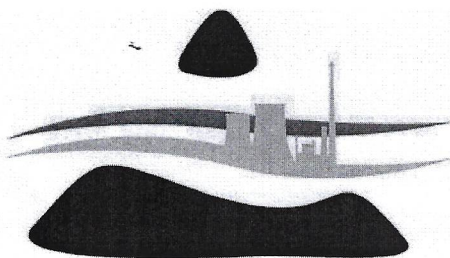


**FEZILE DABI
DISTRICT MUNICIPALITY**



BID DOCUMENT

SCM/BID NO: 055/2025-26

**SUPPLY, INSTALL, CONFIGURE ANTIVIRUS SOFTWARE INCLUDING MAINTENANCE
AND SUPPORT FOR A PERIOD OF THIRTY SIX (36) MONTHS**

CLOSING DATE 17 JUNE 2026 @ 12:00PM

PREPARED FOR/BY:

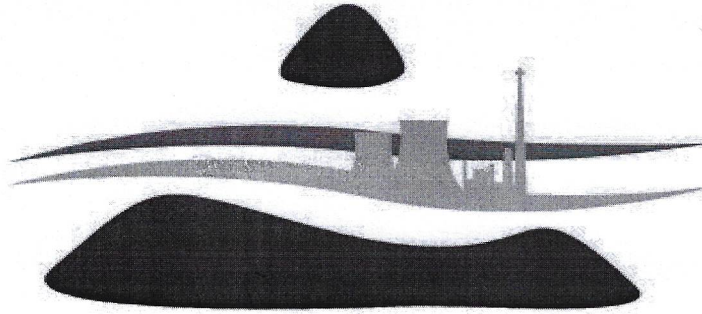
FEZILE DABI DISTRICT MUNICIPALITY
P.O.BOX 10
SASOLBURG
1947

TEL: (016) 970 8600
FAX: (016) 970 8762

ENQUIRIES: SCM UNIT
(016) 970 8600 OR

BIDDER: _____

BID AMOUNT (VAT INCL.): _____



FEZILE DABI DISTRICT MUNICIPALITY

NOTICE NUMBER: FDDM 055/2025-26

Date: 11 June 2026

Dear: Service provider

Request for Formal Written Quotation

Kindly furnish Fezile Dabi District Municipality with a written quotation for the supply of the goods / services as detailed on the below schedule.

**SUPPLY, INSTALL, CONFIGURE ANTIVIRUS SOFTWARE INCLUDING
MAINTENANCE AND SUPPORT FOR A PERIOD OF THIRTY SIX (36) MONTHS**

SPECIFICATIONS

Kindly refer to the attached specification

The quotation must be submitted on the letterhead of your business and can be delivered by hand not later than the 17 June 2026 before 12h00 to: Supply Chain Management Unit of Fezile Dabi District Municipality.

U

The following conditions will apply:

- Prices quoted must be valid for at least (30) days from the date of your offer.
- In a case of an event, preference will be given to local service providers
- Prices quoted must be firm and must be inclusive of vat.
- A firm delivery period must be indicated, NOT LONGER THAN 7 WORKING DAYS AFTER ORDER.
- For all transaction tax Clearance certificate must be attached.
- The service provider MUST complete the following MBDs form (4, 6.1, 8 and 9) failure to complete those forms will led to disqualification.

- Copy of company registration reflecting equity owned by the members and status.
- ALL service providers should complete MBD6.1 form in order to claim points on special goals.
- All quotations will be evaluated in terms of preferential points system as prescribed in the preferential procurement policy regulation of 2022 as adopted by council on the 28 February 2023
- Only companies registered on the CSD will be considered.
- Municipal rates & taxes information in the bid document must be duly completed by Local Municipality or Landlord stamp with Landlord municipal rates and taxes or lease agreement with Landlord municipal rates and taxes or Affidavit with Landlord municipality rates and taxes.
- ID copy/copies of the Director/s of the company.
- Central Supplier Database (CSD) summary report must be attached to the tender/bid document not older than six months.

