6.5. FUNCTIONAL REQUIREMENTS OF IDENTITY PROOFING SOLUTION.....	75
6.6. NON- FUNCTIONAL REQUIREMENTS OF IDENTITY PROOFING SOLUTION.....	78
6.7. GENERAL REQUIREMENTS APPLICABLE TO ALL THREE STREAMS (IGA, PAM AND IDENTITY PROOFING) ...	79
6.8. REQUIREMENTS FOR TRAINING SERVICES ON THE ILM SOLUTION	82
6.9. REQUIREMENTS FOR THE IMPLEMENTATION OF THE ILM SOLUTION	84
6.10. REQUIREMENTS FOR MAINTENANCE AND SUPPORT SERVICES ON THE ILM SOLUTION	94
6.11. REQUIREMENTS FOR PROFESSIONAL SERVICES FOR THE ILM SOLUTION	94
6.12. REQUIREMENTS FOR MANAGED SERVICES.....	96
6.13. REQUIREMENTS FOR CHANGE MANAGEMENT	98
7. DATA HANDLING.....	99
8. PURCHASE ORDERS.....	99
8.1. Redundant Items.....	100
8.2. New Items	100
9. TRADE NAMES OR PROPRIETARY PRODUCTS	101
10. EMPLOYMENT OF SECURITY PERSONNEL	101
11. FORMS FOR CONTRACT ADMINISTRATION.....	101
C.6 SPECIAL CONDITIONS OF CONTRACT	102
C.7 GENERAL CONDITIONS OF CONTRACT	115
C.8 ANNEXURES	125

ANNEXURE A – PRO FORMA INSURANCE BROKER’S WARRANTY	125
ANNEXURE B – MONTHLY PROJECT LABOUR REPORT	126
ANNEXURE C - PRO FORMA PERFORMANCE SECURITY/ GUARANTEE	128
ANNEXURE D - PRO FORMA ADVANCE PAYMENT GUARANTEE	131
ANNEXURE F - TENDER RETURNABLE DOCUMENTS.....	132
<i>Schedule F.1: Contract Price Adjustment and/or Rate of Exchange Variation.....</i>	<i>132</i>
<i>Schedule F.2: Certificate of Authority for Partnerships/ Joint Ventures/ Consortiums</i>	<i>143</i>
<i>Schedule F.3: Declaration for Procurement above R10 million</i>	<i>144</i>
<i>Schedule F.4: Preference Points Claim Form In Terms Of the Preferential Procurement Regulations 2022</i>	<i>145</i>
<i>Schedule F.5: Declaration of Interest – State Employees (MBD 4 amended).....</i>	<i>155</i>
<i>Schedule F.6: Conflict of Interest Declaration</i>	<i>157</i>
<i>Schedule F.7: Declaration of Tenderer’s Past Supply Chain Management Practices (MBD 8)</i>	<i>158</i>
<i>Schedule F.8: Authorisation for the Deduction of Outstanding Amounts Owed to the CCT</i>	<i>160</i>
<i>Schedule F.9: Certificate of Independent Tender Determination</i>	<i>161</i>
<i>Schedule F.10: Proposed Deviations And Qualifications By Tenderer</i>	<i>162</i>
<i>Schedule F.11: List of Other Documents Attached By Tenderer.....</i>	<i>163</i>
<i>Schedule F.12: Record of Addenda to Tender Documents</i>	<i>164</i>
<i>Schedule F.13: Information to Be Provided With the Tender.....</i>	<i>165</i>
<i>Schedule F.14: Appeal Application.....</i>	<i>178</i>
ANNEXURE G – CCT STANDARDS	180
<i>IS&T Standards.....</i>	<i>180</i>
<i>CCT Data Access Specifications</i>	<i>187</i>

THE TENDER

T.1 GENERAL TENDER INFORMATION

- TENDER ADVERTISED** : **29 May 2026**
- SITE VISIT/CLARIFICATION MEETING** : Time: 10am on Date: **5 June 2026**
(Not compulsory, but strongly recommended)
- VENUE FOR SITE VISIT/CLARIFICATION MEETING** : **Cape Town Civic Centre 6th floor Podium Room 2**
12 Hertzog Boulevard, Cape Town
- OR**
- Microsoft Teams**
<https://teams.microsoft.com/meet/361717167943471?p=2B6s367Lkjd5Qy1mM>
- Meeting ID: 361 717 167 943 471**
Passcode: zA7tA9L5
- TENDER BOX & ADDRESS** : **Tender Box as per front cover** at the **Tender & Quotation Boxes Office**, 2nd Floor (Concourse Level), Civic Centre, 12 Hertzog Boulevard, Cape Town.
- : The Tender Document (which includes the Form of Offer and Acceptance) completed and signed in all respects, plus any additional supporting documents required, must be submitted in a sealed envelope with the name and address of the tenderer, the endorsement "**TENDER NO.252S/2025/26: - TENDER DESCRIPTION: SUPPLY, INSTALLATION, MAINTENANCE AND SUPPORT OF IDENTITY LIFECYCLE MANAGEMENT SOLUTION FOR THE CITY OF CAPE TOWN**", the tender box number. and the closing date indicated on the envelope. The sealed envelope must be inserted into the appropriate official tender box before closing time.
- If the tender offer is too large to fit into the abovementioned box or the box is full, please enquire at the public counter (Tender Distribution Office) for alternative instructions. It remains the tenderer's responsibility to ensure that the tender is placed in either the original box or as alternatively instructed.
- CCT TENDER REPRESENTATIVE** : Email: SCM.Tenders21@capetown.gov.za

TENDERERS MUST NOTE THAT WHEREVER THIS DOCUMENT REFERS TO ANY PARTICULAR TRADE MARK, NAME, PATENT, DESIGN, TYPE, SPECIFIC ORIGIN OR PRODUCER, SUCH REFERENCE SHALL BE DEEMED TO BE ACCOMPANIED BY THE WORDS "OR EQUIVALENT"

T.2 CONDITIONS OF TENDER

2.1 General

2.1.1 Actions

2.1.1.1 The City of Cape Town (hereafter referred to as the "CCT") and each tenderer submitting a tender offer (hereinafter referred to as the "tenderer" or the "supplier") shall comply with item T.2 of this Tender Document Goods and Services (hereinafter referred to as these "Conditions of Tender"). The tenderer and the CCT shall collectively hereinafter be referred to as the "Parties" and individually a "Party"). In their dealings with each other, the Parties shall discharge their duties and obligations as set out in these Conditions of Tender, timeously and with integrity, and behave equitably, honestly and transparently, and shall comply with all legal obligations imposed on the Parties herein and in accordance with all applicable laws.

The Parties agree that this tender Tender Document Goods and Services (hereinafter referred to as the "Tender" / "Tender Document"), its evaluation and acceptance and any resulting contract shall also be subject to the CCT's Supply Chain Management Policy ("SCM Policy") that was applicable on the date the bid was advertised and as amended from time to time. If the CCT adopts a new SCM Policy which contemplates that any clause therein would apply to the Contract emanating from this tender (hereinafter referred to as the "Contract"), such clause shall also be applicable to that Contract. Please refer to this document contained on the CCT's website.

Abuse of the supply chain management system is not permitted and may result, inter alia, (1) in the tender being rejected; (2) cancellation of the contract; (3) restriction of the supplier, and/or (4) the exercise by the CCT of any other remedies available to it as provided for in the SCM Policy and/or the Contract and/or this tender and/or any applicable laws .

2.1.1.2 The CCT, the tenderer and their agents and employees involved in the tender process shall avoid conflicts of interest and where a conflict of interest is perceived or known, declare any such conflict of interest, indicating the nature of such conflict. Tenderers shall declare any potential conflict of interest in their tender submissions. Employees, agents and advisors of the CCT shall declare any conflict of interest to the CCT at the start of any deliberations relating to the procurement process or as soon as they become aware of such conflict, and abstain from any decisions where such conflict exists or recuse themselves from the procurement process, as appropriate.

2.1.1.3 The CCT shall not seek, and a tenderer shall not submit a tender, without having a firm intention and capacity to proceed with the contract.

2.1.2 Interpretation

2.1.2.1 The additional requirements contained in Annexure F to the contract (hereinafter referred to as the "returnable documents" / "Returnable Schedules") are part of these Conditions of Tender and are specifically hereby incorporated into these Conditions of Tender.

2.1.2.2 These Conditions of Tender and returnable Documents which are required for CCT's tender evaluation purposes herein, shall form part of the Contract arising from the CCT's corresponding invitation to tender.

2.1.3 Communication during tender process

Verbal or any other form of communication, from the CCT, its employees, agents or advisors during site visits/clarification meetings or at any other time prior to the award of the Contract, will not be regarded as binding on the CCT, unless communicated by the CCT in writing to suppliers / tenderers by its Director: Supply Chain Management or his nominee. Similarly, any communication of the tenderer / supplier that is not reduced to writing by the tenderer / supplier, its employees, agents or advisors, shall not be regarded as binding on the CCT, unless communicated to the CCT in writing by the suppliers / tenderers, or their duly authorised representatives.

2.1.4 The CCT's right to accept or reject any tender offer

2.1.4.1 The CCT may accept or reject any tender offer and may cancel the corresponding tender process or reject all tender offers at any time before the formation of a contract. The CCT may, prior to the award of the tender, cancel a tender if:

- (a) due to changed circumstances, there is no longer a need for the services, works or goods requested;
or
- (b) funds are no longer available to cover the total envisaged expenditure; or
- (c) no acceptable tenders are received;
- (d) there is a material irregularity in the tender process; or
- (e) the Parties are unable to negotiate market related pricing.

The CCT shall not accept or incur any liability to a tenderer for such cancellation or rejection, but will give written reasons for such action upon receiving a written request to do so.

2.1.5 Procurement procedures

2.1.5.1 General

Unless otherwise stated in the Conditions of Tender, a contract will be concluded with the bidder who scores the highest number of tender adjudication points.

Schedules A, B, and C will be treated as one group and awarded together. The CCT intends to appoint one bidder to provide the goods or services on a "winner takes all" basis and one Standby Bidder at the City's discretion as per clause 2.1.5.3.

The contract period shall be for a period of **ten (10) years** from the commencement date of the contract, subject to the MFMA Section 33 process being concluded.

2.1.5.2 Proposal procedure using the two stage-system

A two-stage system will not be followed.

2.1.5.3 Nomination of Standby Bidder

"Standby Bidder" means a bidder, identified by the CCT at the time of awarding a bid that will be considered for award should the contract be terminated for any reason whatsoever. In the event that a contract is terminated during the execution thereof, the CCT may consider the award of the contract, or non-award, to the Standby Bidder in terms of the procedures included its SCM Policy, as amended from time to time.

Unless otherwise stated in the Conditions of Tender, a contract will be concluded with the bidder who scores the highest number of tender adjudication points.

Schedules A, B, and C will be treated as one group and awarded together. The CCT intends to appoint one bidder to provide the goods or services on a "winner takes all" basis. The City may, at its discretion, appoint the next-ranked bidder as a standby bidder provided that the bidder proposes a solution that is identical to the solution offered by the highest ranked bidder.

If the next-ranked bidder's solution is not identical to the solution offered by the highest ranked bidder, the City may appoint the following ranked bidder whose solution is identical, at the City's discretion.

The appointment of a standby bidder does not create an obligation for the City to offer orders in any particular order beyond what is stated above, and the City reserves the right to select suppliers based on operational needs.

2.1.6 Objections, complaints, queries and disputes/ Appeals in terms of Section 62 of the Systems Act/ Access to court

2.1.6.1 Disputes, objections, complaints and queries

In terms of Regulations 49 and 50 of the Local Government: Municipal Finance Management Act, 56 of 2003 Municipal Supply Chain Management Regulations (Board Notice 868 of 2005):

- a) Persons aggrieved by decisions or actions taken by the CCT in the implementation of its supply chain management system, may lodge within 14 days of the decision or action, a written objection or complaint or query or dispute against the decision or action.

2.1.6.2 Appeals

- a) In terms of Section 62 of the Local Government: Municipal Systems Act, 32 of 2000 a person whose rights are affected by a decision taken by the CCT, may appeal against that decision by giving written notice of the appeal and reasons to the City Manager within 21 days of the date of the notification of the decision.
- b) An appeal must contain the following:
 - i. Must be in writing
 - ii. It must set out the reasons for the appeal
 - iii. It must state in which way the Appellant's rights were affected by the decision;
 - iv. It must state the remedy sought; and
 - v. It must be accompanied with a copy of the notification advising the person of the decision
- c) The relevant CCT appeal authority must consider the appeal and **may confirm, vary or revoke** the decision that has been appealed, but no such revocation of a decision may detract from any rights that may have accrued as a result of the decision.

2.1.6.3 Right to approach the courts and rights in terms of Promotion of Administrative Justice Act, 3 of 2000 and Promotion of Access to Information Act, 2 of 2000

The sub- clauses above do not influence any affected person's rights to approach the High Court at any time or its rights in terms of the Promotion of Administrative Justice Act (PAJA) and Promotion of Access to Information Act (PAIA).

- 2.1.6.4** All requests referring to sub clauses 2.1.6.1 and 2.1.6.2 must be submitted in writing to:
The City Manager - C/o the Manager: Legal Compliance Unit, Legal Services Department, Office of the City Manager
Via hand delivery at: 20th Floor, Tower Block, 12 Hertzog Boulevard, Cape Town 8001
Via post at: Private Bag X918, Cape Town, 8000
Via email at: MSA.Appeals@capetown.gov.za

- 2.1.6.5** All requests referring to clause 2.1.6.3 must be submitted in writing to:
The City Manager - C/o the Manager: Access to Information Unit, Legal Service Department, Office of the City Manager
Via hand delivery at: 20th Floor, Tower Block, 12 Hertzog Boulevard, Cape Town 8001
Via post at: Private Bag X918, Cape Town, 8000
Via email at: Access2info.Act@capetown.gov.za

2.1.6.6 The minimum standards regarding accessing and 'processing' of any personal information belonging to another in terms of Protection of Personal Information Act, 2013 (POPIA).

For purposes of this clause 2.1.6.6, the contract and these Conditions of Tender, the terms "data subject", "Personal Information" and "Processing" shall have the meaning as set out in section 1 of POPIA, and "Process" shall have the corresponding meaning.

The CCT, its employees, representatives and sub-contractors may, from time to time, Process the tenderer's and/or its employees', representatives' and/or sub-contractors' Personal Information, for purposes of, and/or relating to, the tender, the contract and these Conditions of Tender, for research purposes, and/or as otherwise may be envisaged in the CCT's Privacy Notice and/or in relation to the CCT's Supply Chain Management Policy or as may be otherwise permitted by law. This includes the Processing of the latter Personal Information by the CCT's due diligence assurance provider, professional advisors and the Appeal Authority as applicable. The CCT's justification for the processing of such aforesaid Personal Information is based on section 11(1)(b) of POPIA, i.e., in terms of which the CCT's Processing of the said Personal Information is necessary to carry out actions for the conclusion and/or performance of the contract, to which the applicable data subject (envisaged in this clause 2.1.6.6 above) is a party.

All requests relating to data protection must be submitted in writing to:
The City Manager - C/o the Information Officer, Office of the City Manager

Via hand delivery at: 20th Floor, Tower Block, 12 Hertzog Boulevard, Cape Town 8001
Via post at: Private Bag X9181, Cape Town, 8000
Via email at: Popia@capetown.gov.za.

2.1.6.7 Compliance to the CCTs Appeals Policy.

In terms of the CCT's Appeals Policy, a fixed upfront administration fee will be charged. In addition, a surcharge may be imposed for vexatious and frivolous or otherwise manifestly inappropriate tender related appeals.

The current approved administration fee is R300.00 and may be paid at any of the Municipal Offices or at the Civic Centre in Cape Town using the GL Data Capture Receipt attached as Schedule F.14: Appeal Application Form. Alternatively, via EFT into the CCT's NEDBANK Account: CITY OF CAPE TOWN and using Reference number: 198158966. You are required to send proof of payment when lodging your appeal.

The current surcharge for vexatious and frivolous or otherwise manifestly inappropriate tender related appeals will be calculated as $\frac{1}{2}$ (Administrative cost of the tender appeal) + 0.25 % (Appellant's tender price).

Should the payment of the administration fee of R300.00 or the surcharge not be received, such fee or surcharge will be added as a Sundry Tariff to the bidder's municipal account.

In the event where the bidder does not have a Municipal account with the CCT, the fee or surcharge may be recovered in terms of the CCT's Credit Control and Debt Collection By-law, 2006 (as amended) and its Credit Control and Debt Collection Policy.

2.1.7 CCT Supplier Database Registration

Tenderers are required to be registered on the CCT Supplier Database as a Supplier. Tenderers must register as such upon being requested to do so in writing and within the period contained in such a request, failing which no orders can be raised or payments processed from the resulting contract. In the case of Joint Venture partnerships this requirement will apply individually to each party of the Joint Venture.

Tenderers who wish to register on the CCT's Supplier Database may collect registration forms from the Supplier Management Unit located within the Supplier Management / Registration Office, 2nd Floor (Concourse Level), Civic Centre, 12 Hertzog Boulevard, Cape Town (Tel 021 400 9242/3/4/5). Registration forms and related information are also available on the CCT's website www.capetown.gov.za (follow the Supply Chain Management link to Supplier registration).

It is each tenderer's responsibility to keep all the information on the CCT Supplier Database updated.

2.1.8 National Treasury Web Based Central Supplier Database (CSD) Registration

Tenderers are required to be registered on the National Treasury Web Based Central Supplier Database (CSD) as a Supplier. Tenderers must register as such upon being requested to do so in writing and within the period contained in such a request, failing which no orders can be raised or payments processed from the resulting contract. In the case of Joint Venture partnerships this requirement will apply individually to each party of the Joint Venture.

Tenderers who wish to register on the National Treasury Web Based Central Supplier Database (CSD) may do so via the web address <https://secure.csd.gov.za>.

It is each tenderer's responsibility to keep all the information on the National Treasury Web Based Central Supplier Database (CSD) updated.

2.2 Tenderer's obligations

2.2.1 Eligibility Criteria

2.2.1.1 Tenderers are obligated to submit a tender offer that complies in all aspects to the conditions as detailed in this tender document and the Conditions of Tender. An acceptable tender must

"COMPLY IN ALL" aspects with the tender, Conditions of Tender, all Specifications (i.e., item C.5 below, hereinafter the "Specifications"), pricing instructions herein and the Contract including its conditions.

2.2.1.1.1 Submit a tender offer

Only those tender submissions from which it can be established, *inter alia* that a clear, irrevocable and unambiguous offer has been made to CCT, by whom the offer has been made and what the offer constitutes, will be declared responsive.

2.2.1.1.2 Compliance with requirements of CCT SCM Policy and procedures

Only those tenders that are compliant with the requirements below will be declared responsive:

- a) A completed **Details of Tenderer** to be provided (applicable schedule below to be completed);
- b) A completed **Certificate of Authority for Partnerships/ Joint Ventures/ Consortiums** to be provided authorising the tender to be made and the signatory to sign the tender on the partnership /joint venture/consortium's (applicable schedule below to be completed);
- c) A copy of the partnership / joint venture / consortium agreement to be provided, where applicable.
- d) A completed **Declaration of Interest – State Employees** to be provided and which does not indicate any non-compliance with the legal requirements relating to state employees (applicable schedule below to be completed);
- e) A completed **Declaration – Conflict of Interest and Declaration of Bidders' past Supply Chain Management Practices** to be provided and which does not indicate any conflict or past practises that renders the tender non-responsive based on the conditions contained thereon (applicable schedules below to be completed);
- f) A completed **Certificate of Independent Bid Determination** to be provided and which does not indicate any non-compliance with the requirements of the schedule (applicable schedule below to be completed);
- g) The tenderer (including any of its representatives, directors or members), has not been restricted in terms of abuse of the Supply Chain Management Policy,
- h) The tenderer's tax matters with SARS are in order, or the tenderer is a foreign supplier that is not required to be registered for tax compliance with SARS;
- i) The tenderer is not an advisor or consultant contracted with the CCT whose prior or current obligations creates any conflict of interest or unfair advantage;
- j) The tenderer is not a person, advisor, corporate entity or a director of such corporate entity, who is directly or indirectly involved or associated with the bid specification committee;
- k) A completed **Authorisation for the Deduction of Outstanding Amounts Owed to the CCT** to be provided and which does not indicate any details that renders the tender non-responsive based on the conditions contained thereon (applicable schedules below to be completed);
- l) The tenderer (including any of its representatives, directors or members), has not been found guilty of contravening the Competition Act 89 of 1998, as amended from time to time;
- m) The tenderer (including any of its representatives, directors or members), has not been found guilty on any other basis listed in the Supply Chain Management Policy.

2.2.1.1.3 Compulsory clarification meeting

Not Applicable.

2.2.1.1.4 OEM Accreditation/ Authorisation

Tenderers must be authorised or accredited by the Original Equipment Manufacturer (OEM) to sell the software solution and to manage all required escalations. If the authorisation or accreditation is issued by a distributor instead of the OEM, proof must be provided showing that the distributor is authorised by the OEM to resell and/or issue such software.

These requirements apply to any offer for an IGA or PAM solution that involves supplying, using, implementing, or supporting products, software, systems, or components for which an Original Equipment Manufacturer/Original Software Manufacturer (OEM/OSM) exists.

At the tender closing date, tenderers must submit all relevant documentation demonstrating their authority to sell, distribute, implement, and support the proposed software solution, and to manage any related warranty processes and escalations.

All letters submitted must adhere to the following requirements:

- Provide contact details of the OEM/OSM/Distributor
- Validity period
- Include the proposed product name(s)

OEM/OSM Declaration

If the tendering entity is the OEM/OSM, a declaration is required in the form of written confirmation on a letterhead, confirming that the tendering entity will supply, support and manage any warranty processes and escalations, as and when required.

Direct Accreditation With OEM/OSM

If the tendering entity has direct Accreditation with the OEM/OSM, the tendering entity must provide valid proof of such accreditation. This proof must be submitted as an official written confirmation, issued on the OEM/OSM's letterhead, and must be valid as at the tender closing date. The confirmation must expressly authorise the tendering entity to resell the OEM/OSM's goods, support and manage any warranty processes and escalations, as and when required.

Accreditation Through A Distributor

If the tendering entity has direct Accreditation with an accredited distributor, the tendering entity must provide two forms of documentary proof confirming such valid accreditations, on the respective entities' official letterheads, valid as at the tender closing date, and expressly authorising to resell goods, support and manage any warranty processes and escalations, as and when required.

The required documentation comprises:

- (a) an authorisation letter issued by the OEM/OSM to the accredited distributor; and
- (b) an authorisation letter issued by the accredited distributor to the tendering entity.

Tenderers are to submit, either with their tender submission (attached to **Schedule F.13A**), or within a specified timeframe after being requested to do so; proof of authority from the OEM to sell/maintain/support the products of the OEM.

2.2.1.1.5 OEM Retail Price List

The tenderer shall provide detailed and comprehensive OEM Retail Price Lists (Attached to **Schedule F.13B** of the tender), for each OEM product listed in the Price Schedules. The OEM price is the Original Equipment Manufacture's Retail Price at the closing date of the tender.

CCT reserves the right to approach the Original Equipment Manufacturers directly for OEM Retail Price Lists, if required to ensure fair, equitable, transparent, competitive and cost-effective evaluation of the Bid as well as during the contract term for verification purposes.

The award of the tender will be based on the OEM(s) indicated by the tenderer, the retail price offered and mark-up percentages (%) the tenderer applies to a specific OEM's Retail Price List.

2.2.1.1.6 Requirements for IGA

Tenderers are requested to provide information regarding their ability to support an IGA solution. To assist the CCT in evaluating the proposed solution, tenderers should submit sufficient and verifiable evidence for each item listed in Schedule F.13F.

Acceptable supporting evidence may include but is not limited to supplier or product information sheets or official vendor documentation or recorded video demonstrations or walkthroughs.

Tenderers must complete Schedule F.13F and attach all relevant evidence to **Schedule F.13F**.

2.2.1.1.7 Requirements for PAM

Tenderers are requested to provide information regarding their ability to support a PAM solution. To assist the CCT in evaluating the proposed solution, tenderers should submit sufficient and verifiable evidence for each item listed in Schedule F.13G.

Acceptable supporting evidence may include but is not limited to supplier or product information sheets or official vendor documentation or recorded video demonstrations or walkthroughs.

Tenderers must complete Schedule F.13G and attach all relevant evidence to **Schedule F.13G**.

2.2.1.1.8 Minimum score for functionality

Only those tenders submitted by tenderers who achieve the minimum score for functionality as stated below will be declared responsive. **In order for the Bid Evaluation Committee to score the offers; tenderers MUST complete Schedules F.13C, F.13D and F.13E of the tender.** Only projects for which sufficient and verifiable evidence is provided will be scored. Projects that cannot be verified will receive zero points.

The description of the functionality criteria and the maximum possible score for each is shown in the table below. The score achieved for functionality will be the sum of the scores achieved, in the evaluation process, for the individual criteria.

Item	Evaluation Criteria	Applicable values/points	Scoring	Weight
2.2.1.1.8.1	<p>Number of years in the Industry:</p> <p>Tenderer to demonstrate knowledge and experience implementing, maintaining and supporting Identity Lifecycle Management (ILM) solutions including Identity Governance and Administration (IGA) solution(s) or Single Sign On (SSO) solution(s) or Privileged Access Management (PAM) solution(s) or Identity Proofing solution(s).</p> <p>Scoring will be based on the total accumulative number of years in delivering ILM solutions and services as confirmed by Schedule F.13C. Overlapping project periods will not be double counted.</p> <p>Please respond to this functionality requirement and provide evidence to your response in Schedule F.13C – Evidence to Functionality: 2.2.1.1.8.1</p>	<ul style="list-style-type: none"> • 0 years • > 0 and < 2 years • ≥ 2 and < 4 years • ≥ 4 and < 6 years • ≥ 6 years 	<ul style="list-style-type: none"> • 0 points • 10 points • 20 points • 30 points • 40 points 	40 points
2.2.1.1.8.2	<p>Previous Implementation Project Size</p> <p>The Tenderer must demonstrate the scale of previously implemented projects, in terms of number of system users of the solution, for the implementation, maintenance, and support of Identity ILM solutions, including IGA or SSO or PAM or Identity Proofing solutions. Tenderers must specify the total number of actual users, not the product's theoretical capacity.</p> <p>Scoring will be based on the largest project size.</p> <p>Please respond to this functionality requirement in Schedule F.13D – Evidence to Functionality: 2.2.1.1.8.2</p>	<ul style="list-style-type: none"> • No response • Small <1000 users • Medium ≥ 1000 users < 5000 users • Large ≥ 5000 users 	<ul style="list-style-type: none"> • 0 points • 10 points • 20 points • 30 points 	30 points

Item	Evaluation Criteria	Applicable values/points	Scoring	Weight
2.2.1.1.8.3	<p>Types of ILM Solutions Implemented</p> <p>Tenderers must indicate the number of different ILM solution types they have successfully implemented, specifically across the following categories:</p> <ul style="list-style-type: none"> • IGA • PAM • Identity Proofing <p>Scoring will be based on the number of distinct solution types implemented, not the number of projects.</p> <p>Tenderers must respond to this requirement and provide verifiable evidence for each solution type in Schedule F.13E – Evidence to Functionality: 2.2.1.1.8.3.</p>	<ul style="list-style-type: none"> • 0 types of ILM Solutions • 1 type of ILM solution • 2 types of ILM solutions • 3 types of ILM solutions 	<ul style="list-style-type: none"> • 0 points • 5 points • 15 points • 30 points 	30 points
	Total			100 points

The minimum qualifying score for functionality is **60** out of a maximum of **100**.

Where the entity tendering is a Joint Venture, the tenderer's tender response must be accompanied by a statement describing exactly what aspects of the work will be undertaken by each party to the joint venture.

Tenderers shall ensure that all relevant information has been submitted with the tender offer in the prescribed format to ensure optimal scoring of functionality points for each Evaluation Criteria. Failure to provide all information **IN THIS TENDER SUBMISSION** could result in the tenderer not being able to achieve the specified minimum scoring.

2.2.2 Cost of tendering

The CCT will not be liable for any costs incurred in the preparation and submission of a tender offer, including the costs of any testing necessary to demonstrate that aspects of the offer complies with requirements.

2.2.3 Check documents

The documents issued by the CCT for the purpose of a tender offer are listed in the index of this tender document.

Before submission of any tender, the tenderer should check the number of pages, and if any are found to be missing or duplicated, or the figures or writing is indistinct, or if the Price Schedule contains any obvious errors, the tenderer must apply to the CCT at once to have the same rectified.

2.2.4 Confidentiality and copyright of documents

The tenderer shall treat as strictly confidential all matters arising in connection with the tender. Use and copy the documents issued by the CCT only for the purpose of preparing and submitting a tender offer in response to the invitation.

2.2.5 Reference documents

The tenderer shall obtain, as necessary for submitting a tender offer, copies of the latest versions of standards, specifications, Conditions of Contract and other publications, which are not attached but which are

incorporated into the tender document(s) by reference.

2.2.6 Acknowledge and comply with notices

The tenderer shall acknowledge receipt of notices to the tender documents, which the CCT may issue, and shall fully comply with all instructions issued in the said notices, and if necessary, apply for an extension of the closing time stated on the front page of the tender document, in order to take the notices into account. Notwithstanding any requests for confirmation of receipt of the said notices issued, the tenderer shall be deemed to have received such notices if the CCT can show proof of transmission thereof via electronic mail, facsimile, or registered post or other lawful means.

2.2.7 Clarification meeting

The tenderer shall attend, where required, a clarification meeting at which tenderers may familiarise themselves with aspects of the proposed work, services or supply and pose questions. Details of the meeting(s) are stated in the General Tender Information (i.e., in item T.1 above).

Tenderers should be represented at the site visit/clarification meeting by a duly authorised person who is suitably qualified and experienced to comprehend the implications of the work involved.

2.2.8 Seek clarification

The tenderer shall request clarification of the tender documents, if necessary, by notifying the CCT at least one week before the closing time stated in the General Tender Information (i.e., in item T.1 above), where possible.

2.2.9 Pricing the tender offer

2.2.9.1 The tenderer shall comply with all pricing instructions as stated on the Price Schedule.

2.2.10 Alterations to documents

The tenderer shall not make any alterations or additions to the tender documents, except to comply with instructions issued by the CCT in writing, or necessary to correct errors made by the tenderer. All signatories to the tender offer shall initial all such alterations.

2.2.11 Alternative tender offers

2.2.11.1 Unless otherwise stated in the Conditions of Tender, the tenderers may submit alternative tender offers only if a main tender offer, strictly in accordance with all the requirements of the tender documents, is also submitted.

If a tenderer wishes to submit an alternative tender offer, he/she/it shall do so as a separate offer on a complete set of tender documents. The alternative tender offer shall be submitted in a separate sealed envelope clearly marked "Alternative Tender" in order to distinguish it from the main tender offer.

Only the alternative of the highest ranked acceptable main tender offer (that is, submitted by the same tenderer) will be considered, and if appropriate, recommended for award.

Alternative tender offers of any but the highest ranked main tender offer will not be considered.

An alternative tender offer to the highest ranked acceptable main tender offer that is priced higher than the main tender offer may be recommended for award, provided that the ranking of the alternative tender offer is higher than the ranking of the next ranked acceptable main tender offer.

The CCT will not be bound to consider alternative tenders and shall have sole discretion in this regard.

In the event that the alternative is accepted, the tenderer warrants that the alternative offer complies in all respects with the CCT's standards and requirements as set out in the tender document.

2.2.11.2 Acceptance of an alternative tender offer by the CCT may be based only on the criteria stated in the Conditions of Tender or applicable criteria otherwise acceptable to the CCT.

2.2.12 Submitting a tender offer

2.2.12.1 The tenderer is required to submit one tender offer only on the original tender documents as issued by the CCT, either as a single tendering entity or as a member in a joint venture to provide the whole of the works, services or supply identified in the Conditions of Contract and described in the Specifications. Only those tenders submitted on the tender documents as issued by the CCT together with all Tender Returnable Documents duly completed and signed will be declared responsive.

2.2.12.2 The tenderer shall return the entire tender document to the CCT after completing it in its entirety, either electronically (if they were issued in electronic format) or by writing legibly in non-erasable ink.

2.2.12.3 The tenderer shall sign the original tender offer where required in terms of the Conditions of Tender. The tender shall be signed by a person duly authorised by the tenderer to do so. Tenders submitted by joint ventures of two or more firms shall be accompanied by the document of formation / founding document of the joint venture or any other document signed by all Parties, in which is defined precisely the conditions under which the joint venture will function, its period of duration, the persons authorised to represent and obligate it, the participation of the several firms forming the joint venture, and any other information necessary to permit a full appraisal of its functioning. Signatories for tenderers proposing to contract as joint ventures shall state which of the signatories is the lead partner.

2.2.12.4 Where a two-envelope system is required in terms of the Conditions of Tender, place and seal the returnable documents listed in the Conditions of Tender in an envelope marked "financial proposal" and place the remaining returnable documents in an envelope marked "technical proposal". Each envelope shall state on the outside the CCT's address and identification details stated in the General Tender Information (i.e., item T.1 above), as well as the tenderer's name and contact address.

2.2.12.5 The tenderer shall seal the original tender offer and copy packages together in an outer package that states on the outside only the CCT's address and identification details as stated in the General Tender Information. . If it is not possible to submit the original tender and the required copies (see 2.2.12.3) in a single envelope, then the tenderer must seal the original and each copy of the tender offer as separate packages marking the packages as "ORIGINAL" and "COPY" in addition to the aforementioned tender submission details.

2.2.12.6 The CCT shall not assume any responsibility for the misplacement or premature opening of the tender offer if the outer package is not sealed and marked as stated.

2.2.12.7 Tender offers submitted by facsimile or e-mail will be rejected by the CCT, unless stated otherwise in the Conditions of Tender.

2.2.12.8 By signing the offer part of the Form of Offer (**Section 5, Part A hereto**) the tenderer warrants and agrees that all information provided in the tender submission is true and correct.

2.2.12.9 Tenderers shall properly deposit its bid in the designated tender box (as detailed on the front page of this tender document) on or before the closing date and before the closing time, in the relevant tender box at the Tender & Quotation Boxes Office situated on the 2nd floor, Concourse Level, Civic Centre, 12 Hertzog Boulevard, Cape Town. If the tender submission is too large to fit in the allocated box, please enquire at the public counter for assistance.

2.2.12.10 The tenderer must record and reference all information submitted contained in other documents for example cover letters, brochures, catalogues, etc. in the Returnable Schedule titled **List of Other Documents Attached by Tenderer**.

2.2.13 Information and data to be completed in all respects

Tender offers, which do not provide all the data or information requested completely and in the form required, may be regarded by the CCT as non-responsive.

2.2.14 Closing time

2.2.14.1 The tenderer shall ensure that the CCT receives the tender offer, together with all applicable documents specified herein, at the address specified in the General Tender Information herein prior to the closing time stated on the front page of the tender document.

2.2.14.2 If the CCT extends the closing time stated on the front page of the tender document for any reason, the requirements of these Conditions of Tender apply equally to the extended deadline.

2.2.14.3 The CCT shall not consider tenders that are received after the closing date and time for such a tender (late tenders).

2.2.15 Tender offer validity and withdrawal of tenders

2.2.15.1 The tenderer shall warrant that the tender offer(s) remains valid, irrevocable and open for acceptance by the CCT at any time for a period of 120 days after the closing date stated on the front page of the tender document.

2.2.15.2 Notwithstanding the period stated in clause 2.2.15.1 above, bids shall remain valid for acceptance for a period of twelve (12) months after the expiry of the original validity period, unless the CCT is notified in writing of anything to the contrary by the bidder. The validity of bids may be further extended by a period of not more than six months subject to mutual agreement by the parties, administrative processes and upon approval by the City Manager, unless the required extension is as a result of an appeal process or court ruling.

In circumstances where the validity period of a tender has expired, and the tender has not been awarded, the tender process is considered "completed", despite there being no decision (award or cancellation) made. This anomaly does not fall under any of the listed grounds of cancellation and should be treated as a "non award". A "non award" is supported as a recommendation to the CCT's Bod Adjudication Committee ("BAC") for noting.

2.2.15.3 A tenderer may request in writing, after the closing date, that its tender offer be withdrawn. Such withdrawal will be permitted or refused at the sole discretion of the CCT after consideration of the reasons for the withdrawal, which shall be fully set out by the tenderer in such written request for withdrawal. Should the tender offer be withdrawn in contravention hereof, the tenderer agrees that:

- a) it shall be liable to the CCT for any additional expense incurred or losses suffered by the CCT in having either to accept another tender or, if new tenders have to be invited, the additional expenses incurred or losses suffered by the invitation of new tenders and the subsequent acceptance of any other tender;
- b) the CCT shall also have the right to recover such additional expenses or losses by set-off against monies which may be due or become due to the tenderer under this or any other tender or contract or against any guarantee or deposit that may have been furnished by the tenderer or on its behalf for the due fulfilment of this or any other tender or contract. Pending the ascertainment of the amount of such additional expenses or losses, the CCT shall be entitled to retain such monies, guarantee or deposit as security for any such expenses or loss, without prejudice to the CCT's other rights and/or remedies available to it in accordance with any applicable laws.

2.2.16 Clarification of tender offer, or additional information, after submission

Tenderer's shall promptly provide clarification of its tender offer, or additional information, in response to a written request to do so from the CCT during the evaluation of tender offers within the time period stated in such request. No change in the competitive position of tenderers or substance of the tender offer is sought, offered, or permitted.

Note: This clause does not preclude the negotiation of the final terms of the contract with a preferred tenderer following a competitive selection process, should the CCT elect to do so.

Failure, or refusal, to provide such clarification or additional information within the time for submission stated in the CCT's written request may render the tender non-responsive.

2.2.17 Provide other material

2.2.17.1 Tenderer's shall promptly provide, upon request by the CCT, any other material that has a bearing on the tender offer, the tenderer's commercial position (including joint venture agreements), preferencing arrangements, or samples of materials, considered necessary by the CCT for the purpose of the evaluation of the tender. Should the tenderer not provide the material, or a satisfactory reason as to why it cannot be provided, by the time for submission stated in the CCT's request, the CCT may regard the tender offer as non-responsive.

2.2.17.2 The tenderer shall provide, on written request by the CCT, where the transaction value inclusive of VAT **exceeds R 10 million**:

- a) audited annual financial statement for the past 3 years, or for the period since establishment if established during the past 3 years, if required by law to prepare annual financial statements for auditing;
- b) a certificate signed by the tenderer certifying that the tenderer has no undisputed commitments for municipal services towards a municipality or other Supplier in respect of which payment is overdue for more than 30 days;
- c) particulars of any contracts awarded to the tenderer 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;
- d) a statement indicating whether any portion of the goods or services are expected to be sourced from outside the Republic, and, if so, what portion and whether any portion of payment from the municipality or municipal entity is expected to be transferred out of the Republic.

Each entity to a Consortium/Joint Venture bid shall submit separate certificates/statements in the above regard.

2.2.18.3 Tenderers shall be required to undertake to fully cooperate with the CCT's external Supplier appointed to perform a due diligence review and risk assessment upon receipt of such written instruction from the CCT.

2.2.18 Samples, Inspections, tests and analysis

Tenderers shall provide access during working hours to premises for inspections, tests and analysis as provided for in the Conditions of Tender or Specifications.

