Glenwood Office Park
Cnr. Oberon & Sprite Streets
Faerie Glen 0043
PO Box 73000, Lynnwood Ridge 0040
Tel: (012) 845-2000 – Fax: (012) 348-1089
Website: www.idt.org.za

Request for Quotation

RFQ Number: IDT-HO-IT- VULNERABILITY ASSESSMENTS AND PENETRATION TESTING - 22102025

Description: APPOINTMENT OF A SERVICE PROVIDER FOR PROVISION OF VULNERABILITY ASSESSMENTS AND PENETRATION TESTING

Closing Date: 31 OCTOBER 2025 @ 12:00PM

Submission of Quotations to be submitted to the following address below:

IDT Head office

Glenwood Office Park, Block B
Cnr Oberon & Sprite Street
Faerie Glen
Pretoria

on or before the closing date and time stipulated above. All quotations received after the closing date and time will not be considered.

Compulsory Returnable Documents that must be submitted with the response for this quotation are the following:

1. National Treasury Central Supplier Database number MAAA_____
2. Name of Company _____
3. Unique SARS Tax Compliance Pin Number (submit valid letter)
4. Duly completed and signed: SDB 4 (**Bidder's Declaration**), attached in this RFQ document.
5. Duly completed and signed: SDB 6.1 (Preference Points Claim Form in Terms of The Preferential Procurement Regulations 2022), attached in this RFQ document.

Compulsory returnable document: SBD 6.1

Source Documents to be submitted with the Bid or RFQ

*CIPC Document	(Company Registration Document will be required for verification (CIPC DOC))
*Woman	(Originally Certified ID Document)
*Youth	(Originally Certified ID Document)
*People with Disability	(Letter from the Dr. Confirming the Disability)
*Black Ownership	(Originally Certified ID Document)

- Non-submission of Source documents will result in the allocation of zero points for specific goals

Detailed Specifications/ Terms of Reference for this RFQ

APPOINTMENT OF A SERVICE PROVIDER FOR PROVISION OF VULNERABILITY ASSESSMENTS AND PENETRATION TESTING.

1. INTRODUCTION

The Independent Development Trust (IDT) is a public entity in South Africa established to support socio-economic development, primarily through social infrastructure delivery. As a Schedule 2 Major Public Entity reporting to Parliament through the Minister of Public Works and Infrastructure, IDT plays a crucial role in implementing government-funded development projects. To enhance its operational efficiency and ensure the alignment of its Information and Communication Technology (ICT) systems with industry best practices, IDT seeks to engage a service provider for the Appointment of a service provider for provision of vulnerability assessments and penetration testing.

2. BACKGROUND

The IDT intends to improve its control environment, and proactively protecting its information asset. The services of a competent service provider with skilled resources are required to assist the IDT to identify cyber / security / ICT vulnerabilities that the organisation's ICT environment could be exposed to and report on recommended remedies / mitigations, and to assist the IDT to address the vulnerabilities and close the gaps. The IDT is committed to implement the mitigation strategies / solutions to minimise, control and / or reduce its ICT vulnerabilities.

The IDT requires the services of a competent service provider for detection of any known or unknown vulnerabilities to prevent hacking, ransomware, data leakage, phishing, and / or insider threats. Further, for the service provider to recommend measures that will enable the IDT to comply with international best practices on technology security posture and work

together with the IDT and all its resources to implement any remedies to improve its security posture.

3. PURPOSE

To invite competent service providers with necessary experience and expertise to:

- Assess IDT systems for any known or unknown vulnerabilities on all infrastructure and systems for detection and prevention of hacking, ransomware, data leakage, phishing, and / or insider threads / exposures in line with IDT governance documentation and risk mitigation plans, and best practices;
    - Conduct cybersecurity awareness and training; and
    - Recommend and assist in the implementation of mitigation plans.

The service provider will be required to provide assurance with regards to the vulnerabilities that may exist within the hosts that operate within the IDT's network; either physical or logical.

4. SCOPE OF WORK

As part of the scope, the service provider will be required to provide the following services over the contract period:

4.1 Vulnerability Assessment

The detailed scope is as follows:

- Scan and discover ALL network devices that are connected to the IDT network;
- Assess all vulnerabilities to all network nodes and devices;
- Perform application-level vulnerability scan;
- Identify the vulnerabilities that can be detected by intruders without credentials (un-credentialed vulnerability scans);
- Identify vulnerabilities that can be detected by intruders with credentials (credentialed scans);
- Measurement of compliance to CIS (Centre for Internet Security) standards with regards to operating systems within the environment;
- Determination of whether exploits are readily available for each vulnerability identified; and
- Formulation of remedial actions to address vulnerabilities identified and shortcoming in terms of CIS compliance.

