REQUEST FOR PROPOSAL
Bid Number: 2026/26

Bid Description: Implementation and Support of a Network Detection and Response solution for a period of three (3) years

Closing Date: 28 September 2026

Closing Time: 12h00 pm

Submission: via Sasria's e-tender portal, click https://procurement.sasria.co.za/

Table of Contents

1. Part 1 - Letter of Invitation 3
2. Part 2 - Instructions 4
   2.1 Sasria 4
   2.2 Contractual commitment 4
   2.3 Confidentiality 4
   2.4 Submission Format (Returnable Schedules) 4
   2.4.1 Schedule 1: 5
   2.4.2 Schedule 2 5
   2.4.3 Schedule 3: 5
   2.4.4 Schedule 4: 5
   2.5 Submission of Bids 5
   2.6 Queries and clarifications 6
   2.7 Reasons for Disqualification or Non- Award 6
   2.8 Sasria's Rights 6
   2.8 Ethical Dealings 8
   2.9 Proposal costs 7
   2.10 Validity period 7
   2.11 Important dates 7
   2.12 Transformation 7
3. Part 3 - RFP Requirements 9
   3.1 Special Instructions 9
   3.2 Background Information 9
   3.3 Scope of Work 10
   3.4 Contract Duration 12
4. Part 4 - Financial Proposal 12
5. Part 5: Qualification and Evaluation Criteria 19
   5.1 Evaluation of proposals 19
   5.2 Evaluation Criteria 19
      5.2.1 Level 1- Governance Verification 19
      5.2.2 Level 2- Technical Evaluation 19
      5.2.3 Level 3 – Preference Point System 20
6 Part 6 – Required Documents 25

ANNEXURE A: CONFIDENTIALITY AND NON DISCLOSURE AGREEMENT 26
ANNEXURE B: ACCEPTANCE OF BID CONDITIONS AND BIDDER'S DETAILS 38
ANNEXURE C: SHAREHOLDER INFORMATION 41
ANNEXURE D: BIDDER'S EXPERIENCE AND PROPOSED PROJECT TEAM 0

1. Part 1 - Letter of Invitation

To the Service Provider:

Sasria SOC Limited hereby invites proposals from capable service providers for the implementation and support of a Network Detection and Response Solution for a period of 36 months.

A service provider will be selected under the procedures described in this Request for Proposal (RFP) document.

The RFP consists of the following documents:

- Part 1 – Letter of Invitation
- Part 2 – Instructions
- Part 3 – RFP Requirements
- Part 4 – Financial Proposal
- Part 5 – Pre-Qualification and Evaluation Criteria
- Part 6 - Required Documents
  - Annexure A: Confidentiality and Non-disclosure Agreement;
  - Annexure B: Acceptance of Bid Conditions;
  - Annexure C: Shareholder Information
  - Annexure D: Bidder's Experience and proposed project team
  - Invitation to Bid (SBD 1): SBD1 is the entire RFP document filled and signed.
  - Disclosure and Declaration (SBD 4);
  - Specific Goal Declaration Form (SBD 6.1)

Note: Failure to provide any one of the documents required may lead to an immediate disqualification of the service provider from the tender process.

Consent to Processing of Personal Information.

In submitting any information or documentation requested above or any other information that may be requested pursuant to this RFP, you are consenting to the processing by Sasria or its stakeholders of your personal information and all other personal information contained therein, as contemplated in the Protection of Personal Information Act, No.4 of 2013 and Regulations promulgated thereunder ("POPI Act"). Further, you declare that you have obtained all consents required by the POPI Act or any other law applicable. Thus, you hereby indemnify Sasria against any civil or criminal action, administrative fine or other penalty or loss that may arise as a result of the processing of any personal information that you submit.

2. Part 2 - Instructions

2.1 Sasria

Sasria SOC Ltd (Sasria) is the only short-term insurer that provides special risk cover to all individuals and businesses that own assets in South Africa, as well as government entities. This is a unique cover against risks such as civil commotion, public disorder, strikes, riots and terrorism, making South Africa one of the few countries in the world that provide this insurance, particularly at affordable premiums.

As a state-owned entity, Sasria has a legislative mandate that governs day-to-day business operations and a broader strategic mandate to make a positive contribution to transformation within the Insurance industry in South Africa. Sasria's core business is the provision of short-term insurance for riots, strikes, terrorism, civil commotion and public disorder to businesses, government entities and individuals.

The Government of the Republic of South Africa, and specifically the National Treasury through the Minister of Finance, is the sole shareholder of Sasria. As such, the company has to comply with a number of legal and regulatory requirements.

Bidders are encouraged to review Sasria's latest Integrated Report, available on its website, to get a better understanding of its business operations and functions.

2.2 Contractual commitment

No commitment of any kind, contractual or otherwise shall exist unless and until a formal written agreement has been executed by or on behalf of Sasria. Any notification of preferred bidder status by Sasria shall not give rise to any enforceable rights by the Bidder. Sasria may cancel this RFP any time prior to the formal written agreement being executed by or on behalf of Sasria.

Sasria reserves the right at its sole discretion, and at any time, to amend, deviate from, postpone, discontinue or terminate the transaction/procurement process without incurring any liability whatsoever to any other party.

Sasria reserves the right not to award this tender to the highest ranked or highest scoring bidder, as it needs to align its procurement practices to governance practices that are in line with its own growth path. These may include but are not limited to: driving socio-economic development objectives that are enshrined in various government policies. Sasria is under no obligation to award the tender in full and may decide to award it in part to one or various tenderers.

2.3 Confidentiality

All bidders to this RFP will be required to sign the confidentiality and non-disclosure agreement outlined on Annexure A in this document.

2.4 Submission Format (Returnable Schedules)

Bidders are required to submit a comprehensively detailed bid responses in accordance with the submission format specified below:

2.4.1 Schedule 1:

Executive Summary (explaining how you understand the requirements of this RFP, summary of your proposed solution and the summary of your experience relevant to the requirements of this RFP)
Annexure B of this RFP document (See Part 6) (duly completed and signed)

2.4.2 Schedule 2

All documents (except Annexure B) listed on Part 6 of this RFP Document (duly completed and signed);

a) CSD report to verify tax compliance;
b) Valid B-BBEE verification certificate or Valid Sworn Affidavit or Valid Specialised Entity Sworn Affidavit. An Exempted Micro Enterprises (EME) with an annual turnover less than R10 million, is only required to obtain a sworn affidavit confirming the annual total revenue and level of black ownership. A Qualifying Small Enterprise (QSE) that has 51% or more black beneficiaries may obtain a sworn affidavit confirming the annual total revenue and level of black ownership.

Submission Requirements to Claim Points Related to Specific Goals:

1. Consortium or Joint Venture – to submit a valid consolidated B-BBEE certificate or Affidavit and a signed Consortium or Joint Venture agreement.
2. Prime Contractor with Subcontractor(s)- Prime Contractor and Subcontractor(s) B-BBEE certificates or Valid Sworn Affidavits are required and a signed subcontracting agreement
3. Individual bidder – must submit a valid B-BBEE certificate or Sworn Affidavit

2.4.3 Schedule 3:

a) Technical Proposal in line with the Technical Evaluation Criteria in Part 5 of this RFP document.

2.4.4 Schedule 4:

a) Financial/ Price Proposal in line with Part 4 of this RFP document.

