

GREATER KOKSTAD MUNICIPALITY



**GREATER
KOKSTAD
MUNICIPALITY**
PROVINCE OF KWAZULU-NATAL

**SPECIFICATION AND BID DOCUMENT
FOR**

**SUPPLY, DELIVER AND MAINTAIN A FULLY INTEGRATED ICT
CYBER SECURITY SOLUTION FOR 36 MONTHS**

BID No- GKM 08-23/24

RE-ADVERTISEMENT

CLOSING DATE: 11 JANUARY 2024

CLOSING TIME: 12H00 PM

NAME OF BIDDER:

POSTAL ADDRESS:

.....
.....

TELEPHONE NUMBER:.....

FAX NUMBER:.....

E- MAIL ADRESS:

TENDER SUM (ALL INCLUSIVE):.....

BID NUMBER AND DESCRIPTION

The bid documents must be clearly marked: **SUPPLY, DELIVER AND MAINTAIN A FULLY INTEGRATED ICT CYBER SECURITY SOLUTION FOR 36 MONTHS**

BID NUMBER: GKM 08-23/24

Bid documents must be deposited in the tender box marked “**SUPPLY, DELIVER AND MAINTAIN A FULLY INTEGRATED ICT CYBER SECURITY SOLUTION FOR 36 MONTHS**” located at the reception area at Adam Kok III Building, 75 Hope Street, Kokstad not later than **11 JANUARY 2024 at 12h00**. Bidders must attach the following mandatory returnable documents to be considered for this bid and must note the applicable conditions:

- Price (s) quoted must be firm and must be inclusive of VAT
- Copy of CSD (Central Supplier Database) summary report
- Copy of company registration documents (compulsory)
- For Joint Venture Agreements, attach the CK's of each of the joint venture members (if applicable)
- Certified ID(s) copies of company director(s)
- Copy of current municipal account for all Director/s and Company (not owing more than 3 months) or copy of lease agreement from the relevant authority if the director/s or company is leasing. If the business is operated from the residence of one of the Director/s, an original affidavit, certified, must be submitted stating the address of the premises. For any other arrangement that is not covered above, director/s must submit an original affidavit, certified clarifying the arrangement. All affidavits must be original affidavits, certified and must be from the SAPS. Affidavits must be signed by the company director/s.
- Printed copy of SARS Tax Pin for further verification.
- Completed and signed Municipal Bidding Document attached to the tender document.

The following conditions will apply:

- Price(s) quoted must be valid for at least 120 days from date of your offer.
- Price(s) quoted must be firm and must be inclusive of VAT and disbursements.
- Your valid tax clearance certificate must be attached.

NB: No quotations will be considered from persons in the service of the state.

ADVERT

RE-ADVERTISEMENT

APPOINTMENT OF A SERVICE PROVIDER FOR THE SUPPLY, DELIVER AND MAINTAIN A FULLY INTEGRATED ICT CYBER SECURITY SOLUTION FOR 36 MONTHS

BID NO: GKM 08-23/24

The Greater Kokstad Municipality invites reputable and experienced service provider to **SUPPLY, DELIVER AND MAINTAIN A FULLY INTEGRATED ICT CYBER SECURITY SOLUTION FOR 36 MONTHS**.

The scope of work and bid requirements is stipulated in the bid document.

This advert is issued in compliance with the Preferential Procurement Regulation, 2022. Evaluation will be done on the following three-stages process in terms of National Treasury Circular No: 53:

Stage 1:

Assessment of Functionality. Only service providers who achieve a minimum of 70 points of the total available points will qualify for stage two of the Evaluation process. Functionality criteria is as follows:

Company Experience	(30 points)
Experience of a Key Personnel	(30 points)
Back-to-back service level agreement with OEM provider	(40 points)

Stage 2:

Evaluation will be done based on the 80/20 preferential point system, where 80 points will be allocated for price and 20 points for specific goals. Bidders must submit the required documentation to claim preference points.

POINTS AWARDED SPECIFIC GOALS

The 80/20 preferential point system will be applied, where 80 points will be allocated for price and 20 points for Municipality's specific goals that is on ownership and RDP Goals.

GOALS 1 - OWNERSHIP	MAX POINTS =14
Business owned more than 50% by black person	5
Business owned less than 50% by black person	2
Business owned more than 50% by women black	4
Business owned less than 50% by women black	2
Business owned more than 50% by black youth	3
Business owned more than 50% by disabled person/military veterans	2
GOAL 2 -RDP	MAX POINTS =6
Business falls under the SMME Category- QSE/EME	3
Promotion of business located within KZN province	2
Promotion of business located in South Africa outside KZN province	1

The tender document **must** be downloaded on the **Greater Kokstad Municipality website** www.kokstad.gov.za at no cost. **The municipality will not be held responsible for any incomplete documents downloaded on the Greater Kokstad Municipality website.**

A COMPULSORY briefing meeting will be held on **12 December 2023 at 11h00**, at Adam Kok III Building, 75 Hope Street, Kokstad. **No late comers will be admitted into the venue.**

Sealed tenders, marked **“Bid No.: “GKM 08-23/24 APPOINTMENT OF A SERVICE PROVIDER TO SUPPLY, DELIVER AND MAINTAIN A FULLY INTEGRATED ICT CYBER SECURITY SOLUTION FOR 36 MONTHS”** must be deposited in the **BOX** located at the Reception Area, 75 Hope Street, Kokstad, not later than **11 January 2024 at 12H00**, where after, bids will be opened in public.

Late, telegraphic, e-mailed or faxed bids will not be considered.

Technical Enquiries: **Mr. Y. Owusu**, Tel. 039 797 6711 Email: yawu.owusu@kokstad.gov.za
Supply Chain Management enquiries: Ms. A. Mahlaka Tel. 039 797 6644, or email: andiswa.mahlaka@kokstad.gov.za

Greater Kokstad Municipality does not bind itself to accept the lowest or any bid and reserves the right to accept the Bid in whole or part, at the rates quoted

MR. S R ZWANE
MUNICIPAL MANAGER
NOTICE NO.: 73-2023/2024

GREATER KOKSTAD MUNICIPALITY



GREATER
KOKSTAD
MUNICIPALITY
PROVINCE OF KWAZULU-NATAL

TERMS OF REFERENCE

SUPPLY, DELIVER AND MAINTAIN A FULLY INTEGRATED ICT CYBER SECURITY SOLUTION FOR 36 MONTHS

GKM 08-23/24

Issued and prepared by:
Greater Kokstad Municipality
75 Hope Street
P.O. Box 8
Kokstad
4700

Municipal Manager: Mr. S.R ZWANE
Contact Person: Mr. Yaw Owusu-Boakye
Tel: 039 797 6711
E-mail: Yaw.Owusu@kokstad.gov.za

NAME OF THE PROJECT: SUPPLY, DELIVER AND MAINTAIN A FULLY INTEGRATED ICT CYBER SECURITY SOLUTION FOR 36 MONTHS

1. BACKGROUND

The Greater Kokstad Municipality (GKM) requires a Holistic Cyber Security Solution for a period of 36 months. GKM's infrastructure comprises of 3 VLANS (Virtual Local Area Networks) across 10 sites, 300 devices (Routers, etc.) and 20 critical devices (Servers & Firewalls) connected to the Network, and 300 users. The activities of all devices connected to the network requires constant monitoring. GKM requires autonomous and real time security monitoring capabilities of analysing, detecting, and stopping threats as they arise.

2. AIMS OF THE PROJECT

To appoint a suitably qualified, ICT Cyber Security Service Provider to supply and install an Enterprise grade ICT Cyber Security Solution which must include:

- A fully Managed SIEM/SOC
- A fully Managed Detection and Response (MDR)
- A fully Managed Data Leakage Prevention (DLP)
- Vulnerability Assessment (VA) and Penetration Testing (PEN)
- A 24x7x365 Service Desk
- Security Training and Knowledge transfer

3. SCOPE AND TECHNICAL REQUIREMENTS

3.1 Managed SIEM/SOC Solution

Provide a SIEM/SOC Solution which offers but is not limited to the following:

- a) A Managed 24X7 SOC service
- b) Log aggregation and ability to normalize logs across different platforms including the securing of logs
- c) Analyzing of log data
- d) Correlation of log data
- e) Archiving of log data
- f) Threat Alerts
- g) Contextualization and Autonomous Response to threats
- h) Automated compliance and customization of reports
- i) Alerts for abnormal events occurring on the network
- j) Use of artificial intelligence to eliminate network threats
- k) a dashboard view for a simplified overview of real-time threats that is simple and intuitive.
- l) Machine learning (ML) capabilities.
- m) Artificial Intelligence (AI) capabilities.

