MICT SETA Head Office, Supply Chain Management 19 Richards Drive, Gallagher Convention Centre, Gallagher House, Level 3 West Wing Tel +27 11 207 2600; E-mail: bidqueries@mict.org.za

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE MEDIA INFORMATION AND COMMUNICATIONS TECHNOLOGIES SECTOR EDUCATION AND TRAINING AUTHORITY

REQUEST FOR BID REF: MICT/SETA/MSS/03/2025

REQUIREMENT DESCRIPTION:

APPOINTMENT OF A SERVICE PROVIDER FOR PROVISION OF MICT SETA MANAGED TECHNOLOGY SECURITY SERVICES FOR A PERIOD OF SIXTY (60) MONTHS

BID CLOSING DATE: 03 JUNE 2025 at 11:00 AM (SOUTH AFRICAN TIME)

MICT SETA Head Office, Supply Chain Management 19 Richards Drive, Gallagher Convention Centre, Gallagher House, Level 3 West Wing Tel +27 11 207 2600; E-mail: bidqueries@mict.org.za

BID REFERENCE NUMBER	**MICT/SETA/MSS/03/2025**
BID DESCRIPTION	**APPOINTMENT OF A SERVICE PROVIDER FOR PROVISION OF MICT SETA MANAGED TECHNOLOGY SECURITY SERVICES FOR A PERIOD OF SIXTY (60) MONTHS**
SUPPLIER BRIEFING SESSION	**Compulsory bidders conference will be held as follows:** **Date: 23 May 2025** **Time: 11:00 am South African Time** **Location: Microsoft Teams** **Meeting ID: 380 100 734 278 6** **Passcode: 2EM2pm94**
BID CLOSING DATE & TIME	**03 June 2025 @ 11:00 am South African Time.** ***Note: A bid will not be considered if it arrives a second after 11:00 am or any time thereafter. Bidders are therefore strongly advised to ensure that bids are dispatched allowing enough time for any unforeseen events that may delay the delivery of the bid.***
INSTRUCTION FOR SUBMISSION OF BID	**NB: Bid must be received in a sealed envelope (1 hard copy and 1 USB) marked with this RFB reference number and deposited in a tender box at the location indicated hereunder.**
LOCATION FOR BID SUBMISSIONS	**MICT SETA Head Office: Reception** **19 Richards Drive, Gallagher Convention Centre** **West Wing, level 3** **Midrand**
BID VALIDITY PERIOD	**Bids received shall remain valid for acceptance for a period of 120 days counted from the closing date of the bid.**

CLARIFICATION AND COMMUNICATION

a. All enquiries relating to this bid must be addressed in writing to bidqueries@mict.org.za five (5) days **before the closing date and time**. Queries received after this period will not be entertained.
b. The bid reference number must be mentioned in all correspondences.
c. Bids sent to any other platform other than the one specified herein will not be considered for evaluation. It is the bidder's responsibility to ensure that the bid is sent to the correct platform and that this is received by the MICT SETA before the closing date and time in MICT SETA's dedicated platform
d. All the documentation submitted in response to this RFP must be in English.

***Note**: Bidders are advised that a response will be disqualified should any attempt be made by a bidder either directly or indirectly to canvass any officer(s) or employees of **MICT- SETA** in respect of the RFB, between the closing and award date of the business.*

MICT SETA Head Office, Supply Chain Management 19 Richards Drive, Gallagher Convention Centre, Gallagher House, Level 3 West Wing Tel +27 11 207 2600; E-mail: bidqueries@mict.org.za

TABLE OF CONTENTS

MICT SETA Head Office, Supply Chain Management 19 Richards Drive, Gallagher Convention Centre, Gallagher House, Level 3 West Wing Tel +27 11 207 2600; E-mail: bidqueries@mict.org.za

SECTION 1: CHECKLIST INFORMATION

RETURNABLE DOCUMENTS CHECKLIST

Request For Bid invitation document must be completed, signed and submitted as a whole by the authorised Company representative. All forms must be properly completed, list below serve as a checklist of your RFB submission.

(Tick in the relevant block below)

DESCRIPTION	YES	NO
CSD Central Supplier Database (CSD) Registration Report. **SUPPLIER REGISTRATION ON CSD** Prospective suppliers must register on the National Treasury Central Supplier database in terms of National Treasury circular no 4A of 2016/17. The bidder shall register prior submitting a proposal/bid.		
SBD 1 - Fully completed with required proof **(Where applicable)**		
CIPC registration documents		
Bidder's eligibility: Form A		
Valid Tax Clearance Certificate (S) and or proof of application endorsed by **SARS** / and or **SARS** issued verification pin		
SBD 4 - Declaration of interest		
SBD 6.1: Preferential Procurement Claim Form		
Copy of joint venture/ consortium or sub-contracting agreement duly signed by all parties. **(Where applicable)**		
Certified Copy of director(s) ID(s) not older than (six) 6 months		
Shareholding Certificate **(Where applicable)**		
Pricing / Financial Proposal envelope and USB **(Must be submitted in a separate sealed envelope)**		
Financial Statements for 2023/2024 FY of the bidder		

Note: This BID must be completed and signed by the authorised Company representative

MICT SETA Head Office, Supply Chain Management 19 Richards Drive, Gallagher Convention Centre, Gallagher House, Level 3 West Wing Tel +27 11 207 2600; E-mail: bidqueries@mict.org.za

SECTION 2: MICT SETA -BID CONDITIONS

1. BID CONDITIONS

a. MICT SETA considers this bid and all related information, either written or verbal, which is provided to the respondent, to be proprietary to MICT SETA. The respondent shall not disclose, publish, or advertise this RFB or related information to any third party without the prior written consent of MICT SETA.
b. Bids for the supply of goods or services described in this document are invited in accordance with the provision of Government Procurement: General Conditions of Contract available for download from http://www.treasury.gov.za/divisions/ocpo/sc/GeneralConditions/
c. MICT SETA does not bind itself to accept the lowest or any RFB, nor shall it be responsible for or pay any expenses or losses which may be incurred by the bidder in the preparation and delivery of the RFB.
d. No Bid shall be deemed to have been accepted unless and until a formal contract / letter of intent is prepared and executed.
e. The technical proposal shall not include any price or financial information, technical proposal containing material financial information may be declared non-responsive.

1.1 MICT SETA reserves the right to:

a. Not evaluate or award RFB that do not comply strictly with the requirements of this RFB.
b. Make a selection solely on the information received in the RFBs and Enter into negotiations with any one or more of preferred bidder(s) based on the criteria specified in the evaluation of this RFB.
c. Contact any bidder during the evaluation process, in order to clarify any information, without informing any other bidders and no change in the content of the RFB shall be sought, offered or permitted.
d. Award a contract to one or more bidder(s).
e. Withdraw or amend the RFB at any stage.
f. Accept a separate RFB or any RFB in part or full at its own discretion.
g. Cancel this RFB or any part thereof at any stage as prescribed in the PPPFA regulation.

2. COST OF BIDDING

The bidder shall bear all costs and expenses associated with preparation and submission of its RFB or RFB, and the MICT SETA shall under no circumstances be responsible or liable for any such costs, regardless of, without limitation, the conduct or outcome of the bidding, evaluation, and selection process.

3. EXTENSION OF PROPOSAL VALIDITY PERIOD

In exceptional circumstances, prior to the expiration of the proposal validity period, MICT SETA may request Bidders to extend the period of validity of their bid proposals in writing and shall be considered integral to the proposal.

