



KAAP AGULHAS MUNISIPALITEIT  
CAPE AGULHAS MUNICIPALITY  
U MASIPALA WASECAPE AGULHAS

**TENDER: ICT SUPPORT SERVICES AND  
LICENSING FOR A PERIOD OF 3 YEARS**

**SCM41/2025/26**

<b>BIDDERS NAME:</b>	_____
<b>CONTACT NUMBERS</b>	<b>Phone:</b>
<b>BBBEE STATUS LEVEL</b>	
<b>CSD REGISTRATION NR</b>	<b>MAAA</b>
<b>BID AMOUNT:</b>	<b>R</b> _____ (VAT inclusive)

<b>1. For Office Use</b>	<b>2. OFFICIAL STAMP</b>
<b>Official 1:</b> .....	
<b>Official 2:</b> .....	

NO.	DESCRIPTION	PAGE NUMBERS
1	Checklist	3
2	Advert	4
3	Invitation to Bid <b>CAMBD 1 (Compulsory Returnable Document)</b>	5 - 6
4	Specification / Terms of reference	7 – 41
5	Annexure B – Technical Evaluation	42 – 59
6	Pricing schedules	60 – 79
7	Compulsory Conditions	80
8	Tax Compliance Status Pin Requirements <b>CAMBD 2 (Compulsory Returnable Document)</b>	81 – 82
9	Authority of Signatory ( <b>Schedule 1 A (Compulsory Returnable Document)</b> )	83 – 84
10	Compulsory Enterprise Questionnaire ( <b>Schedule 1B (Compulsory Returnable Document)</b> )	85
11	Documents of Incorporation ( <b>Schedule 1C (Compulsory Returnable Document)</b> )	86
12	Payment of Municipal Accounts ( <b>Schedule 1D (Compulsory Returnable Document)</b> )	87– 88
13	Broad-Based Black Economic Empowerment (B-BBEE) Status Level Certificates ( <b>Schedule 1D (Compulsory Returnable Document)</b> )	89 – 90
14	Work satisfactorily carried out by the tenderer ( <b>Schedule 1F (Compulsory Returnable Document)</b> )	91-92
15	Special Condition	93– 96
16	Form of Acceptance & Contract Data	97 – 99
17	General Conditions of Contract	100– 105
18	Declaration of Interest <b>CAMBD 4 (Compulsory Returnable Document)</b>	106 – 109
19	Declaration For Procurement Above R10 Million (All Applicable Taxes Included <b>CAMBD 4 (Compulsory Returnable Document)</b> )	110-111
20	Procurement Points Claim Forms in terms of the Preferential Procurement Regulations 2001. <b>CAMBD 6.1 (Compulsory Returnable Document)</b>	112– 116
21	Contract Rendering of Services <b>CAMBD 7.2 (Compulsory Returnable Document)</b>	117 – 118
22	Declaration of Bidder's Past Supply Chain Management Practices <b>CAMBD 8 (Compulsory Returnable Document)</b>	119– 120
23	Certificate of Independent Bid Determination <b>CAMBD 9 (Compulsory Returnable Document)</b>	121 – 123

#### CHECK LIST FOR COMPLETENESS OF BID DOCUMENT

The bidder **MUST ENSURE** that the following checklist is completed, that the necessary documentation is attached to this bid document and that all declarations are signed:

1.	Completed page containing the details of bidder	Yes	No
2.	Specifications & Pricing Schedules - Is the form duly completed and signed?	Yes	No
3.	(CAMBD 2) Are a Tax Compliance status pin attached?	Yes	No
4.	(Schedule 1 A) Authority of Signatory - Is the form duly completed and signed?	Yes	No
5.	(Schedule 1B) Enterprise Questionnaire -Is the form duly completed and signed?	Yes	No
6.	(Schedule 1C) Documents of Incorporation - Is the form duly completed and signed?	Yes	No
7.	(Schedule 1D) Payment of Municipal Accounts - Is the form duly completed and signed?	Yes	No
8.	(Schedule 1E) B-BBEE certificate - Is the form duly completed and signed? Is a <u>certified or an original certificate attached</u>	Yes	No
9.	(Schedule 1F) Schedule of work experience of tenderer- Is the form duly completed and signed?	Yes	No
10.	(Schedule 1G) Document/S to Prove the Company Is A Registered ICT Based Entity	Yes	No
11.	(Schedule 1H) Local I.T. Sales and Support Office (WESTERN CAPE) Is the proof attached?	Yes	No
12.	Schedule 1I) Letter from the "Brand House - Is the proof attached?	Yes	No
13.	Form of Offer - Is the form duly completed and signed?	Yes	No
14.	Contract data - Is the form duly completed and signed?	Yes	No
15.	(CAMBD 4) declaration of interest- Is the form duly completed and signed?	Yes	No
16.	(CAMBD 6.1) Preference points claimed- Is the form duly completed and signed?	Yes	No
17.	(CAMBD 8) Signed declaration of bidder's past supply chain management practices	Yes	No
18.	(CAMBD 9) Prohibition of Restrictive Practices be completed and signed.	Yes	No
19.	<b>All bids must be submitted in writing on the official forms (not re-typed).</b>	Yes	No
20.	Bidder <b>must</b> initial every page of this bid document.	Yes	No

## CERTIFICATION


I, THE UNDERSIGNED (FULL NAME) .....

**CERTIFY THAT THE INFORMATION FURNISHED ON THIS CHECK LIST IS TRUE AND CORRECT.**

Signed ..... Date .....

Name ..... Position .....

Tenderer .....

	<b>CAPE AGULHAS MUNICIPALITY</b>			
	<b>REQUEST FOR TENDERS</b>			
	<b>ADVERTISED ON</b>	<b>MUNICIPAL NOTICE BOARD; MUNICIPAL WEBSITE; NATIONAL TREASURY e-TENDER</b>		
	<b>TENDER NO:</b>	<b>SCM41/2025/26</b>		
<b>Tenders are hereby invited for:</b>	<b>ICT SUPPORT SERVICES AND LICENSING FOR A PERIOD OF 3 YEARS</b>			
<b>PUBLISHED DATE:</b>	<b>12 December 2025</b>	<b>CLOSING DATE:</b>	<b>13 February 2026</b>	
<b>CLOSING TIME:</b>	<b>No later than 12H00.</b> Tenders will be opened immediately thereafter, in public at the Cape Agulhas Municipality, 1 Dirkie Uys Street, Bredasdorp.			
<b>AVAILABILITY OF BID DOCUMENTS:</b>				
Tender documents are available from <b>Me G Koopman</b> at telephone number 028-425-5500 during office hours or email at <a href="mailto:geraldinek@capeagulhas.gov.za">geraldinek@capeagulhas.gov.za</a> .				
<b>Date Available:</b>	<b>12 December 2025</b>	<b>Non-refundable Fee:</b>	<b>R 0. 00</b>	
<b>BID RULES:</b>				
<ol style="list-style-type: none"> <li>Tenders are to be completed in accordance with the conditions and Tender rules contained in the Tender document.</li> <li>The Tender Document &amp; supporting documents must be placed in a sealed envelope and externally endorsed with: THE TENDER NUMBER; DESCRIPTION &amp; CLOSING DATE OF TENDER.</li> <li>Tender Documents must be deposited in the Tender Box, at Municipal Offices, 1 Dirkie Uys Street, Bredasdorp or posted to reach the Municipal Manager, Cape Agulhas Municipality, PO Box 51, Bredasdorp, 7280.</li> <li>Tenders may only be submitted on the Tender documentation issued by the Municipality.</li> <li>A Tax Compliance status pin as issued by the South African Revenue Service, must be submitted together with the tender.</li> <li>The two-stage bidding process will be followed in evaluating this tender. Firstly, it will be evaluated for functionality and thereafter for price and preference.</li> </ol>				
<ol style="list-style-type: none"> <li>The Cape Agulhas Municipality does not bind itself to accept the lowest or any tender and reserves the right to accept any tender, as it may deem expedient.</li> <li>Tenderers are required to be registered on the Accredited Supplier Database (CSD) from the website <a href="https://secure.csd.gov.za">https://secure.csd.gov.za</a></li> </ol>				
<b>Tenders shall be evaluated in terms of the Cape Agulhas Municipality Supply Chain Management Policy &amp; Preferential Procurement</b>		Suppliers may claim preference points in terms of the <b>80/20</b> . <b>Price:</b> 80 <b>Specific Goals: (20)</b> a) B-BBEE Status Level contributor: 10 b) Locality of Supplier: 10 <b>Total Points:</b> 100		
<b>Site Meeting / Information Session</b>		n/a		
		<b>Validity Period</b>		<b>90 days</b>
<b>ANY ENQUIRES REGARDING TECHNICAL INFORMATION MAY BE DIRECTED TO:</b>		<b>ANY ENQUIRES REGARDING THE QUOTING PROCEDURE MAY BE DIRECTED TO:</b>		
<b>Division</b>	<b>ICT</b>	<b>Division</b>	<b>Supply Chain Management</b>	
<b>Contact Person:</b>	<b>Mr Kevin Fourie</b>	<b>Contact Person:</b>	<b>Ms. G Koopman</b>	
<b>Tel:</b>	<b>e-mail Enquires Only</b>	<b>Tel:</b>	<b>e-mail Enquires Only</b>	
<b>E-mail:</b>	<a href="mailto:kevinf@capeagulhas.gov.za">kevinf@capeagulhas.gov.za</a>	<b>E-mail:</b>	<a href="mailto:geraldinek@capeagulhas.gov.za">geraldinek@capeagulhas.gov.za</a>	

**WP RABBETS**  
**MUNICIPAL MANAGER**  
**PO BOX 51**  
**BREDASDORP**  
**7280**

## PART A INVITATION TO BID

<b>YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE CAPE AGULHAS MUNICIPALITY</b>			
BID NUMBER:	SCM41/2025/26	CLOSING DATE:	13 February 2026
DESCRIPTION	ICT SUPPORT SERVICES AND LICENSING FOR A PERIOD OF 3 YEARS		
<b>THE SUCCESSFUL BIDDER WILL BE REQUIRED TO FILL IN AND SIGN A WRITTEN CONTRACT FORM (MBD7).</b>			

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

<b>CAPE AGULHAS MUNICIPALITY</b>
<b>1 DIRKIE UYS STREET</b>
<b>BREDASDORP</b>
<b>7280</b>

<b>SUPPLIER INFORMATION</b>			
NAME OF BIDDER			
POSTAL ADDRESS			
STREET ADDRESS			
TELEPHONE NUMBER	CODE	NUMBER	
CELLPHONE NUMBER			
FACSIMILE NUMBER	CODE	NUMBER	
E-MAIL ADDRESS			
VAT REGISTRATION NUMBER			
TAX COMPLIANCE STATUS	TCS PIN:	OR	CSD No:
B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE [TICK APPLICABLE BOX]	<input type="checkbox"/> Yes <input type="checkbox"/> No	B-BBEE STATUS LEVEL SWORN AFFIDAVIT	<input type="checkbox"/> Yes <input type="checkbox"/> No

**[A B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE/ SWORN AFFIDAVIT (FOR EMES & QSEs) MUST BE SUBMITTED IN ORDER TO QUALIFY FOR PREFERENCE POINTS FOR B-BBEE]**

ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES /WORKS OFFERED?	<input type="checkbox"/> Yes <input type="checkbox"/> No [IF YES ENCLOSE PROOF]	ARE YOU A FOREIGN BASED SUPPLIER FOR THE GOODS /SERVICES /WORKS OFFERED?	<input type="checkbox"/> Yes <input type="checkbox"/> No [IF YES, ANSWER PART B:3]
TOTAL NUMBER OF ITEMS OFFERED		TOTAL BID PRICE	R
SIGNATURE OF BIDDER	.....	DATE	
CAPAMUNICIPALITY UNDER WHICH THIS BID IS SIGNED			

<b>BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO:</b>		<b>TECHNICAL INFORMATION MAY BE DIRECTED TO:</b>	
DEPARTMENT	FINANCE: SCM	DEPARTMENT	ICT
CONTACT PERSON	Geraldine Koopman	CONTACT PERSON	Mr Kevin Fourie
TELEPHONE NUMBER	028 425 5500	TELEPHONE NUMBER	028 425 5500
E-MAIL ADDRESS	<a href="mailto:geraldinek@capeagulhas.gov.za">geraldinek@capeagulhas.gov.za</a>	E-MAIL ADDRESS	<a href="mailto:kevinf@capeagulhas.gov.za">kevinf@capeagulhas.gov.za</a>

## **PART B**

### **TERMS AND CONDITIONS FOR BIDDING**

#### **1. BID SUBMISSION:**

- 1.1. BIDS MUST BE DELIVERED BY THE STIPULATED TIME TO THE CORRECT ADDRESS. LATE BIDS WILL NOT BE ACCEPTED FOR CONSIDERATION.
- 1.2. **ALL BIDS MUST BE SUBMITTED ON THE OFFICIAL FORMS PROVIDED– (NOT TO BE RE-TYPED) OR ONLINE**
- 1.3. THIS BID IS SUBJECT TO THE PREFERENTIAL PROCUREMENT POLICY FRAMEWORK ACT AND THE PREFERENTIAL PROCUREMENT REGULATIONS, 2022, THE GENERAL CONDITIONS OF CONTRACT (GCC) AND, IF APPLICABLE, ANY OTHER SPECIAL CONDITIONS OF CONTRACT.

#### **2. TAX COMPLIANCE REQUIREMENTS**

- 2.1 BIDDERS MUST ENSURE COMPLIANCE WITH THEIR TAX OBLIGATIONS.
- 2.2 BIDDERS ARE REQUIRED TO SUBMIT THEIR UNIQUE PERSONAL IDENTIFICATION NUMBER (PIN) ISSUED BY SARS TO ENABLE THE ORGAN OF STATE TO VIEW THE TAXPAYER'S PROFILE AND TAX STATUS.
- 2.3 APPLICATION FOR THE TAX COMPLIANCE STATUS (TCS) CERTIFICATE OR PIN MAY ALSO BE MADE VIA E-FILING. IN ORDER TO USE THIS PROVISION, TAXPAYERS WILL NEED TO REGISTER WITH SARS AS E-FILERS THROUGH THE WEBSITE WWW.SARS.GOV.ZA.
- 2.4 FOREIGN SUPPLIERS MUST COMPLETE THE PRE-AWARD QUESTIONNAIRE IN PART B:3.
- 2.5 BIDDERS MAY ALSO SUBMIT A PRINTED TCS CERTIFICATE TOGETHER WITH THE BID.
- 2.6 IN BIDS WHERE CONSORTIA / JOINT VENTURES / SUB-CONTRACTORS ARE INVOLVED; EACH PARTY MUST SUBMIT A SEPARATE TCS CERTIFICATE / PIN / CSD NUMBER.
- 2.7 WHERE NO TCS IS AVAILABLE BUT THE BIDDER IS REGISTERED ON THE CENTRAL SUPPLIER DATABASE (CSD), A CSD NUMBER MUST BE PROVIDED.

#### **3. QUESTIONNAIRE TO BIDDING FOREIGN SUPPLIERS**

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

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

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

SIGNATURE OF BIDDER: .....

CAPAMUNICIPALITY UNDER WHICH THIS BID IS SIGNED: .....

DATE: .....

## Contents

1	SCHEDULE A – SCOPE OF SERVICES.....	9
2	ICT PROFESSIONAL SUPPORT AGREEMENT .....	9
3	Support Fees .....	11
4	Security .....	12
4.1	Network security, management, monitoring, reporting and notifications services. ....	12
4.1.1	Network access policy system. ....	12
4.1.2	Cloud Assessment and Monitoring Tool .....	16
4.1.3	Cloud Application Activity & Security Monitoring .....	18
4.2	Compliance .....	19
4.2.1	Cyber Security Framework management tool .....	19
4.3	Dark Web monitoring .....	22
4.4	Security Audit.....	22
4.5	Security Awareness Training & Phishing Simulation Requirements.....	23
4.6	Vulnerability Scanning Tool .....	25
4.7	Penetration Testing.....	26
4.7.1	PROJECT BACKGROUND .....	26
4.7.2	PURPOSE .....	27
4.7.3	SCOPE OF WORK .....	27
4.7.4	PROJECT DESIGN .....	29
4.7.5	CONTRACT TERM .....	30
4.7.6	PROJECT MANAGEMENT ARRANGEMENTS .....	30
4.8	Security Operations Centre (SOC).....	30
4.8.1	SPECIFICATION OF REQUIREMENTS.....	30
4.8.2	Approach to the delivery of the SOC Managed Service.....	31
4.8.3	Technical Requirements of SOC Solution.....	31
4.8.4	Implementation/Project Take-on .....	34
4.9	SIEM, Log Management & Security Automation Requirements.....	34
4.10	IT Documentation & Knowledge Management Platform Requirements .....	35
4.11	Security Component Project Requirements .....	35
5	Monitoring, management, and Audit system.....	35
	SCHEDULE B – TECHNICAL EVALUATION .....	42
1	Organisational requirements .....	42
1.1	Company requirements .....	42
1.2	Support staff requirements .....	43

2	Network Access & Security Assessment Tool .....	45
3	Cloud Application Activity & Security Monitoring .....	46
4	Dark Web Monitoring .....	48
5	Security Awareness Training & Phishing Simulation Requirements .....	48
6	Penetration Testing functional requirements.....	50
7	Security Operations Centre (SOC).....	51
8	SIEM, Log Management & Security Automation Requirements.....	52
9	IT Documentation & Knowledge Management Platform Requirements .....	53
	SCHEDULE C – FUNCTIONAL REQUIREMENTS .....	56
1	Project approach and technical evaluation .....	56
2	The scoring of the tenderer’s experience will be as follows.....	59
3	Functionality Criteria evaluation.....	59
	SCHEDULE D - PRICING.....	60
1	Support Fees .....	61
2	Network access policy system. ....	64
3	Cloud assessment and monitoring tool .....	65
4	Cloud Application Activity & Security Monitoring .....	66
5	Compliance .....	67
5.1	Cyber Security Framework management tool .....	67
6	Dark Web monitoring .....	68
7	Security Audit.....	69
8	Security Awareness Training & Phishing Simulation Requirements .....	70
9	Vulnerability Scanning Tool .....	71
10	Penetration Testing.....	72
11	SIEM, Log Management & Security Automation Requirements.....	73
12	IT Documentation & Knowledge Management Platform Requirements .....	74
13	Security Operations Centre (SOC).....	75
14	Monitoring, management, and Audit system .....	76
15	Pricing Summarized .....	79



## ICT SUPPORT SERVICES AND LICENSING

### 1. SCHEDULE A – SCOPE OF SERVICES

- This tender is based on rates for the period of 36-months.
- Pricing will be used for evaluation purposes and is estimated based on current ICT network environment.

### 2. ICT PROFESSIONAL SUPPORT AGREEMENT

Cape Agulhas Municipality is awaiting bids on the supplying of ICT Systems / Software and services. These services are inclusive of a range of various ICT related services, and the successful bidder will become the ICT service provider as defined in this document for a term of 36 months starting 1 March 2026.

#### 1.1 SCOPE OF SERVICES – Services, Software & Support must include:

- On-site support – including Cyber Security support
- 24-hour response time
- Hardware Infrastructure
- Software Infrastructure (operating systems and the operation of core server/desktop productivity applications on quotation basis).
- Access and Authorization (user account and password help, application-level access problem determination, desktop/client security configuration support. E mail and Internet access support in liaison/conjunction with the relevant ISP or any other Service Provider
- Local area network design
- Wide area network design
- Campus area network design
- Metropolitan area network design
- Other types of network design as may be required.
- Network Infrastructure – Check and verify basic network connectivity. **Cabling, router and switch configurations are excluded.**
- Installation, setup and deployment of new equipment, systems and services.
- **The successful Tenderer** must take responsibility for carry-in and carryout of equipment that do not have on-site warranty against the SLA should it be required.
- Scheduled meetings/reports with nominated ICT personnel to review the SLA performance and usage.
- Governance  
*Services should include but not be limited the review of, and establishment of policies and procedures inclusive of the following existing:*
  - ICT policies and procedures
  - ICT Audits – Governance and security audits
  - ICT Disaster recovery plans
  - Enterprise Architecture
  - ICT Maintenance plan
  - ICT Strategy and implementation plans
  - Cyber security policies, procedures, strategies and plan development
  - Public Key Certificates
  - Mail certificates.
  - Web certificates
  - Wild card certificates

**In order to adhere to the Municipalities` policy “ICT Service Level Agreement Management Policy -**

**External Service Provider”** the Municipality views end user desktop and server support as a critical component to a client’s business. To achieve and maintain service delivery we have set a generic impact level analysis approach to our support.

**DEFINITIONS OF IMPACT LEVELS:**

**Impact Level 1**

Multiple users are directly affected.

Loss of function has a serious and immediate negative impact on the business. Furthermore, no temporary and workable alternative is available to carry on the disrupted activity.

**Impact Level 2**

Limited (two or less) users are directly affected.

A temporary and workable alternative is available to carry on the disrupted activity.

The disruption of activity/function may have some operational impact, but it is not highly critical.

**Impact Level 3**

New computer, server or system setup to replace an older but still operational.

It is a known fact that a system, or component, or software upgrade is required, but the computer is still functional.

Setup of computer peripherals, which has no critical impact on the daily activities of users.

**SERVICE RESPONSE TO EACH IMPACT LEVEL:**

**Response to Impact Level 1**

Upon receipt of service call to Help Desk, its staff must attempt to resolve the reported problem over the phone.

If the problem is not resolved immediately by the Help Desk, its staff must then immediately contact the Desktop Support Service staff via e mail and cell phone. The assignee of this service call will respond telephonically within one hour or less depending on the degree of emergency. Once the service assignee has assessed the situation, he/she will proceed to attempt remote procedure assistance. Should the situation still remain unresolved the tenderer will send a suitable technician to the site.

If the problem is not resolved by the assignee within four hours, the Help Desk staff will escalate the call to the next level by alerting the Coordinator of Desktop Support Service to the situation and the possible need for assistance and/or consultation. The targeted time for problem resolution is regarded as extremely urgent but dependent on mitigating circumstances like client approval, spare parts, equipment availability etc.

**Response to Impact Level 2**

The first response by an assignee from the Desktop Support Service staff must occur within the 4-hour window after the initial service call to the Help Desk, if the problem is not resolved over the phone immediately by the Help Desk staff. The maximum time targeted for problem resolution is within 24 hours (or 3 workdays) by the assignee after the initial service call to the Help Desk. If the problem is not resolved by the assignee within the allowed maximum time, the Help Desk staff must escalate the call to the next level by alerting the Coordinator of the Desktop Support Service to the situation and the possible need for assistance and/or consultation.

### **Response to Impact Level 3**

1. The first response by an assignee from the Desktop Support Service must occur within 4 hours after the initial service call to the Help Desk.
2. Subject to the client's approval, equipment and spare part availability, the specific targeted maximum time for problem resolution or service request is 5 working days (40 hours).
3. An e-mail reminder must be sent to the assignee of the Desktop Support Staff and its Coordinator at the end of day one after the initial service call to the Help Desk, regardless of if the problem or service request has been taken care of. The customer will be kept duly informed by the account manager of the status quo.
4. If the problem or service request has not been addressed in 5 working days after the initial service call to the Help Desk, this open ticket must be escalated to the attention of the Director of the successful company for his/her action.

### **OTHER INFORMATION:**

- Hours of operation of the Help Desk must be at least: 8:00 A.M. to 5:00 P.M., Monday to Friday.
- For after hour emergencies including weekends the Municipality must be provided with contact names and cell numbers.
- Users must be able to contact the Help Desk via telephone, voice mail, e-mail or ticketing system in person at any time including after hours.
- Such service calls should be automatically queued and handled in the sequence of their occurrence.
- The Help Desk must be responsible for assigning each unresolved service call ticket to a staff member of the Desktop Support Service and for logging and tracking of each assignment.
- The assignee of each service call ticket must inform the user through phone or e-mail of the status of the problem resolution. Server crash and software reloads must be done on a quotation basis and in accordance with the Municipalities' procurement policies.
- IT Support Call Logging procedure –must be clearly identified and communicated to the Municipality.

A username (which must be provided) is required when logging a call via email. Login details must be given to Municipal users via email, WhatsApp and/or SMS.

### **3. Support Fees**

ICT Support may be required from time to time covering the Scope of work and any other ICT related professional, security, audit or Governance support services, evaluations, or implementation plans.

In lieu of these requirements rates are required for these services.

*Ad hoc projects may be required from time to time to which the following will then apply:*

- (ii) The successful Tenderer must submit a quotation for approval before commencement of any chargeable service linked to the tendered amounts as per section above.

## **4. Security**

### **4.1 Network security, management, monitoring, reporting and notifications services.**

#### **4.1.1 Network access policy system.**

Cape Agulhas Municipality is awaiting a proposal on ICT security services, including best efforts detection, investigation, monitoring and remediation of misuse and abuse of network resources occurring behind the corporate firewall based upon agreement and implementation of a set of best practices security Policies and Procedures.

These monitoring Policies and Procedures should include but may not necessarily be limited to the following:

#### **Access Control Policies**

##### **1. Authorization of new Devices to be Added to Restricted Networks**

Restricted networks should be tightly controlled to conform to strict network change management policies and procedures. Implementing security controls and applying consistent policies can help protect the organization from these security threats. We need to receive an alert with recommended actions to be taken when new devices have been added to any network segment designated as restricted.

##### **2. Investigate Suspicious Logons by Users**

Computer user login attempts by a particular user that are made outside of normal time frame patterns or from an unusual location indicates behaviour consistent with unauthorized user access or malicious software. When this event is detected, we need to receive an email alert warning of the suspicious activity with recommended actions to be taken. It is possible that an account may have been compromised.

##### **3. Investigate Suspicious Logons to Computers**

Attempts to access a computer using login credentials not normally associated with that particular computer could point to unauthorized user access or use of malicious software. When this event is detected, we need to receive an email alert warning of the suspicious activity with recommended actions to be taken. In such an instance it is possible that an account may have been compromised.

##### **4. Strictly Control the Addition of Printers**

Network printers are vulnerable to security risks just like computers. Connecting to and printing from an unauthorized printer can lead to information loss. Anytime a new printer is found on the network, we need to receive an alert notifying us with recommended actions to be taken to ensure that it is authorized to prevent any potential threat.

##### **5. Restrict Access to Computers with specified roles viz, financial to Authorized Users**

Computers in the network that are used to transmit, process, or store accounting/financial information and other sensitive financial records should only be accessed by authorized users. Trying to prevent users from accessing these resources through group policies, restricted logons and other network "hardening" is best practice. However, we still need to know when unauthorized users attempt to access sensitive systems and login to one of these machines. We need to receive an email alert when unauthorized user attempts to login to one of these accounting/financial computers with recommended actions to be taken.

##### **6. Restrict Access to IT Admin Only Restricted Computers to IT Administrators**

Domain controllers, web servers, database servers, and mail servers should only be accessed by users who are IT Administrators. These devices are critical to the normal operation of the business. Trying to prevent users from accessing these resources through group policies, restricted logons and other network "hardening" is best practice. We need to receive an alert with recommended actions when a user who is not an IT Administrator attempts a login to a computer designated for only IT Administrator access.

##### **7. Restrict Access to Business Owner Type Computers to Authorized Users**

Computers in the network that are designated as "Business Owner Type Computers" may only be accessed by authorized users. These devices often contain confidential, privileged, and other private and sensitive records and should only be accessed by authorized users. Trying to prevent users from accessing these resources through group policies, restricted logons and other network "hardening" is best practice. We need receive an email alert with recommended actions when unauthorized users attempt to login to one of these computers that are designated as a "Business Owner Computer."

## **8. Restrict Access to Systems in the Cardholder Data Environment (CDE) to Authorized Users**

Cardholder Data Environment (CDE) system components that access, use, or maintain Cardholder Data. Only workforce members or business associates who have been authorized to have access to specified Cardholder Data, in accordance with the requirements set forth may access and work with the associated Cardholder Data. We need to receive email alerts with recommended actions to be taken when suspicious or potentially unauthorized users log into computer designated as containing Cardholder Data.

## **9. Restrict IT Administrative Access to a Minimum**

Administrator access rights to computers and other IT resources should be limited to users who have been authorized to this level of system access to perform their role. The Administrator account is the most powerful account on the network, holding the "keys" to the business infrastructure. We need to receive an alert with recommended actions to be taken after a user account has been provided with Administrator rights on the network or a new user has been created with administrator rights. This is to ensure we can verify authenticity of the user access level and minimize Administrator level access to the minimum number of people necessary.

## **10. Restrict Users that are Not Authorized to Log into Multiple Computer Systems**

Computer users, in general, are assigned a specific machine for use in performing their business duties. We need to identify users who should only log into a single computer. When a single desktop user logs into multiple computers, their behaviour is viewed as suspicious and should be investigated further. We need to start receiving email alerts with recommended actions to be taken when tagged users log into more than one computer.

## **11. Strictly Control the Addition of New Local Computer Administrators**

An important part of securing our network is managing the users and groups that have administrative access. When a user account is added to a computer and this account is assigned administrator rights, we need to receive an email alert with recommended actions.

