REQUEST FOR BIDS:

APPOINTMENT OF A SERVICE PROVIDER TO SUPPLY AND IMPLEMENT A SYSTEM INCIDENT EVENT MANAGEMENT SYSTEM (SIEM), NETWORK ACCESS CONTROL (NAC), PRIVILEDGED AND IDENTITY MANAGEMENT SYSTEMS (PAM & IAM) AND A SECURITY OPERATIONS CENTER (SOC) SERVICES INCLUSIVE OF A 3 YEAR SUPPORT AND MAINTENANCE PLAN

(BID NUMBER: PROC T671)

COMPULSORY BRIEFING SESSION: 17 JULY 2025 @11H00-13H00
VENUE: SERVICES SETA HEAD OFFICE
15 SHERBORNE ROAD, PARKTOWN, JOHANNESBURG,
2193

CLOSING DATE AND TIME: 12 August 2025 BEFORE 11H00 AM

Approved

Date: 24 July 25

CONTENTS   PAGE

BID DOCUMENTS CHECK LIST:

VERY IMPORTANT: THE CONTENTS OF THE BID/ TENDER DOCUMENT MUST BE AS FOLLOWS:

The potential bidder must submit four (4) Bid proposals, compile one (1) original, (1) electronic version (USB), make one (1) copy from the original bid document and email proposal to Tenders@serviceseta.org.za in a zipped file up to a maximum size of 100MB.

1. The Services SETA bid documents must be submitted in official format (not to be re-typed).
2. The bid proposal must be properly bonded, punched, numbered and separated per checklist schedule below.

PLEASE SUBMIT THE BID PROPOSAL AS PER AFOREMENTIONED SUBMISSION REQUIREMENTS AND BELOW CHECKLIST SCHEDULE, AS IT MAKES IT EASIER FOR THE BID EVALUATION COMMITTEE TO EVALUATE YOUR PROPOSAL. **Checklist Schedule**

Schedules	Description	Submitted: YES or NO
Schedule 1	The potential bidder must be registered with National Treasury Central Supplier Database (CSD)	
Schedule 2	Bid document must be signed and duly completed, together with all declaration of interest/standard bidding documents (**SBD's 1, 3.3, 4, 6.1 and 7.2**)	
Schedule 3	Provide and attach a copy of **Company Registration Certificate**	
Schedule 4	The potential bidder must provide proof being an OEM partner of the proposed P.A.M, N.A.C, S.I.E.M and I.A.M, solutions, additionally the bidder must be certified for ISO 9001-Quality Management, ISO 27001 -Information Security Management System	
Schedule 5	The potential bidder must submit **Proof of its B-BBEE Status Level of Contributor**	
Schedule 6	The potential bidder must be tax compliant on National Treasury Central Supplier Database (CSD) prior to award.	
Schedule 7	Capacity and Competencies, Resources, and Individuals	
Schedule 8	Project Methodology and Approach	
Schedule 9	Assignment Experience: Testimonials	
Schedule 10	Turnaround Times	

Schedule 11	Identity Documents, Cancelled Cheque or Letter from the Bank Confirming Banking Details	
Schedule 12	Pricing Schedule	
Schedule 12	Bid proposals **(4)** compile one **(1)** original, **(1)** electronic version **(USB),** make one **(1)** copy from the original bid document must be **properly bounded** and email proposal to Tenders@serviceseta.org.za in a zipped file up to a maximum size of 100MB.	

1. INVITATION TO BID **SBD 1**

PART A
INVITATION TO BID

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE (*SERVICES SETA*)					
BID NUMBER:	**PROC T671**	CLOSING DATE:	**30 JULY 2025**	CLOSING TIME:	**11H00AM**
DESCRIPTION	APPOINTMENT OF A SERVICE PROVIDER TO SUPPLY AND IMPLEMENT A SYSTEM INCIDENT EVENT MANAGEMENT SYSTEM (SIEM), NETWORK ACCESS CONTROL (NAC), PRIVILEDGED AND IDENTITY MANAGEMENT SYSTEMS (PAM & IAM) AND A SECURITY OPERATIONS CENTER (SOC) SERVICES INCLUSIVE OF A 3 YEAR SUPPORT AND MAINTENANCE PLAN				

BID RESPONSE DOCUMENTS MAY BE DEPOSITED IN THE BID BOX SITUATED AT *(STREET ADDRESS)*
*(*SERVICES SETA HEAD OFFICE)** **15 SHERBORNE ROAD,** **PARKTOWN,** **JOHANNESBURG** **2193**
NB: ALL BIDS MUST BE SUBMITTED IN THE TENDER BOX The bid **box is open during office hours:** **Monday – Thursday: 8am – 4pm** **Friday: 8am – 3pm**
NOTE! **THE RELEVANT AUTHORITY MUST SIGN IN FULL WHERE ALL PAGES OF THE SBD FORMS REQUIRED AND INITIAL** **BIDS MUST BE SUBMITTED AS 1 ORIGINAL, ELECTRONIC COPY (USB), 1 COPY AND EMAIL PROPOSAL TO Tenders@serviceseta.org.za IN A ZIPPED FILE UP TO A MAXIMUM SIZE OF 100MB, EACH MARKED AS SUCH.**

BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO		TECHNICAL ENQUIRIES MAY BE DIRECTED TO:	
CONTACT PERSON	Conny Mathebula	CONTACT PERSON	Sibusiso Mabaso
TELEPHONE NUMBER	(011) 276 9621	TELEPHONE NUMBER	011) 276 9734
FACSIMILE NUMBER	**N/A**	FACSIMILE NUMBER	**N/A**

E-MAIL ADDRESS	tenders@serviceseta.org.za	E-MAIL ADDRESS	sibusisoma@serviceseta.org.za

SUPPLIER INFORMATION

NAME OF BIDDER	
POSTAL ADDRESS	
STREET ADDRESS	

TELEPHONE NUMBER	CODE		NUMBER	
CELLPHONE NUMBER				
FACSIMILE NUMBER	CODE		NUMBER	
E-MAIL ADDRESS				
VAT REGISTRATION NUMBER				

SUPPLIER COMPLIANCE STATUS	TAX COMPLIANCE SYSTEM PIN:		**OR**	CENTRAL SUPPLIER DATABASE No:	MAAA

ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES OFFERED?	☐ Yes ☐ No [IF YES ENCLOSE PROOF]	ARE YOU A FOREIGN BASED SUPPLIER FOR THE GOODS /SERVICES OFFERED?	☐ Yes ☐ No [IF YES, ANSWER THE QUESTIONNAIRE BELOW]

QUESTIONNAIRE TO BIDDING FOREIGN SUPPLIERS

IS THE ENTITY A RESIDENT OF THE REPUBLIC OF SOUTH AFRICA (RSA)? YES ☐ NO

DOES THE ENTITY HAVE A BRANCH IN THE RSA? YES ☐ NO

DOES THE ENTITY HAVE PERMANENT ESTABLISHMENT IN THE RSA? ☐ YES ☐ NO

DOES THE ENTITY HAVE ANY SOURCE OF INCOME IN THE RSA? ☐ YES ☐ NO

IS THE ENTITY LIABLE IN THE RSA FOR ANY FORM OF TAXATION? YES ☐ NO

IF THE ANSWER IS "NO" TO ALL OF THE ABOVE, THEN IT IS NOT A REQUIREMENT TO REGISTER FOR A TAX COMPLIANCE STATUS SYSTEM PIN CODE FROM THE SOUTH AFRICAN REVENUE SERVICE (SARS) AND IF NOT REGISTER AS PER 2.3 BELOW.

PART B
TERMS AND CONDITIONS FOR BIDDING

1.	BID SUBMISSION:

	BIDS MUST BE DELIVERED BY THE STIPULATED TIME TO THE CORRECT ADDRESS. LATE BIDS WILL NOT BE ACCEPTED FOR CONSIDERATION.
1.2.	**ALL BIDS MUST BE SUBMITTED ON THE OFFICIAL FORMS PROVIDED (NOT TO BE RE-TYPED) OR IN THE MANNER PRESCRIBED IN THE BID DOCUMENT.**
1.3.	THIS BID IS SUBJECT TO THE PREFERENTIAL PROCUREMENT POLICY FRAMEWORK ACT, 2000 AND THE PREFERENTIAL PROCUREMENT REGULATIONS, THE GENERAL CONDITIONS OF CONTRACT (GCC) AND, IF APPLICABLE, ANY OTHER SPECIAL CONDITIONS OF CONTRACT.
1.4.	**THE SUCCESSFUL BIDDER WILL BE REQUIRED TO FILL IN AND SIGN A WRITTEN CONTRACT FORM (SBD7).**

2.	TAX COMPLIANCE REQUIREMENTS

2.1 BIDDERS MUST ENSURE COMPLIANCE WITH THEIR TAX OBLIGATIONS.

2.2 BIDDERS ARE REQUIRED TO SUBMIT THEIR UNIQUE PERSONAL IDENTIFICATION NUMBER (PIN) ISSUED BY SARS TO ENABLE THE ORGAN OF STATE TO VERIFY THE TAXPAYER'S PROFILE AND TAX STATUS.

2.3 APPLICATION FOR TAX COMPLIANCE STATUS (TCS) PIN MAY BE MADE VIA E-FILING THROUGH THE SARS WEBSITE WWW.SARS.GOV.ZA.

2.4 BIDDERS MAY ALSO SUBMIT A PRINTED TCS CERTIFICATE TOGETHER WITH THE BID.

2.5 IN BIDS WHERE CONSORTIA / JOINT VENTURES / SUB-CONTRACTORS ARE INVOLVED; EACH PARTY MUST SUBMIT A SEPARATE TCS CERTIFICATE / PIN / CSD NUMBER.

2.6 WHERE NO TCS PIN IS AVAILABLE BUT THE BIDDER IS REGISTERED ON THE CENTRAL SUPPLIER DATABASE (CSD), A CSD NUMBER MUST BE PROVIDED.

2.7 NO BIDS WILL BE CONSIDERED FROM PERSONS IN THE SERVICE OF THE STATE, COMPANIES
   WITH DIRECTORS WHO ARE PERSONS IN THE SERVICE OF THE STATE, OR
   CLOSE CORPORATIONS WITH MEMBERS PERSONS IN THE SERVICE OF THE STATE."

NB: FAILURE TO PROVIDE / OR COMPLY WITH ANY OF THE ABOVE PARTICULARS MAY RENDER THE BID INVALID.

SIGNATURE OF BIDDER: ………………………………………

CAPACITY UNDER WHICH THIS BID IS SIGNED: ………………………………………
(Proof of authority must be submitted e.g. company resolution)

DATE: ……………………………

SBD 3.3

(Professional Services, Software, Licenses and Hardware)

OFFER TO BE VALID FOR **120** WORKING DAYS FROM THE CLOSING DATE OF BID.

For comparison processes, bidders must indicate their prices on the basis of the following: Year One is inclusive of licensing, support, maintenance and warranties.

Deliverables	Year 1					Year 2					Year 3					Quantity	Amount Exclusive VAT)
	SOC	SEIM	PAM	IAM	NAC	SOC	SEIM	PAM	IAM	NAC	SOC	SEIM	PAM	IAM	NAC		
Software Licensing Costs																3	
Hardware Costs (if applicable)								0			0					1	
Implementation and Configuration								0			0					1	
Change Management			1					0			0					1	
Post Implementation: Service Management, Support and Maintenance cost			1					1	1							3	
Project Management			1					0			0					1	
Project Governance Documentation			1					0			0					1	
Other cost (if any) provides clear breakdown																	
Vat 15 %																	
Total Inclusive of Vat (including all other applicable charges)																	

Please Note the following:

- Services provided must reflect prices in accordance with the terms of reference;

- Bidders are also advised to indicate a total cost breakdown for this assignment;

- Own pricing schedule can be compiled to cover costs as per terms of reference;

- Bidders must clearly state the contract renewal and termination with steps of the termination process clearly identified.

1. Total bid price (incl of all applicable taxes and skills development) R……………………………

2. Period required for commencement with project after acceptance of bid………………

3. Are the rates quoted firm for the full period of contract?   **Yes or No**

4. If not firm for the full period, provide details of the basis on which adjustments will be applied or, for example consumer price index.

    …………………………………………………………..

    …………………………………………………………

   All applicable taxes" includes value- added tax, pay as you earn, income tax, Unemployment

   Insurance fund contributions and skills development levies.

   Any enquiries regarding bidding procedures may be directed to the following members in writing.

   Supply Chain Management

   Email: tenders@serviceseta.org.za

   Or for technical information –

   Email: sibusisoma@serviceseta.org.za

1. PURPOSE OF THE FORM

Any person (natural or juristic) may make an offer or offers in terms of this invitation to bid. In line with the principles of transparency, accountability, impartiality, and ethics as enshrined in the Constitution of the Republic of South Africa and further expressed in various pieces of legislation, it is required for the bidder to make this declaration in respect of the details required hereunder.

Where a person/s are listed in the Register for Tender Defaulters and / or the List of Restricted Suppliers, that person will automatically be disqualified from the bid process.

2. Bidder's declaration

2.1 Is the bidder, or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest in the enterprise,
employed by the state?   **YES/NO**

2.1.1 If so, furnish particulars of the names, individual identity numbers, and, if applicable, state employee numbers of sole proprietor/ directors / trustees / shareholders / members/ partners or any person having a controlling interest in the enterprise, in table below.

Full Name	Identity Number	Name of State institution

2.2 Do you, or any person connected with the bidder, have a relationship with any person who is employed by the procuring institution? **YES/NO**

[1] the power, by one person or a group of persons holding the majority of the equity of an enterprise, alternatively, the person/s having the deciding vote or power to influence or to direct the course and decisions of the enterprise.

2.2.1 If so, furnish particulars:

…………………………………………………………………………………

…………………………………………………………………………………

2.3   Does the bidder or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest in the enterprise have any interest in any other related enterprise whether or not they are bidding for this contract?   **YES/NO**

2.3.1 If so, furnish particulars:

………………………………………………………………………….

………………………………………………………………………….

3   DECLARATION

I, the undersigned, (name) .... in submitting the accompanying bid, do hereby make the following statements that I certify to be true and complete in every respect:

3.1   I have read and I understand the contents of this disclosure;

3.2 I understand that the accompanying bid will be disqualified if this disclosure is found not to be true and complete in every respect;

3.3 The bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with any competitor. However, communication between partners in a joint venture or consortium2 will not be construed as collusive bidding.

3.4 In addition, there have been no consultations, communications, agreements or arrangements with any competitor regarding the quality, quantity, specifications, prices, including methods, factors or formulas used to calculate prices, market allocation, the intention or decision to submit or not to submit the bid, bidding with the intention not to win the bid and conditions or delivery particulars of the products or services to which this bid invitation relates.

3.4 The terms of the accompanying bid have not been, and will not be, disclosed by the bidder, directly or indirectly, to any competitor, prior to the date and time of the official bid opening or of the awarding of the contract.

3.5 There have been no consultations, communications, agreements or arrangements made by the bidder

with any official of the procuring institution in relation to this procurement process prior to and during the bidding process except to provide clarification on the bid submitted where so required by the institution; and the bidder was not involved in the drafting of the specifications or terms of reference for this bid.

[2] Joint venture or Consortium means an association of persons for the purpose of combining their expertise, property, capital, efforts, skill and knowledge in an activity for the execution of a contract.

3.6 I am aware that, in addition and without prejudice to any other remedy provided to combat any restrictive practices related to bids and contracts, bids that are suspicious will be reported to the Competition Commission for investigation and possible imposition of administrative penalties in terms of section 59 of the Competition Act No 89 of 1998 and or may be reported to the National Prosecuting Authority (NPA) for criminal investigation and or may be restricted from conducting business with the public sector for a period not exceeding ten (10) years in terms of the Prevention and Combating of Corrupt Activities Act No 12 of 2004 or any other applicable legislation.

I CERTIFY THAT THE INFORMATION FURNISHED IN PARAGRAPHS 1, 2 and 3 ABOVE IS CORRECT.
I ACCEPT THAT THE STATE MAY REJECT THE BID OR ACT AGAINST ME IN TERMS OF PARAGRAPH 6 OF PFMA SCM INSTRUCTION 03 OF 2021/22 ON PREVENTING AND COMBATING ABUSE IN THE SUPPLY CHAIN MANAGEMENT SYSTEM SHOULD THIS DECLARATION PROVE TO BE FALSE.