MICT SETA Head Office, Supply Chain Management 19 Richards Drive, Gallagher Convention Centre, Gallagher House, Level 3 West Wing Tel +27 11 207 2600; E-mail: bidqueries@mict.org.za

SECTION 3: FORM A: BIDDER'S ELIGIBILITY FORM

Name of Bidder:	
RFB Number:	

We, the undersigned, offer to provide the required services in accordance with the above Request for quotation and hereby declare that our firm, persons, or its directors, including any JV/Consortium /Association members or subcontractors or suppliers for any part of the contract:

a) is not under procurement prohibition by National Treasury, *from doing business with the public sector,*"

b) have not declared bankruptcy, are not involved in bankruptcy or engaged in corrupt / fraudulent practices, and there is no judgment or pending legal action against them that could impair their operations in the foreseeable future;

c) undertake not to engage in prescribed practices, including but not limited to corruption, fraud, coercion, collusion, obstruction, or any other unethical practice, with the MICT SETA or any other party, and to conduct business in a manner that averts any financial, operational, reputational or other undue risk to the MICT SETA.

d) *We declare that all the information and statements made in this Proposal are true and we accept that any misinterpretation or misrepresentation contained in this RFQ submission may lead to elimination of our RFQ submission.*

Name: _____

Title: _____

Date: _____

Signature: _____

MICT SETA Head Office, Supply Chain Management 19 Richards Drive, Gallagher Convention Centre, Gallagher House, Level 3 West Wing Tel +27 11 207 2600; E-mail: bidqueries@mict.org.za

SBD 1: PART A: INVITATION TO BID

SUPPLIER INFORMATION					
NAME OF BIDDER					
POSTAL ADDRESS					
STREET ADDRESS					
TELEPHONE NUMBER	CODE		NUMBER		
CELLPHONE NUMBER					
FACSIMILE NUMBER	CODE		NUMBER		
E-MAIL ADDRESS					
COMPANY REGISTRATION NUMBER					
DATE OF REGISTRATION					
VAT REGISTRATION NUMBER					
	TCS PIN:		**OR**	CSD No:	
AN ACCOUNTING OFFICER AS CONTEMPLATED IN THE CLOSE CORPORATION ACT (CCA) AND NAME THE APPLICABLE IN THE TICK BOX	☐	AN ACCOUNTING OFFICER AS CONTEMPLATED IN THE CLOSE CORPORATION ACT (CCA)			
	☐	A VERIFICATION AGENCY ACCREDITED BY THE SOUTH AFRICAN ACCREDITATION SYSTEM (SANAS)			
	☐	A REGISTERED AUDITOR			
		NAME:			
ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES /WORKS OFFERED?	☐Yes ☐No **[IF YES ENCLOSE PROOF]**		*ARE YOU A FOREIGN BASED SUPPLIER FOR THE GOODS /SERVICES /WORKS OFFERED?*	☐Yes ☐No [**IF YES ANSWER PART B:3 BELOW**]	
SIGNATURE OF BIDDER	……		*DATE*		
CAPACITY UNDER WHICH THIS BID IS SIGNED (Attach proof of authority to sign this bid; e.g. resolution of directors, etc.					
TOTAL NUMBER OF ITEMS OFFERED	Refer to pricing schedule/costing		*TOTAL BID PRICE (ALL INCLUSIVE)*	Refer to pricing schedule/costing	

MICT SETA Head Office, Supply Chain Management 19 Richards Drive, Gallagher Convention Centre, Gallagher House, Level 3 West Wing Tel +27 11 207 2600; E-mail: bidqueries@mict.org.za

PART B: TERMS AND CONDITIONS FOR BIDDING

	BID SUBMISSION:
1.1.	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 ONLINE.**
1.3.	**BIDDERS MUST REGISTER ON THE CENTRAL SUPPLIER DATABASE (CSD) TO UPLOAD MANDATORY INFORMATION NAMELY: (BUSINESS REGISTRATION/ DIRECTORSHIP/ MEMBERSHIP/IDENTITY NUMBERS; TAX COMPLIANCE STATUS; AND BANKING INFORMATION FOR VERIFICATION PURPOSES).**
1.4.	**WHERE A BIDDER IS NOT REGISTERED ON THE CSD, MANDATORY INFORMATION NAMELY: (BUSINESS REGISTRATION/ DIRECTORSHIP/ MEMBERSHIP/IDENTITY NUMBERS; TAX COMPLIANCE STATUS MAY NOT BE SUBMITTED WITH THE BID DOCUMENTATION.**
1.5.	THIS BID IS SUBJECT TO THE PREFERENTIAL PROCUREMENT POLICY FRAMEWORK ACT 2000 AND THE PREFERENTIAL PROCUREMENT REGULATIONS, 2022, THE GENERAL CONDITIONS OF CONTRACT (GCC) AND, IF APPLICABLE, ANY OTHER LEGISLATION OR SPECIAL CONDITIONS OF CONTRACT.
	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 VIEW THE TAXPAYER'S PROFILE AND TAX STATUS.
2.3	APPLICATION FOR TAX COMPLIANCE STATUS (TCS) OR PIN MAY ALSO BE MADE VIA E-FILING. IN ORDER TO USE THIS PROVISION, TAXPAYERS WILL NEED TO REGISTER WITH SARS AS E-FILERS THROUGH THE WEBSITE WWW.SARS.GOV.ZA.
2.4	BIDDERS MAY ALSO SUBMIT A PRINTED TCS TOGETHER WITH THE BID.
2.5	IN BIDS WHERE CONSORTIA / JOINT VENTURES / SUB-CONTRACTORS ARE INVOLVED; EACH PARTY MUST SUBMIT A SEPARATE PROOF OF TCS / PIN / CSD NUMBER.
2.6	WHERE NO TCS IS AVAILABLE BUT THE BIDDER IS REGISTERED ON THE CENTRAL SUPPLIER DATABASE (CSD), A CSD NUMBER MUST BE PROVIDED.
	QUESTIONNAIRE TO BIDDING FOREIGN SUPPLIERS
3.1.	IS THE BIDDER A RESIDENT OF THE REPUBLIC OF SOUTH AFRICA (RSA)? ☐ YES ☐ NO
3.2.	DOES THE BIDDER HAVE A BRANCH IN THE RSA? ☐ YES ☐ NO
3.3.	DOES THE BIDDER HAVE A PERMANENT ESTABLISHMENT IN THE RSA? ☐ YES ☐ NO
3.4.	DOES THE BIDDER HAVE ANY SOURCE OF INCOME IN THE RSA? ☐ YES ☐ NO
	IF THE ANSWER IS "NO" TO ALL OF THE ABOVE, THEN, IT IS NOT A REQUIREMENT TO OBTAIN A TAX COMPLIANCE STATUS / TAX COMPLIANCE SYSTEM PIN CODE FROM THE SOUTH AFRICAN REVENUE SERVICE (SARS) AND IF NOT REGISTER AS PER 2.3 ABOVE.