2.5 Submission of Bids

The closing date and time for the submission of bids is **28 September 2026 at 12h00pm** . Bidders should click on this link https://procurement.sasria.co.za/ to be able to register on the Sasria' Online Tender Portal on or before the closing date and time in order to submit their proposals. Bidders should follow the system prompts and submit all schedules to the Online Tender Portal. All correspondence will be done via the Online Tender Portal. Should bidders not be able to register, they should send the email to Procurement@sasria.co.za for assistance. It is the bidder's responsibility to familiarise themselves with our Online Tender Portal well before the tender close.

It is the bidder's responsibility to ensure that the bid is submitted as directed above and that the submission is received by Sasria before the closing date and time. Therefore, bidders are advised to allow adequate time for submission of bids through Sasria Online Tender Portal to mitigate against any possible technical challenges, which may result in delays in submission of bid responses.

Please note that Sasria Online Tender Portal is configured to receive electronic documents of maximum size of 4MB per file and each Schedule is limited to 30MB. The bidder will not be able to submit a bid unless all four (4) Schedules are completed.

Sasria will not enter into any negotiations regarding bids that could not be submitted on time through the Sasria Online Tender Portal. Sasria will take no responsibility for failure by the bidder to submit their bid response on time due to technical challenges of any sort.

NB: Hand delivered, posted, emailed, or faxed proposals will NOT be accepted or considered for evaluation.

2.6 Queries and clarifications

For all queries and clarifications regarding this Request for Proposal, bidders should click on this link https://procurement.sasria.co.za/ and go to Queries on the portal.

2.7 Reasons for Disqualification or Non- Award

Sasria reserves the right to disqualify / not award a contract to a bidder for one or more of the following reasons, and such disqualification may occur without prior notice to the offending bidder:

failed to provide proof that they are tax compliant with SARS;

submitted incomplete information and documentation according to the requirements of this RFP document; submitted information which contains fraudulent, factually untrue or inaccurate information; received information not available to other potential bidders through fraudulent means;

ailed to comply with mandatory requirements if stipulated in the RFP document;

misrepresented or altered material information in whatever way or manner;

- promised, offered or made gifts, benefits to any Sasria employee;
- canvassed, colluded or lobbied in order to gain unfair advantage;
- committed fraudulent acts;
- will cause perceived or actual reputational, financial or operational risk to Sasria;
- appears in National Treasury's list of restricted / defaulters register;
- prohibited to do business with state organs;
- the bidder is prohibited to do business with the State; and
- acted dishonestly and/or in bad faith etc.

2.8 Ethical Dealings

The Bidder confirms that it is not involved in any form of unethical business practices and hereby warrants that it shall adhere to all ethical standards required of it by virtue of the professional nature of its business.

2.9 Sasria's Rights

Sasria reserves the right to:

- Amend any bid conditions, bid validity period, RFP specifications, or extend the bid closing date, all before the bid closing date. Such amendments will be posted on the Sasria's Tender Portal under Announcements. All prospective bidders should therefore ensure that they visit the website regularly before they submit their bid response to ensure that they are kept updated on any amendments in this regard.
- Award this bid as a whole or in part or not make an award at all.
- Award this bid to more than one bidder.
- Negotiate with all or some of the shortlisted bidders.
- Not accept the lowest priced bid.
- Conduct site visits at bidder's offices and / or at client sites if so required.
- Request any relevant information and/ or documents to verify or clarify information supplied in the bid response in relation, but not limited, to the structure of the bidding entity, bidder's capacity, bidder's B-BBEE profile, Specific Goals, proposed solution, proposed timelines etc.
- Not release information of another bidder that may be considered proprietary, sensitive or confidential
- To restrict a company or person from doing business with the State for a period not exceeding 10 years.

By submitting a bid, the bidder hereby gives consent to Sasria to conduct any form of vetting or due diligence in relation to this tender on the bidding entity and/ or any of its directors / trustees / shareholders / members.

2.10 Proposal costs

All costs and expenses incurred by the bidder relating to their participation in, and preparation of this proposal process shall be borne by the bidder exclusively.

2.11 Validity period

The proposals should remain valid for at least 150 days after the closing date.

2.12 Important dates

Activity	Date
Release of RFP	7 September 2026
Last day of enquiries	22 September 2026
Responses to enquiries	23 September 2026
Closing date and time for submission of proposals	**28 September 2026 at 12h00pm**
Submission Method	Via Sasria's Online Tender Portal: https://procurement.sasria.co.za/

Sasria reserves the right to amend any date specified above. Any changes will be communicated to the interested parties via our Tender Portal.

2.13 Transformation

Sasria promotes transformation in the financial services and other sectors of the South African economy and as such, bidders are encouraged to partner with majority black owned entities (51% black owned and controlled) and businesses that are small to medium sized. Such partnerships may include the formation of a Joint Venture and/ or subcontracting agreement etc., where a portion of the work under this tender would be undertaken by black owned entities. To give effect to this requirement, bidders are required to submit a partnership /

subcontracting proposal detailing the portion of work to be outsourced, level of involvement of the black owned partner and where relevant, submit a consolidated B-BBEE scorecard.

3. Part 3 - RFP Requirements

3.1 Special Instructions

Should a bidder have reason to believe that the Functional Requirements are not open / fair and/or are written for a particular service provider; the bidder must notify Sasria Procurement within five (5) days after publication of the RFP.

3.2 Background Information

Sasria SOC Limited invites proposals from suitably qualified and experienced service providers for the provision, implementation, and support of an enterprise-grade Network Detection and Response (NDR) solution.

As part of its ongoing commitment to strengthening its cybersecurity posture and protecting organisational, stakeholder, and customer interests, Sasria requires an advanced Network Detection and Response solution capable of detecting, investigating, prioritising, and supporting the response to cyber threats across its network, cloud, identity, and hybrid technology environments.

The solution must provide comprehensive visibility into network activity across Sasria's infrastructure, including on-premises, cloud, remote-access, and hybrid environments. It should enable the identification of malicious behaviour, suspicious communications, lateral movement, command-and-control activity, credential misuse, insider threats, ransomware activity, and other advanced attack techniques that may bypass traditional security controls.

The solution will support Sasria's IT Security and Security Operations functions by delivering continuous monitoring, real-time threat detection, behavioural analytics, and actionable threat intelligence. The solution must correlate security events and network activity to provide contextualised threat insights, enabling rapid investigation, prioritisation, containment, and remediation of security incidents while minimising false positives and alert fatigue.

In addition, the solution must align with applicable regulatory and legal requirements, including the Protection of Personal Information Act (POPIA), ensuring that all data collection, processing, storage, and reporting activities are conducted in a lawful, ethical, and secure manner. Consideration must also be given to data residency, data protection, and privacy requirements relevant to a South African public-sector entity.

The proposed solution must integrate seamlessly with Sasria's existing security ecosystem, including Microsoft Sentinel, security monitoring platforms, incident response tools, identity services, endpoint security solutions, and ticketing systems through standard APIs, connectors, and supported integration frameworks. The solution should support automation and orchestration capabilities to enhance incident response and operational efficiency.

The service offering may include a combination of software, cloud services, appliances, professional services, and managed support services and must be delivered as a secure, scalable, resilient, and highly available solution suitable for enterprise and public-sector environments. The solution must meet defined service level requirements, including system availability, operational performance, support responsiveness, and ongoing optimisation.

