Eskom
Pension and Provident Fund

REQUEST FOR PROPOSAL

APPOINTMENT OF A SERVICE PROVIDER FOR THE PROVISIONING OF A SIEM SOLUTION AND SECURITY OPERATIONS CENTRE(SOC) SERVICES

Closing Date: 15 September 2023
Time: 16h00 SA Time

1 REQUEST FOR PROPOSAL

The Eskom Pension and Provident Fund (EPPF, or "the Fund") invites proposals from interested service providers to submit responses to this Request for Proposal (RFP) for the:

- **Provisioning of a SIEM (Security, Information and Event Management) Solution and Security Operations Centre (SOC) Services to EPPF for a for a period of 36 months , as a managed service in order to protect information assets against attacks, including cyber-attacks and also enhance the security posture of EPPF**

PURPOSE OF THE DOCUMENT

The purpose of this RFP document is to provide broad details relevant to the services required and is not intended to provide a detailed overview of every action required.

2 OVERVIEW

The EPPF is a self-administered Defined Benefit (DB) pension fund, regulated by the Financial Sector Conduct Authority (FSCA). The EPPF, as an organisation, is responsible for providing benefit administration and investment management services to the pension fund of Eskom Holdings SOC Ltd and its subsidiaries. The Fund provides retirement, withdrawal, death, and ill-health benefits to members, pensioners and their dependents.

The EPPF's core business activities are Pension Administration and Investment Management The core functions are supported by the Finance, Governance & Assurance, Office of the CE , Human Capital, and Information Technology Departments. The EPPF has assets under management of R169.9 billion and membership comprises 33 494 pensioners, 39 222 active members and 1778 deferred pensioners as at 30 June 2022 (June 2023 membership under review).

The EPPF's vision is to become the most admired pension fund by its peers and members, and its mission is to be a member-centric pension fund. The Fund's strategic objectives, which would enable it to fulfil its mission, are defined under five (5) pillars, representing critical strategic focus areas as noted below.

3 RFP RESPONSE GUIDELINES

3.1 *Point of contact*

This RFP is issued on an open tender notice format with a definite closing date and time.

Respondents are required to submit their responses in expansive detail and on time to qualify for consideration of their responses.

During the open response time, the central point for all queries relevant to the provision of background information and points of clarity relevant to this RFP, will be managed through a central mailbox. In the interest of all parties concerned all queries must be submitted **in writing only** and responses to queries or points of clarity will be published in the "Tenders" section of the Fund's website (www.eppf.co.za).

The electronic mail address for queries is ProcurementOffice@eppf.co.za. No telephonic or verbal queries will be entertained.

After the distribution of this RFP, a ***Non-Compulsory*** briefing session will be conducted with all potential respondents to provide further information and address questions relevant to the RFP.

The briefing session is scheduled for **12:00 pm SA Time on Wednesday, 23 August 2023** via Microsoft Teams. Interested participants to send their email addresses by **Tuesday, 22 August 2023 at 12h00 SA Time** to ProcurementOffice@eppf.co.za. Attendance is limited to two (2) persons per company or Service Provider. Email Subject for all communication relating to this RFP is **Provision of a SIEM Solution and Security Operations Centre (SOC)**

Services. A request with the Microsoft Teams meeting information will then be forwarded to the email address provided.

Respondents must not contact any of the Fund's Board members, executives, consultants or staff to discuss matters related to this RFP or the RFP process. Discussion of this RFP with any person within or associated with the Fund other than the designated contact email as above will result in the disqualification of that respondent from the process.

3.2 *RFP process and submission procedure*

The Fund will review proposals at its discretion against a set of pre-defined criteria and will rate each proposal on its ability to satisfy the requirements stated in this RFP.

In the event that a preferred supplier is selected, such service provider will be formally notified. A formal Agreement will be entered into between the Fund and the successful service provider detailing issues such as the scope of work, remuneration structure and validity of the term of the contract.

Potential service providers are requested to be mindful of the time allowed for responses, the closing date and time, the delivery address for proposals and must note that late or incomplete submissions will not be considered.

The RFP must be submitted with the necessary supporting detail and must at least provide the information requested in this RFP.

The Fund reserves the right to consider any proposal in its entirety or partially and may appoint more than one service provider or no service provider at all. The Fund's decision is final, and no correspondence will be entered into.

3.3 *Submission Date, Time and Address*

The closing date for submission of proposals at the delivery address indicated below is **15 September 2023, 16h00.**

RFPs must be submitted electronically to ProcurementOffice@eppf.co.za.

All proposals must reach the allocated email address on or before the closing time. It remains the responsibility of the respondents to ensure that their proposals reach the Fund before the closing date and time.

Respondents are allowed to send large files via WeTransfer ONLY and must ensure that the hyperlinks provided are fully functional. All documents must be provided in Adobe PDF.

