

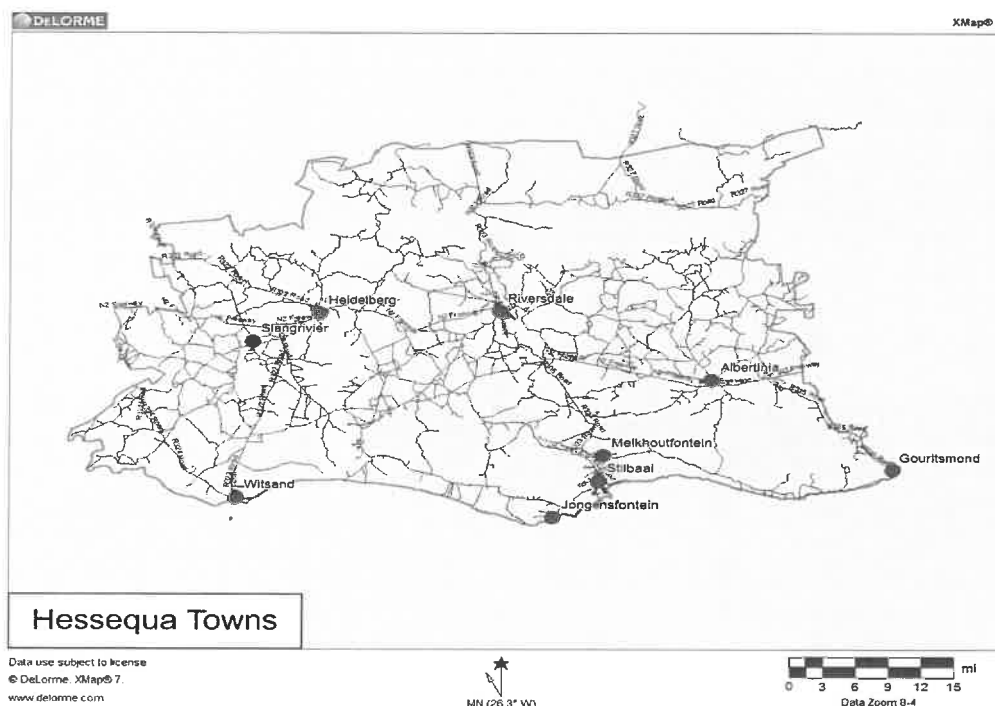
## SECTION 2.1: SPECIFICATIONS

## PROJECT SPECIFICATION

## HES CORP: 10/2526: IMPLEMENTATION AND MANAGEMENT OF AN AUTONOMOUS EMAIL &amp; NETWORK SECURITY &amp; PERFORMANCE MONITORING SOLUTION FOR HESSEQUA MUNICIPALITY.

## 1 Overview

The project entails the implementation of a network & email security solution to mitigate cyber threats which have become more complex, sophisticate and rapid in the current technology climate. Current legacy approaches have become insufficient, it has become a priority to keep threats outside the network and protect personal information. Hessequa Municipality with efficiency in mind, is continually automating business processes and has thus become more reliant on technology to deliver basic services. The Municipality has multiple connected sites where information is being processed across the whole municipal geographical area which include remote offices, camping sites and director's homes all connected to the head office situated in Van den Berg Street, Riversdale, 6670.



## 2. How to Provide the Information Requested

A formal hard copy version of your proposal with all appropriate forms completed, etc. will need to be submitted. In addition to the formal hard copy, 2 electronic files will need to be provided on USB stick – one in a Microsoft Word format, and one in a PDF format. **The Word/ PDF document must be a copy of the response section of this file with the answers inserted in the appropriate places.** A Microsoft Word version of the response section will be made available to prospective vendors. The PDF document must include a PDF version of Word/PDF file, as well as all the other information contained in the hard copy submission (a scan of the hard copy submission would be acceptable). **Do not provide several digital files as only one file only will be looked at.** The purpose of the single file is to provide a quick reference for key word searches and enable a single spread sheet of all vendor solution metrics and prices to be easily created.

Initials of Service Provider's Authority: .....

Answer each question in its entirety by inserting your response into the text boxes in the provided Microsoft Word document. **Expand the text boxes, as necessary.** Please respond fully to each question completely before proceeding to the next question. Do not place additional information in an appendix or annexure; rather place any additional information immediately following the question before proceeding to the next question. Where separate documents are requested which cannot be inserted digitally into the document, please insert them into the hard copy of your response at the back of the paper document. If you feel that a question overlaps another question, then repeat your answer. Do not reference information or documents in annexures, etc. Bidders are required to provide all information relevant to their response to a question in the text box provided. The service to the Hessequa Local Municipality, as may be required for a period of 36 months renting as indicated on this bid document, from the time of the award. The services shall commence from date of appointment, with an option to extend as may be agreed upon by both parties.

## **2 Responsibility for Response Costs**

The respondent shall be solely and fully responsible for all costs associated with the development, preparation, transmittal, and submission of this RFT and any subsequent proposal, including the selection process and associated negotiations. The municipality may, in its sole discretion, ask qualified respondents to present their final proposal in person to the municipality's representatives at the municipality's offices, and the costs of such presentations, as well as the costs of any proof-of-concept implementation required by the municipality, shall be solely the responsibility of the respondent. The municipality assumes no contractual or other obligations because of the issuance of this RFT, the preparation or submission of a later proposal by a respondent, the evaluation of proposals, the respondent's conduct of presentations or proof of concept implementations, or the selection of any respondent for further negotiations. There may be no claims whatsoever for reimbursement from the municipality or any of its consultants for any such costs.