If the Specifications requires the tenderer to provide samples, these shall be provided strictly in accordance with the instructions set out in the Specification.

If such samples are not submitted as required in the bid documents or within any further time stipulated by the CCT in writing, then the bid concerned may be declared non-responsive.

The samples provided by all successful bidders will be retained by the CCT for the duration of any subsequent contract. Bidders are to note that samples are requested for testing purposes therefore samples submitted to the CCT may not in all instances be returned in the same state of supply and in other instances may not be returned at all. Unsuccessful bidders will be advised by the Project Manager or dedicated CCT Official to collect their samples, save in the aforementioned instances where the samples would not be returned.

2.2.19 Certificates

The tenderer must provide the CCT with all certificates as stated below:

2.2.19.1. Preference Points for Specific Goals

In order to qualify for preference points for Specific Goals, it is the responsibility of the tenderer to submit sufficient, relevant and verifiable documentary proof in support of any claim for preference points.

Failure to submit adequate and verifiable evidence may result in the non-awarding of preference points claimed.

Tenderers are further referred to the Preference Schedule for the detailed methodology, scoring criteria, and conditions applicable to the allocation of preference points for Specific Goals.

2.2.19.2 Evidence of tax compliance

Tenderers shall be registered with the South African Revenue Service (SARS) and their tax affairs must be in order and they must be tax compliant subject to the requirements of clause 2.2.1.1.2.h. In this regard, it is the responsibility of the Tenderer to submit evidence in the form of a valid Tax Compliance Status PIN issued by SARS to the CCT at the Supplier Management Unit located within the Supplier Management / Registration Office, 2nd Floor (Concourse Level), Civic Centre, 12 Hertzog Boulevard, Cape Town (Tel 021 400 9242/3/4/5), or included with this tender. The tenderer must record its Tax Compliance Status PIN number on the **Details of Tenderer** pages of the tender submission.

Each party to a Consortium/Joint Venture shall submit a separate Tax Compliance Status Pin.

Before making an award the CCT must verify the bidder's tax compliance status. Where the recommended bidder is not tax compliant, the bidder should be notified of the non-compliant status and be requested to submit to the CCT, within 7 working days, written proof from SARS that they have made arrangement to meet their outstanding tax obligations. The proof of tax compliance submitted by the bidder must be verified by the CCT via CSD or e-Filing. The CCT should reject a bid submitted by the bidder if such bidder fails to provide proof of tax compliance within the timeframe stated herein.

Only foreign suppliers who have answered "NO" to all the questions contained in the Questionnaire to Bidding Foreign Suppliers section on the **Details of Tenderer** pages of the tender submission, are not required to register for a tax compliance status with SARS.

2.2.20 Compliance with Occupational Health and Safety Act, 85 of 1993

Tenderers are to note the requirements of the Occupational Health and Safety Act, 85 of 1993. The Tenderer shall be deemed to have read and fully understood the requirements of the above Act and Regulations and to have allowed for all costs in compliance therewith.

In this regard the Tenderer shall submit **upon written request to do so by the CCT**, a Health and Safety Plan in sufficient detail to demonstrate the necessary competencies and resources to deliver the goods or services all in accordance with the Act, Regulations and Health and Safety Specification.

2.2.21 Claims arising from submission of tender

By responding to the tender herein, the tenderer warrants that it has:

- a) Inspected the Specifications and read and fully understood the Conditions of Contract.
- b) Read and fully understood the whole text of the Specifications and Price Schedule and thoroughly acquainted himself with the nature of the goods or services proposed and generally of all matters which may influence the Contract.
- c) visited the site(s) where delivery of the proposed goods will take place, carefully examined existing conditions, the means of access to the site(s), the conditions under which the delivery is to be made, and acquainted himself with any limitations or restrictions that may be imposed by the Municipal or other Authorities in regard to access and transport of materials, plant and equipment to and from the site(s) and made the necessary provisions for any additional costs involved thereby.
- d) requested the CCT to clarify the actual requirements of anything in the Specifications and Price Schedule, the exact meaning or interpretation of which is not clearly intelligible to the Tenderer.
- e) Received any notices to the tender documents which have been issued in accordance with the CCT's Supply Chain Management Policy.

The CCT will therefore not be liable for the payment of any extra costs or claims arising from the submission of the tender.

2.2.22 Collection and issuing of tender documents

The CCT will only issue tender documents through its Tender Distribution Office and/or the official CCT tender portal. Bidders who obtain documents through any means other than described herein, will not be known to the CCT and may thus not receive tender notices and addendums. Tenderers are not allowed to distribute tender documents to other potential bidders.

It is the responsibility of bidders who obtain documents through any means other than described herein, to notify the CCT tender representative thereof that they are participating in the tender. The CCT accepts no liability for any tender notices or addendums not reaching any bidders, who obtained documents through any means other than described herein or who provided incorrect contact details to the CCT.

2.3 The CCT's undertakings

2.3.1 Respond to requests from the tenderer

2.3.1.1 Unless otherwise stated in the Conditions of Tender, the CCT shall respond to a request for clarification received up to one week (where possible) before the tender closing time stated on the front page of the tender document.

2.3.1.2 The CCT's duly authorised representative for the purpose of this tender is stated on the General Tender Information page above.

2.3.2 Issue Notices

If necessary, the CCT may issue addenda in writing that may amend or amplify the tender documents to each tenderer during the period from the date the tender documents are available until one week before the tender closing time stated in the Tender Data. The CCT reserves its rights to issue addenda less than one week before the tender closing time in exceptional circumstances. If, as a result a tenderer applies for an extension to the closing time stated on the front page of the tender document, the CCT may grant such extension and, shall then notify all tenderers who drew documents.

Notwithstanding any requests for confirmation of receipt of notices issued, the tenderer shall be deemed to have received such notices if the CCT can show proof of transmission thereof via electronic mail, facsimile or registered post.

2.3.3 Opening of tender submissions

2.3.3.1 Unless the two-envelope system is to be followed, CCT shall open tender submissions in the presence of tenderers' agents who choose to attend at the time and place stated in the Conditions of Tender.

Tenders will be opened immediately after the closing time for receipt of tenders as stated on the front page of the tender document, or as stated in any Notice extending the closing date and at the closing venue as stated in the General Tender Information.

2.3.3.2 Announce at the meeting held immediately after the opening of tender submissions, at the closing venue as stated in the General Tender Information, the name of each tenderer whose tender offer is opened and, where possible, the prices indicated.

2.3.3.3 Make available a record of the details announced at the tender opening meeting on the CCT's website (<http://www.capetown.gov.za/en/SupplyChainManagement/Pages/default.aspx>.)

2.3.4 two-envelope system

2.3.4.1 Where stated in the Conditions of Tender that a two-envelope system is to be followed, the CCT shall

open only the technical proposal of tenders in the presence of tenderers' agents who choose to attend at the time and place stated in the Conditions of Tender and announce the name of each tenderer whose technical proposal is opened.

2.3.4.2 The CCT shall evaluate the quality of the technical proposals offered by tenderers, then advise tenderers who have submitted responsive technical proposals of the time and place when the financial proposals will be opened. The CCT shall open only the financial proposals of tenderers, who have submitted responsive technical proposals in accordance with the requirements as stated in the Conditions of Tender, and announce the total price and any preference claimed. Return unopened financial proposals to tenderers whose technical proposals were non responsive.

2.3.5 Non-disclosure

The CCT shall not disclose to tenderers, or to any other person not officially concerned with such processes, information relating to the evaluation and comparison of tender offers and recommendations for the award of a contract, until after the award of the contract to the successful tenderer.

2.3.6 Grounds for rejection and disqualification

The CCT shall determine whether there has been any effort by a tenderer to influence the processing of tender offers and instantly disqualify a tenderer (and his tender offer) if it is established that he engaged in corrupt or fraudulent practices.

2.3.7 Test for responsiveness

2.3.7.1 Appoint a Bid Evaluation Committee and determine after opening whether each tender offer properly received:

- a) complies with the requirements of these Conditions of Tender,
- b) has been properly and fully completed and signed, and
- c) is responsive to the other requirements of the tender documents.

2.3.7.2 A responsive tender is one that conforms to all the terms, conditions, and specifications of the tender documents without material deviation or qualification. A material deviation or qualification is one which, in the CCT's opinion, would:

- a) Detrimentially affect the scope, quality, or performance of the goods, services or supply identified in the Specifications,
- b) Significantly change the CCT'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.

Reject a non-responsive tender offer, and not allow it to be subsequently made responsive by correction or withdrawal of any material deviation or qualification.

The CCT reserves the right to accept a tender offer which does not, in the CCT's opinion, materially and/or substantially deviate from the terms, conditions, and specifications of the tender documents.

2.3.8 Arithmetical errors, omissions and discrepancies

2.3.8.1 Check the responsive tenders for:

- a) The gross misplacement of the decimal point in any unit rate;
- b) Omissions made in completing the Price Schedule; or
- c) Arithmetic errors in:
 - i) line item totals resulting from the product of a unit rate and a quantity in the Price Schedule; or
 - ii) The summation of the prices; or
 - iii) Calculation of individual rates.

2.3.8.2 The CCT must correct the arithmetical errors in the following manner:

- a) Where there is a discrepancy between the amounts in words and amounts in figures, the amount in words shall govern.
- b) If pricing schedules apply and there is an error in the line item total resulting from the product of the unit rate and the quantity, the line item total shall govern and the rate shall be corrected. Where there is an obviously gross misplacement of the decimal point in the unit rate, the line item total as tendered shall govern, and the unit rate shall be corrected.
- c) Where there is an error in the total of the prices either as a result of other corrections required by this checking process or in the tenderer's addition of prices, the total of the prices shall govern and the tenderer will be asked to revise selected item prices (and their rates if Price Schedules apply) to achieve the tendered total of the prices.

Consider the rejection of a tender offer if the tenderer does not correct or accept the correction of the arithmetical error in the manner described above.

2.3.8.3 In the event of tendered rates or lump sums being declared by the CCT to be unacceptable to it because they are not priced, either excessively low or high, or not in proper balance with other rates or lump sums, the tenderer may be required to produce evidence and advance arguments in support of the tendered rates or lump sums objected to. If, after submission of such evidence and any further evidence requested, the CCT is still not satisfied with the tendered rates or lump sums objected to, it may request the tenderer to amend these rates and lump sums along the lines indicated by it.

The tenderer will then have the option to alter and/or amend the rates and lump sums objected to and such other related amounts as are agreed on by the CCT, but this shall be done without altering the tender offer in accordance with this clause.

Should the tenderer fail to amend his tender in a manner acceptable to and within the time stated by the CCT, the CCT may declare the tender as non-responsive.

2.3.9 Clarification of a tender offer

The CCT may, after the closing date, request additional information or clarification from tenderers, in writing on any matter affecting the evaluation of the tender offer or that could give rise to ambiguity in a contract arising from the tender offer, which written request and related response shall not change or affect their competitive position or the substance of their offer. Such request may only be made in writing by the Director: Supply Chain Management using any means as appropriate.

2.3.10 Evaluation of tender offers

2.3.10.1 General

2.3.10.1.1 The CCT may reduce each responsive tender offer to a comparative price and evaluate them using the tender evaluation methods and associated evaluation criteria and weightings that are specified in the Conditions of Tender.

2.3.10.1.2 For evaluation purposes only, the effects of the relevant contract price adjustment methods will be considered in the determination of comparative prices as follows:

- a) If the selected method is based on bidders supplying rates or percentages for outer years, comparative prices would be determined over the entire contract period based on such rates or percentages.
- b) If the selected method is based on a formula, indices, coefficients, etc. that is the same for all bidders during the contract period, comparative prices would be the prices as tendered for year one.
- c) If the selected method is based on a formula, indices, coefficients, etc. that varies between bidders, comparative prices would be determined over the entire contract period based on published indices relevant during the 12 months prior to the closing date of tenders.
- d) If the selected method includes an imported content requiring rate of exchange variation, comparative prices would be determined based on the exchange rates tendered for the prices as

tendered for year one. The rand equivalent of the applicable currency 14 days prior to the closing date of tender will be used (the CCT will check all quoted rates against those supplied by its own bank).

- e) If the selected method is based on suppliers' price lists, comparative prices would be the prices as tendered for year one.
- f) If the selected method is based on suppliers' price lists and / or rate of exchange, comparative prices would be determined as tendered for year one whilst taking into account the tendered percentage subject to rate of exchange (see sub clause (d) for details on the calculation of the rate of exchange).

2.3.10.1.3 Where the scoring of functionality forms part of a bid process, each member of the Bid Evaluation Committee must individually score functionality. The individual scores must then be interrogated and calibrated if required where there are significant discrepancies. The individual scores must then be added together and averaged to determine the final score.

2.3.10.2 Decimal places

Score financial offers, preferences and functionality, as relevant, to two decimal places.

2.3.10.3 Scoring of tenders (price and preference)

2.3.10.3.1 Points for price will be allocated in accordance with the formula set out in this clause based on the price per item / rates as set out in the **Price Schedule (Section C.4)**:

- Based on the sum of the prices/rates in relation to the estimated quantities.

2.3.10.3.2 Points for preference will be allocated in accordance with the provisions of **Preference Schedule** and the table in this clause.

2.3.10.3.3 The terms and conditions of **Preference Schedule** as it relates to preference shall apply in all respects to the tender evaluation process and any subsequent contract.

2.3.10.3.4 Applicable formula:

The 90/10 price/preference points system will be applied to the evaluation of responsive tenders above a Rand value of R50'000'000 (all applicable taxes included), whereby the order(s) will be placed with the tenderer(s) scoring the highest total number of adjudication points.

Price shall be scored as follows:

$$P_s = 90 \times \left(1 - \frac{(P_t - P_{min})}{P_{min}} \right)$$

Where: P_s is the number of points scored for price;
 P_t is the price of the tender under consideration;
 P_{min} is the price of the lowest responsive tender.

Preference points shall be based on the Specific Goal as per below:

#	Specific goals allocated points	Preference Points (90/10)
	<i>Reconstruction and Development Programme (RDP) as published in Government Gazette</i>	
1	<p>Promotion of Micro and Small Enterprises <i>Micro with a turnover up to R20million and Small with a turnover up to R80 million as per National Small Enterprise Act, 1996 (Act No.102 of 1996)</i> <i>SME partnership, sub-contracting, joint venture or consortiums</i></p>	4
2	<p>Enterprise Supplier Development and <u>Socio Economic Development</u></p> <p>> 15% of total expenditure = 3 points > 10% up to 15% of total <u>expenditure</u> = 2 points >= 5% up to 10% of total <u>expenditure</u> = 1 points < 5% of total expenditure = 0 points</p>	3
3	<p>Skills Development OR Employee Share Scheme</p> <p>Skills Development</p> <p>> 5% of total profit = 3 points > 3% up to 5% of total profit = 2 points >= 1% up to 3% of total profit = 1 points < 1% of total profit = 0 points</p> <p><u>OR Employee Share Scheme</u></p> <p>> 15% employee ownership = 3 points > 10% up to 15% employee <u>ownership</u> = 2 point >= 5% up to 10% employee <u>ownership</u> = 1 point < 5% employee <u>ownership</u> = 0 point</p>	3
	Total points	10

2.3.10.5 Risk Analysis

Notwithstanding compliance with regard to any requirements of the tender, the CCT will perform a risk analysis in respect of the following:

- a) reasonableness of the financial offer
- b) reasonableness of unit rates and prices
- c) the tenderer's ability to fulfil its obligations in terms of the tender document, that is, that the tenderer can demonstrate that he/she possesses the necessary professional and technical qualifications, professional and technical competence, financial resources, equipment and other physical facilities, managerial capability, reliability, capacity, experience, reputation, personnel to perform the contract, etc.; the CCT reserves the right to consider a tenderer's existing contracts with the CCT in this regard

- d) any other matter relating to the submitted bid, the tendering entity, matters of compliance, verification of submitted information and documents, etc.

The conclusions drawn from this risk analysis will be used by the CCT in determining the acceptability of the tender offer.

No tenderer will be recommended for an award unless the tenderer has demonstrated to the satisfaction of the CCT that he/she has the resources and skills required.

2.3.11 Negotiations with preferred tenderers

The CCT may negotiate the final terms of a contract with tenderers identified through a competitive tendering process as preferred tenderers provided that such negotiation:

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

If negotiations fail to result in acceptable contract terms, the City Manager (or his delegated authority) may terminate the negotiations and cancel the tender, or invite the next ranked tenderer for negotiations. The original preferred tenderer should be informed of the reasons for termination of the negotiations. If the decision is to invite the next highest ranked tenderer for negotiations, the failed earlier negotiations may not be reopened by the CCT.

Minutes of any such negotiations shall be kept for record purposes.

The provisions of this clause will be equally applicable to any invitation to negotiate with any other tenderers.

In terms of the CCT's SCM Policy, tenders must be cancelled in the event that negotiations fail to achieve a market related price with any of the three highest scoring tenderers.

2.3.12 Acceptance of tender offer

Notwithstanding any other provisions contained in the tender document, the CCT reserves the right to:

2.3.12.1 Accept a tender offer(s) which does not, in the CCT's opinion, materially and/or substantially deviate from the terms, conditions, and specifications of the tender document.

2.3.12.2 Accept the whole tender or part of a tender or any item or part of any item or items from multiple manufacturers, or to accept more than one tender (in the event of a number of items being offered), and the CCT is not obliged to accept the lowest or any tender.

2.3.12.3 Accept the tender offer(s), if in the opinion of the CCT, it does not present any material risk and only if the tenderer(s):

- a) is not under restrictions, has any principals who are under restrictions, or is not currently a supplier to whom notice has been served for abuse of the supply chain management system, preventing participation in the CCT's procurement,
- b) can, as necessary and in relation to the proposed contract, demonstrate that he or she possesses the professional and technical qualifications, professional and technical competence, financial resources, equipment and other physical facilities, managerial capability, reliability, experience and reputation, expertise and the personnel, to perform the contract,
- c) has the legal capacity to enter into the contract,
- d) is not insolvent, in receivership, under Business Rescue as provided for in chapter 6 of the Companies Act, 2008, bankrupt or being wound up, has his affairs administered by a court or a judicial officer, has suspended his business activities, or is subject to legal proceedings in respect of any of the foregoing, complies with the legal requirements, if any, stated in the tender data, and
- e) is able, in the opinion of the CCT, to perform the contract free of conflicts of interest.

If an award cannot be made in terms of anything contained herein, the CCT reserves the right to consider the next ranked tenderer(s).

2.3.12.4 The CCT reserves the right not to make an award, or revoke an award already made, where the implementation of the contract may result in reputational risk or harm to the CCT as a result of (inter alia):

- a) reports of poor governance or unethical behaviour, or both;
- b) association with known notorious individuals and family of notorious individuals;
- c) poor performance issues, known to the CCT;
- d) negative media reports, including negative social media reports;
- e) adverse assurance (e.g. due diligence) report outcomes; and
- f) circumstances where the relevant vendor has employed, or is directed by, anyone who was previously employed in the service of the state (as defined in clause 1.53 of the SCM Policy), where the person is or was negatively implicated in any SCM irregularity.

2.3.12.5 The CCT reserves the right to nominate an Standby Bidder at the time when an award is made and in the event that a contract is terminated during the execution thereof, the CCT may consider the award of the contract, or non-award, to the Standby Bidder in terms of the procedures included its SCM Policy.

2.3.13 Prepare contract documents

2.3.13.1 If necessary, revise documents that shall form part of the contract and that were issued by the CCT as part of the tender documents to take account of:

- a) Notices issued during the tender period,
- b) Inclusion of some of the returnable documents, and
- c) Other revisions agreed between the CCT and the successful tenderer.

2.3.13.2 Complete the schedule of deviations attached to the form of offer and acceptance, if any.


2.3.14 Notice to successful and unsuccessful tenderers

2.3.14.1 Before accepting the tender of the successful tenderer the CCT shall notify the successful tenderer in writing of the decision of the CCT's Bid Adjudication Committee to award the tender to the successful tenderer. No rights shall accrue to the successful tenderer in terms of this notice

2.3.14.2 The CCT shall, at the same time as notifying the successful tenderer of the Bid Adjudication Committee's decision to award the tender to the successful tenderer, also give written notice to the other tenderers informing them that they have been unsuccessful.

2.3.15 Provide written reasons for actions taken

Provide upon request written reasons to tenderers for any action that is taken in applying these Conditions of Tender, but withhold information which is not in the public interest to be divulged, which is considered to prejudice the legitimate commercial interests of tenderers or might prejudice fair competition between tenderers.

TENDER DOCUMENT GOODS AND SERVICES		 CITY OF CAPE TOWN ISIXEKO SASEKAPA STAD KAAPSTAD
SUPPLY CHAIN MANAGEMENT		
SCM - 542	Approved by Branch Manager: February 2024	Version: 10 Page 25 of 80

TENDER NO: 252S/2025/26

TENDER DESCRIPTION: SUPPLY, INSTALLATION, MAINTENANCE AND SUPPORT OF IDENTITY LIFECYCLE MANAGEMENT FOR THE CITY OF CAPE TOWN

CONTRACT PERIOD: 10 YEARS FROM THE COMMENCEMENT DATE OF THE CONTRACT (SUBJECT TO MFMA SECTION 33)

THE CONTRACT

THE CITY OF CAPE TOWN	
A metropolitan municipality, established in terms of the Local Government: Municipal Structures Act, 117 of 1998 read with the Province of the Western Cape: Provincial Gazette 5588 dated 22 September 2000, as amended (“the Purchaser”) herein represented by	
AUTHORISED REPRESENTATIVE	

AND

SUPPLIER	
NAME of Company/Close Corporation or Partnership / Joint Venture/ Consortium or Sole Proprietor /Individual (The “Supplier” / “tenderer”)	
TRADING AS (if different from above)	
REGISTRATION NUMBER	
PHYSICAL ADDRESS / CHOSEN DOMICILIUM CITANI ET EXECTUANDI OF THE SUPPLIER	
AUTHORISED REPRESENTATIVE	
CAPACITY OF AUTHORISED REPRESENTATIVE	

(HEREINAFTER COLLECTIVELY REFERRED TO AS “THE PARTIES” AND INDIVIDUALLY A “PARTY”)

NATURE OF TENDER OFFER (please indicate below)

Main Offer (see clause 2.2.11.1)	
Alternative Offer (see clause 2.2.11.1)	

C.1 DETAILS OF TENDERER/SUPPLIER

1.1 Type of Entity (Please tick one box)

- Individual / Sole Proprietor
 Close Corporation
 Company
- Partnership or Joint Venture or Consortium
 Trust
 Other:

1.2 Required Details (Please provide applicable details in full):

Name of Company / Close Corporation or Partnership / Joint Venture / Consortium or Individual /Sole Proprietor	
Trading as (if different from above)	
Company / Close Corporation registration number (if applicable)	
Postal address	Postal Code _____
Physical address (Chosen Domicilium Citandi Et Executandi)	Postal Code _____
Contact details of the person duly authorised to represent the tenderer	Name: Mr/Ms _____ (Name & Surname) Telephone : (____) _____ Fax :(____) _____ Cellular Telephone: _____ E-mail address: _____
Income tax number	
VAT registration number	
SARS Tax Compliance Status PIN	
CCT Supplier Database Registration Number (See Conditions of Tender)	
National Treasury Central Supplier Database registration number (See Conditions of Tender)	
Is tenderer the accredited representative in South Africa for the Goods / Services / Works offered?	<input type="checkbox"/> Yes <input type="checkbox"/> No If yes, enclose proof
Is tenderer a foreign based supplier for the Goods / Services / Works offered?	<input type="checkbox"/> Yes <input type="checkbox"/> No If yes, answer the Questionnaire to Bidding Foreign Suppliers (below)
Questionnaire to Bidding Foreign Suppliers	a) Is the tenderer a resident of the Republic of South Africa or an entity registered in South Africa? <input type="checkbox"/> Yes <input type="checkbox"/> No
	b) Does the tenderer have a permanent establishment in the Republic of South Africa? <input type="checkbox"/> Yes <input type="checkbox"/> No
	c) Does the tenderer have any source of income in the Republic of South Africa? <input type="checkbox"/> Yes <input type="checkbox"/> No
	d) Is the tenderer liable in the Republic of South Africa for any form of taxation? <input type="checkbox"/> Yes <input type="checkbox"/> No
Other Required registration numbers	

C.2 FORM OF OFFER AND ACCEPTANCE

TENDER 252S/2025/26 - SUPPLY, INSTALLATION, MAINTENANCE AND SUPPORT OF IDENTITY LIFECYCLE MANAGEMENT FOR THE CITY OF CAPE TOWN

C.2.1 Offer (To Be Completed by the Tenderer as Part of Tender Submission)

The tenderer, identified in the offer signature table below,

HEREBY AGREES THAT by signing the *Form of Offer and Acceptance*, the tenderer:

1. confirms that it has examined the documents listed in the Index (including Schedules and Annexures) and has accepted all the Conditions of Tender;
2. confirms that it has received and incorporated any and all notices issued to tenderers issued by the CCT;
3. confirms that it has satisfied itself as to the correctness and validity of the tender offer; that the price(s) and rate(s) offered cover all the goods and/or services specified in the tender documents; that the price(s) and rate(s) cover all its obligations and accepts that any mistakes regarding price(s), rate(s) and calculations will be at its own risk;
4. offers to supply all or any of the goods and/or render all or any of the services described in the tender document to the CCT in accordance with the:
 - 4.1 terms and conditions stipulated in this tender document;
 - 4.2 specifications stipulated in this tender document; and
 - 4.3 at the prices as set out in the **Price Schedule**.
5. accepts full responsibility for the proper execution and fulfilment of all obligations and conditions devolving on it in terms of the Contract.

SIGNED AT _____ (PLACE) ON THE _____ (DAY) OF _____ (MONTH AND YEAR)

For and on behalf of the Supplier
(Duly Authorised)
Name and Surname:

Witness 1 Signature
Name and Surname:

Witness 2 Signature
Name and Surname:

INITIALS OF CCT OFFICIALS		
1	2	3

FORM OF OFFER AND ACCEPTANCE (continued)

TENDER 252S/2025/26 - SUPPLY, INSTALLATION, MAINTENANCE AND SUPPORT OF IDENTITY LIFECYCLE MANAGEMENT FOR THE CITY OF CAPE TOWN

C.2.2 Acceptance (To Be Completed by the CCT)

By signing this part of this *Form of Offer and Acceptance*, the CCT accepts the tenderer's (if awarded the Supplier's) offer. In consideration thereof, the CCT shall pay the Supplier the amount due in accordance with the conditions of contract. Acceptance of the Supplier's offer shall form an agreement between the CCT and the Supplier upon the terms and conditions contained in this document.

The terms of the agreement are contained in the Contract (as defined) including drawings and documents or parts thereof, which may be incorporated by reference.

Deviations from and amendments to the documents listed in the tender data and any addenda thereto as listed in the *Tender Returnable Documents* as well as any changes to the terms of the offer agreed by the tenderer and the CCT during this process of offer and acceptance, are contained in the *Schedule of Deviations* attached to and forming part of this *Form of Offer and Acceptance*. No amendments to or deviations from said documents are valid unless contained in the *Schedule of Deviations*.

The Supplier shall within 2 (two) weeks after receiving a complete, copy of the Contract, including the *Schedule of Deviations* (if any), contact the CCT to arrange the delivery of any securities, bonds, guarantees, proof of insurance and any other documents to be provided in terms the *Special Conditions of Contract*. Failure to fulfil any of these obligations in accordance with those terms shall constitute a repudiation / breach of the agreement.

Notwithstanding anything contained herein, this agreement comes into effect on the Commencement Date, being the date upon which the Supplier confirms receipt from the CCT of 1 (one) complete, signed copy of the Contract, including amendments or deviations contained in the *Schedule of Deviations* (if any).

For and on behalf of the City of Cape Town
(Duly Authorised)
Name and Surname:

Witness 1 Signature
Name and Surname:

Witness 2 Signature
Name and Surname:

FORM OF OFFER AND ACCEPTANCE (continued)

TENDER 252S/2025/26 - SUPPLY, INSTALLATION, MAINTENANCE AND SUPPORT OF IDENTITY LIFECYCLE MANAGEMENT FOR THE CITY OF CAPE TOWN

C.2.4 Confirmation of Receipt (To be Completed by Supplier upon Acceptance)

The Supplier identified in the offer part of the Contract hereby confirms receipt from the CCT of 1 (one) complete, signed copy of the Contract, including the *Schedule of Deviations* (if any) on:

The..... (Day)

Of..... (Month)

20..... (year)

At..... (Place)

For the Supplier: Signature(s)

Name(s)

Capacity

Signature and name of witness:

Signature Name

ONLY TO BE COMPLETED AT ACCEPTANCE STAGE

C.3 OCCUPATIONAL HEALTH AND SAFETY AGREEMENT

AGREEMENT MADE AND ENTERED INTO BETWEEN THE CCT (HEREINAFTER CALLED THE "CCT") AND

.....,
(Supplier/Mandatory/Company/CC Name)

IN TERMS OF SECTION 37(2) OF THE OCCUPATIONAL HEALTH AND SAFETY ACT, 85 OF 1993 AS AMENDED.

I,, representing

....., as an employer in its own right in its own right, do hereby undertake to ensure, as far as is reasonably practicable, that all work will be performed, and all equipment, machinery or plant used in such a manner as to comply with the provisions of the Occupational Health and Safety Act (hereafter "OHSA") and the Regulations promulgated thereunder.

I furthermore confirm that I am/we are registered with the Compensation Commissioner and that all registration and assessment monies due to the Compensation Commissioner have been fully paid or that I/We are insured with an approved licensed compensation insurer.

COID ACT Registration Number:

OR Compensation Insurer: Policy No:

I undertake to appoint, where required, suitable competent persons, in writing, in terms of the requirements of OHSA and the Regulations and to charge him/them with the duty of ensuring that the provisions of OHSA and Regulations as well as the Council's Special Conditions of Contract, Way Leave, Lock-Out and Work Permit Procedures are adhered to as far as reasonably practicable.

I further undertake to ensure that any subcontractors employed by me will enter into an occupational health and safety agreement separately, and that such subcontractors comply with the conditions set.

I hereby declare that I have read and understand the Occupational Health and Safety Specifications contained in this tender and undertake to comply therewith at all times.

I hereby also undertake to comply with the Occupational Health and Safety Specification and Plan submitted and approved in terms thereof.

Signed aton the.....day of.....20....

Witness

Mandatory

Signed at..... on the.....day of.....20

Witness

for and on behalf of
CCT

C.4 PRICE SCHEDULE

Bid specifications may not make any reference to any particular trade mark, name, patent, design, type, specific origin or producer, unless there is no other sufficiently precise or intelligible way of describing the characteristics of the work, in which case such reference must be accompanied by the words "or equivalent".

TENDERERS MUST NOTE THAT WHEREVER THIS DOCUMENT REFERS TO ANY PARTICULAR TRADE MARK, NAME, PATENT, DESIGN, TYPE, SPECIFIC ORIGIN OR PRODUCER, SUCH REFERENCE SHALL BE DEEMED TO BE ACCOMPANIED BY THE WORDS 'OR EQUIVALENT'

Pricing Instructions:

- 5.1 State the rates and prices in Rand unless instructed otherwise in the Conditions of Tender.
- 5.2 Include in the rates, prices, and the tendered total of the prices (if any) all duties, taxes (except Value Added Tax (VAT), and other levies payable by the successful tenderer, such duties, taxes and levies being those applicable 14 days before the closing time stated in the General Tender Information.
- 5.3 All prices tendered must include all expenses, disbursements and costs (e.g. transport, accommodation etc.) that may be required for the execution of the tenderer's obligations in terms of the Contract, and shall cover the cost of all general risks, liabilities and obligations set forth or implied in the Contract as well as overhead charges and profit (in the event that the tender is successful). All prices tendered will be final and binding.
- 5.4 All prices shall be tendered in accordance with the units specified in this schedule.
- 5.5 Where a value is given in the Quantity column, a Rate and Price (the product of the Quantity and Rate) is required to be inserted in the relevant columns.
- 5.6 The successful tenderer is required to perform all tasks listed against each item. The tenderer must therefore tender prices/rates on all items as per the section in the Price Schedule. **An item against which no rate is/are entered, or if anything other than a rate or a nil rate (for example, a zero, a dash or the word "included" or abbreviations thereof) is entered against an item, it will also be regarded as a nil rate having been entered against that item, i.e. that there is no charge for that item. The Tenderer may be requested to clarify nil rates, or items regarded as having nil rates; and the CCT may also perform a risk analysis with regard to the reasonableness of such rates.** This instruction does not apply to optional items (Tables A.7, B.7 and C.7).
- 5.7 Provide fixed rates and prices for the duration of the contract that are not subject to adjustment except as otherwise provided for in clause 17 of the Conditions of Contract and as amplified in the Special Conditions of Contract.
- 5.8 General specifications for items in the (C.4) Price Schedule, appear in section (C.5) SPECIFICATION(S). Tenderers must refer to these specifications when completing the Price Schedule.
- 5.9 **A mark-up percentage (%) is applied to the Original Equipment Manufacturer (OEM) Retail Price to determine the evaluation price.**
- The **mark-up percentage (%)** represents the mark-up amount expressed as a percentage of the OEM Retail Price, calculated as:
 - $\text{Mark-up \%} = (\text{Mark-up amount} / \text{OEM Retail Price}) \times 100$
 - The **Evaluation Price** is the total price used for tender evaluation and ranking, calculated as:
 - $\text{Evaluation Price} = \text{OEM Price} + \text{Mark-up}$
- 5.10 Tenderers are required to indicate where prices are included in a different line item as where indicated in the pricing tables below, e.g. when software maintenance and support is included in the software licence costs.

INITIALS OF CCT OFFICIALS		
1	2	3

SCHEDULE A. SUPPLY OF SOLUTION FOR IDENTITY GOVERNANCE AND ADMINISTRATION (IGA) SOLUTION(S)

TABLE A.1. SUPPLY OF IGA – LICENCING

This table is for the pricing to supply OEM products for an IGA solution in terms of software application and appropriate user / access licences. Tenderers must identify the software OEM or vendor in the indicated column (column 3).

Refer to **Section 6.1 of C.5 Specifications** for the functional requirements of the IGA solution.

The OEM price is for evaluation purposes only.

Item	Description	Source of Goods (OEM or Distributor)	Unit	OEM Price Per Unit	Mark-up (%)	Price per Unit (ZAR excl. VAT) (OEM Price + Mark-up)
A.1.1	Software Licence per user (Annual licence cost)		Per User	R	%	R

TABLE A.2. IMPLEMENTATION OF THE IGA SOLUTION

This table is for the pricing of services to install, configure and deploy the proposed OEM solution for the proposed IGA tool.

Tenderers are to refer to **Section 6.9 of the C.5 Specifications** for the implementation requirements, project methodology and deliverables applicable in the City.

The OEM price is for evaluation purposes only.

Item	Description	Unit	Price per Unit (ZAR excl. VAT)
A.2.1	Implementation of the IGA toolset according to the implementation requirements (which includes Envisioning, Planning, Develop/Build/Integration, Stabilization and Deployment), project methodology and deliverables as described in Section 6.9 of the C.5 Specifications – Requirements for the Implementation of the ILM Solution . Implementation cost must include low code development, integrations, customisations, 3 months' hyper-care support post go-live, project management, change management functions, change management material.	Complete implementation of the IGA solution	R
A.2.2	Configuration of SSO for current applications during the implementation phase of the project.	Per application	R

TABLE A.3. SOFTWARE MAINTENANCE AND SUPPORT OF IGA SOLUTION

This table is for the pricing of software maintenance and support services for the proposed IGA tool.

Tenderers are to refer to **Section 6.10 of the C.5 Specifications** for the maintenance and support requirements.

The OEM price is for evaluation purposes only.

Item	Description	Unit	OEM Price Per Unit	Mark-up (%)	Price per Unit (ZAR excl. VAT)
A.3.1	Software maintenance and support services - IGA	Annual	R	%	R

TABLE A.4. THE IGA SOLUTION - TRAINING

This table is for the pricing of services to train administrators on the proposed IGA tool.

Please refer to **Section 6.8 of the C.5 Specifications** for detailed specifications of the training requirements for the City.

Item	Description	Training delivery	Unit	Price per Unit (ZAR excl. VAT)
A.4.1	Instructor-led administrator training – IGA	Classroom based	Per Administrator	R
A.4.2	Instructor-led administrator training – IGA	Virtual training	Per Administrator	R
A.4.3	Certification training – IGA	Classroom based	Per Administrator	R
A.4.4	Certification training – IGA	Virtual training	Per Administrator	R
A.4.5	Self-paced Web-based Training - IGA	Web-based	Per Administrator	R

TABLE A.5. PROFESSIONAL SERVICES OF THE IGA SOLUTION

This table is for the labour rates associated with the ad-hoc Services of IGA Solution.

Tenderers are to refer to **Section 6.11 of the C.5 Specifications** for the professional services requirements.

Item	Description	Unit	Price per Unit (ZAR excl. VAT)
A.5.1	Project Manager	Per hour	R
A.5.2	Technical Architect/Lead	Per hour	R
A.5.3	Technical Consultant	Per hour	R
A.5.4	Senior Consultant	Per hour	R
A.5.5	Consultant	Per hour	R

TABLE A.6. MANAGED SERVICES FOR THE IGA SOLUTION

This table is for the labour rates associated with the Managed Services of IGA Solution.

Tenderers are to refer to **Section 6.12 of the C.5 Specifications** for the managed services requirements. Type 1, 2 and 3 Resources are defined in this section of the specifications.

Item	Description	Unit	Price per Unit (ZAR excl. VAT)
A.6.1	Type 1 Resource	Per hour	R
A.6.2	Type 2 Resource	Per hour	R
A.6.3	Type 3 Resource	Per hour	R

TABLE A.7. OPTIONAL IGA SOLUTION COMPONENTS

This table is for the pricing of optional IGA solution components for the proposed IGA tool.

Tenderers are to list any additional optional IGA solution components which may offer value over the contract term. Tenderers are to expand lines as required and to include appropriate descriptions and units.

Please note this section does not include items included as part of **C.5 Specifications**. These items will not form part of the evaluation of this tender.

Tenderers may add additional rows to the table below.

Item	Description	Unit	OEM Price Per Unit	Mark-up (%)	Price per Unit (ZAR excl. VAT)
A.7.1			R	%	R
A7.2			R	%	R
A7.3			R	%	R

INITIALS OF CCT OFFICIALS		
1	2	3

SCHEDULE B. SUPPLY OF SOLUTION AND SERVICES FOR PRIVILEGED ACCESS MANAGEMENT (PAM) SOLUTION

Table B.1 SUPPLY OF PAM SOLUTION – SOFTWARE AND LICENCING

This table is for the pricing to supply OEM products for PAM solution in terms of software application and appropriate user / access licenses. Tenderers must identify the software OEM or vendor in the indicated column (column 3).

Refer to **Section 6.3 of C.5 Specifications** for the functional requirements of the PAM solution.

The OEM price is for evaluation purposes only.

Item	Description	Source of Goods Identify OEM or Distributor	Unit	OEM Price Per Unit	Mark-Up (%)	Price per Unit (ZAR excl. VAT) (OEM Price + Mark- up)
B.1.1	PAM Tool / Toolset (Annual licence cost)		Per module	R	%	R
B.1.2	Software Licence per user (Annual licence cost, pricelist detail to be provided)		Per User	R	%	R
B.1.3	Cloud storage cost		Per GB	R	%	R

TABLE B.2. IMPLEMENTATION OF THE PAM SOLUTION

This table is for the pricing of services to install, configure and deploy the proposed OEM solution for the proposed PAM tool.

