MBD1

PART A
INVITATION TO BID

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE THULAMELA MUNICIPALITY					
BID NUMBER:	55/2023/2024	CLOSING DATE:	04 APRIL 2024	CLOSING TIME:	11:00 AM
DESCRIPTION	PROVISION OF INTENSIFIED CYBERSECURITY ROADMAP, STRATEGY AND MAINTENANCE FOR 3 YEARS				

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*

OLD AGRIVEN BUILDING
THOHOYANDOU
0950

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]	☐ Yes ☐ No		B-BBEE STATUS LEVEL SWORN AFFIDAVIT	☐ Yes ☐ 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?**	☐Yes ☐No [IF YES ENCLOSE PROOF]	ARE YOU A FOREIGN BASED SUPPLIER FOR **THE GOODS /SERVICES /WORKS OFFERED?**	☐Yes ☐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	FINANCE	CONTACT PERSON	MR DAVHULA K
CONTACT PERSON	MUDZILI TP	TELEPHONE NUMBER	015 962 7718
TELEPHONE NUMBER	015 962 7629	FACSIMILE NUMBER	015 962 7731
FACSIMILE NUMBER	015 962 4020	E-MAIL ADDRESS	
E-MAIL ADDRESS	mudzilitp@thulamela.gov.za		

PART B
TERMS AND CONDITIONS FOR BIDDING

1.	**BID SUBMISSION:**
1.1.	BIDS MUST BE DELIVERED BY THE STIPULATED TIME TO THE CORRECT ADDRESS. LATE BIDS WILL NOT BE ACCEPTED FOR CONSIDERATION.
1.2.	**ALL BIDS MUST BE SUBMITTED ON THE OFFICIAL FORMS PROVIDED–(NOT TO BE RE-TYPED) OR ONLINE**
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 MAY 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: .....

THULAMELA MUNICIPALITY

INVITATION TO BID

PROVISION OF INTENSIFIED CYBERSECURITY SERVICES WITH CYBERSECURITY ROADMAP, STRATEGY AND MAINTENANCE FOR 3 YEARS

Thulamela Municipality invites prospective service providers for provision of the following service:

BID NUMBER	DESCRIPTION	NON-REFUNDABLE BID PRICE	CONTACT PERSON	EVALUATION CRITERIA
NO: 55/2023/2024	Provision of Intensified Cybersecurity Services with Cybersecurity Roadmap, Strategy and maintenance for 3 Year	R3.00 per page or can be downloaded from Thulamela website (**www.thulamela.gov.za**) for free	Mr Davhula K. (015 962 7718) and/or Mr Mudzili T.P. (015 962 7629)	80/20 preference points system and fuctionality

Tender documents are obtainable from Procurement Office, Office No. 02 at Thulamela Local Municipality Head Office, during the following times: 08:00 to 15:30 (Monday to Friday) at a **non-refundable bid price of R3.00 per page** as from **29 February 2024** or can alternatively be downloaded from Thulamela website **(www.thulamela.gov.za)** for free. The tenderer(s) should also download SCM forms that are found in the SCM-FORMS sub folder on the website and complete as part of the Bid documents.

The service providers must submit the completed Bid documents (in black ink) and hand deliver or courier them to Thulamela Municipality. All completed Bid documents (hand delivered or couriered) must be dropped in the BID BOX before the closing date and time of the Bids closure. The onus is on the service providers to make sure the Bid documents are submitted on time and late submission won't be accepted.

Interested service providers must attend a compulsory briefing session on 14 March 2024 at 10h00. Venue: Thulamela local Municipality Council Chamber.

Interested service providers will be expected to submit the Bid documents with the following compulsory requirements.

- Tax Compliance Status Letter or Tax Compliance Pin Number.
- Company registration documents (e.g., CK).
- Proof of registration on CSD.
- Proof of municipal rates and taxes or municipal service charges owed by the bidder AND ALL its directors, not in arrears for more than 3 months. (The proof of municipal rates and taxes or municipal service charges to be submitted must not be older than three (3) months from the closing date of the bid) Attach valid lease agreement in case of rental of office facilities and municipal clearance in respect of the areas exempted from billing by municipalities.
- List of similar projects completed in the last 5 years by the company with client's contact details, descriptions, and contract values (Attach signed appointment letters and/or purchase orders)

Bids will be assessed under the provisions of the following Acts and its Regulations: Municipal Finance Management Act, (Act 56 of 2003); PPPFA, Supply Chain Management Policy of the municipality in accordance with the specifications and in terms of **80/20 preferential points system and functionality.**

Functionality Score Table:

EVALUATION CRITERIA	POINTS ALLOCATED
Scope of work	10
Firm's similar experience	40
Firm's references	10
Work plan	10
Certifications	30
TOTAL	100

Functionality will be scored out of 100% and bidders who score less than 75% will be disqualified for further evaluation.