- n) The system must support a complete and scalable architecture through the licensing of additional components required to integrate with the various digital environments, including on-premises, cloud and hybrids.
- o) Extensive Reporting

3.2 Managed Detection and Response (MDR) Solution (EPP+EDR)

The end point Monitoring, Detection and Response capability must meet the following minimum criteria:

- a) Ability to provide real-time monitoring, detection, alerting and historic statistics
- b) Support for agent monitoring
- c) Low footprint and impact on services monitored
- d) Ability to provide log storage for audit and forensic purposes for the duration of the contract
- e) Log retention mechanism/technique to automatically move and purge the logs in line with the GKM information retention policy
- f) Ability to archive data and export archived data in a usable format
- g) Monitor Microsoft Windows endpoints (workstations) for performance, activity, system health and configuration changes
- h) Monitor Microsoft Active Directory for performance, activity, system health and configuration changes
- i) Monitor Microsoft Exchange for performance, activity, system health and configuration changes
- j) Monitor Anti-Virus system for activity, system health and configuration changes
- k) Ability to send alerts via email and SMS with the ability to customize the message format and text
- l) Ability to send detailed warnings for potential or imminent issues / threats
- m) Ability to send alerts for all detected critical events
- n) Ability to integrate into the call logging system for tracking of all alerts or incidents
- o) Ability to escalate incidents / warnings / issues
- p) Ability to provide conditional alerting. e.g., when a predetermined threshold or time period is reached, an alert is sent to the next recipient on the escalation list
- q) Patching and upgrades to be performed whenever they become available.
- r) Extensive Reporting

3.3 Data Leakage Prevention (DLP)

The DLP capability must meet the following minimum criteria:

- a) A data Loss and Discovery solution covering:

- Endpoint
 - HTTP's and FTP
 - Email
 - Integration with SIEM
 - Analytics
 - Perform Data Recovery
- b) Responsible for building, managing, and operating the solution, i.e., Implementation, data classification, building policies, and handling other operational activities – policy fine-tuning to mitigate new and emerging threats.
 - c) Assign support personnel for this project with solid experience in building and implementing DLP solutions
 - d) Perform Configuration of Policies: Provide assistance to configure the tool with required rules.
 - e) Support for application version/software infrastructure.
 - f) Evaluate the incidents, escalations, and responses exclusion of the authorized list in data protection policies based on the responses, feedback and management directives.
 - g) Evaluate false positives and false negatives; fine-tune the data protection policies to correct the errors.
 - h) Configure relevant reports as required by GKM.
 - i) Support the solution, including future upgrades of all components of the solution, without any exception for the project duration, which is 1 year.
 - j) Provide the details of the architecture of the proposed solution containing complete details of specifications of components of the proposed solution.
 - k) The proposed solution shall have extensive Reporting, dashboards, and auditing capabilities.
 - l) The Solution must safeguard GKM employees and stakeholders' privacy – balancing the needs of corporate data protection and employee privacy.
 - m) Visibility and control over data including a) Encrypted data; b) Image files etc.
 - n) Manage all DLP security products (e.g., software, appliances) from one administration console, even encryption of files and folders
 - o) The Solution should provide the capability to apply protection policy rules on endpoint devices even if the user is not connected to the GKM network.
 - p) The Solution must be able to detect sensitive data leakage going through cloud- based solutions (OneDrive etc.).
 - q) The Solution must be able to enforce policies to detect data leaks even in image files through Optical Character Recognition technology. In addition, it must standard support file formats such as but not limited to jpeg, png, scanned pdf.
 - r) The Solution must enforce policies to detect low and slow data leaks over a period of time (hours).

- s) The Solution must be implemented on premise and provide data protection for both Cloud and on-premises environment.
- t) The Solution must be able to integrate with the GKM Security Information and Event Management system.
- u) Capture logs of Data Exchange activity on GKM's Information Asset done through any medium like email, internet upload, USB transfer etc. At the same time, intelligently co-relate and analyses these logs with the previous user-based attempts/ incidents and trigger alerts.
- v) Role-based administration for internal administrative tasks and monitoring and enforcement.
- w) As far as it is technically feasible, ensure no unwarranted, illegal or fraudulent misuse of data shared by GKM.
- x) The DLP solution must have the ability to identify and protect:
 - data-in-motion (travelling across the network)
 - data-in-use (being used at the endpoint); and
 - data-at-rest (sitting idle in storage).
- y) The solution should provide built-in/predefined policies/templates for GKM and its environment, and can be accessed, used, and applied simultaneously.
- z) Provide intuitive and easy installation, setup, deployment, the population of policies, and ongoing support.
- aa) The Solution should provide content, context, and destination awareness, allowing administrators to manage who can send what information where and how.
- bb) The proposed DLP solution should have central management console and incident repository. GKM administrators shall use the console to define, deploy and enforce data loss policies, respond to the incidents, analyze, and report violations, and perform system administration. (Proper training to GKM ICT Staff on how to conduct this).
- cc) The proposed DLP solution should block, quarantine, or relocate the channel containing sensitive data.
- dd) The proposed solution should be able to remediate violations of data at rest policies by encrypting or erasing restricted data once it has been identified.

3.4 Vulnerability Assessment (VA) and Penetration Testing (PEN)

- a) The proposed solution should have automated asset discovery capabilities for the following assets.
 - Servers
 - PC's and Laptops
 - Network devices
- b) The solution should provide an ability to scan the network for vulnerabilities using:

- **Authenticated Scan:** authenticated scan is a vulnerability scan that is performed by an authenticated user - a user with login credentials with capabilities to run deep scanning
 - **Non-authenticated Scan:** 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.
- c) Vulnerability scanning on all Network Devices including Cloud implementation.
 - d) Uncover all application vulnerabilities but not limited to, cross-site scripting, command injections, code injections, misconfigurations, insecure cookies and flaws.
 - e) The solution must have the functionality to search for vulnerabilities and assign a risk score continuously.
 - f) Deliver alerting capabilities for when a scan reveals new security risks and vulnerabilities on the GKM's ICT infrastructure.
 - g) Provide capabilities to identify false positives vs real vulnerabilities.
 - h) Provide a solution that has capabilities to monitor vulnerabilities introduced by applications installed on GKM's infrastructure components such as laptop computers.
 - i) Provide allowance for flexible vulnerability assessment schedules.
 - j) The solution must be able to provide a holistic view of the environment where the GKM ICT team is able to drill down at any stage to explore:
 - Assets
 - Vulnerabilities
 - Exploits
 - Policies
 - k) The vulnerability management solution should also be setup to allow NHFC Personnel to run ad- hoc vulnerability scans on the environment, to scan new devices, web applications and systems.
 - l) Provide penetration testing services for NHFC infrastructure that include:
 - Internal Network (LAN)
 - Externally facing Public IP addresses and systems
 - GKM Websites, both Cloud hosted and internally hosted.
 - m) The services must support standard and customized reporting functionality for penetration testing related reports.
 - n) Provision of reporting capabilities with a dashboard that highlights the risk scores (high, medium-high, medium-low, and low) for all vulnerabilities but also provide GKM with an overall risk score based on the volume and severity of vulnerabilities found within the network, applications, and ICT assets and devices.
 - o) Reporting function of the solution must have the following reports but not limited to:

- Automated and comprehensive devices discovery report;
 - Scheduled comprehensive vulnerability scanning reports; and
 - Dashboards reports.
- p) The Bidder must be proficient in information security with an excellent knowledge and practice of ICT Vulnerability Assessment and Penetration testing.
 - q) The Bidder must provide advisory services on the remediation of vulnerabilities strategies.
 - r) The bidder must supply, install, customize, integrate, test and troubleshoot the tools in scope for vulnerability and penetration testing services.
 - s) The Bidder should supply, install, customize, integrate, test and troubleshoot the tools in scope for vulnerability assessment and penetration testing services.
 - t) The Vulnerability Assessment solution must be able to integrate with SIEM and ticketing system.
 - u) Keep an audit trail of all vulnerabilities and applied remediation steps.

3.5 ICT Security Support and Maintenance

GKM does not have capacity to operate and manage the ICT Security Services and expects the service provider to provide all these services from its Security Operation Center to provide assurance for the reliability of the services rendered.

- a) The Service Provider will be expected to provide monitoring and management of all the systems' reliability for the protection of GKM's data and Information.
- b) The Service provider is expected to manage the accesses to all these systems and tools to be deployed on the GKM environment (Cloud or Local) in order to take overall accountability and responsibility of security service to the GKM.
- c) The service provider must be prepared to integrate their systems to the GKM future IT Service Management system for security incidents or breaches to be logged for response and monitoring.
- d) The service provider is expected to report on the security posture of the GKM' ICT environment and make recommendations for improvement of the security.
- e) The service provider will be expected to promptly alert the GKM ICT team and the relevant management about any security incident and provide guidance on the steps to be followed to limit the exposure.
- f) The service provider will be responsible and accountable to drive the security incidents steps and provide reports to the GKM ICT team.
- g) The service provider will be expected to immediately isolate any device that seems to be having uncommon or untrusted behaviors until it has been cleared, deemed safe and reliable by the ICT Management and the business.

- h) The service provider will be responsible to provide regular reports to the ICT Manager and discuss all the service, issues experienced and recommended actions on monthly basis. The Service Provider's report must
- i) The Service Provider must operate a 24x7x365 fully manned Service Desk. This will be required for monitoring, call logging and call assignments.
- k) A Standard Operating Procedure (SOP) must be included in your approach and methodology.

3.6 SECURITY TRAINING AND KNOWLEDGE TRANSFER

- a) The Service Provider is expected to provide Product Training which does not have to be certified.
- b) Provide technical knowledge transfer to ICT staff.

4. MANDATORY REQUIREMENTS

Bidders are required to meet all the mandatory requirements. Proof of product functionality is to be provided for every mandatory requirement.

Failure to provide the relevant documentation and/or certification will result in disqualification.

Bidders are advised to include any hardware or additional resources required for the solution in their response.

