ART A
INVITATION TO BID

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE (*South African National Biodiversity Institute*)					
BID NUMBER:	SANBI: IT514/2023	CLOSING DATE:	24 April 2024	CLOSING TIME:	11:00am
DESCRIPTION	**THE APPOINTMENT OF A SERVICE PROVIDER TO PROVIDE MANAGED INFORMATION SECURITY SERVICES FOR THE SOUTH AFRICAN NATIONAL BIODIVERSITY INSTITUTE (SANBI) FOR A PERIOD OF THREE (3) YEARS.**				

BID RESPONSE DOCUMENTS MAY BE DEPOSITED IN THE BID BOX SITUATED AT *(STREET ADDRESS)*
BID RESPONSE DOCUMENTS MAY BE DEPOSITED IN THE BID BOX SITUATED AT: Biodiversity Centre Pretoria National Botanical Garden, 2 Cussonia Avenue, Brummeria Pretoria
A compulsory briefing session will be conducted at the time and date given as follows: **Date: 10 April 2024** **Time: 11:00** **Venue: Microsoft Teams Meeting**

BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO		**TECHNICAL ENQUIRIES MAY BE DIRECTED TO:**	
CONTACT PERSON		CONTACT PERSON	
TELEPHONE NUMBER		TELEPHONE NUMBER	
FACSIMILE NUMBER		FACSIMILE NUMBER	
E-MAIL ADDRESS	sanbi.tenders@sanbi.org.za	E-MAIL ADDRESS	v.moerane@sanbi.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

B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE	TICK APPLICABLE BOX]	B-BBEE STATUS LEVEL SWORN AFFIDAVIT	[TICK APPLICABLE BOX]
	☐ Yes ☐ No		☐ Yes ☐ No

[A B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE/ SWORN AFFIDAVIT (FOR EMES & QSEs) MUST BE SUBMITTED IN ORDER TO QUALIFY FOR PREFERENCE POINTS FOR B-BBEE]

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 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 A 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:
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 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, 2017, 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: ……...

PRICING SCHEDULE – FIRM PRICES

(PURCHASES)

NOTE: **ONLY FIRM PRICES WILL BE ACCEPTED. NON-FIRM PRICES (INCLUDING PRICES SUBJECT TO RATES OF EXCHANGE VARIATIONS) WILL NOT BE CONSIDERED**

IN CASES WHERE DIFFERENT DELIVERY POINTS INFLUENCE THE PRICING, A SEPARATE PRICING SCHEDULE MUST BE SUBMITTED FOR EACH DELIVERY POINT

Name of bidder……Bid number: **SANBI:IT514-2023**
Closing Time 11:00 Closing date: **24 April 2024**

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

ITEM NO.	QUANTITY	DESCRIPTION	BID PRICE IN RSA CURRENCY
			** (ALL APPLICABLE TAXES INCLUDED)

- Required by: ……
- At: ……
  ……
- **Brand and model** **…….**
- **Country of origin** **…….**
- **Does the offer comply with the specification(s)?**
  ***YES/NO**
- **If not to specification, indicate deviation(s)** **…….**
- **Period required for delivery** **…….**
  ***Delivery: Firm/not firm**
- **Delivery basis** **……**

Note: All delivery costs must be included in the bid price, for delivery at the prescribed destination.

**** "all applicable taxes" includes value- added tax, pay as you earn, income tax, unemployment insurance fund contributions and skills development levies.**

***Delete if not applicable**

SBD 4

BIDDER'S DISCLOSURE

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 interest1 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**

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:

……
……

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.

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.

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

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.

SBD 6.1

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.

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.

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 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)
Categories of persons historically disadvantaged by unfair discrimination on the basis of race. Information will be verified on the CSD report. Points will be allocated based on the percentage of ownership per goal Black Ownership = 10 Points		(10)		
Categories of persons historically disadvantaged by unfair discrimination on the basis of gender.		(5)		

Information will be verified on the CSD report. Points will be allocated based on the percentage of ownership per goal Female Ownership = 5 Points				
Categories of persons historically disadvantaged by unfair discrimination on the basis of disability Information will be verified on the CSD report. Points will be allocated based on the percentage of ownership per goal Disability Ownership = 5 Points		(5)		
Total		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: ……

REQUEST FOR TENDER

FOR

THE APPOINTMENT OF A SERVICE PROVIDER TO PROVIDE MANAGED INFORMATION SECURITY SERVICES FOR THE SOUTH AFRICAN NATIONAL BIODIVERSITY INSTITUTE (SANBI) FOR A PERIOD OF THREE (3) YEARS.