## **12. Strictly Control the Addition of New Users to the Domain**

The addition of new users to the network should be strictly controlled. An important part of securing our network is managing the addition of new users. Any time a new user account has been identified as being added to the network, verify that the new account was authorized. We need to receive an email alert with recommended actions when a new user account has been added to the network.

## **13. Strictly Control the Removal of Users from the Domain**

The removal of users from the network is to be strictly controlled. Any time a user account has been identified as being removed from the network, we need to receive an email alert with recommended action when a user account has been removed from the network.

## **14. Strictly Control the Creation of New User Profiles**

User profiles are created when users access systems for the first time. The appearance of new user profiles indicates successful access to systems. Monitoring the creation of new profiles allows detection of access. Any time a new user profile has been identified as being added to the network we need to receive an email alert with recommended action.

## **Computer Policies**

## **15. Changes on Locked Down Computers should be Strictly Controlled.**

There are some computers in a network where we want to be alerted of any changes to the system that are significant. These can be important systems like Domain Controllers, Exchange Servers, or servers where we have strict change management. We need to receive email alerts with recommended actions of computers designated as "locked down" meaning they should not be tampered with.

## **16. Install Critical Patches for DMZ Computers within 30 Days**

Computers in the DMZ are highly susceptible to malicious attacks and software if left vulnerable due to critical patches not being applied on a timely basis. We need to receive an email alert with recommendations when a threat to a DMZ Computer, results from critical patches not being installed.

## **17. Install Critical Patches on Network Computers within 30 Days**

Computers on the network are highly susceptible to malicious attacks and software if left vulnerable due to critical patches not being applied on a timely basis. A patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes security vulnerabilities and other bugs to improve the usability or performance of the program. We need to receive an email alert arising from vulnerabilities that are a result of critical patches not being timely installed.

## **18. Restrict Internet Access for Computers that are Not Authorized to Access the Internet Directly**

Computers on a network should be prevented from having direct access to the Internet. These can be important systems like accounting systems, systems storing PII, or Cardholder Data, or computers used to perform other sensitive business functions. We need to receive an email alert with recommended actions if at any time designated computers can access the Internet directly and not via the authorized network and Firewall.

## **19. Strictly Control the Clearing of System and Audit Logs**

The clearing of logs can be used as a forensic countermeasure and should be strictly controlled. Only authorized personnel with a justifiable reason should ever clear event logs manually. Any clearing of an event log should be verified to determine if it was authorized. We need to receive an email alert with recommended action when any system or audit log is cleared.

## **20. Enable automatic screen lock on computers with sensitive information.**

Automatic screen lock should be enabled on all computers containing sensitive information to prevent unauthorized access. We need to receive an email alert with recommended action if there are devices with sensitive information that does not have the Automatic screen lock enabled.

## **21. Enable automatic screen lock for users with access to sensitive information.**

Automatic screen lock should be enabled on all computers accessed by users who have access to sensitive information. We need to receive an email alert with recommended action if there are users that have access to sensitive information that does not have the Automatic screen lock enabled on their device.

### **Data Security Policies**

## **22. Only store Personally Identifiable Information (PII) on systems marked as sensitive.**

Personally Identifiable Information (PII) should only be stored on systems specifically marked as containing sensitive information. These systems should have additional safeguards and controls to prevent unauthorized access. We need to receive an email alert with recommended action if there are any devices that are marked sensitive without the additional safeguards and controls in place. We need to receive an email alert with recommended action if there are any devices that are not marked as sensitive but has PII data stored on it.

## **23. Only store cardholder data on designated systems**

Cardholder Data should only be stored on systems specifically marked as part of the Cardholder Data Environment (CDE). These systems should have additional safeguards and controls to prevent unauthorized access.

We need to receive an email alert with recommended action if there are any devices that are marked sensitive without the additional safeguards and controls in place. We need to receive an email alert with recommended action if there are any devices that are not marked as sensitive but has Card Holder data stored on it.

## **24. Detect malicious software and potential security breaches (Breach Detection System)**

We currently have Sophos Central Intercept X Advanced for Endpoint. However, as an additional layer of security we require an independent scan to detect any possible malicious software and potential security breaches. If any detections are detected, we need to receive an email alert with recommended action.

### **Network Security Policies**

## **25. Detect Network Changes to Internal Networks**

Monitoring changes to a private network assist in identifying potential security concerns. Anytime a new device is connected to or disconnected from a network, we need to receive an email alert with recommendation notifying us of the potential rogue device connection or possible theft of equipment.

## **26. Detect Network Changes to Internal Wireless Networks**

Monitoring changes to a private wireless network assist in identifying potential security concerns. Anytime a new device is connected to or disconnected from a wireless network, we need to receive an email alert with recommendation notifying us of the potential rogue device connection or potential theft of equipment. Identified "guest" wireless networks should not generate alerts.

## **27. Only Connect to Authorized Wireless Networks**

Connections to "unauthorized" wireless networks may lead to data loss from unwanted information disclosure. Any time a user connects to a network using an "unauthorized" wireless connection, we need to receive an email alert with recommendation.

## **28. Remediate High Severity Internal Vulnerabilities Immediately (CVSS > 7.0)**

Any identified Internal Vulnerabilities assigned a CVSS Score of 7.0, or higher, represent potential high severity threats and should be remediated immediately. The Common Vulnerability Scoring System (CVSS) is an open industry standard for assessing the severity of computer system security vulnerabilities. CVSS assigns severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. Scores range from 0 to 10, with 10 being the most severe. When high severity internal vulnerabilities are found, we need to be notified with an email alert with recommendation to resolve.

## **29. Remediate Medium Severity Internal Vulnerabilities (CVSS > 4.0)**

Any identified Internal Vulnerabilities assigned a CVSS Score of 4.0, or higher, represent potential medium severity threats and should be remediated as soon as possible. The Common Vulnerability Scoring System (CVSS) is an open industry standard for assessing the severity of computer system security vulnerabilities. CVSS assigns severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. Scores range from 0 to 10, with 10 being the most severe. When medium severity internal vulnerabilities are found, we need to be notified with an email alert with recommendation to resolve.

## **30. Strictly control DNS on Locked Down Networks**

Changes in DNS entries in networks that are locked down should be strictly controlled. Additions may indicate unauthorized devices connecting to the network. Other changes may indicate other issues including theft and should be investigated. We need to be notified with an email alert with recommendation to resolve.

## **31. Strictly control changes to Group Policy**

Group Policies are used to configure computer and user settings. Due to their ability to affect the security settings throughout the network, any changes to Group Policy Objects (GPOs) should be strictly controlled. We need to be notified with an email alert with recommendation to resolve.

## **32. Strictly control changes to the Default Domain Policy**

The Default Domain Policy is applied to all computers and users in the domain by default. New computers and users will be assigned the Default Domain Policy until they are assigned specific policies. Any changes to the Default Domain Policy should be strictly controlled to prevent introducing security vulnerabilities. We need to be notified with an email alert with recommendation to resolve.

#### 4.1.2 Cloud Assessment and Monitoring Tool

Cape Agulhas Municipality is awaiting a proposal on Microsoft Cloud assessment and monitoring system as a service. This is required to manage and assess risk across our entire Microsoft Cloud Environment.

##### 1 The system should assess and document at least the following components:

- Microsoft 365 Cloud Services
  - Office 365
  - Teams
  - SharePoint
  - OneDrive (no need to scan file content)
  - Outlook/Exchange (no need scan email content)
- Microsoft Azure Cloud Services
  - Azure Active Directory

##### 2 Reporting

Reporting is required on at least the following areas is required through this system.

- Assessments on Azure AD

The Azure AD Detail Report must go through the entire Azure Active Directory environment and document all organizations, domains and support services that are turned on for the AD environment. Every detail must be presented in line-item fashion in an editable report document including installed special applications, web URLs to those apps, organizational contacts, distribution lists, proxy addresses, Microsoft service plans and SKUs being used, groups, users, permissions, devices and more. The report must be organized by section with a table of contents to help us locate the specific findings of interest and problem areas must be highlighted in red, making it easy to spot individual problems to be rectified.

- SharePoint assessments

The SharePoint Assessment Report must be a detailed assessment that shows the total number of sites started under management, how many active SharePoint sites there are, what storage requirements there are and include daily trends in the number of sites and storage usage. It should then take the site collections and breaks down all the individual sites so that we can understand what is being published in each, how they are organized, and even what groups they contain. Among other things, the report must help us understand growth trends and better predicts backup needs.

- One Drive Usage reports

The OneDrive Assessment Report must provide a high-level summary report of all OneDrive usage. This overview report must give us a solid handle on how the OneDrive platform is growing and look for spikes in that growth that need to be managed. It also need to look for spikes in activity that may need to be investigated. The report must provide trends over of 30-, 60-, and 90-day increments to give us a solid indicator of storage and bandwidth utilization.

- Outlook Mail Activity reports

The Outlook Mail Activity Report must provide deep dive information about Office 365 usage. The Outlook Mail Activity Report must provide a high-level summary of what emails are being sent and received by our top 10 active senders and active receivers for the reporting period. This report is meant to be run month-over-month to identify the power users who may need more capacity and which mailboxes are not being read at all and likely represent recently inactive users that need to be cleaned up.



- Microsoft Teams assessments

The Microsoft Teams Assessment Report must provide detail about each team in the system, including who the owners are, what channels they have and what kind of user identity audits have been conducted on the channels. There must be individual entries that can be used for audits of the member settings, the guest settings, the message settings, the fun settings and the tab settings. This information must include other types of misconfigurations that might cause security problems, such as having guest members that may have the ability to remove and delete channels.

- Microsoft Cloud Security Assessments

The Microsoft Cloud Security Assessment report must bring together all the security aspects of Microsoft Cloud under one umbrella. It should not only include our own Microsoft Control Score and Secure Score from Microsoft but also show our trending against the average score of our peers.

- Microsoft Cloud Configuration Change reports

The Microsoft Cloud Configuration Change Report must be a very detailed technical report that identifies entity and configuration changes. The changes must be grouped by properties, showing the old values vs. the new values, and then the changes must be grouped together into bands. This report must give us the ability to look at a group of changes together, as well as see how all the properties have changed for that time-period.

- Cloud Risk report

The Cloud Risk Report must span over all the Microsoft Cloud components. It must include an overall Risk Score, an overall Issues Score, as well as a summary list of issues discovered. The issues must come from both the Microsoft controls as well as other best practices. It must identify specific risks that are due to misconfigurations as well as risks created from turning on or off specific running components.

- Cloud Management plan

The Cloud Management Plan must take issues identified in the Risk Report, organizes them by severity and includes specific recommendations on how to remediate them. The report's information must be pulled directly from the Microsoft controls from multiple Cloud components, including SharePoint, OneDrive, Teams, Azure AD itself. It must also identify other types of issues related to misconfigurations and operations.

- Compensating Control Worksheets

The report is required to present the details associated with security exceptions and how Compensating Controls will be or have been implemented to mitigate risks in the cloud environment. This is required to explain and document why various discovered items are possible false positives. The Compensating Controls Worksheet does not alleviate the need for safeguards but must allow for describing of alternative means of mitigating the identified security risk as reference.

#### **4.1.3 Cloud Application Activity & Security Monitoring**

The Municipality requires a comprehensive cloud application activity and security monitoring service to provide continuous visibility, alerts, and reporting across their cloud environment. The service should detect, investigate, and report on unauthorized, anomalous, or risky activity related to user accounts, privileged roles, authentication events, and sensitive data handling.

The following features must form part of the solution.

##### **User & Identity Monitoring**

It must have the ability to tracks user account creation, login activity, privileged account changes, and account credentials usage across cloud applications. The platform must collect behavioural telemetry to detect anomalies and unauthorized access.

##### **Threat Detection**

It must provide for pattern-based detection and machine learning to identify threats such as compromised credentials, impossible travel logins, external device access, shadow accounts and risky file activity.

##### **Automated Remediation**

The solution must make provision for automated responses: locking compromised accounts, terminating risky file shares, and enforcing policy driven actions to stop threats swiftly.

##### **Event Logging & Application Monitoring**

It must have the ability to monitor SaaS application usage and logging across integrations with major platforms (e.g., Microsoft 365, Google Workspace, Salesforce, Okta). Enables visibility into events across organisational SaaS estate.

##### **Reporting & Visibility**

It must provide dashboards and reporting aligned to user behaviour, risk posture and threat events. Enables demonstration of security value and oversight of cloud application security posture.

##### **Integration & Extensibility**

It must integrate with major SaaS platforms, identity systems, RMM/PSA tools (*including that on offer in section 4; Monitoring, management, and Audit system, of this tender request*), and security stacks. It must support workflow integration and centralised investigation and response.

##### **Architecture requirements**

The solution must be provided as a cloud service, accessible anywhere, to make provision for scalability, continuous updates, and centralised management of SaaS application security.

## 4.2 Compliance

### 4.2.1 Cyber Security Framework management tool

Cape Agulhas Municipalities' Information Security approach serves as a comprehensive framework aimed at safeguarding our digital landscape and preserving the integrity of sensitive information. Aligned with the principles of Enterprise Architecture (EA), our approach ensures a cohesive integration of information security practices within our broader ICT Strategy.

In line with this Cyber Security Framework (CSF) approach the Municipality wish to obtain a Cyber Security Framework Management Tool to include from a CSF perspective at least NIST CSF, NIST 800-171, CIS Controls V8, and others.

The system must show a clear alignment of best practices, and other standards to the likes of at least ISO 27001, ITIL and COBIT.

The system must also show alignment between the CSF and POPIA.

#### 1. Standards

The System and Support Services related to this must allow for **at least** the following standards:

- CIS Controls v8
- CMMC 2.0
- Cyber Insurance Readiness
- Essential 8
- PCI DSS
- POPIA
- SOC2
- ISO 27001 & 27002
- NIST CSF 2.0

#### 2. System functional requirements

The system must provide for a logical workflow for assessment purposes of compliance against the standard or set of standards chosen by the Municipality, considering the standards above.

1. Dashboard
  - a. Standards Assessment Progress
  - b. Control Assessment Progress
2. Task summary of completed and outstanding actions.
  - a. Show a list of tasks with details as to what it entails, with links to correspondent section in workflow.
3. Controls and Standards selected.

Each Control have a set of requirements to comply thereto.

The online system and portal provided must cater for a set of requirements that each Control must adhere to. These requirements must clearly be defined to facilitate in the compliance of the relevant Standard.

- a. Controls section
  - i. Here the standards selected must be shown, information included must at least be:
    1. Identifiable key or ID
    2. Name of each Control Brief Description thereof.
    3. Alignment to relevant Standard/requirement ID must be shown.
  - ii. Provide in this section the ability to add own controls.
- b. Requirements Section
  - i. Each requirement standard as aligned to the control must provide information and guidance to include the following:

1. Description
  2. Policy aligned to the control.
  3. Guidance on how to address the control.
  4. Controls related to others must be shown here as well.
4. Baseline Assessment / GAP Analysis
- a. This section must allow for a baseline assessment of current environment against the Controls of the selected standard(s).
  - b. This is to provide enough information to the individual doing the assessment to establish a baseline of the Municipalities' current state as measured against the selected standard(s).
  - c. This section must allow for a selection of response, i.e. Fully, partially, No (None) or uncertain.
  - d. It should also allow for comments to be made per Control or for evidence to be uploaded.
  - e. Allow for assessment owners to assign task(s) to other users of the system.
5. Data Collection
- a. LAN Discovery tool
    - i. This tool must consist of both a network scan and a push scan that can collect data from individual endpoints.
    - ii. It must allow for configuration of both Active Directory and workgroup environments.
  - b. Agents
    - i. The system must allow for discovery agents to be deployed locally on a network if required.
  - c. Cloud scans
    - i. These scans must allow for scanning of Microsoft Cloud assets.
  - d. Device scans and data collector
    - i. This collector must allow for scanning of devices which cannot be accessed remotely. Therefore, the data collector must have the ability to scan devices locally and import the information into the system afterwards.
  - e. External Vulnerability scan
    - i. The Municipality have externally hosted systems and services which may be required to be scanned for vulnerabilities from time to time. The system must allow to import externally scanned systems data from the Network Access policy system into the compliance system.
  - f. Internal Vulnerability scan
    - i. The vulnerability scan results from the Network Access policy system into the compliance system must be imported into the compliance system.
  - g. Scan results / outcome data.
    - i. Scan results from all the data collected in this section must be summarised here.
6. Technical revision
- The Technical revision must combine collected data with manual input to identify technical issues and provide evidence of compliance.

Focus areas must include at least the following:

- a. User Access Review
- b. Inventory of Assets
- c. Inventory of Applications
- d. Azure Enterprise Inventory of Applications
- e. External Information System inventory
- f. External Port use
- g. Identification of Shared files
- h. Assessment of sensitive data as classified by system in terms of the relevant Standard(s).

7. Assessment of Controls
  - a. This Assessment must help the Municipality to establish evidence of compliance for each control applied to the assessment environment.
  - b. It should have the ability to import the data from the Baseline Assessment.
  - c. It must show the status of related requirements with the ability to drill down into these related requirements.
  - d. This section must allow for a selection of response, i.e. Fully, partially, No (None) or uncertain.
  - e. It should also allow for comments to be made per Control or for evidence to be uploaded.
  - f. Allow for assessment owners to assign task(s) to other users of the system.
8. Assessment of Requirements
  - a. This Assessment must audit the compliance status of individual requirements for the selected Standard(s).
9. Action / Project plan section
  - a. This section must list all discovered issues. Issues must be categorized by Technical, Control and Requirements. This section should be initially created after completion of the entire assessment process. It is used to track progress toward issue remediation pending the next assessment.
10. Outcome Section
  - a. This section of the compliance system must provide reports that gives a snapshot of the Evidence of Compliance at a point in time.
  - b. The system must cater for Reports that can be repeatedly generated for the current assessment until they are archived. At which point, a snapshot of the report set must be saved.
  - c. The following reports type must be available:
    - i. Policies and Procedures on Standards, Controls and requirements
    - ii. Standards Assessor Checklist, based on selected Standard(s).
    - iii. Status of each control and standard selected.
    - iv. Technical review reports
      1. Technical assessment(s)
      2. Technical Risk Analysis
      3. Technical Risk Treatment Plan
    - v. Other supporting documents
      1. Application Inventory Review
      2. Asset Inventory Review
      3. Asset Inventory
      4. Drive Encryption Report
      5. External Information Systems Review
      6. External Vulnerability Scan Results
      7. Internal Vulnerability Scan Results
      8. Security Policy Assessment
      9. Sensitive Data File Scan Report
      10. Share Permission Report
      11. User Access Review
      12. Windows Patch Assurance Report
11. Employee portal
  - a. User creation
  - b. User permission must be set according to the Municipalities' policies.
12. Audit Logs
13. General functionality
  - a. Allow for multiple users to work on the same investigation / assessment.
  - b. Allow for assessment owner to assign workload to system users.
  - c. Track who is responsible for relevant control and who assigned the task(s).
  - d. Keep a database of all data inputs and file uploads.
  - e. Provide online portal or website for referencing of system functionality and or implementation guidelines.

### 4.3 Dark Web monitoring

**Cape Agulhas Municipality is awaiting a bid for this service and should include a proposal document or brochure detailing the solution including the following:**

1. Corporate Domain Monitoring  
Monitor the Dark Web for Stolen user credentials (emails/passwords) found indicating the Municipality or a 3rd party application/website that our employees use may have been compromised.
2. Email Monitoring  
To monitor the personal mail addresses of our executive Management and administrative users, in addition to their Municipal email accounts. The preferred system will need to monitor up to at least 10 personal emails, in addition to those within the Municipal network.

### 4.4 Security Audit

The Municipality await a proposal for the performing of an ICT Security Audit focusing on the elements as seen below. The intent of this section is to evaluate if the bidder can successfully assist the Municipality with Risk based ICT Audits in order to contribute to a safe and conducive ICT environment.

#### 1. Security Assessment Methodology

- Provide a high-level security risk assessment looking at technology, processes, and people that support the business.
- Build a Business Risk Profile (BRP), measuring the risk of doing business the Municipality face due to the industry and business model chosen.
- Evaluate and list the current security measures the Municipality has deployed. Focusing on Defence-in-Depth Index (DiDI).
- Measure risk distribution across the area of analysis (AoAs), infrastructure, applications, operations, and people.
- Measure the security maturity of the Municipality.
- Provide Risk Management recommendations taking into account existing technology deployments, current security posture and defense-in-depth strategies in order to ensure the Municipality move toward recognized best practice.
- The assessment must cover broad areas of potential risk across our environment rather than an in-depth analysis of a particular technology or process. The information we require here is to guide us to help focus on specific areas that require more rigorous attention.

#### 2. Vulnerability Assessments

##### Focus areas.

- a. External Internet facing Infrastructure.

This section should consider at least:

- Vulnerabilities
- Data breaches
- Compliance

- b. At the Gateway of the organisation viz, all traffic passing in and out of the organisation.
  - Cape Agulhas Municipality has external facing network utilities and hardware to as gateway.
- c. Internal Server Infrastructure
  - Cape Agulhas Municipality has a range of Information Systems hosted internally.
- d. Wireless Network Infrastructure
  - Integrity of Wi-Fi networks must be tested and reported on.

### 3. Network Assessment

- a. Network reconnaissance using a scanning tool to identify potentially unauthorized devices connected to the network.
- b. Network vulnerability and penetration testing of a sample of hosts (i.e. Servers, web application servers, network infrastructure and end user PC's/ laptops).

### 4. Reporting

A Security Analysis Report and Scorecard that measures risk distribution across the areas of analysis (AoAs)—infrastructure, applications, operations, and people must be made available.

The Scorecard must list items that have met best practise, items that need improvement and items that are severely lacking. This report must also allow for a security plan to be devised that can be constantly measured to ensure successful implementation, revisited, and maintained.

### 5. Additional information

- Approximately 210 users
- SQL Databases, Linux servers and Microsoft based applications
- Scanning of Official websites must be included.
- The maximum hours of the audit should not exceed 200 hours.
- This service may be required on request after the initial appointment period.

## 4.5 Security Awareness Training & Phishing Simulation Requirements

### 1. Scope

Cape Agulhas Municipality has a requirement for a Cybersecurity Awareness Training program as part of a strategy to improve the organisations security posture and security culture. The two main objectives of the program are to promote behaviour change and to educate the user by creating awareness regarding the ever-changing world of Cybersecurity.

The successful bidder is required to provide a training methodology by aligning to standards as set out by the SANS (SysAdmin, Audit, Network, Security) Institute. <https://www.sans.org/>.

The Cybersecurity Awareness Training Program must be a combination of various tool sets and incorporates Instructor led Live Classrooms as least 2 sessions per employee per annum, as well as Computer Based Training combined with Awareness material and constant communication mechanisms. The program must contain measurable metrics that can be reported on.

Key focus areas must include:

- Impact Metrics on behaviour
- Strategic Impact Metrics
- Compliance Metrics
- Ambassador Program Metrics

Physical training facilities with ICT equipment, computers, internet access, projectors etc. to be supplied by Cape Agulhas Municipality in Bredasdorp, Western Cape.

A draft training project plan submitted to Chief Information Officer within 3 months of tender award.

The Cybersecurity Awareness Program at a high level must address the following objectives:

- Securing the Human Factor – Creating awareness and keeping the user informed.
- Reduce risk to the organization – What we do not know we can't manage.
- Maintain compliancy – In terms of Condition 7 of the POPI Act Section 19 D) which is to:

- Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards. [This is a continual obligation to identify security risks on an ongoing basis and implement measures to reduce risks so identified.]
- Reduce costs - freeing up IT security resources to focus on more advanced threats.
- Promote and Protect - the Municipalities' brand and reputation thereby giving ratepayers confidence in dealing with the Municipality.
- Educate the user – Continuous training provided in an easy, non-obtrusive and seamless fashion.
- Training to target 200 users / Officials.

## 2. Project requirements

Meet with the Municipalities' stakeholders to:

- Determine Organisational Structure.
- Identify Departments and Department Heads.
- Appoint Ambassadors to the program from the Municipality.
- Share the program with the relevant stake holders.
- Introduce the methodology, approach, and tools to be utilized.
- Set Training dates for the Ambassadors on the CBT (Computer Based Training Program)
- Set Campaign milestone dates.
- Set the Computer Based Training curriculum per user role for the 12 months.
- Determine Monthly, Quarterly and Annual Review dates.
- Produce a high-level project plan document.
- Conduct Cybersecurity introductory Workshops.
- Distribute Awareness Literature via different mechanisms.
- Ambassadors to demonstrate the Computer Based Training functionality.

## 3. Required outputs.

CREATE MORE RESPONSIBLE BEHAVIOUR BY EMPLOYEES BY:

- Creating Phishing Campaigns – Before and after training to measure the effectiveness of the training.
- Conduct Surveys – Before and after training to measure the effectiveness of the program.
- Behaviour Change metrics by measuring against the 15 Baseline objectives as set out in the SANS.ORG SAM (Security Awareness Module).
- Video Training – Using a system to measure the modules by checking on the progress per candidate, number of views, answers provided and the number of attempts to answer.
- Scheduled Live interaction sessions with employees - Are the employees' questions becoming more sophisticated over time? Are there some security areas that they are resistant to understanding, even after repeated training?
- Instructor led Classroom training. At least twice per annum.
- Quarterly Security Awareness emails to all users
- Provision of Security Awareness collateral in electronic or print format.
- Monthly/Quarterly meetings, as required by the municipality, with Security Awareness Ambassadors
- Provide quarterly updates on security awareness topics.



#### 4. Reporting

- Quarterly feedback reports required with recommendations on outcomes as per training results.
- Identify risk areas or risk profiles per user type or category. I.e., Executive, low end-user etc.
- Present quarterly program status report to ICT Steering Committee
- Post security training review with ICT Steering Committee

Licensing per user must include all requirements as set out in this section.

#### 4.6 Vulnerability Scanning Tool

**Vulnerability Scanning Solution/Tool** should include on-prem internal network scanners, computer-based discovery agents, remote internal scanning by proxy, and **hosted external scanners** to scan public facing IPs/resources for comprehensive vulnerability management. The vulnerability scanning tool should be able to Manage multiple network environments at scale with no limits on the number of scanners you can use on each environment, to manage multiple networks of any size.

**Vulnerability Assessment Scans:** The Vulnerability assessment services, and solution is expected to assist in proactively closing any gaps and maintain a strong security environment for our systems, data, employees, creditors and clients. Data breaches are often the result of unpatched vulnerabilities or misconfigurations, so identifying and eliminating these security gaps, removes that attack vector.

##### **SCHEDULED NETWORK VULNERABILITY SCANNING**

The Solution should allow for each scanner to be configured to run on its own schedule, based on the frequency and time that you want it to run. Ability to use custom scan tasks to set up variable schedules.

##### **BUILT-IN SCAN PROFILES**

Pre-set scans for “Low Impact,” “Standard,” and “Comprehensive” scanning options. There should also be a separate option for creating custom scan profiles to meet specific use-case needs, such as the ability to create scan profiles to target specific TCP and/or UDP ports.

##### **AUTHENTICATED SCANS / CREDENTIAL SCANS**

The solution should be able to Use credentialed/authenticated scans to access an account on a network endpoint.

##### **COMMON VULNERABILITIES AND EXPOSURES SUPPORT**

The Solution should have the ability to search Scan Results for discovered vulnerabilities by Common Vulnerabilities (CVE) ID.

##### **REPORTING**

Vulnerability Assessment Solution needs to provide both summary and high- level reports to enable remediation. These reports assist the ICT department in identifying and tracking security issues in all phases of the cyber exposure lifecycle, translating raw security data into a common language for communicating risk back to the organization. The Vulnerability Assessment solution must provide capabilities to produce detailed reports that must include date of vulnerability discovery, score of the based on common vulnerability and exposures, detailed description of vulnerabilities.

## 4.7 Penetration Testing

The Municipality requires an automated Penetration Testing (Pen Test) service as a SaaS model, that replicates manual internal and external network penetration testing, to evaluate real-time cybersecurity risks monthly.

For internal scans, a local device may be installed and configured to facilitate this service. External scans must be provided for in the SaaS model.

### General Requirements

- Provide a snapshot of a moment in time.
- Alert to issues on network.
- Provide remediation plans.
- Remediation support in the form of professional services.
- Egress filtering testing.
- Authentication attack testing
- Privilege escalation and lateral movement testing.
- Data exfiltration analysis
- Simulated malware testing
- MITRE ATT&CK Framework mappings and analysis
- Identify reputational threat exposure.

### Reporting

- Rank threat severity from Critical to informative.
- Summarize discovered threats.

### 4.7.1 PROJECT BACKGROUND

The Municipality wish to source Vulnerability Assessments and Penetration test services to enable the Municipality to proactively identify threats. This will enable the Municipality to put measures in place that mitigate against the identified vulnerabilities and risks.

The Municipality requires an automated Penetration Testing (Pen Test) service as a SaaS model, that replicates manual internal and external network penetration testing, to evaluate real-time cybersecurity risks monthly.

For internal scans, a local device may be installed and configured to facilitate this service. External scans must be provided for in the SaaS model.