## **3 Scope of this RFT**

With the evolving threat landscape comes the need for extra defence against sophisticated cyber criminals who exploit large and important networks. This is a more pressing concern for governmental organisations that host important data systems which are likely targets for malicious attacks.

Hessequa Municipality is a reputable and well-known organization that has a profile of interest to a range of potential attackers. The Municipality requires complete network visibility in order to thoroughly survey its network. Additionally, the organisation would need a security solution capable of detecting and responding to potential vulnerabilities and actual threats, inside and outside the network, that may aim to target its critical assets, including sensitive information.

Service providers who can render a complete cyber defence solution and associated services are hereby invited to submit proposals for the implementation and management of an autonomous email & network security performance solution to all our sites on a rental basis. Hessequa Municipality wants to enter into a three (3) year agreement with one service provider from date expected of appointment (1 July 2026). The purpose of this tender is to mitigate the risk of potential cyber threats but also to prevent data loss and system downtime which could potentially impact negatively on service delivery.

Hessequa Municipality wishes to procure an affordable, cost-effective email & network security performance monitoring service to secure and ensure information is protected across the network on a reliable platform which include all connected branches and offices to the main building and server room situated in the Civic Centre at 44 Van Den Bergh Street, Riversdale.

The Hessequa Municipal region consists of a large geographical area and serves Riversdale, Albertinia, Gouritsmond, Melkhoutfontein, Still Bay, Jongensfontein, Witsand, Slangrivier and Heidelberg. Some of these towns also have multiple connected sites such as municipal administrative offices, camps, director's homes, and technical outbuildings. The network currently consists of a minimum of **45 x** different points and has about **305 x** users on the network on an ad hoc basis.

The municipality through this **REQUEST FOR TENDER** place a shared responsibility on the successful bidder to assist the Municipality with legislative compliance to applicable laws around data protection.

The technical requirements are focussed on two (2) separate aspects listed in the tables below with reference to:

1. **Network security & performance monitoring**
2. **Email security**

The primary focus of the Municipality will be to firstly secure the network performance & security aspects with email security as a secondary requirement within the constraint of the budget. Therefore, Hessequa reserves the right to either fully or partially implement the required solutions.

Hessequa Municipality has successfully utilized Darktrace for over three years to proactively secure its ICT environment against cyber threats. As the preferred solution, Darktrace has demonstrated its ability to autonomously detect and respond to anomalies across the network with minimal human intervention. The Municipality now seeks to expand or enhance this capability, prioritizing network performance and security, while also addressing email threats within available budget constraints.

Any proposed solution must align with Darktrace's core principles—leveraging machine learning and mathematical modeling rather than static rules, signatures, or historical data. The email security component must passively analyze traffic and metadata to establish a dynamic baseline of normal activity, enabling the detection of novel and sophisticated threats that bypass traditional gateways.

The Municipality values technologies that correlate insights across network and email layers to provide a unified threat assessment. Compliance with POPIA and other legislative standards is essential, and the solution must operate seamlessly with minimal manual oversight. While Darktrace remains the preferred platform, similar technologies that offer equivalent or enhanced capabilities are welcomed, provided they support phased or partial implementation to accommodate budgetary limitations. Please use the following table to indicate the proposed solution(s) and how it relates to the requirements in the second table provided below.

|    | <b>Proposed Solution</b> | <b>Comply (Yes/No)</b> |
|----|--------------------------|------------------------|
| 1. |                          |                        |
| 2. |                          |                        |

| No.  | Requirement Description  | Comply (Yes/No) | Bidder's compliance statement and page reference |
|--|--|-----------------|--|
| <b>NETWORK SECURITY &amp; PERFORMANCE MONITORING</b> |  |                 |  |
| 1.1  | The solution must be able to use multiple techniques of machine learning, containing at least: deep learning, supervised machine learning and unsupervised machine learning. |                 |  |
| 1.2  | After the initial learning period, the solution must automatically provide a complete audit trail of all devices in the environment, pre-sorting at least the                |                 |  |
|  | • Device type  |                 |  |
|  | • Hostname   |                 |  |

Initials of Service Provider's Authority: .....

|     |   |  |  |
|-----|---|--|--|
|     | <ul style="list-style-type: none"> <li>Mac address</li> </ul>   |  |  |
|     | <ul style="list-style-type: none"> <li>The first and last time the device was seen on the network</li> </ul>  |  |  |
| 1.3 | The proposed Solution must provide full network visibility, including traditional and non-traditional IT  |  |  |
| 1.4 | The Proposed Solution should not use any form of Agent Based installations on the End Points to achieve the functionality mentioned in this Bid Requirement. The Proposed solution should integrate with every device residing on the network with an IP Address. Examples of such devices are as below but they are not limited to |  |  |
|     | 1. Servers (physical or VM)   |  |  |
|     | 2. PC/Laptops   |  |  |
|     | 3. Smart Mobile phones/Tablet PCs/Ipads   |  |  |
|     | 4. Access Points  |  |  |
|     | 5. Bio-Metric Solutions   |  |  |
|     | 6. VPN Based Solutions  |  |  |
|     | 7. Any Other Device bearing an IP and connecting to NSSF's network.   |  |  |
| 1.5 | After the initial learning period, the technology must automatically provide a complete audit trail of all subnets found in the network   |  |  |
| 1.6 | The solution must be a self-learning platform and have an adaptive approach, that uses proven methods (with reference to 1.1) to learn about the environment in which it finds itself and detect and respond to deviations from normal activity.  |  |  |
| 1.7 | The solution should have functionalities where the network's baseline must be adaptive and dynamic enough to suit any changes in the environment's behaviour.   |  |  |
| 1.8 | The solution should operate completely based on behavior, where technologies that make use of rules and/or signatures will not be allowed   |  |  |