Tenderers are to refer to **Section 6.9 of C.5 Specifications** for the implementation requirements, project methodology and deliverables applicable in the City.

The OEM price is for evaluation purposes only.

Item	Description	Unit	Price per Unit (ZAR excl. VAT)
B.2.1	<p>Implementation of the PAM toolset according to the implementation requirements (which includes Envisioning, Planning, Develop/Build/Integration, Stabilization and Deployment), project methodology and deliverables as described in section C.5 Specifications – Requirements for the Implementation of the ILM Solution.</p> <p>Implementation cost must include low code development, integrations, customisations, project management, change management functions, change management material.</p>	Complete Installation of PAM solution	R

TABLE B.3. SUPPORT AND MAINTENANCE OF PAM SOLUTION

This table is for the pricing of maintenance and support services for the proposed PAM tool.

Tenderers are to refer to **Section 6.10 of C.5 Specifications** for detail specifications of the maintenance and support requirements.

The OEM price is for evaluation purposes only.

Item	Description	Unit	OEM Price	Mark-up (%)	Price per Unit (ZAR excl. VAT) (OEM Price + Mark-up)
B.3.1	Software maintenance and support services - PAM	Annual	R	%	R

TABLE B.4. THE PAM SOLUTION - TRAINING

This table is for the pricing of services to train administrators on the proposed PAM tool.

Tenderers are to refer to **Section 6.8 of C.5 Specifications** for detail specifications of the training requirements for the City.

Item	Description	Training delivery	Unit	Price per Unit (ZAR excl. VAT)
B.4.1	Instructor-led administrator training – PAM	Classroom based	Per Administrator	R
B.4.2	Instructor-led administrator training – PAM	Virtual training	Per Administrator	R
B.4.3	Certification training – PAM	Classroom based	Per Administrator	R
B.4.4	Certification training – PAM	Virtual training	Per Administrator	R
B.4.5	Self-paced Web-based Training - PAM	Web-based	Per Administrator	R

TABLE B.5. PROFESSIONAL SERVICES OF THE PAM SOLUTION

This table is for the labour rates associated with the ad-hoc Services of PAM Solution.

Tenderers are to refer to **Section 6.11 of C.5 Specifications** for the professional services requirements.

Item	Description	Unit	Price per Unit (ZAR excl. VAT)
B.5.1	Project Manager	Per hour	R
B.5.2	Technical Architect/Lead	Per hour	R
B.5.3	Technical Consultant	Per hour	R
B.5.4	Senior Consultant	Per hour	R
B.5.5	Consultant	Per hour	R

TABLE B.6. MANAGED SERVICES FOR THE PAM SOLUTION

This table is for the labour rates associated with the Managed Services of PAM Solution.

Tenderers are to refer to **Section 6.12 of C.5 Specifications** for the managed services requirements.

Item	Description	Unit	Price per Unit (ZAR excl. VAT)
B.6.1	Type 1 Resource	Per hour	R
B.6.2	Type 2 Resource	Per hour	R
B.6.3	Type 3 Resource	Per hour	R

TABLE B.7. OPTIONAL PAM SOLUTION COMPONENTS

This table is for the pricing of optional PAM solution components for the proposed PAM tool.

Tenderers are to list any additional optional PAM solution components which may offer value over the contract term. Tenderers are to expand lines as required and to include appropriate descriptions and units.

Please note this section does not include items included as part of C.5 Specifications. These items will not form part of the evaluation of this tender.

Tenderers may add additional rows to the table below.

Item	Description	Unit	OEM Price Per Unit	Mark-up (%)	Price per Unit (ZAR excl. VAT)
B.7.1			R	%	R
B7.2			R	%	R
B7.3			R	%	R

INITIALS OF CCT OFFICIALS		
1	2	3

SCHEDULE C. SUPPLY OF SOLUTION AND SERVICES FOR IDENTITY PROOFING SOLUTION

TABLE C.1 SUPPLY OF IDENTITY PROOFING SOLUTION – SOFTWARE AND LICENCING

This table is for the pricing to supply OEM products for identity Proofing solution in terms of software application and appropriate user / access licenses.

Tenderers must identify the software OEM or vendor in the indicated column (column 3).

Tenderers are to refer to **Section 6.5 of C.5 Specifications** for the functional requirements of the Identity Proofing solution.

The OEM price is for evaluation purposes only.

Item	Description	Source of Goods Identify OEM	Unit	OEM Price	Mark-Up (%)	Price per Unit (ZAR excl. VAT) (OEM Price + Mark-up)
C.1.1	Usage fee per user verification (Annual Service cost, pricelist detail to be provided)		Per User Verification	R	%	R

TABLE C.2. IMPLEMENTATION OF THE IDENTITY PROOFING SOLUTION

This table is for the pricing of services to install, configure and deploy the proposed OEM solution for the proposed Identity Proofing tool.

Tenderers are to refer to **Section 6.9 of C.5 Specifications** for the implementation requirements, project methodology and deliverables applicable in the City.

The OEM price is for evaluation purposes only.

Item	Description	Unit	Price per Unit (ZAR excl. VAT)
C.2.1	<p>Implementation of the Identity Proofing toolset according to the implementation requirements (which includes Envisioning, Planning, Develop/Build/Integration, Stabilization and Deployment), project methodology and deliverables as described in section C.5 Specifications – Requirements for the Implementation of the ILM Solution.</p> <p>Implementation cost must include low code development, integrations, customisations, project management, change management functions, change management material</p>	Complete Installation of Identity Proofing solution	R

TABLE C.3. SUPPORT AND MAINTENANCE OF IDENTITY PROOFING SOLUTION

This table is for the pricing of maintenance and support services for the proposed Identity Proofing tool.

Tenderers are to refer to **Section 6.10 of C.5 Specifications** for the maintenance and support requirements.

The OEM price is for evaluation purposes only.

Item	Description	Unit	OEM Price	Mark-up (%)	Price per Unit (ZAR excl. VAT) (OEM Price + Mark-up)
C.3.1	Software maintenance and support services - IDENTITY PROOFING	Annual	R	%	R

TABLE C.4. THE IDENTITY PROOFING SOLUTION - TRAINING

This table is for the pricing of services to train administrators on the proposed Identity Proofing tool.

Tenderers are to refer to **Section 6.8 of C.5 Specifications** for the training requirements for the City.

Item	Description	Training delivery	Unit	Price per Unit (ZAR excl. VAT)
C.4.1	Instructor-led administrator training – IDENTITY PROOFING	Classroom based	Per Administrator	R
C.4.2	Instructor-led administrator training – IDENTITY PROOFING	Virtual training	Per Administrator	R
C.4.3	Certification training – IDENTITY PROOFING	Classroom based	Per Administrator	R
C.4.4	Certification training – IDENTITY PROOFING	Virtual training	Per Administrator	R
C.4.5	Self-paced Web-based Training - IDENTITY PROOFING	Web-based	Per Administrator	R

TABLE C.5. PROFESSIONAL SERVICES FOR THE IDENTITY PROOFING SOLUTION

This table is for the labour rates associated with the ad-hoc Services of Identity Proofing Solution.

Tenderers are to refer to **Section 6.11 of C.5 Specifications** for the professional services requirements.

Item	Description	Unit	Price per Unit (ZAR excl. VAT)
C.5.1	Project Manager	Per hour	R
C.5.2	Technical Architect/Lead	Per hour	R
C.5.3	Technical Consultant	Per hour	R
C.5.4	Senior Consultant	Per hour	R
C.5.5	Consultant	Per hour	R

TABLE C.6. MANAGED SERVICES FOR THE IDENTITY PROOFING SOLUTION

This table is for the labour rates associated with the Managed Services of Identity Proofing Solution.

Tenderers are to refer to **Section 6.12 of C.5 Specifications** for the managed services requirements.

Item	Description	Unit	Price per Unit (ZAR excl. VAT)
C.6.1	Type 1 Resource	Per hour	R
C.6.2	Type 2 Resource	Per hour	R
C.6.3	Type 3 Resource	Per hour	R

TABLE C.7. OPTIONAL IDENTITY PROOFING SERVICE COMPONENTS

This table is for the pricing of optional identity proofing service components for the proposed identity proofing service.

Tenderers are to list any additional optional identity proofing services components which may offer value over the contract term. Tenderers are to expand lines as required and to include appropriate descriptions and units.

Please note this section does not include items included as part of C.5 Specifications. These items will not form part of the evaluation of this tender.

Tenderers may add additional rows to the table below.

Item	Description	Unit	OEM Price Per Unit	Mark-up (%)	Price per Unit (ZAR excl. VAT)
C.7.1			R	%	R
C7.2			R	%	R
C7.3			R	%	R

INITIALS OF CCT OFFICIALS		
1	2	3

C.5 SPECIFICATION(S)

1. ABBREVIATIONS

Abbreviation	Description
AD	Active Directory
AES	Advanced Encryption Standard
AGPM	Advanced Group Policy Management
AI	Artificial Intelligence
API	Application Programming Interface
ARIBA	SAP Ariba
AS	Application Server
AWS	Amazon Web Services
BI	Business Intelligence
BYOK	Bring Your Own Key
CAR	Core Applications Refresh
CC	Close Corporation
CCT	City of Cape Town
CEF	Common Event Format
CLI	Command Line Interface
CPU	Central Processing Unit
CRM	Customer Relationship Management
CRUD	Change, Read, Update, Delete
CSF	Cybersecurity Framework
CSV	Comma-Separated Values
CVE	Common Vulnerabilities and Exposures
DB	Database
DBA	Database Administrator
DHA	Department of Home Affairs
DOB	Date of Birth
ECC	SAP ERP Central Component
EID	Employee Identifier
ERP	Enterprise Resource Planning
EU	European Union
FAQ	Frequently Asked Questions
FIPS	Federal Information Processing Standards
GB	Gigabyte
GDPR	General Data Protection Regulation
GPO	Group Policy Object
GUI	Graphical User Interface
HANA	SAP High-Performance Analytic Appliance
HR	Human Resources
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
IBM	International Business Machines
ID	Identifier / Identity
IDV	Identity Verification
IGA	Identity Governance and Administration
IIS	Internet Information Services
ILM	Identity Lifecycle Management
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
ITSM	Information Technology Service Management
IV	Initialization Vector
JML	Joiner, Mover, Leaver

Abbreviation	Description
JSON	JavaScript Object Notation
KYC	Know Your Customer
LDAP	Lightweight Directory Access Protocol
LTD	Limited
LTS	Long-Term Support
MFA	Multi-Factor Authentication
MS	Microsoft
NET	Network
NGO	Non-Governmental Organisation
NIST	National Institute of Standards and Technology
NPO	Non-Profit Organisation
OEM	Original Equipment Manufacturer
OIDC	OpenID Connect
OS	Operating System
OU	Organisational Unit
OWASP	Open Web Application Security Project
PAD	Presentation Attack Detection
PAM	Privileged Access Management
PC	Personal Computer
PDF	Portable Document Format
PMO	Project Management Office
PMP	Project Management Professional
POPIA	Protection of Personal Information Act
PTY	Proprietary Limited
QA	Quality Assurance
QR	Quick Response
RAM	Random Access Memory
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
RHEL	Red Hat Enterprise Linux
RPO	Recovery Point Objective
RSA	Republic of South Africa / Rivest–Shamir–Adleman
SAML	Security Assertion Markup Language
SAP	Systems, Applications and Products
SBOM	Software Bill of Materials
SCIM	System for Cross-domain Identity Management
SCORM	Sharable Content Object Reference Model
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SLES	SUSE Linux Enterprise Server
SOC	Security Operations Centre
SOX	Sarbanes-Oxley Act
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
SUSE	Software und System-Entwicklung
TLS	Transport Layer Security
UAT	User Acceptance Testing
UNIX	Unix Operating System
VNC	Virtual Network Computing
WAF	Web Application Firewall
WAN	Wide Area Network
WBS	Work Breakdown Structure
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language
ZAR	South African Rand

2. INTRODUCTION AND BACKGROUND

For the City of Cape Town (CCT) to be future-fit, it recognises the need to enable employees to respond to the changing needs and expectations of its citizens, and to do so with speed and accuracy. As a result, the City acknowledges that its digital architecture is critical for basic service delivery, as is highlighted in numerous Identity Proofing objectives and programmes.

There is a need to understanding that this is not only a technology transformation, but rather technology enabling new ways of working to drive efficiencies, data-backed decision-making, and ultimately improved service delivery to citizens.

As a technical consideration in the CCT's CAR (Core Applications Review) Phase II, it was recommended that there are foundational technologies required to be in place prior to the Edge and Core tender processes. These would establish the foundations to enable the future loose coupling. Identity Life-Cycle Management (ILM) was selected as one of the foundational technologies.

Identity Life-Cycle Management (ILM) collectively refers to the people, processes and technologies used to manage the life cycle of identities (profiles) for people, systems, and services. It is a suite of complimentary services operated based on policies, processes and supporting technologies that enable an organization to manage access to its resources over time.

3. OVERVIEW OF CCT ENVIRONMENT

The City of Cape Town has an employee base of 42 000 employees, consisting of permanent, contract, and temporary workers and approximately 1.3 million external identities that make use of the City's systems (E-Services). Of the 42,000 employees, approximately 29 000 users actively access electronic HR services and other corporate systems. The City's technology landscape includes approximately 23 000 devices and an additional 6 000 mobile devices used across the organisation. In addition to standard employee identities, the environment also includes privileged accounts, generic accounts, system accounts, and AI agents that fall outside the employee count. The City furthermore provides digital services to residents and businesses, who represent a significantly larger external user base interacting with municipal platforms and systems.

4. BUSINESS GOAL

The main goal of this implementation is to protect sensitive enterprise systems, assets, and information from unauthorized access or use. An end-to-end ILM implementation will reduce the likelihood and impact of data breaches and ensure that only legitimate authenticated and authorized users have access to City services. Such protection is crucial for the following areas:

- Data and information;
- Software and applications;
- Development, testing, staging, and operational platforms;
- Devices;
- Locations; and
- Integrations.

5. OBJECTIVES

The objectives of the ILM solution outline the specific outcomes the City of Cape Town intends to achieve through the implementation of an integrated Identity Governance and Administration (IGA), Privileged Access Management (PAM), and Identity Proofing capability. These objectives translate the strategic goals of security, compliance, efficiency, and digital enablement into clear, actionable requirements that will guide the design, implementation, and operation of the ILM solution throughout the contract period. The objectives of this project are:

- **Security and Compliance Objectives**
 - Protect sensitive information

- Improve compliance with internal and external policies and regulations
- Enforce secure privileged access (PAM)
- Implement MFA and Zero Trust principles
- **Identity Management Objectives**
 - Establish one digital identity per individual
 - Streamline joiner, mover and leaver processes
 - Improve employee onboarding & role changes
- **External Identity Objectives**
 - Simplify access for residents and business partners
 - Use identity proofing to verify non-staff identities
- **Technology Enablement & Innovation**
 - Prepare for SaaS adoption
 - Strengthen business agility in this fast-paced world, by being able to adopt Software as a Service offering
 - Achieve SSO for current and future applications

6. SCOPE OF WORKS

The Scope of Works defines the full breadth of services, technologies, integrations, and deliverables required to implement a comprehensive Identity Lifecycle Management (ILM) capability for the City of Cape Town. It outlines the responsibilities of the Supplier across the Identity Governance and Administration (IGA), Privileged Access Management (PAM), and Identity Proofing components, ensuring seamless integration with existing systems, alignment with organisational policies, and support for secure, efficient identity and access management throughout the contract period.

6.1. FUNCTIONAL REQUIREMENTS OF IGA SOLUTION

This scope definition is related to **SCHEDULE A in section C.4 Price Schedule** and evidence of the proposed solution should be submitted as required in **SCHEDULE F.13: Information to be provided with the tender**.

6.1.1. Identity Governance and Administration (IGA):

A tool where an identity life cycle is managed via the joiner, mover, leaver process.

The solution must include, but is not limited to, the following functional requirements:

Functional Requirement Category	Functional Requirements – Identity Governance and Administration
6.1.1.1. General	1) The solution must have the ability to periodically check the authoritative source for changes to employee records: <ul style="list-style-type: none"> ● Employee Onboarding ● Employee Leave of Absence, Employee Return from Leave ● Employee Termination ● Contract Worker to Employee Conversion ● Employee to contractor Conversion

Functional Requirement Category	Functional Requirements – Identity Governance and Administration
	<ol style="list-style-type: none"> 2) The solution must have the ability to create a digital identity for the new user using the profile attributes provided by the authoritative data source. 3) The solution must have the ability to initiate the onboarding process when it receives a new hire record from authoritative data source regardless of the start date of the worker. 4) The solution must have the ability to allow managers to initiate onboarding of CCT contractors. 5) The solution must have the ability to create and assign a contractor ID for contractors that are not onboarded through the HR system. 6) The solution must have the ability to activate a disabled identity when converting employees from permanent to contractor. 7) The solution must have the ability to provision access in, but not limited to, the following 3 birth-right platforms for all employees (permanent and contractor): <ul style="list-style-type: none"> • SAP solutions • Microsoft Active Directory • Microsoft Entra ID 8) The solution must have the ability to provision access in the birth-right platforms listed in the previous point for all contractors that are not on the HR system. 9) The solution must have the ability to keep an account in birth-right platform disabled until the start date of the new hire. 10) The solution must have the ability to utilize the profile attributes associated with user's digital identity to provisioning accounts in target platforms. 11) The solution must have the ability for a manager to initiate a request to change existing employees from permanent to contractor. 12) The solution must have the ability to provide the current manager with an option to select a new manager when converting an employee from permanent to contractor. 13) The solution must have the ability to request the manager to review user's access including ability to modify or remove access during the conversion process. 14) The solution must have the ability to provision or de-provision accounts and entitlements based on the access review performed by the manager. 15) The solution must have the ability to disable accounts in target systems when suspending access. 16) The solution must have the ability to enable accounts in target systems when reactivating access. 17) The solution must have the ability to delete accounts in target systems in which account disable functionality is not supported. 18) The solution must have the ability to allow managers to initiate suspension or reactivation of their reporting contractors. 19) The solution must have the ability to capture termination status for external contractors not listed in the HR system. 20) The solution must have the ability to terminate user's access when it receives the change of status to terminate, regardless of the date of the termination.

Functional Requirement Category	Functional Requirements – Identity Governance and Administration
	<p>21) The solution must have the ability to terminate user's access in all systems that are connected to IGA solution and have permissions to perform disable operation.</p> <p>22) The system must have the ability to reactivate suspended access if HR rejects the emergency suspension.</p> <p>23) The system must have the ability to allow managers to initiate access termination of a profiled user.</p> <p>24) The system must have the ability to allow managers or approved HR users to initiate emergency suspension of access of their reporting employees.</p> <p>25) The system must have the ability to provide options to HR to approve or reject emergency suspension.</p> <p>26) The solution must have the ability to set a default expiration date that is 90 calendar days from the creation (or conversion) of a contractor identity.</p> <p>27) The solution must have the ability to allow up to 30 days grace period before disabling a contractors account, for managers to make decision about extending or expiring contractors.</p> <p>28) The solution must have the ability to update the contractor identity with new expiration date when provided by a manager.</p> <p>29) The solution must have the ability to not reset or remove the expiration date when a contractor's identity is updated as part of any other business processes.</p> <p>30) This solution shall seamlessly and natively integrate with ERP systems, other business applications, infrastructure systems.</p> <p>31) The solution shall perform continuous account reconciliation so as to identify and unify application user accounts, eradicating duplicate identities, orphan accounts and also rogue access grants that originate outside this Identity Life-Cycle Management Solution.</p> <p>32) The solution shall continuously check (communicate) designated trusted systems for minimum, basic parameters needed to action automated provisioning of new user accounts (new employees) with authorisation roles on common enterprise applications.</p> <p>33) The solution must support early identity profile creation prior to a new employee's start date, including advanced provisioning of usernames and email addresses. Access must be date-driven and policy-controlled, allowing for restricted pre-start access (such as onboarding communications) while ensuring full access is only enabled on the official commencement date.</p>
<p>6.1.1.2. Ticketing Function</p>	<p>1) The solution must have the ability to open a new onboarding request on the Ticketing solution as part of the onboarding process. The City will implement Service Now as its ticketing system.</p> <p>2) The solution must have the ability to open tickets for birth right access that will be auto provisioned.</p> <p>3) The solution must have the ability to update the onboarding request in the Ticketing solution when additional information is provided by new hire's manager.</p> <p>4) The solution must have the ability to close tickets in the ticketing solution for all accounts that it successfully auto-provisioned to provide birth-right access.</p> <p>5) The solution must have the ability to open a request in ticketing system to terminate user's access.</p>

Functional Requirement Category	Functional Requirements – Identity Governance and Administration
	<p>6) The system must have the ability to open tickets for each connected resource to which it will auto-deprovision access when terminating access.</p> <p>7) The system must have the ability to close tickets corresponding to target resources where it successfully terminates access.</p> <p>8) The solution shall provide user-friendly self-service portal that shall integrate with existing ticketing system to initiate access requests, reviews, approvals; such as user requesting for privileges, Managers completing certification review of their direct reports' roles and entitlement, activating/deactivating accounts with domain admin privileges, etc. The solution would trigger tickets on ticketing system continuously tracking and updating the ticket automatically until ticket is closed.</p>
6.1.1.3. Workflow	<p>1) The solution must have the ability to send email notification to user's manager to notify the pending request for additional information.</p> <p>2) The solution must have the ability to send email notification to IGA solution administrator if the manager doesn't provide additional information within the allocated time.</p> <p>3) The solution must have the ability to send email notification to user's manager about successful provisioning of accounts in birth-right platforms.</p> <p>4) The solution must have the ability to send email notification to user's manager with credentials (username and one-time password - to be sent in separate emails) of new account provisioned to provide birth right access.</p> <p>5) The solution must have the ability to send email notification to user's manager with credentials (username and one-time password - to be sent in separate emails) of enabled or provisioned account when reactivating access.</p> <p>6) The solution must have the ability to trigger a "contractor to employee" workflow if HR creates a new employee record and assigns an existing contractors EID to that record.</p> <p>7) The solution must have the ability to send reminders notification prior to the expiration date.</p> <p>8) The solution must have the ability to escalate a request (approval or manual action) to next level manager if no action is taken within two weeks.</p> <p>9) The solution must have the ability to restrict the escalations for up to 2 levels of manager hierarchy before escalating it to system administrator.</p> <p>10) The solution must have the ability to restrict escalations from being assigned to manager above certain grade.</p>
6.1.1.4. Integration	<p>1) Authentication</p> <p>1) Should be in place for the information users share with the system and their authentication level.</p> <p>2) Security features including rights management, LDAP integration, password encryption, etc.</p> <p>2) Authorisation levels</p> <p>1) These functions determine various system access levels and decide who can CRUD (change, read, update, or delete) information.</p>
6.1.1.5. External Users	<p>1) A solution that will be able to manage external users using Microsoft Entra External ID.</p>

Functional Requirement Category	Functional Requirements – Identity Governance and Administration
6.1.1.6. Audit, Logging and Reporting Requirements	1) The solution shall provide rich audit and reporting (including dashboards) capabilities that allow business users, IT users and auditors to review not only who has/had access to what but also how such access, role, privilege was acquired.
6.1.1.7. SoD	1) The supplier shall develop a reconciled role versus permission matrix with principles that align with City of Cape Town access policies separately for IT applications and for business applications. The matrix shall enumerate all the roles that can be provisioned and explore the permissions that can be applied to the objects, including any constraints.
6.1.1.8. Legal or Regulatory Requirements	1) Should consider and adhere to laws, regulations from the government, and even internal policies that the organization and their systems must follow.
6.1.1.9. Industry Standards and Protocols	1) This solution shall support at minimum industry authorisation standards such as, XACML, OAuth/OAuth2, identity standards such as SAML 2.0. 2) The solution shall support other industry protocols and file formats such as: CSV, JSON, WMS, XML, Text.
6.1.1.10. Self-Service Password Reset	1) The Solution shall provide password management capability that allows changing, resetting passwords across business and IT applications. 2) The password management capability shall address CCT's password complexity requirements. 3) Password complexity requirements to be aligned to ISO 27001 or NIST.
6.1.1.11. RBAC	1) The Solution must have the ability to cater for Role Based Access Control.
6.1.1.12. Substitutions	1) The Solution shall allow the manager or HR to initiate substitutions.
6.1.1.13. Integration into existing source and Target directories	1) The Solution must have the ability to integrate back to existing source directories at a minimum: <ul style="list-style-type: none"> • SAP Directories • Microsoft Active Directory • Microsoft Entra ID 2) The solution must have the ability to integrate to the following Target systems: <ul style="list-style-type: none"> • Service Now • Emergency Policing Incident Control (EPIC) system • Channel Management Contact Centre application • ESRI ArcGIS (SQL Based system) • SQL back-end applications • Oracle back-end applications

Functional Requirement Category	Functional Requirements – Identity Governance and Administration

6.1.2. Single Sign On (SSO):

Provides the capability to authenticate once and be subsequently and automatically authenticated when accessing various source applications. The City has designated Microsoft Entra ID as the primary Identity Provider for internal identities and Microsoft Entra External ID (previously Azure AD B2C) as the Identity Provider for external identities. The Supplier shall be responsible for configuring and onboarding applications to these existing SSO platforms.

The Supplier shall **not supply, license, or replace** the SSO software. The City has already procured and implemented Microsoft Entra ID, while Microsoft Entra External ID requires tenant setup and configuration to be complete by the Supplier.

The solution must include, but is not limited to, the following functional requirements:

Functional Requirement Category	Functional Requirements – Single Sign-on
6.1.2.1. General	<p>The Supplier shall:</p> <ol style="list-style-type: none"> 1) Application Onboarding <ol style="list-style-type: none"> a. Configure approximately 20 custom .NET applications currently using IIS authentication to integrate with Microsoft Entra ID. b. Configure ITSM cloud application for SSO integration. c. Configure channel management instances for SSO integration. d. Configure connection to SAP Cloud Identity Services to federate with Microsoft Entra ID. e. Configure connection to EPIC for SSO integration 2) Microsoft Entra External ID Tenant Setup <ol style="list-style-type: none"> a. Develop and implement user journeys and workflows for onboarding external identities, including registration, authentication, password reset, and multi-factor authentication flows. b. Ensure workflows comply with the City’s identity governance, privacy, and security standards. c. Integrate Microsoft Entra External ID with the City’s Identity Governance Administration (IGA) system to enable centralized lifecycle management, policy enforcement, and audit reporting for external identities. 3) Collaboration <ol style="list-style-type: none"> a. Work with other Suppliers and City employees to ensure successful SSO configuration and application onboarding. b. Coordinate with application owners to validate authentication flows and minimize disruption during migration. 4) Configuration Requirements <ol style="list-style-type: none"> a. Implement secure federation protocols (e.g., SAML, OAuth 2.0, OpenID Connect) as required by each application.

Functional Requirement Category	Functional Requirements – Single Sign-on
	<ul style="list-style-type: none"> b. Apply conditional access policies in line with the City's security standards. c. Ensure proper role-based access control (RBAC) alignment with the City's identity governance framework. <p>5) Testing and Validation</p> <ul style="list-style-type: none"> a. Conduct end-to-end testing of authentication and authorisation flows for both internal and external identities. b. Provide documentation of configuration steps, user journeys, and test results for each application. c. Resolve integration issues in collaboration with stakeholders.

6.1.3. The following tools/functions are out of scope:

- Organizational Governance, Risk and Compliance: Strategy / tool for managing an organization's overall governance, enterprise risk management and compliance with regulations.
- Tools to create Authorisations in any Source Applications.
- Requirement to manage Outlook Calendars and E-mails on behalf of another person.

6.2. NON-FUNCTIONAL REQUIREMENTS for IGA

All requirements in this section are specific to Schedule 1 Identity Governance and Administration (IGA). They do not apply to PAM or Identity Proofing unless explicitly cross-referenced.

6.2.1. Performance Requirements IGA Specific

The following performance requirement applies specifically to the IGA solution:

- Access certification campaigns must support bulk operations of at least 10,000 access review items per campaign without performance degradation.

6.2.2. Integration Requirements IGA Specific

The following integration capabilities are required specifically for the IGA solution:

- The solution must support standard HR system connectors including SAP SuccessFactors, via direct connector or an API import for joiner/mover/leaver (JML) processing.
- The solution must support integration with ITSM platforms (City will implement ServiceNow) for access request workflow management and fulfilment.
- The Solution support integration to SAP module such as but not limited to SAP ARIBA, SAP Cloud Identity Services, SAP Analytics Cloud, SAP S/4HANA and SAP Service Cloud.
- The Solution support integration to Oracle and SQL databases

6.2.3. Regulatory and Governance Requirements IGA Specific

The following governance and compliance requirements apply specifically to the IGA solution:

- The solution must enforce Segregation of Duties (SoD) controls and provide SoD conflict detection and remediation workflows.
- Access certification (attestation) campaigns must support SOX, ISO 27001, and NIST compliance reporting.
- The supplier shall design and implement a role centralization framework across in-scope business applications.

6.2.4. Deployment Requirements

- Only Software as a Service solutions will be considered.
- The solution shall be deployed as 3 tier environment i.e. Development, QA/Test and Production. Development environment cannot communicate with the production environment.

6.3. FUNCTIONAL REQUIREMENTS OF PAM SOLUTION

This scope definition is related to **SCHEDULE B** in section **C.4 Price Schedule** and evidence of the proposed solution should be submitted as required in SCHEDULE F.13: Information to be provided with the tender.

Privileged access management (PAM): Consists of the cybersecurity strategies and technologies for exerting control over the elevated (“privileged”) access and permissions for users, accounts, processes, and systems across an IT environment.

The solution must include, but is not limited to, the following functional requirements:

Functional Requirement Category	Functional Requirements – PAM
<p>6.3.1. Architecture & Integration</p>	<ol style="list-style-type: none"> 1) The solution provides the ability to provide Standard APIs to enable authentication and authorisation integration with key proposed solution environments such as LDAP, Entra ID Windows, and SAP. 2) The solution is able to integrate with different types of third-party target systems (including out-of-the-box connectors to LDAP, Database, and UNIX systems). 3) The solution has the ability to provide workflow features for administrative users to request access, and for authorised approvers to grant this access. 4) The solution supports integration with Identity and Access Management (IAM) products for privileged user account provisioning, de-provisioning and access certification. 5) The solution supports discovery of SSH keys present in supported CCT systems. 6) The solution provides a highly secure centralised repository to store private user and application SSH keys. 7) The solution supports encryption of key storage (at rest). 8) The solution supports authentication to its user interfaces using the City’s SSO and multi-factor authentication. 9) The solution protects credentials within memory (in use). 10) The solution supports encryption of network sessions including user interface and inter vault communication (in transit).

Functional Requirement Category	Functional Requirements – PAM
	<p>11) The solution has the ability to discover privileged accounts on all supported CCT systems.</p> <p>12) The solution provides out-of-the-box capability to integrate with the Directory Services for managing privileged accounts.</p> <p>13) The solution has out-of-the-box capability to integrate with SAP and Microsoft applications for managing privileged accounts.</p> <p>14) The solution has out-of-the-box capability to integrate with the Database solutions such as MS-SQL for managing privileged accounts.</p> <p>15) The solution provides software libraries for development languages allowing for programmatic checkout.</p>
<p>6.3.2. General Security Requirements</p>	<p>1) The solution stores all passwords in encrypted format.</p> <p>2) The solution supports the use of HSM to store master keys for password encryption.</p> <p>3) The solution supports industry standards for encrypting data (such as AES 256).</p> <p>4) The solution protects PAM web portal against OWASP TOP 10 attacks.</p> <p>5) The solution has the ability to perform input validation to ensure confidentiality, integrity, and availability of the solution is not adversely affected.</p> <p>6) The solution ensures that configurations are aligned with CCT Cyber security policies and standards.</p> <p>7) The solution provides the ability to prevent manipulation of system of record data.</p> <p>8) The solution ensures that compromised data can be detected and all passwords changed immediately.</p> <p>9) The solution supports encryption of all session logs, records and receipts.</p> <p>10) The solution automates and enforces best practice privileged account security, including enforcing one-time passwords.</p> <p>11) The solution provides individual accountability and full monitoring of activity on shared accounts.</p>
<p>6.3.3. Cloud API & Mobile</p>	<p>1) The solution supports integration with cloud exchange servers to send notifications when required.</p> <p>2) The solution supports password check-in, check-out using mobile devices.</p> <p>3) The solution supports integration with CCT ticketing system to support workflows for PAM.</p> <p>4) The solution integrates with cloud-based identity stores that can assist in governance of privileged identities including provisioning, de-provisioning, and identifying orphaned accounts.</p> <p>5) The solution supports secure and tamper proof methods to communicate with the management consoles, and APIs of public cloud providers like AWS, Azure or equivalent</p>

Functional Requirement Category	Functional Requirements – PAM
	<ul style="list-style-type: none"> 6) The solution allows the access of privileged accounts of CCT systems, residing on cloud services using a defined workflow. 7) The solution supports methods such as API or web services that can help in automatic provisioning and de-provisioning of endpoints or systems and provision passwords into the vault. 8) The solution supports the retrieval of the embedded cloud services access keys and shared keys from the vault. 9) The solution provides facility to access the cloud services instances seamlessly, without the need to check out the passwords. 10) The solution supports transparent transfer of SSH private key to the end system during login process. 11) The solution has the ability to limit the access to the Cloud instances via a proxy or jump server. 12) The solution has the facility to control access to the cloud services management consoles using Identity and access management features. 13) The solution allows accessing the CLI or PowerShell interfaces seamlessly without the need to know the access key and shared keys. 14) The solution monitors all privileged activity and alert on suspicious behavior in public cloud environments. 15) The solution has the ability to integrate with private cloud and allow integrations with Microsoft Hyper-V or equivalent.
6.3.4. Auditing & Reporting	<ul style="list-style-type: none"> 1) The solution provides support for its users to create ad-hoc reports. 2) The solution supports flexible reporting capabilities to allow owners visibility of access entitlements and operational usage of secrets. 3) The solution has the ability to consume logs via a programmatic interface 4) The solution produces audit logs that must capture all the activities and the responsible parties within the solution 5) The solution provides capabilities to track unauthorised activities and send alerts to the support team/manager. 6) The solution provides alerts and notifications to the administrator in case of password reset operation failures. 7) The solution provides logging and alerting capabilities on access management, operational access, policy and configuration changes. 8) The solution supports sufficient metadata to appropriately log and report on PAM actions and events, while maintaining privacy and security of identity and credential information. 9) The solution provides the ability to produce logs that are readable and perusable. 10) The solution provides the ability to audit administrative accounts, access and roles. 11) The solution logs all successful and failed user authentications into the PAM system including connected target systems.

Functional Requirement Category	Functional Requirements – PAM
	<p>12) The solution logs PAM account management (creation, deletions and modifications).</p> <p>13) The solution must log events such as granting, revoking, and modifying security privileges.</p> <p>14) The solution logs password changes for all target systems.</p> <p>15) The solution logs all PAM account lockouts.</p> <p>16) The solution prevents log manipulation, overwriting and deletion.</p> <p>17) The solution's reporting functionality is available to teams based on their roles and access.</p> <p>18) The solution is able to generate reports that compare data from the PAM record with the original target systems (i.e. Directory Services, Microsoft, SAP etc.)</p> <p>19) The solution reports listings of user accounts, administrative users and roles.</p> <p>20) The solution is able to provide usage reports based on a number of criteria, including, but not limited to:</p> <ul style="list-style-type: none"> • User identity • Login/failed login transactions • Target Account Password resets • Transactions across specified time periods. <p>21) The solution is able to create / amend / delete Administrators and Read-Only user access to the reporting environment and configure granular level of reporting access for these users.</p> <p>22) The solution provides standard defined reports on a scheduled basis (i.e. Daily, weekly, monthly, date range defined etc.)</p> <p>23) The solution delivers the reports in an encrypted and secure manner.</p> <p>24) The solution is able to perform capacity reports (measuring & monitoring) on key functional services and performance targets.</p> <p>25) The solution is able to record all Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), SSH, and SQL sessions launched from the application.</p> <p>26) The solution has an external storage location that stores recorded sessions in an encrypted format.</p> <p>27) The solutions recorded sessions can be traced using any detail, such as the name of the connection, the user who launched the session, or the time at which the session was launched.</p> <p>28) The solution is able to generate reports in Pdf and Excel, CSV.</p>
<p>6.3.5. Performance and Availability</p>	<p>1) The solution provides the ability to be configured in a highly available configuration to meet a stated availability requirement of 99.95%.</p> <p>2) The solution must be able to connect to and manage privileged sessions across more than 10,000 different target systems/devices (e.g. servers, databases, applications, network devices).</p>

Functional Requirement Category	Functional Requirements – PAM
	<ol style="list-style-type: none"> 3) The solution must support enforcing privilege escalation policies (e.g., just-in-time elevation, sudo rights, role elevation) across more than 10,000 target systems/devices. 4) The solution is equipped with load balancing and hot-hot peer to peer replication at the solution suite level. 5) The solution is equipped with load balancing and hot-hot peer to peer replication at the individual product level. 6) The solution is available 24x7 and should be fully redundant without a single point of failure. 7) The solution has the ability to accommodate a minimum percentage increase of 10% for users with elevated privileges per year. 8) The solution is able to support a minimum of 1,000 concurrent active users of privileged session management at any given time for both normal and failover concurrency scenarios. 9) The solution has the ability to work via Wide Area Network (WAN). 10) The solution has the ability to provide users with real-time response for actions being performed in the GUI. 11) The solution ensures that there is no more than a 3 second delay in displaying an action.
6.3.6. Service and Support	<ol style="list-style-type: none"> 1) Vendors/Solution providers provide software and operational (if applicable) 24/7 support. 2) Vendors ensure that an SLA is established for helpdesk response time to ensure that incidents and problems are responded to in a timely manner. 3) Vendors ensure that a support model is in place for outdated version of the product suite to ensure software in place is supported regardless of timing. 4) Vendors ensure that Tier 2 and Tier 3 support is directly available to CCT during the duration of the contract. 5) Hotfixes to critical support issues are available to CCT to ensure that 0-day vulnerabilities and critical vulnerabilities are available for patching. 6) Vendor ensures that product training is provided for CCT staff to administer the solution within the CCT environment. 7) Vendor provides a deployment plan or timeline for implementing a solution for CCT. 8) Vendor describes the ongoing maintenance efforts for the solution deployment.
6.3.7. Monitoring and Recoverability	<ol style="list-style-type: none"> 1) The solution is able to meet the desired Recovery Point Objective (RPO) of 2 hours, if the failure is due to a database loss. 2) The solution is able to meet the desired Recovery Point Objective (RPO) of 12 hours, if the failure is due to a Data Centre Site loss. 3) The solution ensures that all data must be backed up securely and restored when required.