The South African National Biodiversity Institute (SANBI)
Private Bag X101
Silverton
0184
Gauteng

Tender No: SANBI:IT514/2023

Contents

Introduction and background

The South African National Biodiversity Institute (SANBI) is a public entity that is mandated by the National Environmental Management: Biodiversity Act (NEMBA), Act No. 10 of 2004. SANBI's mission is to champion the exploration, conservation, sustainable use, appreciation and enjoyment of South Africa's exceptionally rich biodiversity for all people. SANBI contributes to South Africa's sustainable development by facilitating access to biodiversity data, generating information and knowledge, building capacity, providing policy advice, showcasing and conserving biodiversity in its national botanical and zoological gardens.

Given the business operations of SANBI, which is informed by its mandate, the organisation relies heavily on technology in order to achieve its strategic objectives. The different technologies currently used at SANBI expose the organisation to many information security threats. It was for these reasons that the organisation took a strategic decision and approach to invest in information security, which is aimed at protecting the information assets of SANBI.

The successful bidder will be required to manage daily information security for SANBI. This includes providing or allocating human resources onsite on a daily basis for the duration of the contract. The successful bidder will also be required to provide information security tools in the form of a Security Operations Centre (SOC) and produce monthly information security reports that outline the security posture of the organisation.

SANBI has two (2) datacentres, one in Pretoria and another in Cape Town. The following table shows where SANBI has offices in each of the seven provinces listed below, and where there is Information and Communication Technology (ICT) infrastructure:

i)	PROVINCE	ii)	BOTANICAL GARDEN	iii)	AREA
iv)	Eastern Cape	v)	Kwelera National Botanical Garden	vi)	East London
vii)	Free State	viii)	Free State Botanical Garden	ix)	Bloemfontein
x)	Gauteng	xi)	Pretoria National Botanical Garden	xii)	Pretoria
		xiii)	Walter Sisulu Botanical Garden	xiv)	Roodepoort
		xv)	Pretoria National Zoological Garden	xvi)	Pretoria
xvii)	KwaZulu-Natal	xviii)	KwaZulu-Natal National Botanical Garden	xix)	Pietermaritzburg
		xx)	KwaZulu-Natal Herbarium	xxi)	Durban
xxii)	Limpopo	xxiii)	Thohoyandou National Botanical Garden	xxiv)	Thohoyandou
		xxv)	Mokopane Zoological Garden	xxvi)	Mokopane
xxvii)	Mpumalanga	xxviii)	Lowveld National Botanical Garden	xxix)	Nelspruit
xxx)	Northern Cape	xxxi)	Hantam National Botanical Garden	xxxii) xxxiii)	Nieuwoudtville
xxxiv)	Western Cape	xxxv)	Kirstenbosch National Botanical Garden	xxxvi)	Cape Town
		xxxvii)	Harold Porter National Botanical Garden	xxxviii)	Betty's Bay
		xxxix)	Karoo Desert National Botanical Garden	xl)	Worcester

Invitation to tender

Tenderers are hereby invited to provide Managed Information Security Services for SANBI for a period of three (3) years.

The tender process will be co-ordinated by SANBI's Supply Chain Management (SCM) department, contactable at the following address:

Deputy Director: Supply Chain Management
The South African National Biodiversity Institute (SANBI)
Private Bag X101
Silverton
0184
Email: sanbi.tenders@sanbi.org.za

The tender closes at 11:00 on 24 April 2024.

Compulsory online briefing session and email enquiries

A virtual compulsory briefing session will take place as follows:
Date: 10 April 2023
Time: 11:00 am

Venue: Microsoft Teams, via the following link: Compulsory briefing session
A virtual compulsory briefing session will take place on **10 April 2024** from 11:00 to 12:00 on Microsoft Teams. One representative per Service Provider will be allowed to attend this virtual scheduled compulsory briefing session.

Link: https://teams.microsoft.com/l/meetup-join/19%3ameeting_NDVlYjU0YmMtMzEyMC00MjUwLTk0ZmMtYzM2ODYyNDJkOTU4%40thread.v2/0?context=%7b%22Tid%22%3a%220b847c5e-73e2-4441-8789-9c092d2dd489%22%2c%22Oid%22%3a%220c6c1cd8-b714-4173-86cc-4631abb4f1b7%22%7d

Bidders are encouraged to direct all technical and bidding procedure enquiries to the email addresses below. All responses to questions via email and at the compulsory online briefing session will be communicated via this tender's advertisement webpage on the SANBI website **www.sanbi.org**.