The benefits that will contribute to the Municipality with regard to the Vulnerability Assessment and Penetration Test services include:

- Detection of security weaknesses before attackers do.
- Testing of the Municipalities` cyber security posture.
- Producing a list of vulnerabilities on devices.
- Producing a defined risk assessment for the Municipalities` respective networks.
- Establishing security record with recommendations on how to mitigate against the identified risks.
- Producing a plan for the risks vs. benefits of optimizing the Municipalities` security investments.

Due to the rise of cyber security attacks that Municipalities face, it is becoming increasingly necessary to put controls that will allow for the prevention of attacks. One of the measures in the prevention of attacks is identifying control weakness in the systems such as the networks, applications and databases. Once weaknesses are identified the organisation can put in place measures to close or mitigate against them. The approach that the Municipality will use in this regard is implementing Vulnerability Assessments and Penetration Tests in its ICT environment.

#### 4.7.2 PURPOSE

The purpose of this is to solicit proposals from potential bidders for the Provision of Vulnerability Assessments and Penetration Test Services to the Municipality. This bid document details and incorporates, as far as possible, the tasks and responsibilities of the potential bidder required for the Provision of Vulnerability Assessments and Penetration Test Services.

#### 4.7.3 SCOPE OF WORK

The Vulnerability Assessment and Penetration Test Services program must include the following in scope items:

- **Municipal Asset Discovery:** The ability to have a current, updated enterprise asset inventory is critical to the success of the Vulnerability Assessment program. The service provider is expected to assist the Municipality in the completion of an inventory and blueprint of the Municipalities' networked technology assets. This will be completed through a network discovery process, which is expected to produce a comprehensive inventory detailing the organization's services, workstations and network devices.
- **Vulnerability Assessment Scans:** The Vulnerability assessment services, and solution is expected to assist in proactively closing any gaps and maintain a strong security environment for our systems, data, employees, creditors and clients. Data breaches are often the result of unpatched vulnerabilities or misconfigurations, so identifying and eliminating these security gaps, removes that attack vector.
- **Reporting:** Vulnerability Assessment Solution needs to provide both summary and high- level reports to enable remediation. These reports assist the ICT department in identifying and tracking security issues in all phases of the cyber exposure lifecycle, translating raw security data into a common language for communicating risk back to the organization.
- The Vulnerability Assessment solution must provide capabilities to produce detailed reports that must include date of vulnerability discovery, score of the based on common vulnerability and exposures, detailed description of vulnerabilities.
- **Support:** The bidder is expected to provide support of the vulnerability services software over a period of **36** months.
- **Penetration Tests:** The service provider is expected to include the performance of Penetration testing of all public facing systems. This will be handled on a case by case during scoping sessions for penetration testing. **Four (4)** Penetration tests will be performed every year, for a period of 36 months.

The project will include the following:

- Delivery, configuration, deployment and operation of the Vulnerability Assessment and Penetration Testing Services.
- Provide an implementation plan covering service, deliverables and skills.
- Provide comprehensive reporting on the discovery and result inclusive of mitigating recommendations.
- Comply with internal policies and audit controls.
- Provide Change Management service to the Municipality; and
- Training of personnel.

The project is expected to deliver the following:

NO	DESCRIPTION
	<b>BUSINESS REQUIREMENTS</b>
1.	The proposed solution should have automated asset discovery capabilities for the following assets. <ul style="list-style-type: none"> <li>• Servers</li> <li>• PC's and Laptops</li> <li>• Network devices</li> </ul>
2.	The solution should provide an ability to scan the network for vulnerabilities using: <ul style="list-style-type: none"> <li>- <b>Authenticated Scan:</b> authenticated scan is a vulnerability scan that is performed by an authenticated user– a user with login credentials with capabilities to run deep scanning; and</li> <li>- <b>Non-authenticated Scan:</b> non- authenticated scan performs a vulnerability scan by not using usernames or passwords during the scanning which has capabilities to detect expired certificates, unpatched software, weak passwords, and poor encryption protocols.</li> </ul>
3.	Vulnerability scanning on all Network Devices including Cloud implementations (External and Internal Vulnerability scanning).
4.	Uncover all application vulnerabilities but not limited to, cross-site scripting, command injections, code injections, misconfigurations, insecure cookies and flaws.
5.	The solution must have the functionality to search for vulnerabilities and assign a risk score continuously.
6.	Deliver alerting capabilities for when a scan reveals new security risks and vulnerabilities on the Municipalities` ICT infrastructure.
7.	Provide capabilities to identify false positives vs real vulnerabilities.
8.	Provide a solution that has capabilities to monitor vulnerabilities introduced by applications installed on Municipalities` infrastructure components such as desktop or laptop computers.
9.	Provide allowance for flexible vulnerability assessment schedules.
10.	The solution must be able to provide a holistic view of the environment where the Municipalities` ICT team is able to drill down at any stage to explore: <ul style="list-style-type: none"> <li>• Assets.</li> <li>• Vulnerabilities.</li> <li>• Exploits.</li> <li>• Policies.</li> </ul>
11.	The vulnerability management solution should also be setup to allow to run ad- hoc vulnerability scans on the environment, to scan new devices, web applications and systems.
12.	Provide penetration testing services for Municipal infrastructure that include: <ul style="list-style-type: none"> <li>• Internal Network (LAN).</li> <li>• Externally facing Public IP addresses and systems; and</li> <li>• Municipal Websites, both Cloud hosted and internally hosted.</li> <li>• Other hosted or cloud services or systems</li> </ul>
13.	The services must support standard and customized reporting functionality for penetration testing related reports.
14.	Provision of reporting capabilities with a dashboard that highlights the risk scores (i.e. Business Critical, high, medium, low, and informative) for all vulnerabilities but also provide the Municipality with an overall risk score based on the volume and severity of vulnerabilities found within the network, applications, and ICT assets and devices.

NO	DESCRIPTION
15.	Reporting function of the solution must have the following reports but not limited to: <ul style="list-style-type: none"> <li>Automated and comprehensive devices discovery report.</li> <li>Scheduled comprehensive vulnerability scanning reports; and</li> <li>Dashboards reports.</li> </ul>
16.	The Bidder must be proficient in information security with an excellent knowledge and practice of ICT Vulnerability Assessment and Penetration testing.
17.	The Bidder must provide advisory services on the remediation of vulnerabilities strategies.
18.	The bidder must supply, install, customize, integrate, test and troubleshoot the tools in scope for vulnerability and penetration testing services.
19.	The Bidder should supply, install, customize, integrate, test and troubleshoot the tools in scope for vulnerability assessment and penetration testing services.
	<b>TECHNICAL REQUIREMENTS</b>
20	Penetration Testing (Pen Test) service as a SaaS model
	<b>AUDIT REQUIREMENTS</b>
21.	Keep an audit trail of all vulnerabilities and applied remediation steps.

#### 4.7.4 PROJECT DESIGN

##### 4.7.4.1 Methodology and approach

The service provider must provide Project Management Services for the full implementation of the solution. The Bidder must also provide detailed description of their Project Management process/ methodology in sufficient detail to convey to the Municipality that it is capable of implementing its proposed service on time and on budget. The methodology must indicate clear stage gates which require approval and signoff, triggering payment on completion of key milestones.

The Municipality expects the service provider to provide project documentation, from Project initiation document, project plan, requirements analysis, system architecture, solution documentation and design documents, test plans, training and technical documentation. The Bidder shall clearly specify the proposed approach, methodology and plan for the implementation of the Vulnerability Assessment and Penetration Testing Services.

These include but are not limited to the following:

- Delivery, configuration, deployment and operation of the Vulnerability Assessment and Penetration Testing Services.
- Provide an implementation plan covering service, deliverables and skills.
- Provide comprehensive reporting on the discovery and result inclusive of mitigating recommendations.
- Comply with internal policies and audit controls.
- Provide Change Management service to the Municipality; and
- Training of Municipal personnel.

#### **4.7.5 CONTRACT TERM**

The successful bidder will be appointed for a period of thirty-six (36) months or three (3) years. Duration of contract/ Service Level Agreement will be based on performance which will be reviewed monthly.

#### **4.7.6 PROJECT MANAGEMENT ARRANGEMENTS**

##### **4.7.6.1 Management**

- The Municipality will appoint the service provider in line with its SCM Policy.
- The Municipality will manage and oversee the project and establish a Project Steering Committee for this purpose.
- The Service Provider will be expected to present the inception report, project plan, draft project report to the Project Steering committee and other relevant stakeholders. Thereafter, the service provider will incorporate comments and inputs before presenting the final project report.
- Supplier performance will be conducted in line with SCM policy and Provincial and National Treasury Regulations.

#### **4.8 Security Operations Centre (SOC)**

The Municipality wishes to engage a suitable vendor to provide a 24 x 7 x 365 Managed Security Service encompassing a Security Operations Centre (SOC).

##### **4.8.1 SPECIFICATION OF REQUIREMENTS**

**Tenderers must address each of the requirements in this part of the tender and submit a detailed description in each case which demonstrates how these requirements will be met and their approach to the proposed delivery of the Services. A mere affirmative statement by the Tenderer that it can/will do so, or a reiteration of the tender requirements is NOT sufficient in this regard.**

The Municipality wishes to engage a suitable vendor to provide a a 24 x 7 x 365 Managed Security Service encompassing a Security Operations Centre (SOC) solution which it is proposed to implement on a phased basis as described in 4.10.4 below. The purpose of the SOC will be to monitor and analyse the municipalities` data environment and to alert and advise on remediation. The proposed solution must be capable of operating across firewall zones and provide support for Cloud services incl. Azure.

The objectives from a Municipal perspective include the following:

- To implement a solution to detect and respond to threats, while maintaining all systems and network data in a secure manner.
- To increase resilience by learning about the changing threat landscape (both malicious and non-malicious, internal and external)
- To identify and address negligent or criminal behaviour.
- To derive business intelligence about user behaviour to shape and prioritise the development of technologies.

#### 4.8.2 Approach to the delivery of the SOC Managed Service

The Managed Service provider must have a dedicated, established Security Operations Centre staffed 24/7/365 by appropriately qualified personnel to monitor, investigate and alert on SOC events. The proposed Managed Service must include:

- Solution deployment
- Configuration and management of a SOC solution
- Alerting in respect of significant events to augment and support the Municipalities' internal Security Team and to deal with new and emerging threats as they arise.

Tenderers must clearly describe how each element will be delivered and the expected working relationship, roles and responsibilities both internally and between the SOC and the Municipal internal Security Team which will be the primary contact for the proposed managed service.

##### 4.8.2.1 Threat Detection, Classification and Alert Notification

- Tenderers must provide details on their proposed solution's full range of threat intelligence feeds and the methodologies used to maintain their currency to mitigate the latest threats and vulnerabilities and describe what access to this data the Municipality will have.
- Tenders must clearly describe their full alert management process, including details on how threats, vulnerabilities and suspicious activity will be assessed and classified. The SOC will have differing levels of response based on the level of an event as described below or *equivalent* as relevant to the proposed solution.
  - Category A (High severity/risk)
  - Category B (Medium severity/risk)
  - Category C (Low severity/risk)
- Depending on the severity of an event, the SOC will have different response/investigation targets defined within an SLA and in this regard must provide typical response/alert/escalation time frames for each level of events. Tenderers must describe their approach to managing each of these event priorities.
- Tenderers must fully describe each stage of the process and must provide details of each layer of the SOC event management workflow from initial triage through assessment and RCA and finally to detailed analysis and resolution.
- The response should include details of how the event is detected, classified and remediation advice is reported back to Municipal Security and Technical Support teams together with relevant third-party Service Providers in line with agreed notification procedures.

#### 4.8.3 Technical Requirements of SOC Solution

The Municipality is seeking a SOC solution to be deployed as the primary security event management tool for the proposed service. In this regard, tenderers must clearly describe their rationale for their proposed solution. The SOC solution must be capable of providing a secure means of integration with designated Municipal systems and support the **real-time** collection and analysis of events from host systems, security devices and network devices, combined with contextual and behavioural information for threats, users, assets and data.

- Tenderers must list the primary tools used to deliver the proposed services. Similarly, tenderers must describe the function or service offering they support, and indicate whether they are proprietary, commercial, or open-source encompassing log collection, log management and storage, analytics, reporting, case management and workflow, and incident response.
- **The proposed solution must not have any adverse impact on the day-to-day operations of the Municipality.**
- Tenderers must describe how they propose to maintain the proposed SOC solution in terms of its currency and optimisation and develop procedures to manage and respond to classes and severity of incidents.

- The Service Provider will be required to monitor Municipal endpoints and network infrastructure to identify threats and vulnerabilities, which could compromise data or impact on system availability. This response will include an initial SOC based investigation, alerting and response process which will be defined in a run book agreed at contract commencement. Tenderers must describe their ability to analyse this data and to provide real-time event correlation between data sources, and real-time alerting of security incidents and system health incidents.
- Tenderers must describe their support for the creation and management of customized correlation rules and any limitations, such as data sources, age and query frequency.
- Tenderers must describe their ability to analyse this data to identify when changes in behaviours of users or systems represent risk to our environment.
- Tenderers must describe how false positives are managed, and how false positive feedback from the Municipality will be managed.
- Tenderers must describe support to the Municipality in the configuration of end devices for the purposes of log collection for the SOC solution e.g. configuration of NetFlow or agent installation etc.
- Tenderers must describe how the proposed solution can be tuned and enhanced as the process matures.
- Tenderers must describe the data life cycle management requirements, such as backup of the data stored in the proposed SOC solution.
- Tenderers must describe how Municipalities' data (including data generated by their company about security events and incidents affecting the municipality) will be governed and protected in transit.
- Tenderers must describe the scope of compliance reporting which will be included within the proposed Managed Service.
- Tenderers must also provide details of their approach to and the processes, resources and all relevant tools deployed to provide advanced capabilities to include Artificial Intelligence, Machine Learning, Threat Management and Vulnerability Management capabilities. The Municipalities' decision to avail of any of these features and any other additional feature is optional and will be dependent on price and as a result may not be availed of, during the contract period.
- Tenderers must describe the architecture of the proposed SOC solution, including elements within the SOC data centre (on tenderer's premise, colocations and private and public Cloud services) and within the Municipality, as well as the centrally delivered log management, analytics and portal tiers. Any elements that are delivered by third-party partners must be identified.
- While the Municipality will consider a Cloud or an on-premises solution, Log Collectors must be hosted within the Municipality.
- Tenderers must describe the operating model of their proposal i.e. whether it is appliance based or physical/virtual server. If physical or virtual server based, tenderers must clearly describe the full technical specifications of their proposed solution.
- Tenderers must clearly describe any proposed licensing model to include itemised advanced features together with the terms and product rights of any proposed software.
- Tenderers must provide details of all necessary connectivity requirements such as that between the Municipality and the proposed SOC.
- Tenderers must state whether their solution requires an agent install to collect data and any associated licencing with this agent. Where possible, tenderers should indicate whether this agent can be installed using automated methods.



- The solution must be accessible by the Municipal Security Team for the purposes of report generation and environment status review including real-time visibility of any issues, threats, vulnerabilities or suspicious activity. Tenderers must demonstrate the ability to produce standard and custom management reports, including standard weekly and month end reports, relating to compliance and on any issues, threats, vulnerabilities or suspicious activity. Tenderers must include a list of standard reports together with a clear description of the range of possible customisations. In this regard tenderers must advise how access to the solution will be controlled and reported.
- The successful tenderer must carry out a due diligence audit within the first month of the contract. The Municipalities' decision not to implement any recommendation because of the review will not alter the terms of this contract.

#### 4.8.3.1 Log Sources

The proposed SOC Solution must be capable of integration with log sources and provide alerts on the following:

**Table 1**

**See required integrations.**

Dark Web monitoring	Switches & Routers
Cloud – MS Azure, Amazon	Office 365
Anit-Virus mail protection	Domain Controllers
Anti-Virus / Endpoint protection	Servers (IIS, Windows, Exchange,)
Advanced Threat Protection	Web Application Firewall / Physical Firewall

**The following type of monitoring is required as a minimum:**

Advance breach detection	Crypto Mining detection
Cyber Terrorist Network Connections	Ransomware Detection
Endpoint Event Log Monitor	Firewall Log Analyzer
IOC Detection	Log4j Detection
Malicious File Detection	Microsoft Exchange Threat Detection
Office 365 Login Analysing	Office 365 Log Monitoring
Office 365 Risk Detection	Office 365 Secure Score
Print nightmare vulnerability protection	Pwnd Monitoring
Sophos Monitoring Central and physical firewall(s)	Suspicious Network Services Monitoring
Suspicious Tools Monitoring	Defender for Business monitoring
Report on vulnerabilities from Network access policy system see 4.2.1.	Exchange Hafnium Exploit monitoring
DnsFilter Monitoring	Provide Windows Defender Manager capabilities.
Specify additional detections.	

#### 4.8.3.2 Log Management

- The proposed SOC solution must have a log archival process in place. These archives should be easily searchable from within the SOC for a period of at least 12 months.
- Tenderers must therefore describe the log archive policy of the proposed solution and its capability to search these archived logs within the SOC for 12 months and also the backup processes proposed.
- Tenderers must describe the methods deployed to analyse data over the retention period and the facility to filter or edit large log sources.
- Tenderers must make provision for the handover of data at the end of the proposed contract and in this regard, tenderers must describe their approach to this **mandatory** requirement.

#### **4.8.3.3 System Maintenance**

As well as monitoring, investigating and alerting, the successful tenderer will be required to take part in general SOC application maintenance and housekeeping tasks when required as part of the contract. This includes the editing/removal of rules and alerts that are not performing efficiently in the SOC and the configuration of new rules and alerts when required. Tenderers must describe the processes and methodologies used to meet this requirement.

#### **4.8.4 Implementation/Project Take-on**

As described above, the Municipality is seeking proposals for the provision of SOC Managed Service.

The infrastructure includes the Data Centre and operating environment of Officials in the respective Municipality, and the bidder(s) should ensure that appropriate resources are available for implementation.

The Municipality has over 450 endpoints to include SOC with more than 200 users using various online systems and resources like Microsoft 365.

**The following considerations must be taken into account.**

- Tenderers must include a Project Implementation Plan identifying requirements, processes, timescales, milestones and other relevant information to demonstrate the feasibility of their approach to the delivery of each element of the project. The plan should clearly map out the implementation schedule from the time of contract commencement and what the typical project timeline would be for a similar sized project. The plan should also set out the project approach in terms of the assessment of the existing infrastructure.
- Tenderers must provide details of the key personnel to be deployed on the implementation project, their role, skill set and any relevant expertise that they may have. Tenderers must include Junior/Senior Engineering Day rates and Project Manager costs (if required and by prior arrangement only) associated with the full delivery of the proposal.
- Tenderers must explain their approach to the initial assessment, and how a baseline security level is established. Tenderers must include specifics on their infrastructure requirements, data transfer, data storage and segregation, backup systems and encryption standards.
- Tenderers must also describe the frequency and opportunities for continuous improvement during the implementation phase.

**It is a mandatory requirement that any knowledge transfer of the proposed solution to Municipal technical staff must be provided and will be required at no additional cost.**

#### **4.9 SIEM, Log Management & Security Automation Requirements**

The Municipality requires an enterprise-grade Security Information and Event Management (SIEM) and Security Automation platform that delivers comprehensive log ingestion, threat detection, incident response, and reporting capabilities. The proposed solution must provide real-time visibility across endpoints, servers, cloud platforms, network devices, and third-party systems.

The platform must support advanced analytics, including behavioural baselining, machine-learning-driven anomaly detection, correlation of events, and orchestration of automated response actions.

The objective is to ensure early detection of malicious activity, enable rapid and consistent incident response, and provide reliable auditability and compliance reporting across the environment.

#### 4.10 IT Documentation & Knowledge Management Platform Requirements

The Municipality requires an enterprise-grade IT documentation and knowledge management platform designed to centralise systems information, standardise operational knowledge, secure privileged data, and provide technicians with fast access to accurate documentation. The platform must support structured documentation frameworks, relationship mapping, automation, asset intelligence, password vaulting, IT process standardisation, and integrations with core IT systems such as identity solutions, PSA, RMM, and network tooling. The system must deliver strong security, role-based access, auditing, version control, and compliance alignment, while enabling efficient onboarding, operational continuity, and improved IT service delivery.

#### 4.11 Security Component Project Requirements

Interested bidders are directed to submit a written proposal to the Municipality for this section (Security) as a whole, clearly defining each system and technology and how it aggregates towards the security posture of the Municipality and the proposal must cover in general the following areas:

- Methodology reflecting an understanding of requirements and how this project will be executed.
- Project relevant experience of the company (track record), with examples of prior similar implementations delivered to clients. References on client letter head must be submitted. The Municipality reserves the right to ask for samples of reports on previous work delivered.
- Capacity to undertake the project., as shown by the combined experience of the project team, including project leader, in similar type of project, References contact details must be provided and the Municipality reserves the right to verify information in the CV.

## 2. Monitoring, management, and Audit system

The purpose of this system is to enable the Municipality to be able to control, manage and monitor the ICT environment, inclusive of devices and resources, directly connected to the various LAN's of the Municipality.

The Municipality currently consist of the following, and the applicable system should be able to be segmented in different areas of control, management and alarm notifications and reporting with the capability to handle an ever-growing environment.

1. 36 Active sites on the WAN – expanding continuously.
2. 210 end users on LAN over the active sites
3. 45 end users offline – not connected to LAN but with internet access.
4. 6 Hosting servers with 18 virtual servers
5. SQL databases – SQL 2019 to current – MySQL databases
6. Managed switches
7. Network printers.
8. VOIP devices
9. Time and attendance devices and controllers
10. Total of 708 networked devices

The system should be a hosted solution with a local central agent (pc/device) monitoring segmented probes /agents on the various network segments; to minimize traffic in the network environment and a Demo may be required from the successful Tenderer.

To summarise – with almost immediate effect the Municipality must have a complete view and control of its Network Infrastructure environment 24 x 7 x 365 with Monthly Executive Reports of the network (example must be provide) The Municipality must have one management console for the Network environment including, Servers, Switches, Routers, Desktops, Network Printers and Mobile devices; This solution must enhance productivity within the IT department and reduce risk.

The system/tool should at least have the following features:

- IT Asset Management.
- Hardware warranty management with start/end date with serial numbers on HP/Dell/Toshiba/Acer/Apple Devices.
- Patch Monitoring.
- Exchange Monitoring.
- Active Directory Monitoring.
- Software licence compliance monitoring.
- Monitoring Services 24 x 7 x 365 with email alerts.
- Security Monitoring.
- Remote support tools.
- Basic Connectivity Router and Switch Monitoring.
- Internet Connection Monitoring.
- Website availability monitoring.
- Backup Solution Integration, monitoring and reporting.

The system should further include at least following functionalities:

1. Overview
  - 1.1 Active issue dashboard
  - 1.2 All devices dashboard
  - 1.3 Job status dashboard
2. Segmented dashboards: These dashboards is a standard requirement, but the system should be able to setup additional dashboards should it be required.
  - 2.1 IP phones
  - 2.2 Windows laptops
  - 2.3 Network devices.
  - 2.4 Printers' dashboard
  - 2.5 Server hardware dashboard – Dell
  - 2.6 Probes / agent dashboard for server environment
  - 2.7 Generic workstation dashboard
  - 2.8 Windows workstation dashboard
  - 2.9 Windows workstation probe dashboard
  - 2.10 Server – Application and WMI hardware dashboard
  - 2.11 Servers – SBS application and WMI Hardware dashboard
  - 2.12 Servers – VMware ESXI dashboard
  - 2.13 Manage dashboard settings / configuration / access etc. dashboard.
3. Actions to be performed from system.
  - 3.1 Add/import devices.
  - 3.2 Add sites.
  - 3.3 Domain user management
  - 3.4 Agent / probe download configuration option.
  - 3.5 Backup system recovery point with export option
  - 3.6 File transfer capabilities.
  - 3.7 Patch approvals.

- 3.7.1 Automatic approval – configurable per schedule
- 3.7.2 Approvals per device
- 3.7.3 Approval per patch
- 3.8 Push 3<sup>rd</sup> party software.
- 3.9 Backup solution capabilities for devices in environment
- 3.10 Discover devices on segments of network.
- 3.11 Running of Mac Scripts
- 3.12 Automation of policies
- 3.13 Running scripts
- 3.14 Security manager for AV scanning and monitoring
- 4. Reports
  - 4.1 *Administrative reports*
    - 4.1.1 License usage
  - 4.2 *Assets*
    - 4.2.1 License compliance
    - 4.2.2 License key inventory
  - 4.3 *Availability*
    - 4.3.1 Availability aggregated for one device.
    - 4.3.2 Availability aggregated for one service on one device.
    - 4.3.3 Availability of multiple services on multiple devices
    - 4.3.4 Availability of multiple services on one device
    - 4.3.5 Availability of one service on multiple devices
  - 4.3.6 Status distribution
  - 4.4 *Events*
    - 4.4.1 Incident summary
    - 4.4.2 Notifications sent.
    - 4.4.3 Self-healing
  - 4.5 *Metrics*
    - 4.5.1 Raw monitored data for Active Directory
    - 4.5.2 Service metrics for Active Directory
  - 4.6 *Status*
    - 4.6.1 Configuration Summary – The purpose of this report displays what services are being monitored on each device, what Probe or Agent is monitored the service, how those services are configured, and the thresholds for each service.
    - 4.6.2 Missing patches (summary)
    - 4.6.3 Patch approvals and installations.
    - 4.6.4 Patch installation status.
    - 4.6.5 Patch status (detailed)
    - 4.6.6 Remote control summary
    - 4.6.7 Scheduled tasks summary
    - 4.6.8 Warranty expiry
  - 4.7 *Scheduled report's view*
  - 4.8 Report Manager
    - 4.8.1 *Managed assets*
      - 4.8.1.1 Asset Change Report**  
This report tracks hardware and software changes within a customer's network over time.
      - 4.8.1.2 Device Notes Overview**  
The Device Notes Overview report lists the device notes that have been created across all monitored Service Organizations within a specified number of days before the report generation date.

#### **4.8.1.3 Disk Usage Trending**

This Report provides hard drives information including the total disk size and current usage for tracking purposes.

#### **4.8.1.4 Hardware Inventory Report**

The Report Manager Hardware Inventory Report displays hardware assets that have been discovered on a network.

#### **4.8.1.5 Hardware Upgrade Planning Report**

This report displays hardware assets with components below a minimum hardware configuration that you specify.

#### **4.8.1.6 Last Boot Up Time and Logged In User by Device**

This report displays the last boot-up time and logged-in user for each device on the customer's network.

#### **4.8.1.7 License Key Inventory**

This report provides a list of license keys detected in your environment.

#### **4.8.1.8 License Usage and Comparison Report**

The System License Usage Report presents detailed system license usage information. This report aides the decision for the purchase of additional licenses.

#### **4.8.1.9 Managed Devices by Operating System**

This report displays the breakdown of the number of devices by operating system for the selected customer.

#### **4.8.1.10 Managed Devices SLA Report**

This report displays all devices on a network and identifies them as managed (added or imported to N-central) or unmanaged (discovered but not imported).

#### **4.8.1.11 Managed Devices Summary**

This report displays the breakdown of the number of devices by operating system, devices by device class and a list of devices being monitored for each configured service.

#### **4.8.1.12 Managed Devices Versus Time**

This report shows the change in number of managed devices over time.

#### **4.8.1.13 Patch Approval and Installation Comparison**

This report provides a summary of patch counts, by approval and installation status for one or more customers. Run this report to show how patch installation statuses compares to what has been approved.

#### **4.8.1.14 Patch Details**

This report provides detailed patch information for one or more customers within a specified time period. You can group the report to list patches for each device or devices associated with each patch.

#### **4.8.1.15 Printer Consumables Report**

This report provides an overview of printer paper and toner usage over the reporting period.

#### **4.8.1.16 Shared Folders Overview**

This report lists all shared folders on all devices on the customer's network.

#### **4.8.1.17 Software Inventory Report**

The Software Inventory Report displays discovered software on a network and the devices on which software has been installed.

### **4.8.2 Managed IT Services**

#### **4.8.2.1 Application Availability Report**

This report provides the average availability of services by device.

#### **4.8.2.2 AV Status Report**

The AV Status report summarizes information gathered by the AV Status service on the state of various AV solutions across a customer. For either or Sophos, Symantec Endpoint Protection, Kaspersky and Trend Micro

#### **4.8.2.3 Availability Comparison Report**

This report provides the average availability for all devices and services, and compares them on a daily, weekly, or monthly basis.

#### **4.8.2.4 Capacity Planning Report**

This report provides an overview of the utilization capacity for a customer's devices. In addition, you have the option to display details for each device that is approaching the utilization limit.

#### **4.8.2.5 Data Protection Report**

This report provides the status of customer backup jobs.

#### **4.8.2.6 Downtime Cost Impact Report**

This report provides the cost of downtime of service groupings and calculates the cumulative cost of downtime.

#### **4.8.2.7 Executive Summary Report**

This report allows you to provide a brief Scorecard view of current device statuses in key network areas, with options to include comprehensive summaries, work done and more details where applicable.