………………………………	..…………………………………………
Signature	Date

………………………………	……………………………………………
Position	Name of bidder	**SBD**

6.1
4. PREFERENCE POINTS CLAIM FORM IN TERMS OF THE PREFERENTIAL PROCUREMENT REGULATIONS 2022

This preference form must form part of all tenders invited. It contains general information and serves as a claim form for preference points for specific goals.

NB: BEFORE COMPLETING THIS FORM, TENDERERS MUST STUDY THE GENERAL CONDITIONS, DEFINITIONS AND DIRECTIVES APPLICABLE IN RESPECT OF THE TENDER AND PREFERENTIAL PROCUREMENT REGULATIONS, 2022

**1.	GENERAL CONDITIONS**

1.1	The following preference point systems are applicable to invitations to tender:

- the 80/20 system for requirements with a Rand value of up to R50 000 000 (all applicable taxes included); and

- the 90/10 system for requirements with a Rand value above R50 000 000 (all applicable taxes included).

1.2 To be completed by the organ of state

(*delete whichever is not applicable for this tender*).

a) The applicable preference point system for this tender is the 90/10 preference point system.

b) The applicable preference point system for this tender is the 80/20 preference point system.

c) Either the 90/10 or 80/20 preference point system will be applicable in this tender. The lowest/ highest acceptable tender will be used to determine the accurate system once tenders are received.

1.3 Points for this tender (even in the case of a tender for income-generating contracts) shall be awarded for:
(a) Price; and

(b) Specific Goals.

1.4 To be completed by the organ of state:

The maximum points for this tender are allocated as follows:

	POINTS	POINTS
PRICE	90	80
SPECIFIC GOALS	10	20
Total points for Price and SPECIFIC GOALS	100	100

1.5 Failure on the part of a tenderer to submit proof or documentation required in terms of this tender to claim points for specific goals with the tender, will be interpreted to mean that preference points for specific goals are not claimed.

1.6 The organ of state reserves the right to require of a tenderer, either before a tender is adjudicated or at any time subsequently, to substantiate any claim in regard to preferences, in any manner required by the organ of state.

2. DEFINITIONS

(a) **"tender"** means a written offer in the form determined by an organ of state in response to an invitation to provide goods or services through price quotations, competitive tendering process or any other method envisaged in legislation;

(b) **"price"** means an amount of money tendered for goods or services, and includes all applicable taxes less all unconditional discounts;

(c) **"rand value"** means the total estimated value of a contract in Rand, calculated at the time of bid invitation, and includes all applicable taxes;

(d) **"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; and

(e) **"the Act"** means the Preferential Procurement Policy Framework Act, 2000 (Act No. 5 of 2000).

## 3.	FORMULAE FOR PROCUREMENT OF GOODS AND SERVICES

### 3.1.	POINTS AWARDED FOR PRICE

3.1.1 THE 80/20 OR 90/10 PREFERENCE POINT SYSTEMS

A maximum of 80 or 90 points is allocated for price on the following basis:

80/20   **or**   **90/10**

$$Ps = 80 \left(1 - \frac{Pt - Pmin}{Pmin}\right) \text{ or } \qquad Ps = 90 \left(1 - \frac{Pt - Pmin}{Pmin}\right)$$

Where

Ps   =   Points scored for price of tender under consideration

Pt   =   Price of tender under consideration

Pmin =   Price of lowest acceptable tender

### 3.2.	FORMULAE FOR DISPOSAL OR LEASING OF STATE ASSETS AND INCOME GENERATING PROCUREMENT

### 3.2.1.	POINTS AWARDED FOR PRICE

A maximum of 80 or 90 points is allocated for price on the following basis:

80/20   **or**   **90/10**

$$Ps = 80 \left(1 + \frac{Pt - Pmax}{Pmax}\right) \text{ or } Ps = 90 \left(1 + \frac{Pt - Pmax}{Pmax}\right)$$

- **Where:**

    Ps   =   Points scored for price of tender under consideration

    Pt   =   Price of tender under consideration

    Pmax =   Price of highest acceptable tender

4. POINTS AWARDED FOR SPECIFIC GOALS

4.1. In terms of Regulation 4(2); 5(2); 6(2) and 7(2) of the Preferential Procurement Regulations, preference points must be awarded for specific goals stated in the tender. For the purposes of this tender the tenderer will be allocated points based on the goals stated in table 1 below as may be supported by proof/ documentation stated in the conditions of this tender:

4.2. In cases where organs of state intend to use Regulation 3(2) of the Regulations, which states that, if it is unclear whether the 80/20 or 90/10 preference point system applies, an organ of state must, in the tender documents, stipulate in the case of:

      (a) an invitation for tender for income-generating contracts, that either the 80/20 or 90/10 preference point system will apply and that the highest acceptable tender will be used to determine the applicable preference point system; or

      (b) any other invitation for tender, that either the 80/20 or 90/10 preference point system will apply and that the lowest acceptable tender will be used to determine the applicable preference point system,

then the organ of state must indicate the points allocated for specific goals for both the 90/10 and 80/20 preference point system.

Table 1: Specific goals for the tender and points claimed are indicated per the table below.

(Note to organs of state: Where either the 90/10 or 80/20 preference point system is applicable, corresponding points must also be indicated as such.

Note to tenderers: The tenderer must indicate how they claim points for each preference point system.)

The specific goals allocated points in terms of this tender	Number of points allocated (90/10 system) (To be completed by the organ of state)	Number of points allocated (80/20 system) (To be completed by the organ of state)	Number of points claimed (90/10 system) (To be completed by the tenderer)	Number of points claimed (80/20 system) (To be completed by the tenderer)
Black People Ownership	3	6		
Woman Ownership	4	8		

Youth Ownership	2,5	5		
Disability Ownership	0,5	1		
Total	**10**	**20**		

DECLARATION WITH REGARD TO COMPANY/FIRM

4.3.   Name of company/firm……………………………………………………………………….

4.4.   Company registration number: …………………………………………………………...

4.5.   TYPE OF COMPANY/ FIRM

	☐ Partnership/Joint Venture / Consortium
One-	☐ person business/sole propriety
Close	☐ corporation
Public	☐ Company
Personal	☐ Liability Company
(Pty)	☐ Limited
Non-	☐ Profit Company
State	☐ Owned Company
	[TICK APPLICABLE BOX]

4.6. I, the undersigned, who is duly authorised to do so on behalf of the company/firm, certify that the points claimed, based on the specific goals as advised in the tender, qualifies the company/ firm for the preference(s) shown and I acknowledge that:

i)   The information furnished is true and correct;

ii)   The preference points claimed are in accordance with the General Conditions as indicated in paragraph 1 of this form;

iii)   In the event of a contract being awarded as a result of points claimed as shown in paragraphs 1.4 and 4.2, the contractor may be required to furnish documentary proof to the satisfaction of the organ of state that the claims are correct;

iv)   If the specific goals have been claimed or obtained on a fraudulent basis or any of the conditions of contract have not been fulfilled, the organ of state may, in addition to any other remedy it may have –

(a)   disqualify the person from the tendering process;

(b)   recover costs, losses or damages it has incurred or suffered as a result of that person's conduct;

(c)   cancel the contract and claim any damages which it has suffered as a result of having to make less favourable arrangements due to such cancellation;

(d)   recommend that the tenderer or contractor, its shareholders and directors, or only the shareholders and directors who acted on a fraudulent basis, be restricted from obtaining business from any organ of state for a period not exceeding 10 years, after the *audi alteram partem* (hear the other side) rule has been applied; and

(e)   forward the matter for criminal prosecution, if deemed necessary.

```
                    ..........................................
                    SIGNATURE(S) OF TENDERER(S)


SURNAME AND NAME:      ...............................................

DATE:                  ...............................................

ADDRESS:               ...............................................

                       ...............................................

                       ...............................................
```

5. CONTRACT FORM - RENDERING OF SERVICES   SBD 7.2

THIS FORM MUST BE FILLED IN DUPLICATE BY BOTH THE SERVICE PROVIDER (PART 1) AND THE PURCHASER (PART 2). BOTH FORMS MUST BE SIGNED IN THE ORIGINAL SO THAT THE SERVICE PROVIDER AND THE PURCHASER WOULD BE IN POSSESSION OF ORIGINALLY SIGNED CONTRACTS FOR THEIR RESPECTIVE RECORDS.

PART 1 (TO BE FILLED IN BY THE SERVICE PROVIDER)

1.   I hereby undertake to render services described in the attached bidding documents to (name of the institution) .... in accordance with the requirements and task directives / proposals specifications stipulated in Bid Number .... at the price/s quoted. My offer/s remain binding upon me and open for acceptance by the Purchaser during the validity period indicated and calculated from the closing date of the bid .

2.   The following documents shall be deemed to form and be read and construed as part of this agreement:

(i)   Bidding documents, *viz* - Invitation to bid;
         -     Proof of tax compliance status;
         -     Pricing schedule(s);
         -     Filled in task directive/proposal;
         -     Preference claim form for Preferential Procurement in terms of the Preferential Procurement Regulations;
         -     Bidder's Disclosure form;
         -     Special Conditions of Contract;
(ii)   General Conditions of Contract; and
(iii)   Other (specify)

3.   I confirm that I have satisfied myself as to the correctness and validity of my bid; that the price(s) and rate(s) quoted cover all the services specified in the bidding documents; that the price(s) and rate(s) cover all my obligations and I accept that any mistakes regarding price(s) and rate(s) and calculations will be at my own risk.

4.   I accept full responsibility for the proper execution and fulfilment of all obligations and conditions devolving on me under this agreement as the principal liable for the due fulfillment of this contract.

5.   I declare that I have no participation in any collusive practices with any bidder or any other person regarding this or any other bid.

6.   I confirm that I am duly authorised to sign this contract.

NAME (PRINT)   ……………………………

CAPACITY   …………………………..

SIGNATURE   …………………………..

NAME OF FIRM   ……………………………

DATE   …………………………..

WITNESSES
1   …………………………….

CONTRACT FORM - RENDERING OF SERVICES

PART 2 (TO BE FILLED IN BY THE PURCHASER)

1.   I……………………………………………. in my capacity as…………………….………………………………..
accept your bid under reference number ………………dated .... for the rendering of services indicated hereunder and/or further specified in the annexure(s).

2.   An official order indicating service delivery instructions is forthcoming.

3.   I undertake to make payment for the services rendered in accordance with the terms and conditions of the contract, within 30 (thirty) days after receipt of an invoice.

APPOINTMENT OF A SERVICE PROVIDER TO SUPPLY AND IMPLEMENT A SYSTEM INCIDENT EVENT MANAGEMENT SYSTEM (SIEM), NETWORK ACCESS CONTROL (NAC), PRIVILEDGED AND IDENTITY MANAGEMENT SYSTEMS (PAM) AND A SECURITY OPERATIONS CENTER (SOC) SERVICES INCLUSIVE OF A 3 YEAR SUPPORT AND MAINTENANCE PLAN	PRICE (ALL APPLICABLE TAXES INCLUDED)	COMPLETION DATE	TOTAL PREFERENCE POINTS CLAIMED	POINTS CLAIMED FOR EACH SPECIFIC GOAL

4.   I confirm that I am duly authorised to sign this contract.

SIGNED AT …………………………………ON……………………………..

NAME (PRINT)   ………………………………….

SIGNATURE   …………………………………

OFFICIAL STAMP

	WITNESSES
	…………………………….

6. AUTHORITY
FOR SIGNATORY

Signatories for close corporations and companies shall confirm their authority **by attaching to this form** a duly signed and dated copy of the relevant resolution of their members or their board of directors, as the case may be.

An example for a company is shown below:

" By resolution of the board of directors passed on__20_____   Mr
_____has been duly authorized to sign all

documents in connection with the Tender for Contract _____

No _____and any Contract, which may arise there from on behalf of

_____

SIGNED ON BEHALF OF THE COMPANY:_____

IN   HIS   CAPACITY   AS:

_____

DATE: _____
_

SIGNATURE OF SIGNATORY:_____ _____

AS WITNESSES: 1_____

                      2_____

7. TERMS OF REFERENCE / SPECIFICATIONS

APPOINTMENT OF A SERVICE PROVIDER TO SUPPLY AND IMPLEMENT A SYSTEM INCIDENT EVENT MANAGEMENT SYSTEM (SIEM), NETWORK ACCESS CONTROL (NAC), PRIVILEDGED AND IDENTITY MANAGEMENT SYSTEMS (PAM) AND A SECURITY OPERATIONS CENTER (SOC) SERVICES INCLUSIVE OF A 3 YEAR SUPPORT AND MAINTENANCE PLAN

1. INTRODUCTION AND OVERALL OBJECTIVES

The Services Sector Education and Training Authority (SSETA) was established and registered in March 2000 in terms of the Skills Development Act of 1998. The SETA aims to provide for the skills development needs of the services sector through the bursary awards and implementation of learnerships, disbursement of grants and monitoring of education and training.

The Services Sector Education and Training Authority (Services SETA) hereby invites approved service providers to supply and implement a System Incident Event Management System (SIEM), User Lifecycle, Remote Access, Network Access Control, Priviledged and Identity Management Systems and a Security Operations Center (SOC) services inclusive of a 3-year support and maintenance plan

2. BACKGROUND

Service SETA ICT in currently in the process of implementing its SSIIMS (Services Seta Integrated Information Management) strategy. The SSIIMS strategy is underpinned by the need to ensure integration, optimisation and automation phase of modern workloads in line with today's rapidly evolving digital landscape. The ability to communicate and collaborate effectively across various locations is paramount. The performance requirements of modern business applications far exceed what legacy software and hardware can deliver.

3. SCOPE OF WORK/ DELIVERABLE

3.1 AI Integrated/Powered SOC

- AI-Powered Threat Detection: Use of AI models to detect anomalous behaviour, zero-day attacks, and advanced persistent threats (APTs).
- Automated Incident Response: Implement AI-driven playbooks automate incident response, isolation, and remediation.
- Threat Intelligence and Predictive Analytics: Showcase AI-based predictive analytics for proactive threat hunting.
- Natural Language Processing (NLP): Demonstrate NLP capabilities for analyzing security alerts, logs, and threat intelligence reports.
- Machine Learning (ML) for Risk Scoring: Show how ML models prioritize threats based on risk scores.
- The SOC solution must be deployable on the latest Linux, operable in on-prem or private cloud infrastructures.
- Role-Based Access Control (RBAC) must allow fine-grained control across Super Admin, SOC Manager, and Analyst views.
- System must utilize in-memory, non-linear correlation and AI clustering models to group related incidents.
- Provide an integrated AI Co-Pilot, powered by LLMs, to auto-generate:
- Executive summary of alerts
- Triage instructions
- Threat attribution and campaign linkage
- Remediation scripts and guided responses
- Full multi-tenancy support with auditable user and incident action logs

3.2 SIEM (Security Incident and Event Management) Integrated to Trend Micro Vision One

- SIEM User-friendly: A user-friendly interface that allows security analysts to easily manage and retrieve log data and is characterized by its ease of use, intuitive interface, and customizable features, making it accessible to a wide range of users, including security analysts and administrators, without requiring extensive technical expertise, to ensures efficient incident detection, response, and management, ultimately enhancing the overall security posture of Services SETA.
- Real-time threat detection: An integrated SIEM that identifies and alerts all security incidents.

- Log correlation and analysis: Use logs from Sentinel Microsoft EA E5, TrendMicro Vision One MXDR, and FortiGate 1 x 200E and 9 x T40F next Gen Firewalls, must be collected, correlated, and analysed.
- SIEM Performance: Effectively test SIEM performance, simulate attack scenarios, analyze key performance indicators (KPIs), review alerts and notifications, and evaluate the SIEM's ability to handle data ingestion and scalability. A thorough evaluation should also consider the SIEM's data normalization and correlation capabilities, as well as its ability to reduce false positives.