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

MICT SETA Head Office, Supply Chain Management 19 Richards Drive, Gallagher Convention Centre, Gallagher House, Level 3 West Wing Tel +27 11 207 2600; E-mail: bidqueries@mict.org.za

SECTION 4: BIDDING STRUCTURE

Bidding structure

Indicate the type of bidding structure by marking with an 'X':	
Individual bidder	
Joint Venture	
Consortium	
Subcontractors	
Other	
If the bid is submitted as a Consortium or Joint Venture or Sub-Contracting Arrangement list the members of such Consortium or Joint Venture and Sub-Contractors below:	

Bidder's Information (includes bids submitted Individual or as a Consortium or Joint Venture)

Supplier size type (Large or QSE or EME)	
First time business with MICT SETA (Yes/No)	
Number of existing running contracts and total value	
Total number of Employees	

Entity ownership

Ownership category	**% of ownership**
Black or historically disadvantage individual owned	
Black women owned	
Black youth owned	
People living with disability	
Military veteran	
Other ownership	
Total (100%)	

SECTION 5:
ANNEXURE A: TERMS OF REFERENCE /SPECIFICATION

REQUIREMENT DESCRIPTION: APPOINTMENT OF A SERVICE PROVIDER FOR PROVISION OF MICT SETA MANAGED TECHNOLOGY SECURITY SERVICES FOR A PERIOD OF SIXTY (60) MONTHS

1. INTRODUCTION

The Media, Information and Communication Technologies Sector Education and Training Authority (MICT SETA) is a public entity established in terms of Section 9(1) of the Skills Development Act (Act No. 97 of 1998). The MICT SETA plays a pivotal role in achieving South Africa's skills development and economic growth within the 5 distinct sub-sectors it operates in, i.e., Advertising, Film and Electronic Media, Electronics, Information Technology, and Telecommunications. To deliver on its mandate, key amongst the priorities of the organisation is:

1.1. Organisational sustainability through internal business excellence by resource management such as financial, human capital, technology, and information and knowledge management.
1.2. Increase in innovation through digital transformation.
1.3. Prevention, detection, and resilience against increased risk of cyber crime

2. BACKGROUND

2.1. MICT SETA National Footprint

The MICT SETA national footprint spans several towns in different provinces of the country as articulated below:

PROVINCE	DESCRIPTION	NUMBER OF USERS	ADDRESS
Gauteng	Midrand (Head Office)	119	Block 2, Level 3 West Wing, Gallagher House Gallagher Convention Centre 19 Richards Drive Halfway House Midrand, 1685
KwaZulu-Natal	Durban Regional Office	12	Ridge 8, 14th Floor 32 Vuna Close Umhlanga Ridge Durban, 4319
Eastern Cape	East London Regional Office	6	12 Esplanade Quigney East London 5201

Western Cape	Cape Town Regional Office	8	The Boulevard Office Park Block F, Ground Floor Searle Street Woodstock, 7925
Free State	Bloemfontein Regional Office	2	61 Bastion Street Bloemfontein
North-west	Klerksdorp Satellite Office	1	Vuselela TVET College Jourberton Centre for Engineering Studies 11900 5th Street, Jourberton Township

2.2. Technology Architecture

The MICT SETA Technology Architecture comprise of the following minimum infrastructure:

a. SD-WAN network – CISCO Meraki
b. Microsoft 365 A5
c. Azure AD
d. Mimecast mail control and archive
e. Sentinel One Anti-Virus
f. MS Teams linked telephony
g. CISCO Wi-Fi
h. Third-party connectivity such as IPSEC, APN, and VPN
i. Hosting of business applications on Microsoft Azure and other cloud platforms
j. DR services for key Technology Services
k. The network consists of approximately 260 network notes comprising user ±175 user devices, ±75 network devices, ±10 web applications. Included in the devices are laptops, MacBooks, iPads, network nodes, and other equipment.

2.3. Policy Provision

The MICT SETA Technology and Information Security Policy and Implementation Plan make provision for implementation of minimum acceptable Technology Security services to build resilience on the MICT SETA Technology Services. In summary, the minimum Technology Security Services include:

a. Zero Trust
b. End-to-end protection and detection
c. Patch Management
d. Multi-Factor Authentication (MFA)
e. Security Information and Event Management (SIEM)
f. Incident Management

g. Cybersecurity Training and Awareness
h. Managed Security Operations Centre (SOC)

3. PURPOSE AND OBJECTIVES

3.1. Purpose

3.1.1. The MICT SETA is looking to appoint a suitably skilled and experienced service provider with required accreditations for the provision of Managed Security Services.

3.1.2. The project will assist the MICT SETA to implement the framework of implementation security solutions to protect its information assets to achieve the principles and guidelines for safeguarding Technology and Information Assets and systems as outlined in the Technology and Information Security Policy and Implementation Plan.

3.1.3. The required services under this bid will enable the MICT SETA to cyberattacks and foster a security-aware culture within the organisation.

3.2. Objectives

Through this bid, the MICT SETA seeks to achieve the following objectives:

3.2.1. To implement the collective controls to prevent technology and information related risks from hampering the achievement of the MICT SETA's strategic goals and objectives.

3.2.2. To align management of cybersecurity risks with policies, procedures, and processes that enables management and monitoring the MICT SETA's regulatory, legal, risk, environmental, and operational requirements.

3.2.3. To ensuring cyber-resilience and availability of MICT SETA Technology Systems for improved business continuity,

3.2.4. To implement a roadmap for implementing technology security measures.

3.2.5. To foster a security-aware culture within the organization.

3.2.6. To proactively protect technology and information services from cyberattacks.

3.2.7. To educate and empower MICT SETA user community to make informed cyber risk decisions.

3.2.8. To institute a cyber security incident response capability.

3.2.9. To continually improve resilience of services.

4. PROJECT SCOPE AND REQUIREMENTS

The following sub-sections provide minimum requirements which must be provided by the successful bidder to be appointed through this bid:

4.1. CISO-As-A-Service (CAAS)

The successful bidder must have capacity to deliver services of a certified and experienced Chief Information Security Officer (CISO) and render these as a service to MICT SETA. The CISO must work with MICT SETA to ensure the following security governance processes are in place:

4.1.1. Risk Management and Governance which includes risk strategic planning, cybersecurity audit, risk management, compliance, and business continuity management.

4.1.2. Operations which include processes to identify, protect, detect, respond, and recover.

4.1.3. Business enablement which includes product security, cloud computing, mobile security, emerging technologies security, and security awareness and training.

4.2. Network Access Control (NAC) solution

4.2.1. 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.

4.2.2. Solution must automatically enforce security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area with appropriate notifications to the administrator.

4.2.3. 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.

4.2.4. Solution must support remote access capabilities on its management interface via HTTPS or SSH access.

4.2.5. Solution must be capable of agentless device discovery and control.

4.2.6. The proposed solution must support monitoring of traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, SD-WAN links etc., simultaneously.

4.2.7. The solution should be capable of being bypassed in the event of any failure of the solution.

4.2.8. 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.

4.2.9. Solution must have capability to determine whether users are accessing the network on an authorized, policy-compliant device.

4.2.10. Solution must have capability to establish user identity, location, and access history, which can be used for compliance and reporting.

4.2.11. 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.

4.2.12. 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).

4.2.13. The solution must allow authentication and authorization of users and endpoints via wired, wireless, and VPN with consistent policy throughout the network.

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

4.2.15. The NAC Solution must do the following endpoint checks for compliance for windows endpoints:

a. Check operating system / service packs / hotfixes.
b. Check process, registry, file & application.
c. Check for Antivirus installation / Version / Antivirus Definition Date.
d. Check for Antispyware installation/Version/ Antispyware Definition Date.
e. Check for windows update running & configuration.

4.2.16. Solution must support following remediation options for windows endpoints:

a. File remediation to allow clients download the required file version for compliance.

b. Link remediation to allow clients to click a URL to access a remediation page or resource.
c. Antivirus remediation to update clients with up- to-date file definitions for compliance after remediation.
d. Launch program remediation to remediate clients by launching one or more applications for compliance.
e. Windows update remediation to ensure Automatic.
f. Updates configuration is turned on Windows clients per security policy.

4.2.17. The proposed NAC solution must integrate with existing Network security tools LDAP, MS Active Directory, and RADIUS authentication servers for user authentication.