|      |  |  |  |
|------|--|--|--|
| 1.9  | It must be based on behavior analysis, being able to highlight at least:   |  |  |
|      | a. all unusual connectivity in the network   |  |  |
|      | b. all unusual activities on the network   |  |  |
|      | c. be able to do a detailed tracking of the device, indicating even its history of IPs, if it is in a DHCP scope   |  |  |
|      | d. be able to do a detailed tracking of the user indicating even all the hostnames associated to a certain credential  |  |  |
|      | e. be able to identify a significantly unusual volume of connections   |  |  |
|      | f. identify the level of rarity of a device on the network as well as the rarity level of an external site access  |  |  |
| 1.10 | The solution must be able to automatically alert all unusual and abnormal activities on the network  |  |  |
| 1.11 | The solution must provide simple and fast filters to enable the analysis of violations by at least Users, Devices, and type of violation.  |  |  |
| 1.12 | The solution should have an omni-search search bar that makes it possible to search immediately for a device, IP, subnet, or network host  |  |  |
| 1.13 | The solution must have a user interface where it can be possible to consult the complete System status including at least:   |  |  |
|      | a. the software version, used disk space, CPU consumption and memory consumption   |  |  |
|      | b. the detailing of all active interfaces and respective traffic received through each of them   |  |  |
|      | c. the total bandwidth currently processed, the average bandwidth processed to date, the bandwidth recorded minimum in last 6 days and 1 previous week   |  |  |
|      | d. a detailed analysis of all the traffic received in the device as well as the last time the main protocols were seen, among them, HTTP, HTTPS, FTP, LDAP, SMTP, SSH, SMB, SSDP, POP3, NTLM, IMAP, Kerberos, among others |  |  |
| 1.14 | The solution should not need to share data with a global security cloud to get its security intelligence   |  |  |

|      |  |  |  |
|------|--|--|--|
| 1.15 | The solution must be able to identify new and unknown attack behaviours without making use of signatures or rules  |  |  |
| 1.16 | The solution must be able to identify any abnormal behaviour in the environment and highlight these behaviours in real time  |  |  |
| 1.17 | The solution must be able to identify any new device inserted in the network   |  |  |
| 1.18 | The solution must be able to automatically group devices into groups and clusters by their behaviour similarity  |  |  |
| 1.19 | The solution must have a user interface for the visualization of threats being able to plot in real time the map of any connection made by the internal devices  |  |  |
| 1.20 | The solution must have a feature capable of enabling retrospective analysis of the incident's logs, returning the connection in seconds, minutes, hours or days before a certain anomaly had been identified |  |  |
| 1.21 | The solution should provide an instant overview of what is happening in the organization globally  |  |  |
| 1.22 | The solution should visually represent all network activity and connections between all machines and users (internally and externally)   |  |  |
| 1.23 | The solution should be based on probabilistic mathematical methods, analysing and correlating more than 350 distinct dimensions within the package:  |  |  |
|      | a. creating unique modelling techniques for each user and device, as well as for the relations between them  |  |  |
| 1.24 | The solution must be able to group the anomalies intelligently and by level of criticality   |  |  |
| 1.25 | The solution must be able to do a packet capture in real time permitting a thorough analysis of the incident at the time of the occurrence   |  |  |
| 1.26 | The solution must offer the option of analysing the package in both wireshark and inside its own user interface by itself  |  |  |
| 1.27 | The solution must enable the customization and adaptation of the machine learning to specific conditions and characteristics of the network  |  |  |
| 1.28 | The solution must have LDAP integration  |  |  |

|                                  |   |  |  |
|----------------------------------|---|--|--|
| 1.29                             | The solution must allow the advanced customization of the technology, allowing to consider multiple data parameters when checking a certain behaviour, among the parameters it should be possible to at least have the following options: Connections, external connections, internal connections, data transfer, external data transfer, internal SMB connections, closed-port connections, broadcasts, connected devices, data transfer (client), data transfer (server), among other relevant metrics. |  |  |
| 1.30                             | The solution must allow to import of external whitelists and blacklists   |  |  |
| External Integrations and Report |   |  |  |
| 2.1                              | The solution should enable the automatic creation of executive reports covering at least one overview of:   |  |  |
|                                  | a. the entire deployment summary indicating the total number of devices, total number of subnets and processed media bandwidth  |  |  |
|                                  | b. a summary of breaches per attack phase   |  |  |
|                                  | c. a devices breach summary   |  |  |
|                                  | d. a Top devices summary breaching high priority conditions   |  |  |
|                                  | e. a summary of the most frequent breaches to main compliance items such as misuse of: USB, google drive, outbound RDP, external SQL, among others  |  |  |
|                                  | f. a Top devices summary that most breaches the compliance conditions generating risk to the organization   |  |  |
| 2.2                              | The solution must have a Dynamic Threat Dashboard for a simplified overview of real-time threats that is simple and intuitive and that enables at least:  |  |  |
|                                  | a. an immediate understanding of breaches with a description of what the breaches means   |  |  |
|                                  | b. a recommendation for the action that could be taken  |  |  |
|                                  | c. a filtering for breaches more critical as well as for devices more critical  |  |  |
|                                  | d. a complete breach detailing with device data, history, tags, connections, logs, and device history   |  |  |