- Automated incident response: Showcase automated playbooks for threat containment.
- Data Enrichment: SIEM systems able to enrich log data with additional information, such as threat intelligence, to improve analysis and detection. Effectively test SIEM data enrichment, focus on accuracy, coverage, and relevance. Conduct tests our enrichment process against known good and bad indicators of compromise (IOCs), and ensure the added context improves threat detection and investigation efficiency.
- Compliance reporting: Demonstrate automated reporting for ISO 27001, and POPIA.
- The logging engine must support a sustained ingestion rate of over 3000 EPS, scalable to 30000 EPS, utilizing an advanced hot-log compression mechanism that outperforms conventional storage engines by 40x to 100x. The disk usage for 365 days of 5000 EPS hot storage must not exceed 5 TB, ensuring cost-effective scalability.
- The required disk size for 5000 EPS for 3 years, archive and back up available must not exceed 15 TB.
- Logs must be maintained in a live-accessible, hot-layer state for a minimum of 720 days, with support for max 10-year retention in warm/cold layers.
- Masquerading and Random String Entropy Analysis to detect obfuscated malware behaviors and DGA-based C2 communications.
- SQL-Streaming Rules Engine for immediate, inline analytics of time-series log data with join, filter, group, regex, and suppression support
- Detection logic must be defined in a Rules-as-Code framework (SQL, JSON, Java, MySQL, Python syntax), compatible with DevSecOps pipelines.
- The engine must offer:
- CEP (Complex Event Processing)-based rule chaining.
- Real-time Sigma Rule Execution and support for manual Sigma mapping.
- A wizard-based correlation rule builder with drag-and-drop support for non-technical analysts.
- Native support for MITRE ATT&CK mapping within rules for context-aware alerting.
- Correlation Rule Development Wizard must be available.
- Built in Security Benchmarking, Risk Prioritization and Compliance Reporting must be available

3.3 Identity and Access Management (IAM)

- User lifecycle management: Implement automated user provisioning and deprovisioning across the whole applications and systems landscape.
- Role-based access control (RBAC): Show how access is managed based on user roles.
- Privileged access management: Demonstrate session recording, monitoring, and approval workflows.
- Combining IAM and SIEM: Combining IAM (Identity and Access Management) and SIEM (Security Information and Event Management) provide a more holistic view of Services Seta's security posture by integrating user access information with security event data. This integration to allow for more accurate and timely detection of potential threats and anomalies, as well as improved incident response.
- Multi-factor authentication (MFA): Showcase MFA for remote access to sensitive systems.
- Flexible Deployment Models: Supports both cloud-based and on-premise operation (OnPremise Priority), with compatibility across virtual platforms including ESX and Hyper-V.
- Adaptive Access Controls: Enforcement rules can be created based on user identity, group, IP range, RADIUS client, time, location, and risk profile.
- Token and Biometric Options: Includes OTPs, mobile authenticator apps, push-based approvals, and biometric prompts via mobile application, available on iOS, Android, and Huawei devices.
- Detailed Audit Logging: Provides full audit trails, including token registration status, SMS delivery logs, and syslog-compatible log exports.
- Identity Threat Detection and Response (ITDR) features must be provided.
- Behavioral Learning Engine: Continuously builds user baselines (login times, devices, access patterns) to detect anomalies.
- Automated Response Mechanisms: Initiates MFA, session termination, or account lockdowns upon detection of credential abuse or lateral movement indicators.
- Automated Remediation for Credential Leaks: The system must integrate with the organization's Digital Risk Protection (DRP) solution. Upon detection of leaked or compromised credentials (e.g., from dark web monitoring), the platform must automatically validate the status of these credentials. If still in use, it must trigger an immediate password reset or access revocation workflow, minimizing exposure.
- Threat Intelligence Fusion: Correlates login attempts with known malicious IPs, TOR exit nodes, VPN/proxy traffic, and root/jailbroken device usage.
- Compliance and MITRE Alignment: Supports classification of threats using MITRE ATT&CK framework and generates compliance-aligned forensic reports.
- Simulation and SOAR Integration: Enables attack simulation for security testing and integrates with SOAR and SIEM tools via API for automated remediation.

- Integration to exiting systems: Integration to the following systems will be required (LMIS, DG Portal, Learner Portal, Dynamics 365 FnO and CE, E-Learning).

3.4 Network Access Control (NAC)

- Device compliance checks: Implement endpoint compliance checks before granting network access.
- Guest access management: Implement guest devices are management and isolation.
- Policy-based access control: Implement dynamic access controls based on user roles and device type.
- System Architecture and Scalability
- Must support up to a minimum of 3000 concurrent endpoints with capability for scalable expansion.
- Deployed in a high-availability configuration across two primary data centers.
- Includes redundant application and management servers to ensure fault tolerance and central administration.
- Core Capabilities
- Agentless and Agent-Based Profiling: Visibility and classification of all connected devices using MAC OUI, DHCP, HTTP headers, SNMP, and RADIUS accounting.
- Dynamic Access Control: Real-time enforcement via VLAN assignment, microsegmentation, and adaptive policies based on device type, user identity, and compliance status.
- Captive Portal: Self-service onboarding portals for employees, contractors, guests, and IoT/headless devices, with customizable workflows and branding.
- Automated Compliance Enforcement: Devices not meeting security posture policies should be redirected to a remediation VLAN with intuitive user guidance to restore compliance.
- Policy Automation and Threat Response: Rule-based engine to dynamically react to unauthorized behavior such as MAC spoofing or policy violations.
- VOIP/IP Support: Ensures uninterrupted service for VoIP/IP phones through passthrough mechanisms and VLAN tagging.
- Contextual Intelligence Integration: Shares device context (identity, OS, posture) with SIEM, firewalls, and other security platforms via APIs and syslog.
- Supported Features
- Port-level control and role-based access enforcement.
- Integrated RADIUS support with options for proxy or standalone operation.
- Lightweight agents, optional for enhanced device posture visibility.
- Flexible registration and segmentation for IoT and browser-less devices.
- Application usage control and Acceptable Use Policy (AUP) enforcement.

- Device patch-level visibility with capability to detect 25,000+ CVEs and integrate with endpoint protection engines.
- Real-time dashboards with alerting, auditing, compliance metrics, and system health monitoring.
- Seamless interoperability with multivendor environments.
- Support for IEEE 802.1X, MAC Authentication Bypass (MAB), and fallback captive portal access.
- Directory services integration (Active Directory, RADIUS) with contextual identity-based policy enforcement.
- Deployment Flexibility
- Hybrid Deployment Mode: Ability to operate locally through a headless AAA server while maintaining centralized cloud management ensuring operational continuity during Internet outages.
- Cloud-based or virtual appliance options (VMware, Hyper-V, Azure) with specifications supporting up to 25,000 devices per instance.
- Regulatory Compliance
- Enforces security policies aligned with regulatory frameworks such as NERC, CISA, PCI, HIPAA, SOC2, SOX, GLBA, and POPIA
- Generates audit-ready reports for device activity, compliance enforcement, and access events

3.5 Security Operations Center (SOC) Services

- 24/7 monitoring: Implement real-time monitoring and alerting capabilities.
- Threat intelligence integration: Use of threat intelligence feeds are used for proactive defence.
- Incident response: Demonstrate incident detection, escalation, and response workflows.
- SOC automation: Use of AI and automation for threat hunting and response.
- Provide 24/7 technical support for incident response and troubleshooting.
- Perform AI-driven tuning and optimization of security models for evolving threats.
- Apply software updates, security patches, and compliance audits regularly.
- Conduct periodic security health checks to assess system performance.
- Review and enhance security policies and response playbooks based on emerging risks.

3.6 Reporting and Compliance

- Automated compliance reports: Demonstrate reports for ISO 27001, GDPR, POPIA compliance.
- Audit trail and log management: Showcase secure storage and retrieval of audit logs.
- Security dashboards: Demonstrate dashboards for security posture and incident tracking.

3.7 Continuous Monitoring & Improvement

- Leverage advanced threat analytics to improve proactive threat detection.
- Conduct quarterly security assessments to identify vulnerabilities and areas for enhancement.

- Implement SOC automation and orchestration to reduce response times.
- Generate executive-level security reports with insights on risk posture and incident trends.

3.8 Documentation Requirements

- Technical proposal: Detailing integration, security, and compliance.
- Live demo agenda: Including key features to be demonstrated.
- User manuals and documentation: For post-deployment reference.

a. Network Access Control Deliverables

Functionality Criteria	YES	NO	COMMENTS
1. The offered solution must provide comprehensive visibility of the network by automatically discovering, classifying, and controlling endpoints connected to the network to enable the appropriate services.			
2. Solution must automatically enforce security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area with appropriate notifications to the administrator.			
3. Solution must have centralized architecture with web or GUI based dashboard console for monitoring, reporting, notification, maintaining and policy push for the registered users centrally.			
4. Solution must support remote access capabilities on its management interface via HTTPS or SSH access.			
5. Solution must be capable of agentless device discovery and control.			

6. The proposed solution must support monitoring of traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc., simultaneously.			
7. The solution should be capable of being bypassed in the event of any failure of the solution.			
8. The solution must support approval for guest users connecting into the network and the approval request should have control from multiple administrators to avoid single point of failure.			
9. Solution must have capability to determine whether users are accessing the network on an authorized, policy-compliant device.			

10. Solution must have capability to establish user identity, location, and access history, which can be used for compliance and reporting.			
11. Solution must have capability to grant authenticated users with access to specific segments of the network, or specific applications and services, or both, based on authentication results.			
12. Solution must have capability to assign services based on the assigned user role, group, and associated policy (job role, location, device type, and so on).			
13. The solution must allow authentication and authorization of users and endpoints via wired, wireless, and VPN with consistent policy throughout the network.			

14. The solution must operate within a heterogeneous network with devices from multiple vendors. The solution should support vendor agnostic infrastructure.			

15. The NAC Solution must auto execute the following endpoint checks for compliance for all eligible endpoints: • Block all malicious devices equipped with hardware and software for hacking or spyware. • Check operating system/service packs/hotfixes • Check process, registry, file & application • Check for Antivirus installation/Version/ Antivirus Definition Date • Check for Antispyware installation/Version/ Antispyware Definition Date • Check for windows update running & configuration.			
16. Solution must support following remediation options for windows endpoints: • File remediation to allow clients download the required file version for compliance • Link remediation to allow clients to click a URL to access a remediation page or resource • Antivirus remediation to update clients with up- to-date file definitions for compliance after remediation. • Launch program remediation to remediate clients by launching one or more applications for compliance. • Windows update remediation to ensure Automatic			

• Updates configuration is turned on Windows clients per security policy.			
17. The proposed NAC solution must integrate with existing Network security tools LDAP, MS Active Directory, and RADIUS authentication servers for user authentication.			
18. The proposed solution must be able to integrate with existing Antivirus solution.			
19. Solution must have built-in various reports and can create custom reports like Executive report, detection life cycle report, Top 10 reports for various category and Health reports etc.			
20. Environment currently consists of approximately 450 internal users. The solution should cover a minimum of approximately 3000 end points.			
21. The Proposed NAC Solution must be listed on the Gartner Magic Quadrant, within the last two years.			

b. Privileged Access Management (PAM) Specifications

GENERAL	Bidders Response (Yes/No) [OEM supporting reference links are admissible.]	
Specifications	**Yes/ No**	**Comments**
Gartner Position - Propose solution must be listed in the Gartner MQ report		

1. The proposed solution shall support following functionality		
a) Secure and manage privileged password		
b) Strong authentication and Single Sign on (SSO)		
c) Application to Application password management		
d) Access and Command control		
e) Audit trail and Session Recording		
f) Workflow management		

g) Smart grouping of asset		
h) Scanner and onboarding		

2. Solution must be from leader's quadrant of last published Gartner report for PAM		
3. Solution should provide application driven database.		
4. Solution should be capable of delivering through single appliance for all roles. (Single appliance/server for password/session and reporting etc.)		
High Availability and DR functionality		
1. The solution should have High Availability at DC and DR separately.		
2. The proposed solution shall support for high redundancy or DR architecture even when deployed on different network segments or locations.		

3. The password vault must be highly reliable, the switch over to HA/DR should be seamless without manual intervention, and provisions should be available to recover credentials securely in case of catastrophic failures.		
4. Data replication between different network segments shall be performed natively without the need for external solution or infrastructure		
Asset Management and Discovery		
The solution shall have bulk loading capability to import managed systems, privileged accounts, users, and other necessary objects.		
The solution shall have the capability to record system information for managed systems including but not limited to IP address, MAC address, and DNS name, owner of the system, platform type and version.		
The solution shall allow administrator to define custom attributes for both managed system and privileged account.		
The solution shall have the capability to discover and inventory all privileged and non-privileged accounts in known and unknown systems including but not limited to:		
Windows		
Unix/Linux		
Mac OS		
Directories (AD/LDAP)		
Databases		
Network Devices		

The solution shall provide distributed discovery engine capability that allows asset to be discovered across different isolated network segments and geographical regions and report discovery result back centrally.		

The solution shall have the capability to discover Windows Services and Scheduled Tasks so that privileged credentials used by them can be managed automatically.		
The solution shall have the capability to discover Active Directory domain accounts and automatically link discovered accounts to specific member servers for user to request for access.		
The solution shall have the capability to discover software that are installed and ports are open in the target system.		
The solution shall have the capability to group target systems based on discovered and custom defined system attributes.		
The solution shall have the capability to group systems and accounts based on the result of AD/LDAP query.		
The solution shall have the capability to send email notification to designated personnel upon discovering new target systems or found systems are no longer reachable.		
The solution shall have the capability to discover new privileged accounts and on-board them for password management automatically.		
Password Management / Credential management		
The solution should have a strong inbuilt password vault/management system with single-sign-on feature.		
Password vault should be replicated over a secured channel and offsite data backup; data restoration capabilities should be offered.		

Should be able to create flexible password management policies for assets. A policy can be applied to an object/a group of objects or a group of policies can be applied to an asset/group of assets/objects.		
After dynamically discovering resources /services/ processes, the solution should be able to propagate password changes to relevant targets across the network to avoid the potential for service disruptions and lockouts whenever changes are made.		
Product should allow bulk operations to be performed on managed accounts (such as force password change immediately, reconcile password, verify password). Solution must support scheduled password changes.		
Solution must protect password change process against race conditions like a failed attempt to update password on target system (password in vault should not be updated) or inability/ delay in determining if the password has successfully been updated on target systems or application configuration files (old password shouldn't be removed from the vault).		
The solution should have the capability to reset individual passwords or groups of passwords on-demand, and to schedule automated checks to ensure that each password stored in the database correctly matches the current login for each target account.		

Solution should be able to change password on demand, on the basis of a specific criteria or policy, automatically or manually, support password verification, reconciliation and reporting, set password parameters like constitution, history, and change timings.		
The solution should be able to manage passwords stored as plain or encrypted, hardcoded in system files or user-defined files, database tables, network devices etc. including within application configuration files, code or scripts.		
The solution should restrict the solution administrators from accessing or viewing passwords or approving password requests.		

The proposed solution shall have support password policies Ability to set a minimum password length and complexity for super-user accounts across all systems in a single master policy		
The solution should have provisions to provide credentials for authenticating applications/scripts during run-time.		
100% availability of business applications - The product should support non-connectivity scenarios e.g. network outages, so that the password will still be available to the application, although there is no connection to the secure storage where the password is stored.		
Automated Password Vaulting & Rotation – Stores privileged credentials in an encrypted vault and rotates passwords based on policies.		
Just-In-Time (JIT) Access – Provides time-limited access to credentials instead of long-term ownership.		

Session Recording & Monitoring – Tracks and records privileged sessions for audit and compliance.		

Credential Injection (No Direct Password Exposure) – Users authenticate without ever seeing the actual password.		
Approval Workflows & MFA Enforcement – Requires additional authentication (multi-factor authentication) before accessing sensitive credentials.		

Least Privilege Enforcement – Ensures users only get the minimum necessary access.		
Integrations with SIEM & ITSM – Connects with security monitoring and ticketing systems for monitoring and better governance.		
Eliminates the Need for Stored Passwords – Uses identity-based authentication instead of static credentials.		
FIDO2 & Biometric Authentication Support – Allows authentication via fingerprint, facial recognition, or security keys.		
Adaptive Authentication – Uses risk-based policies to determine authentication requirements dynamically.		
Secure Credential Injection – Logs users into systems without exposing credentials.		
Zero-Trust Security Model – Ensures authentication is based on strong identity verification, not passwords.		
Reduces Phishing & Credential Theft Risks – Eliminates passwordbased attacks such as credential stuffing and phishing.		

Enhanced Compliance & Auditability – Provides detailed logs of access without storing credentials.		
Azure 2 MFA Integration with PAM		
The proposed solution should have functionality to integrate with Azure Multi Factor authentication.		
Access Management		
1 The solution should provide web-based interface for easy access and management.		
2 The solution should be able to automatically and dynamically provision users in real time with trusted Windows domains, popular directories such as AD/ LDAP /TACACS+/RADIUS servers in accordance to the user entitlements and access privileges granted (based on least privileges principle).		
3 The solution should be able to support granular command filtering or context sensitive entitlements on various platforms for super-user privileged management. Solution should also be able to detect and support concurrent login to managed systems as a privileged user		
4 The solution should be capable of organizing / grouping target server device accounts into logical groups and apply granular/finegrained access control to access the individual accounts or the groups of accounts.		
5 The solution must support full Segregation of Duties - e.g. roles are clearly and unambiguously defined with no overlapping. In addition to user access roles and entitlements, solution should also support role based administrative access to provide Segregation of Duties for administrative management and control.		