Key capabilities required include, but are not limited to:

- Continuous network monitoring and visibility across on-premises, cloud, and hybrid environments
- Behavioural analytics and AI-driven threat detection capabilities
- Detection of advanced threats, lateral movement, command-and-control communications, privilege abuse, and insider threats
- Real-time threat prioritisation and risk-based alerting
- Network, identity, cloud, and Microsoft 365 threat correlation
- Threat investigation, threat hunting, and historical forensic analysis capabilities
- Integration with Microsoft Sentinel and other security monitoring platforms
- Support for incident response workflows, case management, and automated response actions
- Secure handling of sensitive information, including encryption, audit logging, and role-based access controls
- Compliance with applicable regulatory frameworks, including POPIA and recognised information security standards
- Comprehensive reporting, operational dashboards, executive threat reporting, and security posture insight

The successful service provider will be expected to provide implementation services, solution configuration, integration, testing, training, knowledge transfer, and comprehensive documentation. The service provider must also provide ongoing technical support, maintenance, software updates, optimisation services, and access to suitably qualified technical resources for the duration of the contract.

The duration of the contract will be three (3) years, inclusive of implementation, support, maintenance, and ongoing operational services.

3.3 Scope of Work

The scope of work defines the deliverables to be provided by the successful Bidder.

No.	Deliverable	Description
1	**Implementation of Network Detection and Response Solution**	The service provider shall provide, implement, configure, and optimise an enterprise-grade Network Detection and Response (NDR) solution. The solution must provide continuous visibility across network, identity, cloud, and SaaS environments; AI-driven behavioural threat detection; entity-based threat prioritisation; attack correlation; threat investigation; threat hunting; and response capabilities across Sasria's on-premises, cloud, and hybrid environments. A detailed implementation plan must be provided, including design, deployment, configuration, testing, integration, go-live, and transition activities.
2	**Training and Knowledge Transfer**	The service provider shall provide role-based training and supporting documentation covering solution administration, monitoring, threat investigation, threat hunting, attack analysis,

		reporting, and incident response processes. Knowledge transfer must enable designated Sasria personnel to effectively operate, manage, and maintain the solution.
3	**Hosting Model**	The solution may be delivered through a secure cloud-hosted Software-as-a-Service (SaaS) model, on-premises deployment, or hybrid architecture. The bidder must provide details of the hosting environment, security controls, data protection measures, availability commitments, disaster recovery capabilities, and applicable compliance certifications or standards.
4	**Network, Identity, Cloud and Microsoft 365 Visibility Onboarding**	The service provider shall configure and onboard network telemetry, east-west and north-south traffic visibility, cloud environments, identity services, Microsoft 365 data sources, and other relevant telemetry required for effective threat detection and monitoring. The solution must establish behavioural baselines and support continuous monitoring, analysis, and threat detection.
5	**Project Management**	The service provider shall apply a structured project management methodology with clearly defined phases, deliverables, timelines, milestones, risks, and responsibilities. The service provider must align with Sasria's project governance and reporting requirements throughout the implementation lifecycle.
6	**Technical Solution Documentation**	The service provider shall provide comprehensive technical documentation describing the proposed solution architecture, deployment model, data flows, behavioural detection methodologies, threat prioritisation capabilities, security controls, integrations, operational procedures, and administrative functions.
7	**Solution Configuration, Support and Maintenance**	The service provider shall perform initial configuration and provide ongoing support and maintenance services for the duration of the contract. Services must include platform maintenance, software updates, threat detection content updates, issue resolution, technical support, solution optimisation, and periodic health reviews in accordance with agreed service levels.
8	**Testing and Validation**	The service provider shall perform testing to validate solution functionality, behavioural threat detection capabilities, cloud and identity

		monitoring, integrations, alerting mechanisms, dashboards, reporting, and response workflows. Testing must include system testing, performance testing, integration testing, threat simulation testing, and user acceptance testing prior to production deployment.
9	**Integration Capabilities**	The solution must support integration with enterprise security and operational platforms through APIs, connectors, or supported integration frameworks. The bidder must demonstrate integration capabilities with Microsoft Sentinel, Microsoft Defender, Microsoft Entra ID, Microsoft 365, SOAR platforms, ITSM solutions, identity providers, firewalls, endpoint security platforms, ticketing systems, and other relevant security technologies.
10	**Detection, Investigation and Reporting Capabilities**	The service provider shall demonstrate how the solution supports threat detection, behavioural analytics, attack correlation, entity prioritisation, threat hunting, incident investigation, attack-chain visibility, and response workflows. The solution must provide operational dashboards, executive reporting, threat intelligence context, and actionable insights to support effective cybersecurity operations and decision-making.
11	**AI-Driven Threat Prioritisation and Attack Correlation**	The solution shall automatically correlate related attack activities across network, identity, cloud, and SaaS environments and prioritise threats based on risk, confidence, severity, and business impact. The solution must provide contextual attack visualisation, attack-chain analysis, and entity-based risk scoring to reduce alert fatigue and improve analyst efficiency.
12	**Investigation Workflows and Threat Intelligence Handling**	The service provider shall demonstrate how the solution supports end-to-end threat investigation workflows, including threat detection, alert prioritisation, incident triage, threat intelligence enrichment, attack correlation, analyst workflows, historical investigation, threat hunting, reporting, and integration with SIEM, SOAR, APIs, and ticketing platforms to enable both automated and manual response actions.

3.4 Contract Duration

The appointed Service Providers will be required to start immediately after signing the contract. The implementation period should preferably be between 1 and 2 months, and from month 3, the solution should be fully operational.The service provider will deliver the Network Detection and Response for a total period of three (3) years, inclusive of implementation, and

subject to periodic performance and service reviews by Sasria to ensure ongoing alignment with risk management, compliance, and operational requirements.

4. Part 4 - Financial Proposal

1 Bidders are required to provide a detailed and comprehensive price proposal i.e. all costs associated the bidder's proposal must be clearly specified and included in the Total Bid Price.

2 All prices must be VAT exclusive and must be quoted in South African Rand (ZAR).

Is the proposed bid price linked to the exchange rate?	Yes	No
If yes, the bidder must indicate CLEARLY which portion of the bid price is linked to the exchange rate:		

3

Payments will be linked to specified deliverables after such deliverables have been approved by Sasria.	Comply	Not Comply

4

Sasria reserves the right to consider the guidelines on consultancy rates as set out in the **National Treasury Instruction 01 of 2024/2025: Cost Containment Measures**, where relevant. The bidder must indicate if their proposed rates are in line with the provisions of the referenced National Treasury Instruction: Cost Containment Measures.	Comply	Not Comply
Substantiate / Comments		

5 PRICING MODEL

5.1 Implementation Costs

Activity/ Deliverable	Resource(s)	Rate/ Hour per resource	Number of hours	Total Cost (VAT Excl.)
Implementation				

Activity/ Deliverable	Resource(s)	Rate/ Hour per resource	Number of hours	Total Cost (VAT Excl.)
Customisation / development / configuration / Integration				
Testing				
Training				
Other Costs (if applicable)				

Activity/ Deliverable	Resource(s)	Rate/ Hour per resource	Number of hours	Total Cost (VAT Excl.)
Disbursements				
Sub-Total (5.1) (VAT Excl.)				

Note: The proposed Total Annual Fee must be inclusive of all required services as outlined in the scope of work (Part 3) above.

5.2 Hosting Costs

Hosting		Total Costs (VAT Excl.)
Year 1		
Year 2		
Year 3		
Sub-Total (5.2) (VAT Excl.)		

5.3 Software Costs (if applicable)

Pricing Instruction: Bidders must provide pricing for the full **36-month (3-year)** contract period. Unit prices must reflect the total cost for the entire contract term, inclusive of all software licensing, subscriptions, support, maintenance, updates, and associated services.