|              |  |  |  |
|--------------|--|--|--|
|              | e. a possibility of opening a more detailed and detailed investigation of the logs and connections with the topology plotted in 3D   |  |  |
| 2.3          | The solution must be OPEN API, supporting integrations with other security elements at least in the following formats:   |  |  |
|              | a. CEF, LEEF, JSON, SYSLOG, TAXII, among others  |  |  |
| 2.4          | The technology must have its own mobile app available in both Google Play Store and Apple Store in order to enable remote management of incidents with no further investment or costing.   |  |  |
| 2.5          | The proposed Solution should have in-built Analyst Feature with AI and ML Capabilities and should minimum deliver the following:   |  |  |
|              | • A high-level Summary of the incident and associated Model Breaches   |  |  |
|              | • A detailed timeline highlighting relevant events related to the incident   |  |  |
|              | • Attack phases involved in the incident.  |  |  |
|              | • Fully automates threat investigations at a speed and scale that no human ever could  |  |  |
|              | • Ability to create a shareable report in different supported formats with all the stake holders within the organization.  |  |  |
|              | • Present a list of related breaches and alerts and have those connect to other breach devices   |  |  |
| Architecture |  |  |  |
| 3.1          | The solution must support a complete and scalable architecture through the licensing of additional components required to integrate with the various digital environments, including on-premise, cloud and hybrids, supporting at least: |  |  |
|              | a. Amazon AWS SaaS, EC2, IAM, S3, VPC and LAMBDA   |  |  |
|              | b. Microsoft Azure   |  |  |
|              | c. Google G-Suite  |  |  |



|     |  |  |  |
|-----|--|--|--|
|     | d. Office 365  |  |  |
|     | d. Virtual components (virtual machines)   |  |  |
|     | e. Scripts for analysis of local servers (sensors for operating systems)   |  |  |
| 3.2 | The solution must support a distributed architecture with components working in the MASTER-SLAVES architecture where all data analysis and correlation is performed locally and only metadata is forwarded to the central site for centralized administration so as not to burden the network. |  |  |
| 3.3 | The solution must consume and analyse raw data (raw packets) through port mirroring (SPAN) or through the use of a TAP   |  |  |
| 3.4 | The proposed technology will not be accepted if it only uses partial analysis of the packages making use of sflow, jflow, netflow, among others, please explain how your technology can comply to this requirement.  |  |  |
| 3.5 | The solution should be supplied in the form of an Appliance manufactured by the same Manufacturer as the software. Manufacturer should provide warranty on the Hardware and Software.  |  |  |
| 3.6 | Supplied hardware appliance from the Manufacturer must be capable of handling up to 5Gbps of throughput  |  |  |
| 3.7 | A single hardware appliance must be supporting the analysis of up to 50,000 devices  |  |  |
| 3.8 | The hardware specified must not exceed standard rack mount 3U size   |  |  |
| 3.9 | The hardware specified must have at least the following physical interfaces:   |  |  |
|     | a. 1x 10/100/1000 BASE-T to act as an administration interface   |  |  |
|     | b. 1x 10/100/1000 BASE-T to act as a remote management interface   |  |  |
|     | c. 3x 10/100/1000 BASE-T to act as copper interfaces for traffic analysis  |  |  |
|     | d. 2 x 10Gbe/1Gbe SFP+ to act as analysis ports SFP+   |  |  |

|                        |   |  |  |
|------------------------|---|--|--|
| 3.10                   | The hardware specified must have a redundant power supply   |  |  |
| Support and Assistance |   |  |  |
| 4.1                    | The solution must have an online portal available for client access by providing at least:  |  |  |
|                        | a. two factor authentication  |  |  |
|                        | b. pre-scheduled quarterly training sessions, without additional cost on the use of the solution and any new functionalities.   |  |  |
|                        | c. a complete library of solution documents, as well as specific fields where the latest product updates, release notes, and FAQs can easily be validated   |  |  |
|                        | d. contains specific feature for the opening of support tickets, which enables fast, simple opening and case detailing. All ticket updates must be updated in the system and be forwarded via email and must have a complete call history track.              |  |  |
|                        | e. it must have fields of debate about Cyber Threats and publications of security experts about current questions.  |  |  |
| 4.2                    | The solution must provide helpdesk / diagnostic and remote support for issues   |  |  |
| 4.3                    | Manufacturer of the Proposed Solution should also have a SOC Facility and should provide Proactive Cyber Assistance. Please submit necessary Document which proves the availability of SOC Facility in the form of Service Brochure/Data Sheet or a document. |  |  |
| WARRANT and SUPPORT    |   |  |  |
| 1                      | Warranty: Three (3) years warranty for Hardware and Software.   |  |  |
| 2                      | Support service shall include:  |  |  |
| 3                      | 1. Helpdesk   |  |  |
| 4                      | 2. Software Updates   |  |  |
| 5                      | 3. Hardware Support   |  |  |

|            |  |  |  |
|------------|--|--|--|
| 6          | All software to be supplied/ delivered and installed must be of the latest version and should form part of the OEM's current product line. |  |  |
| 7          | The Solution End of life shall be not less than 5 years  |  |  |
| Deployment |  |  |  |
| 1          | The Solution shall include Deployment and Implementation services by the OEM and the preferred local partner                               |  |  |