6 It should be capable of having dual control systems (makerchecker) for approval and authorization of critical operations.		
7 The user permission should be only as per his original privilege even he 'SU'es after logging in to the OS. Using root user credentials does not provide root privileges. Capability to restrict users to use RDP or SSH to other end-points.		
8 The solution should have login security by limiting user login by parameters like originating IP address, terminal ID, type of login program or time of the day or geographical location etc. and limited concurrent login sessions by user.		
9 The solution should be capable of maintaining details of shared/pooled accounts by mapping it to the individual users.		
10 The solution should be capable to have command level restrictions, i.e. of assigning specific commands to be run by specific users/groups, from specific nodes etc. The solution should be able to block commands from command line and also in queries as configured for users/groups/target resources.		
11 The solution must be able to integrate with vulnerability management solutions for deep, authenticated scans (e.g. Nexpose by Rapid7) i.e. should be able to provide credentials to these scanning applications during run-time		
Workflows, Auditing/Reporting		
1 The solution should have ability to enforce approval workflow.		
2 The solution should support a workflow approval process that is flexible to assign multiple approvers based on product or model (I.e. require 2 or more approvals before access is allowed).		
3 The Solution should be able to provide delegation of management tasks like approval / review etc. Should support easy customization of approval workflows according to business needs (without requiring code changes). Solution should also be able to support emergency/ break glass scenarios.		

4 The solution should provide a central live Dashboard covering features like management of devices, events and password policies, user activities, event logs etc.		
5 The system should have all regular pre-configured report templates like entitlements reports, user activities, privileged accounts inventory, applications inventory, compliance reports etc., capability to create custom reports based on users, events, activities, target systems, password uses and status etc., ability to run all reports by frequency, on-demand and schedule them.		
6 The reports generation should support CSV, Excel or PDF. This report extraction should not have any performance impact & feature for report extraction should be available on demand & scheduled. The solution should support customizable reports.		
7 The solution should record access to the Web console for password requests, approvals and check-out, delegation changes, reporting and other activities, access to its management console for configuration and reporting, and all password change job activity.		
8 The solution should be able to record sessions, take videos recording of screen shots, keystrokes / commands and output, replay sessions for forensic purposes. And provide optimized search capabilities on different parameters like users, events, time, target resources etc.		
9 The solution should have real-time session monitoring support and full audit trail for user activities in the solution itself.		
10 The solution should be configurable so that events can trigger email/ SMS alerts, run specific programs		
11 The solution should be capable of alerting on actions such as password requests and check-outs, password changes, failed password change jobs, console and web application activities etc. and attempts of access violations (running elevated/ higher privilege commands, modifying password/ user files, adding users to privileged groups etc.).		

12 Solution should have Log retention [all logs, recording, access data, accounting etc.] for minimum 6 months with RAID 5 storage of 1 TB.		
13 The solution shall ensure proper segregation of duties with Role Based Access Control (RBAC) capability such that roles and accesses are properly defined.		
14 The solution shall minimally support requester, approver and reviewer roles for segregation of duties.		
15 The solution shall have the capability to dynamically group managed accounts based on criteria including but not limited to platform type, platform version, domain name, IP address, system name, account name, account privilege, etc. so that they can be effectively granted to appropriate users for request.		
16 The solution must ensure personal accountability when user granted privileged password and session for shared account.		

17 The solution shall support policy driven workflow and allow easy configuration through web interface to route password and session request to appropriate approver(s).		
Solution must support at both DC and DR in HA mode and also with DC-DR functionality.		
a. The users at DC should access the targeted devices primarily through PAM solution at DC.		
b. In case primary PAM at DC fails, the users at DC should seamlessly be able to access the targeted systems through secondary PAM (HA) at DC.		
c. The users at DR should access the targeted systems through PAM at DC but the subsequent sessions should be maintained by DR site.		

d. In case PAM solution at DC fails, the users at DR should be seamlessly able to access the targeted devices through secondary PAM at DC and the subsequent sessions should be maintained by DR site.		
e. In case both PAM at DC fails then all users should be seamlessly able to access the targeted systems through PAM at DR.		
Solution must have capability to support MFA integration with other third-party solutions		
Mandatory Specifications		
Solution must be from a latest leading quadrant Gartner report for PAM systems		
The solution should be a single appliance which caters for password, session management and reporting on one appliance		
Separate database license should not be required for PAM. It must be application driven database and doesn't need any human intervention to manage it. In case separate Database is needed then its price must be included in product cost.		
Solution must have some Upload Utility to onboard privilege accounts in bulk		
Solution have feature to highlight risky session recordings or tag with high score so that auditor can identify those recordings and analyze it quickly		
The solution must have the capability to record system information for managed systems including but not limited to IP address, MAC address, and DNS name, owner of the system, platform type and version.		
OEM must have 24/7 Worldwide HelpDesk and Support Center		

Remote Access Management

The solution must support current Microsoft Operating systems		
The solution must support current Apple OS X Operating systems		
The solution must support common Linux distributions		
The solution should support connection to ChromeOS systems		
The solution should support connection to iOS devices		
The solution should support connection to Android devices		
The solution should support connection to Virtual desktops environments like Citrix, VMWare and Nutanix		
The solution should support connectivity to network devices		
The solution should support connectivity to ATMs, Kiosks, POS Systems, Android, Raspberry Pi, etc		
The solution must be able to connect to virtual machines		
The solution may be deployed on-premises, with high availability model, business continuity and disaster recovery paths. Flexibility for virtualization or cloud deployments must exist as additional options.		
The solution must avoid the use of legacy communication protocols required for access, giving preference to a fully encrypted protocol		
The solution should not require any changes to the network or firewall configurations		

The solution should be routinely tested for vulnerabilities by a thirdparty organisation		
The solution shall support a role based access control methodology		
The solution shall support multi-factor authentication		

The solution should support smart card authentication to endpoints		
The solution should support physical authentication, such as TouchID		
The solution must allow users to terminate support sessions at any time		
The solution must be able to blank the remote system display during a support session		
The solution must allow users to choose which applications are shared with a support representative		
The solution must allow for administrative credentials to be securely entered without revealing the credentials to the support representative		
The solution shall provide distributed discovery engine capability that allows asset to be discovered across different isolated network segments and geographical regions and report discovery result back centrally.		
The solution must have a built-in vault to store credentials		

The solution should have the capability to Associate Credentials to Endpoint		
The solution should have the capability of Local User Account Automatic Rotation		
The solution vault should have the ability of Configurable Password Length		
The Vault should have the ability to store personal passwords		
The solution must keep a complete, tamper-proof recording of all desktop and command shell activity		
The solution must keep a complete log of all session activity		

The solution must retain a log of all chat messages sent and received		
The solution must have the ability to integrate with common ITSM platforms		
The solution should have pre-built integrations with common CRM platforms		
The solution should have pre-built integrations with Microsoft Teams		

The solution must be able to integrate into business applications		
The solution must offer the ability to re-brand or customize the appearance of the user interface		
The solution must be able to connect to systems where there is no preinstalled agent		
The solution must allow technicians to provide support without installation of any software components		
The solution must allow administrators to define standardised messages that representatives can use during a session		
The solution must allow users to initiate a chat session without installing or executing an agent		
The solution must allow representatives to view the end user's web browser activity		
The solution must offer the ability to initiate a support session from a shortcut on the end user's system		

The solution should be able to integrate with SMS messaging to initiate a support session		
The solution must be able to connect to systems that are not directly connected to the internet		

The solution must allow a representative to connect to multiple systems concurrently		
The solution must support a multiple monitor environment		
The solution must allow end users and representatives to transfer files to/from the remote system		
The solution must be able to connect to systems when there is no end user present		
The solution must allow representatives to access systems on different networks without requiring administrative privileges		
The solution should support connection to Intel vPro endpoints		
The solution must support Wake-on-Lan (WOL)		
The solution must allow representatives to connect to endpoints using native protocols, such as RDP, VNC, Telnet and SSH		
The solution should offer representatives the ability to see system information without displaying information on the end-users screen		
The solution should offer representatives the ability to perform system tasks outside of screensharing		

The solution must allow access to command line of an endpoint		
The solution must allow common scripts to be centrally stored for representatives to use in a support session		
The solution must allow for escalation of privileges in a support session		
The solution must allow support representatives to restart a system in session and automatically reconnect when the system is back online		
The solution must allow representatives to instant message each other		
The solution must allow support sessions to be transferred to other support representatives in real time		
The solution should allow representatives to invite other support representatives into an active support session		
The solution must allow representatives to request assistance based on problem/issue type		
The solution should be able to show their screen to and end user in a support session		
The solution should allow representatives to broadcast their screen to multiple participants		

The solution should allow support representatives to use the camera of a mobile device to capture details for a support session		
The solution must support multiple languages		

The solution must log support session activity in a central location		

The solution should offer the ability to capture metrics about support sessions		
The solution should offer administrators the ability to view and manage active support sessions		
The solution should offer the ability to group support representatives to enable features and apply permissions centrally		
The solution must support multiple inbound channels for support sessions		
The solution must offer automatic routing to different inbound channels for support sessions		
The solution must offer the ability to request support from a mobile device		

The solution must be able to broker access for external third-parties to provide support to end users		
The solution must allow technicians to share active sessions with other technicians		
The solution must create a tamper-proof audit trail		
The solution must allow technicians to invite another support representative into a support session on an ad-hoc basis		
The solution must support high-availability		
Does the solution provider offer certified training options for technicians and administrators?		
Does the solution provider aid in the customization of the solution and integration with other support tools?		
Does the solution provider aid in installing and configuring the solution?		
Does the solution provider help the support team follow IT best practices?		

c.   **IDENTITY MANAGEMENT SYSTEM DELIVERABLES**

ITEM	REQUIREMENTS	Response	COMMENT **Indicate how the proposed solution meets the requirement**
1.	Supply cloud-based identity and access management solution with all required software licenses. The proposed solution must have the following capabilities:		
	• Managing identity and access for both on premises and cloud-based business systems.		
	• Provide third-party access management which includes vendors and business partners.		
	• Provide SMS and email based Multi-Factor Authentication (MFA) to help confirm employees' legitimacy before granting access.		
	• Provide secure identity lifecycle management for onboarding and deprovisioning processes.		
	• Provide Single Sign-On (SSO) which allows employees to log into business systems using a single or federated identity.		

ITEM	REQUIREMENTS	Response	COMMENT **Indicate how the proposed solution meets the requirement**

	• Provide risk-based adaptive authentication using factors such as user location, internet protocol (IP) address, time of previous logon, device footprint and more		
	• Enable automated access certification for review of employee and third-party access rights.		
	• Support custom scripts that facilitate identity provisioning for in-house developed applications		
	• Provide self-service access requests through workflow approval rules.		
	• Provide machine learning based user behaviour analytics to mitigate threats such as malicious logins, lateral movement, malware attack, and privilege abuse		
	• Support high availability in case of system and application failures.		
	• Detect and prevent access conflicts of interest and potential risk of fraud.		

	• Must have integration capabilities using industry standard protocols (e.g., SOAP / REST and\or more.)		
	Multi-Factor Authentication • (MFA) on business systems		

ITEM	REQUIREMENTS	Response	COMMENT **Indicate how the proposed solution meets the requirement**
3.	• Single Sign-on		
4.	User Account Lifecycle Management for Employees - through internal HR process and contactors\vendors account management process.		
	• User onboarding/account activation - workflow approval, account provisioning, verification and activation.		
	• Account maintenance and support – privilege\role change, profile update		
	• User offboarding/account termination – disable\delete account.		

5.	Access Management		
	• Automate access request		
	• Authenticate requesting identity.		
	• Authorization of access.		
	• Automate workflow.		
6.	Access attestation		
	• Automate business system owners account review or access review process - to prevent users from accumulating unnecessary privileges and decrease the risk associated with having access to more than what they need to know.		

d. Security Information and Event Monitoring (SIEM) Deliverables

The bidder shall provide an Integrated AI Powered SIEM tool for aggregating and analysing critical events through the collection of security data from network components and the use of correlation rules.

Bidder must submit a proposal detailing the functionality and features of the service with clarity on how the proposed service meets the requirements. The SIEM tool must have the following capabilities:

Key Features/Functionality	YES	NO	Comment
Event Log Analyzer Log Source Configuration			
Enable windows device logging, troubleshoot configuration issues, and provide system requirements for log source			

Enable syslog device (UNIX servers, Firewalls, Routers and layer 3 network devices) logging, troubleshoot configuration issues and provide system requirements for log source			
Enable other device (Print Service) logging, troubleshoot configuration issues and provide system requirements for log source			
Enable SQL server logging, troubleshoot configuration issues and provide system requirements for log source			
Enable IIS server logging, troubleshoot configuration issues and provide system requirements for log source			
Enable windows file integrity monitoring, troubleshoot configuration issues, and provide system requirements for log source			
Enable threat source (Symantec), troubleshoot configuration issues and provide system requirements for log source			
Enable threat data logging (Qualys), troubleshoot configuration issues and provide system requirements for log source			
Enable vCentre logging, troubleshoot configuration issues and provide system requirements for log source			
Enable log forwarder, troubleshoot configuration issues, and provide system requirements for log sources			
Event Log Reporting Configuration			

Enable reporting for all Windows events			
Enable reporting for windows Trend Events			

Enable reporting for windows server threat detection (Dos Attack)			
Enable reporting for windows System events			
Enable reporting for windows Start-up events			
Enable reporting for windows scheduled Monthly Security Audit Logs Review			
Enable reporting for all windows workstation events			
Enable reporting for windows workstation device severity reports			
Enable reporting for windows workstation Logon Reports			
Enable reporting for windows workstation Logoff reports			
Enable reporting for windows workstation windows start-up events			
Enable reporting for windows workstation system events			
Enable reporting for windows workstation windows firewall auditing			
Enable reporting for windows workstation Scheduled tasks			
Enable reporting for windows workstation process tracking			
Enable reporting for windows workstation scheduled Monthly Security Audit Logs Review			
Enable reporting for Linux Server trend reports			
Enable reporting for Linux Server Logon Reports			
Enable reporting for Linux Server Logoff Reports			
Enable reporting for Linux Server Failed Logon Reports			

Enable reporting for Linux User Account Management			
Enable reporting for Linux Server SUDO Commands			
Enable reporting for Linux Server Mail Server Reports			
Enable reporting for Linux Server Threat Reports			
Enable reporting for Linux Server scheduled Monthly Security Audit Logs Review			
Enable reporting for all NGFW Events			
Enable reporting for NGFW flow allowed traffic			
Enable reporting for NGFW denied traffic			
Enable reporting for NGFW and layer 3 network devices Logon Reports			
Enable reporting for NGFW allowed traffic			
Enable reporting for NGFW website Traffic			
Enable reporting for NGFW IDS/IPS Reports			

Event Log Alert Configuration			
Enable daily alerts for System/Server Threats			
Enable daily alerts for Web Server Threats			
Enable daily alerts for Database Treats			
Enable daily alerts for Ransomware Attacks			

Enable weekly alerts for File Integrity Threats			
Enable weekly alerts for Potential Windows Threats			
Enable weekly alerts for potential Unix/Linux Threats			
Enable weekly alerts for Cryptocurrency			
Event Log Correlation			
Capability to correlate User Account Threats for all log sources			
Capability to correlate System/Server Threats			
Capability to correlate Web Server Threats			
Capability to correlate Database Treats			
Capability to correlate Ransomware Attacks			
Capability to correlate File Integrity Threats			
Capability to correlate Potential Windows Threats			
Capability to correlate potential Unix/Linux Threats			
Capability to correlate Cryptocurrency			
Capability to perform active monitoring on Windows Sessions			

Capability to perform active monitoring on Unix/ Linux Sessions			
Capability to perform active monitoring on VPN Sessions			
Event Log Compliance			

Enable compliance reporting for FISMA			
Enable compliance reporting for PCI-DSS			
Enable compliance reporting for SOX			

Enable compliance reporting for HIPAA			
Enable compliance reporting for GLBA			
Enable compliance reporting for ISO 27001:2022			
Enable compliance reporting for GPG			
Enable compliance reporting for GDPR			
Enable compliance reporting for NRC			
Enable compliance reporting for Cyber Essentials			
Enable compliance reporting for COCO			
Enable compliance reporting for NERC			
Enable compliance reporting for FERPA			
System Administration			
Administrator Access			
Administrator access will need to be restricted according to specified profiles and user roles.			
Security			

Positive administrator Identification: Ensuring that each administrator has his/her own individual user id that is used on audit trails.			
Full password security			

e. SECURITY OPERATIONS CENTER (SOC) DELIVERABLES

The bidder shall provide the following SOC SERVICES to monitor the following activities:

a. Provides 24 x 7 x 365 alert monitoring and prioritization, investigation and threat hunting services;

b. Applying artificial intelligence models to customer endpoint data, network data and server information, the service will be able to correlate and prioritize advanced threats;

c. Monitor Network, Hybrid Server Security and Endpoints (For Network, Server and Endpoint threat events) 24x7x365 using proprietary methods to actively hunt for signs of compromise;

d. Advanced AI-powered correlation of endpoint, network and server events, alerts and logs; e. Impact analysis and incident prioritization;

f. Threat response and executive summary report frequency;

g. Provide root cause analysis, mitigation recommendations, and toolkits to assist on how to handle incidents;

h. Provide a wide array of security services, including alert monitoring, alert prioritization, investigation, and threat hunting;

i. The bidder shall perform Indicators of Compromise (IOC) sweeping for the newly identified IOC's;

j. The bidder must provide the below MANDATORY technical resources who will be involved in this assignment.