Proposals may not be faxed, or hand delivered, and proposals received by any other means other than the designated email address, will not be considered and will be rendered invalid.

3.4 *RFP Timelines*

The timelines for the RFP process are as follows:

Activity	Due Date
Distribute RFP Documentation	15 - 21 August 2023
Non-Compulsory Briefing Session	23 August 2023,12h00
Deadline for clarification questions	25 August 2023
Final response to clarification questions	28 August 2023
Closing date for submissions	15 September 2023, 16h00

Please note that the above timelines are indicative and that the Fund reserves the right to change these timelines. Respondents will be advised of any changes and / or notices via EPPF's website.

3.5 *RFP Process Requirements*

The following minimum requirements will be applied to the RFP process:

i. Responses received after the closing date and time will be considered late and **will not** be accepted. If a response is considered late, it will be returned unread to the sender.
ii. All responses must be submitted in full on or before the closing time. The Fund will not allow additions and/or amendments to any response to be submitted after the closing date and time and will not receive submissions in separate parts.

iii. Responses may be withdrawn in writing by a respondent prior to the closing date and time.

iv. All enquiries relevant to the RFP may only be submitted to the indicated point of contact and in writing. Telephonic and/or verbal enquiries will not be entertained.

v. During the course of this RFP process, respondents may acquire confidential information relating to the Fund's business, projects and/or customers. Respondents are required to keep this information strictly confidential at all times (even after the RFP process has been completed) and may not use or attempt to use or allow such information to be used for personal gain or the gain of any other person or institution.

vi. Respondents may not disclose such confidential information to any third party, but to the extent that such disclosure may be necessary for the submission of a formal proposal, must approach the Fund for prior approval to share the information with a third party. This does not apply to information which must, by law, be disclosed or becomes available to and known by the public due to no fault on the part of the respondents.

vii. Respondents must comply with the highest ethical standards in order to promote mutual trust and an environment where business can be conducted with integrity, in a fair and reasonable manner.

viii. Proposals submitted to the Fund must remain valid for a minimum period of 90 days from the closing date.

ix. Respondents will be held to their proposals as submitted. The Fund reserves the right to negotiate the modification of a proposal with the successful respondent in whole or in part.

x. Agreements reached after such modifications with the successful respondent, or parts thereof, and accepted by the Fund will form part of the contract.

xi. Each proposal will be evaluated for general conformity to specifications and the demonstrated capabilities of respondents to execute the scope of work.

xii. Respondents must provide curricula vitae of all key personnel they propose for execution of the scope of work, with clearly defined fields of expertise, functions and responsibilities.

xiii. In general, respondents must indicate the experience and field/s of expertise of their companies and must specifically demonstrate their experience in similar assignments and an understanding of the services required.

xiv. Respondents are responsible for any and all costs and liabilities incurred in responding to this RFP. The Fund will not be responsible for any costs whatsoever or howsoever arising.

xv. The Fund reserves the right to withdraw this RFP for any reason and at any time without incurring any cost or liability.

xvi. The Fund reserves the right to withdraw, at any stage of this process, amend or cancel this RFP, reject or not accept any or all proposals, obtain any information from any lawful source regarding past business history and practices of the respondent, and to take any such information into consideration in the evaluation process.

xvii. The Fund does not have to explain acceptance or rejection of any specific service provider and the Fund's decision is final and binding, no correspondence will be entered into.

3.6 *Compliance requirement: structure of responses*

The structure of proposals is as follows:

3.6.1 Proposals must be electronically generated and signed by the individual(s) legally authorised to bind the respondent. The electronic copies of the RFP proposal and/or examples of work must be provided in Adobe Reader Portable Document Format (PDF), free of any viruses or malicious ware.

3.6.2 Legibility, clarity and completeness are essential.

3.6.3 Responses must be prepared as simply as possible, providing a straightforward, concise description of the interested parties and the capabilities available to satisfy the requirements of the RFP.

3.6.4 The RFP response must be presented in the following format:

Section	Title
1	Executive Summary of Proposal
2	Company background and track record
3.	Proposed team members for the project and their credentials
4	Proposed services
5	Key Deliverables
6	Pricing Structure

7	References (three references to be included)
8	B-BBEE
9	Supporting documentation

3.6.5 Failure to comply with paragraphs 4.6.1 to 4.6.4 will result in the relevant response being disqualified.

3.7 *Evaluation Criteria*

Respondents will be evaluated according to the extent to which they are able to fulfil the requirements of the Fund. Evaluation criteria will place emphasis on the following areas:

Stage 1:

- BBBEE: 20%
- Pricing: 20%
- Functional Ability: 55%
- Data Privacy - POPIA Compliance: 5%

Stage 2(Shortlisted Bidders)

- Solution Demonstration, Presentation and Due diligence: 100%

Respondents must be well established entities with expertise in providing a cyber security services, implementation of a SIEM solution and provision of Security Operations Centre (SOC) services utilising best practice methodology and approach. Respondents are required to indicate the period they have been in operation in this specific environment and must include supporting documents in respect of such specific expertise. We will also require respondents to stipulate their experience with providing cyber security services and strategy for pension/ retirement funds/financial services and public sector entities or to an organisation of a similar size to EPPF.