Description	Licence Metric	Quantity	Unit price	Total Cost (VAT Excl.)
Network Detection and Response (NDR) Subscription	Monitored IP Addresses	1000		
Identity, Cloud and Microsoft 365 Detection	Enterprise Subscription	1		
End-to-End Attack Correlation and Threat Visibility	Enterprise Subscription	1		
Threat Intelligence and Expert Advisory Service	Annual Subscription	1		
Proactive Threat Notification Service	Annual Subscription	1		
Physical / Virtual Sensor Appliance	Appliance	1		
Once-off Costs				
Sub-Total (5.3) (VAT Excl.)				

Note: The price proposal must inclusive of all software related costs. The bidder must provide a detailed breakdown of all elements which make up the cost of the proposed software e.g. software license structure, services included in the license, number of licenses etc.

5.4 Post-Implementation Support and maintenance

Sasria requires a fixed cost on system maintenance and support. The service provider will be required to provide support on a need basis. For comparison purposes, bidders must provide cost for 40 hours of support per month over a period of Three (3) years, the hours will be billed based on Time and Material:

Activity/ Deliverable		Monthly Hours	Annual Hours	Rate per Hour (VAT Excl.)	Monthly Fee (VAT Excl.)	Annual Cost (VAT Excl.)
Maintenance and Support	Year 1	40	480			
	Year 2	40	480			
	Year 3	40	480			
Sub-Total (5.4) (VAT Excl.)						

5.5 Total Bid Price

Please capture your total cost proposal beneath.

Activity/ Deliverable	Amount
Sub-Total (5.1) (VAT Excl.)	
Sub-Total (5.2) (VAT Excl.)	
Sub-Total (5.3) (VAT Excl.)	
Sub-Total (5.4) (VAT Excl.)	
Total Bid Price (5.5) (VAT Excl.)	

Price Declaration Form

Dear Sir,

Having read through and examined the requirements of this RFP No. 2026/12, and its associated conditions, we hereby offer to provide, implement, and support an enterprise-grade Network Detection and Response solution as outlined in the scope of work, for the following total amount:

R..... (Excluding VAT)

In words

R..... (Excluding VAT)

We confirm that this price covers all activities associated with the scope of work, as called for in the RFP document. We confirm that Sasria will incur no additional costs whatsoever, over and above this amount in connection with the delivery of the required services.

We undertake to hold this offer open for acceptance for a period of 150 days from the date of submission of offers. We further undertake that upon final acceptance of our offer; we will commence the scope of work when required to do so by the Sasria.

We understand that you are not bound to accept the lowest or any offer, and that we must bear all costs which we have incurred in connection with preparing and submitting this bid.

We hereby undertake for the period during which this bid remains open for acceptance, not to divulge to any persons, other than the persons to whom the bid is submitted, any information relating to the submission of this bid or the details therein except where such is necessary for the submission of this bid.

SIGNED _____ **DATE** _____

(Print name of signatory) _____

Designation _____

FOR AND ON BEHALF OF: COMPANY NAME _____

Tel No _____

Fax No _____

Cell No _____

5. Part 5: Qualification and Evaluation Criteria

5.1 Evaluation of proposals

The purpose of the RFP is to obtain a complete set of salient information pertaining to the bidding parties. The proposals will accordingly be used to evaluate whether, at Sasria's discretion, an interested party qualifies to proceed to the next stage of this procurement process. All bidding parties will be advised in writing of Sasria's decision, which will be final. No correspondence will be entered into pertaining to the evaluation process, the decisions taken and reasons thereof.

5.2 Evaluation Criteria

5.2.1 Level 1- Governance Verification

The evaluation during this stage is to review bid responses for purposes of assessing compliance with RFP requirements, which requirements include the following:

- Proof of registration with CSD confirming tax compliance status as referenced in Part 2 above.
- Valid B-BBEE certificate or Valid Sworn Affidavit or Valid Specialised Entity Sworn Affidavit as referenced in Part 2 above.
- Duly completed Standard Bidding Document(s) and other requirements, in line with Part 6 of this RFP.
- Technical Proposal in line with the Technical Evaluation Criteria in Part 5 of this RFP document
- Financial/ Price Proposal in line with Part 4 of this RFP document

Note: Failure to comply with the requirements assessed in Level 1 (governance), may lead to disqualification of bids.

5.2.2 Level 2- Technical Evaluation

The evaluation during this level is based on technical criteria (functionality). The technical evaluation will be conducted in 2 phases, as follows:

Phase 1 – Mandatory requirements

Bidders are required to meet the following mandatory requirements and provide sufficient proof as stated below to validate their compliance. failure to meet any one of the mandatory requirements will result in disqualification from further participation in the tender process.

Mandatory requirements to be complied with	Please see attached the following proof to show you will meet the mandatory requirements	Please confirm if you comply by responding "YES" below, or respond "NO" if you do not comply
Technical Team must have IT and Cybersecurity certificate		The bidder must provide suitably qualified technical resources with experience in NDR, SOC operations, threat detection, incident response, and Microsoft security technologies. Resources must hold relevant certifications such as SC-200, SC-100, AZ-500, CompTIA Security+,

		CompTIA CySA+, CEH, CISSP, CISM, or equivalent industry-recognised certifications. Proof of certifications must be submitted with the bid
OEM Authorization		Accreditation letter from original solution manufacture or proof of ownership of the solution.

Note: Failure to submit the above will lead to automatic disqualification.

Phase 2 –Technical Evaluation Criteria

The bidder's proposal should respond comprehensively to the technical evaluation criteria. Only bidders achieving a minimum score of 70 points in this phase will be evaluated further . The technical evaluation criteria are set out below:

Item	Criteria	Points
1	**DETAILED USER REQUIREMENTS** **The bidder's proposed solution must meet the user requirements stipulated in this RFP document (See ANNEXURE E for guideline)** Bidders are required to submit a detailed and comprehensive proposal for a Network Detection and Response, clearly demonstrating how the proposed solution meets or exceeds each functional, technical, and operational requirement outlined below and in **Annexure E** of this RFP document. **<u>Functional and Technical Requirements</u>** **1. Network Visibility and Monitoring** The solution must provide continuous visibility across on-premises, cloud, hybrid, and Microsoft 365 environments, including east-west and north-south network traffic. **2. Behavioural Threat Detection** The solution must detect known and unknown threats using behavioural analytics, machine learning, and threat detection techniques. **3. Identity, Cloud and SaaS Threat Detection** The solution must detect suspicious activity across identity services, cloud platforms, and SaaS applications. **4. Threat Prioritisation and Risk Scoring** The solution must provide automated threat prioritisation and risk scoring based on severity, confidence, and business impact.	55

	5. Attack Correlation and Attack Chain Visibility The solution must correlate related attack activities and provide end-to-end visibility of attack paths and attack chains. **6. Threat Hunting and Investigation** The solution must support threat hunting, forensic investigation, historical analysis, and incident investigation workflows. **7. User Access Control and Role-Based Permissions** The solution must support role-based access control (RBAC), segregation of duties, and audit logging. **8. Alert Management and Incident Response** The solution must support alert management, incident triage, case management, escalation workflows, and response actions. **9. Threat Intelligence Integration** The solution must support threat intelligence enrichment to improve detection, investigation, and response activities. **10. Microsoft Sentinel and Security Platform Integration** The solution must integrate with Microsoft Sentinel, Microsoft Defender, Microsoft Entra ID, SOAR, ITSM, ticketing systems, and other enterprise security platforms. **11. Reporting and Executive Dashboards** The solution must provide configurable dashboards and reporting for operational, tactical, and executive stakeholders. **12. Notifications and Alerting** The solution must provide configurable alerts and notifications through email, APIs, and supported integration methods. **13. Data Security and Compliance** The solution must provide encryption, access controls, audit logging, and secure handling of data in compliance with applicable regulatory requirements, including POPIA. **14. Historical Reporting and Analytics** The solution must support historical analysis, threat trends, attack patterns, and reporting on changes in security posture over time. **15. Technical Architecture and Scalability** The solution must support secure, scalable deployment across enterprise environments and provide high availability and resilience. **Scoring will be allocated as follows:**	