I. Certified CISSP Specialist x1   II. Certified Ethical Hacker x1

III. Certified CISM Specialist x1

IV. Project Manager (PMP/Prince 2) x1

SECURITY OPERATIONS CENTER (SOC) DELIVERABLES

1	Capable of producing reports that monitor activities of IT administrators and domain users reporting on their activities within servers hosting services such as Active directory, SQL databases, Oracle databases, Windows logon events, Linux OS logon events.				
COMPLY	YES			NO	

	Comment:

2	Be able to produce daily reports of all activities within the network for a 24-hour period covering aspects such as:
	Malware & Anti-virus activities.
	Suspicious traffic to malicious sites, backdoor or Torrent ports
	Perimeter Security scans and exploits.
	AD security correlated events- Failed and Lockout accounts including service accounts, multiple host logging from single AD account, Brute force attempts from a single source.
	Correlated internal reconnaissance events, horizontal scans.

COMPLY	YES			NO	

Comment:

3	Be able to produce weekly reports of all activities within core servers: Weekly Active
	Directory activities report.
	Weekly Linux server login report. Weekly
	Windows server logon activities.
	Weekly SQL and Oracle databases activity reports.

COMPLY		YES			NO	

Comment:		

4	Be able to produce alerts for the following incidents: Active Directory group policy violation change. Firewall rules changes. Suspicious traffic to malicious sites. Alerts from the Trend Micro ePO on antivirus events.

COMPLY	YES			NO	

Comment:

5	Be able to produce Monthly security overview report showing aspect such as: Monthly Risk rating and three-month trend security posture. Malware overview report based on Trend Micro endpoint protection. Top account login failures. Top account lockouts. TOR/Backdoor traffic overview Perimeter security overview Overview of incident reported during the month and SLA monthly report

COMPLY	YES			NO	

Comment:

The following buildings are in scope

Johannesburg Head Office:

- 15 Sherborne Street, Parktown
- 20 Eton Street, Parktown **Provincial Offices:**
    a. Port Elizabeth Provincial Office
    b. East London Provincial Office
    c. Western Cape Provincial Office
    d. Durban Provincial Office
    e. Northern Cape Provincial Office
    f. Free State Provincial Office
    g. Mpumalanga Provincial Office
    h. Northwest Provincial Office
    i. Limpopo Provincial Office

Province	City	Physical Address	Number of Access Points
1. Gauteng	Johannesburg	20 Eton Rd, 15 Sherborne Rd	8 26
2. Western Cape	Cape Town	4 Prestwich Street Cape Town 8000	3
3. Eastern Cape	Gqeberha	75 Havelock Street, Gqeberha	3
4. Eastern Cape	East London	3 Elton Street Southernwood East London	3
5. Mpumalanga	Nelspruit	Citrus No.3 Crescent Street	3
6. Northern Cape	Kimberley	38 A Sydney Street, Kimberly	3
7. Free State	Bloemfontein	152 Nelson Mandela Drive Prondeza Building Westdene, Bloemfontein	3

		73 Ramsay Avenue Musgrave, Durban	3
8. KwaZulu Natal	Durban		
9. Limpopo	Polokwane	16 Market Street, Capricorn TVET College Central Office, Old Building, 0699	3
10. Northwest	Klerksdorp	74 Boom Street, Klerksdorp Central	3

Mandatory Documentation Requirements

ICT Project Governance Documentation, Manuals, Handovers and User Training

Sign off documentation: The following documentation will require to be formulated, reviewed and signed off by all designated parties:

- Project Charter
- Project Plan
- Business Requirements Document
- Document the As-IS, Formulate and Document the To Be for the finalized ICT Enterprise Architecture
- Technical Solution Design Document
- Testing Documents
- User Acceptance Testing Document
- Training and User Manual Documentation
- Develop and Document User manuals and Standard Operating Procedures
- Change Management Campaign Documentation
- Deliver some hands-on orientation and training to appropriate Services SETA ICT staff on how to use the applications look after and support the system for the adequate internal provision of at least the second level support and reports.
- Ensure optimal utilization of all licensed products and features
- Ensure that Services SETA unlocks value benefit realization and a return on investment on the EA.
- The service provider must have a 24/7 functional Support and Maintenance Helpdesk.
- Perform advisory role for the EA usage during the contractual tenure ship.
- Local and remote resources for software and hardware deployment support and maintenance services must be critically available during project execution and support phases.

*Important Notice
- Qualifying bidders may be invited to make a presentation of the methodology and approach as part of the selection process.
- Upon appointment, a successfully appointed service provider will be subjected to an ongoing performance management process (based on agreed SLA's) where **penalties** will be administered in the event of non-performance.

SECTION 3 – Professional Services, Support and Maintenance SLA Rate Cards for On Premise and Cloud Based Services

3.1 Technical Systems Support High Level Requirements

- Problem Resolutions
- Support Account Management
- Services Support Assistance
- Modern Service Management
- Monthly SLA Reporting

3.2 Level of Support Requirement Timelines.

24/7 Functional Help Desk Support and Maintenance Personnel with a ticket referencing portal is a prerequisite.

The following Mean Time to Response schedules should be adhered to as enforced by RTOs and RPO of the Business Continuity Plan and the Disaster Recovery Plan

- 2 hours response time to remote or onsite support for mission critical systems
- 4 hours to next business day for remote or on-site support for non-critical mission systems.
    - o Fault Handling: Mean Time to Repair: Average time required to repair a failed component is same business day.
- Service Level Requirement.
    - o Working Days: 5 Days a week [Monday to Friday] o Normal Business Hours: 08:00 hours to 1700 hours. o After Business Hours: 17:00 hours to 07:00 hours o Support on holidays and weekends as and when requested is a must. o Weekends Saturday and Sunday o Month: Calendar Month
- Service Delivery.
    - o Customer Centric Support Services and agreed SLA's. o Adherence to Batho Pele Principle.
    - o Monthly Service Level Agreement Reporting

Bidders might be invited to make a presentation as part of the selection process.

Whilst other tasks may be defined to meet the timeline requirements of the required support services, it is believed that the following shall be the major components of the assignment however not limited to:

Project Resources Requirement	
	Cards

SLA	Rate		
		Key Account Manager	
		Project Manager	
		Technical Manager	
		Technical Team Members	
		HelpDesk Manager	

APPOINTMENT OF A SERVICE PROVIDER TO SUPPLY AND IMPLEMENT A SYSTEM INCIDENT EVENT MANAGEMENT SYSTEM (SIEM), USER LIFECYCLE, REMOTE ACCESS, NETWORK ACCESS CONTROL, PRIVILEDGED AND IDENTITY MANAGEMENT SYSTEMS AND A SECURITY OPERATIONS CENTER (SOC) SERVICES NCLUSIVE OF A 3 YEAR SUPPORT AND MAINTENANCE PLAN	Services Required	Response Time	Junior and Senior Resource Pricing: Decremental Pricing (where applicable)	RATES	
				Junior	Senior
	High Level L2, L3 Consultative Professional Services Hardware and Software Deployments Configuration, Customisation, Support, and Maintenance.	8AM-5PM, 5PM-8AM Mon-Fri Sat-Sun & Public Holidays	**Min:** 1-4 hrs@ R/hr		
			Med: 5-10hrs @ R/Hr		
			Max 10-20 Hrs: @ R/Hr		

DESTINATION Nationwide Services SETA Offices Only	CALL OUT FEES			TRAVEL Provincial Offices Only Rate / kilometer	ACCOMODATION / Person Maximum 3 Persons
	Business Hours / Hour	After Hours excl. Sunday & Public Holidays / Hour	Sundays & Public Holidays / Hour		

Network Access Control (NAC) Live Demonstration Evaluation

Introduction

This section outlines the Terms of Reference (ToR) for the live demonstrations of the Network Access Control (NAC) solution by qualifying bidders. The objective of this exercise is to evaluate the technical capabilities, functionality, and performance of the proposed solutions to ensure they align with the organization's security requirements.

Purpose of the Live Demonstration The

live demonstration aims to:

- Validate the proposed NAC solution's compliance with the functional requirements.
- Assess the ease of deployment, integration, and management of the solution within the existing infrastructure.
- Evaluate the solution's ability to enhance network security, visibility, and access control.
- Facilitate an informed decision-making process based on real-time demonstration results.

Scope of the Demonstration

The demonstration must cover the following areas:

- Deployment and integration capabilities.
- Device visibility and profiling.
- Network access control policies.
- Incident detection and response capabilities.
- Reporting and compliance features.
- Usability and administrative functionalities.

Functional Requirements

The following functional requirements must be demonstrated live by the bidders:

Deployment and Integration

Demonstrate the installation and configuration process in both agent-based and agentless modes.

- Show integration with existing network infrastructure components such as switches, firewalls, VPNs, and SIEM systems.
- Illustrate compatibility with multiple operating systems (Windows, macOS, Linux, and mobile OS).
- Prove the ability to integrate with Active Directory (AD) and other identity management systems for authentication and policy enforcement.

Device Visibility and Profiling

- Demonstrate real-time detection and identification of devices (managed, unmanaged, IoT).
- Show device classification capabilities based on type, OS, and security posture.
- Illustrate the ability to create and manage dynamic device groups.

Network Access Control Policies

- Demonstrate creation and enforcement of access policies based on user roles, device type, security posture, and compliance status.
- Show quarantine capabilities for non-compliant devices and automated remediation workflows.
- Illustrate guest access management including self-registration portals and access expiry policies.
- Demonstrate integration with firewalls and other security systems to enforce network segmentation.

Incident Detection and Response

- Demonstrate detection of abnormal behaviour or security incidents in real-time. • Show automated response actions such as isolating devices or limiting access.
- Illustrate integration with SIEM systems for alerting and incident management.

Reporting and Compliance

- Demonstrate the generation of compliance and audit reports.
- Show predefined and customizable reporting templates.
- Illustrate logging and tracking of access requests and policy violations.

Usability and Administration

- Demonstrate the user interface, including ease of navigation and management.
- Show role-based access controls for administrative functions.
- Illustrate dashboard capabilities for monitoring network health and security status.

Technical Requirements

- Bidders must provide access to a demo environment with relevant use cases.
- The demonstration must be conducted live, either onsite or via a secure remote session.
- All supporting documentation and user manuals must be provided before the demonstration.

PAM Solution Functional Requirements Live Demonstration Evaluation

Introduction

This section outlines the Terms of Reference (ToR) for live demonstrations of the Privileged Access Management (PAM) solution by qualifying bidders. The objective of this exercise is to assess the proposed solution's compliance with security requirements, functional capabilities, and its ability to manage and secure privileged accounts effectively.

Purpose of the Live Demonstration The live

demonstration aims to:

- Validate the compliance of the PAM solution with the defined functional requirements.
- Assess its ability to secure, manage, and monitor privileged accounts across the organization.
- Evaluate deployment, integration, and management capabilities within the existing infrastructure.
- Enable informed decision-making based on real-time demonstration outcomes.

Scope of the Demonstration

The demonstration must cover the following areas:

- Deployment and integration capabilities.
  - Privileged account management.
  - Session management and monitoring.
  - Threat detection and response.
  - Reporting and compliance features.
  - Usability and administrative functionalities.

Functional Requirements

The following functional requirements must be demonstrated live by the bidders:

Deployment and Integration

- Demonstrate the installation and configuration of the PAM solution, including both on-premises and cloud deployment options.
- Show seamless integration with existing IT infrastructure such as Active Directory, LDAP, SIEM, and ticketing systems (e.g., ServiceNow).
- Illustrate compatibility with various platforms including Windows, Linux, Unix, and databases.
- Prove the ability to integrate with multi-factor authentication (MFA) solutions for secure access.

Privileged Account Management

- Demonstrate automated discovery of privileged accounts across networks, devices, and applications.
- Show secure storage, rotation, and management of privileged credentials.
- Illustrate the ability to set password complexity, expiry, and rotation policies.

- Demonstrate the approval workflows for access requests, including just-in-time (JIT) access.
- Show how privileged credentials can be checked out with automatic check-in and credential rotation.

Session Management and Monitoring

- Demonstrate live monitoring of privileged sessions with options to pause, terminate, or take over sessions if necessary.
- Show session recording capabilities including video playback and keystroke logging for auditing purposes.
- Illustrate real-time alerting on suspicious activities during sessions.
- Demonstrate secure remote access for vendors and third parties without VPN.

Threat Detection and Response

- Demonstrate risk-based analytics to detect anomalous behavior associated with privileged accounts.
- Show automated responses such as isolating or disabling accounts in case of suspicious activities.
- Illustrate integration with SIEM systems for real-time threat detection and alerting.

Reporting and Compliance

- Demonstrate the ability to generate compliance reports for standards such as PCI DSS, HIPAA, ISO 27001, and GDPR.
- Show customizable reporting templates for audit trails, access reports, and incident summaries.
- Illustrate audit log retention policies and secure log storage capabilities.

Usability and Administration

- Demonstrate the user interface for administrators, including ease of navigation and access management. Show role-based access controls (RBAC) for managing privileges based on job roles.
- Illustrate centralized policy management for privileges, access, and session monitoring.
- Demonstrate the dashboard's capabilities for monitoring PAM activities and risk scores

Technical Requirements

- Bidders must provide access to a demo environment replicating realistic scenarios.
- The demonstration must be conducted live, either onsite or through a secure remote session.
- All supporting documentation, including user manuals and architecture diagrams, must be provided in advance.

IAM Solution Functional Requirements Live Demonstration Evaluation

Introduction

This section outlines the Terms of Reference (ToR) for live demonstrations of the Identity and Access Management (IAM) solution by qualifying bidders. The purpose of this exercise is to assess the proposed solution's compliance with security requirements, functional capabilities, and its ability to manage and secure identities effectively.

Purpose of the Live Demonstration The live demonstration aims to:

- Validate the compliance of the IAM solution with the defined functional requirements.
- Assess the ability to secure, manage, and monitor identities across the organization.
- Evaluate deployment, integration, and management capabilities within the existing infrastructure.
- Facilitate informed decision-making based on real-time demonstration outcomes.

Scope of the Demonstration

The demonstration must cover the following areas:

- Deployment and integration capabilities.
- Identity and lifecycle management.
- Access management and single sign-on (SSO).
- Multi-factor authentication (MFA).
- Threat detection and response.
- Reporting and compliance features.
- Usability and administrative functionalities.

Functional Requirements

The following functional requirements must be demonstrated live by the bidders:

Deployment and Integration

- Demonstrate the installation and configuration of the IAM solution for both cloud-based and hybrid environments.
  Show seamless integration with existing IT infrastructure such as Active Directory, LDAP, HR systems, and other identity providers.
- Illustrate compatibility with a variety of platforms including Windows, macOS, Linux, and mobile OS.
- Demonstrate API-based integration for custom applications and third-party systems.
- Prove the ability to integrate with SIEM solutions for real-time monitoring and alerting.