Respondents must also provide supporting documentation relevant to issues such as the ownership of the business, management structure and B-BBEE credentials (Minimum of Level 4 required) in the format indicated in this RFP document.

Evaluation criteria will place emphasis on the following areas:

3.7.1 Functional Ability

Service providers must submit a capability statement with:

- A minimum of five (5) years demonstrated experience of successful implementation of a SIEM solution, provisioning of Security Operations Centre (SOC) and cyber security strategy, for similar organization in size to EPPF
- The bidder should be ISO27001 Certified.
- **Cyber Security Services** include building, implementing, and improving cyber security strategy, provision of a SIEM solution, Security Operations Centre (SOC) and other related advisory and consulting services.
- Ability to support EPPF with its end-to-end Cyber Security Programme as and when required
- The capacity and experience of the proposed team, with CVs of team members which need to include qualifications and relevant experience. Some of the team members must have the following credentials:
    - Certified Information Security Professional (CISSP)
    - Offensive Security Certified Professional (OSCP)
    - Certified Ethical Hacker - CEH & Certified Ethical Hacker Practical
- The proposed approach to provisioning of cyber security services, SIEM solution and Security Operations Services(SOC)
- Proposed architecture – Service providers must include the following information as part of the response:
    - Hosting Technology and Infrastructure of the SIEM solution – Hybrid Cloud

Support

- Integration methodologies and technologies supported by the proposed technology - to allow the consumption of data from multi-cloud environments as well as to allow pulling of data by other systems.
- IT Security – including user access authentication/authorization capabilities including integration to Azure Active Directory or other authentication solutions
- Connectivity – Internet Connectivity, VPN and Firewall solution
- Data Privacy - Compliance to POPIA and Data Encryption
- Data Architecture - models, policies, rules or standards governing how and which data is collected, and how it is stored, and put to use in other systems
- Support & Maintenance process

Shortlisted respondents will be invited to make presentations to be scheduled for **9 –13 October 2023.** The presentations will be part of the technical evaluation and scored accordingly. Shortlisted respondents will be contacted by **6 October 2023**.

3.7.2 Fee Structure (Pricing)

Respondents must provide full details of pricing models and assumptions made in the pricing. All prices are to be quoted in South African Rands (ZAR) and **must include VAT** where applicable.

Proposals must be valid for at least 90 days from the closing date of the RFP. If prices are subject to exchange rate fluctuations, respondents must indicate the assumed rates and conditions pertaining to exchange rate fluctuations.

All prices must be disclosed comprehensively.

Please submit pricing fee/schedule as presented in the table below for 36 months:

No.	Item description	Quantity	Rate Per Applicable (Inc VAT)	Total Estimated cost (Inc VAT) Over 36 months
1	**SIEM solution - License Cost**	Refer to 5.2: Scope of Work and Current Environment	Suppliers to provide	Suppliers to provide
2	**SIEM solution - Infrastructure Costs**	Refer to 5.2: Scope of Work and Current Environment	Suppliers to provide	Suppliers to provide
3	**SIEM solution - Support and Maintenance**	36 Months	Suppliers to provide	Suppliers to provide
4	**Security Operations Centre (SOC) Services**	36 Months	Suppliers to provide	Suppliers to provide
5	**Implementation fee (Once-Off)** • Deployment of resources on the project (onsite/remote), incl. Project Management	Suppliers to provide	Suppliers to provide	Suppliers to provide
6	**Training (Once-off) – OEM related**	20 Key Stakeholders	Suppliers to provide	Suppliers to provide
7	**Other costs (if applicable)**			
Total Price Incl. VAT (ZAR)				

Note - To facilitate like-for-like comparison, bidders must submit pricing strictly in accordance with the pricing table above and not utilise a different format. Use of a format different to the pricing format provided, may render your submission disqualified.

Kindly indicate hourly rates for consultancy per resource level (e.g. IT Security Specialist , Technical Engineer, Trainer etc.) – through a rate card **or** by completing the table below.

No.	Level of resources	Proposed Rate (Inc VAT)
1	E.g., IT Security Specialist	
2		
3.		
4		

3.7.3 B-BBEE

The Fund is committed to advancing the objectives of B-BBEE and details of the service provider's B-BBEE credentials, supported by a copy of a rating certificate from a South African National Accreditation System (SANAS) accredited rating institution or an affidavit wherever applicable, with details of the relevant company profile must be provided. As a minimum, specific reference must be made to:

- Ownership structure and shareholding;
- Board representation;
- Executive / Operational Management structure;
- Representation of Black people and women in the proposed team,
- Secondary B-BBEE initiatives, such as procurement from B-BBEE suppliers and other initiatives.