4.2.18. The proposed solution must be able to integrate with existing Antivirus solution.

4.2.19. 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.

4.2.20. Environment currently consists of approximately 200 users. The solution should cover a minimum of approximately 600 end points.

4.3. Zero Trust Password Safe

The proposed solution must be listed in Leader's quadrant of Gartner Magic Quadrant (MQ) report.

4.3.1. Technical Specification

a) The proposed solution must support the following functionality:

i. Secure and manage privileged password.
ii. Strong authentication and Single Sign-On (SSO).
iii. Application to Application password management.
iv. Access and Command control.

v. Audit trail and Session Recording.
vi. Workflow management.
vii. Smart grouping of asset.
viii. Scanner and onboarding.

b) Solution should provide application driven database.
c) Solution should be capable of delivering through single appliance for all roles. (Single appliance / server for password / session and reporting, etc.)

4.3.2. High Availability (HA) and Disaster Recovery (DR) functionality

a) The solution should have High Availability at DC and DR separately.
b) The proposed solution shall support for high redundancy and the DR architecture must be deployed on different network locations.
c) 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 cases of catastrophic failures.
d) Data replication between different network segments shall be performed natively without the need for external solution or infrastructure.

4.3.3. Asset Management and Discovery

a) The solution shall have bulk loading capability to import managed systems, privileged accounts, users, and other necessary objects.
b) The solution shall have the capability to record system information for managed systems including but not limited to IP addresses, MAC addresses, and DNS names, owners of the system, platform types and versions.
c) The solution shall allow administrators to define custom attributes for both managed systems and privileged accounts.
d) The solution shall have the capability to discover and maintain an inventory of all privileged and non-privileged accounts in known and unknown systems including but not limited to:
i. Windows
ii. Unix/Linux
iii. Mac OS
iv. Directories (AD / LDAP)
v. Databases
vi. Network Devices
e) 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.

f) The solution shall have the capability to discover Windows Services and Scheduled Tasks so that privileged credentials used by them can be managed automatically.
g) 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.
h) The solution shall have the capability to discover software that are installed, and ports open in the target system.
i) The solution shall have the capability to group target systems based on discovered and custom defined system attributes.
j) The solution shall have the capability to group systems and accounts based on the results of AD / LDAP query.
k) 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.
l) The solution must integrate with our service desk system.
m) The solution shall have the capability to discover new privileged accounts and on-board them for password management automatically.

4.3.4. Password / Credential management

a) The solution should have a strong in-built password vault / management system with single-sign-on feature.
b) Password vault should be replicated over a secured channel and off-site data backup; with data restoration capabilities.
c) The solution should be able to create flexible password management policies for assets. Policies should be applied to an object / a group of objects, or a group of policies can be applied to an asset / group of assets / objects.
d) 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.
e) The product should allow bulk operations to be performed on managed accounts (such as force password change immediately, reconcile password, verify password). It must also support scheduled password changes.
f) The 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).
g) 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.

h) The 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.
i) 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.
j) The solution should restrict the solution administrators from accessing or viewing passwords or approving password requests.
k) The proposed solution shall have support password policies. It should have an ability to set a minimum password length and complexity for super-user accounts across all systems in a single master policy.
l) The solution should have provisions to provide credentials for authenticating applications / scripts during run-time.
m) The platform should provide 100% availability of business applications. It 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.
n) Ability to automatically rotate application's passwords and SSH Keys based on configured policy without impact to application performance or downtime at the point of time when the data source password is changed.

4.3.5. MFA Integration with Identify and Access Management

The Zero Trust solution must be enabled for Identify and Access Management (IAM) *to enable to:*

a) The proposed solution should have functionality to integrate with Multi Factor Authentication (MFA) tool.
b) Identify and catalogue all privileged accounts including accounts with administrative rights on servers, databases, network devices, and other critical systems.
c) Implementing strict access controls for privileged accounts, and monitoring and recording privileged access activities to detect any suspicious or unauthorized behaviour.
d) Controlling and monitoring sessions initiated by privileged users by recording session activities for auditing and forensic analysis.
e) Enforcing strong password policies for privileged accounts and implementing regular password rotation and secure storage mechanisms.

f) Provision of temporary elevated privileges only when needed for specific tasks and automatically revoking elevated privileges when the task is completed.
g) Allowing users to perform specific privileged tasks without having full administrative rights and limitation of the scope of delegated privileges based on job responsibilities.
h) Evaluation of the risk associated with each access request and adjusting access controls dynamically based on the risk profile of the user, device, or activity.
i) Generation of comprehensive audit logs and reports on privileged access activities and ensuring compliance with regulatory requirements and internal security policies.
j) Coordination with IAM systems to ensure consistency in user provisioning, deprovisioning, access management, and maintaining a centralized view of user identities and access rights.
k) Implementation of automated processes for provisioning and deprovisioning of privileged access and streamlining approval workflows for access requests.
l) Implementation of security measures on endpoints to prevent unauthorised access or data breaches.

4.3.6. Access Management

The Zero Trust solution must be enabled for Access Management to enable:

a) The solution should provide web-based interface for easy access and management.
b) 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 with the user entitlements and access privileges granted (based on least privileges principle).
c) The solution should be able to support granular command filtering and / or context-sensitive entitlements on various platforms for super-user privileged management. The solution should also be able to detect and support concurrent login to managed systems for privileged users.
d) The solution should be capable of organizing / grouping target server device accounts into logical groups and apply granular / fine-grained access control to access individual accounts or groups of accounts.
e) The solution must support full Segregation of Duties; i.e., roles are clearly and unambiguously defined with no overlaps. In addition to user access roles and entitlements, the solution should also support role-based administrative access in order to provide Segregation of Duties for administrative management and control.
f) The solution should be capable of having dual control systems (maker-checker) for approval and authorization of critical operations.

g) The user permission should be only as per his / her original privilege even his / her 'SU'es after logging in to the Operating Systems. Solution must ensure that using root user credentials does not provide root privileges. Further, the solution must provide capability to restrict users to use RDP or SSH to other endpoints.
h) 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 users.
i) The solution should be capable of maintaining details of shared / pooled accounts by mapping them to individual users.
j) 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 in queries as configured for users/groups/target resources.
k) The solution must be able to integrate with vulnerability management solutions for deep, authenticated scans (e.g., Nexpose by Rapid7). This means that the solutions should be able to provide credentials to these scanning applications during run-time.

4.3.7. Workflows, Auditing & Reporting

The Zero Trust solution must be enabled for Workflows Auditing and Reporting to enable:

a) The solution should have ability to enforce approval workflow.
b) 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).
c) The Solution should be able to provide delegation of tasks such as approval or review. It should further support easy customization of approval workflows according to business needs (without requiring code changes). It should also be able to support emergency / break glass scenarios.
d) The solution should provide a central live Dashboard covering features like management of devices, events and password policies, user activities, event logs, etc.
e) 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 frequent, scheduled or on-demand reports.
f) The reports generation should support customisable CSV, Excel, or PDF. The report extraction should not have any performance impact. The

feature for report extraction should be available on demand or scheduled.

g) 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.
h) The solution should be able to record sessions, record videos or screen shots, keystrokes / commands, and output, replay sessions for forensic purposes. It should also provide optimized search capabilities on different parameters like users, events, time, target resources etc.
i) The solution should have real-time session monitoring support and full audit-trail for user activities in the solution itself.
j) The solution should be configurable so that events can trigger email / SMS alerts and run specific programs.
k) 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, and adding users to privileged groups).
l) The solution should have Log retention [all logs, recording, access data, accounting etc.] for minimum 6 months with RAID 5 storage.
m) The solution shall ensure proper segregation of duties with Role Based Access Control (RBAC) capability such that roles and accesses are properly defined.
n) The solution shall minimally support requester, approver, and reviewer roles for segregation of duties.
o) 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.
p) The solution must ensure personal accountability when user granted privileged password and session for shared account.
q) The solution shall support policy driven workflow and allow easy configuration through web interface to route password and session request to appropriate approver(s).