Identity and Lifecycle Management

- Demonstrate automated user provisioning and de-provisioning based on role changes and HR triggers.
- Show capabilities for self-service user registration, profile updates, and password management.
- Illustrate support for role-based access control (RBAC) and attribute-based access control (ABAC).
- Demonstrate the ability to enforce least privilege and zero trust principles.
- Show the ability to handle multiple identity types (employees, contractors, partners, customers).

Access Management and Single Sign-On (SSO)

- Demonstrate SSO capabilities across on-premises, cloud, and hybrid applications using SAML, OIDC, and OAuth 2.0 protocols.
- Show support for adaptive access policies based on device type, network, and user behaviour.
- Demonstrate conditional access controls to restrict access based on risk levels.
- Illustrate integration with VPN solutions for secure remote access.

Multi-Factor Authentication (MFA)

- Demonstrate the implementation of MFA for both internal and external users.
- Show support for various MFA methods such as SMS, TOTP, biometrics, and push notifications.
- Illustrate adaptive MFA capabilities based on user location, device, and access context.
- Demonstrate MFA enforcement for high-risk actions or sensitive applications. **Threat Detection and Response**

- Demonstrate real-time monitoring and alerting for suspicious login activities and brute-force attacks.
- Show risk-based authentication mechanisms to prevent unauthorized access.
- Illustrate integration with SIEM systems for centralized threat detection and response.
- Demonstrate automated response actions such as account lockout and step-up authentication.

Reporting and Compliance

- Demonstrate the ability to generate compliance reports for standards such as PCI DSS, HIPAA, ISO 27001, and GDPR.
- Show customizable reporting templates for audit trails, access logs, and incident summaries.
- Illustrate capabilities for identity governance, including access reviews and certification.

Usability and Administration

- Demonstrate the administrative interface, including ease of navigation and management of identities.
- Show role-based access controls (RBAC) for managing administrative privileges.
- Illustrate centralized policy management for access control, MFA, and identity lifecycle.
- Demonstrate dashboards for monitoring IAM activities and risk scores.

Technical Requirements

- Bidders must provide access to a demo environment replicating realistic scenarios.
- The demonstration must be conducted live, either onsite or through a secure remote session.
- All supporting documentation, including user manuals and architecture diagrams, must be provided in advance.

SIEM Solution Functional Requirements Live Demonstration Evaluation

Introduction

This section outlines the Terms of Reference (ToR) for live demonstrations of the Security Information and Event Management (SIEM) solution by qualifying bidders. The objective of this exercise is to assess the proposed solution's compliance with security requirements, functional capabilities, and its ability to detect, respond to, and manage security incidents effectively. **Purpose of the Live Demonstration** The live demonstration aims to:

- Validate the compliance of the SIEM solution with the defined functional requirements.
- Assess the ability to monitor, detect, and respond to security threats in real-time.
- Evaluate deployment, integration, and management capabilities within the existing infrastructure.
- Facilitate informed decision-making based on real-time demonstration outcomes.

Scope of the Demonstration

The demonstration must cover the following areas:

- Deployment and integration capabilities.
- Log management and data collection.
- Threat detection and incident response.
- Threat intelligence and analytics.
- Reporting and compliance features.
- Usability and administrative functionalities.

Functional Requirements

The following functional requirements must be demonstrated live by the bidders:

Deployment and Integration

- Demonstrate the installation and configuration of the SIEM solution for both on-premises and cloud environments.
- Show seamless integration with existing IT infrastructure such as firewalls, endpoints, Active Directory, IDS/IPS, and cloud services.
- Illustrate compatibility with a variety of log sources and protocols (Syslog, SNMP, Windows Event Logs, etc.).
- Demonstrate API-based integration for custom applications and third-party systems.
- Prove the ability to integrate with ticketing systems (e.g., ServiceNow) for incident management.

Log Management and Data Collection

- Demonstrate automated log collection from diverse sources such as servers, endpoints, network devices, and cloud services.
- Show capabilities for log normalization, parsing, and categorization.
- Illustrate secure log storage with encryption and log retention policies.
- Demonstrate real-time indexing and search capabilities for logs.

Threat Detection and Incident Response

- Demonstrate real-time monitoring and detection of security events, including suspicious logins, malware activity, and lateral movement.
- Show the use of behavioural analytics to detect insider threats and advanced persistent threats (APTs).
- Illustrate automated incident response playbooks for common threats.
- Demonstrate capabilities for threat hunting using custom queries and indicators of compromise (IoCs).
- Show integration with Security Orchestration, Automation, and Response (SOAR) tools for automated responses.

Threat Intelligence and Analytics

- Demonstrate the integration of threat intelligence feeds for enhanced detection accuracy.
- Show risk-based alert prioritization to reduce alert fatigue.
- Illustrate machine learning capabilities for detecting unknown threats and anomaly detection.
- Demonstrate the ability to correlate events across multiple sources to identify complex attack patterns.

Reporting and Compliance

- Demonstrate the ability to generate compliance reports for standards such as PCI DSS, HIPAA, ISO 27001, NIST, and GDPR.
- Show customizable reporting templates for audit trails, access logs, and incident summaries.
- Illustrate capabilities for forensic analysis and investigation with historical data.
- Demonstrate audit log retention policies and secure log storage capabilities.

Usability and Administration

- Demonstrate the administrative interface, including ease of navigation and management of alerts and incidents.
- Show role-based access controls (RBAC) for managing administrative privileges.
- Illustrate centralized policy management for detection rules, alerts, and automated responses.
- Demonstrate dashboards for monitoring security posture, key performance indicators (KPIs), and risk scores.
- Show capabilities for multi-tenant management if applicable.

Scalability and Performance

- Demonstrate the ability to scale log ingestion and processing based on increased log volumes.
- Show performance benchmarks for real-time analysis and alerting with high log throughput.
- Illustrate the ability to scale horizontally or vertically without significant downtime.

Technical Requirements

- Bidders must provide access to a demo environment replicating realistic scenarios.
- The demonstration must be conducted live, either onsite or through a secure remote session.
- All supporting documentation, including user manuals and architecture diagrams, must be provided in advance.

AI-based SOC Solution Functional Requirements Live Demonstration Evaluation

Introduction

This section outlines the Terms of Reference (ToR) for live demonstrations of AI-based Security Operations Center (SOC) solutions by qualifying bidders. The objective of this exercise is to assess the proposed solution's compliance with security requirements, functional capabilities, and its ability to enhance threat detection, response, and management using artificial intelligence and machine learning. **Purpose of the Live Demonstration** The live demonstration aims to:

- Validate the compliance of the AI-based SOC solution with the defined functional requirements.
- Assess the ability to detect, respond to, and manage security incidents effectively using AI and machine learning.
- Evaluate deployment, integration, and management capabilities within the existing infrastructure.
- Enable informed decision-making based on real-time demonstration outcomes.

Scope of the Demonstration

The demonstration must cover the following areas:

- Deployment and integration capabilities.
- AI-based threat detection and analysis.
- Incident response and automation.
- Threat intelligence and predictive analytics.
- Reporting and compliance features.
- Usability and administrative functionalities.

Functional Requirements

The following functional requirements must be demonstrated live by the bidders:

Deployment and Integration

- Demonstrate the installation and configuration of the AI-based SOC solution for both on-premises and cloud environments.
- Show seamless integration with existing security tools (SIEM, EDR, firewalls, IDS/IPS) and IT infrastructure.
- Illustrate compatibility with various log sources and protocols (Syslog, SNMP, Windows Event Logs, etc.).
- Demonstrate API-based integration for custom applications and third-party systems.

- Prove the ability to integrate with IT service management (ITSM) and ticketing systems (e.g., ServiceNow).

AI-based Threat Detection and Analysis

- Demonstrate AI-driven real-time threat detection using anomaly detection, behaviour analytics, and pattern recognition.
- Show capabilities for detecting zero-day threats, insider threats, and advanced persistent threats (APTs).
- Illustrate the use of supervised and unsupervised machine learning models for threat analysis.
- Demonstrate natural language processing (NLP) capabilities for analysing security logs and threat intelligence feeds.
- Show automated risk scoring and alert prioritization to reduce false positives.

Incident Response and Automation

- Demonstrate AI-driven playbooks for automated incident response including containment, eradication, and recovery.
- Show capabilities for automated threat hunting using AI-generated hypotheses.
- Illustrate integration with Security Orchestration, Automation, and Response (SOAR) platforms for coordinated responses.
- Demonstrate capabilities for automated investigation, including root cause analysis and lateral movement tracking.
- Show automated threat mitigation actions such as isolating devices, disabling accounts, and blocking IPs.

Threat Intelligence and Predictive Analytics

- Demonstrate integration with threat intelligence platforms (TIPs) for real-time threat indicators.
- Show predictive analytics capabilities for forecasting potential threats based on historical data and AI models.
- Illustrate the ability to detect and prioritize threats based on threat actor profiles and tactics, techniques, and procedures (TTPs).
- Demonstrate integration with dark web monitoring and external intelligence feeds.

Reporting and Compliance

- Demonstrate the ability to generate compliance reports for standards such as PCI DSS, HIPAA, ISO 27001, NIST, and GDPR.
- Show customizable reporting templates for audit trails, access logs, and incident summaries.
- Illustrate capabilities for forensic analysis and investigation with historical data.
- Demonstrate audit log retention policies and secure log storage capabilities.

Usability and Administration

- Demonstrate the user interface for SOC analysts, including dashboards, alert management, and investigation workflows.
- Show role-based access controls (RBAC) for managing administrative privileges.
- Illustrate centralized policy management for detection rules, alerts, and automated responses.
- Demonstrate capabilities for multi-tenant management if applicable.
- Show dashboard capabilities for monitoring security posture, key performance indicators (KPIs), and risk scores.

Scalability and Performance

- Demonstrate the ability to scale log ingestion and processing based on increased log volumes.
- Show performance benchmarks for real-time analysis and alerting with high log throughput.
- Illustrate the ability to scale horizontally or vertically without significant downtime.

Privacy and Data Security

- Demonstrate data encryption at rest and in transit.
- Show capabilities for anonymizing or pseudonymizing sensitive data in logs and alerts.
- Illustrate compliance with ISO27001, POPIA, and other data privacy regulations.

Technical Requirements

- Bidders must provide access to a demo environment replicating realistic scenarios.
- The demonstration must be conducted live, either onsite or through a secure remote session.

  All supporting documentation, including user manuals and architecture diagrams, must be provided in advance

4. THE DURATION OF ASSIGNMENT

It is envisaged that the project will be for a period of three (3) years from the date of appointment.

5. PRECCA CLAUSES IN TERMS OF SECTION 28

COMPLIANCE WITH THE PROVISIONS OF PREVENTION AND COMBATTING OF CORRUPT ACTIVITIES ACT, 12 OF 2004 (PRECCA)

1.1   The Bidder acknowledges and declares that is aware of the Provisions of the aforementioned Act.

1.2   The Bidder declares that its name and/or that of any of its partners, managers, directors or any other person who wholly or partly exercises or may exercise control over the Bidder has never been endorsed as contemplated in Section 28 of PRECCA.

1.3   Should at any time after the conclusion of the Agreement, the Services SETA be made aware of the endorsement of either the Bidder's name and/or that of any of its partners, managers, directors or any other person who wholly or partly exercises or may exercise control over the Bidder, the Services SETA shall be legally entitled to forthwith cancel the agreement and claim any damages the Services SETA may have incurred as a result of contracting of contract with an entity whose name is endorsed in terms of Section 28 of PRECCA.

6. KINDLY FORWARD THE FOLLOWING BID DOCUMENTS, WHERE A CERTIFIED COPY OF A DOCUMENT IS REQUIRED, IT MUST BE CERTIFIED WITHIN THE LAST THREE (3) MONTHS

QUALIFICATION REQUIREMENT

QUALIFICATION/ GATEKEEPER REQUIREMENT (MANDATORY)	Has the applicable document been attached?	
1. The potential bidder must be registered with National Treasury Central Supplier Database (CSD).	Yes ☐	No ☐
2. Bid document must be signed and duly completed, together with all declaration of interest/ standard bidding documents (**SBD's 1, 3.3, 4, 6.1 and 7.2**).	Yes ☐	No ☐
3. Provide and attach a copy of Company Registration Certificate.	Yes ☐	No ☐
4. The potential bidder must provide proof being an OEM partner of the P.A.M, N.A.C, S.E.I.M and I.A.M, additionally the bidder must be certified for • ISO 9001(Quality Management), • ISO 27001 (Information Security Management System Compliance)	Yes ☐	No ☐
The bidder must comply with the aforementioned qualification requirements above. Failure to abide by any of the requirements will lead to automatic disqualification.		
OTHER IMPORTANT BID REQUIREMENT		

	Has the applicable document been attached?	
1.The tenderer must submit proof of its B-BBEE status level of contributor **PLEASE NOTE:** The tenderer failing to submit proof of B-BBEE status level of contributor or is a non-compliant contributor to B-BBEE may not be disqualified, but may only score points out of 80 for price; and scores Zero(0) points out of 20 for specific goals. Services providers are encouraged to comply with B-BBEE requirements for a more competitive advantage under B-BBEE scoring.	Yes ☐	No ☐
2.The potential bidder must be **Tax Compliant** on National Treasury Central Supplier Database (CSD) prior to award	Yes ☐	No ☐
3. The Supplier status must be active, when verifying with Central Supplier Database (CSD). Provide MAAA number …………………………..	Yes ☐	No ☐
4. Tax Status, the potential bidder must indicate pin number………………………..	Yes ☐	No ☐

7. EVALUATION CRITERIA

The value of this bid is estimated to be above R1 000 000 but below R50 000 000 (all applicable taxes included); therefore the **80/20** system shall be applicable.

Criterion 1- Qualification Requirement

Bidders will first be evaluated in terms of the gatekeeper/minimum requirements. Bidders who do not fulfil all the requirements or do not submit the required documents will be disqualified.

Criterion 2-Functionality Evaluation

Functionality is worth 70 points. The minimum threshold is 65 points. <u>Bidders who score less than 65 points on functionality will therefore be disqualified</u>; those who score 65 points or more will be further evaluated on **Criteria 3.**

Criterion 3-Live Demo Evaluation

Live demo is worth 30 points. The minimum threshold is 20 points. Bidders who score less than 20 points will therefore be disqualified; those who score 20 points or more will be further evaluated on Criteria 4.

Criterion 4-Price and Preference Evaluation

Price and Specific goals (B-BBEE status level of contributor), Evaluation will be conducted on a 80/20 preferential procurement principle.

NOTE: For the purpose of comparison and in order to ensure a meaningful evaluation, bidders must submit detailed information in substantiation of compliance to the evaluation criteria mentioned-above.