POINTS ALLOCATION FOR 80/20 PRINCIPLE:

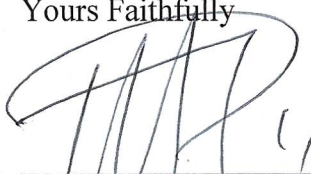
- ❖ PRICE 80
- ❖ Special goals 20

Special Goals	Points Allocation
Locality (within fezile Dabi District municipality) provide proof of address	10
Women Ownership (Provide shareholder certificate with ID copy)	5
Disability (provide Doctors note)	5

Failure to comply with these conditions may invalidate your offer.

NB: Forms for claiming preferential points are available from Supply Chain Management unit offices at a non- refundable cost of R50.00 per copy, **bidders are welcome to request the bid document from SCM unit to be email for free.**

Yours Faithfully



Paseka Molei
ACTING CHIEF FINANCIAL OFFICER

GUIDELINES ON SPECIFICATION FOR PROCUREMENT: – SUPPLY, INSTALL, CONFIGURE, MAINTAIN AND SUPPORT OF ANTIVIRUS SOFTWARE – THIRTY SIX (36) MONTHS

PROJECT NAME:	PROCUREMENT:- SUPPLY, INSTALL, CONFIGURE, MAINTAIN AND SUPPORT OF ANTIVIRUS SOFTWARE			
Prepared by:	Ms. Maletsatsi Mofokeng	Signature:		Date :
Authorized by:	Ms. Gladys Ramaboea Director – Corporate Support Services	Signature:		Date :

Project Initiation Phase – This section of the Procurement Plan provides the Bid Specification Committee with essential information regarding the need to procure a service provider for the **procurement: Supply, install, configure Antivirus Software including maintenance and support for a period of thirty six (36) months.**

Guideline for Terms of reference

This tender is for the appointment of a Service Provider to supply, install, and configure Antivirus Software including maintenance and support for a period of thirty six (36) months.

A. INTRODUCTION

Fezile Dabi District Municipality (FDDM) invites all reputable and experienced service providers to submit proposals for the provision of an Enterprise Antivirus Software and Mail Security for Exchange license for the effective security management of all municipal devices for a period of thirty six (36) months.

B. OBJECTIVES

The objectives of the project are to:

- Protect organizational endpoints against malware, ransomware, spyware, and cyber threats.
- Centralize endpoint security management and reporting.
- Improve threat detection and incident response capabilities.
- Ensure compliance with municipal ICT security policies.
- Minimize downtime caused by security incidents.
- Enhance visibility across all ICT assets and endpoints.

C. CURRENT ENVIRONMENT

FDDM has utilised ESET Endpoint Security for many years as its endpoint security solution for desktops, laptops, servers and email with a central admin console located on one of the servers. We are also using ESET Mail Security for Microsoft Exchange to provide real-time protection for email against viruses, spyware, phishing, and other malicious in FDDM environment.

FDDM has at least approximately 130 employees that are equipped with computers to enable them to perform their day to day duties. The employees use laptops/notebooks as well as desktops.

FDDM network is a Microsoft windows network. The following Operating Systems Platform should be supported with no extra cost:

- Windows 8/8.1/10,11 32 & 64 bits
- Virtual servers running on Windows Server 2008 R2 Standard and Windows Server 2012 Standard
- Virtualization Applications: Hyper-V and VMware Windows Server 2008 R2 Enterprise and 2022 Standard
- Stand alone servers running on Windows Server 2012 R2 Standard, 2019 Standard and 2022 Standard

Desktops/Laptops	Servers	Virtual Servers
Desktops 24	4	9
Laptops 93		
TOTAL	130	

D. SCOPE OF WORK & REQUIREMENTS

The selected service provider shall:

1. Supply of Antivirus Software

- Supply 130 antivirus software licenses for servers, desktops and laptops devices.
- Provide licensing for the required subscription period.
- Ensure licenses are genuine and vendor authorized.
- Ensure compatibility with the municipal operating systems and infrastructure.