- For bidding procedure enquiries: sanbi.tenders@sanbi.org.za
- For technical enquiries: v.moerane@sanbi.org.za

SANBI will not respond to any technical questions received after 18 April 2023.

Scope of work

SANBI requires a Service Provider to provide managed security services to the organisation for a period of three years as per the requirements below. This will include information security resources assigned to SANBI in the following areas: information security operation, information security risk and information security governance.

Requirement of Service Provider

The prospective Service Provider is required to perform the following functions:

4.1.1. Conduct or perform the following daily **information security operations** tasks via the Security Operation Centre (SOC):

- Ensure that all applications, operating systems and firmware are kept at the latest patch level or update as required by vendors.
- Deploy and manage the anti-virus software to all devices including endpoints and servers. In addition, ensure that any virus detected is effectively removed from the network or devices.
- Manage daily user access to applications, operating systems, databases, and all other ICT resources (identity and access management)
- Conduct security audits and record all logins to the databases, servers, and operating systems, as well as log all operations performed on sensitive data.
- Implement any other required information security controls such as security certificates on web applications, encryptions as well as remedial actions from penetration tests and vulnerability assessments.
- Provide email security services.
- Implement and support network security services which includes wi-fi security.
- Provide intrusion detection and prevention.
- Implement data leak prevention.
- Conduct cyber forensic investigations and provide reports, as-and-when required by SANBI

4.1.2. Conduct or perform the following daily **information security risk** functions:

- Perform daily information security monitoring and reporting on the ICT environment, collect and analyse indicators of potential security threats, weaknesses and misconfigurations.
- Liaise with the security operations teams, share the reports and ensure that the security operations team or infrastructure team implement remedial actions to address identified weaknesses.
- Implement and manage information security incidents and response procedures. This includes analysis and investigation of security incidents on the ICT environment, providing investigation reports and recommending appropriate security measures to prevent similar incidents from reoccurring.
- Participate in ICT projects and ensure that appropriate security controls are incorporated into the solutions or systems.
- Conduct penetration tests and vulnerability assessments, as well as implement remedial actions thereof.
- Manage information security in the cloud environment.

4.1.3. Perform the following **information security governance** functions:

- Develop information security standards and procedures for applications, servers, network, databases, and endpoints.
- Conduct ongoing compliance monitoring to ensure that the ICT infrastructure is configured and managed according to security standards and procedures.
- Build information security architecture.
- Build and provide monthly and quarterly reports on the state of information security for SANBI.

Key skills and competencies required

The Service Provider must be self-motivated and results driven, with the ability to work independently and deliver efficiently on the deliverables within the timeframes required.
The Service Provider must assign three (3) information security resources to SANBI for the duration of the contract. Should it become necessary to replace any personnel during the course of this tender they may only be replaced with individuals that have similar or better qualifications or experience. The service provider must be ISO/IEC 27001certified.
The successful Service Provider's team assigned to SANBI must possess the following competencies and certifications:

- Demonstrable expertise and knowledge as an information security specialist to implement and maintain security operations, security risk and security governance functions.
- Experience in the writing and presenting of information security reports based on defined security metrics.
- Experience in conducting cyber forensic investigations on ICT systems.
- Experience in analysing and monitoring the ICT environment from a security perspective.
- Possess appropriate information security certification, such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Ethical Hacker (CEH).

The Service Provider must also have the following additional skills and competencies:

- Excellent organisational and planning skills
- Strong written and verbal communication skills

Requirements for proposals

Mandatory documents required:

Tenders must include the following documentation in their tender submission (**failure to submit this required documentation will lead to disqualification**):

- A letter of Good Standing from the office of the Compensation Commissioner as required by the Compensation for Occupational Injuries and Diseases Act (COIDA), if applicable. The letter should be issued by the Department of Labour
- A copy of the Central Suppliers Database (CSD) registration report.
- Duly completed and signed SBD forms.
- Pricing details (see Section 6). **This must only be included in the 'original' document as per the section on submission below (see Section 7). Inclusion of pricing in any 'copy' (in the PDF file(s) of the document(s) on the memory stick) will result in the tender being rejected.**
- ISO/IEC 27001 Certificate to show that the service provider is certified.

Other documentation required to undertake functionality evaluation.