#### **4.8.2.8 Health Quick View**

This report provides a summary view of the Top 5 critical devices in several system health categories.

#### **4.8.2.9 Monthly Availability Comparison**

The Monthly Availability Comparison report provides month-to-month availability comparison across selected services for the specified number of months before the report generation date.

#### **4.8.2.10 Network Assessment Report**

This report allows you to provide a complete summary of a customer's network that can be used to support a major project or a proposal for Managed Services.

#### **4.8.2.11 Network Health Overview Report**

This report provides a detailed assessment of a network, by availability and performance. It also provides SLA compliance metrics and uptime for key services, such as email and ecommerce applications.

#### **4.8.2.12 Network Oversight Report**

This report provides an overall view of the monitored network: summary of the top 5 critical devices, service availability, utilization details and backup status.

#### **4.8.2.13 Notification Summary Report**

This report provides information on notifications by customer, method, and profile for a specified period.

#### **4.8.2.14 Patch Status**

This report provides a summary of patch status for one or more customers as of a period end date. Run this report to determine if customer environments are up-to-date and see patch counts for each device.

#### **4.8.2.15 Resource Utilization Report**

This report provides a historical overview of CPU, physical memory, virtual memory and disk utilization.

#### **4.8.2.16 Service Availability Report**

This report provides a view on how available the network infrastructure was over the reporting period.

#### **4.8.2.17 Service Dashboard Report**

This report allows you to view the availability of selected services compared to specified thresholds over time.

#### **4.8.2.18 Site Overview Report**

This report is a one-page executive summary of the customer's network.

#### **4.8.2.19 Technical Summary Report**

This report provides a summary of the utilization of CPU, disk, and memory. It also provides details on traffic, availability, and notifications.

#### **4.8.2.20 Ticket Summary Report**

This report provides a high-level summary of open tickets versus closed, average time to resolution, and open ticket age, as well as specific details for each ticket opened within the report period.

#### **4.8.2.21 Traffic Usage Report**

This report provides an overview of the traffic utilization of customer internet devices.

#### **4.8.2.22 Utilization Comparison Report**

This report displays server usage over time for the selected devices.

### **4.8.3 Managed Security**

#### **4.8.3.1 Alert by Category**

Provides Event Log alerts for each category by hour.

#### **4.8.3.2 Alert Summary by Category**

Provides summary of Event Log alerts grouped by category.

#### **4.8.3.3 Critical Error Report**

Provides information on critical Event Log errors by hour.

#### **4.8.3.4 Firewall Incident Trend Report**

This report provides a summary of firewall incidents over time and a breakdown of the incident severity.

#### **4.8.3.5 Incident Summary**

The Incident Summary report shows the number of NOC incidents for each device on a selected customer's network (in descending order) for the specified reporting period.

#### **4.8.3.6 Open Ports Overview**

This report provides a chart of the number of devices by service and information on all open ports detected in your environment.

#### **4.8.3.7 Remote Control Usage**

This report allows you to report on Remote Desktop Support and managed device remote control sessions.

#### **4.8.3.8 Security Alert**

Provides detailed information on Event Log security alerts.

### **5. Configuration settings**

#### **5.1 Asset / Device Discovery – Adding jobs to discover either once of or recurring schedule.**

#### **5.2 Domain user management – Unlock; Enable; Disable; Delete; Reset password; Audit Trial**

#### **5.3 Filter – need to be configured as per user requirements as drop-down options for any discovery job or monitoring or managing function or to define search criteria.**

#### **5.4 Backup Solution**

##### **5.4.1 Dashboard –**

##### **5.4.1.1 Devices (Servers and Workstations)**

##### **5.4.1.2 Microsoft 365 user accounts**

##### **5.4.1.3 Show % of successful backups.**

##### **5.4.1.4 Show % of successful backup in last 24 hours.**

##### **5.4.1.5 Provide configurable integration into backup solution to onboard additional Servers or devices.**



## 5.5 Monitoring

- 5.5.1 Application compliant rules
- 5.5.2 Application compliant settings – all discovered applications and self-selected applications
- 5.5.3 Dashboards – add, remove and create own dashboards.
- 5.5.4 License Compliance – define licenses in environment to monitor for compliance.
- 5.5.5 Wizard to setup monitoring for Service templates, Dashboards, Notifications and Rules
- 5.5.6 Notifications – who receives notifications for various alarms.
- 5.5.7 Rule to be defined for various filters.
- 5.5.8 Service groupings to be monitored.
- 5.5.9 Service templates to standardise on groupings and other to be monitored.
- 6. Patch Management should at least include the following.
  - 6.1 Patch management setup wizard.
  - 6.2 Patch approval by: Patch, Device or automatic approvals.
  - 6.3 Patch enabled rules defining if one or more of the following can be defined- Patch detection, Patch pre-download, Patch installation, System reboot (y/n)
  - 6.4 Patch caching should be available per local site on dedicated device.
  - 6.5 Patch profiles should be able to be defined.
- 7. Scheduling of tasks
  - 7.1 Add / Delete tasks.
  - 7.2 Network share defaults for repositories should be configurable.
  - 7.3 Schedule task profiles to define task for monitoring, self-heal, scanning etc.
  - 7.4 Script/Software repository – system default and own
- 8. Manage security.
  - 8.1 Global exclusion
  - 8.2 Profiles
  - 8.3 Quarantine Management
  - 8.4 Security events
  - 8.5 Update of server's security
- 9. User Management should at least include.
  - 9.1 LDAP server integration
  - 9.2 Two-factor authentication
  - 9.3 User management
  - 9.4 Access group management
  - 9.5 Roles and responsibilities
- 10. Training videos online available accessible through management system clearly categorising the various modules.

## SCHEDULE B – TECHNICAL EVALUATION

The bidder needs to comply to all sections in these technical requirements to be further considered for this rates-based tender.

### 1. Organisational requirements

#### 1.1 Company requirements

The successful bidder must comply to this minimum requirement to be considered for further evaluation.

REQUIREMENT	Proof required	YES / NO	REFERENCE PAGE NUMBER IN YOUR SUBMISSION DOCUMENTATION
Valid and current certifications of the relevant people to be involved in the project as per the requested accreditation list.	CV with certified certificates		
NIST CSF control mapping for the proposed solution	Part of work plan.		
Recommended Project Methodology and approach	As per section 3.11 of this document		
A high-level draft Implementation Plan	Submitted Plan		

## 1.2 Support staff requirements

To ensure that Cape Agulhas Municipality receive proposals with the highest standards of cybersecurity resilience and compliance, the bidders are required to supply proof of specific competencies and industry-recognized certifications across cybersecurity, risk management, and operational resilience. The following certifications are required to fulfil the scope of the tender all of these certifications should be held by qualified team members actively involved in the project execution:

Certification	Acronym	Synopsis	Authorised industry Standards Body	Further Information - Accreditation	Further Information - Accreditation
ISO 27001 Lead Implementer	ISO 27001 LI	An ISO/IEC 27001 Lead Implementer is a professional certification for individuals specializing in implementing and managing Information Security Management Systems (ISMS) based on the ISO/IEC 27001 standard, ensuring organizations meet the requirements of the standard.	<a href="https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27001/iso-iec-27001-lead-implementer">https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27001/iso-iec-27001-lead-implementer</a>	<a href="https://pecb.com/en/about">https://pecb.com/en/about</a>	<a href="https://www.iasonline.org/?post_type=ias_certificate&amp;orderby=org&amp;order=ASC&amp;s=&amp;global=1&amp;service=13574&amp;keyword=PECB&amp;number=&amp;org=&amp;city=&amp;state=&amp;country=&amp;zip=&amp;status=">https://www.iasonline.org/?post_type=ias_certificate&amp;orderby=org&amp;order=ASC&amp;s=&amp;global=1&amp;service=13574&amp;keyword=PECB&amp;number=&amp;org=&amp;city=&amp;state=&amp;country=&amp;zip=&amp;status=</a>
ISO 27001 Lead Auditor	ISO 27001 LI	An ISO 27001 Lead Auditor is a professional certified to conduct audits of an organization's Information Security Management System (ISMS) to ensure it complies with the ISO 27001 standard.	<a href="https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27001/iso-iec-27001-lead-auditor">https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27001/iso-iec-27001-lead-auditor</a>	<a href="https://pecb.com/en/about">https://pecb.com/en/about</a>	<a href="https://www.iasonline.org/?post_type=ias_certificate&amp;orderby=org&amp;order=ASC&amp;s=&amp;global=1&amp;service=13574&amp;keyword=PECB&amp;number=&amp;org=&amp;city=&amp;state=&amp;country=&amp;zip=&amp;status=">https://www.iasonline.org/?post_type=ias_certificate&amp;orderby=org&amp;order=ASC&amp;s=&amp;global=1&amp;service=13574&amp;keyword=PECB&amp;number=&amp;org=&amp;city=&amp;state=&amp;country=&amp;zip=&amp;status=</a>
Certified Governance Risk and Compliance	CGRC	A Certified Governance, Risk, and Compliance (GRC) Professional is an individual with validated expertise in aligning IT and business strategies, managing risks, and ensuring an organization adheres to laws and regulations. This certification demonstrates a professional's ability to integrate governance, risk management, and compliance functions to achieve business objectives while mitigating potential threats.	<a href="https://www.isc2.org/certifications/cgrc">https://www.isc2.org/certifications/cgrc</a>	<a href="https://www.isc2.org/about">https://www.isc2.org/about</a>	<a href="https://anab.ansi.org/about-anab/">https://anab.ansi.org/about-anab/</a>
Multi Cloud Red Team Analyst	MCRTA	A multi-cloud red teaming analyst is a cybersecurity professional who simulates cyberattacks on an organization's systems that are spread across multiple cloud providers like AWS, Azure, and GCP. They identify and exploit misconfigurations and vulnerabilities in these diverse environments to help organizations improve their security posture and prepare for real-world threats.	<a href="https://cyberwarfare.live/product/multi-cloud-red-team-analyst-mcрта/">https://cyberwarfare.live/product/multi-cloud-red-team-analyst-mcрта/</a>	<a href="https://cyberwarfare.live/about-us/">https://cyberwarfare.live/about-us/</a>	Not Applicable

Certification	Acronym	Synopsis	Authorised industry Standards Body	Further Information - Accreditation	Further Information - Accreditation
Cybersecurity Analyst+	CYSA+	(Cybersecurity Analyst+) is an intermediate-level certification for IT professionals that validates skills in threat detection, incident response, and vulnerability management. It focuses on using behavioral analytics to protect networks and devices through continuous security monitoring, and it prepares professionals for roles like Security Analyst or Incident Responder. The certification demonstrates expertise in analyzing security data to identify and address threats and vulnerabilities.	<a href="https://www.comptia.org/en-za/certifications/cybersecurity-analyst/">https://www.comptia.org/en-za/certifications/cybersecurity-analyst/</a>	<a href="https://www.comptia.org/en-za/about-us/">https://www.comptia.org/en-za/about-us/</a>	<a href="https://anabpd.ansi.org/Accreditation/credentialing/personnel-certification/AllDirectoryDetails?&amp;prgID=201&amp;OrgId=93&amp;statusID=4">https://anabpd.ansi.org/Accreditation/credentialing/personnel-certification/AllDirectoryDetails?&amp;prgID=201&amp;OrgId=93&amp;statusID=4</a>
Certified Ethical Hacker	CEH	A Certified Ethical Hacker (CEH) is a cybersecurity professional who is trained to use the same tools and techniques as malicious hackers to find and report vulnerabilities in a computer system, with permission. This certification, offered by EC-Council, validates an individual's skills in assessing security and handling cyber threats in a legal and ethical manner. CEH-certified professionals are skilled in areas like network scanning, vulnerability analysis, and preventing attacks like SQL injection and cross-site scripting.	<a href="https://www.eccouncil.org/train-certify/certified-ethical-hacker-ceh/">https://www.eccouncil.org/train-certify/certified-ethical-hacker-ceh/</a>	<a href="https://www.eccouncil.org/about/">https://www.eccouncil.org/about/</a>	<a href="https://anab.ansi.org/about-anab/">https://anab.ansi.org/about-anab/</a>
Certified Incident Handler	CIH	An EC-Council Certified Incident Handler (ECIH) is a cybersecurity professional who has been certified in a structured process for responding to and managing security incidents. This certification signifies expertise in a wide range of skills, from preparing for and identifying incidents to containing, eradicating, and recovering from them, all while minimizing financial and reputational damage to an organization.	<a href="https://www.eccouncil.org/train-certify/ec-council-certified-incident-handler-ecih/">https://www.eccouncil.org/train-certify/ec-council-certified-incident-handler-ecih/</a>	<a href="https://www.eccouncil.org/about/">https://www.eccouncil.org/about/</a>	<a href="https://anab.ansi.org/about-anab/">https://anab.ansi.org/about-anab/</a>

## 2. Network Access & Security Assessment Tool

NO	REQUIREMENTS	COMPLIANCE	
		YES	NO
1	<b>Authorization of new Devices to be Added to Restricted Networks</b> Restricted networks should be tightly controlled to conform to strict network change management policies and procedures. Implementing security controls and applying consistent policies can help protect the organization from these security threats. We need to receive an alert with recommended actions to be taken when new devices have been added to any network segment designated as restricted.		
2	<b>Investigate Suspicious Logons by Users</b> Computer user login attempts by a particular user that are made outside of normal time frame patterns or from an unusual location indicates behaviour consistent with unauthorized user access or malicious software. When this event is detected, we need to receive an email alert warning of the suspicious activity with recommended actions to be taken.		
3	<b>Investigate Suspicious Logons to Computers</b> Attempts to access a computer using login credentials not normally associated with that particular computer could point to unauthorized user access or use of malicious software. When this event is detected, we need to receive an email alert warning of the suspicious activity with recommended actions to be taken.		
4	<b>Strictly Control the Addition of Printers</b> Network printers are vulnerable to security risks. Connecting to and printing from an unauthorized printer can lead to information loss. Anytime a new printer is found on the network, we need to receive an alert notifying us with recommended actions to be taken to ensure that it is authorized to prevent any potential threat.		
5	<b>Restrict Access to Computers with specified roles.</b> Computers on the network that are used to transmit, process, or store sensitive information and records which should only be accessed by authorized users. Trying to prevent users from accessing these resources through group policies, restricted logons and other network "hardening" is best practice. However, we still need to know when unauthorized users attempt to access sensitive systems and login to one of these machines. We need to receive an email alert when unauthorized user attempts to login to one of these computers with recommended actions to be taken.		

### 3. Cloud Application Activity & Security Monitoring

NO	REQUIREMENTS	COMPLIANCE	
		YES	NO
1	<b>Authorization of New Cloud Accounts</b> All new cloud user accounts created within Azure AD must be strictly controlled to ensure identity governance and prevent unauthorized access. Alerts should be generated in real time whenever a new account is added, including recommended actions to verify legitimacy and apply security controls.		
2	<b>Authorization of Privilege Role Assignments</b> Monitoring is required for all privilege escalations, such as Global Admin, Exchange Admin, SharePoint Admin, or Teams Admin assignments. Alerts must provide context on the account performing the change and recommended steps to validate and remediate if necessary.		
3	<b>Suspicious Sign-in Activity Detection</b> Login attempts from unusual locations, impossible-travel patterns, legacy authentication protocols, or unfamiliar IP ranges must trigger alerts. Reports should include device information, geolocation, and suggested remediation steps to mitigate potential breaches.		
4	<b>Suspicious Sign-ins to Admin Portals</b> Unauthorized attempts to access administrative portals (Azure AD, Exchange Admin Center, Security & Compliance Center, SharePoint Admin, Teams Admin) should trigger immediate alerts with recommended follow-up actions for investigation and account lockout if necessary.		
5	<b>Monitoring of Multi-Factor Authentication Changes</b> Any enablement, disablement, or failed attempts of multi-factor authentication for users should generate alerts, including guidance on verifying user identity and ensuring MFA policies are enforced.		
6	<b>Account Lockouts and Authentication Failures</b> Multiple failed login attempts or account lockouts must be tracked and reported. Alerts should include account details, source IP, and suggested remediation steps to investigate possible brute-force attacks or compromised credentials.		
7	<b>Tracking Creation, Modification, and Deletion of Users</b> All user account lifecycle events, including creation, updates, and deletions, must be logged for auditing purposes. Alerts should provide full context of changes to enable quick detection of unauthorized modifications.		
8	<b>Privileged Account Activity Monitoring</b> Activities performed by privileged accounts, including logins, configuration changes, and access to sensitive resources, must be monitored. Alerts should highlight unusual activity and include recommended actions for review and verification.		
9	<b>Group Membership Changes</b> Changes to security or distribution groups, including creation, deletion, or modifications, must trigger alerts. Reports should highlight who made the change and potential impacts on access permissions.		
10	<b>File Sharing Monitoring – External</b> Files shared externally from OneDrive or SharePoint must be tracked. Alerts should identify sensitive content exposure, unauthorized recipients, and provide remediation guidance such as revoking access.		
11	<b>File Activity Monitoring – Internal</b> Internal file activity, including uploads, downloads, edits, copies, moves, or deletions, should be logged. Alerts should provide visibility into potentially risky or non-compliant activities within internal repositories.		
12	<b>Sensitive Data Movement Detection</b> Events involving sensitive data, such as uploads or sharing of confidential information, must trigger alerts. Recommended remediation actions should include data classification verification and access review.		
13	<b>Mailbox Forwarding Rule Monitoring</b> Creation, modification, deletion, or activation of mailbox forwarding rules must be monitored. Alerts should flag potential email exfiltration attempts and include recommended investigation steps.		
14	<b>Phishing Email Detection and Reporting</b> Monitoring of phishing emails delivered, clicked, or reported by users must trigger alerts. Reports should provide insight into affected users, potential risk, and follow-up remediation actions.		
15	<b>Administrative &amp; Security Activity Tracking for Compliance</b>		

NO	REQUIREMENTS	COMPLIANCE	
		YES	NO
	All administrative and security actions within SaaS applications (including account changes, privilege escalations, policy modifications, and configuration changes) are logged and reported to support compliance monitoring and audit-readiness. Alerts are generated for unusual or high-risk actions, ensuring visibility into activities that could impact compliance.		
16	<b>Integration/API Connection Monitoring</b> Monitoring failed or interrupted connections between cloud services and third-party applications is required. Alerts should include impacted users, applications, and suggested corrective actions to restore secure connections.		
17	<b>Shadow IT Detection</b> Detection of unauthorized SaaS applications or services in use within the environment must generate alerts. Reports should include application name, user adoption, and recommendations to enforce approved app policies.		
18	<b>Service Principal Monitoring</b> Creation, modification, deletion, or use of service principals in Azure AD must be tracked. Alerts should highlight unusual activity, potential automation risks, and recommended review steps.		
19	<b>Risky Sign-in Detection</b> Suspicious login patterns, such as multiple IP logins, logins from foreign locations, or unusual devices, must trigger alerts. Reports should provide full session and device context to facilitate investigation.		
20	<b>Device Activity Monitoring</b> Monitoring new device registrations, logins, logouts, and inactive devices is required. Alerts should detect unauthorized device access and provide guidance on device compliance enforcement.		
21	<b>Security Action Logging</b> Critical actions such as enabling, dismissing, or undoing security configurations must be logged. Alerts should summarize actions, the user performing them, and recommended follow-up.		
22	<b>Individual Account Activity Reporting</b> Detailed reports on user account activity, including authentication, mailbox access, administrative changes, and MFA events, must be available to support audits and investigations.		
23	<b>Organizational File Activity Reporting</b> Reports covering file activity across the organization must provide insight into potential operational or security risks. Reports should highlight sensitive or unusual access patterns.		
24	<b>Risk Assessment Reporting</b> Comprehensive risk assessment reports must evaluate the organization's SaaS security posture, identifying misconfigurations, vulnerabilities, and high-priority issues requiring remediation.		
25	<b>Operational Trend Reporting</b> Trend analysis reports should highlight system usage patterns, security events, and operational anomalies to support proactive management and planning.		
26	<b>Executive Summary Reporting</b> Executive-level summaries must consolidate alerts, risk trends, and remediation actions into clear, digestible formats for leadership decision-making.		
27	<b>Scheduled Report Distribution</b> All security and activity reports must support automated scheduling and delivery to relevant stakeholders, ensuring timely visibility of critical events.		
28	<b>External File Exposure Alerts</b> Detection and alerting for files shared outside approved domains, including external recipients, must include actionable recommendations for access revocation or further investigation.		
29	<b>Security Policy Violation Detection</b> Any deviation from security policies, including conditional access, password complexity, or administrative controls, must trigger alerts and provide remediation guidance.		
30	<b>Remediation Action Tracking</b> The platform must track the completion of all recommended remediation actions following security incidents, ensuring accountability and audit compliance.		

#### 4. Dark Web Monitoring

NO	REQUIREMENTS	COMPLIANCE	
		YES	NO
1	Monitor its corporate domain on the dark web for stolen user credentials (emails/passwords)		
2	Monitor the personal email addresses of the Executive Management and other identified employees. The system will need to monitor at least an accumulative total of 10 personal email in addition to those within the client's corporate domain.		
3	Provide a report/list of the any user credentials (emails/passwords) found on the dark web.		
4	Provide a report with recommendations to remedy or mitigate any risks with any reported user credentials (emails/passwords) found, including recommendations to avoid future recurrence.		
5	Integration - Automated ability to test compromised website credentials on the Pen Test platform.		

#### 5. Security Awareness Training & Phishing Simulation Requirements

NO	REQUIREMENTS	COMPLIANCE	
		YES	NO
1	<b>Training Topic Coverage</b> Training content must span all core cybersecurity domains, including phishing recognition, password hygiene, secure device usage, social engineering tactics, ransomware prevention, safe browsing behaviour, email security, data privacy fundamentals, and incident reporting best practices.		
2	<b>Training Content Library Size</b> The platform must provide a substantial training library containing at least 50+ modules, including videos, interactive lessons, micro-learning segments, and refresher content to support ongoing cybersecurity education throughout the year.		
3	<b>Multi-Language Training Support</b> Training content must be available in multiple languages, ensuring accessibility and comprehension for multilingual user populations.		
4	<b>Training Campaign Creation</b> The system must allow administrators to design structured training campaigns, select specific modules, specify campaign durations, set due dates, and assign content to individual users or defined groups.		
5	<b>Multiple Course Assignment Per Campaign</b> The platform must support assigning multiple training modules within a single campaign, enabling bundled learning paths for deeper awareness development.		
6	<b>Training Invitation Customisation</b> Training invitation emails must be fully customisable, allowing administrators to adjust wording, branding, and messaging to better engage users.		
7	<b>Integrated Quizzes &amp; Knowledge Checks</b> Each training module must include built-in quizzes, assessments, or knowledge checks to validate user understanding and measure learning outcomes.		
8	<b>Training Progress Tracking</b> Administrators must have access to detailed tracking dashboards showing user progress, completion percentages, overdue items, and overall training engagement rates.		
9	<b>Automated Reminder Notifications</b> The platform must send automated reminders to users with incomplete training based on configurable intervals.		
10	<b>User-Level Performance History</b> The system must maintain a historical timeline of each user's training performance, allowing administrators to identify long-term trends, improvement, or recurring areas of weakness.		
11	<b>SANS Model Alignment</b> The programme must include a metrics framework that aligns with SANS best practices, enabling tracking of behaviour change, communication effectiveness, and overall maturity progression.		
12	<b>Phishing Template Library</b> The platform must include a professionally developed library of phishing templates and landing pages that reflect real-world attack techniques, including brand impersonation, business email compromise, and notification-based lures.		



NO	REQUIREMENTS	COMPLIANCE	
		YES	NO
13	<b>Varying Difficulty Levels</b> Templates must include multiple difficulty tiers (e.g., basic, intermediate, advanced) to support progressive testing of user maturity across the organisation.		
14	<b>Custom Phishing Template Editing</b> Administrators must be able to edit or create phishing templates using HTML or built-in editing features, enabling customised scenarios tailored to organisational context.		
15	<b>Phishing Campaign Scheduling</b> Phishing campaigns must support advanced scheduling options including specific start/end times, staggered rollouts, organisational group targeting, and configurable delivery windows.		
16	<b>Randomised Email Delivery</b> The system must support randomised email distribution within a defined time window to reduce campaign predictability and simulate realistic adversary behaviour.		
17	<b>Attachment-Based Phishing</b> The platform must support simulations that include attachments such as PDFs or Microsoft Office files, enabling realistic testing of attachment-based threat vectors.		
18	<b>Credential Capture Simulation</b> Landing pages must support simulated credential-entry forms to assess user behaviour when interacting with suspicious prompts, without storing actual credentials or compromising user data.		
19	<b>Phishing Interaction Tracking</b> The system must track comprehensive user interactions including email opens, clicks, attachment opens, form submissions, and timestamped behavioural indicators.		
20	<b>Automated Remedial Training Assignment</b> The platform must automatically assign targeted training modules to users who fail phishing simulations, based on configurable triggers such as link clicks, attachment opens, or credential-entry attempts.		
21	<b>Real-Time Dashboards</b> Administrators must have access to dynamic dashboards that provide consolidated visibility of training progress and phishing statistics		
22	<b>Campaign Result Drill-Down</b> The platform must provide detailed drill-down capability that allows administrators to inspect individual user events for both training and phishing activities, with timestamps and behavioural context.		
23	<b>Exportable Reporting</b> All reports must be exportable in formats such as CSV or PDF to support offline analysis, executive reporting, and compliance documentation.		
24	<b>Scheduled Reporting</b> The platform must support automated delivery of scheduled reports to predefined recipients, enabling consistent oversight by management or compliance teams.		
25	<b>Directory &amp; User Synchronisation</b> Administrators must be able to manage users via CSV import or synchronise user and group data through directory-based integration methods to maintain accuracy and reduce manual effort.		
26	<b>Role-Based Access Controls</b> The system must include multiple administrative permission levels, allowing granular access control based on assigned roles and responsibilities.		
27	<b>Multi-Factor Authentication for Administrators</b> Administrative access must be protected by multi-factor authentication to ensure secure login and prevent unauthorised access to the management portal.		
28	<b>Audit Logging</b> All critical platform actions, including user enrolments, campaign changes, administrator activities, and user events, must be logged in audit trails to support compliance and investigations.		
29	<b>Deliverability &amp; Safe-Listing Guidance</b> The vendor must provide comprehensive safe-listing and email configuration guidance to ensure reliable delivery of training notifications and phishing simulation emails across various mail environments.		
30	<b>User-Level Performance History</b> The system must maintain a historical record of each user's phishing and training performance over time to show behavioural improvement or regression.		

## 6. Penetration Testing functional requirements.

NO	REQUIREMENTS	COMPLIANCE	
		YES	NO
1	The system should be an automated penetration testing platform and help the organization solve compliance requirements by achieving security best practices and researching multiple vendors to compare numerous factors to meet their offensive security needs. The system should be based on a framework that continuously improves as new threats emerges and existing threats evolve.		
2	<b>System features should include:</b>		
	<ul style="list-style-type: none"> <li>Real-time Activity Tracking</li> </ul>		
	<ul style="list-style-type: none"> <li>The system can perform penetration tests at any time using a scheduler e.g. if/where required to do testing out of business hours this can be scheduled</li> </ul>		
	<ul style="list-style-type: none"> <li>Egress Filtering Testing</li> </ul>		
	<ul style="list-style-type: none"> <li>Authentication Attacks</li> </ul>		
	<ul style="list-style-type: none"> <li>Privilege Escalation &amp; Lateral Movement</li> </ul>		
	<ul style="list-style-type: none"> <li>Data Exfiltration simulation</li> </ul>		
	<ul style="list-style-type: none"> <li>Simulated Malware</li> </ul>		
	<ul style="list-style-type: none"> <li>Grey Box and White Box Tests</li> </ul>		
	<ul style="list-style-type: none"> <li>Reports available within 3 business Days</li> </ul>		
3	<b>System evaluations for Internal and External Network Testing:</b>		
	<ul style="list-style-type: none"> <li>User Profiling</li> </ul>		
	<ul style="list-style-type: none"> <li>Reputational Threats</li> </ul>		
	<ul style="list-style-type: none"> <li>Intelligence Gathering</li> </ul>		
	<ul style="list-style-type: none"> <li>Vulnerability Analysis</li> </ul>		
	<ul style="list-style-type: none"> <li>Exploitation</li> </ul>		
	<ul style="list-style-type: none"> <li>Post-Exploitation</li> </ul>		
4	<b>Internal Network Penetration Testing</b> The System should be able to use an internal physical, or virtual, device connected to the internal environment to discover security vulnerabilities present within the internal network environment. These activities should simulate that of a malicious attacker.		
5	<b>External Network Penetration Testing</b> The System should be able to assume the role of a malicious attacker from the public Internet and identify flaws within the external network environment. These vulnerabilities should include patching, configurations, and authentication issues		
6	<b>Reports and Progress:</b>		
	<ul style="list-style-type: none"> <li>(Optional) Real-Time Status Updates - Email and SMS notifications can be sent out to establish up-to-date progress and activities</li> </ul>		
	<ul style="list-style-type: none"> <li>Executive Summary Report</li> </ul>		
	<ul style="list-style-type: none"> <li>Technical Report</li> </ul>		
	<ul style="list-style-type: none"> <li>Vulnerability Report</li> </ul>		
	<ul style="list-style-type: none"> <li>Activity Report</li> </ul>		
	<ul style="list-style-type: none"> <li>Evidence Artifacts</li> </ul>		
	<ul style="list-style-type: none"> <li>Consolidated Report</li> </ul>		
7	System should have SOC2 Compliance		
8	The Platform should have Crest Accreditation		
9	The Platform must integrate into the Vulnerability Management platform		
10	The Platform must have the automation capability to test the compromised credentials of a user found on the Dark Web platform		
11	System must be securely hosted online and have an audit trail for activity.		