These details must be clearly stated in the order requested and with the headings as above.

3.8 *References*

The Fund will require references from established companies where the respondents conducted similar consulting services. The Fund therefore requires information regarding contactable clients. Respondents must include references from at least three clients in South Africa where they are providing Cyber security services , a SIEM solution and Security Operations Centre (SOC) services in the following format:

- Client name.
- Contact details (telephone and email address).
- Client representative.
- Service description (scope of services delivered and total contract value thereof).

When providing information regarding references it is accepted that the respondent has cleared with the referee that the client can be contacted directly by the Fund or its consultants.

4 RFP SPECIFICATIONS

4.1 *Purpose*

The EPPF seeks to contract with a qualified service provider to provide **a SIEM solution and Managed Security Operations Centre (SOC) services** . Please provide the potential deliverables you would propose that the Fund considers and the KPI's you will be measured against on the below scope of work.

4.2 *Scope of work*

The successful service provider will be required to assist with the following services:

Implementation, Support and Maintenance of a SIEM solution

Provision of Managed Security Operations Centre (SOC) Services

Provision of Cyber Security advisory and consulting services as and when required

SIEM Solution

The SIEM Tool should have the following capabilities

- Collects logs and events data from servers and workstations, network active equipment, firewalls, access control, authentication, antiviruses, and virtualization environment.
- Managing the volume of data is also available with Data Policy Manager, eliminating the need to consider the storing volume.
- The enrichment of data with threat intelligence feeds, user identity and behaviour data
- Indexes all data for security incidents in real-time via built-in alerts, correlation rules and advanced investigation capabilities.
- Detects security incidents in real-time via built-in alerts, correlation rules and advanced investigation capabilities.
- Built-in threat intelligence and incident management platform as well as real time monitoring.
- Detects internal and external threats, threat hunting and behaviour analysis to enable EPPF security teams to see what is hidden and provide understandable, actionable outcomes.
- Audit reports, User activity monitoring and Behavioral monitoring (through agent deployment)
- Integration capabilities to other relevant systems/applications
- Service reporting and dashboards

- Cloud Monitoring

Functional Requirements of the SIEM tool

Collect

- Pre-defined integration and free plugin service starts data ingestion, followed by advanced parsing and indexing techniques.
- It must supports many log collection methods such as SYSLOG, SMB, WMI, FTP, SFTP, LEA, SQL, ORACLE, Flow.
- It classifies and normalizes data, and enriches it with embedded TI services in real time.

Detect

- Correlates the data, detects threats in real-time and lowers the number of false positives according to Mitre Attack framework detects any complex and modern threats and finds the hidden ones, anomalies and IOCs; and uses advanced behaviour techniques to prioritize the insider threats.

Respond

- Eradicate threats and attack proactively on other integrated security tools such as firewalls, DLP, and NAC when detected.
- Mitigates threats and vulnerabilities, and automatically enable remediation actions on other integrated security tools such as AD, EDR and EPP were applicable.

Infrastructure

- Vertical and horizontal, unlimited scalability.
- Cluster, high availability.
- Flixible deployment both on-premises and cloud environments.

Architecture

- It must capture data from:
    - Security devices
    - Infrastructure Services
    - Virtualisation Infrastructure
    - Servers
    - Active Directory
    - User-facing Applications

- Storage devices
- Cloud infrastructure
- Environmental devices
- SaaS solutions

The Features

- Easy Scale Out Architecture
- Customizable Dashboards
- Intelligence Automated Infrastructure and Application Discovery
- Log Collection and Aggregation
- Data Correlation
- Real-Time Operational Context for Rapid Security Analytics
- Analytics and Real-time Threat Alerts
- Automated Incident Mitigation
- Out of the Box compliance Reports
- Performance and Availability Monitoring
- External Technology Integrations
- Change monitoring
- Reporting and incident Management

Training

- The service provider is expected to provide OEM(Original Equipment Manufacturer) related training to EPPF internal staff

Security Operations Centre (SOC) Services

At a minimum the SOC should effectively and efficiently manage security operations by preparing for and responding to cyber risks/threats, facilitate continuity and recovery from cyber-attacks/incidents

The SOC solution must have following broad features:

- Supply and deploy a SOC team that must operate in shifts around the clock, dedicated to and organized to prevent, detect, assess and respond to cybersecurity threats and incidents;
- Provide maintenance and support for all the provisioned SOC components;
- Provide and deploy a secondary site (backup site) for high availability and failover;