- a) The service provider shall provide reference(s) to demonstrate their expertise, experience, and capacity in similar implementations. Signed reference letters on official letterheads from at least 3 clients confirming that the supplier has implemented and supported the tools mentioned.
- b) The service provider shall provide proof that they are certified to implement and support the software tools above. OEM Certificate(s) or letter(s) of authorization from the OEM(s) which clearly details which products/activities the supplier is authorized and qualified to undertake must accompany the proposal.
- c) The service provider shall provide proof that they are ISO9001 and ISO27001 certified. ISO Certificates must accompany the proposal.
- d) The service provider shall provide 4 CV's one of which must at least have 3 of the following resource certifications, CISM, CISSP, CRISC. The other CV's must have OEM Product/Solution Certifications.
- e) Refer to **Annexure A** for the Technical document that **MUST** accompany your response. Failure to do so will be interpreted as "non-Responsive".

- f) The contracted service provider shall submit a detailed Project Plan with timelines.

5. PROJECT MANAGEMENT

- The contracted service provider shall submit a detailed Project Plan with timelines. The Project Plan must cover the entire project and control project execution throughout the various project phases. The Plan must detail the activities necessary to successfully complete the project and shall refer to the other plans developed under the project.

6. EVALUATION CRITERIA

FUNCTIONALITY (100)

About functionality the following criteria will be applicable and the maximum score of each criterion are indicated in brackets. Bidder must score minimum of 70 point to qualify for the next evaluation.

SUPPLY, DELIVER AND MAINTAIN A FULLY INTEGRATED ICT CYBER SECURITY SOLUTION FOR 36 MONTHS				
Technical Evaluation:			Weight	Total
1.	Provide proof of ISO9001 and ISO27001 Certification	Proof of both ISO9001 and ISO27001	20	20
		No Proof provided	0	
2.	Provide proof of OEM Certificate or OEM partnership Letters	Provided OEM Certificate or Partnership Letter	20	20
		No OEM / Partnership	0	
3.	Relevant experience and qualifications of project Manager	Project Manager with certificate in Project Management and 3 or more years of experience reflecting on CV.	15	15
		No relevant experience and qualifications of project personnel	0	
	Relevant experience and qualifications of senior security Analyst	Senior Security Analyst with a certificate in network security and 3 or more years of experience reflecting on CV.	15	15
		No relevant experience and qualifications of Senior Security Analyst	0	

4.	COMPANY EXPERIENCE	3 Similar IT projects with 3 written references corresponding with orders or appointment letters signed.	30	30
		2 Similar IT projects with 2 written references corresponding with orders or appointment letters signed.	20	
		1 Similar IT projects with 1 written reference corresponding with orders or appointment letters signed.	10	
		No IT projects with no written reference corresponding with orders or appointment letters signed.	0	
	Total			100
	Minimum			70

MBD1

PART A

INVITATION TO BID

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE GREATER KOKSTAD MUNICIPALITY					
BID NUMBER:	GKM 08-23/24	CLOSING DATE:	11 JANUARY 2024	CLOSING TIME:	12H00
DESCRIPTION	SUPPLY, DELIVER AND MAINTAIN A FULLY INTEGRATED ICT CYBER SECURITY SOLUTION FOR 36 MONTHS				
THE SUCCESSFUL BIDDER WILL BE REQUIRED TO FILL IN AND SIGN A WRITTEN CONTRACT FORM (MBD7).					
BID RESPONSE DOCUMENTS MAY BE DEPOSITED IN THE BID BOX SITUATED AT (STREET ADDRESS					
75 HOPE STREET KOKSTAD 4700					
SUPPLIER INFORMATION					
NAME OF BIDDER					
POSTAL ADDRESS					
STREET ADDRESS					
TELEPHONE NUMBER	CODE		NUMBER		
CELLPHONE NUMBER					
FACSIMILE NUMBER	CODE		NUMBER		
E-MAIL ADDRESS					
VAT REGISTRATION NUMBER					
TAX COMPLIANCE STATUS	TCS PIN:		OR	CSD No:	
B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE [TICK APPLICABLE BOX]	<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		
CAPACITY UNDER WHICH THIS BID IS SIGNED					
BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO:			TECHNICAL INFORMATION MAY BE DIRECTED TO:		
DEPARTMENT	Budget and Treasury Office		CONTACT PERSON	Yaw Owusu	
CONTACT PERSON	ANDISWA MAHLAKA		TELEPHONE NUMBER	039 797 6600	
TELEPHONE NUMBER	039 797 6644		FACSIMILE NUMBER	039 727 3676	
FACSIMILE NUMBER	039 727 3676		E-MAIL ADDRESS	Yaw.Owusu@kokstad.gov.za	

E-MAIL ADDRESS	Andiswa.mahlaka@Kokstad.gov.za	
----------------	--------------------------------	--

MBD1

PART B TERMS AND CONDITIONS FOR BIDDING

1. BID SUBMISSION:

- 1.1. BIDS MUST BE DELIVERED BY THE STIPULATED TIME TO THE CORRECT ADDRESS. LATE BIDS WILL NOT BE ACCEPTED FOR CONSIDERATION.
- 1.2. **ALL BIDS MUST BE SUBMITTED ON THE OFFICIAL FORMS PROVIDED–(NOT TO BE RE-TYPED)**
- 1.3. THIS BID IS SUBJECT TO THE PREFERENTIAL PROCUREMENT POLICY FRAMEWORK ACT AND THE PREFERENTIAL PROCUREMENT REGULATIONS, 2017, 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 WILL RENDER THE BID INVALID.

NO BIDS WILL BE CONSIDERED FROM PERSONS IN THE SERVICE OF THE STATE.

SIGNATURE OF BIDDER:

.....

CAPACITY UNDER WHICH THIS BID IS SIGNED:

.....

DATE:

.....

**PRICING SCHEDULE – FIRM PRICES
(PURCHASES)**

MBD 3.1

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

MBD

3.1

Service Requirement	Description	Cost Inc VAT
Software and Licensing	Security Information and Event Management	
	Managed Detection & Response	
	Data Leakage Prevention	
	Vulnerability Testing	
Penetration Testing	Penetration Testing	
Installation and configuration	All Solutions	
Managed SOC	All Solutions	
Project Management	A comprehensive project plan includes milestone reporting and a RAIL.	
Support and Maintenance (36 Months)	Proactive maintenance and reporting for a period, including monthly SLA meetings – All Solutions	
<div style="border: 1px solid black; border-radius: 15px; padding: 20px; text-align: center;"> <p style="font-size: 24px; color: gray; margin: 0;">COMPANY STAMP</p> <p style="font-weight: bold; margin-top: 20px;">COMPANY STAMP</p> </div>		
	SUB-TOTAL	
	VAT (15%)	
	TOTAL	

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

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

CONDITIONS OF TENDER

- Price(s) quoted must be valid for at least thirty (30) days from date of offer for evaluation purposes.
- Price(s) quoted must be firm and include VAT (**Non-compliance** with the Value Added Tax Act, 1991; i.e. In terms of this Act **it is mandatory** for any business **to register for VAT** if the income earned in any consecutive twelve (12) month period exceeds or is likely to exceed R 1 million.
NB: Bidder/s failing to comply with this provision of the Value Added Tax Act, 1991 **WILL NOT BE CONSIDERED**, therefore rejected)
- Tenderers original valid tax clearance certificate must be attached.
- Tender original or certified B-BBEE Certificate must be attached to the document
- Tender documents signed by a person who does not have authority to sign will be disqualified.
- Tenderers who did not complete the compulsory questionnaire, who abuse the employer's supply chain management system will not be conceded
- Non-collusion affidavit to be executed by bidder and submitted with the bid.

ANNEXURE C

MBD 4

DECLARATION OF INTEREST

1. No bid will be accepted from persons in the service of the state¹.
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 favoritism, 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 authorized 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, shareholder²):.....
- 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.
.....

¹MSCM Regulations: "in the service of the state" means to be –

- (a) a member of –
 - (i) any municipal council;
 - (ii) any provincial legislature; or
 - (iii) the national Assembly or the national Council of provinces;
- (b) a member of the board of directors of any municipal entity;
- (c) an official of any municipality or municipal entity;
- (d) an employee of any national or provincial department, national or provincial public entity or constitutional institution within the meaning of the Public Finance Management Act, 1999 (Act No.1 of 1999);
- (e) a member of the accounting authority of any national or provincial public entity; or
- (f) an employee of Parliament or a provincial legislature.

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

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

3.9.1 If yes, furnish particulars.....

.....

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

3.10.1 If yes, furnish particulars.

.....

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

3.11.1 If yes, furnish particulars

.....

.....

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

3.12.1 If yes, furnish particulars.

.....

.....

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

3.13.1 If yes, furnish particulars.
.....
.....

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

3.14.1 If yes, furnish particulars:
.....
.....

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

Full Name	Identity Number	State Employee Number

.....
Signature

.....
Date

.....
Capacity

.....
Name of Bidder

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

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

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

1. GENERAL CONDITIONS

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

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

1.2 To be completed by the organ of state

(delete whichever is not applicable for this tender).

- a) The applicable preference point system for this tender is the **90/10** preference point system.
- b) The applicable preference point system for this tender is the **80/20** 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.

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

- (a) Price; and
- (b) Specific Goals.