## 7. Security Operations Centre (SOC)

NO	REQUIREMENTS		COMPLIANCE	
			YES	NO
1	The solution must make provision for endpoint monitoring			
2	The solution must make provision for Network Security			
3	The solution must make provision for M365 security, Azure AD monitoring, M365 malicious logins and Microsoft secure score monitoring.			
4	Full alert process is clearly defined and described for each stage. <ul style="list-style-type: none"> <li>Category A (High severity/risk)</li> <li>Category B (Medium severity/risk)</li> <li>Category C (Low severity/risk)</li> </ul> See section "Threat Detection, Classification and Alert Notification"			
5	The solution must make provision for 24/7/365 monitoring with human SOC analysts			
6	Full Cloud solution with no additional hardware requirements			
7	All log monitoring must be available in a single platform			
8	Must make provision for real time threat monitoring			
9	Breach detection must be aligned to MITRE ATT&CK			
10	The solution must provide for Intrusion monitoring			
11	The solution must make provision for the following.			
	Dark Web monitoring	Switches & Routers		
	Cloud – MS Azure, Amazon	Office 365		
	Anit-Virus mail protection	Domain Controllers		
	Anti-Virus / Endpoint protection	Servers (IIS, Windows, Exchange,)		
	Advanced Threat Protection	Web Application Firewall / Physical Firewall		
12	The solution must make provision for all of the following types of monitoring.			
	Advance breach detection	Crypto Mining detection		
	Cyber Terrorist Network Connections	Ransomware Detection		
	Endpoint Event Log Monitor	Firewall Log Analyzer		
	IOC Detection	Log4j Detection		
	Malicious File Detection	Microsoft Exchange Threat Detection		
	Office 365 Login Analysing	Office 365 Log Monitoring		
	Office 365 Risk Detection	Office 365 Secure Score		
	Print nightmare vulnerability protection	Pwnd Monitoring		
	Sophos Monitoring Central and physical firewall(s)	Suspicious Network Services Monitoring		
	Suspicious Tools Monitoring	Defender for Business monitoring		
	Report on vulnerabilities from Network access policy system see 4.2.1.	Exchange Hafnium Exploit monitoring		
	DnsFilter Monitoring	Provide Windows Defender Manager capabilities.		
	Specify additional detections.			

## 8. SIEM, Log Management & Security Automation Requirements

NO	REQUIREMENTS	COMPLIANCE	
		YES	NO
1	<b>Multi-Source Log Collection</b> The system must ingest logs from multiple sources including endpoints, servers, network devices, cloud services, and third-party applications to support centralised security monitoring.		
2	<b>Standard Log Protocol Support</b> The solution must support industry-standard log ingestion methods such as Syslog, APIs, and agent-based collection to ensure broad compatibility across the environment.		
3	<b>Custom Log Source Integration</b> The platform must allow the addition and parsing of custom log sources or applications to extend monitoring capabilities beyond native integrations.		
4	<b>Long-Term Log Storage</b> Long-term storage of security logs must be supported to meet investigation, audit, and compliance requirements.		
5	<b>Log Encryption</b> All logs must be encrypted both at rest and in transit to ensure data privacy and prevent tampering.		
6	<b>Historical/Raw Log Access</b> Historical or raw log data must be accessible for deep-dive forensic investigations when required.		
7	<b>Custom Correlation Rules</b> The solution must support the creation of custom correlation rules to detect complex attack patterns and environment-specific risks.		
8	<b>Built-In Detection Rules</b> Pre-configured detection rules or signatures must be included to support immediate security value upon deployment.		
9	<b>Automated Event-Triggered Actions</b> The platform must be able to trigger automated actions when specific events or alerts occur to support rapid response.		
10	<b>Behavioural/Machine Learning Analytics</b> Anomaly detection using behavioural analytics or machine learning must be supported to detect deviations from normal activity.		
11	<b>Custom Indicators of Compromise (IoCs)</b> The system must support the creation and management of custom IoCs to track and respond to organisation-specific threats.		
12	<b>Threat Intelligence Integration</b> Integration with external threat intelligence feeds must be supported to enhance detection of emerging threats.		
13	<b>Customizable Indicator Response Actions</b> Response actions associated with detected indicators must be fully customisable.		
14	<b>Real-Time Alert Generation</b> Alerts must be generated in real-time to support rapid investigation and response.		
15	<b>Configurable Alert Severity</b> Alert priority or severity levels must be configurable based on organisational policies and risk levels.		
16	<b>Alert Integration with External Systems</b> Alerts must integrate with external systems (e.g., ITSM, SOAR, PSA, ticketing platforms) to support automated workflows.		
17	<b>Advanced Log Search &amp; Filtering</b> Users must be able to search, filter, pivot, and analyse logs with advanced query capabilities.		
18	<b>Event Timelines for Investigations</b> The system must provide interactive event timelines to support structured investigations.		
19	<b>Log Export Capability</b> Logs must be exportable for offline analysis or ingestion into external forensic or audit tools.		
20	<b>Pre-Built Dashboards</b> The platform must include pre-built dashboards offering visibility into system health, threats, and operational activity.		
21	<b>Scheduled Reporting</b> Reports must support automated scheduling (e.g., daily, weekly, monthly) and delivery to defined stakeholders.		
22	<b>Automation Audit Logs</b> All automated actions must be logged and auditable to support governance and compliance.		
23	<b>Cross-Platform Automation Execution</b> Automated workflows must support actions across multiple platforms, tools, and security systems.		
24	<b>Multi-Factor Authentication</b>		

NO	REQUIREMENTS	COMPLIANCE	
		YES	NO
	Access to the platform must support multi-factor authentication for enhanced security.		
25	<b>Audit Logging of All Actions</b> All user activities and system actions must be logged for auditing and compliance tracking.		
26	<b>Exportable Audit Logs &amp; Reports</b> Audit reports and log data must be exportable for submission to auditors or regulatory bodies.		
27	<b>High-Volume Event Handling</b> The system must support high event ingestion rates (events per second/day) without degradation of performance.		
28	<b>Third-Party Tool Integration</b> Integration with other IT, security, and monitoring tools must be supported to enhance interoperability.		
29	<b>Advanced Behavioural Baseline Profiling</b> The system must detect anomalies by establishing baselines of normal user or device behaviour using machine learning or adaptive analytics.		
30	<b>API Availability</b> A full API must be available for querying data, managing configurations, and executing automated actions.		
31	<b>Advanced Workflow Logic Support</b> Automated workflows must support conditional logic, branching actions, approval steps, and integrations beyond native tools.		

## 9. IT Documentation & Knowledge Management Platform Requirements

NO	REQUIREMENTS	COMPLIANCE	
		YES	NO
1	<b>Centralised Documentation Repository</b> The platform must provide a single repository where all IT documentation is stored and accessible to authorised personnel. It must support structured categorisation to allow users to locate documents quickly and efficiently.		
2	<b>Organisational / Client Hierarchy Structure</b> The system must allow documentation to be organised into multi-level hierarchies such as organisation → location → system → document. Administrators must be able to assign ownership and manage access at each level.		
3	<b>Pre-Built Documentation Templates</b> The platform must provide a library of pre-built templates for SOPs, troubleshooting guides, onboarding materials, and network diagrams. Users must be able to apply these templates to new documentation to maintain consistent structure.		
4	<b>Custom Documentation Templates</b> Administrators must be able to create and configure custom templates tailored to specific processes or workflows. The system must allow these templates to include custom fields, formatting, and content blocks.		
5	<b>Rich Document Editor</b> The platform must provide an editor that supports tables, images, code blocks, embedded media, and file attachments. Users must be able to format documents with advanced styling and organise content for clarity.		
6	<b>Document Versioning</b> All documentation must maintain a full version history with the ability to revert to previous versions. Users must be able to compare changes between versions to track updates accurately.		
7	<b>Linked Documentation Items</b> Documentation must allow linking between assets, systems, passwords, contacts, and related documents. Links must update dynamically when associated items are modified or moved.		
8	<b>SOP / Runbook Support</b> The platform must allow creation of structured, multi-step SOPs and runbooks for standard operations. Steps must include detailed instructions, fields for status tracking, and the ability to assign tasks to users.		
9	<b>Task Checklists</b> The platform must provide reusable checklists for onboarding, offboarding, maintenance, and other repeatable tasks. Checklists must support completion tracking and integration with associated documentation.		
10	<b>Knowledge Base Module</b> Users must be able to create and manage knowledge base articles within the platform. Articles must support rich text, attachments, and categorisation for easy navigation.		
11	<b>Document Tagging &amp; Metadata</b>		

NO	REQUIREMENTS	COMPLIANCE	
		YES	NO
	The platform must support tagging, categories, labels, and custom metadata fields for all documents. Users must be able to filter and sort documentation using these attributes.		
12	<b>Global Search Engine</b> The platform must provide a global search function that indexes all documentation, assets, and passwords. Search results must include relevant metadata and support sorting by type and date.		
13	<b>Advanced Search Filters</b> Search must allow filtering by document type, category, template, asset type, and custom fields. Users must be able to combine multiple filters for precise results.		
14	<b>Relationship Mapping Engine</b> The system must visually map relationships between assets, systems, passwords, and documentation. Users must be able to navigate these maps interactively to understand dependencies.		
15	<b>Configuration (Asset) Documentation</b> The platform must provide dedicated pages to document servers, workstations, network devices, cloud services, and applications. Users must be able to associate configuration items with related documents and passwords.		
16	<b>Flexible Asset Types</b> Administrators must be able to define custom asset types with associated fields. Custom types must support all standard features including relationships, attachments, and metadata.		
17	<b>Asset Relationship Linking</b> Assets must be linked to related systems, users, passwords, and documents. These relationships must update automatically when associated items change.		
18	<b>Password Vault</b> The platform must provide a secure password repository for storing all credentials. Users must be able to organise passwords by system, group, or client.		
19	<b>Permission-Based Password Access</b> The system must allow granular access controls for each password or vault. Administrators must be able to assign read, write, or admin permissions to individuals or groups.		
20	<b>Password Versioning &amp; Logging</b> All password changes must be tracked and versioned automatically. The platform must allow auditing of password access and modifications by user and timestamp.		
21	<b>Personal/Team Password Vaults</b> Users must be able to store personal credentials in a private vault. Teams must have shared vaults that enforce access permissions and auditing.		
22	<b>Password Injection (Browser Extension)</b> The system must provide a secure browser extension to inject credentials into login forms without exposing passwords. Credentials must never be visible in plaintext during auto-fill.		
23	<b>Secure Credential Sharing</b> Administrators must be able to share credentials securely without revealing actual password values. Shared access must respect all permission levels and audit trails.		
24	<b>Contacts &amp; Vendor Management</b> The platform must allow storage of client, vendor, and stakeholder contacts. Users must be able to associate contacts with systems, assets, or documentation.		
25	<b>Network Discovery / Asset Sync</b> The platform must integrate with network discovery and RMM tools to sync devices and configurations. Updates must occur automatically and reflect changes in the infrastructure.		
26	<b>Device Role Identification</b> Assets must be classified by type, role, and operational function. Users must be able to view and filter assets by these classifications.		
27	<b>Automated Configuration Updates</b> Configuration documentation must update automatically when changes are detected in integrated systems. Users must receive notifications of significant updates or discrepancies.		
28	<b>Flexible Import Tools</b> Administrators must be able to bulk import documents, assets, and passwords from CSV or other formats. Imported data must retain relationships, metadata, and field mapping.		
29	<b>Export Functionality</b> The platform must allow exporting of documentation, assets, and passwords in standard formats such as CSV, PDF, or JSON. Exports must preserve structure, metadata, and relationships.		
30	<b>Mobile App Access</b> Users must be able to securely access all documentation and passwords via a mobile app. The app must support search, viewing, and editing of items in real time.		
31	<b>End-User Portal</b>		

NO	REQUIREMENTS	COMPLIANCE	
		YES	NO
	The platform must support a secure portal for clients or end-users to access approved documentation and passwords. Portal access must be fully permission-controlled and configurable per client.		
32	<b>User + Group Access Permissions</b> Administrators must be able to assign role-based access at system, folder, document, and password levels. Permissions must be configurable per user or group and enforceable across all modules.		
33	<b>Single Sign-On (SSO)</b> The system must support SSO via Entra ID, Google Workspace, or SAML providers. Users must be able to authenticate with existing corporate credentials seamlessly.		
34	<b>Multi-Factor Authentication (MFA)</b> The platform must support MFA for all administrative and privileged accounts. MFA must be enforced on login and configurable by administrator.		
35	<b>SOC 2 / ISO 27001 Alignment</b> The platform must maintain SOC 2 or ISO 27001 compliance. Security controls must be documented and auditable by clients.		
36	<b>Audit Logs</b> All system activity must be logged with user, timestamp, and action details. Logs must be searchable and exportable for compliance or operational review.		
37	<b>Time-Stamped Activity Logs</b> Every access, modification, or deletion of documentation, assets, or passwords must be recorded with a timestamp. The system must allow filtering and review of these logs by administrators.		
38	<b>RMM Integration</b> The platform must integrate with RMM tools to synchronise device data, configurations, and status. Integration must allow automated updates to asset documentation and relationships.		
39	<b>Cloud Provider Integration</b> Documentation must link to cloud resources and cloud-based services. Users must be able to view relationships between cloud infrastructure and operational documentation.		
40	<b>Network Diagram Generation</b> The platform must allow creation of network diagrams from discovered relationships. Diagrams must be editable and reflect live changes in asset relationships.		
41	<b>Role-Based Administration</b> Multiple administrative levels must exist with scoped privileges. Administrators must be able to assign roles for operational separation and governance.		
42	<b>API Access</b> The platform must provide a REST API to enable automation and integration with external systems. API endpoints must support reading, writing, and updating documentation, assets, and passwords.		
43	<b>Change Notification Alerts</b> Users must receive notifications when critical documentation, assets, or passwords are updated. Alerts must be configurable by user role and document type.		
44	<b>User Training &amp; Support Resources</b> The vendor must provide training materials, documentation, and community forums for users. Support resources must be accessible for self-learning and troubleshooting platform features.		

The tenderer needs to comply with all sections to be considered for further evaluation.

I HEREBY DECLARE THAT I COMPLY WITH THE TECHNICAL SPECIFICATION AS SET OUT HEREIN.

I FURTHER ACKNOWLEDGE THAT NON-COMPLIANCE WITH ANY ONE OF THE SPECIFICATIONS HEREIN MAY LEAD TO THE CANCELLATION OF A SUCCEEDING AWARD, INCLUDING, BUT NOT LIMITED TO, FINANCIAL PENALTIES.

.....  
Signature

.....  
Date

.....  
Position

.....  
Name of Bidder

## SCHEDULE C – FUNCTIONAL REQUIREMENTS

### Project approach and technical evaluation

	Criteria	Rating	Scoring	Evaluation Indicators	Reference page number in your submission documentation
1.	<b>Adequacy of proposed work plan and proposed methodology</b>	Very Good	100	The important issues are approached in an innovative and efficient way, indicating that the bidder has outstanding knowledge of state-of-the-art approaches. <b>This is clearly linked to all solutions/systems/ services required.</b>	
		Good	70	The approach is specifically tailored to address the specific project objectives and methodology and is sufficiently flexible to accommodate changes that may occur during execution. <b>This is linked to at least 8 of the solutions/system/ services to be provided.</b>	
		Poor	40	The technical approach and/or methodology is poor/is unlikely to satisfy project objectives or requirements. The bidder has misunderstood certain aspects of the scope of work and does not deal with the critical aspects of the project. <b>This is linked to 7 or less of the solutions/systems/ services to be provided.</b>	
2.	<b>Qualifications and competence of the key staff (assigned personnel) in relation to the scope of work. Include short 2-page CV of employees.</b>	Very Good	100	The bidder demonstrates that key staff are exceptionally well qualified and competent in the application of their skills that relate to Cyber- and/or ICT network security projects.. <b>5 years and more.</b>	
		Good	70	The bidder demonstrates that key staff are adequately qualified and competent in the application of their skills that relate to Cyber- and/or ICT network security projects. <b>4 to 5 years</b>	
		Poor	40	The bidder was not able to demonstrate that key staff are reasonably well qualified and competent in the application of their skills that relate to Cyber- and/or ICT network security projects. <b>0 to 3 years.</b>	
3.	<b>Demonstrated bidder's experience. (past performance) in Cyber- and/or ICT network security projects. Include a CV of employees.</b>	Very Good	100	Key staff have outstanding experience in Cyber- and/or ICT network security projects. <b>5 years and more.</b>	
		Good	70	Key staff have adequate experience in Cyber- and/or ICT network security projects. <b>4 to 5 years</b>	
		Poor	40	Key staff have limited experience in Cyber- and/or ICT network security projects. <b>0 to 3 years.</b>	



	Criteria	Rating	Scoring	Evaluation Indicators	Reference page number in your submission documentation
4.	<b>Approach proposed to attain the employer's stated objectives.</b>	Very Good	100	An innovative approach is presented that illustrates the bidder's approach has been tailored to be relevant and meet the client's objectives in all aspects. <b>This is clearly linked to all solutions/systems/ services required.</b>	
		Good	70	The approach presented illustrates that the bidder will adopt an approach that meets the client's objectives. <b>This is linked to at least 8 of the solutions/system/ services to be provided.</b>	
		Poor	40	The approach presented does not meet the client's expectations and will not result in the objectives of the project being fully realized. <b>This is linked to 7 or less of the solutions/systems/ services to be provided.</b>	
5.	<b>Demonstrated experience with respect to Cyber- and/or ICT network security projects.</b>  As per CV's, previous projects worked on.	Very Good	100	Key staff have outstanding experience in specific aspects of the project that were defined as key components of the assignment. <b>5 years and more.</b>	
		Good	70	Key staff have adequate experience in specific aspects of the project that were defined as key components of the assignment. <b>4 to 5 years</b>	
		Poor	40	Key staff have limited experience in specific aspects of the project that were defined as key components of the assignment. <b>0 to 3 years.</b>	
6.	<b>Quality assurance in terms of Security Audit and Cyber Security awareness training which ensure compliance with stated employer's requirements.</b>	Very Good	100	The successful bidders support staff need to be certified in at least ISACA: Certified Information Systems Auditor (CISA) and ITIL (V4) certifications.	
		Good	70	The successful bidder support staff need to be at least ITIL (V4) certified.	
		Poor	40	No Cyber training certifications.	
7.	<b>Organisation, logistics and support resources</b>	Very Good	100	Strong organisational structure, dedicated personnel (organogram), SLA-backed support systems (response times),with documentary evidence.	
		Good	70	The bidder convincingly illustrates that sufficient organisational and support resources will be available for execution of the project.	
		Poor	40	The bidder fails to illustrate that sufficient organisational and support resources will be available for execution of the project.	

	Criteria	Rating	Scoring	Evaluation Indicators	Reference page number in your submission documentation
8.	<b>Demonstrable managerial ability appropriate to the size and nature of the work</b>	Very Good	100	The bidder illustrates extensive knowledge and experience in the project management of projects in Cyber- and/or ICT network security projects. <b>3 Projects or more</b>	
		Good	70	The bidder illustrates adequate knowledge and experience in the project management in Cyber- and/or ICT network security projects. <b>At least 2 projects</b>	
		Poor	40	The bidder illustrates limited knowledge and experience in the project management of projects in Cyber- and/or ICT network security projects. <b>1 Projects or less</b>	

Quality criteria weighting		Maximum number of points
1.	Adequacy of proposed work plan and proposed methodology	20
2.	Qualifications and competence of the key staff (assigned personnel) in relation to the scope of work	15
3.	Demonstrated experience (past performance) in comparable projects	10
4.	Approach proposed to attain the employer's stated objectives	5
5.	Demonstrated experience with respect to specific aspects of the project	15
6.	Quality assurance systems which ensure compliance with stated employer's requirements	10
4.	Organisation, logistics and support resources	5
8.	Demonstrable managerial ability appropriate to the size and nature of the work	20
<b>TOTAL</b>		<b>100</b>

The scoring of the tenderer's experience will be as follows.

Only the scores of 40, 70 or 100 will be allocated to each of the criteria based on the indicators contained in these schedules. The scores of the evaluators will then be averaged, weighted, and then totalled to obtain the final score for quality.

Scoring Criteria	Evaluation Criteria
<b>Poor</b> (score 40)	Tenderer has limited experience.  Years in Cyber- and/or ICT network security projects.: <b>0 – less than 1 years</b>
<b>Satisfactory</b> (score 70)	Tenderer has relevant experience but has not dealt with the critical issues specific to the assignment.  Years in Cyber- and/or ICT network security projects.: <b>2 – less than 3 years</b>
<b>Good</b> (score 90)	Tenderer has extensive experience in relation to the project and has worked previously under similar conditions and circumstances.  Years in Cyber- and/or ICT network security projects.: <b>4 – less than 5 years</b>
<b>Very good</b> (score 100)	Tenderer has outstanding experience in projects of a similar nature.  Years in Cyber- and/or ICT network security projects.: <b>5 years and more</b>

#### Functionality Criteria evaluation

The criteria and maximum score in respect of each of the criteria are as follows:

Functionality / Quality criteria	Sub-criteria	Maximum number of points
Project approach and technical evaluation	Project plan of implementation and technical approach as per specifications	60
Tenderers Experience	Tenderers Experience on Similar Projects	40
<b>Maximum possible score.</b>		<b>100</b>

**BIDDERS HAVE TO OBTAIN A MINIMUM SCORE OF 80 FOR FUNCTIONALITY IN ORDER TO CONTINUE WITH EVALUATION. EVALUATION CONTINUES ON THE 80/20 PREFERENCE POINT SCORING SYSTEM.**

## SCHEDULE D PRICING

- All bids must be submitted on the official forms supplied by the municipality
- Under no circumstances, whatsoever may the bid forms be redrafted.
- The prices cast must include all labour, transport, etc, all related costs of bringing the service to council, without any hidden costs.
- The rate shall remain fixed for the duration of the contract. No other price adjustments, other than the prices and percentage increases disclosed in the tender pricing schedule, shall be allowed.
- The Bidder MUST indicate whether he/she/the entity is a registered VAT Vendor or not.
- In the case of the Bidder not being a registered VAT Vendor, both columns (sub-total/total excluding AND including VAT) must reflect the same amount
- **Please take note that bidders that do not complete the mentioned pricing schedule, will be considered as submitting a non-responsive bid.**
- The quantities indicated are only estimates and might vary during the contract period due to the municipality's operational requirements and available budget. This is only indicated as such for evaluation purposes.
- Rates based tender.

	INDICATE WITH AN „X“							
Are you/is the firm a registered VAT Vendor	YES				NO			
If “YES”, please provide VAT number								

I / We \_\_\_\_\_

(full name of Bidder) the undersigned in my capacity as \_\_\_\_\_

of the firm \_\_\_\_\_

hereby offer to Cape Agulhas Municipality to render the services as described, in accordance with the specification and conditions of contract to the entire satisfaction of the Cape Agulhas Municipality and subject to the conditions of tender, for the amounts indicated hereunder:

Signed .....

Date .....

Name .....

Position .....

Tenderer .....

Support after hand over and sign-off, other than that of the solutions developer will be in terms of section one, "SCOPE OF SERVICES" of this tender. **A detailed quote of each license or service is also required from the Tenderer.**

In the case where any service or license is already included in a different pricing schedule, please indicate Zero value to each year of this pricing schedule but add in black ink at the end of the relevant schedule in what section these costs is already included.

### 3. Support Fees

Is pricing subject to R/\$ fluctuations? \_\_\_\_\_

*For the scope of the tender quantities will be added for evaluation purposes based on current estimates. Please calculate accordingly.*

#### Year 1

DESCRIPTION	QTY (instances)	UNIT PRICE	TOTAL PRICE
Callout Fee	72		
<b>Hourly Cost or part thereof – onsite</b>			
0 – 15 minutes	200		
0 – 60 minutes	60		
0 – 90 minutes	40		
120 minutes plus	48		
<b>Remote Support Desktop</b>			
0 – 15 minutes	216		
0 – 30 minutes	72		
0 – 60 minutes	48		
Cost if remote support is converted to onsite support at or before 30 minutes	48		
<b>Router and switch configuration</b>			
0 – 60 minutes	36		
0 – 70 minutes	36		
0 – 75 minutes	288		
0 – 80 minutes	288		
<b>Server rebuilds or reinstallation</b>			
0 – 60 minutes	35		
0 – 70 minutes	35		
0 – 75 minutes	35		
0 – 80 minutes	260		
<b>Cyber security support &amp; remediation</b>			
0 – 60 minutes	35		
0 – 70 minutes	35		
0 – 75 minutes	35		
0 – 80 minutes	260		
<b>Travel</b>			
Time to and from Bredasdorp average _____ minutes if applicable	288		
R/ KM _____ km if applicable	288		
<b>Sub Total</b>			R
<b>VAT @ 15%</b>			R
<b>TOTAL</b>			R

## Year 2

DESCRIPTION	QTY (instances)	UNIT PRICE	TOTAL PRICE
Callout Fee	72		
<b>Hourly Cost or part thereof – onsite</b>			
0 – 15 minutes	200		
0 – 60 minutes	60		
0 – 90 minutes	40		
120 minutes plus	48		
<b>Remote Support Desktop</b>			
0 – 15 minutes	216		
0 – 30 minutes	72		
0 – 60 minutes	48		
Cost if remote support is converted to onsite support at or before 30 minutes	48		
<b>Router and switch configuration</b>			
0 – 60 minutes	36		
0 – 70 minutes	36		
0 – 75 minutes	288		
0 – 80 minutes	288		
<b>Server rebuilds or reinstallation</b>			
0 – 60 minutes	35		
0 – 70 minutes	35		
0 – 75 minutes	35		
0 – 80 minutes	260		
<b>Cyber security support &amp; remediation</b>			
0 – 60 minutes	35		
0 – 70 minutes	35		
0 – 75 minutes	35		
0 – 80 minutes	260		
<b>Travel</b>			
Time to and from Bredasdorp average _____ minutes if applicable	288		
R/ KM _____ km if applicable	288		
<b>Sub Total</b>			R
<b>VAT @ 15%</b>			R
<b>TOTAL</b>			R

Year 3

DESCRIPTION	QTY (instances)	UNIT PRICE	TOTAL PRICE
Callout Fee	72		
<b>Hourly Cost or part thereof – onsite</b>			
0 – 15 minutes	200		
0 – 60 minutes	60		
0 – 90 minutes	40		
120 minutes plus	48		
<b>Remote Support Desktop</b>			
0 – 15 minutes	216		
0 – 30 minutes	72		
0 – 60 minutes	48		
Cost if remote support is converted to onsite support at or before 30 minutes	48		
<b>Router and switch configuration</b>			
0 – 60 minutes	36		
0 – 70 minutes	36		
0 – 75 minutes	288		
0 – 80 minutes	288		
<b>Server rebuilds or reinstallation</b>			
0 – 60 minutes	35		
0 – 70 minutes	35		
0 – 75 minutes	35		
0 – 80 minutes	260		
<b>Cyber security support &amp; remediation</b>			
0 – 60 minutes	35		
0 – 70 minutes	35		
0 – 75 minutes	35		
0 – 80 minutes	260		
<b>Travel</b>			
Time to and from Bredasdorp average _____ minutes if applicable	288		
R/ KM _____ km if applicable	288		
<b>Sub Total</b>			R
<b>VAT @ 15%</b>			R
<b>TOTAL</b>			R

## 2. Network access policy system.

The Municipality acknowledges that different solutions can be based on various pricings methodologies. Therefore, the bidder is required to complete this pricing schedule as far as possible, and if the pricing methodology differs from the provided schedule, the total column needs to be completed and a detailed quotation based on the bidder's implementation methodology must be submitted as part of the bidding process **with clear indication where this can be found in the document.**

Is pricing subject to R/\$ fluctuations? \_\_\_\_\_

### Year 1

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription inclusive of reporting and support	12		
System implementation handed over and functional in Cape Agulhas municipal environment over all sites to all users and servers	1		
System training for ICT staff	4		
Sub Total			
VAT @ 15%			
TOTAL			

### Year 2

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription inclusive of reporting and support	12		
VAT @ 15%			
TOTAL			

### Year 3

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription inclusive of reporting and support	12		
VAT @ 15%			
TOTAL			



### 3. Cloud assessment and monitoring tool

The Municipality acknowledges that different solutions can be based on various pricings methodologies. Therefore, the bidder is required to complete this pricing schedule as far as possible, and if the pricing methodology differs from the provided schedule, the total column needs to be completed and a detailed quotation based on the bidder's implementation methodology must be submitted as part of the bidding process **with clear indication where this can be found in the document**.