2. Installation and Deployment

- Install and configure centralized management console/dashboard.
- Deploy antivirus agents on desktops, laptops, and servers.
- Configure security and endpoint protection policies.
- Configure automatic updates and scheduled scans.
- Configure quarantine, alerts and notifications settings.
- Configure web protection, email protection and device control policies where applicable.
- Ensure minimal disruption during installation.

3. Security Configuration

- Configure role-based administrative access controls.
- Set up alerts, notifications, and reporting mechanisms.
- Configure malware and ransomware protection
- Configure quarantine and threat response actions.
- Integrate with existing ICT infrastructure where required.

4. Migration & Optimization

- Remove existing antivirus solutions.
- Optimize endpoint performance and policy settings.

5. Testing & Validation

- Conduct solution testing and verification.
- Perform threat detection simulations.
- Validate update mechanisms and reporting functionality.
- Validate malware detection and response capabilities

6. Training & Knowledge Transfer

- Train ICT administrators on system management.
- Provide end-user awareness guidance.
- Provide operational manuals and technical documentation.

7. Support & Maintenance

- Provide post-implementation technical support.
- Provide software updates and patch management assistance.
- Respond to incidents and system issues within agreed SLA timelines.
- Provide periodic system health checks and reporting.
- Apply all software updates/version upgrades released by the respective Original Equipment Manufacturers (OEMs) during the contract period.

E. TECHNICAL REQUIREMENTS

The proposed solution should support:

- Real-time antivirus protection
- Anti-malware and anti-ransomware protection
- Email security and phishing protection
- Endpoint Detection & Response (EDR) capabilities
- Web filtering and URL protection
- Device control and USB protection.
- Centralized cloud or on-premise management
- Automated updates and patch management.
- Threat intelligence integration
- Reporting and analytics
- Remote Connection to network devices
- Compatibility with Windows and servers

F. DELIVERABLES

- Antivirus software licenses for 130
- Installation and configuration of antivirus solution across all FDDM devices (Servers, Desktops and Laptops) 130
- Installation and configuration of Email Gateway Security
- Centralized Management Console
- Security policies and configurations.
- Configure network audits to detect new devices
- Configure auto updates daily
- Configure server to send daily, weekly and monthly automated reports
- All stand alone computers should be implemented in such a way that the PCs should get update automatically from internet on regular basis.
- Training of FDDM ICT employees (2)

G. MINIMUM REQUIREMENTS

- Company profile.
- Proof of valid reseller, accreditation, or authorisation certificate from the relevant (OEM)
- At least four (4) reference letters for similar projects completed.
- At least six (6) years' experience of the technical person in endpoint security solutions.

H. MAINTANANCE AND SUPPORT SERVICES

The appointed service provider shall provide comprehensive maintenance and support services for the antivirus software environment as and when needed, including but not limited to the following:

1. Technical Support Services

- Provision of phone, remote and onsite technical support from Monday-Friday, 08:00 am to 16:30 pm
- Troubleshooting and resolution of antivirus-related issues.
- End-user support for antivirus alerts and notifications.
- Provide support during security incidents and threat outbreaks
- Escalate unresolved issues to the Original Equipment Manufacturer (OEM) where necessary.
- Support for server and workstation antivirus protection.
- Support for email and web protection features.

2. Updates and Patch Management

- Ensure antivirus software versions are kept up to date.
- Deploy security patches and software updates.
- Deployment of security updates and hotfixes.
- Monitoring update compliance across endpoints.
- Verification of successful update deployment.

3. Security and Compliance Management

- Monitoring compliance with municipal security policies.
- Generation of security and compliance reports.
- Reporting on detected threats and remediation activities.
- Monitoring endpoint protection coverage.
- Audit support and compliance assistance.
- Recommendations for improving endpoint security posture.

4. Backup and Recovery Support

- Support for restoration of quarantined files where applicable.
- Recovery support following malware incidents.
- Validation of endpoint recovery processes.