1.4 To be completed by the organ of state:

The maximum points for this tender are allocated as follows:

	POINTS
PRICE	80
SPECIFIC GOALS	20
Total points for Price and SPECIFIC GOALS	100

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

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

2. DEFINITIONS

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

3. FORMULAE FOR PROCUREMENT OF GOODS AND SERVICES

6.1. 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:

$$\begin{array}{ccc} \mathbf{80/20} & \mathbf{or} & \mathbf{90/10} \\ \\ \mathbf{Ps = 80 \left(1 - \frac{Pt - Pmin}{Pmin} \right)} & \mathbf{or} & \mathbf{Ps = 90 \left(1 - \frac{Pt - Pmin}{Pmin} \right)} \end{array}$$

Where

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

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

6.2.1. POINTS AWARDED FOR PRICE

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

$$\begin{array}{ccc} \mathbf{80/20} & \mathbf{or} & \mathbf{90/10} \\ \\ \mathbf{Ps = 80 \left(1 + \frac{Pt - P_{max}}{P_{max}} \right)} & \mathbf{or} & \mathbf{Ps = 90 \left(1 + \frac{Pt - P_{max}}{P_{max}} \right)} \end{array}$$

Where

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

7. POINTS AWARDED FOR SPECIFIC GOALS

- 7.1. 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:
- 7.2. In cases where organs of state intend to use Regulation 3(2) of the Regulations, which states that, if it is unclear whether the 80/20 or 90/10 preference point system applies, an organ of state must, in the tender documents, stipulate in the case of—
- (a) an invitation for tender for income-generating contracts, that either the 80/20 or 90/10 preference point system will apply and that the highest acceptable tender will be used to determine the applicable preference point system; or
 - (b) any other invitation for tender, that either the 80/20 or 90/10 preference point system will apply and that the lowest acceptable tender will be used to determine the applicable preference point system,
- then the organ of state must indicate the points allocated for specific goals for both the 90/10 and 80/20 preference point system.

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

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

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

The specific goals allocated points in terms of this tender	Number of points allocated (80/20 system) (To be completed by the organ of state)	Number of points claimed (80/20 system) (To be completed by the tenderer)
GOALS 1 - OWNERSHIP	MAX POINTS =14	
Business owned more than 50% by black person	5	
Business owned less than 50% by black person	2	
Business owned more than 50% by women black	4	
Business owned less than 50% by women black	2	
Business owned more than 50% by black youth	3	
Business owned more than 50% by disabled person	2	
GOAL 2 -RDP	MAX POINTS =6	
Business falls under the SMME Category- QSE/EME	2	
Promotion of business located within Harry Gwala district	2	
Promotion of business located within KZN province	2	
Promotion of business located in South Africa outside KZN province	1	

DECLARATION WITH REGARD TO COMPANY/FIRM

7.3. Name of company/firm.....

7.4. Company registration number:

7.5. TYPE OF COMPANY/ FIRM

- ☐ Partnership/Joint Venture / Consortium
- ☐ One-person business/sole propriety
- ☐ Close corporation
- ☐ Public Company

- ☐ Personal Liability Company
- ☐ (Pty) Limited
- ☐ Non-Profit Company
- ☐ State Owned Company

[TICK APPLICABLE BOX]

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

- i) The information furnished is true and correct;
- ii) The preference points claimed are in accordance with the General Conditions as indicated in paragraph 1 of this form;
- iii) In the event of a contract being awarded as a result of points claimed as shown in paragraphs 1.4 and 4.2, the contractor may be required to furnish documentary proof to the satisfaction of the organ of state that the claims are correct;
- iv) If the specific goals have been claimed or obtained on a fraudulent basis or any of the conditions of contract have not been fulfilled, the organ of state may, in addition to any other remedy it may have –
 - (a) disqualify the person from the tendering process;
 - (b) recover costs, losses or damages it has incurred or suffered as a result of that person's conduct;
 - (c) cancel the contract and claim any damages which it has suffered as a result of having to make less favourable arrangements due to such cancellation;
 - (d) recommend that the tenderer or contractor, its shareholders and directors, or only the shareholders and directors who acted on a fraudulent basis, be restricted from obtaining business from any organ of state for a period not exceeding 10 years, after the *audi alteram partem* (hear the other side) rule has been applied; and
 - (e) forward the matter for criminal prosecution, if deemed necessary.

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

SURNAME AND NAME:

DATE:

ADDRESS:
.....
.....
.....

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	<p>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?</p> <p>(Companies or persons who are listed on this Database were informed in writing of this restriction by the Accounting Officer/Authority of the institution that imposed the restriction after the <i>audi alteram partem</i> rule was applied).</p> <p>The Database of Restricted Suppliers now resides on the National Treasury's website(www.treasury.gov.za) and can be accessed by clicking on its link at the bottom of the home page.</p>	Yes <input type="checkbox"/>	No <input type="checkbox"/>
4.1.1	If so, furnish particulars:		
4.2	<p>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)?</p> <p>The Register for Tender Defaulters can be accessed on the National Treasury's website (www.treasury.gov.za) by clicking on its link at the bottom of the home page.</p>	Yes <input type="checkbox"/>	No <input type="checkbox"/>

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	Does the bidder or any of its directors owe any municipal rates and taxes or municipal charges to the municipality / municipal entity, or to any other municipality / municipal entity, that is in arrears for more than three months?	Yes <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 bids¹ invited.
- 2 Section 4 (1) (b) (iii) of the Competition Act No. 89 of 1998, as amended, prohibits an agreement between, or concerted practice by, firms, or a decision by an association of firms, if it is between parties in a horizontal relationship and if it involves collusive bidding (or bid rigging).² Collusive bidding is a *pe se* prohibition meaning that it cannot be justified under any grounds.
- 3 Municipal Supply Regulation 38 (1) prescribes that a supply chain management policy must provide measures for the combating of abuse of the supply chain management system, and must enable the accounting officer, among others, to:
 - a. take all reasonable steps to prevent such abuse;
 - b. reject the bid of any bidder if that bidder or any of its directors has abused the supply chain management system of the municipality or municipal entity or has committed any improper conduct in relation to such system; and
 - c. cancel a contract awarded to a person if the person committed any corrupt or fraudulent act during the bidding process or the execution of the contract.
- 4 This MBD serves as a certificate of declaration that would be used by institutions to ensure that, when bids are considered, reasonable steps are taken to prevent any form of bid-rigging.
- 5 In order to give effect to the above, the attached Certificate of Bid Determination (MBD 9) must be completed and submitted with the bid:

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

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

CERTIFICATE OF INDEPENDENT BID DETERMINATION

I, the undersigned, in submitting the accompanying bid:

(Bid Number and Description)

in response to the invitation for the bid made by:

(Name of Municipality / Municipal Entity)

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

I certify, on behalf of: _____ 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 consortium³ 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.

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

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

.....
Signature

.....
Date

.....
Position

.....
Name of Bidder

INSTRUCTIONS TO BIDDERS

PUBLICATION REFERENCE:

In submitting their bid, bidders must respect all instructions, forms, Terms of reference, contract provisions and specifications contained in this bid dossier. Failure to submit a bid containing all the required information and documentation within the deadline specified will lead to the rejection of the bid.

SUBMISSION REQUIREMENTS AND SELECTION CRITERIA

Bidders are required to submit the following documents:

- Price(s) quoted must be firm and must be inclusive of VAT
- Copy of CSD (Central Supplier Database) summary report
- Copy of company registration documents (compulsory)
- For Joint Venture Agreements, attach the CK's of each of the joint venture members (if applicable)
- Certified ID(s) copies of company director(s)
- Copy of current municipal account for all Director/s and Company (not owing more than 3 months) or copy of lease agreement from the relevant authority if the director/s or company is leasing. If the business is operated from the residence of one of the Director/s, an original affidavit, certified, must be submitted stating the address of the premises. For any other arrangement that is not covered above, director/s must submit an original affidavit, certified clarifying the arrangement. All affidavits must be original affidavits, certified and must be from the SAPS. Affidavits must be signed by the company director/s.
- Printed copy of SARS Tax Pin for further verification.
- Completed and signed Municipal Bidding Document attached to the tender document.

1. Services to be provided

These services required by the Contracting Authority are described in these Terms of Reference/Specification.

2. Participating and sub-contracting

- 2.1 Participation in this bid is open to everyone.**
- 2.2 Bids should be submitted by the same service provider or consortium, which has submitted the proposal based on the above. No change whatsoever in the identity or composition of the bidder is permitted;**
- 2.3 Short-listed service provider or consortia are allowed to form alliances with any other firms or to sub-contract to each other for the purpose of this contract;**
- 2.4 Sub-contracting will be allowed, only in so far as it was stated in the initial bid.**
- 2.5 Duplication of bid document is prohibited.**

3. Contents of Bids

Bid must comprise of a financial offer must be submitted with the bid.

4. Financial offer

The financial offer must state the bidder's price in South African Rand for providing the services according to its Technical offer and the bidders offer must be inclusive of vat and any other relevant taxes.

The same person, who signed the corresponding must sign this document.

5. Submission of samples

Where necessary, Prospective service providers may be requested to supply samples to the Municipality to enable verification of SABS and SANS specifications on samples provided and compliance with Local Content Criteria. These are to be supplied at the request of the Municipality prior to the evaluation of compliant bids. **Samples supplied will serve as standard quality.**

6. Variant solutions

Any variant solutions will not be taken into consideration.

Period during which Bid are binding

Bidders are bound by their bids for 120 days after the deadline for the submission of bids. In exceptional cases, before the period of validity expires, the Contracting Authority may ask bidders to extend the period for a specific number of days, which may not exceed 60.

The successful bidder must maintain its bid for a further 60 days from the date of notification that its bid has been selected for the contract.