- Detect threats (internal and external) across the IT environment including data center, cloud environment, users, endpoints, and network.
- Detect known as well as unknown threats by using machine learning and other security analytics.
- Consolidate data and extract actionable insight from a variety of intelligence sources and existing security technologies
- Proactive threat hunting on a daily basis.
- Be Cyber-ready to respond to attacks swiftly.
- Complete analysis and correlation of logs from all the devices/solutions under scope.
- 24x7 uninterrupted security monitoring operations.
- Automate security processes to reduce resource drain and threat response timelines.
- Skilled and capable staff with expertise in at least the following domains must be available:
    - Event monitoring and analysis
    - Incident detection and response
    - Threat hunting and intelligence
    - Security Analytics
- Correlation of low priority alerts with subsequent alerts to detect multi-stage attacks.
- Reduction of remediation time
    - Automated real time prioritization of alerts.
    - Automated data collection for investigation followed by quick analysis on a single window.
    - Assisted remediation steps (integration with security devices to push policy/configuration remotely) for faster mitigation of threats.
- Provide central dashboard to capture risk posture and maturity levels of organization at any given point of time.
    - Detect user anomalies using a combination of rules and machine learning models.
    - Support the creation of rules to exclude specific addressed/IP ranges.
    - Identify and block reconnaissance attacks.
    - Identify and block credential theft attempts form either memory (credential dump, brute force) or network traffic (ARP spoofing, DNS Responder).
    - Identify user account malicious behaviour, indicative of prior compromise.
    - Must have built-in vulnerability management.

- capabilities to define rules on event logs captured from various sources to detect suspicious activities. Examples:
    - Failed login attempts
    - Successful Login attempts from suspicious locations or unusual systems
    - Authorization attempts outside of approved list
    - Logins from unauthorized subnets
    - Vertical & Horizontal port scans
    - Traffic from blacklisted Ips
    - Login attempts at unusual timing
- The proposed solution should prevent tampering of any type of logs and log any attempts to tamper logs. It must provide encrypted transmission of log data to the log management.
- The solution should also monitor for security events on critical business applications, databases and identify network behavior, user behavior anomalies

Current Environment:

- Total of approximately **170 staff** across all business units, all using Windows laptops
- Some staff members use company owned Apple devices (solution should cater for Android devices as well)
- EPPF on-premises infrastructure is currently running on **HPE SimpliVity infrastructure** with approximately **10 virtual servers**
- The Cloud based applications, services and infrastructure are hosted in Microsoft Azure, Amazon Web Services as well as some of the third-party cloud providers , **approximately 30 virtual machines in total**
- The service provider is expected to provide SIEM and security solutions that will allow integration and consumption of data for both on premise and cloud hosted services as well as 3rd party hosted systems
- The system must support a complete and scalable architecture through the licensing of additional components required to integrate with the various digital environments, including on-premises, cloud and hybrids and which include but are not limited to the following that exist in the current environment:
    - Microsoft 365
    - Virtual machines (Vmware)
    - Cisco switches and routers

- Microsoft Servers
- HP Storage
- Microsoft AZURE
- Amazon Web Services

- EPPF strategic goal is to migrate all on-premises to the cloud, and therefore service providers may be expected to provide support as and when applications and infrastructure are being migrated from On-premises to the cloud.

ESTIMATED CONTRACT PERIOD – 36 Months
ESTIMATED CONTRACT START DATE – 01 November 2023

5 REQUIRED SUBMISSIONS

5.1 *Declaration*

Respondents must, on the official letterhead of the company submitting the response, declare that:

a. the information provided in all documentation is true and correct;
b. the signatory of the tender document is duly authorised to do so by means of their role in the company, a special or general resolution of the company responding; and
c. undertake that all information gained from the EPPF through this RFP document or from any other interaction relevant to this RFP, will remain confidential.

5.2 *Company details and stability*

Please provide a response to each of the following questions:

a. How long the company has been in operation within its current specific environment of providing cyber security services/SIEM solution/SOC services.
b. The nature of the business, paying particular attention to core activities.
c. The company's summarised value proposition to its clients.
d. The company's registration number and supporting registration documents.
e. The company's overall organisational structure and key resources within this structure that will be dedicated to the EPPF.
f. If the response to the RFP is made as part of a joint venture with another business entity, details of the commercial relationships between the parties making up the consortium / joint venture / partnership. In addition, provide the following information:

- Copy of the Joint Venture Agreement
- Entity(ies) that will be guaranteeing contract performance;
- Date of Joint Venture formation, if applicable;
- The name of the lead / primary contractor; and
- Details regarding the nature of the agreement between the Joint Venture Partners including the proposed percentage division of work between the constituent members. Each party to the joint venture, if that party is a subsidiary company, is required to give details of the extent to which the holding company and related subsidiaries and associates are prepared to provide guarantees.
- The B-BBEE rating will be the average of the companies' individual ratings, weighted according to their proportionate share in the Joint Venture.