Functional Requirement Category	Functional Requirements – PAM
	<ol style="list-style-type: none"> 4) The solution establishes monitoring for all critical system components. 5) The solution has the ability to integrate with the City's SOC Provider via syslog or API. 6) The solution has in-built recovery mechanism in case of failover situations. 7) The solution offers built-in high availability capability to avoid single point of failure. 8) The solution provides the ability to monitor the up/down status of the application.
6.3.8. Usability and experience	<ol style="list-style-type: none"> 1) The solution provides the ability to apply custom CCT branding. 2) The solution provides a GUI-based Administration console. 3) The solution enforces designated required fields in forms. 4) The solution highlights all required fields on screen that require data entry. 5) The solution allows users to define and choose elements for dashboarding. 6) The solution is able to support CCT's standard browser (Microsoft Edge). 7) The solution is able to bulk import and upload customise data for initial deployment. 8) The solution provides a self-service help page. 9) The solution allows for localisation (time zones, language, currency)
6.3.9. Privileged Password Management	<ol style="list-style-type: none"> 1) The solution provides the ability to establish a default password policy to be assigned to every new and linked account within the system 2) The solution provides the ability to enforce a limit to the amount of time a password can be checked out before it is forcibly changed. 3) The solution ensures that the break-glass administrative account passwords for the PAM system must be maintained outside of the PAM system. 4) The solution allows users to check in and check out passwords from the PAM solution 5) The solution ensures that passwords for inactive accounts in the target system are automatically reset and password policy is enforced 6) The solution ensures that a PAM password will be changed immediately upon expiration (as defined in the password policy set forth by CCT Cyber Security) 7) The solution ensures the enforcement of password policies in all scenarios that require the PAM system to create or update the password of a target system account. 8) The solution provides the ability to define multiple password policies and usage that can be assigned to user accounts.

Functional Requirement Category	Functional Requirements – PAM
	<p>9) The solution has the ability to ensure that there will be no minimum amount of time between password resets for secondary accounts.</p> <p>10) The solution ensures that all new passwords that are created have the correct composition and length in adherence to CCT Information Security Policy.</p> <p>11) The solution provides the ability to automatically change the password on a pre-defined account in a target system.</p> <p>12) The solution provides the ability to track the amount of time it has been since the password has been updated for a linked account in a target system.</p> <p>13) The solution provides the ability for end-users to view the current password for the privileged accounts which they have checked out.</p> <p>14) The solution provides the ability to enforce an immediate automatic password reset for privileged accounts after their usage has come to an end.</p> <p>15) The solution ensures that a password within a user account in the PAM system must be removed once its target account has been deleted or archived (from the target system)</p> <p>16) The solution provides the ability to create a personal safe/container for end users and store all the passwords associated with their target accounts in that user safe/container.</p> <p>17) The solution provides the ability to create a shared safe/container that stores passwords for accounts on multiple target systems and can be accessed by multiple users.</p> <p>18) The solution ensures that once a privileged account has been provisioned and its password vaulted by the PAM solution, any manual changes of the password in the target system are overridden by the PAM system.</p> <p>19) The solution supports the capability to automatically rotate privileged passwords after every retrieval and use.</p> <p>20) The solution supports the capability to automatically rotate privileged passwords after the password has been exposed in hidden/clear text to an internal user.</p>
<p>6.3.10. Privileged Session Management</p>	<p>1) The solution ensures that session connection, maintenance and termination to provide access to privileged systems is secured.</p> <p>2) The solution ensures that Session tokens are created or regenerated after successful authentication.</p> <p>3) The solution leverages platform provided session management and session token mechanisms.</p> <p>4) The solution supports session recording and monitoring of all Privileged sessions initiated using the PAM solution.</p> <p>5) The solution provides a Portal for end-users to access privileged accounts for which they've been authorised.</p> <p>6) The solution supports PAM Administrators & Users to log into the PAM solution using MFA authentication with their primary credentials and MFA pin/token.</p>

Functional Requirement Category	Functional Requirements – PAM
	<p>7) The solution ensures that all users must provide credentials each time they are seeking to access the PAM system. Note: User access here refers to the user's session at the PAM portal and not the session at the endpoint.</p> <p>8) The solution ensures that users are automatically logged out after a predefined period of time in compliance with policy established by Information Security.</p> <p>9) The solution provides the ability to ensure that PAM admins do not authenticate into the portal, via the same user store as the users of the solution. Users will be authenticated against the primary user store (Directory Services) and PAM admins will be authenticated against a custom user store within PAM.</p> <p>10) The solution ensures that the end user's session at the endpoint is not ended, when the user logs out of their PAM portal session. Note: User session here refers to the user's session at the endpoint and not the session at the PAM Portal.</p> <p>11) The solution ensures that end users are only able to search for those privileged accounts which they are authorised to use.</p> <p>12) The solution is capable of restricting end-users' ability to search for and access privileged accounts to only those accounts for which they have a grant.</p> <p>13) The solution is capable of sharing a session with multiple users. Note: Other users may be restricted to only view access with a single user having control over actions.</p> <p>14) The solution is capable of sharing control of active sessions with multiple users.</p> <p>15) The solutions provide the ability to enforce multi user requirements to activate a new session with an end point.</p>
<p>6.3.11. Privilege Escalation</p>	<p>1) The solution allows users to work under standard user accounts, following least privilege best practice.</p> <p>2) The solution supports the seamless elevation of individual applications.</p> <p>3) The solution supports the seamless elevation of application groups.</p> <p>4) The solution supports advanced users, who may need to elevate applications on demand.</p> <p>5) The solution uses a modified security token, local credentials, or domain credentials for application elevation.</p> <p>6) The solution provides granular application control (by publisher, file path, or hash).</p> <p>7) The solution provides the ability to deny applications from executing and provide user feedback.</p> <p>8) The solution provides the ability to quarantine applications if they have been deemed a high risk.</p> <p>9) The solution supports delegated administration.</p> <p>10) The solution ensures that break-glass features are available to escalate privileges to perform administrative tasks on the target system.</p>

Functional Requirement Category	Functional Requirements – PAM
	<p>11) The solution consumes the level of risk on an application before assigning privileges and detects the launch of vulnerable software.</p> <p>12) The solution provides application templates for built-in operating system tasks and common third-party applications.</p> <p>13) Monitoring:</p> <ul style="list-style-type: none"> • The solution has the capability to monitor and flag high risk activities. • The solution performs file and directory monitoring on systems to support escalation of privileges based on defined policies. <p>14) Policies:</p> <ul style="list-style-type: none"> • The solution supports creation of policies that target different users, computers, OU's, security groups, etc. • The solution obeys Group Policy precedence rules when applying multiple GPOs or equivalent. • The solution supports Resultant Set of Policy (RSOP) or equivalent. • The solution supports Advanced Group Policy Management (AGPM) and other third-party group policy change control products.
<p>6.3.12. System Administration and Role Management – (Create)</p>	<p>1) The solution provides ability to create new distinct roles with the PAM solution – e.g. User, PAM Admin and PAM Auditor.</p> <p>2) The solution provides the ability for PAM admins to manually create a privileged account as well as to manually assign a password policy to them.</p> <p>3) The PAM solution provides the capability to automatically create a user's safe, provision the user's privileged accounts in the target system and vault passwords for each provisioned privileged account.</p>
<p>6.3.13. System Administration and Role Management – (Modify)</p>	<p>1) The solution provides the ability to add/remove users to pre-defined roles within the application.</p> <p>2) The solution ensures that once the end user's secondary account has been disabled in the target system, their associated PAM account must be disabled immediately.</p> <p>3) The solutions enable PAM administrators to have the ability to manage the lifecycle of a privileged account (create, update, delete).</p> <p>4) The solution provides the ability to link a user's account within the PAM system to one in a target system by a unique identifier.</p>
<p>6.3.14. System Administration and Role Management – (Delete)</p>	<p>1) The solution ensures that an account within a user repository / safe in the PAM system must be removed once its target account has been deleted or archived (from the target system)</p> <p>2) The solution provides the ability to manually remove a privileged account from the system.</p> <p>3) The solution provides the ability to automatically remove a privileged account based on the archival/deletion of its target account [from the target system].</p>

Functional Requirement Category	Functional Requirements – PAM
	<ol style="list-style-type: none"> 4) The solution provides the ability to automatically remove a user's repository /safe, if there are no more privileged accounts in the target systems for that user. Note: This implies that the user does not have any secondary account. 5) The solution provides the ability for PAM admins to manually remove a privileged account as well as to manually assign a password policy to them. 6) The solution has the ability to disable a user's privileged account for a particular target system for a prescribed number of days before deleting it. Note: PAM deprovisioning begins when the PAM system finds that the target account in the target system associated with a users' account, has been disabled or deleted. 7) The solution ensures that the user is not able to delete any of the privileged accounts in their repository/safe.
6.3.15. System Administration and Role Management	<ol style="list-style-type: none"> 1) The solution provides the ability to verify the identity of users seeking access to the PAM system prior to being allowed entry. 2) The solution ensures that roles and access are configured in compliance with the Role Based Access Control (RBAC) methodology. 3) The solution provides a centralised reporting and management console. 4) The solution has the ability to manage non-domain or disconnected assets. 5) The solution provides the ability to search for a privileged account within the system based on multiple criteria. Note: This applies only to PAM admins. 6) The solution ensures that administrative rights within the PAM system must enforce separation of duties (based on a CCT support model). 7) The solution provides the ability to define the user repository used for authentication of users and PAM administrators. 8) The PAM solution must allow administrators to specify and manage the exact system locations of privileged accounts, to ensure that all privileged accounts are correctly mapped to their target systems. 9) The solution provides the ability to allow PAM administrators to manage authorisation to the system. 10) The solution ensures that the user's access to their accounts within PAM is locked out at the PAM portal, after a predefined number of unsuccessful log on attempts. 11) The solution has a Portal available for system administrators to configure password and usage policies and/or troubleshoot the solution. 12) The solution provides the ability to define the location(s) of the target system accounts. 13) The solution ensures that there are no orphaned accounts within the PAM solution.

Functional Requirement Category	Functional Requirements – PAM
	14) The solution provides the ability to establish a default usage policy to be assigned to every new grant within the system. 15) The solution ensures that a notification is sent to the user after the PAM solution provisions their secondary account and vaults their password.

6.4. NON- FUNCTIONAL REQUIREMENTS OF PAM SOLUTION

All requirements in this section are specific to Privileged Access Management (PAM). They do not apply to IGA or Identity Proofing unless explicitly cross-referenced.

6.4.1. Estimated Sizing

- The City has approximately 400 administrator accounts that is used to manage and monitor systems
- The City has approximately 450 system accounts (Service Accounts)
- The PAM solution preferably supports storage of at least 3 TB for privileged session recordings, based on an estimated 1,000 compressed 1-hour sessions per week retained for 90 days in a single region.

6.4.2. Performance Requirements PAM Specific

The following performance requirement applies specifically to the PAM solution:

- Privileged session initiation (PAM) must complete within 5 seconds from request approval to active session.

6.4.3. On-Premises Infrastructure Requirements PAM

Although the PAM solution is to be delivered as SaaS, it is acknowledged that certain components may require on-premises installation to support hybrid connectivity, session management, or local credential vaulting. Vendors must fully document all required on-premises components. All on-premises infrastructure must be clearly listed with detailed specifications.

6.4.4. Security Requirements PAM Specific

The following security requirement applies specifically to the PAM solution:

- Credentials and secrets (passwords, SSH keys, certificates) stored in the PAM vault must be encrypted with envelope encryption and FIPS 140-2 Level 2 compliant HSMs.

6.5. FUNCTIONAL REQUIREMENTS OF IDENTITY PROOFING SOLUTION

This scope definition is related to **SCHEDULE C** in section **C.4 Price Schedule** and evidence of the proposed solution should be submitted as required in **SCHEDULE F.13: Information to be provided with the tender**.

Identity Proofing is the process of verifying that the claimed identity of a juristic entity or natural person matches their actual identity. It is a detailed authentication process that businesses use to ensure their clients are who they claim to be. To avoid data breaches and fraud, which can be costly, businesses can require multiple steps of identity verification, and Identity Proofing goes beyond basic authentication to add additional verification measures such as government documents, photo IDs, and personal questions.

The requirements for a juristic person are as follow:

- A resolution signed by all directors/members/trustees etc. of the organisation stating who has the delegated authority to transact with the City on their behalf

- ID for all owners/directors/members/trustees etc.
- ID for delegated authority
- Relevant company registration document such as:
 - CK Document: Required for all transactions involving a CC; any supporting letters must be signed by the OWNERS
 - CM Document: Otherwise known as a Company Registration Document; required for all transactions involving a PTY/LTD; any supporting letters must be signed by the DIRECTOR
 - Trust Document / Master's Certificate: Required for all transactions involving a Trust. The document must list all active trustees. Any supporting letters must be signed by all TRUSTEE'S
 - Certificate of Establishment: Required for all transactions involving a Body Corporate; any supporting letters must be signed by two members of the Body Corporate.
 - Letter of Executorship: Required for all transactions involving a deceased persons account. This letter indicates who was named as the person to deal with the deceased estate. A letter of consent signed by the executor must accompany the letter of executorships as well.
 - Constitution of an Organisation: Required for all transactions involving NPO'S, NGO's, PBO's and PLACES OF WORSHIP. The constitution is the key founding document of an organisation. It is a record of agreements on the basic principles of the organisation and is legally binding on all members.

The identity proofing solution must include, but is not limited to, the following functional requirements:

Functional Requirement Category	Functional Requirements – Identity Proofing Solution
6.5.1. Identity Proofing – Natural person (Attributes)	Identity Proofing shall be delivered from the extendable data elements. The claims data elements transmitted to the Identity Proofing tool include the following: <ul style="list-style-type: none"> • First Name • Surname • SA ID Number • Date of Birth (DOB) • Address(s) • Phone Number(s) • Passport Number(s) for foreigners • Biometrics i.e. Face recognition, fingerprints
6.5.2. Identity Proofing – Juristic entity attributes	Identity Proofing shall be delivered from the extendable data elements. The claims data elements transmitted to the Identity Proofing tool include the following as a minimum: <ul style="list-style-type: none"> • First Name • Surname • Company registration number (dependent on the type of company) • Telephone number • Physical address of property the enquiry relates to • Position at company / relation to the business.
6.5.3. Identity Proofing (Integration)	Process both individual requests via API and bulk requests of multiple identities via batch processing.
6.5.4. Identity Proofing (Protocols)	This solution shall support at minimum industry authorisation standards such as OAuth2, identity standards such as SAML 2.0. and OIDC
6.5.5. Identity Proofing (Data Stores)	The system should be able to store verification data from external sources.
6.5.6. Identity Proofing (Sources)	1) Information used to evaluate the identity should be matched through multiple sources of data to increase the accuracy of the evaluation and decrease the likelihood of false positives. Examples of data sources may include, but not be limited to: <ul style="list-style-type: none"> • Consumer Credit Information and/or other financial data; • Social Security Administration information; • Known address information;

Functional Requirement Category	Functional Requirements – Identity Proofing Solution
	<ul style="list-style-type: none"> • Telecommunications Information; and • Billable utilities information. <p>2) The solution should have the widest reach possible. A target for the Identity Proofing solution is to have information returned for 90 percent of the claims submitted for verification. Included in this population will be individuals who:</p> <ul style="list-style-type: none"> • Lack traditional residency history; and • Lack traditional employment history.
6.5.7. Identity Proofing (Scoring)	<p>1) The processes utilized to determine identity scoring should include pattern matching and recognition and evaluation of the information provided to determine identity risk. Process should include (but not be limited to):</p> <ul style="list-style-type: none"> • Fraudulent behavior checks based on fraud indicators; • Pattern recognition (i.e. multiple verification checks, multiple address checks, etc.); • Address checks (valid, deliverable, associated with individual, etc.); • The processes should return a risk score as determined by the CCT, this score shall indicate the risk associated with the information presented. At a minimum the solution should indicate: <ul style="list-style-type: none"> - Synthetic/Fake Identity; - Known Compromised (stolen) Identity; - Ranking of Fraud Potential; - Ranking of Other Issues; and in conjunction with the score cause codes related to the score should be provided.
6.5.8. General	<p>1) The solution must support facial and/or biometric capture (including selfie-based capture) via web and/or mobile interfaces.</p>

6.6. NON- FUNCTIONAL REQUIREMENTS OF IDENTITY PROOFING SOLUTION

All requirements in this section are specific to Identity Proofing. They do not apply to IGA or PAM unless explicitly cross-referenced.

6.6.1. Performance Requirements Identity Proofing Specific

The following performance requirement applies specifically to the Identity Proofing solution:

- Identity Proofing biometric matching must return a result within 10 seconds under normal load.

6.6.2. Identity Proofing Technical Specifications

The following technical requirements are specific to the Identity Proofing solution and cover document verification, biometric matching, authoritative data source integration, and result handling:

- The Identity Proofing solution must support document verification for South African identity documents (RSA ID Book, Smart ID Card, Passport) at minimum.
- Biometric liveness detection must be compliant with ISO 30107-3 PAD Level 2 or equivalent.

- The solution must integrate with the Department of Home Affairs (DHA) or equivalent authoritative identity data source for verification.
- The identity proofing result and confidence score must be accessible via API for integration with downstream onboarding workflows.

6.6.3. Estimated identity verification quantities

The estimated volume of identity verifications per month is approximately 80,000 for calls received through the City's various call queues and emails (Accounts General, Accounts Payable, Motor Vehicle Registration, Traffic, Drivers Licence Testing Centre and Accounts Payable, e-Services).

6.7. GENERAL REQUIREMENTS APPLICABLE TO ALL THREE STREAMS (IGA, PAM AND IDENTITY PROOFING)

All requirements in this section apply equally to Schedule 1 (IGA), Schedule 2 (PAM), and Schedule 3 (Identity Proofing). Vendors must confirm compliance for each solution or module submitted.

6.7.1. Deployment Model

The preferred deployment model is Software-as-a-Service (SaaS). Vendors offering hybrid or on-premises deployment must clearly document all implications, including infrastructure, licensing, and support boundaries.

6.7.2. SaaS Model Compliance

- The solution must be delivered as a cloud-native, multi-tenant or single-tenant SaaS offering hosted and managed by the vendor. The following requirements apply:
- The solution must be delivered as a fully managed SaaS offering with no requirement for the customer to manage application-layer infrastructure.
- The vendor must manage all patching, upgrades, and maintenance of the platform, with prior notification to the customer.
- The vendor shall publish a public or customer-accessible service status and incident notification page (status page).
- The solution must support tenant isolation — customer data must not be accessible to other tenants.
- The vendor must clearly define the data residency options available (e.g., South Africa, EU). Customer must be able to select their preferred data residency region.
- The vendor must provide a documented shared responsibility model delineating vendor vs. customer responsibilities for security, compliance, and operations.
- The vendor must support a clearly documented release management cycle including major, minor, and patch releases, with advance notice of at least 30 days for breaking changes.
- The solution must provide customer-accessible administrative portals and APIs for self-service configuration within agreed boundaries.

6.7.3. Network and Connectivity

- The solution must document all inbound and outbound network port and protocol requirements for on-premises components.
- All outbound connectivity from on-premises components to the SaaS platform preferably use HTTPS (port 443) to minimise firewall changes.
- The solution must support proxy server configuration for environments where direct internet access is not permitted.
- IP allow-listing of SaaS platform egress addresses must be supported and documented, with advance notice of IP changes.

6.7.4. Performance Requirements

- The solution must be designed to deliver consistent, scalable performance under normal and peak operational conditions. Performance must be maintained across all three deployment tiers, with Production having the highest allocation.
- The following performance requirements apply to all three Schedules:
- The solution shall support a minimum of 50,000 identities in the Production environment, with a clear scaling path to 70,000 for internal identities.
- User authentication (SSO / login) must complete within 2 seconds end-to-end under normal load (up to 500 concurrent users).
- Directory synchronisation (identity imports from AD/LDAP/HR systems) must process a minimum of 5,000 records per minute.
- API response times for provisioning operations must not exceed 3 seconds at the 95th percentile under rated load.
- The solution must support at least 1,000 concurrent web portal sessions without performance degradation.
- The vendor must provide a documented performance benchmark and capacity planning guide for all tiers.
- The solution must support horizontal scaling (scale-out) to accommodate growth without architectural changes.

6.7.5. Security Requirements

Authentication and Access Control

- The solution must support multi-factor authentication (MFA) for all administrative and privileged access to the platform.
- The administrative portal must support SSO integration with Microsoft Entra ID using SAML 2.0 or OIDC.
- Role-Based Access Control (RBAC) must be enforced for all platform administration functions with least-privilege principles.
- All service-to-service API calls preferably use OAuth 2.0 / client credentials with short-lived tokens. Static API keys must not be the sole authentication mechanism.

Data Protection and Encryption

- All data at rest must be encrypted using AES-256 or equivalent. Vendor must disclose the encryption key management model.
- All data in transit must be encrypted using TLS 1.2 minimum; TLS 1.3 preferred. **SSLv3, TLS 1.0, and TLS 1.1 must be disabled.**
- Customers must have the option to manage their own encryption keys (Bring Your Own Key – BYOK) or use a Hardware Security Module (HSM) backed key store.
- The vendor must document the data classification model applied to customer data within the platform.

Compliance and Certifications

- The solution must be compliant with the Protection of Personal Information Act (POPIA) or GDPR where applicable, including data subject request management.
- The vendor must comply with the National Cybersecurity Framework applicable in the customer's jurisdiction.

Vulnerability and Patch Management

- The vendor must have a documented vulnerability management programme and publish a security advisory process (CVE disclosure).
- Critical security patches must be applied within 72 hours of release for the Production environment.
- The vendor must conduct annual penetration testing by an independent third party and provide a summary report to customers upon request.
- The solution support Web Application Firewall (WAF) protection at the application layer.
- The vendor maintains a Software Bill of Materials (SBOM) and disclose any use of open-source components and their licence types.

Audit and Non-Repudiation

- All administrative actions, configuration changes, and privileged access events must be logged to an immutable audit log.
- Audit logs must be retained for a minimum of 12 months online and 5 years in archive, consistent with regulatory requirements.
- Audit logs must be exportable to SIEM platforms (e.g., McAfee, Microsoft Sentinel, Splunk, IBM QRadar) via Syslog, Common Event Format (CEF), or API.

6.7.6. Integration and Interoperability Requirements

- The solution must support open API Standards.
- The solution must provide a REST API for all major platform functions (provisioning, access requests, reporting, audit). Full API documentation must be provided.
- The solution support SCIM 2.0 for automated identity provisioning and de-provisioning to and from connected systems.
- The solution must support native connectors for Microsoft Active Directory and Microsoft Entra ID (Azure AD).
- The solution must support SAML 2.0 and OpenID Connect (OIDC) for SSO federation.
- Webhook support be provided for real-time event-driven integration with third-party systems.
- The solution must provide pre-built connectors or integration templates for common enterprise applications not limited to (Microsoft Azure, Microsoft 365, SAP, Google Workspace, etc.).
- LDAP/LDAPS must be supported as a directory source for identity imports.
- The vendor must document all rate limits applicable to API usage.

6.7.7. Monitoring, Observability, and Reporting

- The solution must provide a built-in operational dashboard displaying real-time service health, active sessions, provisioning queue depth, and error rates.
- The solution support export of operational metrics to monitoring platforms such as Azure Monitor, Datadog, Prometheus/Grafana, or Splunk.
- Automated alerting must be configurable for threshold breaches (e.g., failed login spike, provisioning failures, vault unreachability).
- Comprehensive reporting must cover identity lifecycle events, access certification results, privileged session activity, and compliance posture.
- Reports must be exportable in PDF, CSV, and Excel formats. Scheduled report delivery via email must be supported.
- The solution provides an API to extract reporting data for integration with enterprise BI tools (e.g., Power BI).
- Historical reporting data be accessible online for a minimum of 12 months without requiring archive restoration.

6.7.8. Scalability and Capacity Management

- The solution must support elastic scaling of compute and storage resources in response to load, without customer intervention.
- The vendor must provide capacity planning guidance and a documented scaling model aligned to identity volumes and connector counts.
- Licensing must support growth without requiring re-architecture (e.g., per-identity or per-user licensing models that can scale incrementally).

6.7.9. Data Management and Data Sovereignty

- Customer data must be stored within the data residency region selected at onboarding. Cross-region data transfers must require explicit customer consent.
- The vendor must provide a documented data flow diagram identifying all data stores, processing locations, and any sub-processors.
- The vendor must support a data portability mechanism allowing customers to export all identity data, policies, configurations, and audit logs in a standard format (JSON, XML, CSV).

- Upon contract termination, the vendor must provide a data export within 30 days and certify complete deletion of customer data within 60 days.
- Backup and recovery procedures must be documented. Full backups must be taken at minimum daily; incremental backups must occur at minimum hourly for Production.
- The solution support classification and tagging of sensitive identity attributes (e.g., biometric data, government IDs) to enforce differential access controls.

6.7.10. Vendor Support and Service Management

- The vendor must provide 24x7x365 support for P1/P2 Production incidents via phone and an online ticketing portal.
- A dedicated Account Manager or Customer Success Manager must be assigned to the account.
- The vendor provide access to a self-service knowledge base, documentation portal, and community forums.
- The vendor must provide a named escalation path for executive-level incidents with a documented escalation matrix.

Priority	Definition	Initial Response	Resolution Target	Escalation
P1 – Critical	Production outage or data breach impacting all users	30 minutes	4 hours	Immediate executive escalation
P2 – Medium	Major function unavailable, workaround exists	2 hours	8 hours	Management escalation at 4 hours
P3 – Low	Degraded function, workaround available	4 business hours	2 business days	Standard

6.7.11. Regulatory, Compliance, and Governance

- The solution must support compliance with POPIA (South Africa), GDPR, and other applicable data privacy regulations.
- The vendor must support right-to-access and right-to-erasure requests as required by POPIA/GDPR through automated workflows.
- The solution must generate audit-ready compliance reports aligned to common frameworks (ISO 27001, NIST CSF, SOC 2, King IV).
- The vendor must disclose any sub-processors and third-party services used in delivering the SaaS platform.

6.8. REQUIREMENTS FOR TRAINING SERVICES ON THE ILM SOLUTION

The training refers to training of the administrators of the technologies and does not include training of end users.

The pricing for training services must align with the training components set out in **Tables A4, B4 and C4 of Section C.4 Price Schedule.**

All other training deliverables described in this specification (e.g., self-paced learning materials, change-management related materials, refresher training, updates after system enhancements) must be included in the bidder’s overall solution cost and are not separately priced in the pricing schedules.

6.8.1. Administrator Training

The Supplier must provide comprehensive training to designated City of Cape Town (CCT) administrators. This training must equip administrators with the knowledge and capability to independently train end-users, functional leads, and directorate representatives. Administrator training must include configuration understanding, workflow setup, access governance principles, troubleshooting, and system maintenance procedures. The Supplier must offer the following training options:

- Instructor-led training by the Supplier.
- Certification training for administrators. This training must be instructor led, offered by the by the accredited training partner, and can be conducted over a virtual platform.
- Self-paced web-based training: Must be Sharable Content Object Reference Model (SCORM) compliant.

6.8.2. Development of Reusable Training Materials

The Supplier must develop a full suite of training materials that become the property of the CCT, including but not limited to:

- User guides, quick reference guides, video walk-throughs, facilitator manuals, and scenario-based exercises.
- Materials must be designed so that CCT can reuse, adapt, and deliver training for future onboarding, refresher cycles, or internal capability building.

6.8.3. Training for System Upgrades or New Features

The Supplier must provide training whenever system upgrades, new modules, or functional enhancements are deployed where CCT deems it necessary.

This includes demonstrations, impact assessments, updated training material, and targeted upskilling sessions for affected user groups.

6.8.4. Refresher Training

The Supplier must provide refresher training sessions when required by the CCT.

Refresher sessions may apply after periods of limited use, role changes, process updates, or observed compliance gaps.

6.8.5. Targeted and Audience-Specific Training

The Supplier must deliver tailored training for the various ILM user groups, including (but not limited to):

- HR practitioners, IS&T support teams, security administrators, helpdesk/service-desk teams, managers/approvers, and general end-users.
- Training must be designed to address the responsibilities, maturity levels, and functional needs of each audience.

6.8.6. Training Delivery Approach

The Supplier must offer flexible training delivery methodologies to accommodate the operational needs of the City of Cape Town (CCT). Training delivery methods must include, but are not limited to, virtual training, in-person classroom training, hybrid delivery models, self-paced learning, and hands-on, simulation-based training.

Training schedules and formats must be adaptable to CCT shift patterns, directorate availability, and varying levels of organisational readiness to ensure maximum participation and effective knowledge transfer.

For all training sessions, the Supplier must maintain formal attendance registers and provide competency assessments to validate learning outcomes. Post-training evaluation reports must be compiled and submitted to assess training effectiveness and identify any additional skills gaps.

On-site training sessions will be conducted at designated CCT offices within Cape Town. The selected venue will determine the maximum size of each training group. The current available training rooms have the following capacity:

- Room 1 - 13 (Including Trainers PC)
- Room 2 - 9 (Including Trainers PC)
- Room 3 - 13 (Including Trainers PC)

The on-site training will be delivered face-to-face, conducted by the trainer directly with participating users. All costs associated with travel, accommodation, and related expenses must be fully included in the tendered price, in accordance with the pricing instructions outlined in Section C.4 of the Price Schedule, paragraph 5.3.

6.9. REQUIREMENTS FOR THE IMPLEMENTATION OF THE ILM SOLUTION

The following outlines the requirements and deliverables for the full implementation of the ILM solution through to go-live. The phases and deliverables identified here are aligned with the City of Cape Town's Project Management Office (PMO) methodology for implementation projects, and Suppliers are required to familiarise themselves with these requirements when responding to Price Schedules A, B and C in section C.4 (Price Schedule).

The implementation cost quoted in **Tables A.2, B.2 and C.2 of Schedules A, B and C of C.4 Price Schedule** must include all activities required to deliver a complete and stable ILM deployment, including (but not limited to) project management services, change management functions, development and provision of change management material, and hyper-care support for a minimum of three (3) months post go-live. Hyper-care support must include issue resolution, system stabilisation, performance monitoring, knowledge transfer and operational handover to ensure a smooth transition into steady-state operations.

6.9.1. Draft Implementation Plan

The following is the envisaged implementation plan, which will only be finalised once the Supplier has been appointed and presented their plan.

The Identity Lifecycle Management project implementation commences on the assumption that all required data cleansing activities is completed by source and target application owners. With clean and validated datasets in place, the implementation phase will focus on deploying Identity Governance & Administration (IGA), Privileged Access Management (PAM), Single Sign-On (SSO), and Identity Proofing in a structured and phased manner. This approach ensures that the foundation for identity lifecycle processes is accurate, reliable, and aligned with organisational requirements, enabling a smooth transition into system configuration, integration, and eventual go-live within the defined 12-month implementation timeline.

1. Requirements and GAP Analysis (Months 1–2)
 - Collect business, security, and compliance requirements for IGA, PAM, SSO, and Identity Proofing.
 - Identify source and target systems for IGA
 - Perform GAP analysis against current identity processes and tools.
 - Define scope for internal vs. external identities.
 - Identify applications for initial SSO integration.
 - Document privileged accounts and external identity onboarding needs.
2. Solution Design / Detail Design (Months 3–4)
 - Develop high-level and detailed architecture for IGA, PAM, SSO, and Identity Proofing.
 - Define role-based access models, lifecycle workflows, and proofing methods.
 - Design integration points with HR systems, business partner systems, and Microsoft Entra ID / Azure B2C.
 - Establish security policies (MFA, conditional access, JIT privileged access).
 -
3. Build & Configuration (Months 4–12)
 - IGA Internal Identities (Months 4-12): Configure platform, RBAC, joiner/mover/leaver automation.
 - IGA External Identities (Months 6–12): Configure onboarding workflows, lifecycle policies.
 - PAM (Months 5–12): Vaulting, password rotation, session monitoring, JIT access.
 - SSO Initial Phase (Months 5–6): Configure Entra ID and Azure B2C, integrate 5 applications.

- SSO Continuous Onboarding (Months 6–12): Onboard additional applications.
 - Identity Proofing (Months 6–12): Implement verification workflows for external identities.
4. Testing Phase (Months 9-12)
 - Conduct system integration testing across IGA, PAM, SSO, and Proofing.
 - Perform user acceptance testing (UAT) with business stakeholders.
 - Security and compliance validation (penetration testing, audit checks).
 5. Training & Change Management (Months 9–18)
 - Develop training materials for administrators, helpdesk, and end users.
 - Conduct workshops for business units on new identity processes.
 - Communication campaigns to drive adoption and awareness.
 - Change management activities to address resistance and ensure smooth transition.
 6. Deployment & Go-Live (Month 12-14)
 - Rollout of IGA (internal + external), PAM, SSO, and Identity Proofing.
 - Cutover planning and execution.
 - Go-live readiness checklist and stakeholder sign-off.
 7. Operational Support and Close Out
 - Hypercare (Months 15-18): Dedicated support team, issue resolution, fine-tuning.
 - Support & Maintenance (Months 22–120): Incident/problem/change management, quarterly patching, annual certification campaigns.
 - Project Close Out: Lessons learned, documentation handover, formal closure.

The Supplier shall develop a reconciled role-versus-permission matrix aligned with the City's access policies for both IT and business applications. The matrix shall enumerate all provisionable roles and the permissions applicable to each object, including constraints. This artefact shall be baselined prior to go-live and handed over to CCT.

The Supplier shall provide and implement an ILM capability that centralises and automates authorisation, access, and role provisioning and de-provisioning across in-scope systems and establishes the segregation-of-duties (SoD) policy framework and controls. The implemented capability shall be fully configured, tested, and documented prior to go-live.

The implementation of the ILM solution must also take into account the foundational system landscapes described under **Group 1 (SAP Directory Landscape)**, **Group 2 (Microsoft Directory Landscape)**, and **Group 3 (Third-Party Systems)**. These landscapes define the authoritative identity sources and target platforms into which the ILM components (IGA, and PAM and Identity Proofing) must integrate.

The Supplier must ensure that their implementation approach, resource planning, timelines and costings (as reflected in **Tables A.2, B.2 and C.2 of C.4 Price Schedule**) fully accommodate the integration, synchronisation and configuration requirements described in these sections. Work related to Group 3 systems must be supported through the provision of appropriately skilled ad-hoc Professional Services resources as required by the City (as reflected in **Tables A.5, B.5 and C.5 of C.4 Price Schedule**).

6.9.2. SAP Landscape:

Figure 1 references the SAP AS-IS landscape where the identities are stored and the privileges granted to the various applications that should be synchronised to the ILM solutions (IGA, PAM and Identity Proofing).

The City is in the process of upgrading its existing SAP ECC6 and SAP CRM 7.0 landscape to SAP S/4HANA. The implementation to the new SAP environment will begin in January 2027 with and

expected completion date of December 2029. Table 1 below list the future SAP applications to be implemented at the City.

Table 1: Future SAP applications to be implemented at the City

Application	Cloud or On-premises
SAP S/4HANA (Operational & Financial Core)	On-premises
SAP SuccessFactors (HR Application)	Cloud
SAP ARIBA (Procurement Application)	Cloud
SAP Service Cloud	Cloud
SAP Analytics Cloud	Cloud
SAP Cloud Identity Services	Cloud
SAP integration Suite	Cloud

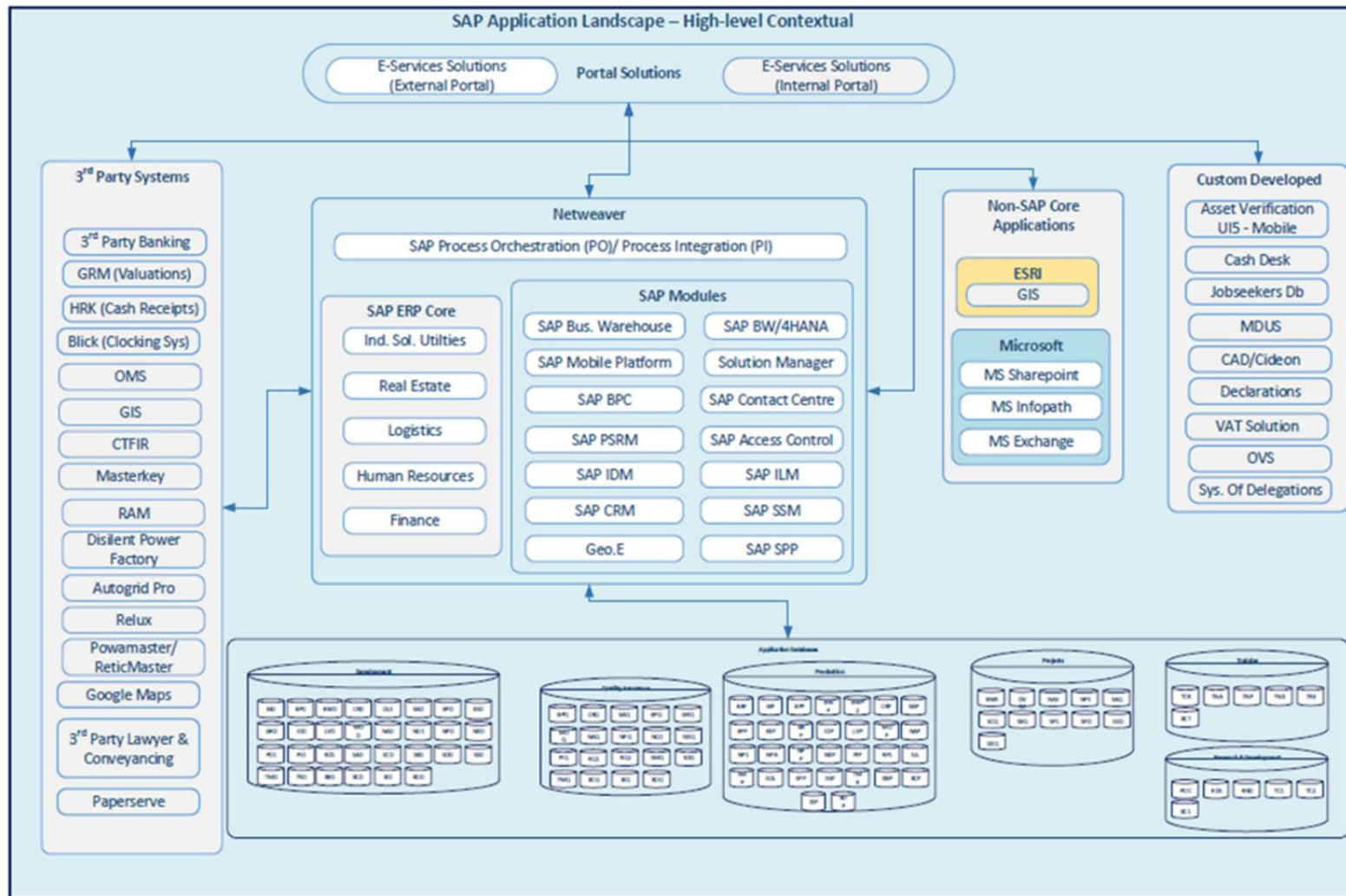


Figure 1: SAP AS-IS landscape

6.9.3. Microsoft Landscape

The below diagram references the Microsoft landscape and the SSO components currently provided. The current identities in these applications, including directory services, should be synchronised / migrated to the IGA and PAM tools.