| No.  | Requirement Description  | Comply (Yes/No) | Bidder's compliance statement and page reference |
|--|--|-----------------|--|
| <b>EMAIL SECURITY</b>                          |  |                 |  |
| <b>Technical Requirements of the Solution.</b> |  |                 |  |
| 1  | The solution must be an API-based email security platform capable of continuously learning, detecting, and remediating advanced threats at the mailbox level, before and after email delivery.   |                 |  |
| 2  | The solution should be based on probabilistic mathematical methods, analysing and correlating distinct dimensions (confirm total # of distinct dimensions)   |                 |  |
| 3  | The Proposed Solution should come with a minimum subscription/support period of 36 months from Day-1 of Deployment.  |                 |  |
| 4  | Behavioural Learning Within Email Layer: The proposed Solution should have this in-built functionality accessible via the integrated Platform single login   |                 |  |
| 5  | The solution must also have the inherent ability to provide an autonomous response module that acts against email-borne attack campaigns. It must then be hosted on a dedicated instance that integrates with the existing behavioural based network monitoring tool installed onsite to provide insight and control over email activity. This insight must establish the correlation of the network to the email platforms.   |                 |  |
| 6  | The solution must passively operate to extract metrics and meta data from the email traffic & platform - to develop a 'normal concept' for email activity. This email solution must use absolutely no rules, signatures, or historical data to detect & neutralize threats, and must be purely based on machine learning and systemic mathematics. By correlating data across email and network traffic, this must allow the solution to evaluate the level of threat posed by an email and to spot unusual, anomalous emails that have bypassed any existing email gateway tools. |                 |  |

|      |  |  |  |
|------|--|--|--|
| 7    | All data ingested by the mail capability must be completely encrypted in transit and at rest within the solution's own form of cloud service or requested service of the current deployed platforms  |  |  |
| 8    | All data retention policies must be able to be fully controlled by the necessary client and can be configured via the systems own built in platforms.  |  |  |
| 9    | The network monitoring part of the solution will need to communicate with the email protection platform to provide it with sufficient information to detect and respond to anomalous email activity. Communications between the two will need to supply information to the network to enable it to respond to email borne threats and to provide additional contextual information to users in the overall User Interface. |  |  |
| 10   | The telemetry data that is exchanged between the network part of the solution and the email platform must be limited to the following:   |  |  |
| 10.1 | a) Probabilistic data structures which describe the pattern of activity, the solutions rarity and frequency scores of visited hosts, domains, file hashes and links seen in the platforms monitored environment. These data structures do not include any of these details in an extractable format  |  |  |
| 10.2 | b) Hostname, IP, MAC address, Operating system, Device label and time of last seen are transferred   |  |  |
| 10.3 | c) Solution Alert information. Notifications of Alerts occurring as a result of anomalous network activity may be transferred to the email platform instance and/or select email data may be transferred to the network for the purposes of security forensics.  |  |  |
| 10.4 | Email addresses, naming, and groups found in emails and any associated email repositories.   |  |  |
| 11   | Access to Email Platform by the vendor must be limited to the following purposes only:   |  |  |
| 11.1 | a) Initial set up, configuration and traffic validation  |  |  |
| 11.2 | b) Access for the creation of customer reports (as part of trial, or as an on-going service agreement)   |  |  |
| 11.3 | c) Security incidents  |  |  |
| 12   | All email data access must be logged and controlled. Logs of all data access must be available through the audit page in the interface, an essential capability needed in the UI. The body content of original emails received must not be available to the manufacturer personnel through the interface and emails must be individually encrypted.  |  |  |

|      |  |  |  |
|------|--|--|--|
| 13   | Advanced Malware & URL Protection, Mailbox-Level BEC Protection (including CEO and Employee Impersonations Spear Phishing and Credential Theft, Supply Chain Attacks   |  |  |
| 14   | The solution must have an online portal available for client access by providing at least:   |  |  |
| 14.1 | a) Two factor authentication   |  |  |
| 14.2 | b) Pre-scheduled periodic training sessions, without additional cost   |  |  |
| 14.3 | c) A complete library of solution documents, as well as specific fields where the latest product updates, release notes, and FAQs can easily be validated  |  |  |
| 14.4 | d) Contain specific feature for the opening of support tickets, which enables fast, simple opening and case detailing. All ticket updates must be updated in the system and be forwarded via email   |  |  |
| 14.5 | e) It must have fields of debate about Cyber Threats and publications of security experts about current questions.   |  |  |
| 15   | The solution proposed must provide helpdesk / diagnostic and remote support for issues   |  |  |
|      |  |  |  |
|      | <b>Integration</b>   |  |  |
| 16   | Solution must provide integration with both cloud (azure) and on prem Active Directory for recipients address validation   |  |  |
|      |  |  |  |
|      | <b>Reporting and Log Search</b>  |  |  |
| 17   | Real-time reporting capabilities   |  |  |
| 18   | Dashboard visibility into message logs   |  |  |
| 19   | System reporting   |  |  |
| 20   | Email Virus detection/stoppage reporting   |  |  |
| 21   | Spam Detection reports   |  |  |
| 22   | Must provide report scheduling capabilities  |  |  |
| 23   | Must provide reports that list changes/updates to the system occurring in real-time  |  |  |
| 24   | Reports must be exportable in multiple formats   |  |  |
|      |  |  |  |
|      | <b>Manageability</b>   |  |  |
| 25   | System overview dashboard - Monitor and report on outbound messages from a centralized, custom system overview dashboard. Unified business reporting with a single view for comprehensive insight across your organization. Get the details of any report for advanced visibility. |  |  |