4.3.8. Solution must support at both DC and DR in HA mode and also with DC-DR functionality.

The Zero Trust solution must be enabled for HA to enable:

a) The users at DC should access the targeted devices primarily through IAM solution at DC.
b) In case primary IAM at DC fails, the users at DC should seamlessly be able to access the targeted systems through secondary IAM (HA) at DC.

c) The users at DR should access the targeted systems through IAM at DC but the subsequent sessions should be maintained by DR site.
d) In case IAM solution at DC fails, the users at DR should be seamlessly able to access the targeted devices through secondary IAM at DC and the subsequent sessions should be maintained by DR site.
e) In case both IAM at DC fails then all users should be seamlessly able to access the targeted systems through IAM at DR.
f) Solution must have capability to support MFA integration with other third-party solutions.

4.3.9. BitLocker

The Zero Trust solution must support BitLocker to provide enhanced security for data at rest, helping to prevent unauthorised access to sensitive information in case a device is lost, stolen, or otherwise compromised by:

a) Encryption of the entire disk drive, including the Windows operating system, system files, and user data.
b) Usage of strong encryption algorithms to protect data.
c) Incorporating pre-boot authentication, requiring users to enter a PIN or use another authentication method (such as a USB key) before the operating system is loaded.
d) Integrating with Microsoft Active Directory, making it easier for administrators to manage encryption and recovery keys in enterprise environments.

4.3.10. Must Have Points

a) Solution must be featured on Leaders' quadrant of Last published Gartner Magic Quadrant report for IAM.
b) The solution should be a single appliance which caters for password, session management and reporting on one appliance.
c) Separate database license should not be required for IAM. It must be application driven database and doesn't need any human intervention to manage. In case separate Database is needed then its price must be included in product cost.
d) The solution must have some Upload Utility to onboard privilege accounts in bulk.
e) The solution must have features to highlight risky session recordings or tag with high score so that auditors can identify those recordings and analyse it immediately.
f) 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.
g) The OEM must have 24/7 Support Centre across the Globe

4.4. Anti-Virus (AV) Solution

The supplied AV solutions should be able to meet the minimum requirements as detailed below:

4.4.1. End-to-end Prevention, Detection and Protection

a) Provide a multi-layered protection against malware, ransomware, exploits and fileless attacks.
b) Provide protection against scanning attacks, MITM, lateral movement and data exfiltration.
c) Use pre-defined behaviour rules coupled with dynamic behaviour profiling to detect malicious anomalies, including user and entity behaviour analysis (UEBA).
d) Provide a wide range of network, user, file decoys to lure advanced attackers into revealing their hidden presence.

4.4.2. Response Automation

a) The solution should provide automated root cause and impact analysis.
b) The solution should provide actionable conclusions on the attack's origin and its affected entities.
c) The solution should enable elimination of malicious presence, activity and infrastructure across user, network, and endpoint attacks.
d) The solution should provide intuitive flow layout of the attack and the automated response flow.
e) The solution should enable the ability to provide quick answers to the following questions:
    i. How the user got infected?
    ii. What was the first point of entry?
    iii. What / who else is part of the same attack?
    iv. Where the threat originated?
    v. How the threat spread?
    vi. How many other users have access or were exposed to the same threat?

4.4.3. Monitoring and Alerts

The AV solution should be enabled for monitoring and alerts for:

a) First line of defence against incoming alerts, prioritizing and notifying customer on critical events
b) Detailed analysis reports on the attacks that targeted the customer.
c) Search for malicious artifacts and IoC within the customer's environment.
d) Remote assistance in isolation and removal of malicious infrastructure, presence, and activity.

4.4.4. Dashboard and Reports

The AV solution should be enabled to provide dashboards and reports for:

a) Provide a single, customisable dashboard of the environment's overall inventory, health, incidents, and alerts.

4.4.5. Integration

The AV solution should be enabled to provide integration for:

a) Integrate with the SD-WAN network and all deployed Firewall and other appliances within the network.
b) Integration with supplied Patch Management solution

4.4.6. Mobile App

The AV solution should offer Mobile App with:

a) Full-featured mobile app for network and infrastructure monitoring.
b) Support iOS, Android and HarmonyOS devices.

4.4.7. Additional Services

Addition Services provided with the AV solution should include:

a) Supply cloud-based AV software
b) Configure pre-requisite settings on all software & hardware to ensure effective AV effectiveness.
c) Enrol all endpoints to the cloud platform.
d) Configure Central Dashboard and daily monitoring report.
e) Train IT Team (installation, Configuration, Monitoring, Threat hunting, Investigations).

4.5. Multi-Factor Authentication (MFA) & Single Sign-on

Supply cloud-based identity and access management solution with all required software licenses. The proposed solution must have the following capabilities:

4.5.1. Technical Specification

The MFA should provide functionality for:

a) Managing identity and access business systems, including cloud-based and offsite hosted systems.
b) Provide third-party access management which includes vendors and business partners.
c) Provide app, SMS and email based Multi-Factor Authentication (MFA) to help confirm employees' legitimacy before granting access.
d) Provide secure identity lifecycle management for onboarding and deprovisioning processes.
e) Provide risk-based adaptive authentication using factors such as user location, internet protocol (IP) address, time of previous logon, device footprint and more.
f) Enable automated access certification for review of employee and third-party access rights.

g) Support custom scripts that facilitate identity provisioning for in-house developed applications.
h) Provide self-service access requests through workflow approval rules.
i) Provide machine learning-based user behaviour analytics to mitigate threats such as malicious logins, lateral movement, malware attack, and privilege abuse.
j) Support high availability in cases of system and application failures.
k) Detect and prevent access conflicts of interest and potential risk of fraud.
l) Must have integration capabilities using industry standard protocols (e.g., SOAP / REST and / or more.)
m) Multi-Factor Authentication (MFA) on business systems.

4.5.2. Single Sign-on

The MFA should be enabled for Single Sign-on which include minimum functionality for:

a) Provide Single Sign-On (SSO) which allows employees to log into business systems using a single or federated identity.
b) User Account Lifecycle Management for Employees - through internal HR process and contactors / vendors' account management process.
c) User on-boarding / account activation – workflow approval, account provisioning, verification, and activation.
d) Account maintenance and support – privilege / role change, profile update.
e) User off-boarding / account termination – disable / delete account.

4.5.3. Access Management

The MFA should be enabled for Access Management which include minimum functionality for:

a) Automate access request.
b) Authenticate requesting identity.
c) Authorization of access.
d) Automate workflow.

4.5.4. Access Attestation

The MFA should be enabled for Access Management which include minimum functionality for:

a) 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 require.

4.6. Security Information and Event Management (SIEM)

The bidder shall provide a SIEM tool for aggregating and analysing critical events through the collection of security data from network components and the use of correlation rules. The SIEM tool must be able to monitor the following activities:

a. Information Security Incident Management.
b. Information Security Analytics e.g., user behaviour analytics.
c. Total Personal Record Exposed.
d. Total Company Records Exposed.
e. Account Takeover Management.
f. Internet of Things Management.
g. Monitor Third-Party Risk and Drive Remediation.
h. Potential Executive Credential Exposed.
i. 24x7x365 Attack Monitoring / Event Monitoring / Mitigation in real-time.
j. Blocking of malicious activity.
k. 24x7x365 Logging of attacks and security events.
l. Call escalating for analysis, mitigation plan & implementation.
m. Alert on security violations, viruses, worms, malware, and any other suspicious security activity.
n. Comprehensive reporting.
o. Monitoring, correlation, incident response, and reporting.