7. Additional information before the deadline for submission of bidders

The bid dossier should be clear enough to avoid the Contracting Authority from having request additional information during the procedure. If the Contracting Authority, either on own initiative or in response to the request of a short-listed candidate, provides additional information on the bid dossier, such information will be sent in writing to all other bidders at the same time.

Bidders may submit questions in writing to the following address up to 10 days before the deadlines for submission of bids, specifying the **publication reference** and the **contract title**:

Attention: Andiswa Mahlaka
Greater Kokstad Municipality
75 Hope Street
P.O. Box 8
KOKSTAD
4700
Email: Andiswa.mahlaka@kokstad.gov.za

Any prospective bidders seeking to arrange individual meetings with either the Contracting Authority during the bid period may be excluded from the bid procedure.

Any clarification of the bid dossier will be communicated simultaneously in writing to all bidders at the latest 7 calendar days before the deadline for submission of bids. No further clarifications will be given after this date.

Visit by individual prospective bidder during the bid period are not permitted other than the site visit for good reasons.

8. Submission of Bids

Bids must be submitted in English such that they are received before the deadline specified by in the letter of invitation to bid.

Any infringement of these rules (e.g. unsealed envelopes) is to be considered a breach of the rules, and will lead to rejection of the bid.

The envelope should carry the following information:

- a) The address for submission of bid indicated above;);
- b) The words "Not to be opened before the bid opening sessions";
- c) The pages of the Technical and Financial offers must be numbered.

9. Alterations or Withdrawal of Bids

9.1 Bidders may alter or withdraw bids by written notification prior to the deadline for submission of bids. No bid may be altered after this deadline.

9.2 Any such notification of alteration or withdrawal shall be prepared and submitted in accordance with clause 8. The envelope must be marked "Alteration" or "Withdrawal" as appropriate.

10. Costs for preparing Bids

No costs incurred by the bidder in preparing and submitting the bid shall be reimbursable. All such costs shall be borne by the bidder. In particular, if proposed key members were interviewed, all costs shall be borne by the bidder.

11. Ownership of Bids

The Contracting Authority retains ownership in all bid received (this excludes intellectual property for all but the successful bidder) under this tendering procedure. Consequently, bidders have no right to have their bids returned to them.

12. Confidentiality

The entire evaluation procedure, from the drawing up of the shortlist to the signature of the contract, is confidential. The Evaluation / Adjudication Committee's decisions are collective and its deliberations are held in closed session. The members of the Evaluation / Adjudication Committee are bound to secrecy.

The evaluation reports and written records are for official use only and may be communicated to neither the bidders nor to any party other than the Contracting Authority.

13. Ethics clauses / Corruptive practices

- a) Any attempt by a bidder to obtain confidential information, enter into unlawful agreements with competitors or influence the Evaluation / Adjudication Committee or the Contracting Authority during the process of examining, clarifying, evaluating, comparing and adjudication bid will lead to the rejection of its bid and may result in administrative penalties.
- b) The bidder must not be affected by any potential conflict of interest.
- c) The Greater Kokstad Municipality reserves the right to suspend or cancel funding to this project if corrupt practices of any kind are discovered at any stage of the award process or during the implementation of a contract, if the Contracting Authority fails to take all appropriate measures to remedy the situation. For the purposes of this provision, "corrupt practices" are the offer of a bribe, gift, gratuity or commission to any person as an inducement or reward for performing or refraining from any act relating to the award of a contract or implementation of a contract already concluded with the Contracting Authority.
- d) Bids will be rejected, or contracts terminated if it emerges that the award or execution of a contract has given rise to unusual commercial expenses. Such unusual commercial expenses are commissions not mentioned in the main contract or not stemming from a properly concluded contract referring to the main contract, commissions not paid in return for any actual and legitimate service, commissions paid to a payee who is not clearly identified or commissions paid to a company which has every appearance of being a front company.

Failure to comply with one or more of the ethics clauses may result in the exclusion of the bidder or contractor from other Community contracts and in penalties.

14. Documentary evidence required from the successful Bidder

The successful bidder will be informed in writing that its bid has been accepted (notification of award). Before the Contracting Authority signs the contract with a Successful bidder, a successful bidder may be requested to provide additional information as deemed necessary by the Contracting Authority.

This evidence or these documents must carry a date, which cannot be more than 180 days in relation to the deadline for the submission of the bidder. In addition, a sworn statement shall be furnished stating that the situations described in these documents have not changed since then.

If the successful bidder fails to provide these documents or is found to have provided false information, the award will be considered null and void. In such a case, the Contracting Authority may award the bid to another bidder or cancel the bid procedure.

15. Signature of contract(s)

Within 7 days of receipt of the contract already signed by the Contracting Authority, the selected bidder shall sign and date the contract and return it to the Contracting Authority.

Failure of the selected bidder to comply with this requirement may constitute grounds for the annulment of the decision to award the contract. In such a case, the Contracting Authority may award the bid to another bidder or cancel the bid procedure.

The other candidates will be informed that their bids were not accepted, by means of a standard letter.

16. Cancellation of the Bids procedure

In the event of cancellation of the bid procedure, bidders will be notified of the cancellation by the Contracting Authority. If the bid procedure is cancelled before the envelopes of any bid has been opened, the unopened and sealed envelopes will be returned to the bidders.

Cancellation may occur when:

- The bid procedure has been unsuccessful, i.e., no qualitatively or financially worthwhile bid has been received or there is no response at all;
- The economic or technical data of the project have been fundamentally altered;
- Exceptional circumstances or *force majeure* render normal performance of the contract impossible;
- All technically compliant bids exceed the financial resources available;
- There have been irregularities in the procedure, in particular where these have prevented fair competition.

In no event shall the Contracting Authority be liable for any damages whatsoever including, without limitation, damages for loss of profits, in any way connected with the cancellation of a bid even if the Contracting Authority has been advised of the possibility of damages.

The publication of a procurement notice does not commit the Contracting Authority to implement the programme or project announced.

17. Intentions to award

Bidders will be informed of the Municipality's intention to award (notification of the intention to award). A notice will be sent to bidders or will be uploaded on the Greater Kokstad Municipality Website.

THE NATIONAL TREASURY
Republic of South Africa



GOVERNMENT PROCUREMENT:
GENERAL CONDITIONS OF CONTRACT

July 2010

TABLE OF CLAUSES

1. Definitions

2. Application
3. General
4. Standards
5. Use of contract documents and information inspection
6. Patent Rights
7. Performance security
8. Inspections, tests and analyses
9. Packing
10. Delivery and documents
11. Insurance
12. Transportation
13. Incidental Services
14. Spare parts
15. Warranty
16. Payment
17. Prices
18. Variation orders
19. Assignment
20. Subcontracts
21. Delays in the supplier's performance
22. Penalties
23. Termination for default
24. Anti-dumping and countervailing duties and rights
25. Force Majeure
26. Termination for insolvency
27. Settlement of Disputes
28. Limitation of Liability
29. Governing language
30. Applicable law
31. Notices
32. Taxes and duties
33. Transfer of contracts
34. Amendments of contracts
35. Prohibition of restrictive practices

General Conditions of Contract

Definitions

1. The following terms shall be interpreted as indicated:

- 1.1 "Closing time" means the date and hour specified in the bidding documents for the receipt of bids.
- 1.2 "Contract" means the written agreement entered into between the purchaser and the supplier, as recorded in the contract form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.
- 1.3 "Contract price" means the price payable to the supplier under the contract for the full and proper performance of his contractual obligations.
- 1.4 "Corrupt practice" means the offering, giving, receiving, or soliciting of any thing of value to influence the action of a public official in the procurement process or in contract execution.
- 1.5 "Countervailing duties" are imposed in cases where an enterprise abroad is subsidized by its government and encouraged to market its products internationally.
- 1.6 "Country of origin" means the place where the goods were mined, grown or produced or from which the services are supplied. Goods are produced when, through manufacturing, processing or substantial and major assembly of components, a commercially recognized new product results that is substantially different in basic characteristics or in purpose or utility from its components.
- 1.7 "Day" means calendar day.
- 1.8 "Delivery" means delivery in compliance of the conditions of the contract or order.
- 1.9 "Delivery ex stock" means immediate delivery directly from stock actually on hand.
- 1.10 "Delivery into consignees store or to his site" means delivered and unloaded in the specified store or depot or on the specified site in compliance with the conditions of the contract or order, the supplier bearing all risks and charges involved until the goods are so delivered and a valid receipt is obtained.
- 1.11 "Dumping" occurs when a private enterprise abroad market its goods on own initiative in the RSA at lower prices than that of the country of origin and which have the potential to harm the local industries in the RSA.