Is pricing subject to R/\$ fluctuations? \_\_\_\_\_

#### Year 1

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
<b>Monthly</b> subscription inclusive of reporting and support	12		
System implementation handed over and functional in Cape Agulhas municipal environment over all sites to all users and servers	1		
System training for ICT staff	4		
Sub Total			
VAT @ 15%			
TOTAL			

#### Year 2

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
<b>Monthly</b> subscription inclusive of reporting and support	12		
VAT @ 15%			
TOTAL			

#### Year 3

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
<b>Monthly</b> subscription inclusive of reporting and support	12		
VAT @ 15%			
TOTAL			

#### 4. Cloud Application Activity & Security Monitoring

##### Year 1

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription inclusive of reporting and support	12		
System implementation handed over and functional in Cape Agulhas municipal environment over all sites to all users and servers	1		
System training for ICT staff	4		
Sub Total			
VAT @ 15%			
TOTAL			

##### Year 2

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription inclusive of reporting and support	12		
VAT @ 15%			
TOTAL			

##### Year 3

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription inclusive of reporting and support	12		
VAT @ 15%			
TOTAL			

## 5. Compliance

Is pricing subject to R/\$ fluctuations? \_\_\_\_\_

### 5.1 Cyber Security Framework management tool

The Municipality acknowledges that different solutions can be based on various pricings methodologies. Therefore, the bidder is required to complete this pricing schedule as far as possible, and if the pricing methodology differs from the provided schedule, the total column needs to be completed and a detailed quotation based on the bidder's implementation methodology must be submitted as part of the bidding process **with clear indication where this can be found in the document.**

Is pricing subject to R/\$ fluctuations? \_\_\_\_\_

#### Year 1

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
<b>Monthly</b> subscription inclusive of reporting and support	12		
System implementation handed over and functional in Cape Agulhas municipal environment over all sites to all users and servers	1		
System training for ICT staff	4		
Sub Total			
VAT @ 15%			
TOTAL			

#### Year 2

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
<b>Monthly</b> subscription inclusive of reporting and support	12		
VAT @ 15%			
TOTAL			

#### Year 3

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
<b>Monthly</b> subscription inclusive of reporting and support	12		
VAT @ 15%			
TOTAL			

## 6. Dark Web monitoring

Is pricing subject to R/\$ fluctuations? \_\_\_\_\_

### Year 1

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription per domain (1 Domain) to include alerts and reports	12		
VAT @ 15%			
TOTAL			

### Year 2

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription per domain (1 Domain) to include alerts and reports	12		
VAT @ 15%			
TOTAL			

### Year 3

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription per domain (1 Domain) to include alerts and reports	12		
VAT @ 15%			
TOTAL			

## 7. Security Audit

Is pricing subject to R/\$ fluctuations? \_\_\_\_\_

### Year 1

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Pricing is requested from service providers to perform Cyber security audit (initial audit)	1		
Audit revision and maturity assessment	3		
Sub Total			
VAT @ 15%			
TOTAL			

### Year 2

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Audit revision and maturity assessment	4		
VAT @ 15%			
TOTAL			

### Year 3

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Audit revision and maturity assessment	4		
VAT @ 15%			
TOTAL			

## 8. Security Awareness Training & Phishing Simulation Requirements

Is pricing subject to R/\$ fluctuations? \_\_\_\_\_

Licensing per user must include all requirements as set out in this section.

### Year 1

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Site survey / planning 1-4 weeks)	1		
Training cost per user, this should include all cost related to on- and off-site training and materials.	210		
Sub Total			
VAT @ 15%			
TOTAL			

### Year 2

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Training cost per user, this should include all cost related to on- and off-site training and materials.	210		
VAT @ 15%			
TOTAL			

### Year 3

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Training cost per user, this should include all cost related to on- and off-site training and materials.	210		
VAT @ 15%			
TOTAL			

## 9. Vulnerability Scanning Tool

### Year 1

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription inclusive of reporting and support)	12		
System implementation handed over and functional in Cape Agulhas municipal environment over all sites to all users and servers	1		
System training for ICT staff	4		
Sub Total			
VAT @ 15%			
TOTAL			

### Year 2

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription inclusive of reporting and support	12		
VAT @ 15%			
TOTAL			

### Year 3

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription inclusive of reporting and support	12		
VAT @ 15%			
TOTAL			

## 10. Penetration Testing

The Municipality acknowledges that different solutions can be based on various pricings methodologies. Therefore, the bidder is required to complete this pricing schedule as far as possible, and if the pricing methodology differs from the provided schedule, the total column needs to be completed and a detailed quotation based on the bidder's implementation methodology must be submitted as part of the bidding process **with clear indication where this can be found in the document**.

Is pricing subject to R/\$ fluctuations? \_\_\_\_\_

### Year 1

DESCRIPTION	RANGE	QTY	UNIT PRICE	TOTAL PRICE
Penetration per IP, 12 months (Internal and External)	0-50	1		
Penetration per IP, 12 months (Internal and External)	51 - 100	1		
Penetration per IP, 12 months (Internal and External)	101-200	1		
Penetration per IP, 12 months (Internal and External)	200+	1		
System implementation handed over and functional in Cape Agulhas municipal environment over all sites to all users.		1		
Other...				
Sub Total				
VAT @ 15%				
TOTAL				

### Year 2

DESCRIPTION	RANGE	QTY	UNIT PRICE	TOTAL PRICE
Penetration per IP, 12 months (Internal and External)	0-50	1		
Penetration per IP, 12 months (Internal and External)	51 - 100	1		
Penetration per IP, 12 months (Internal and External)	101-200	1		
Penetration per IP, 12 months (Internal and External)	200+	1		
Sub Total				
VAT @ 15%				
TOTAL				



### Year 3

DESCRIPTION	RANGE	QTY	UNIT PRICE	TOTAL PRICE
Penetration per IP, 12 months (Internal and External)	0-50	1		
Penetration per IP, 12 months (Internal and External)	51 - 100	1		
Penetration per IP, 12 months (Internal and External)	101-200	1		
Penetration per IP, 12 months (Internal and External)	200+	1		
Sub Total				
VAT @ 15%				
TOTAL				

## 11. SIEM, Log Management & Security Automation Requirements

### Year 1

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription inclusive of reporting and support)	12		
System implementation handed over and functional in Cape Agulhas municipal environment over all sites to all users and servers	1		
System training for ICT staff	4		
Sub Total			
VAT @ 15%			
TOTAL			

### Year 2

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription inclusive of reporting and support	12		
VAT @ 15%			
TOTAL			

### Year 3

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription inclusive of reporting and support	12		
VAT @ 15%			
TOTAL			

## 12. IT Documentation & Knowledge Management Platform Requirements

### Year 1

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription inclusive of reporting and support)	12		
System implementation handed over and functional in Cape Agulhas municipal environment over all sites to all users and servers	1		
System training for ICT staff	4		
Sub Total			
VAT @ 15%			
TOTAL			

### Year 2

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription inclusive of reporting and support	12		
VAT @ 15%			
TOTAL			

### Year 3

DESCRIPTION	QTY	UNIT PRICE	TOTAL PRICE
Monthly subscription inclusive of reporting and support	12		
VAT @ 15%			
TOTAL			

### 13. Security Operations Centre (SOC)

The Municipality acknowledges that different solutions can be based on various pricings methodologies. Therefore, the bidder is required to complete this pricing schedule as far as possible, and if the pricing methodology differs from the provided schedule, the total column needs to be completed and a detailed quotation based on the bidder's implementation methodology must be submitted as part of the bidding process **with clear indication where this can be found in the document.**

Is pricing subject to R/\$ fluctuations? \_\_\_\_\_

#### Year 1

DESCRIPTION	RANGE	QTY	UNIT PRICE	PRICE
SOC device license 12 months	0-50	0-50		
SOC device license 12 months	51 - 100	51 - 100		
SOC device license 12 months	101-200	101-200		
SOC device license 12 months	200+	200+		
System implementation handed over and functional in Cape Agulhas municipal environment over all sites to all users.		1		
System training for 4 ICT staff members		4		
Other...				
			Sub Total	
			VAT @ 15%	
			TOTAL	

#### Year 2

DESCRIPTION	RANGE	QTY	UNIT PRICE	TOTAL PRICE
SOC device license 12 months	0-50	50		
SOC device license 12 months	51 - 100	50		
SOC device license 12 months	101-200	100		
SOC device license 12 months	200+	100		
Other...				
			Sub Total	
			VAT @ 15%	
			TOTAL	

#### Year 3

DESCRIPTION	RANGE	QTY	UNIT PRICE	TOTAL PRICE
SOC device license 12 months	0-50	50		
SOC device license 12 months	51 - 100	51 - 100		
SOC device license 12 months	101-200	101-200		
SOC device license 12 months	200+	200+		
Other...				
			Sub Total	
			VAT @ 15%	
			TOTAL	

#### 14. Monitoring, management, and Audit system

The pricing schedule can be defined inclusive of all descriptions (features) or as a whole with the implementation and commissioning handed over to the Municipality as a working solution.

Support after hand over and sign of, other than that of the solutions developer will be in terms of section one, "SCOPE OF SERVICES" of this tender. **A detailed solutions proposal and pricing for this system is also required from the Tenderer.**

Is pricing subject to R/\$ fluctuations? \_\_\_\_\_

#### Year 1

DESCRIPTION	QTY	OR	UNIT PRICE	PRICE	
Active Directory monitoring	1				
Backup monitoring	15				
Patch monitoring	258				
Detailed asset reporting	708				
Network device performance and reporting	450				
Standard desktop performance and monitoring	240				
Endpoint Security monitoring and reporting	240				
Virtual Server host monitoring and reporting	18				
Patch Management	258				
Onsite support 8 hours a month transferrable over 12 months	12				
Remote support	SLA				
Sub Total if quoting on inclusive of all requirements above					
Desktop support training	4				
Remove existing system agents from environment 39 sites 258 devices	12				
Remove, update or change security credentials of existing covered devices to new solution specification	1				
System implementation handed over and functional in Cape Agulhas Municipal environment over all sites	1				
			Sub Total		
			VAT @ 15%		
			TOTAL		

## Year 2

DESCRIPTION	QTY		UNIT PRICE	PRICE
Active Directory monitoring	1	OR		
Backup monitoring	15			
Patch monitoring	258			
Detailed asset reporting	690			
Network device performance and reporting	450			
Standard desktop performance and monitoring	240			
Endpoint Security monitoring and reporting	240			
Virtual Server host monitoring and reporting	18			
Patch Management	258			
Onsite support 8 hours a month transferrable over 12 months	12			
Remote support	SLA			
Sub Total if quoting on inclusive of all requirements above				
Desktop support training	4			
			Sub Total	
			VAT @ 15%	
			TOTAL	

### Year 3

DESCRIPTION	QTY		UNIT PRICE	PRICE
Active Directory monitoring	1	<div> <div></div> <div>OR</div> <div></div> </div>		
Backup monitoring	15			
Patch monitoring	258			
Detailed asset reporting	690			
Network device performance and reporting	450			
Standard desktop performance and monitoring	240			
Endpoint Security monitoring and reporting	240			
Virtual Server host monitoring and reporting	18			
Patch Management	258			
Onsite support 8 hours a month transferrable over 12 months	12			
Remote support	SLA			
Sub Total if quoting on inclusive of all requirements above				
Desktop support training	4			
			Sub Total	
			VAT @ 15%	
			TOTAL	

## 15. Pricing Summarized

The Tenderer must summarize the pricing as provided in this tender document, below and provide **brochures, datasheets, and full detailed quotes on specified description where applicable.**

NR	DESCRIPTION	YEAR	PRICE
1	Support fees*	1 - 3	
2	Network access policy system	1 - 3	
3	Cloud assessment and monitoring tool	1 - 3	
4	Cloud Application Activity & Security Monitoring	1 - 3	
5	Cyber Security Framework Management Platform	1 - 3	
6	Dark Web monitoring	1 - 3	
7	Security Audit	1 - 3	
8	Security Awareness Training & Phishing Simulation Requirements	1 - 3	
9	Vulnerability Scanning Tool	1 - 3	
10	Penetration Testing	1 - 3	
11	SIEM, Log Management & Security Automation Requirements	1 - 3	
12	IT Documentation & Knowledge Management Platform Requirements	1 - 3	
13	Security Operations Centre (SOC)	1 - 3	
14	Monitoring, management, and audit solution	1 - 3	
<b>TOTAL (TO BE CARRIED OVER TO COVER PAGE AND FORM OF OFFER)</b>			<b>R</b>

- a. The tendered prices should be based on the Rate of Exchange of the date when the tender is published. The successful tenderer will have the opportunity to adjust the prices to the Rate of Exchange of the date of commencement for Schedules C (where indicated as applicable),
- b. The prices quoted on are to be fixed for a period of 3 years and only the prices on Schedule C (where indicated applicable), will be allowed to be adjusted by the successful tenderer over the period and that change will be limited to solely the rate of Exchange at the time of the placing of the order for the particular item. No price increases will be permitted.
- c. The rate of exchange inserted in the column shall be the closing spot selling rate quoted by the Municipalities' main banker, ABSA BANK, on the AFORESAID dates as listed in points a) and b) – The Municipality will supply the rate provided by its main banker to the successful tenderer.

**THE FOLLOWING COMPULSORY CONDITIONS WILL APPLY:**

- Quotations must also be supplied on an **official company letterhead** of line items where applicable.
- **Council may accept a tender in full, partially or not at all.**
- Invoices must not be issued before goods / services have been supplied / rendered.
- The successful bidder must provide a Statement of Work (SOW) for each category listed in the tender document within 7 days of appointment.

**NB: THE COMPANY MUST BE COMPLIANT IN TERMS OF ALL OF THE FOLLOWING CONDITIONS:**

1. No quotations will be considered from persons in the service of the state, **nor any person/s, entities not registered as a valid ICT company.**
2. Supply relevant document/s to prove the company is a registered ICT based entity.<sup>iii</sup>
3. Company must have a local I.T. Sales and Support office (Western Cape).
4. Company must complete the form attached hereto to **indicate at least 3 contactable references** to which similar services have been rendered within government or organs of the state.<sup>i</sup>
5. Company must provide a letter from the "BRAND HOUSE" to prove it is a registered brand reseller.<sup>ii</sup>

**Failure to comply with ANY of the conditions above or failure to submit the relevant documents WILL invalidate your offer.**

**2. Explanation of specific compulsory conditions**

- i. The company must have a sales and support office in the Western Cape. Proof hereof will be provided through the inclusion of the municipal account or other relevant documents.
- ii. The company must provide a letter from the "BRAND HOUSE". Please note that the "BRAND HOUSE" refers to the Brand Administration Office in South Africa and not the distributor or supplier. *Example, if you supply Samsung products, you should include a letter from Samsung and not a distribution office, like Tarsus or Axis.*
- iii. Company must provide proof of registration as an ICT Company. This can include documents such as a Close Corporation (CC) or Company certificates. Please note it should make reference to the Information Technology sector. Certificates that indicate phrases like, "general sales" or "general trade" is not acceptable.

Signed ..... Date .....

Name ..... Position .....

Tenderer .....



It is a condition of bid that the taxes of the successful bidder must be in order, or that Satisfactory arrangements have been made with South African Revenue Service (SARS) to meet the bidder's tax obligations.

- 1 In order to meet this requirement bidders are required to request their Tax Compliance Status which will include a unique PIN which you can provide to any third party (**if requested**) to enable them to verify your tax compliance status online via eFiling.
- 2 Request a TCC via eFiling which will give you the option to print the TCC Or request a TCC at a SARS branch where a SARS agent will be able to print or email the TCC to you.
- 3 The Tax Compliance Status Requirements are also applicable to foreign bidders / individuals who wish to submit bids.
- 4 A **Tax Compliance Status** is a holistic view of your tax compliance level across all your registered tax types.
- 5 If your tax compliance status is compliant, the SARS agent will be able to print or email you your TCC to the registered email address which SARS has on record for you.
- 6 **Please note:** If your tax compliance status reflects that you are non-compliant, you will not receive a TCC until you have rectified your compliance.
- 7 The **Tax Compliance status pin must** be submitted together with the bid. **Failure to submit a Tax Compliance status pin will result in the invalidation of the tender.**
- 8 In bids where Consortia / Joint Ventures / Sub-contractors are involved; each party must submit a separate **Tax Compliance Pin**.
- 9 **Please note that not all government institutions and private organisations will be able to utilise the Tax Compliance Status PIN at this stage and in such instances, you must supply a printed TCC. It is envisaged that the PIN will, in time, replace the paper TCC.**

## TAX COMPLIANCE STATUS PIN

In terms of the Municipal Preferential Procurement Policy, tenderers must ensure that they are up to date with payments of taxes.

The tenderer **must** attach to this page a **Tax Compliance status pin**, as issued by the South African Revenue Service.

**Failure to submit a Tax Compliance status pin will result in the invalidation of the tender.**

Signed .....

Date .....

Name .....

Position .....

Tenderer .....

### SCHEDULE 1A: AUTHORITY OF SIGNATORY

Indicate the status of the tenderer by ticking the appropriate box hereunder. The tenderer must complete the certificate set out below for the relevant category.

A Company	B Partnership	C Joint Venture	D Sole Proprietor	E Close Corporation

#### A. Certificate for company

I,....., chairperson of the board of directors of ..... hereby confirm that by resolution of the board (copy attached) taken on .....20...., Mr/Mrs.....acting in the capacity of.....,was authorised to sign all documents in connection with this tender and any contract resulting from it on behalf of the company.

As witness

1.....  
Chairman  
2.....  
Date

#### B. Certificate of partnership

We, the undersigned, being the key partners in the business trading as ..... hereby authorise Mr/Mrs....., acting in the capacity of.....to sign all documents in connection with the tender for Contract.....and any contract resulting from it on our behalf.

NAME	ADDRESS	SIGNATURE	DATE

NOTE: This certificate is to be completed and signed by all of the key partners upon who rests the direction of the affairs of the Partnership as a whole.

#### C. Certificate for Joint Venture

We, the undersigned, are submitting this tender offer in Joint Venture and hereby authorise Mr/Mrs....., authorised signatory of the company .....,

acting in the capacity of lead partner, to sign all documents in connection with the tender offer for Contract.....and any other contract resulting from it on our behalf.

This authorisation is evidenced by the attached power of attorney signed by legally authorised signatories of all the partners to the Joint Venture.

NAME OF FIRM	ADDRESS	AUTHORISING SIGNATURE, NAME & CAPAMUNICIPALITY
Lead partner		

#### D. Certificate for sole proprietor

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

As Witness:

1.....  
Signature: Sole owner

2.....  
Date

#### E. Certificate for Close Corporation

We, the undersigned, being the key members in the business trading as.....hereby authorise Mr/Mrs.....

Acting in the capacity of....., to sign all documents in connection with the tender for Contract.....and any contract resulting from it on our behalf.

NAME	ADDRESS	SIGNATURE	DATE

NOTE: This certificate is to be complete and signed by all the key members upon whom rests the direction of the affairs of the Close Corporation as a whole.

#### SCHEDULE 1B: COMPULSORY ENTERPRISE QUESTIONNAIRE

The following particulars **must** be furnished. In the case of a joint venture, separate enterprise questionnaires in respect of each partner must be completed and submitted.

**Section 1: Enterprise details**

<b>Name of enterprise</b>	
<b>Contact Person</b>	
<b>Email</b>	
<b>Telephone</b>	
<b>Cellphone</b>	
<b>Fax</b>	
<b>Physical Address</b>	
<b>Postal Address</b>	
<b>Central supplier database registration number</b>	MAAA

**Section 2: Particulars of companies and close corporations**

<b>Company / Close Corporation registration number:</b>	
---	--

**Section 3: SARS information:**

<b>Tax reference number:</b>	
<b>VAT registration number, if any:</b>	

**Section 4: CIDB registration number:** N/A

**Section 5: Particulars of principles**

**Principle:** means a natural person who is a partner in partnership, a sole proprietor, a director of a company established in terms of the Companies Act of 2008 (Act. No. 71 of 2008) a member of a close corporation registered in terms of the Close Corporation Act, 1984 (Act No.69 of 1984)

Full name of principal	Identity number*	Personal income tax number*

\* Please complete and attach copies of Identity documents.

**Section 6: Banking Details of companies and close corporations**

Bank name and branch: .....

Bank account number: .....

Name of account holder: .....

Signed ..... Date .....

Name ..... Position .....

Tenderer .....

**SCHEDULE 1C: DOCUMENTS OF INCORPORATION (CK2)**

The Tenderer **must** attach to this page a copy of the certificate of incorporation of his/her company, close corporation or partnership. In the case of a joint venture between two or more firms, the tenderer shall attach a copy of the document of incorporation of the joint venture.

Signed .....

Date .....

Name .....

Position .....

Tenderer.....

**SCHEDULE 1D: PAYMENT OF MUNICIPAL ACCOUNTS**

In terms of the Municipal Supply Chain Management Policy and System and its Preferential Procurement Policy, tenderers **must** ensure that they are up-to date with their payments of municipal accounts.

The tenderer **must attach to this page**, a Latest Municipal account, which provides proof that his payment of Municipal accounts is up-to-date and complete the certificate for municipal services on the next page. In the event of leasing, a lease agreement **Must** be attached to the tender document.

Signed ..... Date .....

Name ..... Position .....

Tenderer .....

## CERTIFICATE FOR MUNICIPAL SERVICES (COMPULSORY TO COMPLETE)

### DECLARATION IN TERMS OF CLAUSE 112(1) OF THE MUNICIPAL FINANCE MANAGEMENT ACT (NO.56 OF 2003) - (To be signed in the presence of a Commissioner of Oaths)

I, \_\_\_\_\_, \_\_\_\_\_ (full name and ID no.), hereby acknowledge that according to SCM Regulation 38(1)(d)(i), the Municipality 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 Cape Agulhas Municipality, or to any other municipality or municipal entity, are in arrears for more than 3 (three) months.

I declare that I am duly authorised to act on behalf of \_\_\_\_\_ (name of the firm) and hereby declare, that to the best of my personal knowledge, neither the firm nor any director/member/partner of said firm is in arrears on any of its municipal accounts with any municipality in the Republic of South Africa, for a period longer than 3 (three) months.

I further hereby certify that the information set out in this schedule and/or attachment(s) hereto is true and correct. The Tenderer acknowledges that failure to properly and truthfully complete this schedule may result in the tender being disqualified, and/or in the event that the tenderer is successful, the cancellation of the contract.

PHYSICAL BUSINESS ADDRESS(ES) OF THE TENDERER	MUNICIPAL ACCOUNT NUMBER

#### FURTHER DETAILS OF THE BIDDER'S Director / Shareholder Partners, ect.:

Director /Shareholder / partner	Physical address of the Business	Municipal Account number(s)	Physical residential address of the Director / shareholder / partner	Municipal Account number(s)

**NB:** Please attach certified copy(ies) of ID document(s)

If the entity or any of its Directors/Shareholders/Partners, etc. rents/leases premises, a copy of the rental/lease agreement must be submitted with this tender.

**Number of sheets appended by the tenderer to this schedule (If nil, enter NIL)**

<b>Signature</b>	<b>Position</b>	<b>Date</b>

<p style="text-align: center;"><b>COMMISSIONER OF OATHS</b></p> <p>Signed and sworn to before me at _____, on this _____ day of _____ 20____</p> <p>by the Deponent, who has acknowledged that he/she knows and understands the contents of this Affidavit, it is true and correct to the best of his/her knowledge and that he/she has no objection to taking the prescribed oath, and that the prescribed oath will be binding on his/her conscience.</p> <p><b>COMMISSIONER OF OATHS:-</b></p> <p>Position: _____</p> <p>Address: _____</p> <p>Tel: _____</p>	<p><b>Apply official stamp of authority on this page:</b></p>
--	---



## SCHEDULE 1E: BROAD-BASED BLACK ECONOMIC EMPOWERMENT (B-BBEE) STATUS LEVEL CERTIFICATES

A bidder who qualifies as an EME in terms of the B-BBEE Act **must** submit a sworn affidavit confirming Annual Total Revenue and Level of Black Ownership.

A Bidder other than EME or QSE **must submit their original and valid B-BBEE status level verification certificate or a certified copy** thereof, substantiating their B-BBEE rating issued by a Registered Auditor approved by IRBA or a Verification Agency accredited by SANAS.

MINIMUM REQUIREMENTS FOR VALID B-BBEE STATUS LEVEL VERIFICATION CERTIFICATES (The following information must be on the face of the certificate)	Indicate with (x)	
	yes	no
The name and the physical location of the measured entity		
The registration number and, where applicable, the VAT number of the measured entity		
The date of issue and date of expiry		
The certificate number for identification and reference		
The scorecard that was used (for example EME, QSE or Generic)		
The name and / or logo of the verification Agency		
The SANAS logo		
The certificate must be signed by the authorized person from the Verification Agency		
The B-BBEE Status level of Contribution obtained by the measured entity.		

Failure on the part of a bidder **to claim, fill in and/or to sign CAMBD 6.1 and submit a B-BBEE Verification Certificate from a Verification Agency accredited by the South African Accreditation System (SANAS), or a Registered Auditor approved by the Independent Regulatory Board of Auditors (IRBA) or a sworn affidavit confirming annual turnover and level of black ownership in case of an EME and QSE together with the bid, will be interpreted to mean that preference points for B-BBEE status level of contribution are not claimed.**

Signed ..... Date .....

Name ..... Position .....

Tenderer .....

## FOR INFORMATION PURPOSES ONLY

PLEASE NOTE THE FOLLOWING REQUIREMENTS REGARDING VALIDATION OF B-BBEE SCORE.

### 1 EMEs

#### **ONLY THE FOLLOWING WILL BE ACCEPTED:**

- 1.1. **A VALID ORIGINAL** sworn affidavit, confirming annual turnover and level of black ownership
- or
- 1.2. **A VALID** affidavit / certificate issued by Companies Intellectual Property Commission (CIPC);
- or
- 1.3. **A VALID ORIGINAL** B-BBEE status level verification certificate **OR A CERTIFIED COPY** thereof, substantiating their B-BBEE rating issued by:
  - 1.3.1. A registered Auditor approved by the Independent Regulatory Board for Auditors (IRBA); or
  - 1.3.2. A verification Agency accredited by the South African National Accreditation System (SANAS).

### 2. QSEs

#### **ONLY THE FOLLOWING WILL BE ACCEPTED:**

- 2.1. **A VALID ORIGINAL** sworn affidavit, confirming annual turnover and level of black ownership
- or
- 2.2. **A VALID ORIGINAL** B-BBEE status level verification certificate **OR A CERTIFIED COPY** thereof, substantiating their B-BBEE rating issued by:
  - 2.2.1. A registered Auditor approved by IRBA; or
  - 2.2.2. A verification Agency accredited by SANAS.

### 2. BIDDERS OTHER THAN EMEs & QSE's

- 3.1. The bidder **MUST** submit either a **VALID ORIGINAL B-BBEE** status level verification certificate **OR A CERTIFIED COPY** thereof, substantiating their **B-BBEE** rating issued by:
  - 3.1.1. A Registered Auditor approved by IRBA; or
  - 3.1.2. A Verification Agency accredited by SANAS.

**WHEN CONFIRMING THE VALIDITY OF CERTIFICATES ISSUED BY AN AUDITOR REGISTERED WITH IRBA, THE FOLLOWING SHOULD BE DETAILED ON THE FACE OF THE CERTIFICATE:**

- 4.1. The Auditor's letterhead with FULL contact details;
- 4.2. The Auditor's practice number;
- 4.3. The name and physical location of the measured entity;
- 4.4. The registration number and, where applicable, the VAT number of the measured entity;
- 4.5. The date of issue and date of expiry;
- 4.6. The B-BBEE Status Level of Contribution obtained by the measured entity; and
- 4.7. The total black shareholding and total black female shareholding.

## SCHEDULE 1F: SCHEDULE OF WORK SATISFACTORILY CARRIED OUT BY THE TENDERER

The following is a statement of projects successfully completed by your company. This schedule will be used to conduct a risk assessment of the Tenderers capacity to undertake the project and all information must be completed in full or the Tender may be considered non-responsive. Indication of Competence / Ability to Perform Successfully

List of recent or previous work of a similar nature within the last 5 years undertaken by the firm **MUST** be completed, **excluding references from Cape Agulhas Municipality.**

Employer (Name, Tel, Fax, Email)		Nature of work	Value of work (Incl. VAT)	Date started	Date completed
1.	Name of entity		R	<div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div> <div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div> <div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div>	<div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div> <div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div> <div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div>
	Contact Person				
	Tel				
	Email				
2.	Name of entity		R	<div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div> <div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div> <div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div>	<div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div> <div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div> <div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div>
	Contact Person				
	Tel				
	Email				
3.	Name of entity		R	<div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div> <div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div> <div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div>	<div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div> <div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div> <div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div>
	Contact Person				
	Tel				
	Email				
4.	Name of entity		R	<div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div> <div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div> <div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div>	<div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div> <div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div> <div style="border-bottom: 1px solid black; width: 100px; display: inline-block;"></div>
	Contact Person				
	Tel				
	Email				

*The Cape Agulhas Municipality will verify all information submitted in terms of this bid and any information that is incorrect will result in that bid being automatically disqualified and not considered further. Therefore, it is stressed that the contact firm or person of the bidder must be willing to confirm the information in writing on the request by the Municipality.*

*The Bidder hereby confirms that the information given above is true and correct:*

Signed.....