4.6.1. Event Log Analyzer Log Source Configuration

The SIEM should be enabled for event log analyser and log secure configuration which include minimum functionality to:

a) Enable windows device logging, troubleshoot configuration issues, and provide system requirements for log source.

b) Enable syslog device (hosted servers and cloud platforms, Firewalls, SD-WAN devices, and switches) logging, troubleshoot configuration issues, and provide system requirements for log source.

c) Enable other device (Print Service) logging, troubleshoot configuration issues, and provide system requirements for log source.

d) Enable database server logging, troubleshoot configuration issues, and provide system requirements for log source.

e) Enable IIS server logging, troubleshoot configuration issues and provide system requirements for log source.

f) Enable windows file integrity monitoring, troubleshoot configuration issues, and provide system requirements for log source.

g) Enable threat source (AV), troubleshoot configuration issues, and provide system requirements for log source.

h) Enable threat data logging troubleshoot configuration issues and provide system requirements for log source.

i) Enable log forwarder, troubleshoot configuration issues, and provide system requirements for log sources.

4.6.2. Event Log Reporting Configuration

The SIEM should be enabled for event log reporting configuration which include functionality to:

a) Enable reporting for all Windows events.

b) Enable reporting for windows Trend Events.

c) Enable reporting for windows server threat detection (DDos Attack).

d) Enable reporting for windows System events.

e) Enable reporting for windows Start-up events.

f) Enable reporting for windows scheduled Monthly Security Audit Logs Review

g) Enable reporting for all windows workstation events, device severity reports, workstation logon reports, workstation logoff reports, start-up events, system events, widows firewall auditing, scheduled tasks, process tracking, and scheduled monthly security audit logs review.

h) Enable reporting for server (hosted and cloud) trend reports, logon reports, logoff reports, failed logon reports, User Account Management, SUDO commands, Mail Server Reports, Threat Reports, scheduled monthly security audit logs review.

i) Enable reporting for NGFW flow allowed traffic, denied traffic, network equipment device logon reports, website traffic, and IPS / IDS reports.

4.6.3. Event Log Alert Configuration

The SIEM should be enabled for event log alert configuration which include functionality for:

a) Enable daily alerts for System / Server Threats.

b) Enable daily alerts for Web Server Threats.

c) Enable daily alerts for Database Treats.

d) Enable daily alerts for Ransomware Attacks.

e) Enable weekly alerts for File Integrity Threats.

f) Enable weekly alerts for Potential Windows Threats.

g) Enable weekly alerts for potential Unix / Linux Threats.

h) Enable weekly alerts for incidents violating the processes of cryptography in line with the relevant security policies.

4.6.4. Event Log Correlation

The SIEM should be enabled for event log correlation which include functionality for:

a) Capability to correlate User Account Threats for all log sources.

b) Capability to correlate System/Server Threats

c) Capability to correlate Web Server Threats

d) Capability to correlate Database Treats

e) Capability to correlate Ransomware Attacks

f) Capability to correlate File Integrity Threats

g) Capability to correlate Potential Windows Threats

h) Capability to correlate potential Unix/Linux Threats

i) Capability to correlate Cryptocurrency.

j) Capability to perform active monitoring on Windows Sessions

k) Capability to perform active monitoring on Unix/ Linux Sessions

l) Capability to perform active monitoring on VPN Sessions

4.6.5. Event Log Compliance

a) The SIEM event log my comply with key local and international reporting requirements such as POPIA, GDPR, and ISO 27001

4.6.6. System Administration

The SIEM system administration must follow the provisions of MICT SETA approved Access Management Policies with the restricted access according to specified profiles and user roles, and password security for privileged accounts such as:

a) Administrative access to be restricted according to specified profiles and user roles.

b) Full password security

4.7. Incident Management

The successful bidder will be required to treat all incidents according to MICT SETA policies and procedures such as the Incident Management SOP.

4.8. Cybersecurity Training and Awareness

Training and awareness should be delivered through implementation of automated continuous security awareness program to reduce cybersecurity risks from employees of the MICT SETA. The following interventions shall be implemented to raise awareness and improve the culture of cyber risk mitigations according to the provisions of the MICT SETA Technology and Information Security Policy:

a) Train end-users to recognise and report suspicious cyberattacks (phishing, baiting, tailgating, etc.) as well as train employees to properly handle (store, transfer, and destroy) sensitive data.
b) Security awareness or skills training targeted for specific roles such as end-users, System Administrators, Developers, and Service Desk Administrators.
c) Create a culture of cybersecurity awareness throughout the SETA to enable Users to taking ownership of their cybersecurity responsibilities and to being proactive in identifying and reporting potential threats.
d) Assist management to demonstrate leadership support for cybersecurity initiatives by proactively promoting and participating in cybersecurity awareness to reinforce the importance of security practices across the MICT SETA.

4.9. Managed Security Operations Centre (SOC)

The appointed service provider will be required to provide Managed SOC Services as follows:

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 must be able to correlate and prioritize advanced threats;
c. Monitor Network, on-prem and / or hosted systems security and Endpoints (For Network, Server, and Endpoint threat events) 24 x 7 x 365 using proprietary methods to actively hunt for signs of compromise;
d. Advanced AI-powered correlation of endpoint, network and on-prem and / or hosted platforms 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. Perform Indicators of Compromise (IoC) sweeping for the newly identified IoC's;

5. PROJECT METHODOLOGY AND APPROACH

Bidders must submit a detailed Project Plan (GANTT chart) including methodology statement that response to the project. The Gantt Chart must provide activities for the successful implementation of the project and its activities. The activities must include the following, *inter alia*:

5.1. Project Duration

The project duration shall be a period of three (03) years. The project duration and billing milestones shall be aligned with the Scope of Work (SoW). The SoW shall, *amongst others*,

include items listed in this bid document. Support and maintenance of services as articulated in the bid document, including but not limited to the following:

5.2. Project Implementation Plan

***Project Plan**: must demonstrate the following key areas of consideration:*

a) Project Management methodology

b) Project Phases (based on delivery timelines)

c) Project Activities as per the scope of work

d) Timelines

e) Resource Allocations

5.3. Project Methodology

The project Methodology must articulate how ALL the activities of the project / contract are to be performed regularly according to the below schedules:

5.3.1. Daily / Monthly

- The NAC solution
- Zero Trust
- End-to-end protection
- MFA
- SIEM
- Managed SOC
- VAPT remedial actions
- Incident Management

5.3.2. Monthly / Quarterly:

a) CISO services
b) Data collection
c) Penetration testing
d) Presentation of results
e) ICT capacity building
f) Cybersecurity awareness messages

5.3.3. Annually:

a) Cybersecurity awareness during cybersecurity month

5.4. Reporting

The following reports will be required:

5.4.1. Incident and Quarterly Reports which must include:

a) All incidents and problems experienced during the period under review
b) Planned activities for the coming period.

c) Other related processes of the project.

5.4.2. Project Closeout Report to be submitted at the end of the contract. The Closeout Report shall include the following:

a) Handover process for transition to MICT SETA and / or any other representative of MICT SETA.

b) Transfer of MICT SETA Intellectual Property (IP) which might have been transferred / generated upon commencement of the contract or during execution of services.

c) Recommendations for future management security services projects.