	• The proposed solution complies with all the technical stipulated requirements compliance to all requirements: (55 points) 100%. • The proposed solution only complies with majority of the stipulated requirements (39 points) 70% • The proposed solution only complies with half of the requirements (30 Point) 30% • The proposed solution does not comply with any of the stipulated requirements (0 points) 0%	
2	**BIDDER'S PROJECT LEAD MEMBER** **The bidder must submit a comprehensive CV for the proposed Project Technical Lead, demonstrating experience in the implementation of Network Detection and Response (NDR), Security Operations (SOC), Threat Detection, Threat Hunting, Incident Response, or similar cybersecurity solutions. The CV must clearly indicate the individual's role, responsibilities, project involvement, and relevant experience** Relevant certifications may include SC-100, SC-200, AZ-500, CompTIA Security+, CompTIA CySA+, CEH, CISSP, GIAC, Cisco Security, or equivalent industry-recognised cybersecurity certifications. **<u>The points will be allocated as follows:</u>** • 8 years and more relevant experience in the implementation of Third-Party Risk Management (TPRM) or similar GRC solutions, supported by relevant qualifications - **30 points (100%)** • 6–7 years' relevant experience in the implementation of TPRM or similar GRC solutions, supported by relevant qualifications – **21 points (70%)** • 2–3 years' relevant experience in the implementation of TPRM or similar GRC solutions, supported by relevant qualifications **- 9 points (30%)** • Less than 2 years or non-submission of a comprehensive CV and/or no relevant qualifications and experience provided - **0 points (0%)**	30
3	**BIDDER'S EXPERIENCE** **The bidder must provide verifiable reference letters demonstrating successful implementation of Network Detection and Response (NDR), Security Operations (SOC), Threat Detection, Incident Response, or similar cybersecurity solutions.** To substantiate this experience, the bidder must submit reference letters from clients where the proposed solution has been successfully implemented. **<u>Reference letters must:</u>** • Be issued on the client's official letterhead. • Be signed by an authorised representative. • Include a contactable telephone number and email address. • Describe the NDR, SOC, threat detection, or related cybersecurity solution implemented. • Confirm the scope of work, project duration, and successful completion of the implementation.	15

	• Not be older than five (5) years from the RFP closing date. **Scoring will be allocated as follows:** • 3 reference letters (15 points) 100% • 2 reference letters (10 points) 70% • 1 reference letters (5 point) 30% • No reference letters (0 point) 0%	
Total		100

Note: Bidders must achieve a minimum score of (70%) points in Phase 2 of the technical criteria, to be considered for the next level (Phase 3- Solution Demonstration) of the evaluation process.

Phase 3 – Solution demonstration Evaluation Criteria
Bidders that are eligible for evaluation in this stage will be given notification of 5 days in advance to prepare for demo.

Item	Criteria	Points
A	**Adherence to requirements** The service provider must clearly demonstrate the proposed solution and the compliance to the deliverables and scope of the RFP as described in 3.3 and detailed requirements in **ANNEXURE E**. **The Service provider must present a Demo on the actual solution so to illustrate the solution's functionality.** **Scoring will be allocated as follows:** • 90-100% of the Requirements (100 points) 100% • 80-89% of Requirement met (80 points) 80% • 70-79% of Requirement met (70 points) 70% • Below 70% of Requirement met (0 points) 0%	100.00
Total		**100**

Note: Bidders that achieved 70 points and above for solution demonstration will be considered for the next level of the evaluation process i.e., Price and Specific goals.

5.2.3 Level 3- Preference Point System

The following preference points system will be used for this tender:

CRITERIA	POINTS
Price	80
Specific goals	20
TOTAL	**100 points**

Criteria for Specific Goals

Specific Goal to be measured	Points allocated out of a maximum 20.00 points	Points allocated of a maximum 10.00 points	Proof required to allocate points
1. The tenderer is: a) An Exempted Micro Enterprise (EME) or	15.00	7.5	Valid Sworn Affidavit or Valid Specialized Entity Sworn Affidavit

b) A Qualifying Small Enterprise (QSE) or	15.00	7.5	Valid B-BBEE certificate or Sworn Affidavit for QSE that are at least 51% black owned
c) A Generic enterprise	10.00	5.00	Valid B-BBEE certificate
d) A Generic enterprise (Prime Contractor) subcontracting at least 20% of the contract to either a EME or QSE.	15.00	7.5	1. Valid B-BBEE certificate and 2. A signed subcontracting agreement (between the Prime Contractor and Subcontracting parties) 3. Sworn Affidavit for EME or QSE that are at least 51% black owned
2. Additional points if the tenderer is at least 51% black Owned *(a Prime contractors B-BBEE certificate or Affidavit will be used in the case of subcontracting arrangements)*	5.00	2.5	Valid B-BBEE certificate or Valid Sworn Affidavit

Below is the specific goal(s) allocated for this RFP. Bidders are required to provide valid and sufficient proof as indicated in the table below to claim the preference points indicated.

Please note the following:

Failure on the part of a tenderer to submit proof or documentation required in terms of this RFP to claim points for specific goals, may result to preference points for specific goals are not claimed or allocated.

- Sasria reserves the right to require of a tenderer, either before the RFP is adjudicated or at any time subsequently, to substantiate any claim regarding preferences points, in any manner required by Sasria.

6 Part 6 – Required Documents

STANDARD BIDDING DOCUMENTS

In addition to the Annexures listed below, the following documents must be completed, signed and submitted together with the bid response:

- Invitation to Bid (SBD 1)

  Disclosure and Declarations Form (SBD 4)
- Preferential Points Claim Form (SBD 6.1);

Note: Failure to submit these documents may lead to disqualification of the bid or preference points not being awarded to the tenderer.

ANNEXURE A: CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

MEMORANDUM OF AGREEMENT

Entered into between:

Sasria SOC Ltd

A company duly incorporated under the laws of *Republic of South Africa*, having its main place of business at 36 Fricker Road, Illovo, Sandton Johannesburg, with registration number: 1979/000287/30

(Hereinafter referred to as “the Discloser”)

And

…….

A company duly incorporated under the laws of Republic of South Africa, having its main place of business
at……, with

registration number:……..

(Hereinafter referred to as “the Recipient”)

PREAMBLE

Whereas the Discloser will disclose certain confidential information to the Recipient, for purposes
of_____
____;

And whereas the Recipient wishes to receive confidential information on the condition that the Recipient will not disclose the same to any third party or make use thereof in any manner except as set out below.