Service Providers interested in this Request for Tender (RFT) should submit a concise written proposal that addresses the scope of work. Failure to submit these documents will not result in disqualification, however, the information contained in them is required for evaluation purposes. The proposal must include:

- Company profile detailing the technical information security ability of the team to fulfil the requirements of this RFT.
- Details of the Service Provider, including relevant skills, experience, competencies and track record. Short CVs (each CV not more than three (3) pages in total) of each

team member who will be involved in this work, detailing their qualifications/training, specialist skills and knowledge, and their relevant experience of similar work related to their role for this tender.
- Detailed proposal and work plan that explains how the Service Provider plans to fulfil the scope of work and requirements of the RFT.
- Contactable references of at least four current or recent clients for which similar work has been done in the last five years These must include contract duration, services rendered, referee contacts, value of contract and whether the client is satisfied with the service rendered.
- A list of at least three similar projects carried out within the past five years, with a short description of the work, including the scale of the project.

B. **Note: The budget must only be included in the 'original' document as per the section on submission below. Inclusion of pricing in the electronic copy delivered on the USB will result in the tender being rejected (see Section 7).**

Pricing

The final price, using the format provided in Annexure B, must be inclusive of VAT and will be considered the total cost for the duration of the contract. The requirements to design, plan, implement and manage the information security services are detailed in Annexure B.
The service provider will be required to make two (2) types of payments as follows:

- Once-off payment for designing the information security services and development of the information security architecture, standards and procedures.
- Annual payments for the duration of the contract (i.e. year 1, year 2 and year 3)

For this bid, the Service Provider must provide costing for professional fees (rate per month) for each information security resource assigned to SANBI in the following areas: Information Security Governance, Information Security Operations and Information Security Risk.

Submission of tender

The final price must be inclusive of VAT and will be considered the fees for the duration of the contract.

This is a two-envelope tender process. Service Providers are to submit **one (1) pack** of original proposals, marked "ORIGINAL" in an envelope, with pricing included, and **one (1) electronic copy on USB**, marked "COPY" in a second envelope. The electronic copy on USB must exclude pricing details.

Financial and pricing details must only be included in the pack marked "ORIGINAL".
NB. Failure to submit:

- one pack of original documents with pricing included; and
- one electronic copy on USB without pricing data

in the prescribed manner WILL lead to the bid being disqualified.

Tenders can be submitted in the tender box located in the reception area of the Biodiversity Centre Building at the Pretoria National Botanical Garden, 2 Cussonia Avenue, Brummeria, Pretoria, during office hours before the tender closing date and time.

Normal office hours are from 08:00 to 16:00 daily. E-mailed and faxed submissions will not be accepted. Late submissions will be disqualified.

Evaluation criteria

In accordance with the National Treasury Instruction Note on the Amended Guidelines in Respect of Bids that include Functionality as Criterion for Evaluation (issued 3 September 2010), this bid will be evaluated in the following stages:

The **first stage** will evaluate functionality according to the criteria listed in the table below:

<table>
<tr><th>Functionality Evaluation Criteria</th><th>Weight**</th></tr>
<tr><td>

Technical merit of the proposal

Technical merit of proposal including approach and understanding of the ToR in terms of:

- Design and deployment of the information security services.

<table>
<tr><th>Sub-Criteria</th><th>Points</th></tr>
<tr><td>Plan how best to approach the solution deployment</td><td>2</td></tr>
<tr><td>Design how the plan will be carried out effectively</td><td>2</td></tr>
<tr><td>Test the deployment to ensure it works as expected</td><td>2</td></tr>
<tr><td>Break the deployment into manageable sized tasks</td><td>2</td></tr>
<tr><td>Install the solution and move the activities to the production platform</td><td>2</td></tr>
</table>

- Management of the project to implement the information security services. Provide detailed project plan indicating how the project will be implemented for the three (3) security areas.

<table>
<tr><th>Sub-Criteria</th><th>Points</th></tr>
<tr><td>If no project plan submitted</td><td>0</td></tr>
<tr><td>Information security operations</td><td>4</td></tr>
<tr><td>Information security governance</td><td>3</td></tr>
<tr><td>Information security risk</td><td>3</td></tr>
</table>

</td><td>

55

(10)

(10)

</td></tr>
</table>

- Management of the daily information security operations.