High-Level Enterprise Productivity Solution Architecture Landscape

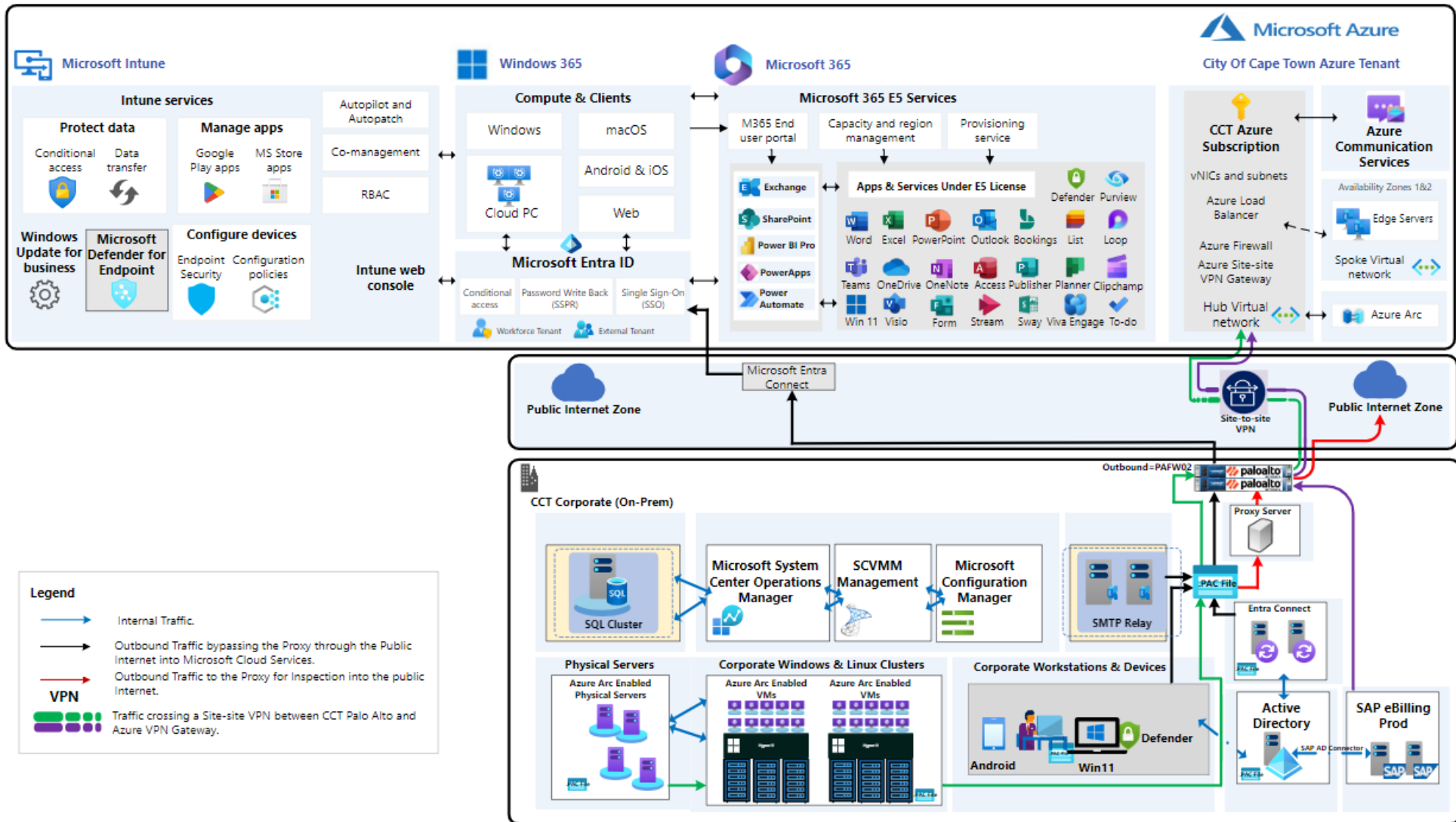


Figure 2: High-level productivity solution architecture landscape

6.9.4. Third Party Systems

All listed third party systems in the table below will be handled through the Ad-hoc Professional Services and Bidders need to allocate experienced Professional Service Resources for this tender. The integration activities associated with third party systems must also be considered together with the implementation requirements outlined in the subsequent section to ensure full alignment with the ILM solution architecture and delivery approach.

Table 2: Third party systems

No.	Application System	Purpose	OS Version	Database Version
1	ACL	Audit Tool	Win 2019	N/A
2	TeamMate	Audit document management	Win 2012	SQL 2014
3	BarnOwl (Risk)	Risk management	Win 2019	SQL 2019
4	BarnOwl (IA)	Audit document management	Win 2019	SQL 2022
5	BarnOwl (Water)	Water Demand Management Regulatory	-	-
6	BesAccess/Blick	Time and attendance	Win 2019	SQL 2019
7	BesAccess/Safr	Time and attendance	Win 2019	Mongo
8	Juta	Legal library	Win 2019	N/A
9	Revenue Reporting	Analytics/reporting	Win2019	SQL 2019
10	Library Management System - Symphony App	Library management system (books etc)	Oracle 11	Oracle DB
11	Library Management System - Enterprise App (OPAC)	Library management system (books etc)	PostGress	PostGress
12	Library Management System - web services	Library management system (books etc)	-	N/A
13	Helios (iForce) (TMT)	Traffic Contravention	-	-
14	dTims	Asset management	Win 2019	SQL 2019
15	RAMS (dTims) Viewer	Asset management viewer	Win 2019	SQL 2019
16	Samras	Cash Receipting (new)	Win 2019	SQL 2019
17	Sage	Accounting system	Win 2019	SQL 2019
18	GRM - Valuations		Win 2019	SQL 2019
19	Axim (PACS)	Xray - digitised management system	Win 2019	PostGress
20	Wayleave Management System	Wayleave management system	Win 2019	SQL 2019
21	Civil Designer License Server	License Server for civil designer	Win 2012	N/A
22	DataSource - MetroFile	MVR	Win 2019	SQL 2022
23	LIMS - LabWare	Water Quality etc	Win 2019	SQL 2022
24	ICARUS - New Pos	Cash Receipting (new)	-	-
25	Forensics Case Management System	Forensic Services	-	-

6.9.4.1. Project Initiation Phase:

The Project Initiation phase begins with a Business or IS&T need, problem or opportunity being identified and the requirements thereof specified. These requirements are then communicated to IS&T, who evaluate the request for viability. The output documentation of this phase is a Project Initiation Document.

6.9.4.2. Project Planning Phase:

The Project Planning phase follows on from the approval of the project (Project Initiation phase) and involves the scoping of the project in more detail and the planning of the project tasks and activities needed to execute the project. This includes reaffirming the identified benefits and potential risks the project could encounter. The output documentation of this phase is a Project Charter document, Benefits Realisation Register, Risk Register and a Project Plan.

6.9.4.3. Project Execution Phase:

The Project Execution phase follows on from the Project Planning phase and involves the execution of the project plan and the management processes undertaken to monitor and control the deliverables of the project. Once all of the deliverables have been produced and the customer has accepted the final product, the project is ready for closure. The output documentation of this phase is Agenda's and Minutes of Meetings, Project Progress Reports, Project Change Requests, Risk Register, Issues Register and Benefits Realisation Register.

6.9.4.4. Project Closure Phase:

The Project Closure phase follows on from the Project Execution phase and involves the monitoring and support of the implemented solution in Production for an agreed period of time and the subsequent closure of the project. The output documentation of this phase is the Project Closure Report.

6.9.4.5. Post Project Review Phase:

The Post Project Review phase is an optional phase which follows on from the Project Closure phase at an agreed period of lapsed time and involves the measurement of the benefits, as determined in the benefits realisation register. The output documentation of this phase is the Updated Benefits Realisation Register.

6.9.5. IS&T Project Management Methodology & Deliverables

Figure 3 below depicts the project management methodology that is being utilised for the CAR programme. The ILM project will seek to adopt the best practices from this methodology.

6.9.5.1. Project gates to be passed

The project life cycle and associated activities are governed by formal stage-gate reviews. Progression to the next phase is contingent on successful completion and approval at each of the following gates, as illustrated in the diagram that follows:

The CCT has adopted a standard project lifecycle, illustrated in Figure 4 **Error! Reference source not found.** below. The 'Stage Gates' control the process and serve as quality checkpoints, outlining the activities that must be completed or reviewed, as well as the key decisions that must be made before a project proposal can progress to the next stage of development. Each gate is designed to gather vital information, strategic, technical, financial, operational, and commercial, to manage the risks associated with project planning and execution. By navigating this programme and its individual projects through the gate review process, high-quality deliverables can be achieved. These gate reviews will be integrated into the project plan.

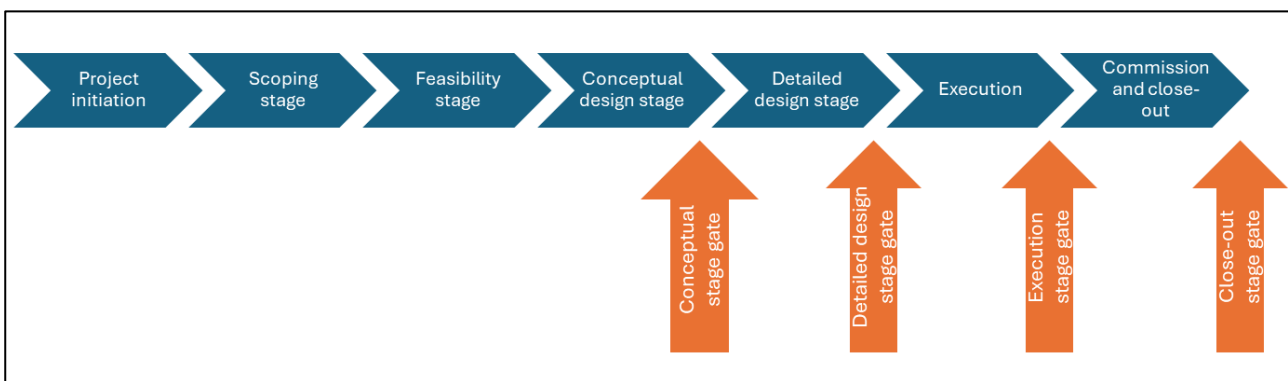


Figure 4: Project lifecycle

6.9.5.2. Service provider obligations in relation to stage gates

The Service Provider shall support and enable the City's formal stage-gate governance process and shall be accountable for the preparation, quality, and submission of all information required to support gate decisions. Compliance with stage-gate requirements is a material obligation under this Agreement. Without limiting the generality of the above, the Service Provider shall:

1. Support City Governance Processes

Provide ongoing technical, financial, operational, and commercial support to authorised City officials for the purposes of stage-gate reviews, including attendance at gate review meetings, governance forums, and decision-making workshops when reasonably required by the City.

2. Prepare and Submit Mandatory Gate Deliverables

Prepare, compile, and submit all documentation, analyses, models, and supporting evidence required to satisfy the entry and exit criteria of each stage gate, in accordance with:

- the City's approved project lifecycle,
- applicable City policies and procedures, and
- any additional gate-specific requirements issued by the City.

Such deliverables shall, where applicable, include scope definitions, implementation plans, cost estimates, financial models, risk registers, procurement strategies, technical designs, statutory compliance assessments, and governance submissions.

3. Provide Verifiable Evidence of Gate Readiness

Provide clear, structured, and auditable evidence demonstrating that all stage-gate requirements and deliverables applicable to a given gate have been met.

This evidence shall explicitly:

- demonstrate readiness to progress to the next project phase,
- identify all key assumptions, dependencies, constraints, and exclusions, and

- disclose all material risks and residual issues requiring City acceptance or mitigation.

4. Ensure Quality, Accuracy, and Compliance

Ensure that all stage-gate submissions are complete, accurate, internally consistent, and compliant with applicable legislation, regulations, and City policies. The Service Provider shall implement appropriate quality assurance and peer review processes prior to submission to the City.

5. Address Gate Conditions and Review Comments

Respond to all findings, comments, conditions, or requests for clarification arising from stage-gate reviews within timeframes agreed with the City. The Service Provider shall update and resubmit deliverables as required to enable closure of gate conditions.

6. Integrate Stage Gates into Project Planning

Incorporate all stage-gate milestones, deliverables, dependencies, and approval points into the project plan and programme. The Service Provider shall not proceed with activities associated with a subsequent project phase unless formally approved by the City.

7. Limitations on Authority

The Service Provider shall have no authority to approve or waive stage-gate requirements or to authorise progression between project phases. All gate approvals remain the sole prerogative of the City. Failure by the Service Provider to adequately support a stage-gate review, or to provide complete and compliant deliverables for a stage gate, may result in delays to gate approval and shall not constitute grounds for extension of time or additional compensation unless explicitly agreed in writing by the City.

6.10. REQUIREMENTS FOR MAINTENANCE AND SUPPORT SERVICES ON THE ILM SOLUTION

The Supplier must provide comprehensive maintenance and support services for the proposed IGA, PAM, and Identity Proofing tools to ensure the ongoing stability, security, and performance of the ILM solution.

Maintenance services must include regular software updates, patches, upgrades, bug fixes, security remediation in line with vendor recommendations and CCT security standards including additional integration when any of the aforementioned are applied.

Support services must provide responsive incident and problem resolution, escalation to specialised support resources where required, and adherence to agreed performance metrics.

All maintenance and support services must be delivered in accordance with the detailed requirements set out in the ILM Specifications and must support uninterrupted business operations and regulatory compliance throughout the contract period.

The Supplier shall maintain the role-permission matrix in line with approved changes to organisational structures, applications and policies, ensuring it remains accurate and auditable throughout the contract term.

The Supplier shall maintain and support the ILM capability, including:

- Execution and monitoring of automated provisioning/de-provisioning workflows;
- Operation and continuous enforcement of Segregation of Duty (SoD) policies, resolution of SoD conflicts, and periodic SoD reporting;
- Monitoring and remediation of connectors/integrations; and
- Support for periodic access reviews/certifications and audit requests.

Refer to **Tables A3, B3 and C3 of Schedules A, B and C in section (C.4) Price Schedule.**

6.11. REQUIREMENTS FOR PROFESSIONAL SERVICES FOR THE ILM SOLUTION

The Supplier must provide ad-hoc professional services to support the IGA, SSO, PAM, and Identity Proofing components of the ILM solution.

These services will be delivered on a time-and-materials or task-order basis using the labour rates specified in the pricing schedule.

The Supplier must ensure that all personnel deployed for ad-hoc work are suitably qualified,

experienced in large-scale ILM environments, and capable of performing specialised configuration, enhancement, troubleshooting, or integration activities as required by the City of Cape Town (CCT).

All new resources proposed by the Supplier must be submitted to the CCT Contract Manager for approval prior to commencing any work.

All ad-hoc services must align with the approved ILM architecture, security standards, operational procedures, and the maintenance and support requirements set out in the ILM Specifications.

The following table contains the minimum qualification and experience for the professional services resources:

System	Resource	Minimum requirements
1. IGA	1.1. Project Manager	7 years' Project Management experience PMP certification or equivalent
	1.2. Technical Architect/Lead	8 years' experience solution architecture, 5 years specific to IGA
	1.3. Technical Consultant	3 years' experience on at least one IGA tool implementation
	1.4. Senior Consultant	8 years' experience
	1.5. Consultant	5 years' experience
2. PAM	2.1. Project Manager	7 years' Project Management experience, PMP certification or equivalent
	2.2. Technical Architect/Lead	8 years solution architecture, 5 years specific to PAM solutions
	2.3. Technical Consultant	3 years' experience on at least one PAM tool implementation
	2.4. Senior Consultant	8 years' experience
	2.5. Consultant	5 years' experience
3. Identity Proofing	3.1. Project Manager	7 years' Project Management experience PMP certification or equivalent
	3.2. Technical Architect/Lead	8 years' solution architecture, 5 years specific to IDV/KYC
	3.3. Technical Consultant	3 years' experience on at least one IDV/KYC project
	3.4. Senior Consultant	8 years' experience
	3.5. Consultant	5 years' experience

Refer to **Tables A5, B5 and C5 of Schedules A, B and C in section (C.4) Price Schedule.**

6.12. REQUIREMENTS FOR MANAGED SERVICES

The Supplier must deliver managed services that ensure the continuous, stable and secure operation of the City’s ILM environment, including the IGA, SSO configurations, PAM and Identity Proofing components. These services must cover routine operational activities, advanced application-level support, and specialised technical functions across the infrastructure and database layers. Managed services must provide proactive monitoring, timely incident resolution, performance optimisation, configuration management, and reliable execution of all maintenance tasks in line with the City’s operational and security standards.

The Supplier is required to supply appropriately skilled resources across the three defined resource types: administrative, application-technical, and infrastructure-specialist. The Supplier must ensure that all work aligns with ILM architecture, governance processes, and service-level requirements. The Supplier must also maintain accurate documentation, support audits, implement best-practice controls, and collaborate closely with the City’s teams to uphold service continuity, regulatory compliance, and high-quality operational outcomes across the contract period.

Managed Services Resource Type	Definition or Description
Managed Service Resource Type 1	<p>Type 1 resources provide routine, low-complexity, operational and administrative support services that do not require deep system architecture, database, or infrastructure expertise. These tasks are repeatable, standardised, and procedural in nature:</p> <p>A. User Administration</p> <ul style="list-style-type: none"> • Creation, modification, and deactivation of user accounts • Password resets • Role assignment and permission updates • Access reviews • Enforcement of predefined security policies <p>B. Application Administration (Routine)</p> <ul style="list-style-type: none"> • Maintenance of system parameters • Updating lookup values and reference data • Managing user profiles • Configuring standard workflows (non-technical adjustments) • Standard configuration updates that do not alter core system architecture <p>C. Reporting</p> <ul style="list-style-type: none"> • Generation of standard reports • Generation of compliance reports • Scheduled report execution • Exporting system data to approved formats • Assistance with standard dashboards • Minor formatting adjustments to existing reports

Managed Services Resource Type	Definition or Description
Managed Service Resource Type 2	<p>Type 2 resources provide intermediate to advanced application and system-level support. They address configuration changes, monitoring, and controlled enhancements within the application layer. These tasks require technical expertise but do not extend to core infrastructure or database architecture management:</p> <p>A. System and Application Monitoring</p> <ul style="list-style-type: none"> • Monitoring application health • Log analysis • Performance threshold monitoring • Proactive identification of system degradation • Incident trend analysis <p>B. Configuration Management</p> <ul style="list-style-type: none"> • Complex workflow configuration • Business rule configuration • System parameter adjustments impacting multiple modules • Interface configuration updates • Integration endpoint configuration <p>C. Low-Code / No-Code Development</p> <ul style="list-style-type: none"> • Development of forms using platform tools • Configuration-based feature enhancements • Creating or modifying dashboards • Report development (custom reports) • Minor automation using built-in tools <p>D. Release and Patch Coordination</p> <ul style="list-style-type: none"> • Coordinating patch deployments • Pre-release validation • Configuration validation post-deployment • Support during upgrade activities <p>E. Incident Resolution (Application Layer)</p> <ul style="list-style-type: none"> • Diagnosing application-level defects • Reproducing application issues • Supporting root cause analysis in collaboration with vendor

Managed Services Resource Type	Definition or Description
Managed Service Resource Type 3	<p>Type 3 resources provide specialised technical services at the database, operating system, and infrastructure level. These tasks are high-risk, high-impact, and require specialist technical expertise.</p> <p>A. Database Administration (DBA)</p> <ul style="list-style-type: none"> • Database installation and configuration • Database upgrades and patching • Backup and restore management • Database replication management • Index management • Storage optimisation <p>B. Database Performance Tuning</p> <ul style="list-style-type: none"> • Query optimisation • Execution plan analysis • Performance bottleneck identification • Memory and resource allocation tuning • Transaction log optimisation <p>C. Infrastructure Management</p> <ul style="list-style-type: none"> • Server provisioning • Virtual machine management • Storage allocation • High availability configuration • Disaster recovery environment management <p>D. Operating System Administration</p> <ul style="list-style-type: none"> • OS patching and upgrades • Security hardening • Access control configuration • Service management • Performance monitoring at OS level <p>E. Security and Compliance (Technical Layer)</p> <ul style="list-style-type: none"> • Implementation of security controls • Encryption configuration • Certificate management • System-level audit logging

6.13. REQUIREMENTS FOR CHANGE MANAGEMENT

The Supplier must provide comprehensive change management support to ensure that the ILM solution is adopted effectively across the CCT. The Supplier’s responsibilities must extend beyond the technical implementation and include a structured, people-centred change management approach that supports behavioural, process, and organisational change.

At a minimum, the Supplier must:

6.13.1. Deliver a Change-Management Strategy and Plan

The Supplier must develop and execute a formal change-management plan aligned to CCT's organisational context and in conjunction with the City's Change Manager, outlining stakeholder engagement, readiness assessments, communication cycles, and adoption milestones.

The Supplier must develop and submit a comprehensive Change Management Plan no later than three (3) months after contract commencement.

This ensures that the Supplier actively supports both the technology transition and the people-side of ILM, enabling sustainable adoption across the organisation.

6.13.2. Support Stakeholder Engagement and Adoption

The Supplier must identify key stakeholder groups with the City's Change Manager, assess their readiness and impact, and provide targeted interventions to ensure understanding, buy-in, and behavioural adoption of ILM processes.

6.13.3. Communication and Awareness Material

The CCT will be responsible for the designing, branding, and printing of all communication and awareness material, including artwork, posters, and other physical materials for placement at City premises such as City offices, libraries, and community centres.

The Supplier must support the CCT by providing input content and messaging (e.g., FAQs, process overviews, change notices) to ensure accuracy and alignment with the implemented solutions.

All change-management support activities must be included in the implementation cost of the solutions as listed in **Schedules A2, B2 and C2 in Section C.4 Price Schedule**.

6.13.4. Integrate Change Management with Training

The Supplier must ensure that the training programme reinforces change-management outcomes by addressing behavioural shifts, new responsibilities, and process expectations for different user groups.

6.13.5. Monitor and Report on Adoption

The Supplier must define and track adoption metrics, gather feedback, and propose corrective actions where uptake is slow or where additional interventions are required.

7. DATA HANDLING

The CCT will provide the Supplier with the necessary master data for internal and external identities required for ILM configuration, role mapping, and provisioning processes.

The Supplier is responsible for analysing and validating this data to ensure accuracy, consistency, and readiness for integration into the ILM solution.

The Supplier must identify data gaps, duplications, inconsistencies, and incorrect reporting structures, and propose corrective actions for CCT review.

All data-handling activities must align with agreed data-governance standards and must not alter authoritative source records without CCT approval.

The Supplier must also support the establishment of ongoing data-quality routines to maintain clean and reliable HR master data throughout the project lifecycle.

8. PURCHASE ORDERS

The City retains the privilege to liaise with the OEM/Distributor to validate the precision of the prices presented to the Supplier and to ensure the correct implementation of the mark-up %, as stipulated in the pricing schedule for each respective Purchase Order.

The process that will be followed:

- a) The City representative shall initiate communication with the Supplier to request a quotation.
- b) The Supplier shall furnish the requested quotation within the timeframe to be agreed at contracting stage. Each submitted quote must include the most recent and officially endorsed OEM price list applicable to the goods or equipment being procured.
- c) Correspond to the exact model, part number, or configuration specified in the tender or technical schedule.
- d) OEM/Distributor prices, properly addressed to the Supplier.

- e) Subsequently, the City representative will evaluate the provided quotation from the Supplier. This evaluation involves verifying whether the prices sourced from the OEM/Distributor have been accurately reflected in the Supplier's quote for each requested item.
- f) Upon completion of the above steps and identification of no discrepancies, the City representative will proceed to confirm the accurate application of the Mark-up % as outlined in the Pricing Schedule.
- g) The Municipality reserves the right to request clarification, verification, or additional supporting documentation should discrepancies arise. Failure to provide an updated OEM price list may result in the rejection of the quotation, Purchase Order, or any related claim for payment.

The Contract Price List as per C.4 Price Schedule provided at tender stage shall:

- a) Form an integral part of the contract and shall be used as the baseline for all items required to be procured.
- b) Be applicable to all items, components, materials, equipment or services described in the tender specifications.
- c) Be used as the reference against which all subsequent pricing claims will be evaluated for compliance, accuracy, and value for money.
- d) The Supplier may not alter, revise, or substitute any items contained in the tender-stage price list without prior written approval from the City of Cape Town.

8.1. Redundant Items

Identification of Redundant Items

The Supplier shall notify the Municipality in writing if any item listed in the contract becomes *redundant, obsolete, discontinued, or superseded* by an updated OEM model or specification.

Verification and Approval

Upon receiving notification, the City of Cape Town reserves the right to:

- a) request supporting documentation from the Supplier, including OEM discontinuation notices, product lifecycle statements, or catalogue updates;
- b) verify redundancy through independent market research or OEM confirmation; and
- c) determine whether the item will be formally removed, replaced, or substituted.

The Supplier may not unilaterally replace a redundant item with a newer model, alternative item, or updated configuration without *prior written approval* from the City of Cape Town.

Replacement Item Requirements. Where a substitute item is proposed, it must:

- a) meet or exceed the original technical specifications;
- b) be accompanied by an updated OEM-verified price list;
- c) offer comparable or improved functionality; and
- d) be provided at a price that reflects value-for-money.

8.2. New Items

New items may only be proposed or requested under the following circumstances:

- a) **OEM Product Updates or New Releases:** Where the OEM introduces new models, upgraded products, or revised specifications that enhance performance or functionality.
- b) **Discontinuation of Existing Items:** When existing contracted items are phased out, discontinued, or replaced by the OEM, necessitating a suitable alternative to maintain continuity.
- c) **Technological Advancements:** Where new items provide improved efficiency, enhanced capabilities, or updated features in line with technological progress.
- d) **Compliance Requirements:** When regulatory, safety, or industry standards change, requiring updated items to maintain lawful or safe operations.
- e) **Improved Value for Money:** Where new items offer superior lifecycle cost benefits, reduced maintenance requirements, or improved durability, consistent with value-for-money principles outlined in procurement guidelines.
- f) **Supply Chain Limitations:** Where older items experience stock shortages, long lead times, or manufacturing constraints that hinder service continuity.

Submission Requirements for New Items

- a) Any new item proposed for inclusion must be accompanied by:
- b) the official OEM datasheet or specification;
- c) the current OEM-verified price list;
- d) warranty, support, and lifecycle information;
- e) a technical comparison to the original item(s).

Evaluation and Approval

New items will be assessed by the CCT based on technical compliance, compatibility, total cost of ownership, and overall value for money in accordance with applicable procurement policies and guidelines. Inclusion of new items is subject to written approval and formal approval by the City of Cape Town.

Prohibition on Unauthorised Substitution

No new item may be supplied, quoted, or invoiced under this contract without prior written approval from the City of Cape Town. Any unauthorised substitution may result in rejection of the item, non-payment, or other contractual remedies.

9. TRADE NAMES OR PROPRIETARY PRODUCTS

Bid specifications may not make any reference to any particular trademark, name, patent, design, type, specific origin or producer, unless there is no other sufficiently precise or intelligible way of describing the characteristics of the work, in which case such reference must be accompanied by the words “or equivalent”.

10. EMPLOYMENT OF SECURITY PERSONNEL

Not Applicable

11. FORMS FOR CONTRACT ADMINISTRATION

The Supplier shall, if applicable, complete, sign and submit with each invoice, the following:

- a) Monthly Project Labour Report

11.1 Monthly Project Labour Report

Not applicable

C.6 SPECIAL CONDITIONS OF CONTRACT

The following Special Conditions of Contract, referring to the National Treasury – Conditions of Contract (revised July 2010), are applicable to this agreement.

1. Definitions

Insert new clause 1.1A with the following:

- 1.1A “Commencement Date” means the date the Supplier confirms receipt from the Purchaser of 1 (one) complete, signed copy of the Contract, the *Schedule of Deviations* (if any).
- 1.1B “Conditions of Contract” means the general conditions of contract and special conditions of contract including all other contract data incorporated by reference.

Delete Clause 1.15 and substitute with the following

- 1.15 The word ‘Goods’ is to be replaced everywhere it occurs in the GCC with the phrase ‘Goods and / or Services’ which means all of the equipment, machinery, materials, services, products, consumables, etc. that the Supplier is required to deliver to the Purchaser under the agreement. This definition shall also be applicable, as the context requires, anywhere where the words “supplies” and “services” occurs in the GCC.

Delete Clause 1.19 and substitute with the following

- 1.19 The word ‘Order’ is to be replaced everywhere it occurs in the GCC with the words ‘Purchase Order’ which means the official purchase order authorised and released on the Purchaser’s SAP System.

Delete Clause 1.21 and substitute with the following:

- 1.21 ‘Purchaser’ means the City of Cape Town. The address of the Purchaser is 12 Hertzog Boulevard, Cape Town, 8001 (chosen domicilium citandi et executandi).

Delete Clause 1.24 and substitute with the following:

- 1.24 ‘Services’ means the provision of the specific services set out and on the basis as provided for in this Agreement, by Supplier to Purchaser.

Add the following after Clause 1.25:

- 1.26 “Supplier” means the provider of Goods and / or Services with whom the Contract is concluded also referred to as “contractor” in the GCC.
- 1.27 "Intellectual Property" means any and all intellectual property rights of any nature anywhere in the world whether registered, registerable or otherwise, including patents, trademarks, registered designs and domain names, applications for any of the foregoing, trade or business names, copyright and rights in the nature of copyright, design rights, rights in databases, know-how, trade secrets and any other intellectual property rights which subsist in computer software, computer programs, websites, documents, information, techniques, business methods, drawings, logos, instruction manuals, lists and procedures and particulars of customers, marketing methods and procedures and advertising literature, including the "look and feel" of any websites
- 1.28 “Working Day” means Monday to Friday excluding weekends and Public Holidays (in the Republic of South Africa).
- 1.29 “Deliverables” means those things to be delivered by Supplier to Purchaser under this Agreement and to be delivered in tangible form described as being the Supplier’s responsibility in the Specifications and specifically indicated to be such a Deliverable.
- 1.30 “System” means the solution, including all components, modules, interfaces, and functionalities, as defined in the scope of solution set out in the Tender.

3. General Obligations

Delete Clause 3.2 in its entirety and replace with the following clauses.

- 3.2 The Parties will be liable to each other arising out of or in connection with any breach of the obligations detailed or implied in this contract, subject to clause 28.
- 3.3 If the Supplier is a joint venture, all parties in a joint venture or consortium shall be jointly and severally liable to the Purchaser in terms of the Contract and shall carry individually the minimum levels of insurance stated in the Contract, if any.
- 3.4 The Parties shall comply with all laws, regulations and bylaws of local or other authorities having jurisdiction regarding the Delivery of the Goods and/or Services and give all notices and pay all charges required by such authorities.
- 3.4.1 The Parties agree that this Contract shall also be subject to the CCT's Supply Chain Management Policy ("SCM Policy") that was applicable on the date the bid was advertised as amended from time to time. If the Purchaser adopts a new SCM Policy which contemplates that any clause therein would apply to the Contract emanating from this tender, such clause shall also be applicable to the Contract. Please refer to this document contained on the CCT's website.
- 3.4.2 Abuse of the supply chain management system is not permitted and may result in termination of the Contract, restriction of the Supplier, and/or the exercise by the CCT of any other remedies available to it as described in the SCM Policy or in law.
- 3.5 The Supplier shall:
- 3.5.1 Arrange for the documents listed below to be provided to the Purchaser prior to the issuing of the Purchase Order by the Purchaser and no later than the periods as set out in the Contract:
- a) Proof of Insurance (Refer to Clause 11) or Insurance Broker's Warrantee,
 - b) Letter of good standing from the Compensation Commissioner, or a licensed compensation insurer (Refer to Clause 11),
 - c) Initial delivery programme, and
 - d) Other requirements as detailed in the Contract.
- 3.5.2 Only when notified of the acceptance of the bid on the Date of Commencement of Contract, the Supplier shall commence with and carry out the Delivery of the Goods and/or Services in accordance with the Contract, to the satisfaction, of the Purchaser.
- 3.5.3 Provide all of the necessary materials, labour, plant and equipment required for the delivery of the Goods and/or Services including any temporary services that may be required.
- 3.5.4 Insure his workmen and employees against death or injury arising out of the delivery of the Goods.
- 3.5.5 Be continuously represented during the Delivery of the Goods and/or Services by a competent representative duly authorised to execute instructions.
- 3.5.6 In the event of a loss resulting in a claim against the insurance policies stated in clause 11, pay the first amount (excess) as required by the insurance policy.
- 3.5.7 Comply with all written instructions from the Purchaser subject to clause 18.
- 3.5.8 Complete and Deliver the goods within the period stated in clause 10, or any extensions thereof in terms of clause 21.
- 3.5.9 Make good at his own expense, all incomplete and defective Goods during the warranty period.
- 3.5.10 Pay to the Purchaser any penalty for delay as due on demand by the Purchaser. The Supplier hereby consents to such amounts being deducted from any payment due to the Supplier.
- 3.5.11 Comply with the provisions of the OHAS Act & all relevant regulations.

- 3.5.12 Comply with all laws relating to wages and conditions generally governing the employment of labour in the Cape Town area and any applicable Bargaining Council agreements.
- 3.5.13 Deliver the Goods in accordance with the Contract and with all reasonable care, diligence and skill in accordance with generally accepted professional techniques and standards.
- 3.6 The Purchaser shall:
 - 3.6.1 Issue Purchaser Orders for the Goods and/or Services required under this Contract. No liability for payment will ensue for arising out of the Delivery of the Goods and/or Services, unless a Purchase Order has been issued to the Supplier.
 - 3.6.2 Make payment to the Supplier for the Goods and/or Services as set out herein.
 - 3.6.3 Take possession of the Goods and /or Services upon Delivery by the Supplier.
 - 3.6.4 Regularly inspect the Goods to establish that it is being delivered in compliance with the Contract.
 - 3.6.5 Give any instructions and/or explanations and/or variations to the Supplier including any relevant advice to assist the Supplier to understand the Contract.
 - 3.6.6 Grant or refuse any extension of time requested by the Supplier of the period stated in clause 10.
 - 3.6.7 Inspect the Goods and/or Services to determine if, in the opinion of the Purchaser, it has been delivered in compliance with the Contract, alternatively in such a state that it can be properly used for the purpose for which it was intended.
 - 3.6.8 Brief the Supplier and issue all documents, information, etc. in accordance with the contract.

5. Use of contract documents and information; inspection, copyright, confidentiality, etc.

Add at the end of clause 5.1:

- 5.1 Save that the Supplier will be entitled to disclose the contract to any affiliate or subsidiary of Supplier for its internal business purposes and to any external professional advisor as may be needed in order to obtain any professional advice or input pertaining to finance, legal or any regulatory matters arising out of or in connection with the Contract.

Add the following after clause 5.4:

- 5.5 Copyright of all documents prepared by the Supplier in accordance with the relevant provisions of the Copyright Act (Act 98 of 1978) relating to the Contract shall be vested in the Purchaser. Where copyright is vested in the Supplier, the Purchaser shall be entitled to use the documents or copy them only for the purposes for which they are intended in regard to the agreement and need not obtain the Supplier's permission to copy it for such use. Where copyright is vested in the Purchaser, the Supplier shall not be liable in any way for the use of any of the information other than as originally intended in terms of the agreement and the Purchaser hereby indemnifies the Supplier against any claim which may be made against it by any person / entity, arising from the use of such documentation for other purposes.

The ownership of data and factual information collected by the Supplier and paid for by the Purchaser shall, after payment, vest with the Purchaser.

- 5.6 **Publicity and publication**
The Supplier shall not release public or media statements or publish material related to the services or agreement within two (2) years of Delivery of the Goods, without the written approval of the Purchaser, which approval shall not be unreasonably withheld.
- 5.7 **Confidentiality**
Both Parties shall keep all information obtained by them in the context of the agreement, confidential and shall not divulge it without the written approval of the other Party.

5.8 Intellectual Property

- 5.8.1 The Supplier acknowledges that it shall not acquire any right, title or interest in or to the Intellectual Property of the Purchaser.
- 5.8.2 The Supplier hereby assigns to the Purchaser, all Intellectual Property created, developed or otherwise brought into existence by it for the purposes of the agreement, unless the Parties expressly agree otherwise in writing.
- 5.8.3 The Supplier shall, and warrants that it shall:
 - 5.8.3.1 Not be entitled to use the Purchaser's Intellectual Property for any purpose other than as contemplated in the agreement;
 - 5.8.3.2 not modify, add to, change or alter the Purchaser's Intellectual Property, or any information or data related thereto, nor may the Supplier produce any product as a result of, including and/or arising from any such information, data and Intellectual Property, and in the event that it does produce any such product, the product shall be, and be deemed in law to be, owned by the Purchaser;
 - 5.8.3.3 Not apply for or obtain registration of any domain name, trademark or design which is similar to any Intellectual Property of the Purchaser;
 - 5.8.3.4 Comply with all reasonable directions or instructions given to it by the Purchaser in relation to the form and manner of use of the CCT Intellectual Property, including without limitation, any brand guidelines which the Purchaser may provide to the Supplier from time to time;
 - 5.8.3.5 Ensure that its employees, directors, members and contractors comply strictly with the provisions of this Clause 5.8.3.4 above unless the Purchaser expressly agrees to the contrary, in writing and only after obtaining due internal authority for such agreement.
- 5.8.4 The Supplier represents and warrants to the Purchaser that, in providing Goods and/or Services for the duration of the agreement it will not infringe or make unauthorised use of the Intellectual Property rights of any third party and hereby indemnifies the Purchaser from any claims, liability, loss, damages, costs, and expenses arising from the infringement or unauthorised use by the Supplier of any third party's Intellectual Property rights.
- 5.8.5 Upon expiry of the contract period and in the event that the Contract is terminated, ended or is declared void, any and all of the Purchaser's Intellectual Property, and any and all information and data related thereto, shall be immediately handed over to the Purchaser by the Supplier and no copies thereof shall be retained by the Supplier unless the Purchaser expressly and in writing, after obtaining due internal authority, agrees otherwise.

Add the following after clause 5.8:

5.9 **Protection of Personal Information Act of 2013**

By submitting a tender to the Purchaser, (and by concluding any ensuing related agreement with the City of Cape Town, if applicable), the Tenderer thereby acknowledges and unconditionally agrees:

- 5.9.1 that the tenderer has been informed of the purpose of the collection and processing of its personal information as defined in the Protection of Personal Information Act of 2013 ("POPIA"), which, for the avoidance of doubt is for, and in relation to, the tender process and the negotiation, conclusion, performance and enforcement of the ensuing agreement, if applicable, as well as for the City of Cape Town's reporting purposes;
- 5.9.2 to the collection and processing of the tenderer's personal information by the City of Cape Town and agrees to make available to the City of Cape Town, all information reasonably required by the City of Cape Town for the above purposes;
- 5.9.3 that the personal information the City of Cape Town collects from the tenderer or about the tenderer may be further processed for other activities and/or purposes which are lawful, reasonable, relevant and not excessive in relation to the purposes set out above, for which it was originally collected;

- 5.9.4 that, the tenderer indemnifies the City of Cape Town and its officials, employees, and directors and undertakes to keep the City of Cape Town and its officials, employees, and directors indemnified in respect of any claim, loss, demands, liability, costs and expenses of whatsoever nature which may be made against the City of Cape Town (including the costs incurred in defending or contesting any such claim) in relation to the tenderer or the tenderer's employees', representatives' and/or sub-Suppliers' non-compliance with POPIA and/or the City of Cape Town's failure to obtain the tenderer's consent or to notify the tenderer of the reason for the processing of the tenderer's personal information;
- 5.9.5 to the disclosure of the tenderer's personal information by the City of Cape Town to any third party, where the City of Cape Town has a legal or contractual obligation to disclose such personal information to the third party (or a legitimate interest exists therein);
- 5.9.6 that, under POPIA, the tenderer may request to access, confirm, request the correction, destruction, or deletion of, or request a description of, personal information held by the City of Cape Town in relation to you, subject to applicable law; and that under POPIA, subject to applicable law, the tenderer also has the right to be notified of a personal information breach and the right to object to, or restrict, the City of Cape Town's processing of its personal information.
- 5.10 **PERFORMANCE MONITORING**
- 5.10.1 As required by section 116(2)(b) of the Local Government: Municipal Financial Management Act 56 of 2003, the CCT shall monitor the performance of the Supplier on at least a monthly basis, and the Supplier agrees to provide the CCT with its full cooperation in this regard.