The Discloser and the Recipient hereby agree to the following:

1. Definitions

Unless the contrary is clearly indicated, the following words and/or phrases, when used in this Agreement, shall have the following meaning:

1.1 **"Agreement"** shall mean this written document together with all written appendices, annexures, exhibits or amendments attached to it from time to time;

1.2 **"Commencement Date"** shall mean the date of last signature of this agreement;

1.3 **"Confidential Information"** shall mean all information which:

1.3.1 pertains to the Disclosing Purpose, disclosed, revealed or exchanged by the Discloser to the Recipient, and which pertains to, but is not limited to all intellectual property rights, all trade secrets, all agreements (whether in writing or not) which exist at the time of revealing the content thereof to the Recipient, the content of all possible future agreements which the Discloser intends to enter into with any other party, all knowledge obtained by way of research and development, irrespective of whether the aforementioned information that is revealed is applicable to technical, business or financial aspects of the Discloser; and/or

1.3.2 any information of whatever nature, which has been or may be submitted by the Discloser to the Recipient, whether in writing or in electronic form or pursuant to discussions between the Parties, or which can be obtained by

examination, testing, visual inspection or analysis, including, without limitation, business or financial data, know-how, formulae, processes, specifications, sample reports, models, customer lists, computer software, inventions or ideas; and/or

1.3.3 Any dispute between the Parties resulting from this Agreement; and/or

1.3.4 Any fault or defect in any aspect of the business of the Discloser, irrespective of whether the Discloser knows about such a fault or defect;

1.4 **"Notice"** shall mean a written document;

1.5 "**Parties"** shall mean both the Discloser **(Sasria SOC Ltd)** and the Recipient.

1.6 **"Board"** shall mean Board of Directors of the Discloser.

1.7 "**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;

1.8 **"Specific Goals"** means specific goals as contemplated in section 2(1)(d) of the Act which may include contracting with persons, or categories of persons, historically disadvantaged by unfair discrimination on the basis of race, gender and disability including the implementation of programmes of the Reconstruction and Development Programme as published in Government Gazette No. 16085 dated 23 November 1994;

2. Obligations of the Recipient

The Recipient shall:

2.1 use the confidential information disclosed to it solely for the purposes of ……
……
……..and for no other purpose whatsoever ("Disclosing Purpose");

2.2 treat and safeguard the Confidential Information as private and confidential;

2.3 ensure proper and secure storage of all Confidential Information;

2.4 not at any time without the prior written consent of the Discloser or another

employee of the disclosure from which he received the information,

2.4.1 disclose or reveal to any person or party either the fact that discussions or negotiations are taking, or have taken place between the Board, employee and another employee or the content of any such discussions or other facts relating to the Disclosing Purpose, except where required by law or any governmental, or regulatory body;

2.5 not create the impression with or lead any third party to interpret or construe any

e) condition contained in this Agreement, that this Agreement is an Agency Agreement and/or Partnership Agreement and/or a Joint Venture and/or any other similar arrangement;

2.6 not allege that this Agreement grants it, either directly, or by implication, or by estoppel or otherwise a license under any patent or patent application, or that it is entitled to utilize the Confidential Information in any way contrary to the stipulations contained in this Agreement;

2.7 on termination of this Agreement act with the Confidential Information in accordance with a Notice delivered to it by the Discloser and if no such Notice was delivered, the Recipient shall destroy the Confidential Information in a similar manner to which it would destroy information that it would consider to be its own Confidential Information.

3. Obligations of the Discloser

Subject to clause 2, the Discloser shall:

3.1 disclose to the Recipient, in writing any relevant information in their possession or under their care; and

3.2 furnish the Recipient at least 7 (seven) calendar days prior to this Agreement being terminated, for whatever reason, with a Notice instructing the Recipient about what it should do with the Confidential Information once the Agreement has been terminated.

4. Exclusions

The provisions of **Clause 3** above will not apply to any Confidential Information which:

4.1 is at the time of disclosure to the Recipient, within the public domain and could be obtained by any person with no more than reasonable diligence;

4.2 come into the public domain and could be obtained after such disclosure,

otherwise than by reason of a breach of any of the undertakings contained in this Agreement;

4.3 is subsequently provided to the Recipient by a person who has not obtained such

information from the Discloser, provided that, in any such case, such information was not obtained illegally or disclosed by any person in breach of any undertaking or duty as to confidentiality whether expressed or implied;

4.4 is disclosed with the written approval of the Discloser;

4.5 is or becomes available to a third party from the Discloser on an unrestricted basis;

4.6 is obliged to be reproduced under an order of court or government agency of competent jurisdiction.

5. Commencement

This Agreement shall commence on the Commencement Date.

6. Cancellation

6.1 The Agreement shall not terminate automatically. Either party must be able to terminate on written notice to the other party once the Disclosing Purpose is completed. The obligations of confidentiality under this Agreement shall continue to apply after assignment or termination of this Agreement.

6.2 The Parties further agree that either Party shall have the right at any time to give notice in writing to terminate this Agreement forthwith in the event of a material breach of any of the terms and conditions of the Agreement. If the breach in question is one which can effectively be remedied, the Parties shall endeavour to jointly try to remedy such breach, failing which, the Agreement shall be terminated.

7. Interpretation

7.1 The clause headings in this Agreement have been inserted for convenience only and will not be taken into consideration in the interpretation of this Agreement;

7.2 Any reference in this Agreement to the singular includes the plural and *vice versa*;

7.3 Any reference in this Agreement to natural persons includes legal persons and references to any gender include references to the other genders and *vice versa*.

8. Dispute Resolution

8.1 A dispute concerning or arising out of this Agreement exists once a party notifies the others in writing of the nature of the dispute and requires it to be resolved under this clause. The parties must refer any dispute to be resolved by -

- negotiation; failing which
- mediation; failing which
- arbitration

8.2 Within ten (10) Business Days of notification, the parties must seek an amicable resolution to the dispute by referring it to designated and authorized representatives of each of the parties to negotiate and resolve it by the parties signing an agreement resolving it within fifteen (15) Business Days

8.3 If negotiation fails, the parties must refer the dispute for resolution by mediation under the rules of the Arbitration Foundation of Southern Africa (or its successor or body nominated in writing by it in its stead)(”AFSA“).

8.4 If mediation fails, the parties must refer the dispute within fifteen (15) Business Days for resolution by arbitration (including any appeal against the arbitrator’s decision) by one arbitrator (appointed by agreement between the parties) as an expedited arbitration in Sandton under the then current rules for expedited arbitration of AFSA.

8.5 If the parties cannot agree on any arbitrator within a period of ten Business Days after the referral, the arbitrator will be appointed by the Secretariat of AFSA.

8.6 The periods for negotiation or mediation may be shortened or lengthened by written agreement between the parties.

8.7 This clause will not preclude any party from access to an appropriate court of law for interim relief in respect of urgent matters by way of an interdict, or mandamus pending finalisation of this dispute resolution process, for which purpose the parties irrevocably submit to the jurisdiction of a division of the High Court of the Republic of South Africa.

8.8 This clause is a separate, divisible agreement from the rest of this Agreement and must remain in effect even if the Agreement terminates, is nullified, or cancelled for any reason or cause.

9. Domicilium and Notices

The Parties elect the following addresses as their respective *domicilium citandi et executandi,* at which all notices and other communications must be delivered for the purposes of this Agreement:

9.1 Discloser:

9.1.1 by hand at 36 Fricker Road, Illovo, S*andton, Johannesburg*

Marked for the attention of: …….

9.1.2 by post at: **P.O. Box 653367, Benmore, 2010**

Marked for the attention of …….

9.1.3 by telefax at (011) 447 8624

Marked for the attention of **…….**

9.2 Recipient:

9.2.1 by hand at ……..

Marked for the attention of…….

9.2.2 by post to: _____

Marked for the attention of: ……

9.2.3 by telefax at ……Marked for the attention of: ……

9.3 Any notice or communication required or permitted to be given in terms of this agreement shall only be valid and effective if it is in writing.