- 1.12 "Force majeure" means an event beyond the control of the supplier and not involving the supplier's fault or negligence and not foreseeable. Such events may include, but is not restricted to, acts of the purchaser in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.
- 1.13 "Fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of any bidder, and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the bidder of the benefits of free and open competition.
- 1.14 "GCC" means the General Conditions of Contract.
- 1.15 "Goods" means all of the equipment, machinery, and/or other materials that the supplier is required to supply to the purchaser under the contract.
- 1.16 "Imported content" means that portion of the bidding price represented by the cost of components, parts or materials which have been or are still to be imported (whether by the supplier or his subcontractors) and which costs are inclusive of the costs abroad, plus freight and other direct importation costs such as landing costs, dock dues, import duty, sales duty or other similar tax or duty at the South African place of entry as well as transportation and handling charges to the factory in the Republic where the goods covered by the bid will be manufactured.
- 1.17 "Local content" means that portion of the bidding price, which is not included in the imported content provided that local manufacture does take place.
- 1.18 "Manufacture" means the production of products in a factory using labour, materials, components and machinery and includes other related value-adding activities.
- 1.19 "Order" means an official written order issued for the supply of goods or works or the rendering of a service.
- 1.20 "Project site," where applicable, means the place indicated in bidding documents.
- 1.21 "Purchaser" means the organization purchasing the goods.
- 1.22 "Republic" means the Republic of South Africa.
- 1.23 "SCC" means the Special Conditions of Contract.
- 1.24 "Services" means those functional services ancillary to the

supply of the goods, such as transportation and any other incidental services, such as installation, commissioning, provision of technical assistance, training, catering, gardening, security, maintenance and other such obligations of the supplier covered under the contract.

1.25 "Supplier" means the successful bidder who is awarded the contract to maintain and administer the required and specified service(s) to the State.

1.26 "Tort" means in breach of contract.

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

1.28 "Written" or "in writing" means hand-written in ink or any form of electronic or mechanical writing.

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

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

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

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

3.2 Invitations to bid are usually published in locally distributed news media and on the municipality/municipal entity website.

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

**5. Use of
contract
documents
and
information
inspection**

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

Be extended only so far as may be necessary for the purpose of 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 the purposes of performing the contract.
- 5.3 Any documents 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 supplier's performance under the contract if so required by the purchaser
- 5.4 The supplier shall permit the purchaser to inspect the supplier's records relating to the performance of the supplier and to have them audited by auditors appointed by the purchaser, if so required by the purchaser.

- 6 Patent Rights** 6.1 The supplier shall indemnify the purchaser against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the goods or any part thereof by the purchaser.

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

7 Performance security

- 7.1 Within thirty (30) days of receipt of the notification of contract award, the successful bidder shall furnish to the purchaser the performance security of the amount specified in SCC.
- 7.2 The proceeds of the performance security shall be payable to the purchaser as compensation for any loss resulting from the supplier's failure to complete his obligations under the contract.
- 7.3 The performance security shall be denominated in the currency of the contract, or in a freely convertible currency acceptable to the purchaser and shall be in one of the following forms:
- (a) a bank guarantee or an irrevocable letter of credit issued by a reputable bank located in the purchaser's country or abroad, acceptable to the purchaser, in the form provided in the bidding documents or another form acceptable to the purchaser; or
 - (b) a cashier's or certified cheque.
- 7.4 The performance security will be discharged by the purchaser and returned to the supplier not later than thirty (30) days following the date of completion of the supplier's performance obligations under the contract, including any warranty obligations, unless otherwise specified.

8 Inspections , tests and analyses

- a. All pre-bidding testing will be for the account of the bidder.
- b. If it is a bid condition that goods to be produced or services to be rendered should at any stage be subject to inspections, tests and analyses, the bidder or contractor's premises shall be open, at all reasonable hours, for inspection by a representative of the purchaser or organization acting on behalf of the purchaser.
- c. 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.
- d. 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.
- e. 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.
- f. Goods and services which are referred to in clauses 8.2 and 8.3 and which do not comply with the contract requirements may be rejected.
- g. 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.
- h. The provisions of clauses 8.4 to 8.7 shall not prejudice the right of the purchaser to cancel the contract on account of a breach of the conditions thereof, or to act in terms of Clause 22 of GCC.

9 Packing

9.1 The supplier shall provide such packing of the goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in the contract. The packing shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packing, case size

weights shall take into consideration, where appropriate, the remoteness of the goods' final destination and the absence of heavy handling facilities at all points in transit.

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

10 Delivery and documents

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

11 Insurance

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

12 Transportation

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

13 Incidental Services

- a. The supplier may be required to provide any or all of the following services, including additional services, if any:
 - i. performance or supervision of on-site assembly and/or commissioning of the supplied goods;
 - ii. furnishing of tools required for assembly and/or maintenance of the supplied goods;
 - iii. furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied goods;
 - iv. 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
 - v. 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.
- b. Prices charged by the supplier for incidental services, if not included in the contract price for the goods, shall be agreed

upon in advance by the parties and shall not exceed the prevailing rates charged to other parties by the supplier for similar services.

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

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

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

15.2 This warranty shall remain valid for twelve (12) months after the goods, or any portion thereof as the case may be, have been delivered to and accepted at the final destination indicated in the contract, or for eighteen (18) months after the date of shipment from the port or place of loading in the source country, whichever period concludes earlier, unless specified otherwise.

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

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

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

16 **Payment** 16.1 The method and conditions of payment to be made to the supplier under this contract shall be specified.

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

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

16.4 Payment will be made in Rand unless otherwise stipulated.

17 Prices

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

18 Variation orders

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

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

20 Subcontracts

a. The supplier shall notify the purchaser in writing of all subcontracts awarded under this contracts if not already specified in the bid. Such notification, in the original bid or later, shall not relieve the supplier from any liability or obligation under the contract.

21 Delays in the supplier's performance

- 21.1 Delivery of the goods and performance of services shall be made by the supplier in accordance with the time schedule prescribed by the purchaser in the contract.
- 21.2 If at any time during performance of the contract, the supplier or its subcontractor(s) should encounter conditions impeding timely delivery of the goods and performance of services, the supplier shall promptly notify the purchaser in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the supplier's notice, the purchaser shall evaluate the situation and may at his discretion extend
- the supplier's time for performance, with or without the imposition of penalties, in which case the extension shall be ratified by the parties by amendment of contract.
- 21.3 The right is reserved to procure outside of the contract small quantities or to have minor essential services executed if an emergency arises, the supplier's point of supply is not situated at or near the place where the
- 21.4 goods are required, or the supplier's services are not readily available.
- 21.5 Except as provided under GCC Clause 25, a delay by the supplier in the performance of its delivery obligations shall render the supplier liable to the imposition of penalties, pursuant to GCC Clause 22, unless an extension of time is agreed upon pursuant to GCC Clause 22.2 without the application of penalties.
- 21.6 Upon any delay beyond the delivery period in the case of a goods contract, the purchaser shall, without cancelling the contract, be entitled to purchase goods of a similar quality and up to the same quantity in substitution of the goods not supplied in conformity with the contract and to return any goods delivered later at the supplier's expense and risk, or to cancel the contract and buy such goods as may be required to complete the contract and without prejudice to his other rights, be entitled to claim damages from the supplier.

- 22 Penalties** 22.1 Subject to GCC Clause 25, if the supplier fails to deliver any or all of the goods or to perform the services within the period(s) specified in the contract, the purchaser shall, without prejudice to its other remedies under the contract, deduct from the contract price, as a penalty, a sum calculated on the delivered price of the delayed goods or unperformed services using the current prime interest rate calculated for

each day of the delay until actual delivery or performance. The purchaser may also consider termination of the contract pursuant to GCC Clause 23.

23 Termination for default

- 23.1 The purchaser, without prejudice to any other remedy for breach of contract, by written notice of default sent to the supplier, may terminate this contract in whole or in part:
- (a) if the supplier fails to deliver any or all of the goods within the period(s) specified in the contract, or within any extension thereof granted by the purchaser pursuant to GCC Clause 21.2;
 - (b) if the supplier fails to perform any other obligation(s) under the contract; or
 - (c) if the supplier, in the judgement of the purchaser, has engaged in corrupt or fraudulent practices in competing for or in executing the contract.
- 23.2 In the event the purchaser terminates the contract in whole or in part, the purchaser may procure, upon such terms and in such manner, as it deems appropriate, goods, works or services similar to those undelivered, and the supplier shall be liable to the purchaser for any excess costs for such similar goods, works or services. However, the supplier shall continue performance of the contract to the extent not terminated.
- 23.3 Where the purchaser terminates the contract in whole or in part, the purchaser may decide to impose a restriction penalty on the supplier by prohibiting such supplier from doing business with the public sector for a period not exceeding 10 years.
- 23.4 If a purchaser intends imposing a restriction on a supplier or any person associated with the supplier, the supplier will be allowed a time period of not more than fourteen (14) days to provide reasons why the envisaged restriction should not be imposed. Should the supplier fail to respond within the stipulated fourteen (14) days the purchaser may regard the supplier as having no objection and proceed with the restriction.
- 23.5 Any restriction imposed on any person by the purchaser will, at the discretion of the purchaser, also be applicable to any other enterprise or any partner, manager, director or other person who wholly or partly exercises or exercised or may exercise control over the enterprise of the first-mentioned person, and with which enterprise or person the first-mentioned person, is or was in the opinion of the purchaser actively associated.
- 23.6 If a restriction is imposed, the purchaser must, within five (5) working days of such imposition, furnish the National Treasury, with the following information:
- (i) the name and address of the supplier and / or person restricted by the purchaser;
 - (ii) the date of commencement of the restriction
 - (iii) the period of restriction; and
 - (iv) the reasons for the restriction.

These details will be loaded in the National Treasury's central database of suppliers or persons prohibited from doing business with the public sector.