6. COMPANY PROFILE

This Request for Proposal is open to consulting entities that have the following profile:

6.1. In possession of valid ISO27001 certification

6.2. Competent and experienced resources with years providing similar services

6.3. Previous track record with at least five (05) references of rendering similar services in the past 05 years.

6.4. Service provider must demonstrate applicable local or international standards on providing the required services.

6.5. The consulting entity must have qualified personnel in cyber security, penetration testing and familiarity with industry best practice frameworks as outlined under Mandatory Requirements section:

7. CONFIDENTIALITY TERMS AND CONDITIONS

7.1. The successful bidder will be bound to comply with MICT SETA confidentiality processes, including the non-disclosure agreement to ensure that it does not share any data / information gathered during the contract with any other person or entity without prior permission of MCT SETA. The data / information must not be used for any other purpose except for the originally intended.

7.2. The successful bidder will be subjected to compliance with the requirements of the POPI Act and the MICT SETA POPIA policies.

7.3. MICT SETA undertake to maintain confidentiality relating to any unpublished information supplied by the successful bidder as part of this Request for Proposal and will only use any information provided for the purposes of evaluating the proposal.

MICT SETA Head Office, Supply Chain Management 19 Richards Drive, Gallagher Convention Centre, Gallagher House, Level 3 West Wing Tel +27 11 207 2600; E-mail: bidqueries@mict.org.za

8. PRICING SCHEDULE

Name of bidder: _____ **Bid number:** _____

Closing date: _____

Bid shall remain valid for acceptance for a period of **120 days** counted from the closing date.

Bidders to provide further cost breakdown where necessary under each line item, and sub-total and the overall RFB price (Total) should be included. The below table is for illustration only:

ITEM #	DESCRIPTION OF SERVICES	UNIT COSTS (Each item)	FREQUENCY (Once-off, Monthly, Quarterly, Annually)	QTY	TOTAL COST
1	Subscription of software and licences • NAC • Zero Trust • End-to-end protection • MFA • SIEM • Incident Management • Cybersecurity Training and Awareness	**R**			**R**
2	Technical Project Resources	**R**			**R**
3	CISO-As-A-Service	**R**			**R**
5	Training and Skills Transfer	**R**			**R**
6	Managed SOC Services	**R**			**R**
7	Project Management	**R**			**R**
				Sub-Total	**R**
				VAT @15%	**R**
				Total	**R**

NB: Bidders must submit this pricing schedule and related Annexure on a Separate envelope.

MICT SETA Head Office, Supply Chain Management 19 Richards Drive, Gallagher Convention Centre, Gallagher House, Level 3 West Wing Tel +27 11 207 2600; E-mail: bidqueries@mict.org.za

I/We, the undersigned, agree that this bidding price shall remain binding on me/us and open for acceptance for the period stipulated above.

Authorised Company Representative: .....

Capacity under which this quote is signed: .....

Signature: .....

Date: .....

SECTION 9: BID EVALUATION CRITERIA

MICT SETA complies with the provisions of the Public Finance Management Act, Act No. 1 of 1999 as amended; Treasury Regulations of 2005; the Preferential Procurement Policy Framework Act, Act No. 5 of 2000; Preferential Procurement Regulations of 2022; and the MICT SETA Supply Chain Management (SCM) Policy.

Bids received will be evaluated on the following set criteria.

9.1. BIDDERS CONFERENCE

9.1.1. Bidder must attend compulsory bidders conference

Proof of compliance to bidder's conference
Bidder must complete and sign the attendance register of the virtual compulsory briefing session held on Microsoft Office.

Please note: Non-attendance of the compulsory bidders' conference will automatically disqualify any prospective bidder from further evaluation process.

9.2. MANDATORY CRITERIA

9.2.1. Mandatory Criteria 1:
The bidder must hold **valid** International Standards Organisation certification to provide and deliver Managed Security Management Systems and / or Services.

Proof of Compliance to Mandatory criteria 1:
The bidder must submit a **valid** certification of ISO 27001: 2013 (Information Security Management)

9.2.2. Mandatory Criteria 2:
The bidder must be OEM or authorised to provide the products / services proposed to deliver according to the requirements of this bid.

Proof of Compliance to Mandatory criteria 2:
Proof of Evidence on bidder's product accreditation by OEM or proof of ownership if bidder is the OEM:

a) **All products proposed for NAC services**
b) **All products proposed for Zero Trust services**
c) **All products proposed for end-to-end protection and detection services**
d) **All products proposed for MFA services**
e) **All products proposed for SIEM services**
f) **All products proposed for Incident Management**
g) **All products proposed for Cybersecurity training and awareness**
h) **All products proposed for Managed SOC services**

NB: The above is to mention some of the products. Any other products / services with no accreditations or ownership letter will not be recognised in the evaluation of this bid. This will lead to non-responsive bid.

9.2.3. Mandatory Criteria 3:

The bidder must submit copies of valid certification of all technical lead/Project lead personnel certification in cybersecurity and familiar with industry best practices required to deliver on the bid.

Proof of Compliance to Mandatory criteria 3:

The certification must, at a minimum, include technical resources with the following certification:

a) Project Team Lead with Certified CISA, CISSP, CRISC or Certified Ethical Specialist (CEH) - x1

b) Project Manager with (PMP / Prince 2, or other equivalent Project Management certification) - x1 – CISM certification would be an added advantage

The certifications provided must align to the CVs of personnel proposed technical lead/Project lead personnel in the functional criteria.

NB: Failure to comply with the requirements of set mandatory criteria will lead to bidder's proposal being eliminated from further evaluation process.

9.3. FUNCTIONAL EVALUATION CRITERIA

Only bidders that have complied to the requirements of the set mandatory criteria will be considered for functionality evaluation. Bids submitted will be evaluated on technically functionality out of a maximum of **100 points**. A threshold of **80** out of the **100** points has been set.

Only bidders that have met or exceeded the qualification threshold on technical functionality of **80** points will qualify for further evaluation on Price and Specific Goals.

Note: All bidders achieving less than the set threshold of 80 points will be declared non-responsive.

Assessment of evaluation of the functional/ technical criteria will be based on the table below:

Note: Bidders that do not meet the requirements of set functional criteria will be eliminated from further evaluation process.

FUNCTIONAL CRITERIA			
NO	**CATEGORY**	**FUNCTIONAL EVALUATION CRITERIA**	**MAXIMUM POINTS**
1	**SOLUTION PROPOSAL**	The Bidder must submit a proposal for the Managed Security Services. The proposal must cover the minimum requirements for the proposed solution as detailed in the bid and summarised below: • **CISO-As-A-Service (CAAS)** requirements and services • **Network Access Control (NAC)** requirements and services • **Zero Trust** requirements and services • **End-to-end protection and detection** requirements and services • **Multi Factor Authentication (MFA)** requirements and services	**35**