9.4 Any notice addressed to either of the Parties and contained in a correctly addressed envelope and sent by registered post to it at its chosen address or delivered by hand at its chosen address to a responsible person on any day of the week between 09h00 and 16h00, excluding Saturdays, Sundays and South African public holidays, shall be deemed to have been received, unless the contrary is proved, if sent by registered post, on the 14th (fourteenth) calendar day after posting and, in the case of hand delivery, on the day of delivery.

9.5 Any notice sent by telefax to either of the Parties at its telefax number shall be deemed, unless the contrary is proved, to have been received:

9.5.1 if it is transmitted on any day of the week between 09h00 and 16h00, excluding

Saturdays, Sundays and South African public holidays, within 2 (two) hours of transmission;

9.5.2 if it is transmitted outside of these times, within 2 (two) hours of the commencement any day of the week between 09h00 and 16h00, excluding Saturdays, Sundays and South African public holidays, after it has been transmitted.

10. Entire Agreement and Variations

10.1 This Agreement constitutes the whole agreement between the Parties and supersedes all prior verbal or written agreements or understandings or representations by or between the Parties regarding the subject matter of this Agreement, and the Parties will not be entitled to rely, in any dispute regarding this Agreement, on any terms, conditions or representations not expressly contained in this Agreement.

10.2 No variation of or addition to this Agreement will be of any force or effect unless reduced to writing and signed by or on behalf of the Parties.

10.3 Neither party to this Agreement has given any warranty or made any representation to the other party, other than any warranty or representation which may be expressly set out in this Agreement.

11. Data Security

11.1. The Recipient shall, at all times, ensure compliance with any local and international laws, regulations, policies or codes that may be enacted from time to time and put in place and maintain sufficient measures, policies and systems to manage and secure against all forms of risk to any information that may be shared or accessed through a computer or any other form of electronic communication pursuant to the Agreement. For purposes of this clause 0,

"Information" shall mean, but not be limited to:

11.1.1. all cyber related information, including data; a computer program; output of a computer program; a computer system; article; data message; a computer data storage medium; output of a computer program and output of data;
f)

11.1.2. Personal Information as defined in section 1 of the Protection of Personal Information Act No. 4 OF 2013 ("POPIA") read with Section 1 of the Promotion of Access to Information Act No. 2 of 2000; and

11.1.3. Any other information that may be shared or accessed pursuant to the Agreement.

11.2. The Recipient shall notify the Discloser in writing of any cybercrimes or any suspected cybercrimes in its knowledge and to report such crimes or suspected crimes to the relevant authorities in accordance with applicable laws, within 10 days of becoming aware of such crime or suspected crime.

12. Protection Of Personal Information

12.1. For purposes of this clause 112 -

12.1.1. the following terms shall bear meanings contemplated in Section 1 of the POPIA: **consent; data subject; electronic communication; information officer; operator; person; personal information; processing; record; Regulator; responsible party; special information**; as well as any terms derived from these terms.

12.1.2. **"binding corporate rules"** means personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country; and **"group of undertakings"** means a controlling undertaking and its controlled undertakings.

12.2. The Parties acknowledge and agree that, in relation to personal information that may be processed pursuant to the Agreement, the Discloser is the responsible party and the

Recipient is the operator.

12.3. The Recipient must process such personal information only with the knowledge or authorisation of the Discloser and treat personal information which comes to its knowledge as confidential and must not disclose it, unless so required by law.

12.4. The Recipient must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information and unlawful access to or processing of personal information.

12.5. In order to give effect to the obligations set out in this clause 112, the Recipient must take reasonable measures to-

12.5.1. identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

12.5.2. establish and maintain appropriate safeguards against the risks identified;

12.5.3. regularly verify that the safeguards are effectively implemented; and

12.5.4. ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

12.6. The Recipient shall have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

12.7. The Recipient shall notify the Discloser immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

12.8. The Recipient shall appoint an information officer and an appropriate number of deputy information officers as may be required by the POPIA, and must provide the Discloser with the details of such officers, whose responsibilities shall include-

12.8.1. the encouragement of compliance, by the Recipient, with the conditions for the lawful processing of personal information;

12.8.2. dealing with requests made to the Recipient pursuant to the POPIA;

12.8.3. working with the Regulator in relation to investigations conducted under the POPIA;

12.8.4. otherwise ensuring compliance by the Recipient with the provisions of the POPIA; and

12.8.5. as may be prescribed by the POPIA.

12.9. The Recipient shall not transfer personal information about a data subject to a third party who is in a foreign country without Prior written consent of the Discloser. The Discloser will not grant such consent unless-

12.9.1. the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that-

12.9.1.1. effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and

12.9.1.2. includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

12.9.2. the data subject consents to the transfer;

12.9.3. the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;

12.9.4. the transfer is necessary for the conclusion or performance of a contract concluded in

the interest of the data subject between the responsible party and a third party; or

12.9.5. the transfer is for the benefit of the data subject, and-

12.9.5.1. it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

12.9.5.2. if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

12.10. The Recipient shall process personal information of data subjects in accordance with the conditions for the lawful processing of personal information as contemplated in the POPIA, and shall at all times put sufficient measures in place to ensure compliance with the POPIA, including compliance with any compliance notices and information notices served on the Recipient under the POPIA.

13. Assignment, Cession and Delegation

Neither of the Parties shall be entitled to assign, cede, delegate or transfer any rights, obligations, share or interest acquired in terms of this Agreement, in whole or in part, to any other party or person without the prior written consent of the other, which consent shall not unreasonably be withheld or delayed.

14. Relaxation

No indulgence, leniency or extension of a right, which either of the Parties may have in terms of this Agreement, and which either party ("the grantor") may grant or show to the other party, shall in any way prejudice the grantor, or preclude the grantor from exercising any of the rights that it has derived from this Agreement, or be construed as a waiver by the grantor of that right.

15. Waiver

No waiver on the part of either party to this Agreement of any rights arising from a breach of any provision of this Agreement will constitute a waiver of rights in respect of any subsequent breach of the same or any other provision.

16. Severability

In the event that any of the terms of this Agreement are found to be invalid, unlawful or unenforceable, such terms will be severable from the remaining terms, which will continue to be valid and enforceable.

17. Governing Law

The validity and interpretation of this Agreement will be governed by the laws of the Republic of South Africa.

SIGNATURES

I, the undersigned, **……** , herewith confirms that my position within the Recipient is that of **……** and state that I am duly authorised to enter into this Agreement, which I herewith do, on this the **…….**day, of **……..,** for and on behalf of the Recipient.

I, the undersigned **……**, herewith confirms that my position within the Discloser is that of Executive Manager: …….. and state that I am duly authorised to enter into this Agreement, which I herewith do, on this the _____ day, of …….. by signing this Agreement, for and on behalf of the Discloser.

_____

Signature for and on behalf of Discloser

_____

Signature for and on behalf of Recipient

ANNEXURE B: ACCEPTANCE OF BID CONDITIONS AND BIDDER'S DETAILS

RFP No:

Name of Bidder: _____

Authorised signatory: _____

Name of Authorised Signatory _____

Position of Authorised Signatory _____

By signing above the bidder hereby accept full responsibility for the proper execution and fulfilment of all obligations and conditions devolving on him/her under this RFP.

[*Note to the Bidder: The Bidder must complete all relevant information set out below*.]