Date.....

Name.....

Tenderer.....

## **SCHEDULE 1F: REFERENCES**

### **ASSESSMENT OF BIDDER'S PAST PERFORMANCE BY INDEPENDENT REFERENCE**

**(This must be sent by the bidder to the references listed in the Schedule of Work Satisfactorily Carried Out by the Tenderer. This form must be completed for each project listed in Schedule 1F by the authorized persons of the bidder's current or previous clients. Forms which are neither complete, nor signed nor stamped will not be considered for evaluation.**

**All assessment forms must be attached with the tender submission**

<b>Name of the Entity:</b>					
<b>Contact Person:</b>					
<b>Contact Number:</b>					
<b>Email Address:</b>					
<b>Description of Work/Projects:</b>					
<b>Tender Number:</b>					
<b>Date of Commencement:</b>					
<b>Duration of Contract:</b>					
<b>Contract Completion Date:</b>					
<b>Name of Bidder:</b>					
<b>Your assessment of the Contractor's performance in the following areas: Please tick one of the blocks on the righthand side: 1=Poor; 5=Excellent</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
Turn-around times					
Quality of Product/ Service					
Accessibility and Availability					
Reliability					
Customer Satisfaction					
<b>1=Poor; 2=Unsatisfactory; 3=Average; 4=Good; 5=Excellent</b>					
<b>COMMENTS</b>					
<b>SIGNATURE OF THE RESPONSIBLE OFFICIAL:</b>					
<b>OFFICIAL STAMP:</b>					

**SIGNED ON BEHALF OF TENDERER:** .....

## **SPECIAL CONDITIONS**

The following general conditions will apply to the tender:

1. **All bids must be submitted on the official forms supplied by the municipality.**
2. Under no circumstances, whatsoever may the bid forms be redrafted.
3. Subject to the provisions of clause 5 of this document, no alterations / corrections to the information in the document (including pricing) may be performed by pasting another page over it with glue.
4. **The use of correction fluid / tape is prohibited.**
5. Notwithstanding the provisions of clause 3 of this document, alterations and/or corrections may only be affected as follows:
  - 5.1 By striking a straight line in black ink through the incorrect information in such a manner that the information that has been struck through remains legible; writing, the altered or corrected information as appropriate (under, above or next to the information to be corrected) and initialing in the margin next to each and every alteration or correction.
  - 5.2 All corrections/alterations to the Pricing Schedule / Bill of Quantities (BoQ) and / or any pricing not effected in accordance with clause 5.1 above, will be rejected.
6. Bids submitted must be complete in all respects.
  - 6.1 The bidder is advised to check the number of pages and to satisfy himself that none are missing or duplicated.
  - 6.2 The bidder must ensure that his/her bid document is securely bound.
    - 6.2.1 All supporting documents must be submitted by either stapling it to the relevant form in the bid document, or by submitting a bound annexure containing all supporting documents.
    - 6.2.2 The Municipality will not take any responsibility for missing / lost pages, in cases where the bidder submits loose pages (not securely attached to the bid document or annexure with supporting documents).
7. All schedules as well as the following documents **must** be completed and submitted with the bid documents, failure to complete and submit the following will invalidate your bid:
  - a) **CAMBD 1** - Invitation to Bid
  - b) **CAMBD 4** - Declaration of Interest
  - c) **CAMBD 6.1** - Preference Points Form in Terms of The Preferential Procurement Regulations 2022
  - d) **CAMBD 8** - Declaration of Bidder's Past Supply Chain Management Practices
  - e) **CAMBD 9** - Certificate of Independent Bid Determination
  - f) Form of Offer and Acceptance
8. We undertake to make payment for the services rendered in accordance with the terms and conditions of the contract, within 30 (thirty) days after receipt of an invoice.
9. A firm completion period/date must be indicated from the official order date.
10. No bid will be accepted from persons in the service of the state.
11. Sealed tender marked "**Tender Nr: SCM41/2025/26 ICT SUPPORT SERVICES AND LICENSING FOR A PERIOD OF 3 YEARS**" must be placed in the tender box at the Municipal Offices, 1 Dirkie Uys Street, Bredasdorp or posted to reach the Municipal Manager, Cape Agulhas Municipality, PO Box 51, Bredasdorp, 7280 not later than 12:00 on **Friday, 13 February 2026** after which it will be opened in the public.
12. Any bid received without the "Bid Number and / or Title" clearly endorsed on the envelope will not be opened and read out during the bid opening session and will not be considered.
13. Council reserves the right not to accept any tender. No faxes or e-mails will be accepted and **only the supplied municipal tender form may be used.**
14. A Tax Compliance status pin as issued by the South African Revenue Service, **must** be submitted with the tender, otherwise the tender will be disqualified.
15. The 80/20 scoring system, as stated in the Cape Agulhas Municipal Supply Chain Management Policy, will be used when considering tenders.
16. **PAYMENT OF MUNICIPAL ACCOUNTS (SCHEDULE 1 D)**

The tenderer **must attach**, a Latest Municipal account, which provides proof that his payment of Municipal accounts is up-to-date and complete the **certificate for municipal services** and must be verified by the Municipality where account is held. In the event of leasing, a lease agreement **must** be attached to the tender document.

17. Please note that any suspicious collusive bidding behaviour and restrictive practices by bidders will be reported to the Competition Commission for investigation and possible imposition of administrative penalties.
18. **The tender must be valid up to 90 days after the closing date.**
19. Any bid received after the appointed time for the closing of bids shall not be considered but **shall be filled unopened** with other bids received, which bid(s) can be returned to the bidder at his request and cost.
20. **PRICING**
  - 20.1 Rates and prices offered by the bidder **must** be written into the pricing schedule or form of offer of this document by hand, completed in full and originally signed by the duly authorized signatory.
  - 20.2 All prices shall be quoted in South African currency, and be **INCLUSIVE OF Value Added Tax (VAT)**
  - 20.3 Bid prices must include all expenses, disbursements, and costs (e.g., transport, accommodation etc..) which may be required for the execution of the bidder's obligations in terms of the contract. Bid prices 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 bid is successful), unless otherwise specified.
  - 20.4 All bid prices will be final and binding.
  - 20.5 A bid will not be invalidated if the amount in words and the amount in figures do not correspond, in which case the amount in words shall be read out at the bid opening and shall be deemed to be the bid amount; therefore, where there is a discrepancy between the amount in figures and the amount in words, the amount in words shall apply.
  - 20.6 Where the value of an intended contract will exceed R1 ,000 ,000.00 (R1 million) it is the bidder's responsibility to be registered with the South African Revenue Services (SARS) for VAT purposes in order to be able to issue tax invoices. The municipality will deem the price above R 1 000 000,00 (R1 million) to be VAT inclusive even if it indicated that no VAT is charged. Please ensure that provision is made for VAT in these instances.
  - 20.7 If a bidder becomes a registered VAT vendor during the contract period, the prices/rates as per the initial award will be considered to be inclusive of VAT and no price adjustment (s) will be allowed.
- 20.8 The annual price increase is equal to **CPI (related to the area)** per annum
- 20.9 Price escalation (rise and fall in terms of CPAF indices) will apply for all industry related increases but will only be accepted by the Municipality if claim is substantiated with proof of evidence and that such evidence is submitted prior to implementation.
21. **ADMISSION OF BIDS**
  - 21.1 Bidders shall be allowed to submit bids by mail, by courier or by hand into the bid box or at the physical address of the municipality (reception, over the counter at the SCMU as applicable) before the closing time of the bids.
  - 21.2 Bids received via courier services must be submitted in time and deposited into the bid box by the courier services. Officials may not deposit bids into the bid box on behalf of courier services and the Municipality accepts no responsibility for late delivery by courier services or for delivery at the wrong address.
  - 21.3 Tenders that are deposited in the incorrect box or late will not be considered.
22. **BID OPENING**
  - 22.1 Bids shall be opened in public at the Cape Agulhas Municipal Offices as soon as possible after the closing time for the receipt of bids.
  - 22.2 Where practical, prices will be read out at the time of opening bids.
  - 22.3 The Municipality will record in a register (which is open to public inspection) and publish on its website, the details of bids received by the closing date and time.
  - 22.4 Any bid received after the appointed time for the closing of bids **shall not be considered** but shall be filed unopened with the other bids received, which bid(s) can be returned to the bidder at his request and cost.
23. **ARITHMETICAL ERRORS, OMISSIONS AND DISCREPANCIES**
  - 23.1 Check responsive tenders for discrepancies between amounts in words and amounts in figures. Where there is a discrepancy between the amounts in figures and the amount in words, the amount in words shall govern.
  - 23.2 Check the highest ranked tender or tenderer with the highest number of tender evaluation points after the evaluation of tender offers in accordance with paragraph 20 for:
    - a) the gross misplacement of the decimal point in any unit rate;

- b) omissions made in completing the pricing schedule or bills of quantities; or
  - c) arithmetic errors in:
    - i) line-item totals resulting from the product of a unit rate and a quantity in bills of quantities or schedules of prices; or
    - ii) the summation of the prices.
- 23.3 Notify the tenderer of all errors or omissions that are identified in the tender offer and either confirm the tender offer as tendered or accept the corrected total of prices.
- 23.4 Where the tenderer elects to confirm the tender offer as tendered, correct the errors as follows:
  - a) If bills of quantities or 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 quoted shall govern, and the unit rate shall be corrected.
  - b) 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 bills of quantities apply) to achieve the tendered total of the prices.
- 24. REQUIREMENTS OF A VALID BID:**
- 24.1 The following duly completed documents and / or information must be submitted with the submission of the bid. Failure to comply with this requirement will invalidate the bid. The bid will not be considered, and no further correspondence will be entered into with regard to the following matters:
  - 24.1.1 Non-submission of a valid Tax Clearance Certificate and / or PIN,
  - 24.1.2 Incomplete Pricing Schedule or Bill of Quantities,
  - 24.1.3 A Form of Offer not signed in non-erasable ink,
  - 24.1.4 Bid submissions with material alterations / corrections not in compliance with Clause 3 and 5 above will be rejected.
- 24.2 The Municipality may, after the closing date, request additional information or clarification of tenders in writing, which will include the following:
  - 24.2.1 To obtain a copy of the most recent municipal account(s) from the recommended bidder;
  - 24.2.2 To clarify or verify pricing where the prices are unclear or an obvious mistake has been detected, e.g. a total price was given instead of a unit price or vice versa;
  - 24.2.3 To obtain the personal income tax number(s) from the recommended bidder;
  - 24.2.4 To obtain a valid Tax compliance status PIN if the certificate has expired or become inactive after the closing date of the tender;
  - 24.2.5 To obtain a valid letter of good standing from the Workmen's Compensation Commissioner, the latest assessment and proof of payment thereof;
  - 24.2.6 To obtain a valid and original B-BBEE certificate or sworn affidavit to verify preference points claimed by a bidder where the bidder submitted only a copy of the B-BBEE certificate or sworn affidavit with the bid submission.
  - 24.2.6.1 If a bidder fails to submit a B-BBEE certificate or a sworn affidavit with the bid submission, the Municipality will not request or allow the bidder to submit it afterwards.**
- 25. TEST FOR RESPONSIVENESS**
- 25.1 **A bid will be considered non-responsive if:**
  - 25.1.1 the bid is not in compliance with the specifications.
  - 25.1.2 the bidder has not fully completed and signed where required, all the returnable documents as listed in the bid document and/or
  - 25.1.3 the bidder has failed to clarify or submit any supporting documentation within 3 business days of being requested to do so in writing

25.2 The Municipality reserves the right **to accept or reject:**

25.2.1 any variation, deviation, bid offer, or alternative bid offer; may cancel the bidding process and reject all bid offers at any time before the formation of a contract.

25.2.2 The Municipality has the right to summarily disqualify any bidder who, either at the date of submission of a bid or at the date of its award, is indebted to the Municipality in

respect of any Municipal rate and taxes or municipal service charges for more than three months. However, an agreement signed by the bidder whereby the bidder agrees that a percentage or fixed amounts at the discretion of the municipality, be deducted from payments due to him/her for this bid, until the debt is paid in full, will also be accepted by the Municipality.

#### **POPIA DISCLAIMER**

The Information Officer (Municipal Manager) undertakes that all personal and confidential information will be processed lawfully and in a reasonable manner that does not infringe the privacy of you or your organization as the data subject. The processing is necessary and complies with an obligation imposed by law on us, the responsible party and the processing protects your rights to effective service delivery.

For more details, you can refer to the Cape Agulhas Municipality, Privacy Policy available at [www.capeagulhas.gov.za](http://www.capeagulhas.gov.za)  
*The Protection of Personal Information Act (POPIA), Act No. 4 of 2013*

Signed .....

Date .....

Name .....

Position .....

Tenderer .....



# Form of Offer and Acceptance

## Offer

The Employer, identified in the acceptance signature block, has solicited offers to enter into a contract for the procurement of:

### CONTRACT: SCM41/2025/26 ICT SUPPORT SERVICES AND LICENSING FOR A PERIOD OF 3 YEARS

The tenderer, identified in the offer signature block, has examined the documents listed in the tender data and addenda thereto as listed in the returnable schedules, and by submitting this offer has accepted the conditions of tender.

By the representative of the tenderer, deemed to be duly authorized, signing this part of this form of offer and acceptance, the tenderer offers to perform all of the obligations and liabilities of the service provider under the contract including compliance with all its terms and conditions according to their true intent and meaning for an amount to be determined in accordance with the conditions of contract identified in the contract data.

### The offered total of the prices inclusive of value added tax is

..... Rands (in words);

R.....in figures

This offer may be accepted by the Employer by signing the acceptance part of this form of offer and acceptance and returning one copy of this document to the tenderer before the end of the period of validity stated in the tender data, whereupon the tenderer becomes the party named as the service provider in the conditions of contract identified in the contract data.

Signature .....

Name .....

Cape Agulhas Municipality .....

### for the tenderer

(Name and address of organization) .....

Name and signature of witness ..... Date .....

.....

## Acceptance (TO BE COMPLETED BY THE MUNICIPALITY)

By signing this part of this form of offer and acceptance, the employer identified below accepts the tenderer's offer. In consideration thereof, the employer shall pay the service provider the amount due in accordance with the conditions of contract identified in the contract data. Acceptance of the tenderer's offer shall form an agreement between the employer and the tenderer upon the terms and conditions contained in this agreement and in the contract that is the subject of this agreement.

The terms of the contract, are contained in:

Part C1: Agreements and contract data, (which includes this agreement)  
Part C2: Pricing data

and drawings and documents or parts thereof, which may be incorporated by reference into Parts above.

Deviations from and amendments to the documents listed in the tender data and any addenda thereto as listed in the tender schedules as well as any changes to the terms of the offer agreed by the tenderer and the employer during this process of offer and acceptance, are contained in the schedule of deviations attached to and forming part of this agreement. No amendments to or deviations from said documents are valid unless contained in this schedule.

The tenderer shall within two weeks after receiving a completed copy of this agreement, including the schedule of deviations (if any), contact the employer's representative (whose details are given in the contract data) to arrange the delivery of any bonds, guarantees, proof of insurance and any other documentation to be provided in terms of the conditions of contract identified in the contract data at, or just after, the date this agreement comes into effect. Failure to fulfill any of these obligations in accordance with those terms shall constitute a repudiation of this agreement.

Notwithstanding anything contained herein, this agreement comes into effect on the date when the tenderer receives one fully completed original copy of this document, including the schedule of deviations (if any). Unless the tenderer (now Contractor) within five working days of the date of such receipt notifies the employer in writing of any reason why he cannot accept the contents of this agreement, this agreement shall constitute a binding contract between the parties.

Signature .....

Name .....

Cape Agulhas Municipality .....

for the

**Employer** CAPE AGULHAS MUNICIPALITY  
1 DIRKIE UYS STREET  
BREDASDORP  
7280

Name and .....

signature .....

of witness .....

Date .....

.....

## Contract Data

### Part 1: Contract Data provided by the Employer

#### GENERAL CONDITIONS OF CONTRACT - National Treasury General Conditions of Contract

The General Conditions of Contract, as issued by the National treasury, is applicable to this Contract and is obtainable from [www.treasury.gov.za](http://www.treasury.gov.za)

The General Conditions of Contract shall be read in conjunction with the special condition as set out on pages 5 – 123. The Special Conditions shall have precedence in the interpretation of any ambiguity or inconsistency between it and the General Conditions of Contract.

The Employer is: **Cape Agulhas Municipality**  
**PO Box 51,**  
**Bredasdorp,**  
**7280**

The Employer's Telephone Number is: **028 425 5500**

The Employer's VAT Registration Number is: **4570109571**

The designated contact person of the Cape Agulhas Municipality is:

Name: Kevin Fourie

Telephone: 028 425 5500

E-mail: [kevinf@capeagulhas.gov.za](mailto:kevinf@capeagulhas.gov.za)

### Part 2: Data provided by the Service Provider

The **Service Provider** is: .....

Postal Address: .....  
.....

Physical Address: .....  
.....

Telephone: .....

The **authorized and designated representative** of the Service Provider is:

Name: .....

The address for receipt of communication is:

Address: .....  
.....

Telephone: .....

Email: .....

**SIGNED ON BEHALF OF TENDERER:** .....

CAPE AGULHAS MUNICIPALITY	
GENERAL CONDITIONS OF CONTRACT	
<b>1. DEFINITIONS</b>	
The following terms shall be interpreted as indicated:	
"Closing time"	means the date and hour specified in the bidding documents for the receipt of bids.
"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.
"Contract price"	means the price payable to the supplier under the contract for the full and proper performance of his contractual obligations.
"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.
"Countervailing duties"	are imposed in cases where an enterprise abroad is subsidized by its government and encouraged to market its products internationally
"Country of origin"	means the place where the goods were mined, grown or produced or from which the services are supplied. Goods are produced when, through manufacturing, processing or substantial and major assembly of components, a commercially recognized new product results that is substantially different in basic characteristics or in purpose or utility from its components.
"Day"	means calendar day.
"Delivery"	means delivery in compliance of the conditions of the contract or order.
"Delivery ex stock"	means immediate delivery directly from stock actually on hand
"Delivery into consignees store or to his site"	means delivered and unloaded in the specified store or depot or on the specified site in compliance with the conditions of the contract or order, the supplier bearing all risks and charges involved until the supplies are so delivered and a valid receipt is obtained.
"Dumping"	occurs when a private enterprise abroad market its goods on own initiative in the RSA at lower prices than that of the country of origin and which have the potential to harm the local industries in the RSA.
"Force majeure"	means an event beyond the control of the supplier and not involving the supplier's fault or negligence and not foreseeable. Such events may include, but is not restricted to, acts of the purchaser in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.
"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.
"GCC"	means the General Conditions of Contract.
"Goods"	means all of the equipment, machinery, and/or other materials that the supplier is required to supply to the purchaser under the contract.
"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.
"Local content"	means that portion of the bidding price which is not included in the imported content provided that local manufacture does take place.
"Manufacture"	means the production of products in a factory using labour, materials, components and machinery and includes other related value-adding activities.
"Order"	means an official written order issued for the supply of goods or works or the rendering of a service.
"Project site"	where applicable, means the place indicated in bidding documents.
"Purchaser"	means the organization purchasing the goods.
"Republic"	means the Republic of South Africa.
"SCC"	means the Special Conditions of Contract.
"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.
"Supplier"	means the successful bidder who is awarded the contract to maintain and administer the required and specified service(s) to the State.
"Tort"	means in breach of contract.
"Turnkey"	means a procurement process where one service provider assumes total responsibility for all aspects of the project and delivers the full end product / service required by the contract.
"Written" or "in writing"	means handwritten in ink or any form of electronic or mechanical writing.
<b>2. Application</b>	

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.
<b>3. General</b>	
3.1.	Unless otherwise indicated in the bidding documents, the purchaser shall not be liable for any expense incurred in the preparation and submission of a bid. Where applicable a non-refundable fee for documents may be charged.
3.2.	Invitations to bid are usually published in locally distributed news media and on the municipality / municipal entity website.
<b>4. Standards</b>	
4.1.	The goods supplied shall conform to the standards mentioned in the bidding documents and specifications.
<b>5. Use of contract documents and information; inspection.</b>	
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 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.
<b>6. Patent rights</b>	
6.1.	The supplier shall indemnify the purchaser against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the goods or any part thereof by the purchaser.
6.2.	When a supplier developed documentation / projects for the municipality / municipal entity, the intellectual, copy and patent rights or ownership of such documents or projects will vest in the municipality / municipal entity.
<b>7. Performance security</b>	
7.1.	Within thirty (30) days of receipt of the notification of contract award, the successful bidder shall furnish to the purchaser the performance security of the amount specified in SCC.
7.2.	The proceeds of the performance security shall be payable to the purchaser as compensation for any loss resulting from the supplier's failure to complete his obligations under the contract.
7.3.	The performance security shall be denominated in the currency of the contract or in a freely convertible currency acceptable to the purchaser and shall be in one of the following forms:
7.3.1.	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
7.3.2.	a cashier's or certified cheque
7.4.	The performance security will be discharged by the purchaser and returned to the supplier not later than thirty (30) days following the date of completion of the supplier's performance obligations under the contract, including any warranty obligations, unless otherwise specified.
<b>8. Inspections, tests and analyses</b>	
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 inspections tests and analysis, the bidder or contractor's premises shall be open, at all reasonable hours, for inspection by a representative of the purchaser or an organization acting on behalf of the purchaser.
8.3.	If there are no inspection requirements indicated in the bidding documents and no mention is made in the contract, but during the contract period it is decided that inspections shall be carried out, the purchaser shall itself make the necessary arrangements, including payment arrangements with the testing authority concerned.
8.4.	If the inspections, tests and analyses referred to in clauses 8.2 and 8.3 show the goods to be in accordance with the contract requirements, the cost of the inspections, tests and analyses shall be defrayed by the purchaser.
8.5.	Where the goods or services referred to in clauses 8.2 and 8.3 do not comply with the contract requirements, irrespective of whether such goods or services are accepted or not, the cost in connection with these inspections, tests or analyses shall be defrayed by the supplier.
8.6.	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 goods may on or after delivery be inspected, tested or analysed and may be rejected if found not to comply with the requirements of the contract. Such rejected goods shall be held at the cost and risk of the supplier who shall, when called upon, remove them immediately at his own cost and forthwith substitute them with goods which do comply with the requirements of the contract. Failing such removal the rejected goods shall be returned at the suppliers cost and risk. Should the supplier fail to provide the substitute goods forthwith, the purchaser may, without giving the supplier further opportunity to substitute the rejected goods, purchase such goods as may be necessary at the expense of the supplier.
8.8.	The provisions of clauses 8.4 to 8.7 shall not prejudice the right of the purchaser to cancel the contract on account of a breach of the conditions thereof, or to act in terms of Clause 22 of GCC.

9.1.	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, and in any subsequent instructions ordered by the purchaser.
<b>10. Delivery</b>	
10.1.	Delivery of the goods shall be made by the supplier in accordance with the documents and terms specified in the contract. The details of shipping and/or other documents to be furnished by the supplier are specified.
<b>11. Insurance</b>	
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.
<b>12. Transportation</b>	
12.1.	Should a price other than an all-inclusive delivered price be required, this shall be specified.
<b>13. Incidental</b>	
13.1.	The supplier may be required to provide any or all of the following services, including additional services, if any: <ul style="list-style-type: none"> <li>13.1.1. performance or supervision of on-site assembly and/or commissioning of the supplied goods;</li> <li>13.1.2. furnishing of tools required for assembly and/or maintenance of the supplied goods;</li> <li>13.1.3. furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied goods;</li> <li>13.1.4. 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</li> <li>13.1.5. 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.</li> </ul>
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.
<b>14. Spare parts</b>	
14.1.	As specified, the supplier may be required to provide any or all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the supplier: <ul style="list-style-type: none"> <li>14.1.1. 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;</li> <li>14.1.2. in the event of termination of production of the spare parts: <ul style="list-style-type: none"> <li>14.1.2.1. advance notification to the purchaser of the pending termination, in sufficient time to permit the purchaser to procure needed requirements; and</li> <li>14.1.2.2. following such termination, furnishing at no cost to the purchaser, the blueprints, drawings, and specifications of the spare parts, if requested.</li> </ul> </li> </ul>
<b>15. Warranty</b>	
15.1.	The supplier warrants that the goods supplied under the contract are new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials unless provided otherwise in the contract. The supplier further warrants that all goods supplied under this contract shall have no defect, arising from design, materials, or workmanship (except when the design and/or material is required by the purchaser's specifications) or from any act or omission of the supplier, that may develop under normal use of the supplied goods in the conditions prevailing in the country of final destination.
15.2.	This warranty shall remain valid for twelve (12) months after the goods, or any portion thereof as the case may be, have been delivered to and accepted at the final destination indicated in the contract, or for eighteen (18) months after the date of shipment from the port or place of loading in the source country, whichever period concludes earlier, unless specified otherwise in SCC.
15.3.	The purchaser shall promptly notify the supplier in writing of any claims arising under this warranty.
15.4.	Upon receipt of such notice, the supplier shall, within the period specified in SCC and with all reasonable speed, repair or replace the defective goods or parts thereof, without costs to the purchaser.
15.5.	If the supplier, having been notified, fails to remedy the defect(s) within the period specified, 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.
<b>16. Payment</b>	
16.1.	The method and conditions of payment to be made to the supplier under this contract shall be specified.
16.2.	The supplier shall furnish the purchaser with an invoice accompanied by a copy of the delivery note and upon fulfillment of other obligations stipulated in the contract.
16.3.	Payments shall be made by the purchaser no later than thirty (30) days after submission of an invoice, statement or claim by the supplier.
16.4.	Payment will be made in Rand unless otherwise stipulated.

<b>17. Prices</b>
17.1. Prices charged by the supplier for goods delivered and services performed under the contract shall not vary from the prices quoted by the supplier in his bid, with the exception of any price adjustments authorized or in the purchaser's request for bid validity extension, as the case may be.
<b>18. Variation orders</b>
18.1. In cases where the estimated value of the envisaged changes in purchase does not vary more than 15% of the total value of the original contract, the contractor may be instructed to deliver the goods or render the services as such. In cases of measurable quantities, the contractor may be approached to reduce the unit price and such offers, may be accepted provided that there is no escalation in price.
<b>19. Assignment</b>
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.
<b>20. Subcontracts</b>
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.
<b>21. Delays in the supplier's performance</b>
21.1. Delivery of the goods and performance of services shall be made by the supplier in accordance with the time schedule prescribed by the purchaser in the contract.
21.2. If at any time during performance of the contract, the supplier or its subcontractor(s) should encounter conditions impeding timely delivery of the goods and performance of services, the supplier shall promptly notify the purchaser in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the supplier's notice, the purchaser shall evaluate the situation and may at his discretion extend the supplier's time for performance, with or without the imposition of penalties, in which case the extension shall be ratified by the parties by amendment of contract.
21.3. The right is reserved to procure outside of the contract small quantities or to have minor essential services executed if an emergency arises, the supplier's point of supply is not situated at or near the place where the supplies are required, or the supplier's services are not readily available.
21.4. Except as provided under GCC Clause 25, a delay by the supplier in the performance of its delivery obligations shall render the supplier liable to the imposition of penalties, pursuant to GCC Clause 22, unless an extension of time is agreed upon pursuant to GCC Clause 22 without the application of penalties.
21.5. 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.
<b>22. Penalties</b>
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.
<b>23. Termination for default</b>
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: 23.1.1. 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; 23.1.2. if the Supplier fails to perform any other obligation(s) under the contract; or 23.1.3. if the supplier, in the judgment of the purchaser, has engaged in corrupt or fraudulent practices in competing for or in executing the contract.
23.2. In the event the purchaser terminates the contract in whole or in part, the purchaser may procure, upon such terms and in such manner as it deems appropriate, goods, works or services similar to those undelivered, and the supplier shall be liable to the purchaser for any excess costs for such similar goods, works or services. However, the supplier shall continue performance of the contract to the extent not terminated.
23.3. Where the purchaser terminates the contract in whole or in part, the purchaser may decide to impose a restriction penalty on the supplier by prohibiting such supplier from doing business with the public sector for a period not exceeding 10 years.
23.4. If a purchaser intends imposing a restriction on a supplier or any person associated with the supplier, the supplier will be allowed a time period of not more than fourteen (14) days to provide reasons why the envisaged restriction should not be imposed. Should the supplier fail to respond within the stipulated fourteen (14) days the purchaser may regard the supplier as having no objection and proceed with the restriction.
23.5. Any restriction imposed on any person by the purchaser will, at the discretion of the purchaser, also be applicable to any other enterprise or any partner, manager, director or other person who wholly or partly exercises or exercised or may exercise control over the enterprise of the first-mentioned person, and with which enterprise or person the first-mentioned person, is or was in the opinion of the purchase actively associated.
23.6. If a restriction is imposed, the purchaser must, within five (5) working days of such imposition, furnish the National Treasury, with the following information: 23.6.1. the name and address of the supplier and / or person restricted by the purchaser; 23.6.2. the date of commencement of the restriction 23.6.3. the period of restriction; and 23.6.4. the reasons for the restriction. These details will be loaded in the National Treasury's central database of suppliers or persons prohibited from doing business with the public sector.