5.3 *Local Presence and Experience*

i. Provide details of the head office location.
ii. If the head office location is not in South Africa, also provide details of local company offices, support and visibility.
iii. Provide the year of establishment of the South African business and the number of employees currently employed.
iv. Provide instances of the company's experience in providing cyber security services/SIEM solution
v. Provide evidence of the company's experience in engaging with clients at executive and board level.

5.4 *Implementation Plan*

Respondents are required to detail their approach to provisioning of cyber security services and implementation linked to the scope of work, with specific focus on SIEM solution and SOC services

5.5 *Approach*

i. Describe how your organisation would approach this engagement, and methodologies to be adopted. Please detail the phases, activities and milestones involved.
ii. Describe how and when the required capabilities and resources from your organisation will be deployed.
iii. Describe the resources required from the Fund.

5.6 *Supporting Documentation*

Respondents **must** include the following supporting documentation within their proposals:
Mandatory documents;

- A detailed statement of the company's B-BBEE credentials as required in the above, supported by a rating certificate from a SANAS accredited rating institution or a B-BBEE affidavit.
- Recent audited Financial Statement of the specific entity that will be submitting the proposal, and if successful, contracting with the Fund. Group or any other entity's Annual Financial Statements will not be accepted. Respondents who are not required by law to have audited financial statements must include a letter signed by an authorised official confirming that the respondent is not required by law to have audited financial statements and accordingly, is unable to provide same. Failure to submit a complete set of financial statements i.e. all pages or redaction/blanking out or omission of any portion of the financial statements will render the submission incomplete and will lead to disqualification at the evaluation stage.
- Respondents must complete the EPPF POPIA Self Compliance Forms (EPPF Operator Privacy Due Diligence Form and Operator Privacy Compliance Self-Assessment Form) provided on the EPPF website.

In the case of a Joint Venture the above-mentioned documentation, with the exception of the B-BBEE credentials, need only be supplied for the primary entity.

Administrative documentations;

- Declaration (Formal letter) as per (6.1) under Further required submissions
- Certified copies of CIPC company registration documentation. In the case of respondents who are not companies as envisaged in the Companies Act of 2008, equivalent founding documents must be submitted;
- A valid Tax Clearance Certificate and/or PIN indicating good standing with the South African Revenue Services (SARS);

Respondents will be disqualified from the RFP process if any of the details and/or mandatory documents listed in 6.6 above are not submitted.

6 Appendix A – Terms of business

1. Background

The Fund wishes to appoint a suitable service provider to provide cyber security services.

By submitting a response to the RFP sent out by the Fund, a respondent automatically undertakes to be bound by, and agrees to, the conditions set out in this entire document.

Respondents that do not consider themselves bound by the provisions of this entire document should not respond to the RFP, as submission of a response pre-supposes agreement to the terms of this agreement.

2. Terms of Business

The Fund hereby sets out the Terms of Business and the respondent hereby accepts the conditions that will apply to the work to be done by the service provider appointed in terms of the RFP detailed in this agreement.

Once signed by both parties, these Terms of Business will form part of the basis of a suitable Agreement between the Fund and the successful service provider.

An additional agreement detailing the services to be rendered will be entered into. These Terms of Business will establish the basis of such an agreement to provide the services as outlined in the RFP, and will serve to explain the conditions under which the appointment of the preferred service provider is made, but may also be extended in the Agreement to include other matters not necessarily addressed in this RFP.

3. The services to be provided

3.1. **The Services**

The service provider will provide the services described in the RFP, and at the location(s) to be set out in the Agreement. The services described in the RFP are not an exhaustive list of all services to be performed by the successful respondent.

Where the Agreement refers to services to be performed, this means that the service provider will provide the Fund with the Services and will be responsible for the management

and control of the services and the quality of any deliverables listed in or referred to in the Agreement.

Where the Agreement refers to Services to assist the successful service provider this means that the Fund will use reasonable skill and care, as specified, to assist the service provider with its work, but the service provider will be responsible for the overall management and control of the Services and for the results to be achieved from using the Services.

3.2. **The service provider's staff**

Where individual members of the service provider's staff (including partners and directors) are named in the Agreement the service provider will make every reasonable effort to ensure that the named individual(s) are available to support its work for the Fund stated in the Agreement.

Where the service provider considers changes in its named staff necessary or appropriate, for reason of, inter alia, resignation, relocation, training or illness, the service provider may make the changes after giving the Fund reasonable notice and will provide the Fund with details of replacement staff.

3.3. **Contract Management**

Both parties may designate a contact person that will be responsible for managing all issues relating to the performance of the Agreement.