|    |   |  |  |
|----|---|--|--|
| 26 | Detailed message tracking - Track a message by envelope recipient, envelope sender, subject, attachments                            |  |  |
|    |   |  |  |
|    | <b>Summary of Capabilities:</b>   |  |  |
| 27 | Virus inspection/protection   |  |  |
| 28 | Malware inspection/protection (including malformed web addresses)   |  |  |
| 29 | Phishing inspection/protection  |  |  |
| 30 | Attachment inspection/protection  |  |  |
| 31 | Detection of Data Loss  |  |  |
| 32 | Sender ID checks  |  |  |
| 33 | Protection against malicious URLs   |  |  |
| 34 | Protection against executable files (direct or compressed), malicious code, scripts, and malformed web addresses                    |  |  |
| 35 | Centralized management  |  |  |
| 36 | Whitelisting/blacklisting capabilities (Per user or globally)   |  |  |
| 37 | Alert, notification, summary dashboards, built-in reporting and blocking  |  |  |
| 38 | Deep email header inspection  |  |  |
| 39 | Advanced detection against targeted email attacks like spear phishing attacks, zero-day attack and exploits,                        |  |  |
| 40 | Detection of C-level impersonation  |  |  |
| 41 | Detection of public contact addresses   |  |  |
| 42 | Detection of unusual topics for internal staff  |  |  |
| 43 | Detection of internal staff compromise via outbound mail inspection   |  |  |
| 44 | Detection of suspicious new supplier language   |  |  |
| 45 | Geolocation and detection of unusual emailing locations   |  |  |
| 46 | Autonomous grouping of high-volume email campaigns  |  |  |
| 47 | Ability to filter with unlimited complexity   |  |  |
| 48 | Detect phishing links in QR codes   |  |  |
| 49 | DLP detection that require no predefined rule sets.   |  |  |
| 50 | Integration with Microsoft quarantine that will permit security end users to release email using native Microsoft quarantine tools. |  |  |

Note: Prospective bidders are also encouraged to submit any alternative proposals (if any) which they feel will better suit the situation at Hessequa Municipality along with the proposal which is in line with the above minimum specifications.

#### 4 Technical Evaluation of Responses to this RFT

The factors that are considered important by the municipality include, but are not limited to, the following. (**Note:** no order of importance, weighting, or other priority is assigned to these factors or reflected by their order in the list.)

- Project understanding and soundness of the proposed solution, including the detail and accuracy of the proposed solution.
- References provided by the respondent, particularly from projects of similar complexity and scope.
- The cost proposal, including long-term costs of the solution, recurring maintenance and support costs, and other fees.
- Compliance with RFT requirements, including, but not limited to, the ability of the specific solution (design(s), equipment, software and services) proposed to satisfy the RFT's functional, performance, and other requirements for the solution.
- The ability to add to the skills base of the region through skills training and technology transfer.
- Presentation of evidence of the ability to comply with all the usual business probity conditions associated with being a vendor to a government entity.
- Any other factors the municipality considers relevant to the evaluation of the proposal.

#### 5 Requirements and Response Section

Respondents to this RFT must follow exactly the format presented in this section.

Respondents are required to define their proposed solution in appropriate detail and to describe the ways in which it meets the requirements defined in the RFT. Respondents are also required to define and elaborate on any other features, functions and/or capabilities included in their proposals, but not stated as requirements in the RFT.

##### 5.1 GENERAL INFORMATION

###### 5.1.1 Contact Information

Provide the name, title, address, telephone and Email address for the primary contact for this tender

Name

Title

Address

Telephone

E-Mail

###### 5.1.2 Consortium

State all the members of your bidding consortium and indicate if applicable the primary and secondary contractors and their roles in the implementation e.g.

Initials of Service Provider's Authority: .....

| Vendor | Status               | Role                              |
|--------|----------------------|-----------------------------------|
| AAA    | Primary              | Legally responsible for project   |
| BBB    | Software Partner     | Active partnership or consultancy |
| CCC    | Hardware Partner     | Hardware Supplier                 |
| DDD    | Secondary Contractor | Document defines agreement        |
| EEE    | Secondary Contractor | Document defines agreement        |

Note: accreditation and partnership agreements must be attached.  
Please complete the following:

| Vendor | Status  | Role |
|--------|---------|------|
|        | Primary |      |
|        |         |      |
|        |         |      |
|        |         |      |

## 5.2 Contract Award

While it is the preferred option of the municipality to award this contract to a single bidder, it is a mandatory condition that bidders accept and acknowledge that the municipality reserves the right to:

- Not award this tender in its entirety.
- Award this tender in part.
- Negotiate prices with the preferred bidder within the constraints of the budget. (exp. call cost)

Please indicate below that you understand and accept this condition.

|                       |               |
|-----------------------|---------------|
| Understand and Accept | Do not accept |
|                       |               |

**Note that if you do not accept this condition, your response will be marked as non-responsive and will not be evaluated further.**

## 5.3 Solution proposed

### 5.3.1 Executive Summary

Outline the broad approach and technical solution(s) that you propose will meet these projects goals. Respond in the text box below.



### 5.3.2 Detailed Design

Respondents are required to specify in detail how the solution will be designed and how proposed connectivity to each location will be achieved.

Respond in the text box below. Use tables and diagrams if necessary.