A	B	C	D	E	F	G	H
FUNCTIONALITY	**REQUIREMENT**	**SCORE QUALIFICATION**	**MEASUREMENT (what must be provided/ demonstrated as minimum)**				
			Indicate what pages/ section in proposal?	Weigh ted Points	Yes	No	Score
Capacity and competencies	Proactive Key Account and Project Management Technical Resources and Help Desk Support Capacity	The service provider must clearly indicate the potential and availability of resources • The service provider must have assigned a Key Account Manager with a master's degree in business administration and a Project Manager who possess at Min, bachelor's degree in information systems technology, or computer science, supported by (Project Management Professional) certification. (include 2 CVs no less than 5 years' experience in management of SIEM and SOC projects) **=0-10pts** • The service provider must present a minimum of 5 Technical Team's CVs showing proven experience in implementation of SIEM and SOC services inclusive of support and maintenance. •	Bid Proposal What page (s) or section where information may find? State **page (s) number** .... or State **section/ tab** .... on your proposal.	**30pts**	☐	☐	

		Cyber Security Analysts Qualifications and Experienced CVs of technical resources with Min bachelor's degree in information systems technology, or Computer Science or Software Engineering and. Industry, Qualifications Microsoft: Azure, M365 Security Administrator and either CISM/CISSP/CompTIA Security+ and CEH min V10 Telecommunications and Networks Security Specialist Resource with Industrial Qualifications and Experienced CVs certified in either CompTIA Security+ /CCNA/HPe ATP Security Networking and Operations Associate. AI Specialist, Experience in AI, Machine Learning, NLP, Integration Developer Expertise in middleware, iPaaS, RESTful APIs, SOAP, and JSON ITSM Help Desk Resource with Industrial Qualifications and Experienced CVs Certified in ITIL Foundation 2/3/4. (include 5 CVs no less than 3years experience) =0-20pts					
Methodology and Project Approach	Advanced Project Initiation & Planning, Stakeholder Alignment, establishment of a project steerco, Define project scope,	Provide a clear methodology, exhibit high level understanding define project objectives, scope, and key deliverables. Identify key stakeholders and assign roles and responsibilities. Propose best fit solution/s and design for a SIEM, NAC, PAM, IAM, and	Bid Proposal What page (s) or section of your proposal bid committee may find clear project plan	**15 pts**			

| | objectives, and deliverables for SIEM, NAC, PAM, IAM, and SOC, and project reporting as per best practise standards | SOC as guided by best practise, to address the problem statements herein this document. **=0-5pts**

The service provider must present in their methodology and approach an in-depth, understanding of IT infrastructures, compliant security postures, (ISO 27001, NIST, POPIA) to achieve functional requirements herein this document. Define system architecture and integration strategy across existing IT and cloud environments.
Security: Data protection, user access controls, encryption. Implementation of security hardening measures. Ensure 24/7 SOC monitoring, escalation processes, and automated responses. Compliance: Audit Tracking, Policy enforcement, regulatory reporting, automated compliance checks. **=0-5pts**

The service provider must present in their methodology and approach an in-depth strategy for AI powered solution deployment & configuration, User Acceptance Testing (UAT) & Quality Assurance Implement User Training & Change Management. **=0-5pts**

The service provider must present in their methodology and approach ability to provide documentation & knowledge transfer, Deployment & Go-Live supported by a maintenance strategy post migration, SLA Management, compliance and performance review, continuous improvements and optimization | State **page (s) number**
....
or
State **section/ tab**
....
on your proposal. | | | | |

Assignment Experience Testimonials	The potential bidder must provide and attach three formal testimonial/ references letters with letterhead and contactable details signed by company representative.	Bidder to submit (3) three or more written testimonials letters from customers whose solutions were deployed not older than two (2) years ago testifying to quality of services, and in relation to being an accredited SIEM and SOC Implementation Partner = total of **15pts** (below). • Three (3) and above testimonial **=0- 15pts** • Two (2) testimonials **=010pts** One (1) written testimonial **= 0-5pts** No written testimonial **=0pt**	• Bid Proposal • Provide and attach three (3) written testimonial letters What page (s) or section where information may be found? State **page (s) number ......** or State **section/ tab ....** on your proposal.	**15pts**		
Turnaround Times	Contract Management	Provide a detailed turnaround time strategy for milestones delivery provide a draft project plan within the bidder's proposal tied to timelines for the supply, delivery, installation, configuration, go live, handover of the solution and commitment to service delivery on warranty coverage. • 26 weeks turnaround time **=010pts** • 52 weeks turnaround time **=07pts** • 78 weeks turnaround time **=0- 4pts** • 104 weeks and more turnaround time **=0pt**	Turnaround time for management of the engagement and requests • State **page (s) number ....** or State **section/ tab ....** on your proposal.	**10pts**		

Note that Evaluation Committee will use their own discretion to assess quality of all bid proposals received in relation to above functionality criteria and may further verify information submitted from relevant sources/ your client and use their own discretion to score your proposal accordingly.					
Total weighted Points				**70**	

The minimum functionality threshold is **65** points. <u>Bidders who score less than **65** points on functionality will therefore be disqualified</u>; those who score **65** points or more will be further evaluated on **Criteria 3**.			
Price and Preference points used: **80/20** preferential procurement principle	**80** (Price)	R………………………..,………..	
	20 (BEE Status)	Level……… and points………….	

	Name of Evaluator:			
	Signature:		**Date:**	……………/………………………./2025

CRITERION 2- FUNCTIONALITY

Demo Evaluation

Criteria	Description	Weighting
1. Physical Site Visit	Evaluation Focus: Security measures preventing unauthorized physical access to the SOC. Measures to prevent unauthorized physical access to the SOC	0-2 pts
SOC Infrastructure and Technology Stack	Evaluation Focus: Tools and infrastructure in use for security monitoring and response. Network, power, cooling, storage, redundancy, and toolset setup	0-2 pts
Staffing and Skills Readiness	Evaluation Focus: SOC staffing levels, roles, and expertise. Onsite staff, certifications (e.g., CEH, CISSP), SOC staffing model	0-3pts
Compliance and Documentation	Evaluation Focus: SOC alignment with industry and regulatory standards. SOPs, compliance status (e.g., ISO 27001), policies, audit readiness	0-3pts

Incident Response Capabilities and Procedures	Evaluation Focus: SOC's ability to detect, respond, and recover from security incidents. Incident Response (IR) playbooks, forensic readiness, reporting chain	0-2pts
Client Reporting and Communication Facilities	Evaluation Focus: Transparency and client engagement mechanisms. Reporting tools, client comms channels, SLA-based feedback tools	0-3 pts
Real-Time Threat Detection and Response (SIEM & SOC)	Evaluation Focus: Demonstrate the ability to detect, prioritize, and respond to live security incidents in realtime using the SIEM platform. - SIEM correlation rules, SOC alert workflow, incident lifecycle	0-3 pts
Role-Based Access Control and Policy Enforcement (PAM & IAM)	Evaluation Focus: Showcase how identity and access are governed, with emphasis on least privilege enforcement, session recording, and multi-factor authentication. Identity lifecycle, policy management, privileged access workflows	0 – 3pts
Network Access Control Capabilities (NAC)	Evaluation Focus: Demonstrate how the system controls access based on device posture, location, and user role Device profiling, access control enforcement, posture assessment	0 – 3pts

System Architecture & Integration Demonstration	Evaluation Focus: Present end-to-end architecture with integration into existing on-prem and cloud environments. Integration with endpoints, SIEM, Identity Access Management (IAM), ticketing, cloud connectors	0 - 2pts
AI-Powered Automation & Predictive Analytics	Evaluation Focus: Show how AI/ML improves detection, reduces false positives, and supports predictive security. AI-driven threat scoring, automated response triggers	0 – 2pts
Usability, Training, and Change Management Tools	Evaluation Focus: Illustrate end-user interface and available tools for onboarding, training, and administration. Ease of use, user onboarding, training modules, change management plan	0 – 2pts
Total points		30pts

THE NATIONAL TREASURY

Republic of South Africa

_____

GOVERNMENT PROCUREMENT: GENERAL CONDITIONS OF   CONTRACT   **July 2010**

NOTES

The purpose of this document is to:

(i)   Draw special attention to certain general conditions applicable to government bids, contracts and orders; and;

(ii)   To ensure that clients be familiar with regard to the rights and obligations of all parties involved in doing business with government.

In this document words in the singular also mean in the plural and vice versa and words in the masculine also mean in the feminine and neuter.

The General Conditions of Contract will form part of all bid documents and may not be amended.

. Special Conditions of Contract (SCC) relevant to a specific bid, should be compiled separately for every bid (if (applicable) and will supplement the General Conditions of Contract. Whenever there is a conflict, the provisions in the SCC shall prevail.

TABLE OF CLAUSES

General Conditions of Contract

1. Definitions

1. The following terms shall be interpreted as indicated:

1.1 "Closing time" means the date and hour specified in the bidding documents for the receipt of bids.

1.2 "Contract" means the written agreement entered into between the purchaser and the supplier, as recorded in the contract form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

1.3 "Contract price" means the price payable to the supplier under the contract for the full and proper performance of his contractual obligations.

1.4 "Corrupt practice" means the offering, giving, receiving, or soliciting of anything of value to influence the action of a public official in the procurement process or in contract execution.

1.5 "Countervailing duties" are imposed in cases where an enterprise abroad is subsidized by its government and encouraged to market its products internationally.

1.6 "Country of origin" means the place where the goods were mined, grown or produced or from which the services are supplied. Goods are produced when, through manufacturing, processing or substantial and major assembly of components, a commercially recognized new product results that is substantially different in basic characteristics or in purpose or utility from its components.

1.7 "Day" means calendar day.

1.8 "Delivery" means delivery in compliance of the conditions of the contract or order.

1.9 "Delivery ex stock" means immediate delivery directly from stock actually on hand.

1.10 "Delivery into consignees store or to his site" means delivered and unloaded in the specified store or depot or on the specified site in compliance with the conditions of the contract or order, the supplier bearing all risks and charges involved until the supplies are so delivered and a valid receipt is obtained.

1.11 "Dumping" occurs when a private enterprise abroad market its goods on own initiative in the RSA at lower prices than that of the country of origin and which have the potential to harm the local industries in the RSA.

1.12 "Force majeure" means an event beyond the control of the supplier and not involving the supplier's fault or negligence and not foreseeable. Such events may include, but is not restricted to, acts of the

purchaser in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.

1.13   "Fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of any bidder, and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the bidder of the benefits of free and open competition.

1.14   "GCC" means the General Conditions of Contract.

1.15   "Goods" means all of the equipment, machinery, and/or other materials that the supplier is required to supply to the purchaser under the contract.

1.16   "Imported content" means that portion of the bidding price represented by the cost of components, parts or materials which have been or are still to be imported (whether by the supplier or his subcontractors) and which costs are inclusive of the costs abroad, plus freight and other direct importation costs such as landing costs, dock dues, import duty, sales duty or other similar tax or duty at the South African place of entry as well as transportation and handling charges to the factory in the Republic where the supplies covered by the bid will be manufactured.

1.17   "Local content" means that portion of the bidding price which is not included in the imported content provided that local manufacture does take place.

1.18   "Manufacture" means the production of products in a factory using labour, materials, components and machinery and includes other related value-adding activities.

1.19   "Order" means an official written order issued for the supply of goods or works or the rendering of a service.

1.20   "Project site," where applicable, means the place indicated in bidding documents.

1.21   "Purchaser" means the organization purchasing the goods.

1.22   "Republic" means the Republic of South Africa.

1.23   "SCC" means the Special Conditions of Contract.

1.24   "Services" means those functional services ancillary to the supply of the goods, such as transportation and any other incidental services, such as installation, commissioning, provision of technical assistance, training, catering, gardening, security, maintenance and other such obligations of the supplier covered under the contract.

1.25   "Written" or "in writing" means handwritten in ink or any form of electronic or mechanical writing.

2. Application

2.1 These general conditions are applicable to all bids, contracts and orders including bids for functional and

professional services, sales, hiring, letting and the granting or acquiring of rights, but excluding immovable property, unless otherwise indicated in the bidding documents.

2.2 Where applicable, special conditions of contract are also laid down to cover specific supplies, services or works.

2.3 Where such special conditions of contract are in conflict with these general conditions, the special conditions shall apply.

3. General

3.1 Unless otherwise indicated in the bidding documents, the purchaser shall not be liable for any expense incurred in the preparation and submission of a bid. Where applicable a non-refundable fee for documents may be charged.

3.2 With certain exceptions, invitations to bid are only published in the Government Tender Bulletin. The Government Tender Bulletin may be obtained directly from the Government Printer, Private Bag X85, Pretoria 0001, or accessed electronically from www.treasury.gov.za

4. Standards

4.1 The goods supplied shall conform to the standards mentioned in the bidding documents and specifications.

5. Use of contract documents and information; inspection.

5.1 The supplier shall not, without the purchaser's prior written consent, disclose the contract, or any provision thereof, or any specification, plan, drawing, pattern, sample, or information furnished by or on behalf of the purchaser in connection therewith, to any person other than a person employed by the supplier in the performance of the contract. Disclosure to any such employed person shall be made in confidence and shall extend only so far as may be necessary for purposes of such performance.

5.2 The supplier shall not, without the purchaser's prior written consent, make use of any document or information mentioned in GCC clause 5.1 except for purposes of performing the contract.

5.3 Any document, other than the contract itself mentioned in GCC clause 5.1 shall remain the property of the purchaser and shall be returned (all copies) to the purchaser on completion of the supplier's performance under the contract if so required by the purchaser.

5.4   The supplier shall permit the purchaser to inspect the supplier's records relating to the performance of the supplier and to have them audited by auditors appointed by the purchaser, if so required by the purchaser.

6. Patent rights

6.1 The supplier shall indemnify the purchaser against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the goods or any part thereof by the purchaser.

7. Performance security

7.1.1 Within thirty (30) days of receipt of the notification of contract award, the successful bidder shall furnish to the purchaser the performance security of the amount specified in SCC.

7.1.2 The proceeds of the performance security shall be payable to the purchaser as compensation for any loss resulting from the supplier's failure to complete his obligations under the contract.

7.3 The performance security shall be denominated in the currency of the contract, or in a freely convertible currency acceptable to the purchaser and shall be in one of the following forms:

(a) a bank guarantee or an irrevocable letter of credit issued by a reputable bank located in the purchaser's country or abroad, acceptable to the purchaser, in the form provided in the bidding documents or another form acceptable to the purchaser; or

(b) a cashier's or certified cheque

7.4 The performance security will be discharged by the purchaser and returned to the supplier not later than thirty (30) days following the date of completion of the supplier's performance obligations under the contract, including any warranty obligations, unless otherwise specified in SCC.

8. Inspections, tests and analyses

8.1   All pre-bidding testing will be for the account of the bidder.

8.2 If it is a bid condition that supplies to be produced or services to be rendered should at any stage during production or execution or on completion be subject to inspection, the premises of the bidder or contractor shall be open, at all reasonable hours, for inspection by a representative of the Department or an organization acting on behalf of the Department.

8.3 If there are no inspection requirements indicated in the bidding documents and no mention is made in the contract, but during the contract period it is decided that inspections shall be carried out, the

purchaser shall itself make the necessary arrangements, including payment arrangements with the testing authority concerned.

8.4 If the inspections, tests and analyses referred to in clauses 8.2 and 8.3 show the supplies to be in accordance with the contract requirements, the cost of the inspections, tests and analyses shall be defrayed by the purchaser.

8.5 Where the supplies or services referred to in clauses 8.2 and 8.3 do not comply with the contract requirements, irrespective of whether such supplies or services are accepted or not, the cost in connection with these inspections, tests or analyses shall be defrayed by the supplier.

8.6 Supplies and services which are referred to in clauses 8.2 and 8.3 and which do not comply with the contract requirements may be rejected. 8.7 Any contract supplies may on or after delivery be inspected, tested or analyzed and may be rejected if found not to comply with the requirements of the contract. Such rejected supplies shall be held at the cost and risk of the supplier who shall, when called upon, remove them immediately at his own cost and forthwith substitute them with supplies which do comply with the requirements of the contract. Failing such removal the rejected supplies shall be returned at the suppliers cost and risk. Should the supplier fail to provide the substitute supplies forthwith, the purchaser may, without giving the supplier further opportunity to substitute the rejected supplies, purchase such supplies as may be necessary at the expense of the supplier.

8.8 The provisions of clauses 8.4 to 8.7 shall not prejudice the right of the purchaser to cancel the contract on account of a breach of the conditions thereof, or to act in terms of Clause 23 of GCC.

9. Packing

9.1 The supplier shall provide such packing of the goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in the contract. The packing shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packing, case size and weights shall take into consideration, where appropriate, the remoteness of the goods' final destination and the absence of heavy handling facilities at all points in transit.

9.2 The packing, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the contract, including additional requirements, if any, specified in SCC, and in any subsequent instructions ordered by the purchaser.

10. Delivery and documents

10.1 Delivery of the goods shall be made by the supplier in accordance with the terms specified in the contract. The details of shipping and/or other documents to be furnished by the supplier are specified in SCC.

(i) advance notification to the purchaser of the pending termination, in sufficient time to permit the purchaser to procure needed requirements; and

(ii) following such termination, furnishing at no cost to the purchaser, the blueprints, drawings, and specifications of the spare parts, if requested.

15. **Warranty**

15.1 The supplier warrants that the goods supplied under the contract are new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials, unless provided otherwise in the contract.

15.2 The supplier further warrants that all goods supplied under this contract shall have no defect, arising from design, materials, or workmanship (except when the design and/or material is required by the purchaser's specifications) or from any act or omission of the supplier, that may develop under normal use of the supplied goods in the conditions prevailing in the country of final destination.

15.3 This warranty shall remain valid for twelve (12) months after the goods, or any portion thereof as the case may be, have been delivered to and accepted at the final destination indicated in the contract, or for eighteen (18) months after the date of shipment from the port or place of loading in the source country, whichever period concludes earlier, unless specified otherwise in the SCC.

15.4 The purchaser shall promptly notify the supplier in writing of any claims arising under this warranty.

15.5 Upon receipt of such notice, the supplier shall, within the period specified in the SCC and with all reasonable speed, repair or replace the defective goods or parts thereof, without costs to the purchaser.