3.4. **Deliverables**

3.4.1. **Preparation and Delivery**

The Fund will incorporate the deliverables listed or referred to in the RFP into the Agreement to be signed with the preferred service provider.

4. Fees and Payment

4.1. **Payment of services**

The Fund agrees to pay for the Services as set out in the Agreement. All invoices will be payable within thirty days from date of receipt thereof.

5. Term, Suspension and Termination

5.1. **Duration of Contract**

The Agreement will apply from the Commencement Date stated, or where no Commencement Date is specified, from the date of signature of the Agreement by both parties. The Agreement will continue until all the Services and deliverables have been provided unless it is terminated earlier in accordance with the terms set out below.

5.2. **Termination of the Contract**

Unless stated otherwise in the Agreement, the Contract may be terminated by either party at any time by giving the other party no less than 30 days written notice. The Fund however reserves the right to terminate the Agreement by giving 24 hours written notice.
Where the Contract is terminated in this way the Fund will pay the service provider for all Services provided and completed up to the date of termination.

5.3. **Termination for Breach of Contract**

The Agreement may be terminated by either party by written notice with immediate effect if the other commits a material breach of any term of the Agreement that is not remedied within 10 days of dispatch of a written request to remedy the same, where such breach is capable of being remedied.

5.4. **Termination for Insolvency**

The Agreement may be terminated by either party by written notice in the event that the other party is unable to pay its debts or has been placed under administration, judicial manager, liquidator or similar person or officer appointed or compromises generally with its creditors or ceases for any other reason to carry on business or in the reasonable opinion of the other party any of these events appears likely.

6. Confidentiality and Conflicts of Interests

6.1. By signing the Agreement, each party is under a professional obligation not to disclose to a third party any information confidential to the other party. Similarly, reports by the service provider are for the use of the Fund alone and may not be disclosed to third parties without the Fund's prior written consent.

6.2. Notwithstanding 6.1 above, either party will be entitled to disclose confidential information of the other to a third party to the extent required by law or where the said information is already known to the public due to no fault on the other party, provided that in the former case (and without breaching any legal requirement), where reasonably practicable not less than five business days' notice in writing is first given to the other party.

6.3. Respondents are required to declare any relationship (family, friend, other) between themselves and any person employed by the EPPF who may be involved with the evaluation and or adjudication of this RFP. Such declarations may be included as part of the Respondent's proposal. In addition, service providers with such an interest may be required to complete the EPPF's standard declaration of interest form.

7. Liability

7.1. The service provider shall use reasonable skills and care expected from an expert in its industry in the provision and delivery of the services and the deliverables in terms of the Agreement.

7.2. The service provider shall accept liability to pay compensation for damages and losses suffered by the Fund arising as a direct result of breach of contract, misconduct, dishonesty/fraud or negligence (including gross negligence) on its part or third parties acting on behalf of the service provider in respect of Services provided in connection with, or arising out of the Agreement (or any variation or addition thereto).

8. General

8.1. **Force Majeure**

Neither of the parties to the Agreement will be liable to the other for any delay or failure to fulfil obligations caused by circumstances beyond its reasonable control.

8.2. **Assignment**

Neither of the parties to the Agreement may cede, assign, delegate, transfer, encumber, charge nor otherwise seek to deal in any of its rights or obligations under the Agreement without the prior written consent of the other party.

8.3. **Notices**

Notices must be served either personally, sent by prepaid registered post or faxed to the address of the other party given in the Agreement or to any other address as the parties may have notified during the period of the agreement. Any notice sent by registered post will be deemed to have been delivered 10 days after sending. Any notice sent by fax or served personally will be deemed to have been delivered on the first working day following its dispatch.

8.4. **Amendment**

Any amendment or consensual variation, cancellation or termination of the Agreement, or any of its terms, will not be effective unless agreed in writing and signed by both parties.

8.5. **Survival**

The confidentiality clause in the Agreement shall survive the termination or expiry of the agreement and shall continue to bind the parties to the agreement.

8.6. **Electronic Communications**

During the provision of the Services, the Fund may from time to time communicate electronically. However, as the service provider is aware, the electronic transmission of information cannot be guaranteed to be secure or error-free and such information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete or otherwise be adversely affected or unsafe to use.

Accordingly, whilst the Fund carries out commercially reasonable procedures to check for the most commonly known viruses and to check the integrity of data, it remains the service provider's responsibility to carry out a virus check on any documents before launching them, whether to be sent or to be received on disk or otherwise. Therefore and notwithstanding any collateral contract, warranty or representation, the Fund will have no liability to the service provider on any basis, whether in contract, delict (including negligence) or otherwise, in respect of any error or omission arising from or in connection with the electronic communication of information to or from the service provider and the service provider's reliance on such information and including (but not limited to) the acts or omissions of the relevant service providers.