4.2 Penetration Testing

The Service Provider will be required to perform a non-intrusive penetration testing within the IDT network, which must include but not limited to the following:

4.2.1 Network

- Testing should be conducted from outside of the IDT's network;
- Assess the perimeter defence of the hosts and services exposed to the Internet;
- Conduct a Firewall Assessment;
- Perform brute force attacks;
- Perform spoofing;

4.2.2 Web Applications

For web applications, the penetration test should cover the following:

- Injection;
- Broken Authentication and Session Management;
- Cross Site Scripting;
- Insecure direct object references;
- Security misconfiguration;
- Sensitive data exposure;
- Missing function level access control;
- Cross Site Request Forgery;
- Using components with known vulnerabilities;
- Invalidated redirects and forwards.

4.3 User Awareness, Training and Skills Transfer

User Awareness:

The appointed service provider will be required to conduct training as follows:

- Regular training on cybersecurity to raise awareness, including all-inclusive training during the Cybersecurity Awareness month, which training should focus on industry trends, amongst others.

Training and Skills Transfer: The bidder's proposal must outline skills transfer plan that articulates how knowledge and skills which will be transferred to the IDT IT Team to build capacity.

The training / skills transfer plan outlines the following aspects:

- Objectives and goals of the skills transfer plan.
- Nature and scope of the knowledge and skills to be transferred (e.g., Cybersecurity governance, Policy development, Security Incident response.)

4.4 Inclusions

Is it estimated that this project will cover the following quantities:

- User devices = +/- 450
- Network devices (printers included) = +/- 75
- Web applications = +/- 10
- Servers = +/- 20 (12 Virtual and 7 Physical)

4.5 Exclusions

This is a full vulnerability assessment and penetration testing project which should include all scope required for the nature of these projects.

There are no exclusions to the scope. It is an assumption of the IDT that the bidder possesses the necessary skills set to deliver on the scope of this project. No exclusions of data in terms of best practice will be accepted in conducting this assignment.

5. PROJECT METHODOLOGY AND APPROACH

Provide 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*:

Yearly:

- Data collection.
- Penetration testing.
- Vulnerability assessments.
- Presentation of results.
- ICT capacity building.
- Cybersecurity awareness messages.

Annually:

- Vulnerability awareness during cybersecurity month

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

- Project Management methodology.
- Project Phases (based on delivery timelines).
- Project Activities.
- Timelines.
- Resource Allocations.

User Awareness, Training and Skills Transfer:

- As detailed in Section 4.3 of the ToR Document

Closeout:

- Closeout Report

6. PROJECT DURATION AND FREQUENCY OF ACTIVITIES

The project duration shall be a period of one year six months (18 months). The project duration and billing milestones shall be aligned with the Scope of Work (SoW). The SoW shall amongst others include items listed under the preceding sections (Scope of Work & Project Methodology and Approach). The first VAPT engagement to start upon signing of the appointment letter, SLA and the second VAPT engagement twelve (12) months later. IDT has offices across all the 9 provinces of South Africa, with the work to be performed at its Head Office in Pretoria.

Failure to deliver as per SoW alignment may lead to contract termination.

7. COMPANY PROFILE

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

7.1 Competent and experienced resources with more than 5 years providing similar services will be required.

7.2 Previous track record with at least 3 references of rendering similar services in the past 10 years.

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

7.4 The consulting entity must have qualified personnel in cyber security, penetration testing and familiarity with industry best practice frameworks as outlined below:

7.4.1 Certified Ethical Hacker.

7.4.2 Certified Penetration Testing Professional / CISA / CISSP.

8. DELIVERABLES AND EXPECTATIONS

The service provider must deliver the following:

8.1 A detailed report on the findings of the assignment for the scope as covered under Section 4: Scope of Work of this terms of reference. This should include:

8.1.1 A detailed security assessment report and presentation on all discovered Vulnerabilities.

8.1.2 Ratings of identified vulnerabilities in terms of likelihood and impact.

8.1.3 Provide the vulnerability raw data to IDT.

8.1.4 Immediately report any critical risk vulnerability that may be identified.

8.1.5 Recommendations on Remedial Actions for all identified vulnerabilities.

Yearly Reports: Reports must be produced yearly for the work is performed in line with the scope of work. The reports should include, but not limited to:

- Threats to the environment.
- Recommendations for remediation of identified risks, threats, and vulnerabilities prioritised based on impact, likelihood, and criticality.

Project Closeout Report: with Executive Summary presentation will be required at the end of the project. The report must include:

- key findings from the risk assessment and lead a conclusive discussion on the cybersecurity audit report.
- Summary of vulnerabilities that may have been identified during vulnerability assessments and penetration testing exercises with clear dashboard on how the services provider would have assisted the IDT to improve on its cybersecurity posture.
- Further recommendations on future work.