5. Reporting

- Provide monthly maintenance and support reports.
- Provide incident and resolution reports.
- Provide security threat and vulnerability reports.
- Provide recommendations for improvements and risk mitigation

I. SERVICE AVAILABILITY

No.	Priority	Description	Response Time	Resolution Time
1.	Critical	Complete service outage	15 Minutes	1-4 Hours
2.	High	Service affecting multiple users	30 Minutes	1-4 Hours
3.	Medium	Limited impact affecting individual users	1 Hours	1-4 Hours
4.	Low	Minor issues	1 Hours	1-4 Hours

J. ROLES AND RESPONSIBILITIES

1. Service Provider Responsibilities

The Service Provider shall:

- Supply genuine and licensed Antivirus Software
- Install and configure the solution professionally
- Ensure antivirus definitions remain updated
- Provide qualified technical personnel
- Monitor and respond to threats where applicable
- Provide technical support and maintenance
- Maintain confidentiality of Client information
- Provide regular system health and incident reports

2. Municipal Responsibilities

- Provide access to authorised personnel to current systems and infrastructure
- Assign project representatives
- Ensure availability of network connectivity, hardware compatible and operating systems
- Provide required approvals for changes and maintenance activities
- Communicate system changes that may affect the antivirus solution
- Ensure timely approvals and cooperation implementation

K. DURATION OF THE CONTRACT

State how long the contract will take

Thirty Six (36) months

NB: renewable based on performance

L. CONFIDENTIALITY, INTELLECTUAL PROPERTY AND DATA PROTECTION

The service provider shall:

- Treat all municipal information and ICT infrastructure details as confidential and shall not disclose such information to third parties without written consent from the Municipality.
- Comply with POPIA and applicable data protection legislation.
- Ensure secure handling of municipal data.
- Sign confidentiality and non-disclosure agreements where required.
- All reports, documentation, configurations, and deliverables produced during the contract period shall remain the property of the Municipality.

M. MAINTENANCE AND SUPPORT PERIOD

The maintenance and support contract shall be for a period of thirty six (36) months including:

- Technical support
- Configuration adjustments
- Fault resolution
- Software update assistance

NB: Maintenance and Support at No Costs

N. PERFORMANCE MANAGEMENT

In terms of Section 116 (2) of the MFMA, the municipality is required by Law to monitor the performance of service providers on a monthly basis in line with the performance areas as stipulated in the Service Level Agreement (SLA). The monitoring of provider will be done on a monthly basis during the supply, install, and configure Antivirus Software including maintenance and support for a period of thirty six (36) months.

O. PENALTIES FOR NON-PERFORMANCE

Failure to meet agreed SLA standards may result in:

- Service credits
- Financial penalties
- Extension of support period
- Corrective

action

requirements

P. PRICING SCHEDULE

No.	Description	Quantity	Unit Price	Total excl VAT Year 1	Total excl VAT Year 2	Total excl VAT Year 3
1.	Antivirus Software License	130	R	R	R	R
2.	Installation and Configuration		R	R	R	R
3.	Training ICT Staff	2	R	R	R	R
4.			R	R	R	R
5.			R	R	R	R
SUB-TOTAL				R	R	R
VAT @ 15%				R	R	R
TOTAL incl VAT				R	R	R

S. EVALUATION CRITERIA

CRITERIA	SUB-CRITERIA	POINTS
A. COMPANY EXPERIENCE	Service provider must attach contactable references where supply or provisioning of anti-virus software licenses were supplied, installed and configured within the last ten years. Points will be allocated as follows: ▪ 1 reference 15 points ▪ 2-3 references 30 points ▪ 4 or more references 50 points NB: Reference letters must be on company letter head, signed off by client	50
B. OEM LETTER/CERTIFICATION	Service provider must provide a valid reseller, accreditation, or authorisation certificate from the relevant Original Equipment Manufacturer (OEM) This certificate must serve as official proof that the bidder is an authorised partner, reseller, or distributor, duly accredited to sell, install, and support the proposed equipment	30
C. EXPERIENCE AND QUALIFICATION	Service provider must attached CVs and relevant certifications of the Project Manager or Engineer. Years of experience of key staff on same work Points will be allocated as follows: • 1-2 years 10 point • 3-5 years 15 points • 6 + years 20 points	20
TOTAL		100

The bidder must obtain 80% points or more for further evaluation