If the communication relates to a matter of significance on which the service provider wishes to rely and is concerned about the possible effects of electronic transmission, the service provider should request a hard copy of such transmission from the Fund.

8.7. **Validity of contract provisions**

If any provision of the Agreement is held to be invalid, in whole or in part, such provision shall be deemed not to form part of the agreement. In any event the enforceability of the remainder of the agreement will not be affected.

8.8. **Conflict**

In the event of any conflict between the Agreement and any other document that forms part of the agreement, the Agreement shall prevail except where amended by specific reference to the relevant Clause of the Terms of Business. In the event and only to the extent of any conflict between the Agreement and any referenced or attached document other than the Terms of Business, the Agreement will take precedence.

8.9. **Applicability**

The Agreement shall apply to work undertaken in relation to the service provider, its holding company or any of its subsidiary, associated or related companies, agents or sub-contractors providing services in terms of the agreement.

9. Dispute Resolution and Governing Law

Should any dispute arise between the Fund and the service provider, both parties will attempt to resolve the dispute in good faith through senior-level negotiations. If the dispute is not resolved through negotiation or mediation within a reasonable time both parties agree that it shall be finally resolved in accordance with the rules of the Arbitration Foundation of South Africa by an arbitrator or arbitrators appointed by the Foundation and agreed upon by both parties. The arbitration clause does not prohibit a party from seeking relief in a dispute where urgency can be proved, and where, as a result, application can be made for an urgent interdict, urgent declaratory order or other urgent relief to any court of competent jurisdiction, on condition that such urgent relief is only of an interim nature pending the determination of the dispute by the arbitrator. The parties submit in this regard, to the non-exclusive jurisdiction of the Gauteng Local Division, Johannesburg.

The Terms of Business and the Agreement shall be subject to South African law.

10. Quotation/Proposal Conditions Validity of Quotations

Quotations must be valid for at least 90 days from the closing date of the tender. Include original valid tax clearance certificates, proof of registration of the business, audited annual financial statements and the latest B-BBEE certification.

Disqualifying Criteria

- Failure to submit before the specified date and time
- Failure to comply with paragraph 4.6.1 to 4.6.4 of the RFP.
- A minimum of five (5) years demonstrated experience of successful provisioning of Cyber security Services/SIEM tool.
- Failure to submit requested mandatory supporting documentation in 6.6.
- Acceptance of the RFP terms and conditions – contract terms and condition shall be discussed and negotiated with the successful Bidder.

VAT

VAT must be included in all prices and costs quoted, where applicable.

Closing Date for Proposal Submission

The closing date and time for submission of proposals at the delivery address indicated is
15 September 2023 at 16h00 SA Time.

The Fund reserves the right to withdraw, at any stage of this process, amend or cancel this RFP, reject or not accept any or all proposals, obtain any information from any lawful source regarding past business history and practices of the respondent, and to take any such information into consideration in the evaluation process.

11. Acceptance

By signature of this document, the service provider agrees to be bound by the terms of business contained herein.

Signed in acceptance on behalf of ……being duly authorised thereto.

Signed at……. on this……day of……..2023

Name & Surname……

Designation……..

Signature……

Annexure A - Disqualifying checklist

No.	Document required or requirement(s)	Submitted? Yes/No
1.	Submitted as per the closing date and time.	
2.	Compliance requirement: structure of responses (4.6.1 to 4.6.4)	
3.	A minimum of five (5) years demonstrated experience of successful implementation of cyber security services and strategy as well as a SIEM solution and SOC services, with a focus on pension/ retirement funds or financial institutions or an organization of a similar size to EPPF	
4.	Acceptance of the RFP terms and conditions – contract terms and condition shall be discussed and negotiated with the successful Bidder.	
5.	A detailed statement of the company's B-BBEE credentials as required in the above, supported by a rating certificate from a SANAS accredited rating institution or a B-BBEE affidavit.	
6.	Recent Audited Financial Statement of the specific entity that will be submitting the proposal. Group or any other entity's Annual Financial Statements will not be accepted. Respondents who are not required by law to have audited financial statements must include a letter signed by an authorised official confirming that the respondent is not required by law to have audited financial statements and accordingly, is unable to provide the same.	
7.	Respondents must complete the EPPF POPIA Self Compliance Forms (EPPF Operator Privacy Due Diligence Form and Operator Privacy Compliance Self-Assessment Form)	
8.	Declaration (Formal letter) as per (6.1) under Further required submissions	
9.	A valid Tax Clearance Certificate and/or PIN indicating good standing with the South African Revenue Services (SARS).	
10.	Certified copies of CIPC company registration documentation. In the case of respondents who are not companies as envisaged in the Companies Act of 2008, equivalent founding documents must be submitted.	

NB - Please make use of the above checklist to ensure that all minimum requirements are met and to avoid being disqualified.