9. CONFIDENTIALITY TERMS AND CONDITIONS

9.1 The Service Provider shall maintain complete confidentiality and shall not share any data/information gathered during the accomplishment of the assignment, with any other person or entity without prior permission by IDT.

9.2 The Service Provider must be compliant with the requirements of the POPI Act.

9.3 IDT undertake to maintain confidentiality relating to any unpublished information supplied by the Service Provider as part as part of this Request for Proposal and will only use any information provided for the purposes of evaluating the proposal.

10. COSTING MODEL

10.1 The process objectives together with scope of work should be considered when compiling the pricing for the delivery of the services.

10.2 All costing must be projected inclusive of any applicable taxes. These costs should consider unit costs and hourly rates.

10.3 Costing must be done inclusive of any applicable travel or allowances of any kind and should therefore be inclusive of all foreseeable costs to achieve the project objectives.

NB: The below model is for illustrative purposes only.

Bidders are required to provide details costs of the project.

11. PRICING SCHEDULE

Bidders to provide further cost breakdown where necessary under each line item, and sub-total and the overall RFQ price (Total) should be included.

The table below is for illustration only:

Requirement Description **APPOINTMENT OF A SERVICE PROVIDER FOR PROVISION OF VULNERABILITY ASSESSMENTS AND PENETRATION TESTING.** **Prices are to be quoted at an all-inclusive rate.**				
Item	**Requirement Description**	**Quantity**	**Unit Price**	**Line Total**
1.	Yearly Network vulnerability assessments and penetration testing, All-inclusive, In-Scope as per Section 4 of BID Document for a period of 18 Months	**2**	**R**	**R**
2.	Annual User Awareness campaigns	**1**		
3.	Yearly ICT Training and Skills Transfer	**2**		
4.	Project Management and Handover (Closeout)	**1**		
Sub-Total				
VAT@15%				
TOTAL PRICE (INCLUDING VAT)				

Complete below:

Delivery Address: **IDT Head office**
Glenwood Office Park, Block B
Cnr Oberon & Sprite Street
Faerie Glen

1. Indicate Delivery period after order receipt…….
2. Is delivery period fixed? **Yes/No**
3. Is the price(s) fixed? **Yes/No**
4. Is the quote strictly to specification? **Yes/No**

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: ……

12. EVALUATION CRITERIA

The IDT 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 IDT Supply Chain Management (SCM) Policy.

- **RFQs received will be evaluated on Mandatory Requirements, Functional Criteria, and Price and Specific Goals comparison.**

12.1. STAGE 1A: MANDATORY REQUIREMENTS

The bidder must have qualified Lead Technical Implementer in cyber security, penetration testing and proficiency in industry best practice frameworks, a Professional who will provide Implementation leadership to the project.
Certified copies should not be older than six (06) months:

Proof of compliance:

- Bidder must attach the following professional certifications for the Lead Technical Implementer who will be involved in the project:

  o Certified copy of:

  - Valid Certified Ethical Hacking,
  - Certified Penetration Testing Professional **OR** CISA **AND** CISSP certification.

Note: Bidders that do not meet the Mandatory Requirements of set mandatory criteria will be eliminated from further evaluation process.

12.2. STAGE 1B: FUNCTIONAL EVALUATION CRITERIA

Only bidders that have met 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 will be declared non-responsive.

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

NO.	FUNCTIONAL EVALUATION CRITERIA	WEIGHT
1.	**Project Methodology and Approach** Bidders are required to provide a **detailed** Project Methodology and Approach Proposal for the services required, including all dependencies. The proposal should cover all areas of the scope of the bid including, but not limited to, the following elements: **[50 points]**.	**50**
	o Vulnerability Assessment o Penetration Testing o User Awareness, Training and Skills transfer o Reporting o Project Closeout This Project Plan should clearly indicate the following (but not limited to): o Project team and resource allocation; o Project deliverables; o Project sub-activities; and o Project timelines. **Points for Project Methodology and Approach will be allocated as follows:** • A detailed project methodology and approach that meets all the ten (10) elements **= 50 points** • A detailed project methodology and approach that meets only nine (09) elements **= 45 points** • A detailed project methodology and approach that meets only eight (08) elements **= 40 points** • A detailed project methodology and approach that meets only seven (07) elements **= 35 points** • A detailed project methodology and approach that meets only six (06) elements **= 30 points** • A detailed project methodology and approach that meets only five (05) elements **= 25 points** • A detailed project methodology and approach that meets only four (04) elements **= 20 points** • A detailed project methodology and approach that meets only three (03) elements **= 15 points** • A detailed project methodology and approach that meets only two (02) elements **= 10 points** • A detailed project methodology and approach that meets only one (01) element **= 05 points** • A project methodology and approach that meets none of the ten (10) elements or not detailed **= 0 points** **NB: all elements of the project scope must be covered in detail, no points will be awarded for project methodology and approach not detailed.**	

2. Bidder Experience and References **10**

The bidder must submit proof of relevant experience in rendering similar cybersecurity assessment projects (as outlined in the scope of work), within the past 10 years, particularly on:

- Vulnerability Assessment; and
- Penetration Testing.