### 5.4 Procurement and Installation Services

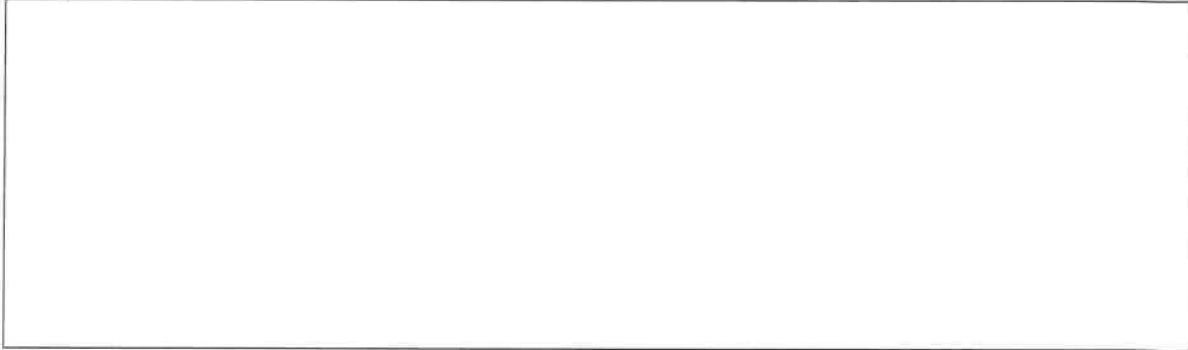
Respondents should describe how the installation and configuration services required for the successful deployment of the proposed solution would be provided. This should include, but not be limited to, the following:

- The installation and configuration of the proposed solution and all network components, computers, servers, access points, routers, bridges, managed switches and other network equipment.
- Coordination with the municipality and any other parties required for access to any of the beforementioned cognizant of any internal ICT governance compliance procedures.

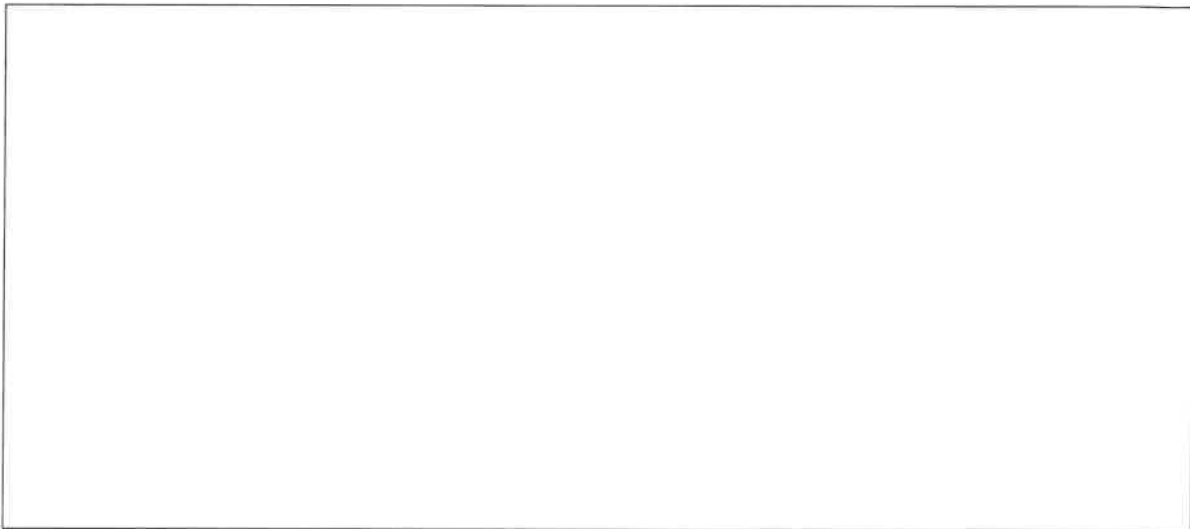
Initials of Service Provider's Authority: .....

- The ramp-up and activation of all services defined as requirements in this RFT, to include but not be limited to customer service, technical support, hosting, network security & performance monitoring and email security solutions, processes and personnel.
- The configuration and integration of all components in the network to meet the requirements defined in this RFT.

Respond in the text box below.



Include a project plan and discuss how you will meet the timeframes required by the municipality i.e. that services must be available from 1 July 2026. If you believe that these timeframes are unrealistic, please explain why and propose your suggested timeframes.



## **5.5 Scalability**

Indicate the scalability of the proposed solution to accommodate growing requirements (exp. additional licences, devices, servers, ect.)? Please discuss in more detail below including issues like timeframes, cost, etc.

### 5.6 Network Performance Monitoring & Management Services

Respondents should explain how the proposed network & email solutions would be monitored and managed. At a minimum, please define and elaborate on how the proposed solution addresses the five ISO network management functions summarized below.

- **Performance Management** – Measures and makes available various aspects of network performance so that inter-network performance can be maintained at an acceptable level. Examples of performance variables that might be provided include, but are not limited to network throughput, user response times, and component utilization.
- **Configuration Management** – Monitor network and solution configuration information so that the effect of configuration changes (intentional or non-intentional) can be tracked and managed.
- **Accounting Management** – Measure network-utilization parameters so that individual or group users on the network can be regulated appropriately. Such regulation should minimize network problems and maximize the fairness of network access across all domains and users.
- **Fault Management** – Detect, log, notify support organizations and users (where appropriate) of, and (to the extent possible) automatically fix network problems to keep the network running effectively. This should include proactive determination of symptoms, isolation of problems and rapid resolution.
- **Security Management** – Control access to network and solution resources according to defined policies so that the network cannot be sabotaged (intentionally or unintentionally) and those without appropriate authorization cannot access sensitive information.