Specific Goals Categories (CSD will be used for verification)	Number of Points (80/20 system) 20 Points breakdown
1. 100% Black ownership	10
2. 100% Women ownership	5
3. Youth	3
4. Disability (Medical certificate will be used to verify the disability status of the bidder).	2

Sealed bid documents must be submitted in envelopes clearly indicating ***"BID NUMBER AND DESCRIPTION"*** on the outside and must reach the undersigned by depositing it into the official Bid Box at the front of the main entrance to

Thohoyandou Civic Centre, Old Agriven Building, Thohoyandou, by no later than 11:00 on, 04 April 2024.

The Municipality is not bound to accept the lowest Bid and reserves the right to accept any part of a Bid. Bids must remain valid for a period of ninety (90) days after closing date of the submission thereof.

Bids may only be submitted on the bid documentation provided by the municipality.

NB:
Bids which are late, incomplete, unsigned, completed by pencil, sent by telegraph, facsimile, electronically (Fax), or E- mail and without the compulsory requirements will be disqualified.

MAKUMULE M.T.
MUNICIPAL MANAGER

08/03/2024
DATE

Provision of Intensified Cybersecurity Service with Cybersecurity Roadmap, Strategy, and maintenance for 3 Years.			
Qty	**Description**	**Unit Price**	**Total Price**
Cybersecurity risk and vulnerability assessment	The bidder should conduct a comprehensive vulnerability assessment of the entire ICT infrastructure and not limited to: ✓ Server Infrastructure including Virtual servers. ✓ Operating System Configuration ✓ Denial Of Service Attacks ✓ Firewall Rules Review ✓ System Identification ✓ Vulnerability Canning ✓ Wi-Fi Infrastructure ✓ Network Scanning ✓ LAN, DMZ&WAN ✓ Network Nodes ✓ Port Scanning ✓ Spoofing		
Penetration Testing (White, Grey and Black Box)	The testing must be non-disruptive and nonintrusive. Any potential disruptive techniques must be disclosed for the TLM management to determine how the testing will proceed. The bidder should perform the pen testing using white, grey and the black box approach and cover the following but not limited to: ✓ Unauthenticated testing from the perspective of an attacker on the internal ✓ network including full port scanning, service enumeration and exploitation. ✓ Social engineering attacks such as phishing and malicious USB attacks ✓ External Environment - including reporting Domain: www.TLM.org.za and subdomains. ✓ Remote Access for Users/Network VPN Testing Pentest of vulnerabilities identified in the TLM. ✓ Internal Networks (LAN, Wi-Fi & Remote) penetration testing. ✓ Authenticated Web Applications penetration testing. ✓ DMZ "demilitarized zone" Penetration testing. ✓ Internal environment - including reporting.		
Identify Gaps	The bidder should identify gaps against the cybersecurity framework/s i.e., ISO 27001 and should use a work protected approach which includes identification of gaps on ICT Platforms, procedures, controls, data, and people as listed but not limited to: ✓ Conduct cybersecurity response maturity assessment using applicable tools. ✓ All hosted services (i.e., Microsoft platforms, Mimecast etc.) ✓ Critical Systems and Applications Configuration Analysis ✓ Physical Security review (Data Centre) ✓ Current Policy & Procedures review ✓ Test current security controls. ✓ Wireless connection ✓ Mobile Devices		