23.7.	If a court of law convicts a person of an offence as contemplated in sections 12 or 13 of the Prevention and Combating of Corrupt Activities Act, No. 12 of 2004, the court may also rule that such person's name be endorsed on the Register for Tender Defaulters. When a person's name has been endorsed on the Register, the person will be prohibited from doing business with the public sector for a period not less than five years and not more than 10 years. The National Treasury is empowered to determine the period of restriction and each case will be dealt with on its own merits. According to section 32 of the Act the Register must be open to the public. The Register can be perused on the National Treasury website.
<b>24. Anti-dumping and countervailing duties and rights</b>	
24.1.	When, after the date of bid, provisional payments are required, or antidumping or countervailing duties are imposed, or the amount of a provisional payment or anti-dumping or countervailing right is increased in respect of any dumped or subsidized import, the State is not liable for any amount so required or imposed, or for the amount of any such increase. When, after the said date, such a provisional payment is no longer required or any such anti-dumping or countervailing right is abolished, or where the amount of such provisional payment or any such right is reduced, any such favourable difference shall on demand be paid forthwith by the contractor to the State or the State may deduct such amounts from moneys (if any) which may otherwise be due to the contractor in regard to supplies or services which he delivered or rendered, or is to deliver or render in terms of the contract or any other contract or any other amount which may be due to him.
<b>25. Force Majeure</b>	
25.1.	Notwithstanding the provisions of GCC Clauses 22 and 23, the supplier shall not be liable for forfeiture of its performance security, damages, or termination for default if and to the extent that his delay in performance or other failure to perform his obligations under the contract is the result of an event of force majeure.
25.2.	If a force majeure situation arises, the supplier shall promptly notify the purchaser in writing of such condition and the cause thereof. Unless otherwise directed by the purchaser in writing, the supplier shall continue to perform its obligations under the contract as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the force majeure event.
<b>26. Termination for insolvency</b>	
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.
<b>27. Settlement of Disputes</b>	
27.1.	If any dispute or difference of any kind whatsoever arises between the purchaser and the supplier in connection with or arising out of the contract, the parties shall make every effort to resolve amicably such dispute or difference by mutual consultation.
27.2.	If, after thirty (30) days, the parties have failed to resolve their dispute or difference by such mutual consultation, then either the purchaser or the supplier may give notice to the other party of his intention to commence with mediation. No mediation in respect of this matter may be commenced unless such notice is given to the other party.
27.3.	Should it not be possible to settle a dispute by means of mediation, it may be settled in a South African court of law.
27.4.	Notwithstanding any reference to mediation and/or court proceedings herein,
27.4.1.	the parties shall continue to perform their respective obligations under the contract unless they otherwise agree; and
27.4.2.	the purchaser shall pay the supplier any monies due for goods delivered and / or services rendered according to the prescripts of the contract.
<b>28. Limitation of liability</b>	
28.1.	Except in cases of criminal negligence or wilful misconduct, and in the case of infringement pursuant to Clause 6;
28.1.1.	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
28.1.2.	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.
<b>29. Governing language</b>	
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.
<b>30. Applicable law</b>	
30.1.	The contract shall be interpreted in accordance with South African laws, unless otherwise specified.
<b>31. Notices</b>	
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.
<b>32. Taxes and duties</b>	
32.1.	A foreign supplier shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed outside the purchaser's country.
32.2.	A local supplier shall be entirely responsible for all taxes, duties, license fees, etc., incurred until delivery of the contracted goods to the purchaser.
32.3.	No contract shall be concluded with any bidder whose tax matters are not in order. Prior to the award of a bid SARS must have certified that the tax matters of the preferred bidder are in order.
32.4.	No contract shall be concluded with any bidder whose municipal rates and taxes and municipal services charges are in arrears.



<b>33. Transfer of contracts</b>	
33.1.	The contractor shall not abandon, transfer, cede, assign or sublet a contract or part thereof without the written permission of the purchaser.
<b>34. Amendment of contracts</b>	
34.1.	No agreement to amend or vary a contract or order or the conditions, stipulations or provisions thereof shall be valid and of any force unless such agreement to amend or vary is entered into in writing and signed by the contracting parties. Any waiver of the requirement that the agreement to amend or vary shall be in writing, shall also be in writing.
<b>35. Prohibition of restrictive practices</b>	
35.1.	In terms of section 4 (1) (b) (iii) of the Competition Act No. 89 of 1998, as amended, an agreement between, or concerted practice by, firms, or a decision by an association of firms, is prohibited if it is between parties in a horizontal relationship and if a bidder(s) is / are or a contractor(s) was / were involved in collusive bidding.
35.2.	If a bidder(s) or contractor(s) based on reasonable grounds or evidence obtained by the purchaser has / have engaged in the restrictive practice referred to above, the purchaser may refer the matter to the Competition Commission for investigation and possible imposition of administrative penalties as contemplated in section 59 of the Competition Act No 89 Of 1998.
35.3.	If a bidder(s) or contractor(s) has / have been found guilty by the Competition Commission of the restrictive practice referred to above, the purchaser may, in addition and without prejudice to any other remedy provided for, invalidate the bid(s) for such item(s) offered, and / or terminate the contract in whole or part, and / or restrict the bidder(s) or contractor(s) from conducting business with the public sector for a period not exceeding ten (10) years and / or claim damages from the bidder(s) or contractor(s) concerned.
<b><i>General Conditions of Contract (revised July 2010)</i></b>	

### DECLARATION OF INTEREST

1. No bid will be accepted from persons in the service of the state<sup>1</sup>.
2. Any person, having a kinship with persons in the service of the state, including a blood relationship, may make an offer or offers in terms of this invitation to bid. In view of possible allegations of favouritism, should the resulting bid, or part thereof, be awarded to persons connected with or related to persons in service of the state, it is required that the bidder or their authorised representative declare their position in relation to the evaluating/adjudicating authority.
3. In order to give effect to the above, the following questionnaire must be completed and submitted with the bid.

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

3.2 Identity Number: .....

3.3 Position occupied in the Company (director, trustee, shareholder<sup>2</sup>):.....

3.4 Company Registration Number: .....

3.5 Tax Reference Number:.....

3.6 VAT Registration Number: .....

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

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

3.8.1 If yes, furnish particulars. ....

.....

<sup>1</sup>MSCM Regulations: "in the service of the state" means to be –

(a) a member of –

- (i) any municipal council;
- (ii) any provincial legislature; or
- (iii) the national Assembly or the national Council of provinces;

(b) a member of the board of directors of any municipal entity;

(c) an official of any municipality or municipal entity;

(d) an employee of any national or provincial department, national or provincial public entity or constitutional institution within the meaning of the Public Finance Management Act, 1999 (Act No.1 of 1999);

(e) a member of the accounting authority of any national or provincial public entity; or

(f) an employee of Parliament or a provincial legislature.

(g) A Person who is an advisor or consultant contracted with the Municipality.

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

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

3.9.1 If yes, furnish particulars

**Section 3.9.1: Record of service of the state**

Indicate by marking the relevant boxes with a cross, if any sole proprietor, partner in a partnership or director, manager, principal shareholder or stakeholder in a company or close corporation is currently or has been within the last 12 months in the service of any of the following:

- ☐ a member of any municipal council
- ☐ a member of any provincial legislature
- ☐ a member of the National Assembly or the National Council of Province
- ☐ a member of the board of directors of any municipal entity
- ☐ an official of any municipality or municipal entity
- ☐ an employee of any provincial department, national or provincial public entity or constitutional institution within the meaning of the Public Finance Management Act, 1999 (Act 1 of 1999)
- ☐ a member of an accounting authority of any national or provincial public entity
- ☐ an employee of Parliament or a provincial legislature
- ☐ A Person who is an advisor or consultant contracted with the Municipality

If any of the above boxes are marked, disclose the following: (insert separate page if necessary)

Name of sole proprietor, partner, director, manager, principal shareholder or stakeholder	Name of institution, public office, board or organ of state and position held	Status of service (tick appropriate column)	
		current	Within last 12 months

\* Insert separate page if necessary

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

3.10.1 If yes, furnish particulars.

.....

.....

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

3.11.1 If yes, furnish particulars

.....

.....

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

3.12.1 If yes, furnish particulars.

.....

.....

3.13 Are any spouse, child or parent of the company's directors trustees, managers, principle shareholders or stakeholders in service of the state?

YES / NO

3.13.1 If yes, furnish particulars.

**Section 3.13.1: Record of spouses, children and parents in the service of the state**

Indicate by marking the relevant boxes with a cross, if any spouse, child or parent of a sole proprietor, partner in a partnership or director, manager, principal shareholder or stakeholder in a company or close corporation is currently or has been within the last 12 months been in the service of any of the following:

- |  |   |
|--|---|
| <input type="checkbox"/> a member of any municipal council                                     | <input type="checkbox"/> an employee of any provincial department, national or provincial public entity or constitutional institution within the meaning of the Public Finance Management Act, 1999 (Act 1 of 1999) |
| <input type="checkbox"/> a member of any provincial legislature                                |   |
| <input type="checkbox"/> a member of the National Assembly or the National Council of Province | <input type="checkbox"/> a member of an accounting authority of any national or provincial public entity  |
| <input type="checkbox"/> a member of the board of directors of any municipal entity            | <input type="checkbox"/> an employee of Parliament or a provincial legislature  |
| <input type="checkbox"/> an official of any municipality or municipal entity                   | <input type="checkbox"/> A Person who is an advisor or consultant contracted with the Municipality  |

Name of spouse, child or parent	Name of institution, public office, board or organ of state and position held	Status of service (tick appropriate column)	
		current	Within last 12 months

\* Insert separate page if necessary

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:

.....

.....

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

Full Name	Identity Number	State Employee Number

.....  
**Signature**

.....  
**Date**

.....  
**Capacity**

.....  
**Name of Bidder**

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

**CAMBD 5**

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

1 Are you by law required to prepare annual financial statements for auditing?

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

**\*YES / NO**

.....  
.....

2 Do you have any outstanding undisputed commitments for municipal services towards any municipality for more than three months or any other service provider in respect of which payment is overdue for more than 30 days?

**\*YES / NO**

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

2.2 If yes, provide particulars.

.....  
.....  
.....  
.....

3 Has any contract been awarded to you by an organ of state during the past five years, including particulars of any material non-compliance or dispute concerning the execution of such contract?

**\*YES / NO**

3.1 If yes, furnish particulars

.....  
.....

4. Will any portion of goods or services be sourced from outside the Republic, and, if so, what portion and whether any portion of payment from the municipality / municipal entity is expected to be transferred out of the Republic? **\*YES / NO**

4.1 If yes, furnish particulars

.....

.....

#### CERTIFICATION

I, THE UNDERSIGNED (NAME) .....

**CERTIFY THAT THE INFORMATION FURNISHED ON THIS DECLARATION FORM IS CORRECT.**

**I ACCEPT THAT THE STATE MAY ACT AGAINST ME SHOULD THIS DECLARATION PROVE TO BE**

**FALSE.**

.....  
Signature

.....  
Date

.....  
Position

.....  
Name of Bidder

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

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

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

### 1. GENERAL CONDITIONS

1.1 The following preference point systems are applicable to all bids:

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

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

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

c) Either the **90/10 or 80/20 preference point system** will be applicable in this tender. The lowest/ highest acceptable tender will be used to determine the accurate system once tenders are received.

1.2 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.

1.3 The maximum points for this tender are allocated as follows:

		POINTS
PRICE		80
SPECIFIC GOALS	50% of the 20 Points	20
• B-BBEE STATUS LEVEL OF CONTRIBUTOR	10	
• LOCALITY OF SUPPLIER	10	
Total points for Price and SPECIFIC GOALS		100

1.4 **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

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



## 2. DEFINITIONS

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

## 3. FORMULAE FOR PROCUREMENT OF GOODS AND SERVICES

### 3.1 POINTS AWARDED FOR PRICE

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

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

<b>80/20</b>	<b>or</b>	<b>90/10</b>	
$Ps = 80 \left( 1 - \frac{Pt - P_{min}}{P_{min}} \right)$	or	$Ps = 90 \left( 1 - \frac{Pt - P_{min}}{P_{min}} \right)$	

Where

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

## 4. POINTS AWARDED FOR SPECIFIC GOALS

- 4.1 In terms of Regulation 4(2); 5(2); 6(2) and 7(2) of the Preferential Procurement Regulations, preference points must be awarded for specific goals stated in the tender. For the purposes of this tender the tenderer will be allocated points based on the goals stated in table 1 below as may be supported by proof/ documentation stated in the conditions of this tender:
- 4.2 In cases where organs of state intend to use Regulation 3(2) of the Regulations, which states that, if it is unclear whether the 80/20 or 90/10 preference point system applies, an organ of state must, in the tender documents, stipulate in the case of—
  - (a) an invitation for tender for income-generating contracts, that either the 80/20 or 90/10 preference point system will apply and that the highest acceptable tender will be used to determine the applicable preference point system; or
  - (b) any other invitation for tender, that either the 80/20 or 90/10 preference point system will apply and that the lowest acceptable tender will be used to determine the applicable preference point system, then the organ of state must indicate the points allocated for specific goals for both the 90/10 and 80/20 preference point system.

## 5. POINTS AWARDED FOR SPECIFIC GOALS

- 5.1 The tendering conditions will stipulate the specific goals, as contemplated in section 2(1)(d)(ii) of the Preferential Procurement Act, to be attained.
- 5.2 A maximum of 20 points (80/20 preference points system) or 10 (90/10) preference points system), will be allocated for specific goals. These goals are:
- (a) contracting with persons, or categories of persons, historically disadvantaged by unfair discrimination on the basis of race, gender or disability.
  - (b) local labour and/ or promotion of enterprises located in the municipal area (phased in approach to be applied for other RDP goals)
- 5.3 Regarding paragraph 5.2 (a) at least **50% of the 20 points** will be allocated to promote this goal and points will be allocated in terms of the BBBEE scorecard as follows.

B-BBEE Status Level of Contributor	Number of Points for Preference (80/20)	Number of Points for Preference (90/10)
1	10	5
2	9	4.5
3	7	3.5
4	6	3
5	4	2
6	3	1.5
7	2	1
8	1	0.5
Non-compliant contributor	0	0

- 5.4 A tenderer **must submit proof** of its BBBEE status level contributor [scorecard].
- 5.5 A tenderer failing to submit proof of BBBEE status level of contributor –
- 5.5.1 may only score in terms of the 80/90-point formula for price; and
  - 5.5.2 scores 0 points for BBBEE status level of contributor, which is in line with section 2 (1) (d) (i) of the Act, where the supplier or service provider did not provide proof thereof.
- 5.6 Regarding paragraph 9.2 (b) a maximum of **50% of the 20/10 points** will be allocated to promote this goal. Points will be allocated as follows.

LOCALITY OF SUPPLIER ( <b>SUBMIT PROOF OF REGISTERED BUSINESS ADDRESS</b> ) E.G MUNICIPAL ACCOUNT OR LEASE AGREEMENT	50% of the 20 Points = <u>10</u>
Within the boundaries of the <b>Cape Agulhas Municipality</b>	10
Within the boundaries of the <b>Overberg</b>	5
Within the boundaries of the <b>Western Cape</b>	2
Outside of the boundaries of the Western Cape	0

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

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

The specific goals allocated points in terms of this tender	Number of points allocated (80/20 system)	B-BBEE Status Level of Contribution as reflected on the B-BBEE Certificate (To be completed by the tenderer)	Number of points claimed (80/20 system) (To be completed by the tenderer)
<b>SPECIFIC GOALS</b>	<b>20</b>		
<b>1. B-BBEE STATUS LEVEL OF CONTRIBUTOR</b>	<b>10</b>	_____	_____
<b>2. LOCALITY OF SUPPLIER</b>	<b>10</b>	<b>Indicate (YES/NO)</b>	<b>Number of points claimed (maximum 10 points)</b>
<ul style="list-style-type: none"> <li>Within the boundaries of the <b>Cape Agulhas Municipality</b></li> </ul>	10	_____	_____
<ul style="list-style-type: none"> <li>Within the boundaries of the <b>Overberg</b></li> </ul>	5	_____	
<ul style="list-style-type: none"> <li>Within the boundaries of the <b>Western Cape</b></li> </ul>	2	_____	
<ul style="list-style-type: none"> <li>Outside of the boundaries of the Western Cape</li> </ul>	0	_____	

#### 5.7 Promotion of Local area suppliers

The tenderer must be located within the geographical area specified and must have a fully functional office / premises from where it operates.

5.7.1. The registered address as reflected on the Companies and Intellectual Property Commission (CIPC) report.

5.7.2. Municipal account registered in the name of the tenderer not older than 3 months.

5.7.3. Where the tenderer is not the owner of the property:

5.7.3.1. A valid lease agreement; or

5.7.3.2. A sworn affidavit not older than 3 months from the property owner that the address used to claim points in paragraph.

5.7.2 (Table 1) above is being rented out to the tenderer at no cost.

5.7.3. The registered address as reflected on the Companies and Intellectual Property Commission report.

- Cape Agulhas Municipality will reserve the right to use any and all available information at its disposal, including conducting site visit and inspections to verify a bidders claim of having a local office within the Cape Agulhas Municipal area and that the bidder or principal of the bidder (in the event of the bidder being a legal entity) is domiciled within the Cape Agulhas Municipal area.
- The principle of substance over legal form, as defined in the Standards of Generally Recognised Accounting Practice (GRAP), will be applied in such assessments. (This means that even though a bidder may present a rental agreement, the claim of having a local office will be assessed in its actual substance and not by just accepting the legal documentation).
- The purpose of the locality points is to promote local economic development within the Cape Agulhas Municipal area and any bidder attempting to circumvent the substance of this initiative through any means, including by means of fronting, will be reported to the National Treasury for blacklisting on the Central Supplier Database (CSD).

5.8. Where the tenderer submitted incorrect or outdated information (municipal account, lease agreement or sworn affidavit) or none of the above, it will be interpreted to mean that preference points for Promotion of Local area of supplier are not claimed.

**6. DECLARATION WITH REGARD TO COMPANY/FIRM**

6.1 Name of company/firm:.....

6.2 Company registration number.....

6.3 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]

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

- i) The information furnished is true and correct;
- ii) The preference points claimed are in accordance with the General Conditions as indicated in paragraph 1 of this form;
- iii) In the event of a contract being awarded as a result of points claimed as shown in paragraphs 1.4 and 6.1, the contractor may be required to furnish documentary proof to the satisfaction of the purchaser that the claims are correct;
- iv) If the specific goals has been claimed or obtained on a fraudulent basis or any of the conditions of contract have not been fulfilled, the purchaser may, in addition to any other remedy it may have –
  - (a) disqualify the person from the tendering process;
  - (b) recover costs, losses or damages it has incurred or suffered as a result of that person's conduct;
  - (c) cancel the contract and claim any damages which it has suffered as a result of having to make less favourable arrangements due to such cancellation;
  - (d) recommend that the tenderer or contractor, its shareholders and directors, or only the shareholders and directors who acted on a fraudulent basis, be restricted by the National Treasury 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 forward the matter for criminal prosecution, if deemed necessary.

.....  
**SIGNATURE(S) OF TENDERER(S)**

**SURNAME AND NAME:** .....

**DATE:** .....

**ADDRESS:** .....

.....

.....

**CONTRACT FORM - RENDERING OF SERVICES**

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

**PART 1 (TO BE FILLED IN BY THE BIDDER)**

1. I hereby undertake to supply all or any of the goods and/or works described in the attached bidding documents to **Cape Agulhas Municipality** in accordance with the requirements and specifications stipulated in bid number **SCM41/2025/26** at the price/s quoted. My offer/s remain binding upon me and open for acceptance by the purchaser during the validity period indicated and calculated from the closing time of bid.
2. The following documents shall be deemed to form and be read and construed as part of this agreement:
  - (i) Bidding documents, viz
    - Invitation to bid;
    - Tax clearance certificate;
    - Pricing schedule(s);
    - Technical Specification(s);
    - Preference claims for Broad Based Black Economic Empowerment Status Level of Contribution in terms of the Preferential Procurement Regulations 2022;
    - Declaration of interest;
    - Declaration of bidder's past SCM practices;
    - Certificate of Independent Bid Determination;
    - Special Conditions of Contract;
  - (ii) General Conditions of Contract; and
  - (iii) Other (specify)
3. I confirm that I have satisfied myself as to the correctness and validity of my bid; that the price(s) and rate(s) quoted cover all the goods and/or works specified in the bidding documents; that the price(s) and rate(s) cover all my obligations and I accept that any mistakes regarding price(s) and rate(s) and calculations will be at my own risk.
4. I accept full responsibility for the proper execution and fulfilment of all obligations and conditions devolving on me under this agreement as the principal liable for the due fulfillment of this contract.
5. I declare that I have no participation in any collusive practices with any bidder or any other person regarding this or any other bid.
6. I confirm that I am duly authorized to sign this contract.

NAME (PRINT) .....

CAPAMUNICIPALITY .....

SIGNATURE .....

NAME OF FIRM .....

DATE .....

**WITNESSES**

1 .....

2. ....

DATE: .....

## CONTRACT FORM - RENDERING OF SERVICES

## PART 2 (TO BE FILLED IN BY THE MUNICIPALITY)

1. I **WESSEL RABBETS** in my Cape Municipality as **MUNICIPAL MANAGER** accept your bid under reference number **SCM41/2025/26** dated **13 February 2026** for the rendering of services indicated hereunder and/or further specified in the annexure(s).
2. An official order indicating delivery instructions is forthcoming.
3. I undertake to make payment for the goods/works delivered in accordance with the terms and conditions of the contract, within 30 (thirty) days after receipt of an invoice accompanied by the delivery note.

DESCRIPTION OF SERVICE	PRICE (ALL APPLICABLE TAXES INCLUDED)	COMPLETION DATE	B-BBEE STATUS LEVEL

4. I confirm that I am duly authorized to sign this contract.

SIGNED AT .....ON.....

NAME (PRINT) .....

SIGNATURE .....

OFFICIAL STAMP

WITNESSES

1. ....

2. ....

DATE .....

## DECLARATION OF BIDDER'S PAST SUPPLY CHAIN MANAGEMENT PRACTICES

- 1 This Municipal Bidding Document must form part of all bids invited.
- 2 It serves as a declaration to be used by municipalities and municipal entities in ensuring that when goods and services are being procured, all reasonable steps are taken to combat the abuse of the supply chain management system.
- 3 The bid of any bidder may be rejected if that bidder, or any of its directors have:
  - a. abused the municipality's / municipal entity's supply chain management system or committed any improper conduct in relation to such system;
  - b. been convicted for fraud or corruption during the past five years;
  - c. willfully neglected, reneged on or failed to comply with any government, municipal or other public sector contract during the past five years; or
  - d. been listed in the Register for Tender Defaulters in terms of section 29 of the Prevention and Combating of Corrupt Activities Act (No 12 of 2004).
- 4 **In order to give effect to the above, the following questionnaire must be completed and submitted with the bid.**

Item	Question	Yes	No
4.1	Is the bidder or any of its directors listed on the National Treasury's Database of Restricted Suppliers as companies or persons prohibited from doing business with the public sector? <b>(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).</b>  The Database of Restricted Suppliers now resides on the National Treasury's website( <a href="http://www.treasury.gov.za">www.treasury.gov.za</a> ) and can be accessed by clicking on its link at the bottom of the home page.	Yes <input type="checkbox"/>	No <input type="checkbox"/>
4.1.1	If so, furnish particulars:		
4.2	Is the bidder or any of its directors listed on the Register for Tender Defaulters in terms of section 29 of the Prevention and Combating of Corrupt Activities Act (No 12 of 2004)? The Register for Tender Defaulters can be accessed on the National Treasury's website ( <a href="http://www.treasury.gov.za">www.treasury.gov.za</a> ) by clicking on its link at the bottom of the home page.	Yes <input type="checkbox"/>	No <input type="checkbox"/>
4.2.1	If so, furnish particulars:		
4.3	Was the bidder or any of its directors convicted by a court of law (including a court of law outside the Republic of South Africa) for fraud or corruption during the past five years?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
4.3.1	If so, furnish particulars:		

Item	Question	Yes	No
4.4	the bidder or any of its directors owe any municipal rates and taxes or municipal charges to the municipality / municipal entity, or to any other municipality / municipal entity, that is in arrears for more than three months?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
4.4.1	If so, furnish particulars:		
4.5	Was any contract between the bidder and the municipality / municipal entity or any other organ of state terminated during the past five years on account of failure to perform on or comply with the contract?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
4.7.1	If so, furnish particulars:		

### CERTIFICATION

I, THE UNDERSIGNED (FULL NAME) ..... CERTIFY THAT THE INFORMATION FURNISHED ON THIS DECLARATION FORM TRUE AND CORRECT.

I ACCEPT THAT, IN ADDITION TO CANCELLATION OF A CONTRACT, ACTION MAY BE TAKEN AGAINST ME SHOULD THIS DECLARATION PROVE TO BE FALSE.

.....  
Signature

.....  
Date

.....  
Position

.....  
Name of Bidder



## CERTIFICATE OF INDEPENDENT BID DETERMINATION

- 1 This Municipal Bidding Document (MBD) must form part of all bids<sup>1</sup> invited.
- 2 Section 4 (1) (b) (iii) of the Competition Act No. 89 of 1998, as amended, prohibits an agreement between, or concerted practice by, firms, or a decision by an association of firms, if it is between parties in a horizontal relationship and if it involves collusive bidding (or bid rigging).<sup>2</sup> Collusive bidding is a *pe se* prohibition meaning that it cannot be justified under any grounds.
- 3 Municipal Supply Regulation 38 (1) prescribes that a supply chain management policy must provide measures for the combating of abuse of the supply chain management system, and must enable the accounting officer, among others, to:
  - a. take all reasonable steps to prevent such abuse;
  - b. reject the bid of any bidder if that bidder or any of its directors has abused the supply chain management system of the municipality or municipal entity or has committed any improper conduct in relation to such system; and
  - c. cancel a contract awarded to a person if the person committed any corrupt or fraudulent act during the bidding process or the execution of the contract.
- 4 This MBD serves as a certificate of declaration that would be used by institutions to ensure that, when bids are considered, reasonable steps are taken to prevent any form of bid-rigging.
- 5 In order to give effect to the above, the attached Certificate of Bid Determination (MBD 9) must be completed and submitted with the bid:**

<sup>1</sup> Includes price quotations, advertised competitive bids, limited bids and proposals.

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

## **CERTIFICATE OF INDEPENDENT BID DETERMINATION**

I, the undersigned, in submitting the accompanying bid:

### **SCM41/2025/26 ICT SUPPORT SERVICES AND LICENSING FOR A PERIOD OF 3 YEARS**

in response to the invitation for the bid made by:

#### **CAPE AGULHAS MUNICIPALITY**

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

I certify, on behalf of: \_\_\_\_\_ that:  
(Name of Bidder)

1. I have read and I understand the contents of this Certificate;
2. I understand that the accompanying bid will be disqualified if this Certificate is found not to be true and complete in every respect;
3. I am authorized by the bidder to sign this Certificate, and to submit the accompanying bid, on behalf of the bidder;
4. Each person whose signature appears on the accompanying bid has been authorized by the bidder to determine the terms of, and to sign, the bid, on behalf of the bidder;
5. For the purposes of this Certificate and the accompanying bid, I understand that the word "competitor" shall include any individual or organization, other than the bidder, whether or not affiliated with the bidder, who:
  - (a) has been requested to submit a bid in response to this bid invitation;
  - (b) could potentially submit a bid in response to this bid invitation, based on their qualifications, abilities or experience; and
  - (c) provides the same goods and services as the bidder and/or is in the same line of business as the bidder

6. The bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with any competitor. However communication between partners in a joint venture or consortium<sup>3</sup> will not be construed as collusive bidding.
7. In particular, without limiting the generality of paragraphs 6 above, there has been no consultation, communication, agreement or arrangement with any competitor regarding:
  - (a) prices;
  - (b) geographical area where product or service will be rendered (market allocation)
  - (c) methods, factors or formulas used to calculate prices;
  - (d) the intention or decision to submit or not to submit, a bid;
  - (e) the submission of a bid which does not meet the specifications and conditions of the bid; or
  - (f) bidding with the intention not to win the bid.
8. In addition, there have been no consultations, communications, agreements or arrangements with any competitor regarding the quality, quantity, specifications and conditions or delivery particulars of the products or services to which this bid invitation relates.
9. The terms of the accompanying bid have not been, and will not be, disclosed by the bidder, directly or indirectly, to any competitor, prior to the date and time of the official bid opening or of the awarding of the contract.

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