15.6 If the supplier, having been notified, fails to remedy the defect(s) within the period specified in the SCC, the purchaser may proceed to take such remedial action as may be necessary, at the supplier's risk and expense and without prejudice to any other rights which the purchaser may have against the supplier under the contract.

16. **Payment**

16.1 The method and conditions of payment to be made to the supplier under this contract shall be specified in the SCC.

(i) Advance notification to the purchaser of the pending termination, in sufficient time to permit the purchaser to procure needed requirements; and

(ii) following such termination, furnishing at no cost to the purchaser, the blueprints, drawings, and specifications of the spare parts, if requested.

15. Warranty

15.1 The supplier warrants that the goods supplied under the contract are new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials unless provided otherwise in the contract. The supplier further warrants that all goods supplied under this contract shall have no defect, arising from design, materials, or workmanship (except when the design and/or material is required by the purchaser's specifications) or from any act or omission of the supplier, that may develop under normal use of the supplied goods in the conditions prevailing in the country of final destination.

15.2 This warranty shall remain valid for twelve (12) months after the goods, or any portion thereof as the case may be, have been delivered to and accepted at the final destination indicated in the contract, or for eighteen (18) months after the date of shipment from the port or place of loading in the source country, whichever period concludes earlier, unless specified otherwise in SCC.

15.3 The purchaser shall promptly notify the supplier in writing of any claims arising under this warranty.

15.4 Upon receipt of such notice, the supplier shall, within the period specified in SCC and with all reasonable speed, repair or replace the defective goods or parts thereof, without costs to the purchaser.

15.5 If the supplier, having been notified, fails to remedy the defect(s) within the period specified in SCC, the purchaser may proceed to take such remedial action as may be necessary, at the supplier's risk and expense and without prejudice to any other rights which the purchaser may have against the supplier under the contract.

16. Payment

16.1 The method and conditions of payment to be made to the supplier under this contract shall be specified in SCC.

16.2 The supplier shall furnish the purchaser with an invoice accompanied by a copy of the delivery note and upon fulfillment of other obligations stipulated in the contract.

16.3 Payments shall be made promptly by the purchaser, but in no case later than thirty (30) days after submission of an invoice or claim by the supplier.

16.4 Payment will be made in Rand unless otherwise stipulated in SCC.

17. Prices

17.1 Prices charged by the supplier for goods delivered and services performed under the contract shall not vary from the prices quoted by the supplier in his bid, with the exception of any price adjustments authorized in SCC or in the purchaser's request for bid validity extension, as the case may be.

18. Contract amendments

18.1 No variation in or modification of the terms of the contract shall be made except by written amendment signed by the parties concerned.

19. Assignment

19.1 The supplier shall not assign, in whole or in part, its obligations to perform under the contract, except with the purchaser's prior written consent.

20. Subcontracts

20.1 The supplier shall notify the purchaser in writing of all subcontracts awarded under this contracts if not already specified in the bid. Such notification, in the original bid or later, shall not relieve the supplier from any liability or obligation under the contract.

21. Delays in the supplier's performance

21.1 Delivery of the goods and performance of services shall be made by the supplier in accordance with the time schedule prescribed by the purchaser in the contract.

21.2 If at any time during performance of the contract, the supplier or its subcontractor(s) should encounter conditions impeding timely delivery of the goods and performance of services, the supplier shall promptly notify the purchaser in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the supplier's notice, the purchaser shall evaluate the situation and may at his discretion extend the supplier's time for performance, with or without the imposition of penalties, in which case the extension shall be ratified by the parties by amendment of contract.

21.3 No provision in a contract shall be deemed to prohibit the obtaining of supplies or services from a national department, provincial department, or a local authority.

21.4 The right is reserved to procure outside of the contract small quantities or to have minor essential services executed if an emergency arises, the supplier's point of supply is not situated at or near the place where the supplies are required, or the supplier's services are not readily available.

21.5 Except as provided under GCC Clause 25, a delay by the supplier in the performance of its delivery obligations shall render the supplier liable to the imposition of penalties, pursuant to GCC Clause unless an extension of time is agreed upon pursuant to GCC Clause 21.2 without the application of penalties.

21.6 Upon any delay beyond the delivery period in the case of a supplies contract, the purchaser shall, without canceling the contract, be entitled to purchase supplies of a similar quality and up to the same quantity in substitution of the goods not supplied in conformity with the contract and to return any goods delivered later at the supplier's expense and risk, or to cancel the contract and buy such goods as may be required to complete the contract and without prejudice to his other rights, be entitled to claim damages from the supplier.

22. Penalties

22.1 Subject to GCC Clause 25, if the supplier fails to deliver any or all of the goods or to perform the services within the period(s) specified in the contract, the purchaser shall, without prejudice to its other remedies under the contract, deduct from the contract price, as a penalty, a sum calculated on the delivered price of the delayed goods or unperformed services using the current prime interest rate calculated for each day of the delay until actual delivery or performance. The purchaser may also consider termination of the contract pursuant to GCC Clause 23.

23. Termination for default

23.1 The purchaser, without prejudice to any other remedy for breach of contract, by written notice of default sent to the supplier, may terminate this contract in whole or in part:

(a)   if the supplier fails to deliver any or all of the goods within the period(s) specified in the contract, or within any extension thereof granted by the purchaser pursuant to GCC Clause 21.2;

(b)   if the Supplier fails to perform any other obligation(s) under the contract; or

(c)   if the supplier, in the judgment of the purchaser, has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

23.2   In the event the purchaser terminates the contract in whole or in part, the purchaser may procure, upon such terms and in such manner as it deems appropriate, goods, works or services similar to those undelivered, and the supplier shall be liable to the purchaser for any excess costs for such similar goods, works or services. However, the supplier shall continue performance of the contract to the extent not terminated.

23.3 Where the purchaser terminates the contract in whole or in part, the purchaser may decide to impose a restriction penalty on the supplier by prohibiting such supplier from doing business with the public sector for a period not exceeding 10 years.

23.4 If a purchaser intends imposing a restriction on a supplier or any person associated with the supplier, the supplier will be allowed a time period of not more than fourteen (14) days to provide reasons why the envisaged restriction should not be imposed. Should the supplier fail to respond within the stipulated fourteen (14) days the purchaser may regard the intended penalty as not objected against and may impose it on the supplier.

23.5 Any restriction imposed on any person by the Accounting Officer / Authority will, at the discretion of the Accounting Officer / Authority, also be applicable to any other enterprise or any partner, manager, director or other person who wholly or partly exercises or exercised or may exercise control over the enterprise of the first-mentioned person, and with which enterprise or person the first-mentioned person, is or was in the opinion of the Accounting Officer / Authority actively associated.

23.6 If a restriction is imposed, the purchaser must, within five (5) working days of such imposition, furnish the National Treasury, with the following information:

(i) the name and address of the supplier and / or person restricted by the purchaser;

(ii) the date of commencement of the restriction

(iii) the period of restriction; and

(iv) the reasons for the restriction.

These details will be loaded in the National Treasury's central database of suppliers or persons prohibited from doing business with the public sector.

23.7 If a court of law convicts a person of an offence as contemplated in sections 12 or 13 of the Prevention and Combating of Corrupt Activities Act, No. 12 of 2004, the court may also rule that such person's name be endorsed on the Register for Tender Defaulters. When a person's name has been endorsed on the Register, the person will be prohibited from doing business with the public sector for a period not less than five years and not more than 10 years. The National Treasury is empowered to determine the period of restriction and each case will be dealt with on its own merits. According to section 32 of the Act the Register must be open to the public. The Register can be perused on the National Treasury website.

24. Anti-dumping and countervailing duties and rights

24.1 When, after the date of bid, provisional payments are required, or antidumping or countervailing duties are imposed, or the amount of a provisional payment or anti-dumping or countervailing right is increased in respect of any dumped or subsidized import, the State is not liable for any amount so required or imposed, or for the amount of any such increase. When, after the said date, such a provisional payment is no longer required or any such anti-dumping or countervailing right is abolished, or where the amount of such provisional payment or any such right is reduced, any such

favourable difference shall on demand be paid forthwith by the contractor to the State or the State may deduct such amounts from moneys (if any) which may otherwise be due to the contractor in regard to supplies or services which he delivered or rendered, or is to deliver or render in terms of the contract or any other contract or any other amount which may be due to him.

25. Force Majeure

25.1 Notwithstanding the provisions of GCC Clauses 22 and 23, the supplier shall not be liable for forfeiture of its performance security, damages, or termination for default if and to the extent that his delay in performance or other failure to perform his obligations under the contract is the result of an event of force majeure.

25.2 If a force majeure situation arises, the supplier shall promptly notify the purchaser in writing of such condition and the cause thereof. Unless otherwise directed by the purchaser in writing, the supplier shall continue to perform its obligations under the contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the force majeure event.

26. Termination for insolvency

26.1 The purchaser may at any time terminate the contract by giving written notice to the supplier if the supplier becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the supplier, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the purchaser.

27. Settlement of Disputes

27.1 If any dispute or difference of any kind whatsoever arises between the purchaser and the supplier in connection with or arising out of the contract, the parties shall make every effort to resolve amicably such dispute or difference by mutual consultation.

27.2 If, after thirty (30) days, the parties have failed to resolve their dispute or difference by such mutual consultation, then either the purchaser or the supplier may give notice to the other party of his intention to commence with mediation. No mediation in respect of this matter may be commenced unless such notice is given to the other party.

27.3 Should it not be possible to settle a dispute by means of mediation, it may be settled in a South African court of law.

27.4 Mediation proceedings shall be conducted in accordance with the rules of procedure specified in the SCC.

27.5 Notwithstanding any reference to mediation and/or court proceedings herein,

(a) the parties shall continue to perform their respective obligations under the contract unless they otherwise agree; and

(b) the purchaser shall pay the supplier any monies due the supplier.

28. Limitation of liability

28.1 Except in cases of criminal negligence or willful misconduct, and in the case of infringement pursuant to Clause 6;

    (a)   the supplier shall not be liable to the purchaser, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the supplier to pay penalties and/or damages to the purchaser; and

    (b)   the aggregate liability of the supplier to the purchaser, whether under the contract, in tort or otherwise, shall not exceed the total contract price, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.

29. Governing language

29.1 The contract shall be written in English. All correspondence and other documents pertaining to the contract that is exchanged by the parties shall also be written in English.

30. Applicable law

30.1 The contract shall be interpreted in accordance with South African laws, unless otherwise specified in SCC.

31. Notices

31.1 Every written acceptance of a bid shall be posted to the supplier concerned by registered or certified mail and any other notice to him shall be posted by ordinary mail to the address furnished in his bid or to the address notified later by him in writing and such posting shall be deemed to be proper service of such notice

31.2 The time mentioned in the contract documents for performing any act after such aforesaid notice has been given, shall be reckoned from the date of posting of such notice.

32. Taxes and duties

32.1 A foreign supplier shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed outside the purchaser's country.

32.2 A local supplier shall be entirely responsible for all taxes, duties, license fees, etc., incurred until delivery of the contracted goods to the purchaser.

32.3 No contract shall be concluded with any bidder whose tax matters are not in order. Prior to the award of a bid the Department must be in possession of a tax clearance certificate, submitted by the bidder. This certificate must be an original issued by the South African Revenue Services.

33. National Industrial Participation (NIP) Programme

33.1 The NIP Programme administered by the Department of Trade and Industry shall be applicable to all contracts that are subject to the NIP obligation.

34 Prohibition of Restrictive practices

34.1 In terms of section 4 (1) (b) (iii) of the Competition Act No. 89 of 1998, as amended, an agreement between, or concerted practice by, firms, or a decision by an association of firms, is prohibited if it is between parties in a horizontal relationship and if a bidder (s) is / are or a contractor(s) was / were involved in collusive bidding (or bid rigging).

34.2 If a bidder(s) or contractor(s), based on reasonable grounds or evidence obtained by the purchaser, has / have engaged in the restrictive practice referred to above, the purchaser may refer the matter to the Competition Commission for investigation and possible imposition of administrative penalties as contemplated in the Competition Act No. 89 of 1998.

34.3 If a bidder(s) or contractor(s), has / have been found guilty by the Competition Commission of the restrictive practice referred to above, the purchaser may, in addition and without prejudice to any other remedy provided for, invalidate the bid(s) for such item(s) offered, and / or terminate the contract in whole or part, and / or restrict the bidder(s) or contractor(s) from conducting business with the public sector for a period not exceeding ten (10) years and / or claim damages from the bidder(s) or contractor(s) concerned.

11. SERVICES SETA SUPPLIER DECLARATION FORM

The Supply Chain Management Manager

SSETA Vendor Management has received a request to load your company on to the SSETA vendor database. Please furnish us with the following to enable us to process this request:

1. Complete the "Supplier Declaration Form" **(SDF)** on page 2 of this letter
2. **Original** cancelled cheque **OR** letter from the bank verifying banking details (**with bank stamp)**
3. **Certified** copy of Identity document of Shareholders/Directors/Members (where applicable)
4. **Certified** copy of certificate of incorporation, CM29 / CM9 (name change)
5. **Certified** copy of share Certificates of Shareholders, CK1 / CK2 (if CC)
6. A letter with the company's letterhead confirming physical and postal addresses
7. **Original** or **certified** copy of SARS Tax Clearance certificate and Vat registration certificate
8. Proof of company registered with National Treasury Central Supplier Database (CSD)

9. Tax compliant on National Treasury Central Supplier Database (CSD) prior to award (Refer above 8)
10. **Proof of B-BBEE status level of contributor"** means:
     - B-BBEE Status level certificate issued by an authorized body or person; A sworn affidavit as prescribed by the B-BBEE Codes of Good Practice;
     - Any other requirement prescribed in terms of the B-BBEE Act;

NB: ▪ *Failure to submit the above documentation will delay the vendor creation process* .

▪ *Where applicable, the respective Services SETA business unit processing your application may request further information from you. E.g. proof of an existence of a Service/Business contract between your business and the SSETA.*

IMPORTANT NOTES:

a) **If your annual turnover is less than R10million,** then in terms of the DTI codes, you are classified as an Exempted Micro Enterprise (EME). If the company is classified as an EME, the company is only required to obtain a sworn affidavit on an annual basis, confirming the following:

    Annual Total Revenue of R10milion or less and

    Level of Black Ownership.

b) **If your annual turnover is between R10million and R50million**, then in terms of the DTI codes, you are classified as a Qualifying Small Enterprise (QSE). A QSE must comply with all of the elements of B-BBEE for the purposes of measurement.

Enhanced B-BBEE recognition level for QSE:

    A QSE which is 100% Black Owned qualifies for a Level One B-BBEE recognition.

    A QSE which is at least 51% Black Owned qualifies for a Level Two B-BBEE recognition level

    In the above cases the QSEs mentioned above are only required to obtain an sworn affidavit on an annual basis confirming the following:

    Annual Total Revenue of R50million or less;

    Level of Ownership

c) **If your annual turnover is in excess of R50million**, then in terms of the DTI codes, you are classified as a Large Enterprise and you claim a specific BEE level based on all 5 elements of the BBBEE Generic score-card. Please include your BEE certificate in your submission as confirmation of your status.
   NB: BBBEE certificate and detailed scorecard should be obtained from an accredited rating agency (permanent SANAS Member).

d) **To avoid PAYE tax being automatically deducted from any invoices received from you,** you must also contact the SSETA person who lodged this request on your behalf, so as to be correctly classified in terms of Tax legislation.

e) Unfortunately, **No payments can be made to a vendor** until the vendor has been registered,

f) vendor cannot be registered until the vendor application form, together with its supporting documentation, has been received and processed.

g) Please return the completed Supplier Declaration Form (SDF) together with the required supporting documents mentioned above to the SSETA Official who is intending to procure your company's services/products in order that he/she should complete an Internal SSETA Departmental Questionnaire before referring the matter to the appropriate SSETA Vendor Office.

SUPPLIER DECLARATION FORM

Company Trading Name	
Company Registered Name	

Company Registration Number Or ID Number If A Sole Proprietor	

Form of entity	CC	Trust	Pty Ltd	Limited	Partnership	Sole Proprietor

VAT number (if registered)	
Company Telephone Number	
Company Fax Number	
Company E-Mail Address	
Company Website Address	

Bank Name		Bank Account Number	

Postal Address			
		Code	

Physical Address			
		Code	

Contact Person	
Designation	
Telephone	

Email	