Please note that the successful vendor will be expected to provide statistical /traffic reports or equivalent graphs/logs (daily, weekly, monthly and yearly statistics) about traffic across network.

As part of the bid, reference the solution name and sample responses/screenshots of the monitoring solution used for abovementioned reporting. Also discuss if and how your solution complies with industry standards. All relevant information will need to be securely retained for a period specified by the municipality for audit and analysis purposes.

Respond in the text box below.

Initials of Service Provider's Authority: .....

**5.7 Customer Service and Technical Support Services****5.7.1 Respondents should explain their approach to the provision of customer service and technical support via a call center or other mechanism.**

This should be capable of handling:

- Billing, invoice, and/or settlement charges between the municipality and the service provider, if used (customer service issues).
- Technical problems reported by users (technical support issues).

Other aspects of the customer service mechanism that the vendor will be expected to provide are:

- The ability to also report an issue and obtain a resolution via e-mail, web-based interface and instant messaging (IM).
- Availability of a dedicated technical expert, with knowledge of and capability to resolve all technical aspects of the network or email, should be available on a telephone or cellphone basis, 24x 7x 365.
- Proactive notification network or email problems, outages and other issues affecting the solution via e-mail and web interface is expected.
- The development, maintenance and hosting of a library containing electronically available frequently asked questions ('FAQs') to aid in self-support will be an advantage.
- A secure, managed database of all call tracking detail, resolutions, etc. This should be fault tolerant and backed up on a regular schedule and should allow secure login from private residences by municipality officials.
- The creation and delivery of pre-defined and event-related ad-hoc reports on access issues wait times, abandoned calls, resolution times and other standard customer service and technical support metrics.

Respond in the text box below.

**5.7.2 Additional aspects of support**

In addition to the requirements stated above, respondents are encouraged to elaborate in their proposals on the following issues:

- Estimates for Service Level Agreements (SLAs): call response times, issue resolution times, and similar obligations that can be committed to by the respondent.
- Any additional features and functions supported by their customer service offering.
- Any preliminary call and support process flows including escalation.
- Any additional features for knowledge management and/or other technologies that will result in improved customer service and technical support.

Respond in the text box below.

**5.8 Presentation**

The municipality may request a functional evaluation of the written response to this RFT based on the scope of this tender covered under section 2.1 with specific reference to the minimum technical requirements.

**5.9 Reference Site Inspections**

The municipality may, at its sole discretion contact any of the provided references of the respondent's work at one or more sites where the respondent's and/or a proposed subcontractor's products are installed, or services have been provided. Please provide a list of reference sites in the following text box.

Respond in the text box below.

**5.10 Credible Solution Provider****5.10.1 Company Background**

Year and country of incorporation.

|  |
|--|
|  |
|--|

Provide appropriate general business background information to substantiate your credibility as a competent solution provider in response to this tender. Respond in the textbox below.

|  |
|--|
|  |
|--|

**5.10.2 Key Subcontractors**

Please give the name of any key subcontractors that you envisage using to implement your recommended solution, and their role in the implementation

| Partner | Role |
|---------|------|
|         |      |
|         |      |
|         |      |

**5.10.3 Current Customers:**

Provide a general description of your client base. Highlight any clients to whom you have provided similar implementations of the proposed solution. Please indicate:

- Scale: Number of customers and customer user base
- Location: Geographic distribution of customers: local (Western Cape), national (South Africa) & international.
- Potential, if any, for any conflict of interest arising between an existing customer and the municipality.

Respond in the text box below.

**5.10.4 Experience:**

List your experience with organisations with a similar profile to the municipality i.e. provincial government, local government, utilities, or another public sector. Respond in the text box below.

**5.10.5 Staff Experience:**

Please list the key staff that you will allocate to this project and their experience relevant to this assignment. Respond in the text box below.

**5.10.6 Geographic Coverage:**

Provide a description of your presence (e.g. Head office, distributor, agent, resource base) internationally, in South Africa, and in the Western Cape specifically.)

Initials of Service Provider's Authority: .....

Respond in the text box below.

**5.10.7 Client References:**

Provide at least three contactable references of previous customers where your company has implemented a similar solution to that which you are proposing for the municipality. Ideally these should be organisations of similar scale and complexity as the municipality.

Please include:

- A short description of the solution implemented including products used, number of users and the exact role that your organization played (be specific).
- The length of time taken to implement the solution in calendar days.
- Name any critical subcontractors or alliance partners that worked with you on these projects.

Respond in the text box below, and/or insert supporting documentation in the hard copy of your response after this page.

**5.10.8 Other Relevant Experience:**

List any other relevant experience in associated or related industry sectors. Respond in the text box below.



**Failure to provide the information as stated above tables, will result in your tender being declared non-responsive.**

DECLARATION,

I, THE UNDERSIGNED (NAME).....  
CERTIFY THAT THE INFORMATION FURNISHED ABOVE IS CORRECT. I ACCEPT THAT THE MUNICIPALITY MAY ACT  
AGAINST ME SHOULD THIS DECLARATION PROVE TO BE FALSE.

AUTHORISED SIGNATURE: .....

NAME: .....

CAPACITY: .....DATE: .....

Initials of Service Provider's Authority: .....