Develop a *Cybersecurity Strategy*	The bidder must develop a Cybersecurity Strategy containing the essential elements of cybersecurity, but not limited to: ✓ Identifying the TLM's awareness of information security to effectively identify and create a sustainable information security governance framework (including Policy, Standards and Processes) to provide a consistent approach to managing information security risks, both internally and at key third party suppliers. ✓ Protecting the TLM by developing a strategy that includes additional controls to manage ICT environment and user access. Strategy to improve effective user training and to increase overall awareness of information security risks and threats. ✓ Detect by proving guidance on appropriate systems, capabilities, processes, and procedures to detect information security events as early as possible. ✓ The ability to effectively respond and recover from any information cybersecurity incidents, to maintain effective operations across the TLM and retaining stakeholder confidence. The strategy should include plans for business resilience and to restore any key services that might be impaired by an information security event in an efficient and effective manner. ✓ Ensure that the strategy is underpinned by supporting proper governance, policy, and data ownership to provide the required control that will allow the TLM to demonstrate its consistent approach to cybersecurity and threats.		
Additional Required	The Municipality is expecting to receive the following: ✓ Security Gap analysis report (Findings per area). ✓ Revised ICT Security policy and procedures. ✓ Cybersecurity response maturity results. ✓ Cybersecurity Strategy with implementation plan ✓ Proper Budgets Costing for full implementation of the strategy. ✓ Road Map to deal with Cybersecurity (Costed)		
3 Year Expectations	The Municipality is expecting the following: ✓ 1 x Cybersecurity Assessment process and Report per semester ✓ 1 x Vulnerability Testing process and Report per semester ✓ 1 x Pen testing process and Report per semester ✓ Automated and comprehensive devices discovery report ✓ Analyse and report on Cyber-attacks flagged by the tool with solutions on how to curb them. ✓ Report on road map milestones and Cybersecurity Strategy ✓ How much will this cost the Municipality quarterly to report all.		
Skills Transfer	✓ The successful service provider will be expected to train ICT officials on how to utilize Asset Inventory and Vulnerability Tool effectively. ✓ Train ICT officials on the identification and management of vulnerabilities and penetration tests. ✓ Train officials on other possible Cyber attacks		
	To be included on the scope		
	Security Assessment and Planning		
	Identity and Access Management (IAM)		
	Network Security Enhancements		
	Endpoint Protection and Endpoint Detection and Response (EDR)		
	Vulnerability Management Including Remediations		
	Professional Services Including Monitoring and Support		
	Data Protection and Encryption		
	Incident Response and Forensics		
	Continuous Monitoring and Threat Intelligence (Professional		

	Cloud Security Integration		
	Advanced Threat Detection and Deception		
	Security Operations Centre (SOC) Enhancement		
	Third-Party Risk Management		
	Review and Optimization		
	✓ Proposal with Costs to be broken into Three (3) year o Start with Vulnerability Assessment and Penetration test o Create a Cyber Security Strategy with road map o Identify Gaps and align to Cyber Strategy o Stipulate how you will sort issues within the three year period and how it will affect budgets annually o Professional Services and Maintenance Plan and Reporting with costs o Additional matters that could require re-assessment ✓ Solution to ensure that all systems are POPIA compliant		

TECHNICAL EVALUATION CRITERIA

Items	Evaluation Report	Description	Points Allocations – Details Description	Ratings	Weight
1.	Scope of work	Bidder must provide a detailed framework/s to be used to perform the assessment.	No framework provided.	0	10
			Framework provided; scope is partially covered, and the TLM will assess the quality of the solution provided.	05	
			Framework provided; scope is fully covered, and the TLM will assess the quality of the solution provided.	10	
2.	Experience	Profile of the bidder, including experience of the bidder in providing similar services to both private and public clients with a minimum of 3 years' experience in ICT / Cybersecurity	2x Appointment and Reference letters for Cybersecurity **R300K**+ all 2(15 per letter)	10	40
			2x Appointment and Reference letters for Cybersecurity **R500K**+ all 2(25 per letter)	20	
			2x Appointment and Reference letters for Cybersecurity **R1M**+ all 2(40 per letter)	40	
3.	References	The bidder should provide reference letters on a client letterhead. The letters should be signed, indicate the scope of work not more than five years and must have contactable references.	No reference letters attached.	0	10
			Three Letters = 6 points Four Letters = *8* points Five letters or more = 10 points (2 *points per letter).*	10	
4.	Work plan	Detailed plan provided. The plan details how the proposed solution will be implemented and covers all proposals and provides timelines. TLM will *assess the quality of the plan provided, including Road Map and Cybersecurity Strategy.*	No plan provided.	0	10
			The plan partially addresses the scope of how to deliver the TOR and will be implemented within 3 months. TLM will assess the quality of the plan provided.	01- 05	
			The plan fully details the proposed solution within 3 *months* and covers the scope of how to deliver the three-year TOR. TLM will assess the quality of the plan provided.	06 -10	
5.	Certifications (All the certifications should be certified as a duplicate of the primary certification to guarantee its authenticity. Failure to submit certified certificates will lead to a score of zero)	Provide certifications of resources who will be responsible for the proposed solution e.g., Certified Information Security Manager (CISM) certification, Certified Information Systems Auditor (CISA) certification, Certified in Risk and Information Systems Control (CRISC) certification, CompTIA *Security* Certification, CompTIA Advanced Security* Practitioner (CASP+); Certified Information Systems Security Professional (CISSP), Systems Security Certified Practitioner (SSCP). Global Information Assurance Certification (GIAC) Security Essentials *Certification (GSEC).* *GIAC Certified Incident* Handler (GC1H). Offensive Security Certified Professional (OSCP). Certified Ethical Hacker (CEH); and any other Cybersecurity certification not listed.	No proof submitted.	0	30
			Certified Ethical Hacker (CEH)	10	
			Certified Certificates provided, meeting the proposed solution with at least four certifications related to Cybersecurity. (5 points per certificate)	20	
Total Score					**100**
Minimum Qualifying Score					**75**