23.7

23.8 . If a court of law convicts a person of an offence as contemplated in

sections 12 or 13 of the Prevention and Combating of Corrupt Activities Act, No. 12 of 2004, the court may also rule that such person's name be endorsed on the Register for Tender Defaulters. When a person's name has been endorsed on the Register, the person will be prohibited from doing business with the public sector for a period not less than five years and not more than 10 years. The National Treasury is empowered to determine the period of restriction and each case will be dealt with on its own merits. According to section 32 of the Act the Register must be open to the public. The Register can be perused on the National Treasury website

24 Anti-dumping and countervailing duties and rights

24.1 When, after the date of bid, provisional payments are required, or anti-dumping or countervailing duties are imposed, or the amount of a provisional payment or anti-dumping or countervailing right is increased in respect of any dumped or subsidized import, the State is not liable for any amount so required or imposed, or for the amount of any such increase. When, after the said date, such a provisional payment is no longer required or any such anti-dumping or countervailing right is abolished, or where the amount of such provisional payment or any such right is reduced, any such favourable difference shall on demand be paid forthwith by the supplier to the purchaser or the purchaser may deduct such amounts from moneys (if any) which may otherwise be due to the supplier in regard to goods or services which he delivered or rendered, or is to deliver or render in terms of the contract or any other contract or any other amount which may be due to him.

25 Force Majeure

- a. 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.
- b. If a force majeure situation arises, the supplier shall promptly notify the purchaser in writing of such condition and the cause thereof. Unless otherwise directed by the purchaser in writing, the supplier shall continue to perform its obligations under the contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the force majeure event.

26 Termination for insolvency

26.1 The purchaser may at any time terminate the contract by giving written notice to the supplier if the supplier becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the supplier, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to the purchaser.

**27 Settlement
of Disputes**

- 27.1 If any dispute or difference of any kind whatsoever arises between the purchaser and the supplier in connection with or arising out of the contract, the parties shall make every effort to resolve amicably such dispute or difference by mutual consultation.
- 27.2 If, after thirty (30) days, the parties have failed to resolve their dispute or difference by such mutual consultation, then either the purchaser or the supplier may give notice to the other party of his intention to commence with mediation. No mediation in respect of this matter may be commenced unless such notice is given to the other party.

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

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

- (a) the parties shall continue to perform their respective obligations under the contract unless they otherwise agree; and
- (b) the purchaser shall pay the supplier any monies due the supplier for goods delivered and / or services rendered according to the prescripts of the contract.

28. Limitation of Liability

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

- (a) the supplier shall not be liable to the purchaser, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the supplier to pay penalties and/or damages to the purchaser; and
- (b) the aggregate liability of the supplier to the purchaser, whether under the contract, in tort or otherwise, shall not exceed the total contract price, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.

28 Governing language

- a. 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.

29 Applicable law

- a. The contract shall be interpreted in accordance with South African laws, unless otherwise specified.

30 Notices

30.1 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 Taxes and
duties**

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

32.1 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.

32 Transfer of contracts

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

33 Amendment of contracts

- 33.1 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.

34 Prohibition of restrictive practices

35.1 In terms of section 4 (1) (b) (iii) of the Competition Act No. 89 of 1998, as amended, an agreement between, or concerted practice by, firms, or a decision by an association of firms, is prohibited if it is between parties in a horizontal relationship and if a bidder(s) is

/ are or a contractor(s) was / were involved in collusive bidding.

35.2 If a bidder(s) or contractor(s) based on reasonable grounds or evidence obtained by the purchaser has / have engaged in the restrictive practice referred to above, the purchaser may refer the matter to the Competition Commission for investigation and possible imposition of administrative penalties as contemplated in section 59 of the Competition Act No 89 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.

ANNEXURE A - MANDATORY

4. MANDATORY REQUIREMENTS

BIDDERS SHALL RESPOND IN FULL TO EACH ITEM IN THE FORMAT PROVIDED. THIS FORMAT SHALL BE FOLLOWED AS THE RESPONSE IN THE SPACE PROVIDED WILL BE THE RESPONSE USED FOR THE EVALUATION AND ASSESSMENT. (Only the space required for your response can be increased. No other change to the format of this document will be accepted.)

Responses, provided in the space allowed, that are not clear or inadequate or the lack thereof shall be interpreted as “Not Compliant” even though the compliance column is declared as “Comply” and/or the Tenderer’s offer meets the requirement.

Bidders shall ensure that the response correctly addresses the requirements stated. Responses not addressing the requirement of the specific paragraph shall be interpreted as “Not Compliant”.

Bidders shall declare compliance to each and every paragraph of this Technical, Logistical and Project Management volume in the column labelled “Compliance” as follows:

- Noted: noted and accepted (applicable to articles not containing requirements)
- C: fully compliant
- PC: partly compliant
- NC: not compliant.

For paragraphs marked “C”, “PC” or “NC”, Tenderers shall include a statement as to the nature of the variation and may additionally supply supporting information in the space provided to demonstrate how the proposal meets the needs of GKM.

4.1 Supplier Experience and Qualification

- 4.1.1 The service provider shall provide reference(s) to demonstrate their expertise, experience and capacity in similar implementations. Reference letters from at least 3 enterprise clients confirming that the supplier has implemented and supported all the tools mentioned in 3.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

- The service provider shall provide proof that they are certified to implement and support the software tools above. OEM Certificate(s) or letter(s) of authorization

from the OEM(s) which clearly details which products/activities the supplier is authorized and qualified to undertake must accompany the proposal.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

- The service provider shall provide proof that they are ISO9001 and ISO27001 certified. ISO Certificates must accompany the proposal.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

- The service provider shall provide CV's and at least 3 of the following resource certifications, ISMS, CEH, CISM, CISSP, CRISC.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2 Functional Deliverables

- 4.2.1 Managed SIEM/SOC

4.2.1.1 The proposed Automated Cybersecurity Risk Assessment solution shall provide GKM Administrators the ability to capture Cybersecurity Risks into the system where they will be listed in the order of priority.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
-----------------------------	---

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

4.2.1.2 The proposed solution shall also perform an automated analysis and capturing of Cybersecurity Risks.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2.1.3 The solution shall prioritize Cybersecurity Risks based on the auto calculated impact to business operations.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2.1.4 The proposed solution shall include a graphical presentation of real time Cybersecurity Risks.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2.1.5 The solution shall provide an automated list of recommended Risk Mitigation steps for each of the risks.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2.1.6 The solution shall allow GKM administrators to amend and modify Risk Mitigation steps where necessary.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

Cybersecurity Threat Detection and Incident response

4.2.1.7 The solution shall be able to automatically discover IT assets on the internal network as well as those in the cloud.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2.1.8 The Cybersecurity Threat Detection solution shall have the capacity to collect logs from Endpoints, Firewalls and Anti-Virus software.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
-----------------------------	---

[INSERT FULL RESPONSE FOR EVALUATION HERE]
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

4.2.1.9 Once logs from multiple security platforms are collected, the solution shall aggregate them into a single pane.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2.1.10 The solution shall perform automated vulnerability scanning and threat analysis.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2.1.11 The solution shall be compatible with and able to collect logs from all endpoints, network and security products on any operating system.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2.1.12 When a threat is detected, the solution shall automatically initiate an incident response.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2.1.13 The incident response shall include e-mail and SMS notifications to relevant GKM stakeholders including the IT Service Desk.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2.1.14 The solution shall come standard with a customizable reporting dashboard.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2.1.15 The reporting dashboard shall include among other things, threat and event reporting including compliance reporting.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	

[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]

Security Operations Centre

4.2.1.16 In addition to the Threat Detection and Incident response solution, the service provider shall also provide a 24/7 Security Operations Centre (SOC) as a service to GKM.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2.1.17 The SOC shall ensure that the GKM ICT Infrastructure and services are monitored continuously for any threats and security events.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

Software

4.2.1.18 The solutions offered shall include all the licences/ subscriptions for three years with warranty & support for all the components offered.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2.1.19 The system/ firmware proposed shall be the latest and most stable. The successful bidder shall ensure that all the patches are updated from time to time during the entire contract without any additional costs to GKM.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2.1.20 In addition to the above, should it happen that any other software is required to meet the tender requirements, the bidder must include it in the pricing proposal.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2.1.21 Provide a Standard Operating Procedure (SOP) for the Managed SOC.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

TRAINING

4.2.1.22 The successful bidder shall be required to provide training to designated GKM system administrators to use and manage the systems which will include technical and administration training. Purpose of these training is to enable the system administrators to handle the day to day system operation.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.2.1.23 The training shall include knowledge transfer of the deployed solution architecture and design.