7. Performance Security

Delete clause 7.1 to 7.4 and replace with the following:

Not Applicable. Tenderers must disregard the **Pro Forma Performance Security/ Guarantee** and are not required to furnish same.

8. Inspections, tests and analyses

Delete Clause 8.2 and substitute with the following:

- 8.2 If it is a bid condition that Goods and/or Services to be produced or services to be rendered should at any stage during production or execution or on completion be subject to inspection, the premises of the bidder or Supplier shall be open, at all reasonable hours, for inspection by a representative of the Purchaser or an organisation acting on behalf of the Purchaser.

10. Delivery and documents

Delete clauses 10.1 and 10.2 and replace with the following:

- 10.1 Delivery of the goods shall be made by the Supplier in accordance with the terms specified in the contract. The time for Delivery of the goods shall be the date as stated on the Purchase Order. In the case of agreements for Delivery of goods in terms of framework or panel agreements, Purchase Orders for the supply and delivery of goods may be raised up until the expiry of a framework or panel agreement, provided that the goods can be delivered within 30 (thirty) days of expiry of the framework or panel agreement. In this context, the "goods" does not include services and carries its ordinary meaning. All Purchase Orders other than for the supply and Delivery of goods (i.e. supply of services, professional services or constructions works), must be completed prior to the expiry of the contract period.
- 10.2 The Purchaser shall determine, in its sole discretion, whether the Goods and/or Services have been delivered in compliance with the Contract, alternatively in such a state that it can be properly used for the purpose for which it was intended. Goods, including Deliverables will be tested and signed off in accordance with pre-agreed acceptance criteria/specifications and testing procedures and within agreed timeframes. The only basis for rejection will be if the Good and Deliverables do not substantially comply with the agreed criteria and/or specifications. When the Purchaser determines that the Goods

and/or Services have been satisfactorily delivered, the Purchaser must issue an appropriate certification, or written approval, to that effect. Invoicing may only occur, and must be dated, on or after the date of such written acceptance of the Goods.

11. Insurance

Add the following after clause 11.1:

- 11.2 Without limiting the obligations of the Supplier in terms of this Contract, the Supplier shall effect and maintain the following additional insurances:
- 11.2.1 Public liability insurances, in the name of the Supplier, covering the Supplier and the Purchaser against liability for the death of or injury to any person, or loss of or damage to any property, arising out of or in the course of this Contract, in an amount not less than **R20 million** for any single claim;
- 11.2.2 Motor Vehicle Liability Insurance, in respect of all vehicles owned and / or leased by the Supplier, and used for the purposes of delivering the Services to the CCT under this Agreement, comprising, at a minimum, "Balance of Third Party" risks including Passenger Liability Indemnity;
- 11.2.3 Registration / insurance in terms of the Compensation for Occupational Injuries and Disease Act, Act 130 of 1993. This can either take the form of a certified copy of a valid Letter of Good Standing issued by the Compensation Commissioner, or proof of insurance with a licenced compensation insurer, from either the Supplier's broker or the insurance company itself (see the Pro Forma Insurance Broker's Warranty).
- 11.2.4 In the case of Contracts for delivery of professional services, Professional indemnity insurance providing cover in an amount of not less than **R5 million** in respect of each and every claim during the contract period.
- 11.2.5 In the event of under insurance or the insurer's repudiation of any claim for whatever reason, the Purchaser will retain its right of recourse against the Supplier.
- 11.3 The Supplier shall be obliged to furnish the Purchaser with proof of such insurance as the Purchaser may require from time to time for the duration of this Contract. Evidence that the insurances have been effected in terms of this clause, shall be either in the form of an insurance broker's warranty worded precisely as per the pro forma version contained in the Pro forma Insurance Broker's Warranty or copies of certificates of insurance evidencing the insurance policies.

15. Warranty

Add to Clause 15.2:

- 15.2 Not applicable.

16. Payment

Delete Clause 16.1 in its entirety and replace with the following:

- 16.1 Payment of invoices will be made:
- 16.1.1 Within 30 (thirty) days of receiving the relevant invoice or statement from the Supplier, unless otherwise prescribed for certain categories of expenditure or specific contractual requirements in accordance with any other applicable policies of the Purchaser.
- 16.1.2 Notwithstanding anything contained above, the Purchaser shall not be liable for payment of any invoice that pre-dates the date of delivery of any Goods and/or Services.

Delete Clause 16.2 in its entirety and replace with the following:

- 16.2 The Supplier shall furnish the purchaser's Accounts Payable Department with an original tax invoice, clearly showing the amount due in respect of each and every claim for payment.

Add the following after clause 16.4

- 16.5 Notwithstanding any amount stated on the Purchase Order, the Supplier shall only be entitled to payment for Goods and/or Services actually delivered in terms of the Specification and Drawings, or any variations thereof made in accordance with clause 18. Any contingency sum included shall be for the sole use, and at the discretion, of the Purchaser.
- 16.6 The Purchaser will only make advanced payments to the Supplier in strict compliance with the terms and conditions as contained in the Pro forma Advanced Payment Guarantee and only once the authenticity of such guarantee has been verified by the Purchaser's Treasury Department.
- 16.7 Project Milestones, Deliverables and Payment Schedule
- 16.7.1 The detailed project milestones, deliverables, and associated payment schedule shall be finalized and mutually agreed upon during the contracting stage. No milestone or payment obligation shall become binding until formally documented and signed by both parties. Acceptance criteria/specifications and testing procedures within agreed timeframes will be pre-agreed at contracting stage.

17. Prices

Add the following after clause 17.1

- 17.2 If as a result of an award of a contract beyond the original tender validity period, the contract execution will be completed beyond a period of twelve (12) months from the expiry of the original tender validity period, then the contract may be subject to contract price adjustment for that period beyond such twelve (12) months. An appropriate contract price adjustment formula will be determined by the Purchaser delegated authority if such was not included in the bid documents.
- 17.3 If as a result of any extension of time granted, the contract execution will be completed beyond a period of twelve (12) months from the expiry of the original tender validity period, then contract price adjustment may apply to that period beyond such twelve (12) months. An appropriate contract price adjustment formula will be determined by the Director: Supply Chain Management if such was not included in the bid documents.
- 17.4 The prices for the goods and/or Services delivered and services performed shall be subject to contract price adjustment in terms of Schedule F.1 Contract Price Adjustment.

18. Contract Amendments

Delete the heading of clause 18 and replace with the following:

18. Contract Amendments and Variations

Add the following to clause 18.1:

Variations means changes to the Goods and/or Services, extension of the contract period or increases in the value of the Contract as a result of written instructions issued by the Purchaser to the Supplier. Such changes are subject to prior approval by the Purchaser's delegated authority. Should the Supplier deliver any Goods not described in a written instruction from the Purchaser, the Purchaser's liability for payment shall no arise until such time as the change has been duly approved and such approval communicated to the Purchaser.

20. Subcontracts

Add the following after clause 20.1:

- 20.2 The Supplier shall be liable for the acts, defaults and negligence of any subcontractor, his agents or employees as fully as if they were the acts, defaults or negligence of the Supplier.
- 20.3 Any appointment of a subcontractor shall not amount to a contract between the Purchaser and the subcontractor, or a responsibility or liability on the part of the Purchaser to the subcontractor and shall not relieve the Supplier from any liability or obligation under the Contract.

21. Delays in the supplier's performance

Delete Clause 21.2 in its entirety and replace with the following:

21.2 If at any time during the performance of obligations contained in the Contract the Supplier or its subcontractors should encounter conditions beyond their reasonable control which impede the timely delivery of the Goods and/or Services, the Supplier shall notify the Purchaser in writing, within 7 (seven) days of first having become aware of these conditions, of the facts of the delay, its cause(s) and its probable duration. As soon as practicable after receipt of the Supplier's notice, the Purchaser shall evaluate the situation, and may at his discretion extend the time for Delivery.

Where additional time is granted, the Purchaser shall also determine whether or not the Supplier is entitled to payment for additional costs in respect thereof. The principle to be applied in this regard is that where the Purchaser or any of its agents are responsible for the delay, reasonable costs shall be paid. In respect of delays that were beyond the reasonable control of both the Supplier and the Purchaser, additional time only (no costs) will be granted.

The Purchaser shall notify the Supplier in writing of his decision(s) in the above regard.

21.3 No provision in this Contract shall be deemed to prohibit the obtaining of Goods and/or Services from a national department, provincial department, or a local authority.

22. Penalties

Delete clause 22.1 and replace with the following:

22.1 Subject to GCC Clause 25, if the Supplier fails to deliver any or all of the Goods and/or Services within the period(s) specified in the Contract, the Purchaser shall, without prejudice to its other remedies under the Contract, deduct from amounts payable, as a penalty, a sum as stated herein for each day of the delay until actual Delivery or performance.

22.2 The Purchaser shall, without prejudice to its other remedies under the contract, deduct from amounts payable, financial penalties as contained on the Preference Schedule for breaches of the conditions upon which preference points were awarded.

22.3 A Performance Penalty will be incurred at a rate of 1% of the Grand Total for the following project phases over the Contract period:

- Analysis,
- Detail Design,
- Customization,
- Supply, Installation,
- Maintenance,
- Support and
- Change Management/ Training.

The maximum penalty per calendar month is limited to 10% of the Grand Total for Analysis Detail Design, Configuration / Customisation, Supply, Installation, Maintenance, Support and Change Management/ Training over the contract period.

#	Performance Element	Performance Measure	Performance Metrics	Penalty
1	Implementation & Delivery Delays	If the vendor fails to meet the agreed project milestones (e.g., Analysis, details design, customization / configuration completion, system testing, go-live).	Timelines in respect of the various phases of the project implementation.	1% of the total contract value of phase per week of delay, capped at 10% of the total contract value of phase. Beyond 20 weeks of delay, the City reserves the right to terminate the contract.

#	Performance Element	Performance Measure	Performance Metrics	Penalty
2	System Availability & Uptime (Any disruption that has a material impact on the ability to deliver a service will be regarded as downtime.)	The system is classified as mission-critical and must meet agreed Service Level Agreements (SLAs). Minimum uptime: 99.95% per month.	Minimum uptime: 99.95% per month.	For every 0.1% drop below SLA, the vendor pays 2% of the monthly support and maintenance fee. Sustained non-compliance for 3 consecutive months gives the City the right to terminate.
3	Incident Response & Resolution (Refer to Section 6.10 Requirements for Maintenance and Support)	Supplier must provide 24x7 support with defined response and resolution times.	Severity/Priority 1 = less than 30 minutes response, less than 4 hours resolution. Severity/Priority 2 = less than 3 hours response, less than 8 hours resolution. Severity/Priority 3 = less than 4 hours response, less than 2 Business days resolution.	Failure to meet resolution SLA within the allocated time period: -Severity 1 incident: R5,000 penalty per hour delay or part thereof. -Severity 2 incident: R3,000 per hour delay or part thereof. -Severity 3 incident: R2,000 per day of delay or part thereof.

Severity/Priority Level	SLA Response Time	SLA Resolution Time	Definition	Example
Severity/Priority 1: (Critical / Major Outage)	Non-automated response less than 30 minutes acknowledging issue.	Resolution time of 4 hours	Complete service outage or severe degradation affecting all users. No workaround available.	System is completely down or inaccessible. PAM vault unavailable, preventing all privileged access; IGA portal down during an access certification campaign. Critical integrations Security breach or data compromise impacting operational continuity
Severity/Priority 2: (Medium)	Response less than 2 hours	Resolution time of 8 hours	Major functionality impaired, impacting a large group of users. Workaround may exist but is not sustainable.	Identity Proofing service failing to verify contractors; SSO integration broken for a critical application.
Severity/Priority 3: (Low)	Response less than 4 hours	Resolution time of 2 business days	Partial loss of functionality with limited impact. Workaround available.	Password rotation delayed for a subset of service accounts; reporting dashboard not generating compliance reports.

23. Termination for default

Delete the heading of clause 23 and replace with the following:

23. Termination

Add the following to the end of clause 23.1:

If the Supplier fails to remedy the breach in terms of such notice.

Add the following after clause 23.7:

23.8 In addition to the grounds for termination due to default by the Supplier, the Contract may also be terminated:

23.8.1 Upon the death of the Supplier who was a Sole Proprietor, or a sole member of a Close Corporation, in which case the contract will terminate forthwith.

23.8.2 If the Parties, by mutual agreement, terminate the Contract.

23.8.3 If a material irregularity vitiates the procurement process leading to the conclusion of the Contract, rendering the procurement process and the conclusion of the resulting Contract unfair, inequitable, non-transparent, uncompetitive or not cost-effective the Contract may be terminated by the Purchaser (upon conclusion of applicable processes by the City Manager as described in the Purchaser's SCM Policy).

23.8.4 Reputational risk or harm to the Purchaser

The Purchaser, without prejudice to any other remedy for breach of contract, by written notice of default sent to the Supplier, may terminate the contract if the implementation of the contract may result in reputational risk or harm to the Purchaser as a result of (inter alia):

- a) reports of poor governance and/or unethical behaviour;
- b) association with known notorious individuals and family of notorious individuals;
- c) poor performance issues, known to the Purchaser
- d) negative social media reports;
- e) adverse assurance (e.g. due diligence) report outcomes; or
- f) circumstances where the relevant vendor has employed, or is directed by, anyone who was previously employed in the service of the state (as defined in clause 1.53), where the person is or was negatively implicated in any SCM irregularity.

By or in relation to the Supplier, the Contract may be terminated by the Purchaser after providing notice to the Supplier.

23.9 If the Contract is terminated in terms of clause 23.8, all obligations that were due and enforceable prior to the date of the termination, must be performed by the relevant Party.

26. Termination for insolvency

Delete clause 26.1 and replace with the following:

- 26.1 In the event of the Supplier becoming bankrupt or otherwise insolvent the Purchaser may elect to:
- 26.1.1 At any time, terminate the Contract by giving written notice to the Supplier; or
- 26.1.2 Accept a Supplier's proposal (via the liquidator) to render delivery utilising the appropriate contractual mechanisms or takes steps to ensure its rights are protected and any negative impact on service delivery is mitigated.
- 26.2 In the event of the Purchaser electing to cancel the Contract in accordance with clause 26.1.1 above, the Purchaser shall make payment of all verified and signed off invoices. In the event of there being any dispute in respect of any outstanding invoices such dispute shall be dealt with in accordance with the dispute resolution mechanism in the Contract.

27. Settlement of Disputes

Amend clause 27.1 as follows:

- 27.1 If any dispute or difference of any kind whatsoever, with the exception of termination in terms of clause 23 arises between the Purchaser and the Supplier in connection with or arising out of the Contract, the Parties shall make every effort to resolve such dispute or difference amicably, by mutual consultation.

Delete Clause 27.2 in its entirety and replace with the following:

- 27.2 Should the Parties fail to resolve any dispute by way of mutual consultation, either party shall be entitled to refer the matter for mediation before an independent and impartial person appointed by the City Manager in accordance with Regulation 50(1) of the Local Government: Municipal Finance Management Act, 56 of 2003 – Municipal Supply Chain Management Regulations (Notice 868 of 2005). Such referral shall be done by either party giving written notice to the other of its intention to commence with mediation. No mediation may be commenced unless such notice is given to the other party.

Irrespective whether the mediation resolves the dispute, the Parties shall bear their own costs concerning the mediation and share the costs of the mediator and related costs equally.

The mediator shall agree the procedures, representation and dates for the mediation process with the Parties. The mediator may meet the Parties together or individually to enable a settlement.

Where the Parties reach settlement of the dispute or any part thereof, the mediator shall record such agreement and on signing thereof by the Parties the agreement shall be final and binding.

Save for reference to any portion of any settlement or decision which has been agreed to be final and binding on the Parties, no reference shall be made by or on behalf of either party in any subsequent court proceedings, to any outcome of an amicable settlement by mutual consultation, or the fact that any particular evidence was given, or to any submission, statement or admission made in the course of amicable settlement by mutual consultation or mediation.

28. Limitation of Liability

Delete clause 28.1 (a) and (b) and replace with the following:

- (a) notwithstanding any provision to the contrary contained in this contract, neither the supplier nor any of its officers, directors, employees, agents contractors, consultants or other representatives shall be liable to the purchaser, whether in contract, tort, or otherwise, for any indirect, incidental, special or consequential loss or damage of any kind, including without limitation the loss of use, loss of production, or loss of profits or interest costs, loss of goodwill, lost or damaged data or software, costs of substitute products/services and/or loss of business or business opportunities (whether foreseeable or unforeseeable), provided that this exclusion shall not apply to any obligation of the supplier to pay penalties and/or damages to the purchaser;

- (b) the aggregate liability of the Supplier to the Purchaser, whether under the Contract, in tort or

otherwise, shall not exceed the sums insured in terms of clause 11 in respect of insurable events, or where no such amounts are stated, to an amount equal to twice the Contract price, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.

Add the following after clause 28.1:

28.2 Without detracting from, and in addition to, any of the other indemnities in this Contract, the Supplier shall be solely liable for and hereby indemnifies and holds harmless the Purchaser against all claims, charges, damages, costs, actions, liability, demands and/or proceedings and expense in connection with:

- a) personal injury or loss of life to any individual;
- b) loss of or damage to property;

arising from, out of, or in connection with the performance by the Supplier in terms of this Contract, save to the extent caused by the gross negligence or wilful misconduct of the Purchaser.

28.3 The Supplier and/or its employees, agents, concessionaires, suppliers, sub-contractors or customers shall not have any claim of any nature against the purchaser for any loss, damage, injury or death which any of them may directly or indirectly suffer, whether or not such loss, damages, injury or death is caused through negligence of the Purchaser or its agents or employees.

28.4 Notwithstanding anything to the contrary contained in this Contract, under no circumstances whatsoever, including as a result of its negligent (including grossly negligent) acts or omissions or those of its servants, agents or contractors or other persons for whom in law it may be liable, shall any party or its servants (in whose favour this constitutes a *stipulatio alteri*) be liable for any indirect, extrinsic, special, penal, punitive, exemplary or consequential loss or damage of any kind whatsoever, whether or not the loss was actually foreseen or reasonably foreseeable), sustained by the other party, its directors and/or servants, including but not limited to any loss of profits, loss of operation time, corruption or loss of information and/or loss of contracts.

28.5 Each party agrees to waive all claims against the other insofar as the aggregate of compensation which might otherwise be payable exceeds the aforesaid maximum amounts payable.

31. Notices

Delete clauses 31.1 and 31.2 and replace with the following:

31.1 Any notice, request, consent, approvals or other communications made between the Parties pursuant to the Contract shall be in writing and forwarded to the addresses specified in the Contract and may be given as set out hereunder and shall be deemed to have been received when:

- a) hand delivered – on the day delivery of delivery or the next Working Day,
- b) sent by registered mail – five (5) Working Days after mailing,
- c) sent by email or telefax – one (1) Working Day after transmission.

32. Taxes and Duties

Delete the final sentence of 32.3 and replace with the following:

. In this regard, it is the responsibility of the Tenderer to submit evidence in the form of a valid Tax Compliance Status PIN issued by SARS to the CCT at the Supplier Management Unit located within the Supplier Management / Registration Office, 2nd Floor (Concourse Level), Civic Centre, 12 Hertzog Boulevard, Cape Town (Tel 021 400 9242/3/4/5), or included with this tender.

Add the following after clause 32.3:

32.4 The VAT registration number of the CCT is 4500193497.

ADDITIONAL CONDITIONS OF CONTRACT

Add the following Clause after Clause 34:

35. Reporting Obligations

35.1 The Supplier shall complete, sign and submit with each delivery note, all the documents as required in the Specifications including Monthly Project Labour Reports (Annexure B). Any failure in this regard may result in a delay in the processing of payments.

36. Adherence to IS&T Standards

36.1 The Supplier is referred to Annexure G. The Supplier shall ensure that all services, systems, and solutions delivered under this Contract comply with the IS&T Standards and CCT Data Access Specifications respectively.

C.7 GENERAL CONDITIONS OF CONTRACT

(National Treasury - General Conditions of Contract (revised July 2010))

TABLE OF CLAUSES

1. Definitions
2. Application
3. General
4. Standards
5. Use of contract documents and information; inspection
6. Patent rights
7. Performance security
8. Inspections, tests and analysis
9. Packing
10. Delivery and documents
11. Insurance
12. Transportation
13. Incidental services
14. Spare parts
15. Warranty
16. Payment
17. Prices
18. Contract amendments
19. Assignment
20. Subcontracts
21. Delays in the supplier's performance
22. Penalties
23. Termination for default
24. Dumping and countervailing duties
25. Force majeure
26. Termination for insolvency
27. Settlement of disputes
28. Limitation of liability
29. Governing language
30. Applicable law
31. Notices
32. Taxes and duties
33. National Industrial Participation Programme (NIPP)
34. Prohibition of restrictive practices

1. Definitions

1. The following terms shall be interpreted as indicated:

- 1.1 'Closing time' means the date and hour specified in the bidding documents for the receipt of bids.
- 1.2 'Contract' means the written agreement entered into between the purchaser and the supplier, as recorded in the contract form signed by the Parties, including all attachments and appendices thereto and all documents incorporated by reference therein.
- 1.3 'Contract price' means the price payable to the supplier under the contract for the full and proper performance of his or her 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 in which an enterprise abroad is subsidised 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 recognised new product results that is substantially different in basic characteristics or in purpose or utility from its components.
- 1.7 'Day' means calendar day.
- 1.8 'Delivery' means delivery in compliance with the conditions of the contract or order.
- 1.9 'Delivery ex stock' means immediate delivery directly from stock actually on hand.
- 1.10 'Delivery into consignee's store or to his site' means delivered and unloaded in the specified store or depot or on the specified site in compliance with the conditions of the contract or order, the supplier bearing all risks and charges involved until the supplies are so delivered and a valid receipt is obtained.
- 1.11 'Dumping' occurs when a private enterprise abroad markets its goods on its own initiative in the RSA at lower prices than that of the country of origin, and which action has the potential to harm the local industries in the RSA.
- 1.12 'Force majeure' means an event beyond the control of the supplier, not involving the supplier's fault or negligence, and not foreseeable. Such events may include, but are not restricted to, acts of the purchaser in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.
- 1.13 'Fraudulent practice' means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of any bidder, and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial, non-competitive levels and to deprive the bidder of the benefits of free and open competition.
- 1.14 'GCC' means the General Conditions of Contract.
- 1.15 'Goods' means all of the equipment, machinery, and/or other materials that the supplier is required to supply to the purchaser under the contract.
- 1.16 'Imported content' means that portion of the bidding price represented by the cost of components, parts or materials which have been or are still to be imported (whether by the supplier or his subcontractors) and which costs are inclusive of the costs abroad, plus freight and other direct importation costs such as landing costs, dock dues, import duty, sales duty or other similar tax or duty at the South African place of entry as well as transportation and handling charges to the factory in the Republic where the supplies covered by the bid will be manufactured.
- 1.17 'Local content' means that portion of the bidding price which is not included in the imported content, provided that local manufacture does take place.
- 1.18 'Manufacture' means the production of products in a factory using labour, materials, components and machinery, and includes other, related value-adding activities.
- 1.19 'Order' means an official written order issued for the supply of goods or works or the rendering of a service.
- 1.20 'Project site', where applicable, means the place indicated in bidding documents.
- 1.21 'Purchaser' means the organisation purchasing the goods.
- 1.22 'Republic' means the Republic of South Africa.
- 1.23 'SCC' means the Special Conditions of Contract.

1.24 'Services' means those functional services ancillary to the supply of the goods, such as transportation and any other incidental services, such as installation, commissioning, provision of technical assistance, training, catering, gardening, security, maintenance, and other such obligations of the supplier covered under the contract.

1.25 'Written' or 'in writing' means handwritten in ink or any form of electronic or mechanical writing.

2. Application

2.1 These general conditions are applicable to all bids, contracts and orders, including bids for functional and professional services, sales, hiring, letting and the granting or acquiring of rights, but excluding immovable property, unless otherwise indicated in the bidding documents.

2.2 Where applicable, special conditions of contract are also laid down to cover specific supplies, services or works.

2.3 Where such special conditions of contract are in conflict with these general conditions, the special conditions shall apply.

3. General

3.1 Unless otherwise indicated in the bidding documents, the purchaser shall not be liable for any expense incurred in the preparation and submission of a bid. Where applicable, a non-refundable fee for documents may be charged.

3.2 With certain exceptions, invitations to bid are only published in the Government Tender Bulletin. The Government Tender Bulletin may be obtained directly from the Government Printer, Private Bag X85, Pretoria 0001, or accessed electronically from www.treasury.gov.za.

4. Standards

4.1 The goods supplied shall conform to the standards mentioned in the bidding documents and specifications.

5. Use of contract documents and information; inspection.

5.1 The supplier shall not, without the purchaser's prior written consent, disclose the contract, or any provision thereof, or any specification, plan, drawing, pattern, sample, or information furnished by or on behalf of the purchaser in connection therewith, to any person other than a person employed by the supplier in the performance of the contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for the 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 the use of the goods or any part thereof by the purchaser.

7. Performance Security

- 7.1 Within 30 (thirty) 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 the 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.
- 1.3 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 30 (thirty) days following the date of completion of the supplier's performance obligations under the contract, including any warranty obligations, unless otherwise specified in the SCC.

8. Inspections, tests and analyses

- 8.1 All pre-bidding testing will be for the account of the bidder.
- 8.2 If it is a bid condition that supplies to be produced or services to be rendered should at any stage during production or execution or on completion be subject to inspection, the premises of the bidder or contractor shall be open, at all reasonable hours, for inspection by a representative of the Department or an organisation acting on behalf of the Department.
- 8.3 If there are no inspection requirements indicated in the bidding documents and no mention of such is made in the contract, but during the contract period it is decided that inspections shall be carried out, the purchaser shall itself make the necessary arrangements, including payment arrangements with the testing authority concerned.
- 8.4 If the inspections, tests and analyses referred to in clauses 8.2 and 8.3 show the supplies to be in accordance with the contract requirements, the cost of the inspections, tests and analyses shall be defrayed by the purchaser.
- 8.5 Where the supplies or services referred to in clauses 8.2 and 8.3 do not comply with the contract requirements, irrespective of whether such supplies or services are accepted or not, the cost in connection with these inspections, tests or analyses shall be defrayed by the supplier.
- 8.6 Supplies and services which are referred to in clauses 8.2 and 8.3 and which do not comply with the contract requirements may be rejected.
- 8.7 Any contract supplies may on or after delivery be inspected, tested or analysed and may be rejected if found not to comply with the requirements of the contract. Such rejected supplies shall be held at the cost and risk of the supplier, who shall, when called upon, remove them immediately at his own cost and forthwith substitute them with supplies which do comply with the requirements of the contract. Failing such removal, the rejected supplies shall be returned at the suppliers cost and risk. Should the supplier fail to provide the substitute supplies forthwith, the purchaser may, without giving the supplier further opportunity to substitute the rejected supplies, purchase such supplies as may be necessary at the expense of the supplier.
- 8.8 The provisions of clauses 8.4 to 8.7 shall not prejudice the right of the purchaser to cancel the contract on account of a breach of the conditions thereof, or to act in terms of Clause 23 of the GCC.

9. Packing

- 9.1 The supplier shall provide such packing of the goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in the contract. The packing shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packing, case size and weights shall take into consideration, where appropriate, the remoteness of the goods' final destination and the absence of heavy handling facilities at all points in transit.

9.2 The packing, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the contract, including additional requirements, if any, specified in the SCC, and in any subsequent instructions ordered by the purchaser.

10. Delivery and documents

10.1 Delivery of the goods shall be made by the supplier in accordance with the terms specified in the contract. The details of shipping and/or other documents to be furnished by the supplier are specified in the SCC.

10.2 Documents to be submitted by the supplier are specified in the SCC.

11. Insurance

11.1 The goods supplied under the contract shall be fully insured, in a freely convertible currency, against loss or damage incidental to manufacture or acquisition, transportation, storage and delivery in the manner specified in the SCC.

12. Transportation

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

13. Incidental Services

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

- (a) performance or supervision of on-site assembly, and/or commissioning of the supplied goods;
- (b) furnishing of tools required for the assembly and/or maintenance of the supplied goods;
- (c) furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied goods;
- (d) performance or supervision or maintenance and/or repair of the supplied goods, for a period of time agreed by the Parties, provided that this service shall not relieve the supplier of any warranty obligations under this contract; and
- (e) training of the purchaser's personnel, at the supplier's plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the supplied goods.

13.2 Prices charged by the supplier for incidental services, if not included in the contract price for the goods, shall be agreed upon in advance by the Parties and shall not exceed the prevailing rates charged to other Parties by the supplier for similar services.

14. Spare parts

14.1 As specified in the SCC, the supplier may be required to provide any or all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the supplier:

- (a) such spare parts as the purchaser may elect to purchase from the supplier, provided that this election shall not relieve the supplier of any warranty obligations under the contract; and
- (b) in the event of termination of production of the spare parts:
 - (i) Advance notification to the purchaser of the pending termination, in sufficient time to permit the purchaser to procure needed requirements; and
 - (ii) following such termination, furnishing at no cost to the purchaser, the blueprints, drawings, and specifications of the spare parts, if requested.

15. Warranty

15.1 The supplier warrants that the goods supplied under the contract are new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials unless provided otherwise in the contract. The supplier further warrants that all goods supplied under this contract shall have no defect arising from design, materials, or workmanship (except when the design and/or material is required by the purchaser's specifications), or from any act or omission of the

supplier, that may develop under normal use of the supplied goods in the conditions prevailing in the country of final destination.

15.2 This warranty shall remain valid for 12 (twelve) 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 18 (eighteen) months after the date of shipment from the port or place of loading in the source country, whichever period concludes earlier, unless specified otherwise in the SCC.

15.3 The purchaser shall notify the supplier promptly, in writing, of any claims arising under this warranty.

15.4 Upon receipt of such notice, the supplier shall, within the period specified in the SCC and with all reasonable speed, repair or replace the defective goods or parts thereof, without costs to the purchaser.

15.5 If the supplier, having been notified, fails to remedy the defect(s) within the period specified in the SCC, the purchaser may proceed to take such remedial action as may be necessary, at the supplier's risk and expense and without prejudice to any other rights which the purchaser may have against the supplier under the contract.

16. Payment

16.1 The method and conditions of payment to be made to the supplier under this contract shall be specified in the SCC.

16.2 The supplier shall furnish the purchaser with an invoice accompanied by a copy of the delivery note and upon fulfilment of any other obligations stipulated in the contract.

16.3 Payments shall be made promptly by the purchaser, but in no case later than 30 (thirty) days after submission of an invoice or claim by the supplier.

16.4 Payment will be made in Rand unless otherwise stipulated in the SCC.

17. Prices

17.1 Prices charged by the supplier for goods delivered and services performed under the contract shall not vary from the prices tendered by the supplier in his bid, with the exception of any price adjustments authorized in the SCC or in the purchaser's request for bid validity extension, as the case may be.

18. Contract Amendments

18.1 No variation in or modification of the terms of the contract shall be made except by written amendment signed by the Parties concerned.

19. Assignment

19.1 The supplier shall not assign, in whole or in part, its obligations to perform under the contract, except with the purchaser's prior written consent.

20. Subcontracts

20.1 The supplier shall notify the purchaser in writing of all subcontracts awarded under this contract 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 the 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 or her discretion extend the supplier's time for performance, with or without the imposition of penalties, in which case the extension shall be ratified by the Parties by amendment of contract.

- 21.3 No provision in a contract shall be deemed to prohibit the obtaining of supplies or services from a national department, provincial department, or a local authority.
- 21.4 The right is reserved to procure, outside of the contract, small quantities of supplies; or to have minor essential services executed if an emergency arises, or the supplier's point of supply is not situated at or near the place where the supplies are required, or the supplier's services are not readily available.
- 21.5 Except as provided under GCC Clause 25, a delay by the supplier in the performance of its delivery obligations shall render the supplier liable to the imposition of penalties, pursuant to GCC Clause 22, unless an extension of time is agreed upon pursuant to GCC Clause 21.2 without the application of penalties.
- 21.6 Upon any delay beyond the delivery period in the case of a supplies contract, the purchaser shall, without cancelling the contract, be entitled to purchase supplies of a similar quality and up to the same quantity in substitution of the goods not supplied in conformity with the contract and to return any goods delivered later at the supplier's expense and risk, or to cancel the contract and buy such goods as may be required to complete the contract and, without prejudice to his other rights, be entitled to claim damages from the supplier.

22. Penalties

- 22.1 Subject to GCC Clause 25, if the supplier fails to deliver any or all of the goods or to perform the services within the period(s) specified in the contract, the purchaser shall, without prejudice to its other remedies under the contract, deduct from the contract price, as a penalty, a sum calculated on the delivered price of the delayed goods or unperformed services, using the current prime interest rate, calculated for each day of the delay until actual delivery or performance. The purchaser may also consider termination of the contract pursuant to GCC Clause 23.

23. Termination for default

- 23.1 The purchaser, without prejudice to any other remedy for breach of contract, by written notice of default sent to the supplier, may terminate this contract in whole or in part:
- (a) if the supplier fails to deliver any or all of the goods within the period(s) specified in the contract, or within any extension thereof granted by the purchaser pursuant to GCC Clause 21.2;
 - (b) if the supplier fails to perform any other obligation(s) under the contract; or
 - (c) if the supplier, in the judgment of the purchaser, has engaged in corrupt or fraudulent practices in competing for or in executing the contract.
- 23.2 In the event the purchaser terminates the contract in whole or in part, the purchaser may procure, upon such terms and in such manner as it deems appropriate, goods, works or services similar to those undelivered, and the supplier shall be liable to the purchaser for any excess costs for such similar goods, works or services. However, the supplier shall continue performance of the contract to the extent not terminated.
- 23.3 Where the purchaser terminates the contract in whole or in part, the purchaser may decide to impose a restriction penalty on the supplier by prohibiting such supplier from doing business with the public sector for a period not exceeding 10 years.
- 23.4 If a purchaser intends imposing a restriction on a supplier or any person associated with the supplier, the supplier will be allowed a time period of not more than 14 (fourteen) days to provide reasons why the envisaged restriction should not be imposed. Should the supplier fail to respond within the stipulated 14 (fourteen) days the purchaser may regard the intended penalty as not objected against and may impose it on the supplier.
- 23.5 Any restriction imposed on any person by the Accounting Officer/Authority will, at the discretion of the Accounting Officer/Authority, also be applicable to any other enterprise or any partner, manager,

director or other person who wholly or partly exercises or exercised or may exercise control over the enterprise of the first-mentioned person, and with which enterprise or person the first-mentioned person is or was, in the opinion of the Accounting Officer/Authority, actively associated.

23.6 If a restriction is imposed, the purchaser must, within 5 (five) 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, Act 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 of not less than five years and not more than 10 years. The National Treasury is empowered to determine the period of restriction, and each case will be dealt with on its own merits. According to section 32 of the Act the Register must be open to the public. The Register can be perused on the National Treasury website.

24. Anti-dumping and countervailing duties and rights

24.1 When, after the date of bid, provisional payments are required, or 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 subsidised import, the State is not liable for any amount so required or imposed, or for the amount of any such increase. When, after the said date, such a provisional payment is no longer required or any such anti-dumping or countervailing right is abolished, or where the amount of such provisional payment or any such right is reduced, any such favourable difference shall, on demand, be paid forthwith by the contractor to the State, or the State may deduct such amounts from moneys (if any) which may otherwise be due to the contractor in regard to supplies or services which he or she 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 or her.

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 notify the purchaser promptly, 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 such dispute or difference amicably, by mutual consultation.

27.2 If, after 30 (thirty) days, the Parties have failed to resolve their dispute or difference by such mutual consultation, then either the purchaser or the supplier may give notice to the other party of his

intention to commence with mediation. No mediation in respect of this matter may be commenced unless such notice is given to the other party.

27.3 Should it not be possible to settle a dispute by means of mediation, it may be settled in a South African court of law.

27.4 Mediation proceedings shall be conducted in accordance with the rules of procedure specified in the SCC.

27.5 Notwithstanding any reference to mediation and/or court proceedings herein,

- (a) the Parties shall continue to perform their respective obligations under the contract unless they otherwise agree; and
- (b) the purchaser shall pay the supplier any monies due to the supplier.

28. Limitation of Liability

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

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 in the SCC.

31. Notices

31.1 Every written acceptance of a bid shall be posted to the supplier concerned by registered or certified mail, and any other notice to him shall be posted by ordinary mail, to the address furnished in his bid or to the address notified later by him in writing; and such posting shall be deemed to be proper service of such notice.

31.2 The time mentioned in the contract documents for performing any act after such aforesaid notice has been given, shall be reckoned from the date of posting of such notice.

32. Taxes and Duties

32.1 A foreign supplier shall be entirely responsible for all taxes, stamp duties, licence fees, and other such levies imposed outside the purchaser's country.

32.2 A local supplier shall be entirely responsible for all taxes, duties, licence fees, etc., incurred until delivery of the contracted goods to the purchaser.

32.3 No contract shall be concluded with any bidder whose tax matters are not in order. Prior to the award of a bid the Department must be in possession of a tax clearance certificate submitted by the bidder. This certificate must be an original issued by the South African Revenue Services.

33. National Industrial Participation (NIP) Programme

33.1 The NIP Programme administered by the Department of Trade and Industry shall be applicable to all contracts that are subject to the NIP obligation.

34 Prohibition of Restrictive practices

- 34.1 In terms of section 4 (1) (b) (iii) of the Competition Act, Act 89 of 1998, as amended, an agreement between or concerted practice by firms, or a decision by an association of firms, is prohibited if it is between Parties in a horizontal relationship and if a bidder(s) is/are or a contractor(s) was/were involved in collusive bidding (or bid rigging).
- 34.2 If a bidder(s) or contractor(s), based on reasonable grounds or evidence obtained by the purchaser, has/have engaged in the restrictive practice referred to above, the purchaser may refer the matter to the Competition Commission for investigation and possible imposition of administrative penalties as contemplated in the Competition Act, Act 89 of 1998.
- 34.3 If a bidder(s) or contractor(s) has/have been found guilty by the Competition Commission of the restrictive practice referred to above, the purchaser may, in addition and without prejudice to any other remedy provided for, invalidate the bid(s) for such item(s) offered, and/or terminate the contract in whole or part, and/or restrict the bidder(s) or contractor(s) from conducting business with the public sector for a period not exceeding 10 (ten) years and/or claim damages from the bidder(s) or contractor(s) concerned.

C.8 ANNEXURES

Annexure A – Pro Forma Insurance Broker’s Warranty



Letterhead of supplier’s Insurance Broker

Date _____

CCT
City Manager
Civic Centre
12 Hertzog Boulevard
Cape Town
8000

Dear Sir

TENDER NO.: 252S/2025/26

TENDER DESCRIPTION: SUPPLY, INSTALLATION, MAINTENANCE AND SUPPORT OF IDENTITY LIFECYCLE MANAGEMENT SOLUTION FOR THE CITY OF CAPE TOWN

NAME OF SUPPLIER: _____

I, the undersigned, do hereby confirm and warrant that all the insurances required in terms of the abovementioned contract have been issued and/or in the case of blanket/umbrella policies, have been endorsed to reflect the interests of the CCT with regard to the abovementioned contract, and that all the insurances and endorsements, etc., are all in accordance with the requirements of the contract.