		• **Security Information Event Monitoring (SIEM)** requirements and services • **Incident Management** requirements and services • **Cybersecurity training and awareness** requirements and services • **Managed SOC services** requirements and services **Points on submission of proposed Managed Security Services solution will be allocated as follows:** • Bidder submitted a proposal that meets or exceeds all components of the Managed Security Service solution requirements of the bid **= 35 points** • Bidder submitted a proposal that does not meet all the components Managed Security Service solution **= 00 points** **NB: Non-compliance with the minimum requirements will be declared non-responsive.**	
2	**EXPERIENCE AND REFERENCES**	The bidder must submit reference letters indicating experience in rendering Managed Security Services or similar services (as outlined in the scope of work) in the past five (5) years. The reference letters must at least include: o CISO, o Cybersecurity Training and Awareness and o Managed SOC services monitoring at least 500 devices from a single client. Reference letters with contactable references for Managed Security Services or similar services, in the past five (5) years, are required. The reference letters must be from Bidder's clients within the Republic of South Africa (RSA), must indicate project duration, must be on company letterhead, and signed by the Bidder's client. **[10 points]** **Points on submission of reference letters, with experience in Managed Security Services or similar will be allocated as follows:** • Five (05) or more signed reference letters from different clients, with five (05) years' experience or more **= 10 points** • Four (04) signed reference letters from different clients, with five (05) years' experience **= 08 points** • Three (03) signed reference letters from different clients, with five (05) years' experience **= 06 points** • Two (02) signed reference letters from different clients, with five (05) years' experience **= 04 points** • One (01) signed reference letters from different clients, with five (05) years' experience **= 02 points** • No reference letters submitted **= 0 points**	**10**

		NOTE: The MICT SETA may verify the Reference Letters prior. Bidders with no track record of rendering similar services will be deemed non-responsive.	
3	**PROJECT METHODOLOGY AND APPROACH**	Bidders are required to provide a detailed Project Implementation Methodology, approach, and Project Implementation Plan in executing the project and support services. • The methodology and approach should include all elements of the bid, as per the following section and subsections: 1) 4.1CAAS 2) 4.2 NAC 3) 4.3 Zero Trust Password Safe 4) 4.4 Anti-Virus Solution 5) 4.5 Multi Factor Authentication 6) 4.6 SIEM 7) 4.7 Incident Management 8) 4.8 Cybersecurity Training and Awareness 9) 4.10 Managed SOC 10) 5.2 Project Implementation Plan 11) 5.3 Project Methodology 12) 5.4 Reporting **Points on submission of Project Implementation Methodology and Approach will be allocated as follows [20 points]:** • A detailed methodology and approach that meets all elements of the bid as per section 4, 5.2, 5.3 and 5.4 of this bid **= 25 points** • A methodology and approach that does not meet all elements as per section 4, 5.2, 5.3 and 5.4 of this bid **= 0 points** The Project Plan should clearly indicate the following (but not limited to key processes: 1) Project team and resource allocation; 2) Project deliverables; 3) Project sub-activities; and 4) Project timelines. **Points on submission of Project Plan will be allocated as follows: [10 points]** • Detailed project plan that meets four (04) areas of the project plan **= 10 Points** • Detailed project plan that meets three (03) areas of the project plan **= 07 Points** • Detailed project plan that meets two (02) area of the project plan **= 05 Points**	**35**

		• Detailed project plan that meets only one (01) area of the project plan **= 03 Points** • Project implementation plan that meets none of the areas of the project plan / non submission of the project implementation plan **= 00 Points** **NB: all elements must be covered in detail.**	
4	**PROJECT TEAM**	CVs of key Project Team members to be attached, specifically for the Project Manager and Technical Lead: [**20 points**]. **Project Manager *(certified with PMP / Prince 2, or other equivalent Project Management certification)*.** Relevant experience of Project Manager. Profile or CV should clearly indicate experience in Managed Security Services or similar the projects, and names of clients: **[10 points]**. **Points on submission of CV or profile of Project Manager with experience on managed security services or relevant projects will be allocated as follows:** • CV of project Manager with Five (05) years and above experience in managed security services or relevant projects **= 10 points** • CV of project Manager with four (04) years' experience in managed security services or relevant projects • **= 08 points** • CV of project Manager with three (03) years' experience in managed security services or relevant projects **= 08 points** • CV of project Manager with Less than three (03) years in managed security services or relevant projects **= 00 points** **Technical Lead *(certified with CISA, CISSP, CRISC, CEH or related qualification)*.** Relevant experience of Project Technical Lead in managing similar Managed Security Projects. Profile or CV should clearly indicate experience in Managed Security Services or similar the project, and names of clients: [**10 points**]. **Points on submission of CV or profile of Project Technical Lead with experience on managed security services or relevant projects will be allocated as follows:** • CV of Project Technical Lead with Five (05) years and above experience in managed security services or relevant projects **= 10 points** • CV of Project Technical Lead with four (04) years in managed security services or relevant projects **= 08 points** • CV of Project Technical Lead with three (03) years in managed security services or relevant projects **= 05 points**	**20**

		• CV of Project Technical Lead with Less than three (03) years' experience in managed security services or relevant projects **= 00 points** **Note: the projects in this factor refer to those delivered by the project team in any current or past company, not limited to the bidding company, i.e., linked to the individual.** **Bidders with no project competent team members will fail risk analysis on their capacity to deliver on the project and will therefore be deemed non-responsive.**	
TOTAL			**100**
MINIMUM THRESHOLD			**80**

9.4. PRICE AND SPECIFIC GOALS

Only bidder/s or bid proposals received that have met the requirements of set evaluation criteria will qualify for further evaluation on Price and Specific Goals according to the 80/20 preference point system in terms of the Preferential Procurement Regulations 2022, where 80 points will be for Price and 20 points will be for Specific Goals. Bids will be awarded to the bidder scoring the highest points.

Specific Goal to be evaluated out of **20 Points**:

Criteria	Points
Enterprise owned by historically disadvantaged persons.	10
Enterprise owned by historically disadvantaged women.	05
Enterprise owned by historically disadvantaged youth.	05
Total	**20**

** **Enterprises that are not owned by historically disadvantaged persons will be allocated 0 points.**

Bidder must submit the following documents:
- Certified ID copies of the company's directors as per the CIPC documents. (Certified copies must not be older than six (06) months).
- CIPC Documents and/or share certificate (for companies with more than one (01) Director).

Failure on the part of a service provider to submit proof or documentation required in terms of this Bid to claim points for specific goals, will be interpreted to mean that preference points for specific goals are not claimed

MICT SETA Head Office; Supply Chain Management 19 Richards Drive, Gallagher Convention Centre, Gallagher House, Level 3 West Wing Tel: +27 11 207 2600, E-mail: bidqueries@mict.org.za

SBD 4

BIDDER'S DICLOSURE

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[1] 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

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

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**

[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.

MICT SETA Head Office; Supply Chain Management 19 Richards Drive, Gallagher Convention Centre, Gallagher House, Level 3 West Wing Tel +27 11 207 2600, E-mail: bidqueries@mict.org.za

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 consortium[2] 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.

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.

[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.

MICT SETA Head Office; Supply Chain Management 19 Richards Drive, Gallagher Convention Centre, Gallagher House, Level 3 West Wing Tel: +27 11 207 2600, E-mail: bidqueries@mict.org.za

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

PREFERENCE PROCUREMENT CLAIM FORM

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

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

b) the **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
PRICE	**80**
SPECIFIC GOALS	**20**
Total points for Price and SPECIFIC GOALS	**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.

MICT SETA Head Office; Supply Chain Management 19 Richards Drive, Gallagher Convention Centre, Gallagher House, Level 3 West Wing Tel +27 11 207 2600, E-mail: bidqueries@mict.org.za

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**

$$Ps = 80\left(1 - \frac{Pt - P\,min}{P\,min}\right) \quad \text{or} \quad Ps = 90\left(1 - \frac{Pt - P\,min}{P\,min}\right)$$

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**

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

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 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 (80/20 system) (To be completed by the organ of state)	Number of points claimed (80/20 system) (To be completed by the tenderer)
Enterprises which are at least 51% owned by historically disadvantaged persons.	10	
Enterprises which are at least 51% owned by historically disadvantaged women.	05	
Enterprises which are at least 51% owned by historically disadvantaged youth.	05	

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: .....

.....