Reference letters with contactable references for similar projects are required. The reference letters must be from Bidder's clients within the Republic of South Africa (RSA), must be on company letterhead, and signed by the Bidder's client: **[10 points]**.

Points for Experience and References will be allocated as follows:

- Five (05) or more signed reference letters from different clients **= 10 points**
- Four (04) signed reference letters from different clients **= 08 points**
- Three (03) signed reference letters from different clients **= 06 points**
- Two (02) signed reference letters from different clients **= 04 points**
- One signed reference letter **= 02 points**
- No reference letters submitted **= 0 points**

Important: In the event of sub-contracting, the bidder must furnish the above reference letters of the main bidder.
IDT reserves the right to contact references prior to award.

3.	**Project Team Certificates and Experience**	**40**

Profiles or CVs of key project team members to be attached, specifically for the Project Manager and Technical Lead Implementer: [**40 points**].

Project Manager. Relevant experience in Project Management, Profiles or CVs should clearly indicate the projects managed, project duration/ period, and names of clients: **[20 points]**.

Points for Project Manager experience will be allocated as follows:

- Five (05) years and above project management experience **= 20 points**
- Four (04) years and above project management experience **= 16 points**
- Three (03) years and above project management experience **= 12 points**
- Two (02) years and above project management experience **= 08 points**
- One (01) year and above project management experience **= 04 points**
- Less than one (01) year project management experience **= 0 points**

Technical Lead Implementer. Relevant experience of Project Technical Lead Security Specialist in implementing similar projects. Profile or CV should clearly indicate the projects implemented, project duration/ period, and names of clients: **[20 points].**

Points for Technical Lead Implementer experience will be allocated as follows:

- Five (05) years and above IT Security project implementation experience **= 20 points**
- Four (04) years and above IT Security project implementation experience **= 15 points**
- Three (03) years and above IT Security project implementation experience **= 09 points**
- Two (02) years and above IT Security project implementation experience **= 06 points**
- One (01) year and above IT Security project implementation experience **= 03 points**
- Less than one (01) year IT Security project implementation experience = **0 points**

Note: the projects in this factor refer to those delivered by the project team in any past company, not limited to the bidding company, i.e., linked to the individual.

MINIMUM THRESHOLD	**80**
TOTAL	**100**

Service providers must quote the IDT a total price inclusive of VAT for the service that will be rendered, and the quoted price must be valid for at least thirty (90) days after the closing date of this Request for Quotation.

- All SCM and Technical queries related to this RFQ must be submitted in writing to Ictbids@idt.org.za

NB: No query shall be allowed 12 hours prior to the closing date and time of this Request for quotation.

NB: The Independent Development Trust Reserve the right to withdraw or cancel this RFQ without prior notification to the respondents

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 interest in the enterprise, employed by the state?

YES / NO

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

Full Name	Identity Number	Name of State institution

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

2.2.1 If so, furnish particulars:

……

……

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

2.3.1 If so, furnish particulars:

……

……

3 DECLARATION

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

3.1 I have read, and I understand the contents of this disclosure.

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

3.3 The bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with any competitor. However, communication between partners in a joint venture or consortium 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

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**

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

a) 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	**90**	**80**
SPECIFIC GOALS	**10**	**20**
TARGETED GROUP		
Women	3	6
Youth	3	6
People with Disabilities	2	4
Black People	2	4
Total points for Price and SPECIFIC GOALS	**100**	**100**

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

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

2. DEFINITIONS

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

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

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

(d) **"tender for income-generating contracts"** means a written offer in the form determined by an organ of state in response to an invitation for the origination of income-generating contracts through any method envisaged in legislation that will result in a legal agreement between the organ of state and a third party that produces revenue for the organ of state, and includes, but is not limited to, leasing and disposal of assets and concession contracts, excluding direct sales and disposal of assets through public auctions; and

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

3. FORMULAE FOR PROCUREMENT OF GOODS AND SERVICES

3.1. POINTS AWARDED FOR PRICE

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

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

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

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

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**

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

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)
Women	3	6		
Youth	3	6		
People with Disabilities	2	4		
Black People	2	4		

Source Documents to be submitted with the Bid or RFQ

*CIPC Document	(Company Registration Document will be required for verification (CIPC DOC))
*Woman	(Originally Certified ID Document)
*Youth	(Originally Certified ID Document)
*People with Disability	(Letter from the Dr. Confirming the Disability)
*Black Ownership	(Originally Certified ID Document)

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: ……

……

……

……