I furthermore confirm that all premiums in the above regard have been paid.

Yours faithfully

Signed: _____

For: _____ (Supplier’s Insurance Broker)

Annexure B – Monthly Project Labour Report

ANNEX 1

CITY OF CAPE TOWN MONTHLY PROJECT LABOUR REPORT



Instructions for completing and submitting forms

General

- 1 The Monthly Project Labour Reports must be completed in full, using typed, proper case characters; alternatively, should a computer not be available, handwritten in black ink.
- 2 Incomplete / incorrect / illegible forms will not be accepted.
- 3 Any conditions relating to targeted labour stipulated in the Contract (in the case of contracted out services or works) shall apply to the completion and submission of these forms.
- 4 This document is available in Microsoft Excel format upon request from the City's EPWP office, tel 021 400 9406, email EPWPLR@capetown.gov.za.

Project Details

- 5 If a field is not applicable insert the letters: NA
- 6 Only the Project Number supplied by the Corporate EPWP Office must be inserted. The Project Number can be obtained from the Coordinator or Project Manager or from the e-mail address in point 4 above.
- 7 On completion of the contract or works project the anticipated end date must be updated to reflect the actual end date.

Beneficiary Details and Work Information

- 8 Care must be taken to ensure that beneficiary details correspond accurately with the beneficiary's ID document.

- 9 A new beneficiary is one in respect of which a new employment contract is signed in the current month. A certified ID copy must accompany this labour report on submission.
- 10 Was the beneficiary sourced from the City's job seeker database?
- 11 The contract end date as stated in the beneficiary's employment contract.
- 12 Where a beneficiary has not worked in a particular month, the beneficiary's name shall not be reflected on this form at all for the month in question.
- 13 Training will be recorded separately from normal working days and together shall not exceed the maximum of 23 days per month
- 14 Workers earning more than the maximum daily rate (currently R450 excluding any benefits) shall not be reflected on this form at all.
- 15 Signed hardcopy forms must be scanned and submitted to the City's project manager in electronic (.pdf) format, together with the completed form in Microsoft Excel format.
- 16 Scanned copies of all applicable supporting documentation must be submitted along with each monthly project labour report. Copies of employment contracts and ID documents are only required in respect of new beneficiaries.
- 17 If a computer is not available hardcopy forms and supporting documentation will be accepted.

PROJECT DETAILS

Numbers in cells below e.g (6) refer to the relevant instruction above for completing and submitting forms

CONTRACT OR WORKS PROJECT NAME: (6)		EPWP SUPPLIED PROJECT NUMBER: (6)																		
DIRECTORATE:		DEPARTMENT:																		
CONTRACTOR OR VENDOR NAME:		CONTRACTOR OR VENDOR E-MAIL ADDRESS:																		
CONTRACTOR OR VENDOR CONTACT PERSON:		CONTRACTOR OR VENDOR TEL. NUMBER:																		
PROJECT LABOUR REPORT CURRENT MONTH (mark with "X")		CELL WORK																		
JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	YEAR								

ACTUAL START DATE (yyyy/mm/dd)												ANTICIPATED / ACTUAL END DATE (yyyy/mm/dd) (7)											
TOTAL PROJECT EXPENDITURE / VALUE OF WORK DONE TO-DATE (INCLUDING ALL COSTS, BUT EXCLUDING VAT)												R											

MONTHLY PROJECT LABOUR REPORT



BENEFICIARY DETAILS AND WORK INFORMATION

CONTRACT OR WORKS PROJECT NUMBER:	
-----------------------------------	--

Year	Month

Sheet		
1	of	

	(8)	(8)	(8)	(9)			(10)		(11)	(12)	(13)	(14)
No.	First name	Surname	ID number	New Beneficiary (Y/N)	Gender (M/F)	Disabled (Y/N)	Job seeker database (Y/N)	Contract start date (DDMMYY)	Contract end date (DDMMYY)	No. days worked this month (excl. training)	Training days	Rate of pay per day (R - c)
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												
16												
17												
18												
19												
20												

0 0 R -

Declared by Contractor or Vendor to be true and correct:	Name		Signature	
	Date			

Received by Employer's Agent / Representative:	Name		Signature	
	Date			

Annexure C - Pro Forma Performance Security/ Guarantee

GUARANTEE PERFORMANCE SECURITY

GUARANTOR DETAILS AND DEFINITIONS

"Guarantor" means:

Physical address of Guarantor:

"Supplier" means:

"Contract Sum" means: The accepted tender amount (INCLUSIVE OF VAT) of R.....

Amount in words:

"Guaranteed Sum" means: The maximum amount of R

Amount in words:

"Contract" means: The agreement made in terms of the Form of Offer and Acceptance for tender no ...and such amendments or additions to the contract as may be agreed in writing between the Parties.

PERFORMANCE GUARANTEE

1. The Guarantor's liability shall be limited to the amount of the Guaranteed Sum.
2. The Guarantor's period of liability shall be from and including the date of issue of this Guarantee/Performance Security up to and including the termination of the Contract or the date of payment in full of the Guaranteed Sum, whichever occurs first.
3. The Guarantor hereby acknowledges that:
 - 3.1 any reference in this Guarantee/Performance to "Contract" is made for the purpose of convenience and shall not be construed as any intention whatsoever to create an accessory obligation or any intention whatsoever to create a suretyship;
 - 3.2 Its obligation under this Guarantee/Performance Security is restricted to the payment of money.
4. Subject to the Guarantor's maximum liability referred to in 1, the Guarantor hereby undertakes to pay the CCT the sum due and payable upon receipt of the documents identified in 4.1 to 4.2:
 - 4.1 A copy of a first written demand issued by the CCT to the Supplier stating that payment of a sum which is due and payable has not been made by the Supplier in terms of the Contract and failing such payment within seven (7) calendar days, the CCT intends to call upon the Guarantor to make payment in terms of 4.2;
 - 4.2 A first written demand issued by the CCT to the Guarantor at the Guarantor's physical address with a copy to the Supplier stating that a period of seven (7) days has elapsed since the first written demand in terms of 4.1 and the sum has still not been paid.
5. Subject to the Guarantor's maximum liability referred to in 1, the Guarantor undertakes to pay to the CCT the Guaranteed Sum or the full outstanding balance upon receipt of a first written demand from the CCT to the Guarantor at the Guarantor's physical address calling up this Guarantee / Performance Security, such demand stating that:
 - 5.1 The Contract has been terminated due to the Supplier's default and that this Guarantee/Performance Security is called up in terms of 5; or
 - 5.2 a provisional or final sequestration or liquidation court order has been granted against the Supplier and that the Guarantee/Performance Guarantee is called up in terms of 5; and

- 5.3 *The aforesaid written demand is accompanied by a copy of the notice of termination and/or the provisional/final sequestration and/or the provisional liquidation court order.*
- 6. *It is recorded that the aggregate amount of payments required to be made by the Guarantor in terms of 4 and 5 shall not exceed the Guarantor's maximum liability in terms of 1.*
- 7. *Where the Guarantor has made payment in terms of 5, the CCT shall upon the termination date of the Contract, submit an expense account to the Guarantor showing how all monies received in terms of this Guarantee/Performance Security have been expended and shall refund to the Guarantor any resulting surplus. All monies refunded to the Guarantor in terms of this Guarantee/Performance Security shall bear interest at the prime overdraft rate of the CCT's bank compounded monthly and calculated from the date payment was made by the Guarantor to the CCT until the date of refund.*
- 8. *Payment by the Guarantor in terms of 4 or 5 shall be made within seven (7) calendar days upon receipt of the first written demand to the Guarantor.*
- 9. *The CCT shall have the absolute right to arrange its affairs with the Supplier in any manner which the CCT may deem fit and the Guarantor shall not have the right to claim his release from this Guarantee /Performance Security on account of any conduct alleged to be prejudicial to the Guarantor.*
- 10. *The Guarantor chooses the physical address as stated above for the service of all notices for all purposes in connection herewith.*
- 11. *This Guarantee/Performance Security is neither negotiable nor transferable and shall expire in terms of 2, where after no claims will be considered by the Guarantor. The original of this Guarantee / Performance Security shall be returned to the Guarantor after it has expired.*
- 12. *This Guarantee/Performance Security, with the required demand notices in terms of 4 or 5, shall be regarded as a liquid document for the purposes of obtaining a court order.*
- 13. *Where this Guarantee/Performance Security is issued in the Republic of South Africa the Guarantor hereby consents in terms of Section 45 of the Magistrate's Courts Act No 32 of 1944, as amended, to the jurisdiction of the Magistrate's Court of any district having jurisdiction in terms of Section 28 of the said Act, notwithstanding that the amount of the claim may exceed the jurisdiction of the Magistrate's Court.*

Signed at

Date

Guarantor's signatory (1)

Capacity

Guarantor's signatory (2)

Capacity

Witness signatory (1)

Witness signatory (2)

Approved Financial Institution as at 13 August 2025:

- 1.1 National Banks
 - ABSA Bank Limited
 - FirstRand Bank Limited
 - Investec Bank Limited
 - Nedbank Limited
 - Standard Bank of South Africa Limited

- 1.2 International Banks (with branches in South Africa)
 - Barclays Bank PLC
 - Citibank NA
 - Credit Agricole Corporate and Investment Bank
 - HSBC Bank PLC
 - JPMorgan Chase Bank
 - Societe Generale
 - Standard Chartered Bank

- 1.3 Insurance Companies
 - American International Group Inc (AIG)
 - Bryte Insurance Company Limited
 - Coface SA
 - Compass Insurance Company Limited
 - Credit Guarantee Insurance Corporation of Africa Limited
 - Guardrisk Insurance Company Limited
 - Hollard Insurance Company Limited
 - Infiniti Insurance Limited
 - Lombard Insurance Company Limited
 - Old Mutual Alternative Risk Transfer Insure Limited (OMART Insure)
 - New National Assurance Company Limited
 - PSG Konsult Ltd (previously Absa Insurance)
 - Regent Insurance Company Limited
 - Renasa Insurance Company Limited
 - Santam Limited

Annexure D - Pro Forma Advance Payment Guarantee

Not Applicable

Annexure F - Tender Returnable Documents

<h3 style="margin: 0;">Schedule F.1: Contract Price Adjustment and/or Rate of Exchange Variation</h3>

1. TENDER CONDITIONS

- 1.1 The Contract Price Adjustment (CPA) mechanism and/or provisions relating to Rate of Exchange (RoE) Variation, contained in this schedule is compulsory and binding on all Tenderers/Suppliers and this schedule (the parts relevant to the particular tender) must be completed by all Tenderers / Suppliers.
- 1.2 Tenderers/Suppliers are not permitted to amend, vary, alter or delete this schedule or any part thereof unless otherwise stated in this schedule.
- 1.3 Tenderers are not permitted to offer fixed and firm prices except as provided for in the Price Schedule.

2. CPA PROVISIONS SELECTION

- 2.1 The prices stipulated on the Price Schedule are subject to adjustment as set out below.
- 2.2 Tenderer to indicate the specific CPA and/or RoE provisions applicable to their bid by marking the relevant checkboxes below. Tenderers to note that the CPA and/or RoE provisions are not exclusive and multiple CPA Types can exist if the bid contains both local and foreign exchange based pricing. In such cases the CPA and/or ROE provision applies only to that particular portion of the tendered price.
- 2.3 The CPA and/or RoE provisions applicable to this tender and resulting contract are to be indicated below by checking the relevant boxes (with multiple selections only where indicated permissible):

	<u>Indicate option</u>	<u>CPA Type</u>	<u>Period</u>	<u>Refer to Section</u>
A	<div style="border: 1px solid black; padding: 2px; width: 40px; margin: 0 auto;">N/A</div>	FIRM PRICES as per Pricing Schedule	Annual	<i>Pricing Schedule C.4 and Schedule F.1 (A)</i>
<u>LOCAL (RSA) TENDER CONTENT:</u>				
EITHER				
B	<div style="border: 1px solid black; padding: 2px; width: 40px; margin: 0 auto;">N/A</div>	SEIFSA Index based CPA	Monthly / Quarterly	<i>Schedule F.1 (B)</i>
OR				
C	<div style="border: 1px solid black; padding: 2px; width: 40px; margin: 0 auto;">N/A</div>	Pricelist / Quotation Based CPA	Ad-Hoc	<i>Schedule F.1 (C)</i>
OR				
D	<div style="border: 1px solid black; padding: 2px; width: 40px; margin: 0 auto;">X</div>	STATS SA CPI Index Based CPA	Annually	<i>Schedule F.1 (D)</i>
OR/AND				
E	<div style="border: 1px solid black; padding: 2px; width: 40px; margin: 0 auto;">N/A</div>	Sectorial Determination 1: Contract Cleaning Sector	Annually	<i>Schedule F.1 (E)</i>
OR				
E	<div style="border: 1px solid black; padding: 2px; width: 40px; margin: 0 auto;">N/A</div>	Sectorial Determination 6: Private Security Sector	Annually	<i>Schedule F.1 (E)</i>
<u>IMPORTED GOODS AND / OR COMPONENTS (IF APPLICABLE)</u>				
F	<div style="border: 1px solid black; padding: 2px; width: 40px; margin: 0 auto;">N/A</div>	ROE based CPA	Ad-Hoc	<i>Schedule F.1 (F)</i>
AND (IF REQUIRED), EITHER				
G	<div style="border: 1px solid black; padding: 2px; width: 40px; margin: 0 auto;">N/A</div>	Pricelist / Quotation based CPA	Ad-Hoc / Periodic	<i>Schedule F.1 (G)</i>
OR				
H	<div style="border: 1px solid black; padding: 2px; width: 40px; margin: 0 auto;">N/A</div>	Overseas CPI / PPI index based CPA	Ad-Hoc / Periodic	<i>Schedule F.1 (H)</i>

2.4 CPA and/or RoE provisions marked as **not applicable** is not relevant and will not apply to this tender and resulting contract.

3. CONTRACT CPA APPLICATIONS AND ADMINISTRATION

3.1 Any claim for variation in the contract price (either CPA or RoE adjustments) must be submitted in writing:

- i. By letter to: Director **[Details to be provided at contract stage]**, City of Cape Town, P O Box 655, Cape Town, 8000 or
- ii. By email to: **[Details to be provided at contract stage]**

at least 14 days prior to the month upon which the adjustment would become effective in the case of prices being set in advance, and as soon as relevant indices are available and no later than 60 days after the date of delivery of goods or the completion of the project (i.e. date of issue of the Taking-Over Certificate, if applicable) in the case of adjustments being claimed retrospectively for Goods or Services. The latter case is only applicable where specifically provided for in the CPA provisions.

3.2 When submitting a request for CPA and/or RoE adjustment the Supplier shall indicate the Rand Value claimed for each item listed on C.4 - Price Schedule, clearly indicating the item number as per C.4 - Price Schedule. Percentage increases will not be considered. A mere notification of a request for CPA without stating the new price claimed for each item shall, for the purpose of this clause, not be regarded as a valid request.

3.3 The CCT reserves the right to request the Supplier to submit auditor's certificates or such other documentary proof as it may require in order to verify a claim for CPA or RoE adjustments. Price adjustments will not be processed until such time as the Supplier submits such auditor's certificates or other documentary proof to the CCT. Should the Supplier fail to submit the auditor's certificates or other documentary proof to the CCT within 30 days from the written request, it shall be presumed that the Supplier has abandoned his request.

3.4 The CCT reserves the right to withhold payment of any claim for adjustment while only provisional figures are available and until such time as the final (revised) figures are issued by the relevant authority.

3.5 The CCT will confirm in writing once processing of the CPA or RoE adjustments have been completed including the effective date of the adjustments.

3.6 Where pricelist-based and other non-index based CPA requests are investigated and found to be not reasonable and market related, the CCT reserves the right to reject such requests. Where disputes arise with respect to such rejected requests the CCT reserves the right to procure the Goods from other available Suppliers until such time as the dispute is resolved.

3.7 Unless indicated otherwise in the relevant schedule below, all Purchase Orders issued on or after the effective date of the adjustment shall be issued at, and the Goods or Services supplied, invoiced and paid for at the adjusted prices. The relevant adjustment will not be applied to Purchase Orders issued prior to the effective date.

F.1 (A) – FIRM PRICES

NOT APPLICABLE

F.1 (B) LOCAL SOUTH AFRICAN CONTENT – SEIFSA INDICES

NOT APPLICABLE

F.1 (C) LOCAL SOUTH AFRICAN CONTENT - SUPPLIER/ MANUFACTURER PRICE LIST/QUOTATIONS

NOT APPLICABLE

F.1 (D) LOCAL SOUTH AFRICAN CONTENT - STATS SA CONSUMER PRICE INDEX

1. Applicable where the Tenderer/Suppliers has indicated their tendered prices are subject to adjustment based on changes in the Statistics South Africa (STATS SA) Consumer Price Indices.
2. A minimum of 10% of the tender/contract price as per C.4 Pricing Schedule shall be fixed and free of variation for the duration of the contract.
3. A total of 90% of the tender/contract price as per C.4 Pricing Schedule shall be adjusted annually in accordance with clause 5 below.
4. STATS SA Consumer Price Index is applicable to Tables A4, A5 and A6 in Schedule A, Tables B4, B5 and B6 in Schedule B and Tables C4, C5 and C6 in Schedule C of the C.4 Price Schedule.
5. The Contract Price(s) shall remain FIRM for the first 12 calendar months from date of Commencement Date of Contract and Suppliers are not permitted to requests CPA during this period.
6. The Contract Price(s) will thereafter be subject to adjustment annually based on the average percentage of change over 12 months as published by STATS SA: Consumer Price Index (P0141–Table B2 – CPI headline year-on-year rates) as follows:
 - 5.1 CPA applicable from the start of the 13th month to the end of the 24th month calculated as follows:
 - a) The base month for the price adjustment being three (3) calendar months prior to Commencement Date of Contract; and
 - b) The end month shall be three (3) calendar months prior to the 12th month.
 - 5.2 CPA applicable from the start of the 25th month to end of the 36th month calculated as follows:
 - a) The base month for the price adjustment shall be three (3) calendar months prior to the 13th month; and
 - b) The end month shall be three (3) calendar months prior to 24th month.
 - 5.3 CPA applicable from the start of the 37th month to end of the 48th month calculated as follows:
 - a) The base month for the price adjustment shall be three (3) calendar months prior to the 25th month; and
 - b) The end month shall be three (3) calendar months prior to 36th month.
 - 5.4 CPA applicable from the start of the 49th month to end of the 60th month calculated as follows:
 - a) The base month for the price adjustment shall be three (3) calendar months prior to the 37th month; and
 - b) The end month shall be three (3) calendar months prior to 48th month.
 - 5.5 CPA applicable from the start of the 61st month to end of the 72nd month calculated as follows:
 - a) The base month for the price adjustment shall be three (3) calendar months prior to the 49th month; and
 - b) The end month shall be three (3) calendar months prior to 60th month.
 - 5.6 CPA applicable from the start of the 73rd month to end of the 84th month calculated as follows:
 - a) The base month for the price adjustment shall be three (3) calendar months prior to the 61st month; and
 - b) The end month shall be three (3) calendar months prior to 72nd month.
 - 5.7 CPA applicable from the start of the 85th month to end of the 96th month calculated as follows:
 - a) The base month for the price adjustment shall be three (3) calendar months prior to the 73rd month; and
 - b) The end month shall be three (3) calendar months prior to 84th month.
 - 5.8 CPA applicable from the start of the 97th month to end of the 108th month calculated as follows:
 - a) The base month for the price adjustment shall be three (3) calendar months prior to the 85th month; and

- b) The end month shall be three (3) calendar months prior to 96th month.
- 5.9 CPA applicable from the start of the 109th month to end of the 120th month calculated as follows:
- a) The base month for the price adjustment shall be three (3) calendar months prior to the 97th month; and
 - b) The end month shall be three (3) calendar months prior to 108th month.
- 5.10 The average CPI percentage will be calculated using the base month to the end month (both included) divided by the number of months. (12 months totalled/12 to achieve the average CPI)
7. Subject to prior approval by the CCT delegated authority, in the event of any extension of the contract period, the CPA applicable beyond month 120 of the contract will follow the same principle in determining the base month (i.e. 3 calendar months prior to 109th month) and end date (3 calendar months prior to 120th month) as outlined above.

F.1. (E) LOCAL SOUTH AFRICAN CONTENT – SECTORIAL DETERMINATION

NOT APPLICABLE

**F.1. (F) GOODS AND/OR COMPONENTS IMPORTED FROM OUTSIDE OF SOUTH AFRICA
RATE OF EXCHANGE PRICE VARIATIONS**

NOT APPLICABLE

**F.1. (G) GOODS AND/OR COMPONENTS IMPORTED FROM OUTSIDE OF SOUTH AFRICA -
MANUFACTURER/SUPPLIER PRICE/QUOTATION LIST**

NOT APPLICABLE

**F.1. (H) GOODS AND/OR COMPONENTS IMPORTED FROM OUTSIDE OF SOUTH AFRICA - BASED
ON FOREIGN INDICES**

NOT APPLICABLE

Schedule F.2: Certificate of Authority for Partnerships/ Joint Ventures/ Consortia

This schedule is to be completed if the tender is submitted by a partnership/joint venture/ consortium.

1. We, the undersigned, are submitting this tender offer as a partnership/ joint venture/ consortium and hereby authorize Mr/Ms _____, of the authorised entity _____, acting in the capacity of Lead Partner, to sign all documents in connection with the tender offer and any contract resulting from it on the partnership/joint venture/ consortium’s behalf.

2. By signing this schedule the partners to the partnership/joint venture/ consortium:
 - 2.1 warrant that the tender submitted is in accordance with the main business and objectives of the partnership/joint venture/ consortium;
 - 2.2 agree that the CCT shall make all payments in terms of this Contract into the following bank account of the Lead Partner:
 Account Holder: _____
 Financial Institution: _____
 Branch Code: _____
 Account No.: _____
 - 2.3 agree that in the event that there is a change in the partnership/ joint venture/ consortium and/or should a dispute arise between the partnership/joint venture/ consortium partners, that the CCT shall continue to make any/all payments due and payable in terms of the Contract into the aforesaid bank account until such time as the CCT is presented with a Court Order or an original agreement (signed by each and every partner of the partnership/joint venture/ consortium) notifying the CCT of the details of the new bank account into which it is required to make payment.
 - 2.4 agree that they shall be jointly and severally liable to the CCT for the due and proper fulfilment by the successful tenderer/supplier of its obligations in terms of the Contract as well as any damages suffered by the CCT as a result of breach by the successful tenderer/supplier. The partnership/joint venture/ consortium partners hereby renounce the benefits of excussion and division.

SIGNED BY THE PARTNERS OF THE PARTNERSHIP/ JOINT VENTURE/ CONSORTIUM		
NAME OF FIRM	ADDRESS	DULY AUTHORISED SIGNATORY
Lead partner		Signature..... Name..... Designation.....
		Signature..... Name..... Designation.....
		Signature..... Name..... Designation.....
		Signature..... Name..... Designation.....

Note: A copy of the Joint Venture Agreement shall be appended to *List of Other Documents Attached by Tenderer Schedule*.

Schedule F.3: Declaration for Procurement above R10 million

If the value of the transaction is expected to exceed R10 million (VAT included) the tenderer shall complete the following questionnaire, attach the necessary documents and sign this schedule:

1. Are you by law required to prepare annual financial statements for auditing? **(Please mark with X)**

YES		NO	
-----	--	----	--

If YES, submit audited annual financial statements:

- (i) For the past three years, or
- (ii) Since the date of establishment of the tenderer (if established during the past three years)

By attaching such audited financial statements to **List of Other Documents Attached by Tenderer Schedule**.

2. Do you have any outstanding undisputed commitments for municipal services towards the CCT or other municipality in respect of which payment is overdue for more than 30 (thirty) days? **(Please mark with X)**

YES		NO	
-----	--	----	--

2.1 If NO, this serves to certify that the tenderer has no undisputed commitments for municipal services towards any municipality for more than three (3) (three) months in respect of which payment is overdue for more than 30 (thirty) days.

2.2 If YES, provide particulars:

3. Has any contract been awarded to you by an organ of state during the past five (5) years? **(Please mark with X)**

YES		NO	
-----	--	----	--

If YES, insert particulars in the table below including particulars of any material non-compliance or dispute concerning the execution of such contract. Alternatively attach the particulars to **List of Other Documents Attached by Tenderer** schedule in the same format as the table below:

Organ of State	Contract Description	Contract Period	Non-compliance/dispute (if any)

4. Will any portion of the goods or services be sourced from outside the Republic, and if so, what portion and whether any portion of payment from the CCT is expected to be transferred out of the Republic? **(Please mark with X)**

YES		NO	
-----	--	----	--

If YES, furnish particulars below

The tenderer hereby certifies that the information set out in this schedule and/or attached hereto is true and correct, and acknowledges that failure to properly and truthfully complete this schedule may result in steps being taken against the tenderer, the tender being disqualified, and/or (in the event that the tenderer is successful) the cancellation of the contract, restriction of the tenderer or the exercise by the CCT of any other remedies available to it.

 Signature
 Print name:
 On behalf of the tenderer (duly authorised)

 Date

Schedule F.4: Preference Points Claim Form In Terms Of the Preferential Procurement Regulations 2022

1. GENERAL CONDITIONS

- 1.1 The following preference point systems are applicable to invitations to tender:
 - the 90/10 system for requirements with a Rand value above R50 000 000 (all applicable taxes included).

1.2 To be completed by the organ of state

The applicable preference point system for this tender is the 90/10 preference point system.

- 1.3 Points for this tender (even in the case of a tender for income-generating contracts) shall be awarded for:
 (a) Price; and
 (b) Specific Goals.

1.4 To be completed by the organ of state:

The maximum points for this tender are allocated as follows:

	POINTS
PRICE	90
SPECIFIC GOALS	10
Total points for Price and SPECIFIC GOALS	100

- 1.5 Failure on the part of a tenderer to submit proof or documentation required in terms of this tender to claim points for specific goals with the tender, will be interpreted to mean that preference points for specific goals are not claimed.
- 1.6 The organ of state reserves the right to require of a tenderer, either before a tender is adjudicated or at any time subsequently, to substantiate any claim in regard to preferences, in any manner required by the organ of state.

2. DEFINITIONS

The following definitions shall apply to this schedule:

- (a) "tender" means a written offer in the form determined by an organ of state in response to an invitation to provide goods or services through price quotations, competitive tendering process or any other method envisaged in legislation;
- (b) "price" means an amount of money tendered for goods or services, and includes all applicable taxes less all unconditional discounts;
- (c) "rand value" means the total estimated value of a contract in Rand, calculated at the time of bid invitation, and includes all applicable taxes;
- (d) "tender for income-generating contracts" means a written offer in the form determined by an organ of state in response to an invitation for the origination of income-generating contracts through any method envisaged in legislation that will result in a legal agreement between the organ of state and a third party that produces revenue for the organ of state, and includes, but is not limited to, leasing and disposal of assets and concession contracts, excluding direct sales and disposal of assets through public auctions; and
- (e) "The Act" means the Preferential Procurement Policy Framework Act, 2000 (Act No. 5 of 2000).

3. FORMULAE FOR PROCUREMENT OF GOODS AND SERVICES

POINTS AWARDED FOR PRICE

THE 80/20 OR 90/10 PREFERENCE POINT SYSTEMS

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

90/10

Where

Ps = Points scored for price of tender under consideration

Pt = Price of tender under consideration

Pmin = Price of lowest acceptable tender

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

NOT APPLICABLE

5. POINTS AWARDED FOR SPECIFIC GOALS

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

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

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

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

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

Table 1: Specific Goals (SG) – Points Allocated and Claimed

Tenderers must indicate the preference points claimed for each specific goal applicable to them, for the purposes of this tender.

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

The specific goals allocated points in terms of this tender	To be Completed by the Organ of State	To be Completed by the Tenderer
	Number of points Allocated (90/10 system)	Number of points claimed (90/10 system)
Promotion of Micro and Small Enterprises	4	
Enterprise Supplier Development and Socio-Economic Development	3	
Skills Development <u>OR</u> Employee Share Scheme	3	

DECLARATION WITH REGARD TO COMPANY/FIRM

5.3 Name of company/firm.....

5.4 Company registration number:

5.5 TYPE OF COMPANY/ FIRM

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

[Tick applicable box]

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

- i) The information furnished is true and correct;
- ii) The preference points claimed are in accordance with the General Conditions as indicated in paragraph 1 of this form;
- iii) In the event of a contract being awarded as a result of points claimed as shown in paragraphs 4.1 and 4.2, the Supplier may be required to furnish documentary proof to the satisfaction of the organ of state that the claims are correct;
- iv) If the specific goals have been claimed or obtained on a fraudulent basis or any of the conditions of contract have not been fulfilled, the organ of state may, in addition to any other remedy it may have –
 - (a) disqualify the person from the tendering process;
 - (b) recover costs, losses or damages it has incurred or suffered as a result of that person's conduct;
 - (c) cancel the contract and claim any damages which it has suffered as a result of having to make less favourable arrangements due to such cancellation;
 - (d) recommend that the tenderer or Supplier, 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.

<i>Signature of Tenderer</i>	<i>Date</i>	<i>Name and Surname</i>	<i>Address</i>

For official use.		
SIGNATURE OF CCT OFFICIALS AT TENDER OPENING		
1.	2.	3.

Table 2: Specific Goals – Declaration by the Tenderer

Tenderers must complete this table to declare the amounts and percentages applicable to the specific goals they are claiming.

NB: In completing Table 2 below, please consult **Notes for Verification** below

The specific goals allocated points in terms of this tender	To be Completed by the Tenderer	
	Refer to “Notes for verification”	Amount Declared (excluding VAT)
<u>SG1</u> Promotion of Micro and Small Enterprises	(i) Total Turnover	
<u>SG2</u> Enterprise Supplier Development and Socio Economic Development	(ii) Total Enterprise Supplier Development Expenditure	
	(iii) Total Socio Economic Development Expenditure	
	(iv) Total Expenditure	
<u>SG3.1</u> Skills Development	(v) Total Skills Development Expenditure	
	(vi) Total Profit	
OR <u>SG3.2</u> Employee Share Scheme	(vii) Employee Share Scheme Ownership %	

Tenderer Confirmation:

I confirm that the amounts declared in Table 2 above are accurate and in accordance with the *‘The Broad-Based Black Economic Empowerment (B-BBEE) Act 53 of 2003, as amended.* .

Signature of Tenderer (Authorised to represent the tenderer)	Date	Name and Surname	Address

Notes for Verification:

All amounts disclosed should be as per the most recent Annual Financial Statements (not older than 12 months) and defined as per the B-BBEE Act

- SG1 – Specific Goal 1
Promotion of Micro and Small Enterprises
 (i) Total Turnover
 Micro enterprises with a turnover of up to R20million and Small enterprises with a turnover up to R80 million, as per National Small Enterprise Act, 1996 (Act No.102 of 1996)

- SG2 – Specific Goal 2
Enterprise Supplier Development and Socio-Economic Development
 (ii) Total Enterprise Supplier Development Expenditure
 Qualifying expenditure as defined in the B-BBEE Act: Statement 400 "THE GENERAL PRINCIPLES FOR MEASURING ENTERPRISE AND SUPPLIER DEVELOPMENT"

 (iii) Total Enterprise Socio Economic Development Expenditure
 Qualifying expenditure as defined in the B-BBEE Act: Statement 500 "THE GENERAL PRINCIPLES FOR MEASURING THE SOCIO - ECONOMIC DEVELOPMENT ELEMENT"

 (iv) Total Expenditure
 Total Expenditure as per the most recent Annual Financial Statements (not older than 12 months)

- SG3.1 – Specific Goal 3
Skills Development
 (v) Total Skills Development Expenditure
 Qualifying expenditure as defined in the B-BBEE Act: Statement 300 "THE GENERAL PRINCIPLES FOR MEASURING SKILLS DEVELOPMENT"

 (vi) Total Profit
 Total Profit as per the most recent Annual Financial Statements (not older than 12 months)

- SG3.2 – Specific Goal 3
Employee Share Scheme
 (vii) Employee Share Scheme Ownership %
 Total employee ownership as per employee share certificate at the date of tender closing.

The below table (Table 3) must be completed by a B-BBEE Verification Agency (*Note 1) **OR** Commissioner of Oaths
 (Refer to *Note 3.2 for the detailed declaration):

Table 3:

Signature and Stamp	Date	Name and Surname	Address

***Note 1**

1.1 Tendering entity that undergoes B-BBEE verification

- Where a tendering entity undergoes B-BBEE verification, a B-BBEE certificate valid as at the date of tender closing, must be attached to the bid submission or must be made available upon request within the specified period.
- All amounts disclosed in Table 2, should be amounts used in the B-BBEE verification process undergone by the tendering entity
- The B-BBEE verification agency must complete Table 3 above, to confirm the following amounts disclosed by the bidder in Table 2:
 - (ii) Total Enterprise Supplier Development Expenditure;
 - (iii) Total Socio Economic Development Expenditure;
 - (v) Total Skills Development Expenditure
- Where the tendering entity is a Joint Venture/ Consortium, the amounts in Table 2 must be consolidated, with an accompanying consolidated B-BBEE certificate valid as at the date of tender closing must be attached to the bid submission or must be made available upon request within the specified period.

1.2 If the tendering entity does not undergo B-BBEE verification and qualifies as a B-BBEE Qualifying Small Enterprise (QSE) and Exempted Micro-Enterprises (EME)

- Table 3 must be completed by a Commissioner of Oaths to confirm the following amounts disclosed by the bidder in Table 2:
 - (ii) Total Enterprise Supplier Development Expenditure;
 - (iii) Total Socio Economic Development Expenditure;
 - (v) Total Skills Development Expenditure

***Note 2**

2.1 The tendering entity must attach with the bid submission or must be made available upon request within the specified period; the most recent (where applicable) audited financial statements to enable validation of the following amounts disclosed by the bidder in Table 2:

- (i) Total Turnover
- (iv) Total Expenditure
- (vi) Total Profit

2.2 Companies who are required to be audited by legislation, must submit audited financial statements, not older than 12 months with the bid submission or must be made available upon request within the specified period.

***Note 3**

Sworn affidavit to be deposed by the Commissioner of Oaths to the QSE or EME.

I, the undersigned,

Full Name and Surname <i>(Authorised to represent the tenderer)</i>	
Identity Number	

Hereby declare under oath as follows

3.1 The contents of this statement are to the best of my knowledge a true reflection of facts.

3.2 I am a Member/ Director/ Owner of the following enterprise and am duly authorised to act on its behalf.

Enterprise Name:	
Trading Name (If Applicable):	
Registration Number:	
Enterprise Physical Address:	
Type of Entity (CC, Pty (Ltd), Sole Prop etc):	
Nature of Business:	

3.3 I hereby declare under oath that based on the Financial Statements / Management Accounts and information available on the latest financial year end _____

3.3.1 The annual Total Revenue was less than R50 000 000.00 (Fifty Million Rand);

3.3.2 The following amounts disclosed in Table 2 are accurate, complete, consistent with the BBBEE Act (see Notes for Verification) and based on the Financial Statements / Management Accounts and information available on the latest financial year end _____

As per Table 2	Amount Declared (excluding VAT)
(ii) Total Enterprise Supplier Development Expenditure	
(iii) Total Socio Economic Development Expenditure	
(iv) Total Expenditure	
(v) Total Skills Development Expenditure	

As per Table 2	Amount Declared (excluding VAT)
(vi) Total Profit	
(vii) Employee Share Scheme Ownership %	

3.4 I know and understand the contents of this affidavit and I have no objection to take the prescribed oath and consider the oath binding on my conscience and on the owners of the enterprise which I represent I this matter.

3.5 The sworn affidavit will be valid for a period of 12 months from the date signed by the commissioner.

Commissioner of Oaths
Signature, Date and Stamp

Deponent Signature and Date

3.6 KEY NOTES OF DETERMINING VALIDITY OF SWORN AFFIDAVITS

<p>BBBEE Certificates/ Sworn Affidavits</p>	<p>Returnable for declaration requirement must be attached with the bid submission or must be made available upon request within the specified period</p> <ul style="list-style-type: none"> - Certified and Valid copy of BBBEE Certificate issued by a SANAS Accredited Verification Agent, or - Certified and Valid copy of Sworn Affidavit for either EME or QSE (see key notes below to determine Validity of a Sworn Affidavit); or - Valid copy of BBBEE Certificate issued by CIPC for EME's only <p>KEY NOTES OF DETERMINING VALIDITY OF SWORN AFFIDAVITS</p> <p>Tenderers submitting Sworn Affidavits must ensure that the affidavits meet the following key pointers to ensure their validity:</p> <p>(a) Name/s of deponent as they appear in the identity document and the identity number.</p> <p>(b) Designation of the deponent as the Director/ Member must be indicated in order to know that person is duly authorised to depose of an affidavit (mark the applicable</p>
--	--

option).

(c) Name of enterprise as per enterprise registration documents issued by CIPC, where applicable, and enterprise business address.

(d) Amounts as per Table 2 must be inserted **(No blank spaces to be left).**

(e) Indicate total revenue for the year under review and whether it is based on audited financial statements or management accounts **(mark the applicable option).**

(f) Financial year end as per the enterprise's registration documents, which was used to determine the total revenue (financial year end to be stipulated by day/ month/ year).

(g) Date deponent signed and date of Commissioner of Oath must be the same.

(The sworn affidavit must be signed in the presence of the Commissioner of Oath. Furthermore the Commissioner must also sign ad stamp).

(h) Commissioner of Oath cannot be an employee or ex officio of the enterprise because, a person cannot by law, commission a sworn affidavit in which they have an interest.

If the relevant documentation/ information as stipulated in the enquiry is not submitted and/or does not meet the above requirements; tenderers will be disqualified.

Schedule F.5: Declaration of Interest – State Employees (MBD 4 amended)
--

1. No bid will be accepted from:
 - 1.1 persons in the service of the state¹, or
 - 1.2 if the person is not a natural person, of which any director, manager or principal shareholder or stakeholder is in the service of the state, or
 - 1.3 from persons, or entities of which any director, manager or principal shareholder or stakeholder, has been in the service of the City of Cape Town (CCT) during the previous twelve (12) months, or
 - 1.4 from an entity who has employed a former CCT employee who was at a level of T14 or higher at the time of leaving the CCT's employ and involved in any of the CCT's bid committees for the bid submitted, if:
 - 1.4.1 the CCT employee left the CCT's employment voluntarily, during the previous twelve (12) months;
 - 1.5 a person who was a CCT employee, or an entity that employs a CCT employee, if
 - 1.5.1 the CCT employee left the CCT's employment whilst under investigation for alleged misconduct, or
 - 1.5.2 was facing disciplinary action or potential disciplinary action by the CCT, or
 - 1.5.3 was involved in a dispute against the CCT during the previous thirty six (36) months.

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 tenderer or their authorised representative declare their position in relation to the evaluating/adjudicating authority.