COMPLIANCE (C/PC/NC)	<i>Responding(C/PC/NC) will not automatically be accepted as indicated.</i>
[INSERT FULL RESPONSE FOR EVALUATION HERE]	
[INSERT REFERENCE TO ADDITIONAL INFORMATION HERE]	

4.3 MANAGED DETECTION & RESPONSE

Requirement	Compliant (Yes/No)	Substantiation
Policy Enforcement and Malware Control		
• The proposed solution must support a cloud-based intelligence platform that provides reputation feeds on files and bad hashes to make decisions.		
• The proposed solution must support a single autonomous agent for both EPP & EDR, to protect data with prevention, detection, responses, and threat hunting in one agent.		
• The proposed solution must support both preventive Static AI and Behavioral AI engines that protect from (unknown) malicious files and malicious activities in real-time whether that endpoint is online or offline.		
• This proposed solution is required to include protection capabilities on the endpoint agent without depending on any external analysis systems/resources (like sandboxes or cloud-based AIs)		
• This proposed solution is required dynamically display in the forensics details all behavioral indicators the Agent discovers throughout the entire threat life cycle, even when the threat evolves, not when the threat is detected only.		
• This proposed solution must include detailed Mitre Attack Framework Mapping in its forensics details		

<ul style="list-style-type: none"> • The proposed solution is required to protect against wide classes of malicious software such as viruses, Trojans, spyware, APTs, etc. and shall categorize detected attacks. (Please describe the scope of your protection) 		
<ul style="list-style-type: none"> • The proposed solution is required to support the detection of zero-day malicious file/file-less attacks, and ransomware attacks and adopt behavioral analysis/intelligence in carrying out detection. Remediation and or reversal to the known good state of an endpoint in the event of a ransomware infection/attack. 		
<ul style="list-style-type: none"> • The proposed solution shall support a wide range of endpoints (Workstations, Servers, VDI) , including operating systems Microsoft Windows, Linux, Oracle, Mac OS etc.) 		
<ul style="list-style-type: none"> • The proposed solution is required to support the ability to build file policy filtering based on manually inputted IOC hashes and automated hash feeds from third party solutions or Open Source feeds solutions such as Virus Total, • Looking glass, etc. 		
<p>This product shall provide full EDR capabilities that collects and re-linked of IOCs and support a powerful interface to query, pivot, hunt with advanced query language, on different OS platforms (windows, Linux and Mac)</p>		
<ul style="list-style-type: none"> • This product should provide a graphical Storyline pivoting to up-level analyst speed • on any incident 		
<ul style="list-style-type: none"> • This product shall provide Full EDR search queries for behavioral indicators that is mapped to Mitre ATT&CK framework 		
<ul style="list-style-type: none"> • This product shall provide full response capabilities: mitigation, remediation, rollback, network quarantine, get logs, get files, device control (USB ports), FW control, Secure Remote Shell (full PowerShell on Windows, full Bash on MacOS), orchestration of 3rd party security products using APIs 		

<ul style="list-style-type: none"> ● This product shall provide the remediation on all Oss (Windows, Linux and MacOS) capability in both manual and automatic way based on Behavioral AI analysis 		
<ul style="list-style-type: none"> ● This product shall provide a rollback feature where damaged or impacted files can be restored from a secured location on the same endpoint and not depending on external storage, rollback shouldn't as well depend on a file size limitation. 		
<ul style="list-style-type: none"> ● This product shall provide the ability to acquire the threat file or any other file from the endpoint for further investigation 		
Scalability		
<ul style="list-style-type: none"> ● This Product shall support on-Prem infrastructure deployment of the Management server(s) 		
<ul style="list-style-type: none"> ● This product shall architecturally “scale” in larger deployments. 		
<ul style="list-style-type: none"> ● This product shall support a multi-tenancy environment with an MSSP model. 		
<ul style="list-style-type: none"> ● This product shall support centralizing dashboards from different tenants without breaking the multi-tenancy concept. 		
<ul style="list-style-type: none"> ● This product shall support multi-tenancy for the administration console. 		
<ul style="list-style-type: none"> ● This product shall support distributed appliance-engine model with an appliance-based centralized log storage for distributed events. 		
<ul style="list-style-type: none"> ● This product shall provide a storage system that supports segregation of log data based on tenant. 		
<ul style="list-style-type: none"> ● This product shall have capacity to store massive amounts of both real-time and historical events long-term (say 3 months minimum). (Please describe your storage retention capacity). 		

<ul style="list-style-type: none"> • This product shall support centralized administration in a geographically dispersed deployment. 		
<ul style="list-style-type: none"> • This product shall support high tolerance and resiliency during failures. 		
<ul style="list-style-type: none"> • This product shall detect and alert early enough, failures in either event sources (the main appliances) or its management box in which case shall not lead to temporal loss of logs. 		
Access Control		
<ul style="list-style-type: none"> • This product shall support multitenancy with role-based access and delegated administration control. 		
<ul style="list-style-type: none"> • This product shall support the access of many Admin Roles (Admins, C-Levels, IR roles, IT, SoC, Viewers,) and multiple Admin sessions. 		
<ul style="list-style-type: none"> • This Product and its RBAC roles can be customized and configure permissions for each role. 		
<ul style="list-style-type: none"> • This product shall provide support for multi-factor authentication on both the admin console. 		
Monitoring		
<ul style="list-style-type: none"> • This product shall provide customized, group-specific and predefined suspicious user activity monitoring and reporting for event and audit logs. 		
<ul style="list-style-type: none"> • This product shall have mechanisms/rules to detect shared administrative privileges. 		
<ul style="list-style-type: none"> • This Product shall provide the visibility into SSL traffic for use in hunting operations. 		

<ul style="list-style-type: none"> ● “Administrators have the ability to execute system commands remotely via the console or the API. These are examples of remote commands: <ul style="list-style-type: none"> ○ Get configuration ○ Configure firewall logging ○ Decommission ○ Disconnect from network / reconnect to network ○ Fetch logs ○ File fetch (any file) ○ Initiate scan / abort scan ○ Move to another site ○ Reboot ○ Remote shell ○ Threat Hunting Search ○ Send message to agent OS UI ○ Show applications ○ Shut down ○ Uninstall ○ Update software ○ View threats 		
● This Product provides Device control for USB		
● This Product should provide different access permission to Device Control (allow read and write, allow read only.)		
● This Product provides Bluetooth Device control		
● This Product provides Native OS firewall control for Windows, Mac, Linux. The Firewall control should support Location Awareness		
● This Product provides different Firewall rules including FQDN rules support, and Firewall Control Support for Multiple Remote Hosts in a Rule		
● This Product provides Application and version inventory + Vulnerability/Risk assessment		
● This Product provides different types of whitelisting and exclusions (including exclusions by file hashes, file/folder paths, signer Identity, File types, and by Browser)		

<ul style="list-style-type: none"> • This product provides Blacklisting on different policy levels (global, sites, and groups) 		
<ul style="list-style-type: none"> • This product should provide Continuous visibility into any IP-connected device, including IOT devices 		
<ul style="list-style-type: none"> • This product should investigate unmanaged devices. Unveils device metadata such as Device Type, Operating System, IP Address, MAC Address, Manufacturer, Open Ports, and more 		
<ul style="list-style-type: none"> • This product should control and reduce the attack surface and integrates with local firewall control to effectively isolate unmanaged or rogue devices 		
<ul style="list-style-type: none"> • This product should provide an agent anti-tampering with unique random passphrases 		
Governance and Compliance		
<ul style="list-style-type: none"> • The Service Provider is required to be ISO 27001: Information Security Management Systems & ISO 9001 certified (Proof to be Provided) 		
<ul style="list-style-type: none"> • Project Management certified (Proof to be provided) 		
Integration		
<ul style="list-style-type: none"> • This product shall provide easy integration with Security Incidents and Events Management systems (SIEM) for real-time incident management and shall also integrate well with network management tools. 		
<ul style="list-style-type: none"> • This product shall support Complete API support/interface that can integrate in both ways into other security tools with receive remote instructions from other appliances such as SIEM to take specific decisions on its behalf. 		

<ul style="list-style-type: none"> • This product shall provide easy integration with external Sandboxing solutions for the purpose of utilizing discovered bad hashes/files as well as integration with firewalls to blacklist compromised machines until remediation actions are carried out. 		
<ul style="list-style-type: none"> • This product shall support configuration at both the GUI and CLI 		
Performance		
<ul style="list-style-type: none"> • The Product shall have as little impact to the endpoint as possible with less consumption on CPU and memory (under 1% CPU load and 1 GB memory usage or less) on all OS platforms supported 		
<ul style="list-style-type: none"> • This product shall ensure high performance during peak hours of network transactions ensuring that endpoint performance is not impacted in any form. 		
<ul style="list-style-type: none"> • This product shall support collection and analysis of endpoint telemetry, such as file I/O, network connections, process execution, log-on events, or registry changes and on-demand access to current-state data from all systems. 		
<ul style="list-style-type: none"> • This product shall support enterprise-wide for any type of file “at rest” by name or hash on demand and historical. 		
<ul style="list-style-type: none"> • This product shall support combined, complete but simple search queries using a combination of methods such as regular expression, fully unstructured text search, etc. simultaneously without impacting search performance. 		
Reporting		
<ul style="list-style-type: none"> • This product shall provide a very good reporting interface for viewing real-time logs and ability to generate recurring customized reports. 		

<ul style="list-style-type: none"> • This product shall support exporting of reports in different formats including PDF and CSV and with pre-built report templates customizable to the organization's need. 		
<ul style="list-style-type: none"> • This product shall provide customized reporting based on an Open API platform 		
Virtualization		
<ul style="list-style-type: none"> • This solution shall support a virtual representation of this product in VM environment which will enhance the daily customization test needs of the customer's security research team. 		
Managed Detection Response (MDR), Digital Forensics Incident Response (DFIR)		
<ul style="list-style-type: none"> • The solution must offer managed detection response (MDR) service 24/7 to assist the customer's security team. 		
<ul style="list-style-type: none"> • The solution must have an integrated threat intelligence offering with the endpoints. 		
<ul style="list-style-type: none"> • The solution must offer an integrated sandbox analyzer for malware analysis. 		
<ul style="list-style-type: none"> • The solution must integrate with a SOAR and SIEM platform. 		
<ul style="list-style-type: none"> • The solution must integrate with a SOC Platform 		
<ul style="list-style-type: none"> • Provide a Standard Operating Procedure (SOC) for the Managed Detection and Response (MDR). 		