Functionality Score Sheet

Items	Evaluation Report	Description	Points Allocations – Details Description	Ratings	Score	Total
1.	Scope of work	Bidder must provide a detailed framework/s to be used to perform the assessment.	No framework provided.	0		
			Framework provided; scope is partially covered, and the TLM will assess the quality of the solution provided.	05		
			Framework provided; scope is fully covered, and the TLM will assess the quality of the solution provided.	10		
2.	Experience	Profile of the bidder, including experience of the bidder in providing similar services to both private and public clients with a minimum of 3 years' experience in ICT / Cybersecurity	2x Appointment and Reference letters for Cybersecurity **R300K**+ all 2(15 per letter)	10		
			2x Appointment and Reference letters for Cybersecurity **R500K**+ all 2(25 per letter)	20		
			2x Appointment and Reference letters for Cybersecurity **R1M**+ all 2(40 per letter)	40		
3.	References	The bidder should provide reference letters on a client letterhead. The letters should be signed, indicate the scope of work not more than five years and must have contactable references.	No reference letters attached.	0		
			Three Letters = 6 points Four Letters = *8* points Five letters or more = 10 points (2 *points per letter).*	10		
4.	Work plan	Detailed plan provided. The plan details how the proposed solution will be implemented and covers all proposals and provides timelines. TLM will *assess the quality of the plan provided, including Road Map and Cybersecurity Strategy.*	No plan provided.	0		
			The plan partially addresses the scope of how to deliver the TOR and will be implemented within 3 months. TLM will assess the quality of the plan provided.	01- 05		
			The plan fully details the proposed solution within 3 *months* and covers the scope of how to deliver the three-year TOR. TLM will assess the quality of the plan provided.	06 -10		
5.	Certifications (All the certifications should be certified as a duplicate of the primary certification to guarantee its authenticity. Failure to submit certified certificates will lead to a score of zero)	Provide certifications of resources who will be responsible for the proposed solution e.g., Certified Information Security Manager (CISM) certification, Certified Information Systems Auditor (CISA) certification, Certified in Risk and Information Systems Control (CRISC) certification, CompTIA *Security* Certification, CompTIA Advanced Security* Practitioner (CASP+); Certified Information Systems Security Professional (CISSP), Systems Security Certified Practitioner (SSCP). Global Information Assurance Certification (GIAC) Security Essentials *Certification (GSEC). GIAC Certified Incident* Handler (GC1H). Offensive Security Certified Professional (OSCP). Certified Ethical Hacker (CEH); and any other Cybersecurity certification not listed.	No proof submitted.	0		
			Certified Ethical Hacker (CEH)	10		
			Certified Certificates provided, meeting the proposed solution with at least four certifications related to Cybersecurity. (5 points per certificate)	20		
Total Score					**100**	
Minimum Qualifying Score					**75**	

BID NO. 54/2022/2023: PROVISION OF INTENSIFIED CYBERSECURITY SERVICES WITH CYBERSECURITY ROADMAP AND STRATEGY FOR 3 YEAR

The following is a statement of similar work executed by the company/ies in the last five (5) years:

Employer, Contact person and telephone number	Description of contract	Value of work inclusive of VAT (Rand) if applicable	Date Completed