CENTRAL SUPPLIER DATABASE (CSD) INFORMATION

Bidders are required to be registered on the Central Supplier Database (CSD) of National Treasury. Failure to submit the requested information may lead to disqualification. Bidders are therefore required to submit as part of this proposal both their CSD supplier number and CSD unique registration reference numbers below:	
Supplier Number	
Unique registration reference number	

BIDDING STRUCTURE

Indicate the type of Bidding Structure by marking with an 'X':	
Individual Bidder	
Joint Venture/ Consortium	
Prime Contractor with Sub Contractor(s)	
Other	

REQUIRED INFORMATION

If Individual Bidder:	
Name of Company	
Registration Number	
Vat registration Number	
Contact Person	
Telephone Number	

If Individual Bidder:	
Cell phone Number	
Fax Number	
Email address	
Postal Address	
Physical Address	

If Joint Venture or Consortium, indicate the following for each partner:	
Partner 1	
Name of Company	
Registration Number	
Vat registration Number	
Contact Person	
Telephone Number	
Cell phone Number	
Fax Number	
Email address	
Postal Address	
Physical Address	
Scope of work and the value as a % of the total value of the contract	
Partner 2	
Name of Company	
Registration Number	
Vat registration Number	
Contact Person	
Telephone Number	
Cell phone Number	
Fax Number	
Email address	
Postal Address	
Physical Address	
Scope of work and the value as a % of the total value of the contract	

If bidder is a Prime Contractor using Sub-contractors, indicate the following:	
Prime Contractor	
Name of Company	
Registration Number	
Vat registration Number	
Contact Person	
Telephone Number	
Cell phone Number	
Fax Number	
Email address	
Postal Address	
Physical Address	
Sub-contractors	
Name of Company	
Company Registration Number	
Vat registration Number	
Contact Person	
Telephone Number	
Cell phone Number	
Fax Number	
Email address	
Postal Address	
Physical Address	
Subcontracted work as a % of the total value of the contract	

ANNEXURE C: SHAREHOLDER INFORMATION

[*Note: the bidder must complete the information set out below. If the bidder requires more space than is provided below it must prepare a document in substantially the same format setting out all the information referred to below and return it with Returnable Schedule 2.*]

1 Shareholders/ Members

Name of the shareholder	ID Number	Race	Gender	% Shares

Note: The bidder must also attach the detailed Company/ Group Structure where relevant.

2 Black Shareholders/ Members as per the B-BBEE Certificate

Name of the shareholder	ID Number	Race	Gender	% Shares
Total Black Shareholding % as per the current and valid B-BBEE Certificate or Affidavit				

ANNEXURE D: BIDDER'S EXPERIENCE AND PROPOSED PROJECT TEAM

[*Note: the bidder must complete the information set out below. If the bidder requires more space than is provided below it must prepare a document in substantially the same format setting out all the information referred to below and return it with Returnable Schedule 3.*]

Table (a): Details of the bidder's current and experience in Implementing and Supporting a Network Detection and Response Solution for a period of 3 years. Note that client reference letters should be attached to your bid response / proposal.

Client' Name	Project description	Project Cost	Project period (Start and End Dates)	Description of service performed and extent of Bidder's responsibilities	Name, title and telephone contact of client

Table (b): Details of the key personnel of the bidders' proposed team:

Name	Position	Role / Duties in this Project	Relevant Project Experience	
			Project description, Client, Project period	Project Cost

ANNEXURE E

DETAILED USER REQUIREMENTS COMPLIANCE MATRIX

Network Detection and Response (NDR) Solution

Instructions to Bidders:

Bidders must indicate compliance with each requirement by marking **"Yes"** or **"No"** and provide a concise but clear response explaining **how** the requirement is met.

Where "No" is indicated, bidders must provide a motivation and describe any alternative approach

1. Network Visibility and Monitoring

Ref	Requirement	Yes/No	Bidder Response / Explanation
1.1	Provides continuous visibility across on-premises, cloud, and hybrid environments.		
1.2	Monitors east-west and north-south network traffic.		
1.3	Supports visibility of network, identity, cloud, and Microsoft 365 activity.		
1.4	Supports onboarding and monitoring of multiple network data sources.		
1.5	Provides centralised visibility of monitored assets and entities.		

2. Threat Detection and Analytics

Ref	Requirement	Yes/No	Bidder Response / Explanation
2.1	Supports behavioural threat detection using advanced analytics and machine learning.		
2.2	Detects command-and-control communications, lateral movement, and suspicious network behaviour.		

2.3	Detects compromised accounts, credential misuse, and identity-based attacks.		
2.4	Detects threats across cloud and Microsoft 365 environments.		
2.5	Supports threat intelligence enrichment of alerts and detections.		

]

3. Threat Prioritisation and Attack Correlation

Ref	Requirement	Yes/No	Bidder Response / Explanation
3.1	Provides automated threat prioritisation based on risk and severity.		
3.2	Correlates related attack activities across multiple environments.		
3.3	Provides attack-chain visibility and contextual threat analysis.		
3.4	Supports entity-based risk scoring and prioritisation.		
3.5	Reduces false positives through intelligent threat correlation.		

4. Threat Investigation and Threat Hunting

Ref	Requirement	Yes/No	Bidder Response / Explanation
4.1	Supports incident investigation and forensic analysis.		
4.2	Supports threat hunting across historical and real-time data.		
4.3	Maintains historical security telemetry for investigations.		
4.4	Provides search, filtering, and investigation capabilities.		
4.5	Supports export of investigation data and reports.		

5. Incident Response and Alert Management

Ref	Requirement	Yes/No	Bidder Response / Explanation
5.1	Supports incident triage and alert management workflows.		
5.2	Supports automated and manual response actions.		
5.3	Supports escalation and case management workflows.		
5.4	Provides configurable alerting and notification mechanisms.		
5.5	Supports prioritisation of alerts based on severity and risk.		

6. Dashboards, Reporting and Analytics

Ref	Requirement	Yes/No	Bidder Response / Explanation
6.1	Provides operational dashboards for security monitoring.		
6.2	Provides management-level security reporting.		
6.3	Provides executive reporting and cyber risk visibility.		
6.4	Supports on-demand report generation.		
6.5	Supports historical analytics and trend reporting.		

7. Integration Capabilities

Ref	Requirement	Yes/No	Bidder Response / Explanation
7.1	Integrates with Microsoft Sentinel.		
7.2	Integrates with Microsoft Defender and Microsoft Entra ID.		

7.3	Supports integration with SOAR and ITSM solutions.		
7.4	Supports integration using APIs and supported connectors.		
7.5	Supports integration with endpoint security and firewall technologies.		

8. User Access and Security Controls

Ref	Requirement	Yes/No	Bidder Response / Explanation
8.1	Supports Role-Based Access Control (RBAC).		
8.2	Supports segregation of duties.		
8.3	Supports Multi-Factor Authentication (MFA).		
8.4	Provides audit logging of user and administrative activities.		
8.5	Supports secure access to sensitive security information.		

9. Platform Availability and Security

Ref	Requirement	Yes/No	Bidder Response / Explanation
9.1	Delivered as a secure SaaS, on-premises, or hybrid solution.		
9.2	Provides scalable and resilient platform architecture.		
9.3	Supports high availability and business continuity requirements.		
9.4	Includes vendor support and service management aligned to SLA requirements.		
9.5	Provides platform health and performance monitoring.		

10. Compliance and Data Protection

Ref	Requirement	Yes/No	Bidder Response / Explanation
10.1	Supports secure handling and protection of security monitoring data.		
10.2	Provides encryption of data in transit and at rest.		
10.3	Provides comprehensive audit logging capabilities.		
10.4	Supports compliance with POPIA and applicable security standards.		
10.5	Supports retention and protection of historical security data.		