Sub-Criteria	Points
If none of the security areas are not specified	0
Patch management and firmware upgrade	2
Deploy and manage anti-virus software	2
Daily user access management	2
Conduct security audits	1
Deployment and management of security certificates and encryption	1
Provide email security services	2
Manage network security services	2
Deploy and manage intrusion detection and intrusion prevention solution	1
Deploy and manage data leak prevention solution	1
Conduct cyber forensic investigation	1

(15)

- Implementing and maintaining information security governance.

Sub-Criteria	Points
If none of the security areas are not specified	0
Develop information security standards	2
Build information security architecture	2
Conduct compliance monitoring	2
Conduct information security awareness	2
Build monthly and quarterly security reports	2

(10)

- Implementing and managing information security risks.

Sub-Criteria	Points
If none of the security areas are not specified	0
Daily security monitoring	2
Security incident and response	2
Conduct compliance monitoring	2
Penetration tests and vulnerability assessment	2

	Implement remedial actions for vulnerabilities	2	(10)

Team capacity — **25**

Experience, skills and competencies of the information security resources or consultants who will be assigned to SANBI for this project

- Comprehensive CV(s) highlighting experience and skills in project management — (5)

Sub-Criteria	Points
Zero years of experience	0
1 – 2 years of experience	2
3 – 5 years of experience	3
6 or more years of experience	5

- Comprehensive CV(s) highlighting experience and skills in information security governance, information security operations and information security risk. — (15)

Sub-Criteria	Points
Zero years of experience	0
1 – 2 years of experience	5
3 – 5 years of experience	10
6 or more years of experience	15

- Comprehensive CV(s) highlighting experience and skills in information security services design and deployment. — (5)

Sub-Criteria	Points
Zero years of experience	0
1 – 2 years of experience	2
3 – 5 years of experience	3
6 or more years of experience	5

Past experience and overall track record — **20**

• Quality of references for four (4) relevant current or recent clients, within the last five years, for which similar work has been conducted The reference letters must indicate description of service, contract period, contract value and how the service provider performed or delivered the services • Ability to undertake the work, through reference to the scope and scale of similar work done for past and present clients within the last five years	(15) (5)
TOTAL	**100**

** Service Providers who fail to score a minimum of 70 points out of a possible 100 points on functionality criteria will not be eligible for further consideration.

Sufficient information must be provided to allow the Bid Evaluation Committee to evaluate bids against these functionality criteria.

The second stage will evaluate the price and preference points of those bids that meet the minimum threshold for functionality.
In accordance with the Preferential Procurement Regulations, 2022 pertaining to the Preferential Procurement Policy Framework Act (No. 5 of 2000), the 80/20 point system will be applied in evaluating proposals that qualify for further consideration, where price constitutes 80 points and a maximum of 20 points will be awarded based on the bidder's specific goals, Central Suppliers Database (CSD) report will be utilised to verify specific points claimed.

Contract period

The appointment will be for a period of three (3) years. The contractual appointment period will be as stipulated in the Independent Contract Agreement and Service Level Agreement

SANBI
Biodiversity for Life
South African National Biodiversity Institute

ANNEXURE B: QUOTATION TEMPLATE

The quotation for the work must clearly state the daily rates of the Service Provider per activity outlined in the proposed work plan, with VAT listed separately.

NB: Financial or pricing details should ONLY be included in the printed document pack marked 'ORIGINAL', and not in the PDF file(s) of the document(s) on the memory stick.

Once-Off Payment	**Cost per item/activity** (Itemise lines as required to correspond to activities set out in the proposal)	**Cost**	**VAT**	**Total cost over the contract period**
Design the information security services.		R	R	R
		R	R	R
		R	R	R
Develop information security architecture, standards and procedures.		R	R	R
		R	R	R
		R	R	R
SUB TOTAL COST				**R**

Annual Payment	**Cost per item / activity** (Itemise lines to correspond to activities set out in the proposal)	**Cost per year**	**Cost**	**VAT**	**Total cost**
Project management for information security services.		Year 1	R	R	R
		Year 2	R	R	R
		Year 3	R	R	R
Information security governance		Year 1	R	R	R
		Year 2	R	R	R
		Year 3	R	R	R
Information security operations		Year 1	R	R	R
		Year 2	R	R	R
		Year 3	R	R	R
Information security risk		Year 1	R	R	R
		Year 2	R	R	R
		Year 3	R	R	R
Professional services for all three (3) information security resources / consultants		Year 1	R	R	R
		Year 2	R	R	R
		Year 3	R	R	R

SUB TOTAL COST	**R**
GRAND TOTAL COST	**R**