3. In order to give effect to the above, the following questionnaire must be completed and submitted with the bid.
 - 3.1 Full Name of tenderer or his or her representative: _____
 - 3.2 Identity Number: _____
 - 3.3 Position occupied in the Company (director, trustee, shareholder²): _____
 - 3.4 Company or Close Corporation Registration Number: _____
 - 3.5 Tax Reference Number: _____
 - 3.6 VAT Registration Number: _____
 - 3.7 The names of all directors / trustees / shareholders members, their individual identity numbers and state employee numbers must be indicated in paragraph 4 below.
 - 3.8 Are you presently in the service of the state? **YES / NO**
 - 3.8.1 If yes, furnish particulars: _____
 - 3.9 Have you been in the service of the state for the past twelve months? **YES / NO**
 - 3.9.1 If yes, furnish particulars: _____
 - 3.10 Do you have any relationship (family, friend, other) with persons in the service of the state and who may be involved with the evaluation and or adjudication of this bid? **YES / NO**
 - 3.10.1 If yes, furnish particulars: _____
 - 3.11 Are you, aware of any relationship (family, friend, other) between any other tenderer and any persons in the service of the state who may be involved with the evaluation and or adjudication of this bid? **YES / NO**
 - 3.11.1 If yes, furnish particulars: _____
 - 3.12 Are any of the company's directors, trustees, managers, principle shareholders or stakeholders in service of the state? **YES / NO**
 - 3.12.1 If yes, furnish particulars: _____

- 3.13 Are any spouse, child or parent of the company’s directors, trustees, managers, principle shareholders or stakeholders in service of the state? **YES / NO**
 3.13.1 If yes, furnish particulars: _____
- 3.14 Do you or any of the directors, trustees, managers, principle shareholders, or stakeholders of this company have any interest in any other related companies or business whether or not they are bidding for this contract? **YES / NO**
 3.14.1 If yes, furnish particulars: _____
- 3.15 Have you, or any of the directors, trustees, managers, principle shareholders, or stakeholders of this company been in the service of the CCT in the past twelve months? **YES / NO**
 3.15.1 If yes, furnish particulars: _____
- 3.16 Do you have any employees who was in the service of the CCT at a level of T14 or higher at the time they left the employ of the CCT, and who was involved in any of the CCT’s bid committees for this bid? **YES / NO**
 3.16.1 If yes, furnish particulars: _____

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

Full Name	Identity Number	State Employee Number

If the above table does not sufficient to provide the details of all directors / trustees / shareholders, please append full details to the tender submission.

The tenderer hereby certifies that the information set out in this schedule and/or attached hereto is true and correct, and acknowledges that failure to properly and truthfully complete this schedule may result in steps being taken against the tenderer, the tender being disqualified, and/or (in the event that the tenderer is successful) the cancellation of the contract, restriction of the tenderer or the exercise by the CCT of any other remedies available to it.

 Signature
 Print name: _____ Date
 On behalf of the tenderer (duly authorised)

1MSCM Regulations: “in the service of the state” means to be –

- (a) a member of –
 - (i) any municipal council;
 - (ii) any provincial legislature; or
 - (iii) the national Assembly or the national Council of provinces;
- (b) a member of the board of directors of any municipal entity;
- (c) an official of any municipality or municipal entity;
- (d) an employee of any national or provincial department, national or provincial public entity or constitutional institution within the meaning of the Public Finance Management Act, 1999 (Act No.1 of 1999);
- (e) an executive member of the accounting authority of any national or provincial public entity; or
- (f) an employee of Parliament or a provincial legislature.

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

Schedule F.6: Conflict of Interest Declaration

1. The tenderer shall declare whether it has any conflict of interest in the transaction for which the tender is submitted. **(Please mark with X)**

YES		NO	
-----	--	----	--

1.1 If yes, the tenderer is required to set out the particulars in the table below:

2. The tenderer shall declare whether it has directly or through a representative or intermediary promised, offered or granted:

2.1 Any inducement or reward to the CCT for or in connection with the award of this contract; or

2.2 Any reward, gift, favour or hospitality to any official or any other role player involved in the implementation of the supply chain management policy. **(Please mark with X)**

YES		NO	
-----	--	----	--

If yes, the tenderer is required to set out the particulars in the table below:

Should the tenderer be aware of any corrupt or fraudulent transactions relating to the procurement process of the CCT, please contact the following:

The CCT's anti-corruption hotline at 0800 32 31 30 (toll free)

The tenderer hereby certifies that the information set out in this schedule and/or attached hereto is true and correct, and acknowledges that failure to properly and truthfully complete this schedule may result in steps being taken against the tenderer, the tender being disqualified, and/or (in the event that the tenderer is successful) the cancellation of the contract, restriction of the tenderer or the exercise by the CCT of any other remedies available to it.

 Signature
 Print name:
 On behalf of the tenderer (duly authorised)

 Date

Schedule F.7: Declaration of Tenderer's Past Supply Chain Management Practices (MBD 8)

Where the entity tendering is a partnership/joint venture/consortium, each party to the partnership/joint venture/consortium must sign a declaration in terms of the Municipal Finance Management Act, Act 56 Of 2003, and attach it to this schedule.

1 The tender offer of any tenderer may be rejected if that tenderer or any of its directors/members have:

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

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

Item	Question	Yes	No
2.1	<p>Is the tenderer or any of its directors/members listed on the National Treasury's Database of Restricted Suppliers as companies or persons prohibited from doing business with the public sector?</p> <p>(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 <i>audi alteram partem</i> rule was applied).</p> <p>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.</p>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2.1.1	If so, furnish particulars:		
2.2	<p>Is the tenderer or any of its directors/members 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) or Database of Restricted Suppliers?</p> <p>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.</p>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2.2.1	If so, furnish particulars:		
2.3	<p>Was the tenderer or any of its directors/members 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?</p>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2.3.1	If so, furnish particulars:		
Item	Question	Yes	No

2.4	Does the tenderer 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 <input type="checkbox"/>	No <input type="checkbox"/>
2.4.1	If so, furnish particulars:		
2.5	Was any contract between the tenderer 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 <input type="checkbox"/>	No <input type="checkbox"/>
2.5.1	If so, furnish particulars:		

The tenderer hereby certifies that the information set out in this schedule and/or attached hereto is true and correct, and acknowledges that failure to properly and truthfully complete this schedule may result in steps being taken against the tenderer, the tender being disqualified, and/or (in the event that the tenderer is successful) the cancellation of the contract,, restriction of the tenderer or the exercise by the CCT of any other remedies available to it.

 Signature
 Print name:
 On behalf of the tenderer (duly authorised)

 Date

Schedule F.8: Authorisation for the Deduction of Outstanding Amounts Owed to the CCT

To: THE CITY MANAGER, City of Cape Town

From: _____
(Name of tenderer)

RE: AUTHORISATION FOR THE DEDUCTION OF OUTSTANDING AMOUNTS OWED TO THE CCT

The tenderer:

- a) hereby acknowledges that according to SCM Regulation 38(1)(d)(i) the City Manager may reject the tender of the tenderer if any municipal rates and taxes or municipal service charges owed by the tenderer (or any of its directors/members/partners) to the CCT, or to any other municipality or municipal entity, are in arrears for more than 3 (three) months; and
- b) therefore hereby agrees and authorises the CCT to deduct the full amount outstanding by the Tenderer or any of its directors/members/partners from any payment due to the tenderer; and
- c) confirms the information as set out in the tables below for the purpose of giving effect to b) above;

Physical Business address(es) of the tenderer	Municipal Account number(s)	Inside the CCT municipal boundary (Yes/No)

If there is not enough space for all the names, please attach the information to **List of other documents attached by tenderer** schedule in the same format:

Name of Director / Member / Partner	Identity Number	Physical residential address of Director / Member / Partner	Municipal Account number(s)	Inside the CCT municipal boundary (Yes/No)

The tenderer hereby certifies that the information set out in this schedule and/or attached hereto is true and correct, and acknowledges that failure to properly and truthfully complete this schedule may result in steps being taken against the tenderer, the tender being disqualified, and/or (in the event that the tenderer is successful) the cancellation of the contract, restriction of the tenderer or the exercise by the CCT of any other remedies available to it.

Signature
Print name:
On behalf of the tenderer (duly authorised)

Date

Schedule F.9: Certificate of Independent Tender Determination

I, the undersigned, in submitting this tender number **252S/2025/26** and tender description: SUPPLY, INSTALLATION, MAINTENANCE AND SUPPORT OF AN IDENTITY LIFECYCLE MANAGEMENT SOLUTION FOR THE CITY OF CAPE TOWN in response to the tender invitation made by THE CCT, do hereby make the following statements, which I certify to be true and complete in every respect:

I certify, on behalf of: _____ (Name of tenderer) that:

1. I have read and I understand the contents of this Certificate;
2. I understand that this tender will be disqualified if this Certificate is found not to be true and complete in every respect;
3. I am authorised by the tenderer to sign this Certificate, and to submit this tender, on behalf of the tenderer;
4. Each person whose signature appears on this tender has been authorised by the tenderer to determine the terms of, and to sign, the tender on behalf of the tenderer;
5. For the purposes of this Certificate and this tender, I understand that the word 'competitor' shall include any individual or organisation other than the tenderer, whether or not affiliated with the tenderer, who:
 - (a) has been requested to submit a tender in response to this tender invitation;
 - (b) could potentially submit a tender in response to this tender invitation, based on their qualifications, abilities or experience; and
 - (c) provides the same goods and services as the tenderer and/or is in the same line of business as the tenderer.
6. The tenderer has arrived at this tender independently from and without consultation, communication, agreement or arrangement with any competitor. However, communication between partners in a joint venture or consortium¹ will not be construed as collusive price quoting.
7. In particular, without limiting the generality of paragraphs 5 and 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 tender;
 - (e) the submission of a tender which does not meet the specifications and conditions of the tender; or
 - (f) tendering with the intention not to win the contract.
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 tender invitation relates.
9. The terms of this tender have not been and will not be disclosed by the tenderer, directly or indirectly, to any competitor, prior to the date and time of the official tender 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 tenders and contracts, tenders 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, Act 89 of 1998, and/o/r 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 10 (ten) years in terms of the Prevention and Combating of Corrupt Activities Act, Act 12 of 2004, or any other applicable legislation.

Signature

Print name:

On behalf of the tenderer (duly authorised)

Date

(¹ Consortium: 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

Schedule F.11: List of Other Documents Attached By Tenderer
--

The tenderer has attached to this schedule, the following additional documentation:

	Date of Document	Title of Document or Description (refer to clauses / schedules of this tender document where applicable)
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		

Attach additional pages if more space is required.

 Signature
 Print name:
 On behalf of the tenderer (duly authorised)

 Date

Schedule F.12: Record of Addenda to Tender Documents

We confirm that the following communications received from the CCT before the submission of this tender offer, amending the tender documents, have been taken into account in this tender offer:

	Date	Title or Details
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

Attach additional pages if more space is required.

 Signature
 Print name:
 On behalf of the tenderer (duly authorised)

 Date

Schedule F.13: Information to Be Provided With the Tender

The following information shall be provided with the Tender:

- a. **OEM Accreditation/ Authorisation**
Tenderers are to attach proof of OEM Accreditation/ Authorisation to Schedule F.13A as per clause 2.2.1.1.4 of the Eligibility Criteria.
- b. **OEM Retail Price List**
Tenderers are to attach to Schedule F.13B the OEM Retail Price List as per clause 2.2.1.1.5 of the Eligibility Criteria.
- c. **Functionality:**
Tenderer's are to complete the evidence to Functionality Schedules i.e. Schedules F.13C, F.13D and F.13E as per clause 2.2.1.1.8 of the Eligibility Criteria.
- d. **Requirements for Identity Governance and Administration:**
Tenderer's are to complete the evidence to Schedules F.13F as per clause 2.2.1.1.6 of the Tenderer's Obligations.
- e. **Requirements for PAM:**
Tenderer's are to complete the evidence to Schedules F.13G as per clause 2.2.1.1.7 of the Tenderer's Obligations.
- f. **On-premise infrastructure and software requirements for PAM**
Tenderer's are to complete the evidence to Schedules F.13H.
- g. **Optional items**
Tenderer's are to complete the evidence with regards to the optional items to Schedules F.13I.

Schedule F.13A - Evidence to Eligibility Requirement 2.2.1.1.4 – OEM Accreditation/ Authorisation

Tenderers are to attach hereto proof of OEM Accreditation/ Authorisation as per clause 2.2.1.1.4 of the Eligibility Criteria for each OEM product listed in the Price Schedules A, B and C.

Signature
Print name:
On behalf of the tenderer (duly authorised)

Date

Schedule F.13B - Evidence to Eligibility Requirement 2.2.1.1.5 – OEM Retail Price List

Tenderers are to attach hereto proof of a comprehensive OEM Retail Price Lists as per clause 2.2.1.1.5 of the Eligibility Criteria, for each OEM product listed in the Price Schedules A, B and C.

Signature
Print name:
On behalf of the tenderer (duly authorised)

Date

Schedule F.13C - 2.2.1.1.8.1 Evidence to Functionality Requirement– Number of years in the Industry

Please provide evidence of the number of years the tenderer has been actively providing Identity Lifecycle Management (ILM) solutions including Identity Governance and Administration (IGA) solution(s) or Single Sign On (SSO) solution(s) or Privileged Access Management (PAM) solution(s) or Identity Proofing solution(s) to their client base. The Tenderer must specify client organisations, the solution/s provided, the implementation dates and duration of each project. The tenderer must also provide reference contact details for verification purposes.

No.	CLIENT	SOLUTION/S PROVIDED	DATE FROM	DATE TO	DURATION	PROJECT REFERENCE (Name, Active contact details)
1						Name:
						Contact details:
2						Name:
						Contact details:
3						Name:
						Contact details:
4						Name:
						Contact details:
5						Name:
						Contact details:

 Signature
 Print name:
 On behalf of the tenderer (duly authorised)

 Date

Schedule F.13D - 2.2.1.1.8.2 Evidence to Functionality Requirement – Previous Implementation Project Size

Tenderers must list completed projects involving Identity Lifecycle Management (ILM) solutions, including Identity Governance and Administration (IGA), Single Sign-On (SSO), Privileged Access Management (PAM), and/or Identity Proofing solutions. Tenderers must specify the name of the client organisations, the solution/s provided, the scale of previously implemented projects by specifying the number of users supported and the implementation dates and duration of each project. The tenderer must also provide reference contact details for verification purposes.

No.	CLIENT	SOLUTION/S PROVIDED	NUMBER OF SYSTEM USERS	DATE FROM	DATE TO	DURATION	PROJECT REFERENCE (Name, Active contact details)
1							Name:
							Contact details:
2							Name:
							Contact details:
3							Name:
							Contact details:
4							Name:
							Contact details:
5							Name:
							Contact details:

 Signature
 Print name:
 On behalf of the tenderer (duly authorised)

 Date

Schedule F.13E - 2.2.1.1.8.3 Evidence to Functionality Requirement– Types of ILM solutions implemented

Tenderers must indicate the number of different ILM solution types they have successfully implemented, specifically across the following categories: IGA, PAM and Identity Proofing. The tenderer must also provide reference contact details for verification purposes.

No.	CLIENT	TYPE OF SOLUTION/S PROVIDED (IGA, PAM or Identity Proofing)	DATE FROM	DATE TO	DURATION	PROJECT REFERENCE (Name, Active contact details)
1						Name: Contact details:
2						Name: Contact details:
3						Name: Contact details:
4						Name: Contact details:
5						Name: Contact details:

Signature
Print name:
On behalf of the tenderer (duly authorised)

Date

Schedule F.13F - 2.2.1.1.6 Requirements for IGA

The Tenderer must provide sufficient and verifiable evidence for each requirement to demonstrate compliance. Acceptable evidence may include, but is not limited to, supplier or product information sheets or official vendor documentation or recorded video demonstrations or walkthroughs.

No.	Category	Requirement	Evidence submitted (specify document/file name)	Reference: Page no. or Time stamp in video
1.	Identity Lifecycle	Integration with authoritative HR sources (SAP SuccessFactors) for onboarding, extended leave, termination, conversions		
2.	Identity Lifecycle	Joiners, movers and leavers in SAP, Microsoft AD, Microsoft Entra ID		
3.	Identity Lifecycle	Enforcement of account activation only on start date		
4.	Identity Lifecycle	Suspension, reactivation, disable, delete accounts		
5.	Identity Lifecycle	Continuous account reconciliation of user accounts in target systems		
6.	Access Governance	Support Role-Based Access Control (RBAC)		
7.	Access Governance	Support Segregation of Duties (SoD).		
8.	Workflow	Automated notifications & credential delivery		
9.	Workflow	Escalation workflows (at minimum 2 levels)		
10.	Workflow	Emergency suspension workflows with HR approval		

TENDER NO: 252S/2025/26

No.	Category	Requirement	Evidence submitted (specify document/file name)	Reference: Page no. or Time stamp in video
11.	Security	Support for SAML 2.0, OAuth/OAuth2, OIDC		
12.	External Users	Management via Microsoft Entra External ID		
13.	Reporting	Audit & reporting dashboards		

Signature
Print name:
On behalf of the tenderer (duly authorised)

Date

Schedule F.13G - 2.2.1.1.7 Requirements for (Privilege Access Management) PAM

The Tenderer must provide sufficient and verifiable evidence for each requirement to demonstrate compliance. Acceptable evidence may include, but is not limited to, supplier or product information sheets or official vendor documentation or recorded video demonstrations or walkthroughs.

No.	Category	Requirement	Evidence submitted (specify document/file name)	Reference: Page no. or Time stamp in video
1.	Architecture & Integration	Discovery and secure storage of SSH keys		
2.	Architecture & Integration	SSO + MFA authentication support (Microsoft Entra ID Primary IDP)		
3.	Architecture & Integration	Privileged account discovery across windows and Linux		
4.	General Security	Must store all passwords in encrypted format (AES-256 or equivalent).		
5.	General Security	Must enforce one-time passwords and privileged account security best practices.		
6.	General Security	Must provide accountability and monitoring of shared accounts.		
7.	Cloud & Mobile	Must support password check-in/check-out via mobile devices.		
8.	Cloud & Mobile	Must integrate with cloud identity stores and ticketing systems.		
9.	Cloud & Mobile	Must monitor privileged activity in cloud environments and alert on suspicious behaviour.		
10.	Auditing & Reporting	Must produce audit logs capturing all activities and responsible parties.		

TENDER NO: 252S/2025/26

No.	Category	Requirement	Evidence submitted (specify document/file name)	Reference: Page no. or Time stamp in video
11.	Auditing & Reporting	Must log successful/failed authentications, account management, password changes, and lockouts.		
12.	Auditing & Reporting	Must prevent log manipulation or deletion.		
13.	Performance & Availability	Must support high availability with 99.95% uptime.		
14.	Usability	Must provide GUI-based administration console.		
15.	Usability	Must support custom branding and localization.		
16.	Usability	Must support standard browsers and bulk data import.		
17.	Privileged Password Management	Must support automatic password rotation and reset after usage.		
18.	Privileged Password Management	Must override manual password changes in target systems		
19.	Privileged Session Management	Must secure session connection, maintenance, and termination.		
20.	Privileged Session Management	Must support MFA authentication for administrators.		
21.	Privileged Session Management	Must enforce automatic logout after inactivity.		
22.	Privileged Session Management	Must support session recording, monitoring, and multi-user session sharing.		
23.	Privilege Escalation	Must support least privilege enforcement with seamless elevation of applications.		

TENDER NO: 252S/2025/26

No.	Category	Requirement	Evidence submitted (specify document/file name)	Reference: Page no. or Time stamp in video
24.	Privilege Escalation	Must provide granular application control and risk-based privilege assignment.		
25.	Privilege Escalation	Must support break-glass feature for emergency escalation.		
26.	Privilege Escalation	Must support policy creation and enforcement.		
27.	System Administration & Role Management	Must support RBAC with distinct roles (User, Admin, Auditor).		
28.	System Administration & Role Management	Must support lifecycle management of privileged accounts (create, update, delete).		
29.	System Administration & Role Management	Must lock accounts after failed login attempts.		
30.	System Administration & Role Management	Must prevent orphaned accounts.		

 Signature
 Print name:
 On behalf of the tenderer (duly authorised)

 Date

Schedule F.13H – On-premise infrastructure and software requirements for PAM

Tenderers are to complete the tables below with all on-premise infrastructure and software requirements for PAM.

INFRASTRUCTURE REQUIREMENTS FOR PAM

No.	Item Name	Model	Description	Quantity
1.				
2.				
3.				
4.				
5.				

SOFTWARE REQUIREMENTS FOR PAM

No.	Item Name	Version	Description	Quantity
1.				
2.				
3.				
4.				
5.				

Signature
Print name:
On behalf of the tenderer (duly authorised)

Date

Schedule F.13I – Optional items

Tenderers to clearly list and describe the details of all optional items priced in Tables A.7, B.7, and C.7 of the C.4 Price Schedule, including the item description.

Tenderers may add rows to the tables below where required.

IGA OPTIONAL ITEMS

	Item Name	Model	Description
1.			
2.			
3.			
4.			
5.			

PAM OPTIONAL ITEMS

	Item Name	Model	Description
1.			
2.			
3.			
4.			
5.			

IDENTITY PROOFING OPTIONAL ITEMS

	Item Name	Model	Description
1.			
2.			
3.			
4.			
5.			

 Signature
 Print name:
 On behalf of the tenderer (duly authorised)

 Date

Schedule F.14: Appeal Application

ANNEXURE 'A'

OFFICIAL RECEIPT
(Valid only if printed
by official cash
receiving machine)

IRISITI ESESIKWENI
(Isemthethweni kuphela
xa ishicilelwe
ngumatshini wokukhupa
irisiti osesikweni.)

AMPTELIKE KWITANSIE
(Geldig alleenlik indien deur
amptelike kontantvangs
masjien gedruk.)

GL DATA CAPTURE RECEIPT
(CASHIER TO RETAIN A COPY)

RECEIPT NO: _____

DATE: _____

SAP GL:

8 1 0 1 0 0

PROFIT CENTRE:

1 3 0 5 0 0 0 1

NAME/COMPANY NAME:

AMOUNT:

R 3 0 0 - 0 0

SERVICE DEPARTMENT DETAILS-

DEPARTMENT: LEGAL SERVICES: APPEALS UNIT

EMAIL: MSA.Appeals@capetown.gov.za

OFFICIAL RECEIPT
(Valid only if printed
by official cash
receiving machine)

IRISITI ESESIKWENI
(Isemthethweni kuphela
xa ishicilelwe
ngumatshini wokukhupa
irisiti osesikweni.)

AMPTELIKE KWITANSIE
(Geldig alleenlik indien deur
amptelike kontantvangs
masjien gedruk.)

GL DATA CAPTURE RECEIPT
(CASHIER TO RETAIN A COPY)

RECEIPT NO: _____

DATE: _____

SAP GL:

8 1 0 1 0 0

PROFIT CENTRE:

1 3 0 5 0 0 0 1

NAME/COMPANY NAME:

AMOUNT:

R 3 0 0 - 0 0

SERVICE DEPARTMENT DETAILS-

DEPARTMENT: LEGAL SERVICES: APPEALS UNIT

EMAIL: MSA.Appeals@capetown.gov.za

CIVIC CENTRE IZIKO LOLUNTU BURGERSENTRUM

12 HERTZOG BOULEVARD CAPE TOWN 8001 P O BOX 298 CAPE TOWN 8000
www.capetown.gov.za

Making progress possible. Together.

Annexure G – CCT Standards

IS&T Standards

G.1.1 Introduction

This schedule provides Tenderers with technical information regarding the City's current IT environment. It also provides the City's compulsory Architectural standards for the proposed solution.

G.1.2 Section A: General Architectural Standards

For the current City of Cape Town's Information Technology Environment three of the largest technology decisions taken by the City of Cape Town are as follows:

1. SAP for structured business processes which covers the City's back-office systems.
2. Microsoft for unstructured business processes which covers the standardisation of the desktops and backend servers on Microsoft technology
3. Esri for Spatial, which covers the implementation of ArcGIS Enterprise Environment desktop and backend servers.

The table below contains all CCT landscape details that supports our core and unstructured business processes. The versions specified can be regarded as the lowest version listed and could be higher as newer versions are released and implemented.

Table G.1.1 CCT Landscape Details

Technology Domain	Software Vendor	Current Standard Minimum	Status
Anti-virus software	Microsoft	Microsoft Defender for Endpoint as the minimum standard	Current
		Microsoft Defender for Servers	Current
Authorisation and Authentication	ESRI	Named User Authentication 10.7.1	Upgrading (no new requirements)
		Named User Authentication 11.3.0	Current
	Microsoft	Microsoft Active Directory Services (Microsoft Server 2012)	Current
	SAP	SAP ABAP NetWeaver Authorisation	Current
		SAP Business Objects Authentication	Current
		SAP Cloud Identity Authentication & Authorisation	Current
		SAP HANA Enterprise Authentication & Authorisation	Current
Cybersecurity, Fixed Networks Security	Citrix	Citrix NetScaler	Current
	Palo Alto	Palo Alto	Current
Database	ESRI	ArcGIS geodatabase version 10.7.1	Upgrading (no new requirements)
	Microsoft	MS SQL 2019	Current
	Open Source	MariaDB 10 (minimum)	Current
	Oracle	Oracle 19C	Current
	SAP	SAP HANA 2.0 SP03	Current
Front End Services and Endpoint computing	ESRI	ArcGIS Pro 2.92 (minimum standard)	Current
		ArcMap 10.7.1 Suite- ArcGIS System getting upgraded to 11.3 that is due for completion in July 2025.	Upgrading (no new requirements)
		ArcMap 11.3 Suite- ArcGIS System	Current

TENDER NO: 252S/2025/26

		Exchange Online	Current
		Microsoft 365	Current
		MS Edge Chromium as the minimum standard browser	Current
		Office 365	Current
		SharePoint 2016	Upgrading (no new requirements)
		Microsoft Teams	Current
		Windows 10 64-bit Professional – changing to Windows 11 in the coming years through the CAR Project.	Upgrading (no new requirements)
		Windows 11	Current
	SAP	SAP GUI 8.50 (minimum standard)	Current
		SAP Netweaver 7.5	Current
Middleware / Integration	ESRI	ArcGIS API for JavaScript 3.x/4.x	Current
		ArcGIS Desktop 10.7.1 AddIns	Current
		ArcGIS Pro SDK AddIns	Current
		ArcGIS System getting upgraded to 11.3 that is due for completion in July 2025.	Current
		ArcObjects C# SDK 10.7.1	Upgrading (no new requirements)
		Esri Mediator – Integration of PVC objects with SAP LUM	Current
	Microsoft	ASP.NET, MVC Web API, WCF Web Services (WDSL & JSON/XML REST)	Current
	None	WCF	Current
		Web API	Current
	SAP	GEO.e – Integration of Transport assets with SAP PM and FI	Current
		GIS iSAP Portal	Current
		SAP Process Orchestration NetWeaver 7.5 (minimum standard)	Current
Mobile field devices	Google (Open Source)	Android 10 (and above is not supported at present)	Current
		Android 4.4.4 operating system (minimum standard)	Current
		Angular 1 (EPIC)	Upgrading
		Angular 8 (EPIC)	Upgrading
		Angular 19 and above	Current
	SAP	Agentry	Current
		FIORI	Current
		SAP Afaria 7 mobile management system (minimum standard)	Current
		UI5	Current
Non-SAP Applications and Databases on VM	ESRI	ArcGIS 10.7.1	Upgrading (no new requirements)
		ArcGIS 11.3.0	Future
Operating System	ESRI	ArcGIS 10.7.1	Upgrading (no new requirements)
		ArcGIS 11.3.0	Future
	Microsoft	Microsoft Windows Server 2019	Current
	Open Source	RedHat Enterprise Linux (RHEL) 7.5	Current

		SUSE Linux Enterprise Server 12 SP4	Current
	SAP	SUSE Linux Enterprise Server 15	Current
Portal / Web Hosting	ESRI	ArcGIS Portal Version 10.7.1 - ArcGIS System getting upgraded to 11.3 that is due for completion in July 2025.	Current
	Microsoft	Windows 2019+ Server Running IIS 8.5 as the minimum standard	Current
	None	HTTPS	Current
	Open Source	Apache 2.4 (minimum)	Current
		Tomcat 8.5 (minimum)	Current
	SAP	SAP ABAP NetWeaver Internet Communication Framework (Rest, ODATA, SOAP)	Current
		SAP Java NetWeaver Portal	Current
Program Development	ESRI	ArcGIS API for JavaScript 3.x/4.x	Current
		ArcGIS Pro SDK,	Current
		ArcGIS System getting upgraded to 11.3 that is due for completion in July 2025.	Current
		ArcObjects C# SDK 10.7.1	Upgrading (no new requirements)
	Microsoft	.NET Framework 4.8 (minimum standard)	Current
	Google (Open Source)	Angular 8.2.14 and above Ionic 5 and above	Current
	None	REST	Current
		WCF and Web API Services,	Current
	Oracle (Open Source)	OpenJDK	Current
		JavaScript	Current
	SAP	SAP ABAP NetWeaver 7.4	Current
		SAP Business Objects 4.n	Current
		SAP HANA 2.0 Enterprise Platform	Current
	Records Management	SAP	Public Sector Records Management SAP NetWeaver 7.4
Security and Business Continuity	AppViewX	AppViewX CERT+ for Non-MS certificates and lifecycle management	Current
	Cohesity / Veritas	Cohesity Alta SAAS Protection (ASP)	Current
	ESRI	ArcGIS version 10.7.1 - ArcGIS System getting upgraded to 11.3 that is due for completion in July 2025.	Upgrading (no new requirements)
	IBM	IBM tape libraries for long term data retention	Current
	Microsoft	Defender for Office attack simulation and training	Current
		Microsoft Active Directory Certificate Services (ADCS) 2022	Current
		Microsoft Defender for Cloud	Current
		Microsoft Defender for Cloud Apps	Current
		Microsoft Purview Information Protection	Current
	Tenable	Tenable.IO (aka Tenable Vulnerability Management for WAS scans)	Current
		Tenable.SC for vulnerability management	Current
	Veritas	Veritas Flex backup appliances for disk based backups	Current
		Veritas NetBackup 10.1	Current
	Veritas / Cohesity	Veritas Access appliances for long term data retention	Current

Server Management	ESRI	ArcGIS 10.7.1	Upgrading (no new requirements)
		ArcGIS 11.3.0	Future
	Microsoft	System Centre Suite 2016	Current
	SAP	SAP Solution Manager 7.2	Current
Server Virtual Machines	IBM	IBM Power Series 10 Virtual Machine	Current
	Microsoft	Microsoft Hyper -V	Current
	Oracle	Oracle Virtualbox 5 (minimum)	Current
Integration Methods	File Transfer	FTPS	Current
	Email	POP3 SMTP IMAP COAP	Current
	Rest SOAP	HTTPS/1 HTTPS/2 HTTPS/3 Web Sockets	Current
	Message Queue Pub-Sub	Kafka Protocol AMQP ZMQ MQTT Active MQ	Current
	Data Transfer	ODBC Oracle JDBC	Current
	Security Protocols	LDAPS OAuth 2.0 Open ID Connect (OIDC)	Current
	Runtime	Only the Open components of the Java Platform SE/EE must be used eg Open JDK	Current
	Spatial	GeoJSON	Current

The table below contains the Current SAP Solutions SAP instances to reflect the version and Service Pack details.

Table G.1.2 CCT Current SAP Solutions Versions and Service Pack Details

Technology Domain	Product Instances	Version Details	SP/Level
SAP- Enterprise Resource Planning	SAP ECC6.0	<ul style="list-style-type: none"> SAP NetWeaver 7.4, EHP7 for SAP ERP 6.0 	<ul style="list-style-type: none"> SP29 SP26
	PSRM	<ul style="list-style-type: none"> SAP NetWeaver 7.5 	<ul style="list-style-type: none"> SP 24
	Corp CRM	<ul style="list-style-type: none"> SAP NetWeaver 7.5, EHP4 for SAP CRM 7.0 	<ul style="list-style-type: none"> SP 22 SP 17
	EPIC CRM	<ul style="list-style-type: none"> SAP NetWeaver 7.5 EHP4 for SAP CRM 7.0 	<ul style="list-style-type: none"> SP28 SP21
	BW	<ul style="list-style-type: none"> SAP BPC 11.1, FOR SAP BW/4HANA BW4HANA 	<ul style="list-style-type: none"> SP12 SP09

G.1.3 Minimum Network Standards

The City of Cape Town's minimum standards are defined as follows:

- a. The City's network is spread over a wide Metropolitan Area (MAN) mainly configured to run the Multi-Protocol Label Switching (MPLS) for fast data packet switching and transmission.
- b. Desktops typically have a 100-Mbps Local Area Network (LAN) connection, while the Wide Area Network (WAN) connections vary between 1-Gbps at the access layer to 10Gbps towards the distribution and network Core Layers.
- c. The current minimum bandwidth for a service provider leased connection is 20-Mbps and a minimum connection for a self-provided link is 1-Gbps for WAN links.
- d. Servers in the Datacentres are linked to a minimum of 1 Gbps of connectivity and varying to 10Gbps with Data Centre distribution @ 40Gbps and the Data Core @ 400-Gbps.

G.1.4 Minimum Desktop Hardware Standards

The City of Cape Town's minimum desktop hardware specifications are defined as per the table below:

Table G.1.3 CCT Desktop Hardware Standards

Component	Standard
Processor	Intel® Core™ i5-8500
Memory	8GB
Chip Set	Q370 (Latest Intel AMT 9.0 with full Intel® vPro™ manageability)
Windows Operating System	Windows 11 Professional Edition
Hard Drive	320GB HDD
Graphics	Intel HD 4600
Memory Slots	2

G.1.5 Mandatory and Compulsory Standards

The City of Cape Town's Information Systems and Technology (IS&T) department identified IT architecture standards that MUST be complied with. These mandatory standards are defined as follows:

- a. IP protocol only on the network.
- b. The use of Secure Transport Layer Security (TLS) version 1.2 between all application components.
- c. Encryption of all data in transit which has been classified as confidential, sensitive and personal identifiable information.
- d. Separate database and application server architecture.
- e. ODBC or OLEDB connections between applications and databases.
- f. Full relational database design, using stored procedures.
- g. All DLLs must be wrapped as COM+ objects (preferably written in .NET).
- h. Minimum requirement .Net Framework to be used version 4.7.1 in order to fully support TLS version 1.2.
- i. Scheduled events via DTS on SQL Server.
- j. Application security (i.e. user accounts) at the application or database level (not at the OS level).
- k. Applications and Databases hosted on Virtual Machine (VM) Servers created using MS Hyper-V (only).
- l. Solution must function within a Microsoft Managed Environment.
- m. PC thick clients must not function requiring administrative rights.
- n. PC thick clients must be packable and deployable across a network using System Centre

Configuration Manager (SCCM) to locked-down managed personal computers.

- o. Solution interfaces with SAP must be SAP architectural compliant (preferably certified).
- p. All confidential data must be encrypted and comply with POPIA/GDPR standards where required.
- q. No direct connections to the internet will be permitted. In the case where a web application needs access to the internet it will only be permitted via an HTTPS proxy.
- r. Outbound internet connections allowed via proxy only on HTTPS on port 443.
- s. Webserver Software (Tomcat/Apache etc.) must have all vendor provided security patches to known CVEs applied.
- t. All open source components / dependencies used by applications must comply will all/if any licensing requirements.
- u. Industry IT governance and best practises must be adhered to i.e. COBIT, Microsoft Technet etc.
- v. The City of Cape Town's IS&T password management Standard Operating Procedure to be adhered to where applicable.
- w. The City of Cape Town's IS&T Network Access Standard Operating Procedure to be adhered to where applicable.
- x. Ensure that industry best practises are followed regards to general Change and/or User Management processes.
- y. Only the Open components of the Java Platform SE/EE must be used e.g. OpenJDK or licensing must be provided by the service provider.

G.1.6 Optional Preferred Standards

The City of Cape Town's Information Systems and Technology (IS&T) department identified IT architecture standards that is optional and preferred standards. These preferred standards are defined as follows:

- a. Application Solutions hosted on Microsoft Platforms.
- b. Web applications rather than thick client/server applications.
- c. If thick client applications are used, these needs to be packaged in the Microsoft Installer format (MSI).
- d. Application architecture to be modular, and –tiered.
- e. Version control to be used for all application layers, and release management to include detailed release notes.
- f. The ability to co-exist with other 3rd party applications on the same hardware.
- g. Application solutions not hosted on Microsoft platforms but on platforms such as Linux will be reviewed and considered based on the proposal put forward and as it complies with the requirements above.
- h. Hardware, Application, Data, Web services and any form of license verification and authentication must be hosted and conducted On Premises.
- i. Java supported is per the following:
- j. Primary - 100% Open JDK free version as latest as possible.
- k. Tertiary - Only <1% devices to contain commercial Java flavour / Run Time (Oracle or any other commercial provider) vendor must submit as a line item e.g. Library application.
- l. Java supported is per the following:
- m. The City of Cape Town's preference is to use the latest Open JDK free version. At present, the City of Cape Town has Open JRE xxx installed on all windows machines in the path \\..... The Tenderer must be aware that the City of Cape Town will continually update the version of Open JDK to keep its cyber security posture up to date. As a supplier you are expected to do the same and the City of Cape Town will not be liable if you fall behind our Open JRE version levels.
- n. Alternately, any commercial Java / Run Time (be it Oracle or any other commercial provider) can be used, as long as the vendor provides this commercial version as part of the cost of its tender submission. The onus is on the vendor to continually update their commercial version of Java in order to ensure that the City of Cape Town keeps its cyber security posture up to date. Any negative

audit findings will be for the supplier account to remedy.

G.1.7 Unsupported Standards

The City of Cape Town's Information Systems and Technology (IS&T) department identified IT architecture standards that are EXPLICITLY NOT SUPPORTED. These standards are defined as follows:

- a. Active X Controls – the managed desktop environment does not permit these.
- b. Mapped Network Drives or UNC paths between workstations and application servers.
- c. Mapped Network Drives between application/web/database servers.
- d. Mapped Network Drives or UNC paths between workstations.
- e. IP addressing - use DNS addressing instead.
- f. Application and database on the same server.
- g. Microsoft Access developed applications local or on a server.
- h. Applications written in such a manner whereby usernames and password are embedded in the application code.
- i. Thin client solutions such RDS and Terminal Servicer.
- j. Oracle Java JDK or SE not supported.

CCT Data Access Specifications

G.2.1 Introduction

This schedule provides prospective Tenderers with technical CCT Data Strategy specifications.

The Data Strategy specifications must be read in conjunction with the CCT Information Technology (IT) standards and in itself cannot be deemed as the exclusive standards for the City.

G.2.2 Specifications

For Secured Network Accessible End Points to Production data the expectation is:

- a. Production data will be available via a network accessible programmatic interface that is conformant to at least one of the following:

Paradigm	Protocols	Serialisation/Data Formats
REST SOAP	HTTP/1 (IETF Datatracker - RFC7230)	JSON (IETF Datatracker - RFC8259) XML (W3 - Version 1.0, 1.1)
OData (v4.01 or greater)	HTTP/2 (IETF Datatracker - RFC7540)	YAML (YAML - Version 1.2)
GraphQL (October 2021)	HTTP/3 (draft-ietf-quic-http-34) WebSockets (RFC6455)	Protocol Buffer (Proto3 – Version 3.0) CAP'N Proto (capnp – Version 1.0)
	COAP (IETF Datatracker - RFC7252)	

- b. Provide Application Programming Interface (API) documentation that completely describe the API's functionality covering the following:
 - I. guides, tutorials, examples and use cases;
 - II. encouraged – capturing the API specification in a formal specification languages, such as the OpenAPI standards (<https://www.openapis.org/>) or TypeSpec (<https://typespec.io/>).
- c. The APIs should make use of a single, standard CCT authentication and permission management regime, making use of multi-factor authentication where possible.
- d. The APIs should be accessible by either a system or human user.